



SCMS SCHOOL OF ENGINEERING AND TECHNOLOGY, KARUKUTTY

3.3.1 Number of research papers published per teacher in the Journals notified on UGC CARE list during 2018-2019

Sl. No.	Title of paper	Name of the author/s	Department of the teacher	Name of journal	Calendar Year of publication	ISSN number	Link to the recognition in UGC enlistment of the Journal /Digital Object Identifier (doi) number		
							Link to website of the Journal	Link to article / paper / abstract of the article	Is it listed in UGC Care list
1	In search of a self in the novels The Bluest Eye by Toni Morrison and The God of Small Things by Arundati Roy	Jane Theresa	Basic Science and Humanities	Pune Research, An Internal Journal of Research In English	October 2018	ISSN 2454-3454	http://puneresearch.com/english	http://puneresearch.com/media/data/issues/5b8eca/56340900.pdf	UGC CARE
2	Comparison of classifier strength for detection of retinal hemorrhages	Sreeja K A	ECE	International Journal of Innovative Technology and Exploring Engineering, 2019, 8(6), pp. 688-693	April 2019	ISSN: 2278-3075	https://www.ijitee.org/	https://www.ijitee.org/wp-content/uploads/papers/v8i6s3/F11370486S319.pdf	SCOPUS
3	Hybrid brainactuated muscle interface for the physically disabled	Vinoj P.G	ECE	Basic & Clinical Pharmacology & Toxicology Journal	August 2018	ISSN:1742-7843	https://onlinelibrary.wiley.com/page/journal/17427843/homepage/forauthors.html	https://onlinelibrary.wiley.com/doi/10.1111/bcpt.13100	SCI

4	An Experimental Investigation on Wear and Corrosion Characteristics of Mg-Co Nan	Sajith E	ME	Materials Research Express	June 2018	10.1088/2053-1591/aac862	https://iopscience.iop.org/journal/2053-1591	https://iopscience.iop.org/article/10.1088/2053-1591/aac862/meta	SCI
5	Parametric Study of Heat Transfer and Pressure Drop Characteristics of a Rectangular Offset Strip Fin Compact Heat Exchanger	Dr. Ajith Kumar R	ME	Chemical Engineering Transactions	December 2018	ISSN: 1381-1386.	https://www.aidic.it/cet/	https://www.cetjournal.it/index.php/cet/article/view/CET1871231	SCOPUS
6	Numerical study on the influence of mass and stiffness ratios on the vortex induced motion of an elastically mounted cylinder for harnessing power	Dr. Sheeja Janardhanan	ME	Energies	SEPT 2018	EISSN 1996-1073	https://www.mdpi.com/journal/energies	https://www.mdpi.com/1996-1073/11/10/2580	SCI
7	Effect of Copper Slag and Granite Powder on the Mechanical Properties of Reclaimed Asphalt Pavement Aggregate Concrete	Aswini .J	CE	International Journal of Sustainable Construction Engineering & Technology	December 2018	ISSN : 2180-3242	https://publisher.uthm.edu.my/ojs/index.php/IJSCET/article/view/2707	https://publisher.uthm.edu.my/ojs/index.php/IJSCET/article/view/2707	SCOPUS

8	Identification of Android malware using refined system calls	Dr Vinod P	CSE	Concurrency and Computation	May 2019	ISSN:1532-0634	https://onlinelibrary.wiley.com/journal/15320634	https://onlinelibrary.wiley.com/doi/10.1002/cpe.5311	SCI
9	A Secure Reversible Data Hiding System for Embedding EPR in Medical Images	Dr Varun G Menon	CSE	Current Signal Transduction Therapy	January 2019	ISSN :1574-3624	https://benthamscience.com/public/journals/current-signal-transduction-therapy	http://www.eurekaselect.com/article/97053	SCOPUS
10	A Secure and Efficient Lightweight Symmetric Encryption Scheme for Transfer of Text Files between Embedded IoT Devices	Dr Varun G Menon	CSE	Symmetry	February 2019	ISSN: 2073-8994	https://www.mdpi.com/journal/symmetry	https://www.mdpi.com/2073-8994/11/2/293	SCI
11	A machine learning based approach to detect malicious android apps using discriminant system calls	Dr Vinod P	CSE	Future Generation Computer Systems	May 2019	ISSN: 1872-7115	https://www.sciencedirect.com/journal/future-generation-computer-systems	https://www.sciencedirect.com/science/article/abs/pii/S0167739X18306216	SCI
Total number of research papers published per teacher in the Journals notified on UGC CARE list during 2018-2019									11



Joshi
PRINCIPAL
 SCMS SCHOOL OF ENGINEERING & TECH
 VIDYANAGAR, PALLISSERY, KARUK
 ERNAKULAM, KERALA-683 57

Parametric Study of Heat Transfer and Pressure Drop Characteristics of a Rectangular Offset Strip Fin Compact Heat Exchanger

 Rahul VR^a, Ajith Kumar R^{b,*}
^a Vidya Academy of Science and Technology, Thrissur

^b SCMS School of Engineering and Technology, Ernakulam
 ajithscms@gmail.com

Compact heat exchangers are of great topics of interest while we are dealing with the enhancement of heat transfer rate. In this study, a rectangular offset strip fin compact heat exchanger is taken into consideration. The purpose of this study is to develop a numerical model to study the heat transfer characteristics as well as the pressure drop characteristics. The parametric study was done in FLUENT with a three dimensional computational domain in which air is selected as working fluid. The analysis was confined to the flow in laminar region and so the Reynolds number was limited to 1000. The variation of friction factor and Colburn factor with Reynolds number is also analysed. The results obtained were analysed and were also compared with an existing correlation. The findings of this study may serve as a helping tool to develop a correlation for fluid flow in offset strip fin geometry.

1. Introduction

The compact heat exchangers are defined as those heat exchangers having ratio of the heat transfer surface area to its volume, β (area density) greater than or equal to $700 \text{ m}^2/\text{m}^3$. Compact heat exchangers are commonly used in gas-to-gas and gas-to-liquid (or liquid-to-gas) heat exchangers to counteract with the low heat transfer coefficient associated with gas flow with increased surface area. They found applications in many engineering sectors such as refrigeration, power, automotive, process, cryogenics etc. Various types of plate fin compact heat exchanger surfaces such as plain rectangular, plain trapezoidal, offset strip fin, wavy, louvered and perforated configurations are available. Here a rectangular offset strip fin heat exchanger is considered. They cause high heat transfer enhancement when compared to other surface configurations. This is due to the breaking or interruption of boundary layers formed on the uninterrupted fin surface and their dissipation in the fin wakes.

The monograph on the experimental investigations on offset strip fin geometry by (Kays et al., 1984) is still being used as a sourcebook. (Joshi et al., 1987) presented analytical models to predict the heat transfer coefficient and friction factor of offset strip fin geometry in both laminar and turbulent regimes. (Wieting 1975) developed empirical correlations for heat transfer and flow friction characteristics of offset strip fin geometry for Reynolds numbers in both laminar and turbulent ranges excluding the intermediate transition region. (Manglik et al., 1995) too developed single heat transfer and pressure drop correlations for all flow regimes after reanalysing previous experimental studies. (Saidi et al., 2001) conducted a numerical investigation of heat transfer enhancement in offset strip fin surface in self- sustained oscillatory flows. (Bhowmik et al., 2009) used a three-dimensional model to study the heat transfer and pressure drop characteristics of offset strip fin geometry with water as working medium. (Asadi et al., 2013) conducted case studies on the functions of friction and colburn factors in compact heat exchangers. (Muzychka et al., 2009) presented a model for thermal – hydraulic characteristics for offset strip fin geometry for large Prandtl number liquids. This study mainly focuses on analysing the heat transfer and pressure drop characteristics of offset strip fin geometry. The basic offset strip fin geometry is shown in figure 1. As per the experiments conducted and correlations developed by (Wieting 1975), the flow with Reynolds number ≤ 1000 is primarily laminar and flow having

Reynolds number range ≥ 2000 is primarily turbulent. In this study we are only dealing with laminar flow. The heat transfer enhancement in offset strip fin is due to the periodic starting and formation of boundary layers over the fin length and their dissipation in fin wakes.

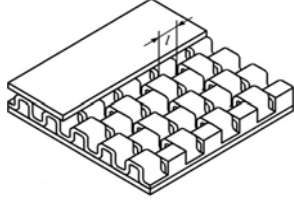


Figure 1: Offset strip fin geometry

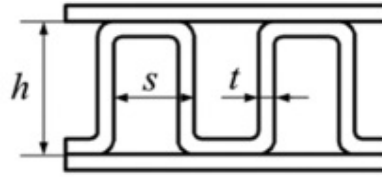


Figure 2: Nomenclature of offset strip fin

2. Problem description

The initial dimensions chosen were from the geometry designated as $\frac{1}{4}$ (s) – 11.1 used by (Kays et al., 1984). A three-dimensional computation domain was created using Solidworks as shown in figure 3. This simplification is based on the assumption that the flow is fully developed and it shows a periodic pattern (fully developed periodic flow). ANSYS FLUENT was used for studying heat transfer and pressure drop characteristics.

As the flow in the offset strip fin geometry shows a fully developed periodic pattern, the inlet and outlet sections were given periodic boundary condition. The fins and the parting sheets were specified to be in isothermal condition (350 K). No slip condition was given for wall boundaries. The material for fin was specified as aluminium and the working fluid as air. The air is modelled as an ideal incompressible gas. The air enters the offset strip fin geometry at a low temperature (249 K) and as it flows through the geometry, the temperature of air increases.

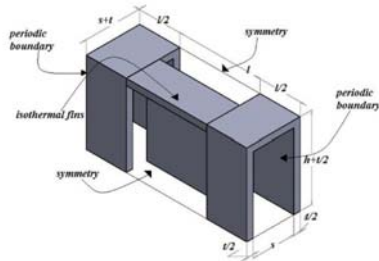


Figure 3: Computational domain

In this study a pressure-based solver was used. The semi implicit method for pressure – linked equation (SIMPLE) was used to solve the continuity, momentum and energy equations. The fluid flow was considered to be steady and incompressible. A convergence criterion of 10^{-4} was selected for the continuity and momentum equations and a convergence criterion of 10^{-6} was selected for the energy equation.

The continuity equation is given by:

$$\frac{\partial(\rho u)}{\partial x} + \frac{\partial(\rho v)}{\partial y} + \frac{\partial(\rho w)}{\partial z} = 0 \quad (1)$$

The momentum equation in x-direction is given by:

$$\rho \left(u \frac{\partial u}{\partial x} + v \frac{\partial v}{\partial y} + w \frac{\partial w}{\partial z} \right) = -\frac{\partial P}{\partial x} + \mu \left(\frac{\partial^2 u}{\partial x^2} + \frac{\partial^2 u}{\partial y^2} + \frac{\partial^2 u}{\partial z^2} \right) \quad (2)$$

The Reynolds number for the flow is given by:

$$Re = \frac{U_c D_h}{\nu} \quad (3)$$

Now the free flow area denoted as A_{ff} for the computational domain can be written as, $A_{ff} = sh$. The hydraulic diameter D_h is given by:

$$D_h = \frac{4 A_{ff}}{A/l} = \frac{4shl}{2(sl+hl+th)+ts} \quad (4)$$

The friction factor f is given by:

$$f = \frac{2\Delta P}{\rho U_c} \left(\frac{D_h}{4 L_m} \right) \quad (5)$$

The Colburn j factor is given by:

$$j = \frac{\bar{h} Pr^{2/3}}{\rho C_p U_m} \quad (6)$$

3. Results and discussions

The computational domain was analysed in FLUENT and the obtained results were compared with an existing correlation made by Manglik & Bergles (1995). They had given the correlations for the friction factor as well as for the Colburn factor. The correlations were:

$$f = \frac{9.6243 Re^{-0.7422} \alpha^{-0.1856} \delta^{0.3053} \gamma^{-0.2659}}{1 + (7.669 \times 10^{-8} Re^{4.429} \alpha^{0.920} \delta^{3.767} \gamma^{0.236})} \quad (7)$$

$$j = \frac{0.6522 Re^{-0.5403} \alpha^{-0.1541} \delta^{0.1499} \gamma^{-0.0678}}{1 + (5.269 \times 10^{-5} Re^{1.340} \alpha^{0.504} \delta^{30.456} \gamma^{-1.055})} \quad (8)$$

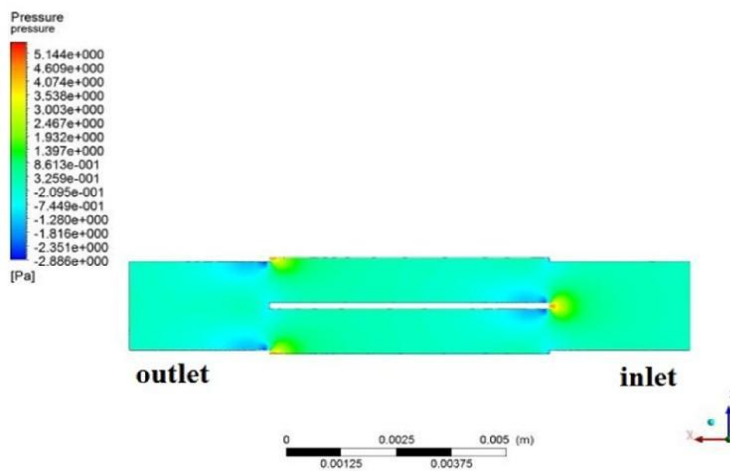


Figure 4: Pressure contour

The pressure, temperature and velocity contours for a flow through an offset strip fin geometry ($Re = 500$) are shown in figures 4, 5 and 6 respectively. It was observed that there occurs a pressure drop as the fluid flows through the offset strip fin geometry. Also, the periodic behaviour of the flow can clearly be observed from the velocity contour.

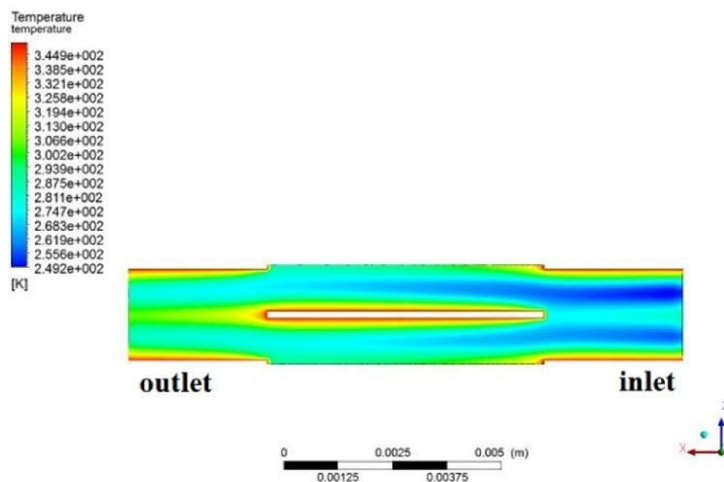


Figure 5: Temperature contour

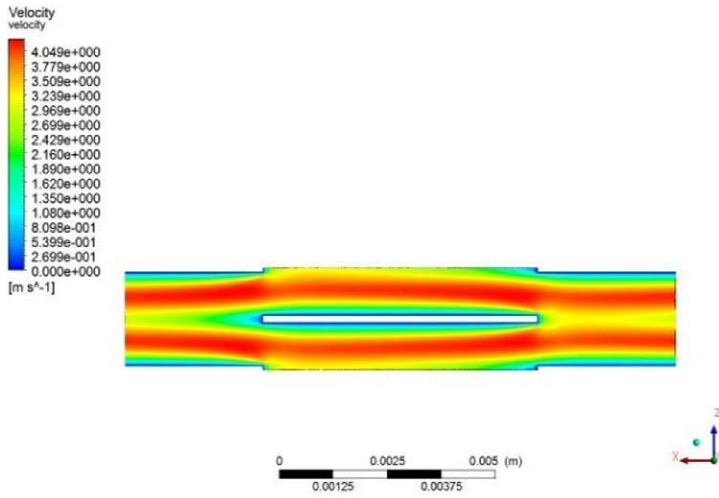


Figure 6: Velocity contour

3.1 Variation of f and j factors with Reynolds number

Initially, the variation of f and j factors with respect to Reynolds number was analysed. From the figure 7 below it is clear that the functions of f and j factors decrease with increasing Reynolds number. At lower flow velocities the air spends more time around the fins and thus it helps in enhancing the heat transfer rate. As the flow velocity increases the time spend by air around the fins decreases resulting in less heat transfer. The computed results of f factor obtained were very close to the values predicted by the Manglik & Bergles correlation, and the j factors deviated by about 12%. And also, the values of friction factors were about 10 times the values of j factors at the same Reynolds number.

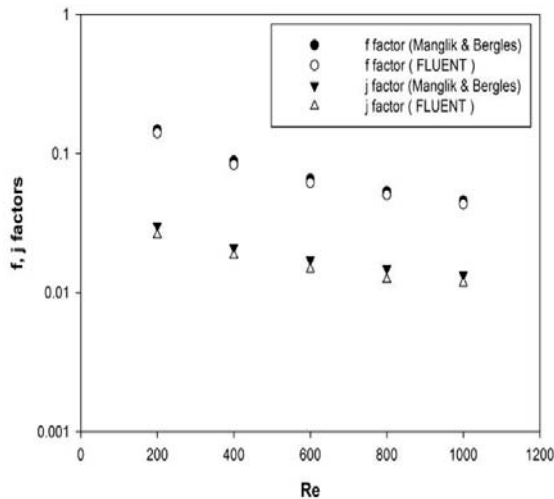


Figure 7: Variation of f and j factors with Reynolds number

3.2 Variation of f and j factors with dimensionless parameter α

Now the heat transfer and pressure drop characteristics of the offset strip fin geometry was analysed by varying the dimensionless parameter $\alpha = s/h$. The dimensionless parameter α was varied by changing the fin height h . The variation of f & j factors with variation of α is shown in figure 8. At low values of α , the functions of f and j factors are high and the trend shows that the f and j factors decrease with increasing values of α .

The f and j factor variation obtained by FLUENT with respect to α , deviated from the predicted f factor by about 5% and the from the predicted j factor by about 12%.

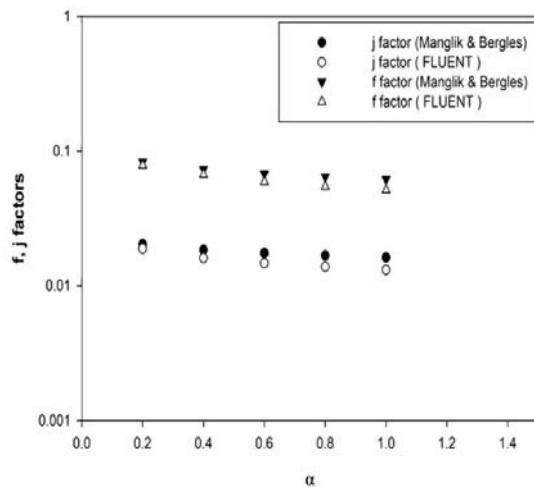


Figure 8: Variation of f and j factors with dimensionless parameter α

3.3 Variation of f and j factors with dimensionless parameter δ

The f & j factor variations with respect to the dimensionless parameter $\delta = t/l$ was also obtained. Both the offset fin length and fin thickness will have an influence on the flow field. When the fins are thicker, they offer large form drag. Also, in an offset strip fin geometry having smaller offset fin length, the breaking of boundary layers formed on the uninterrupted fin length and their dissipation in fin wakes will be more often when compared to a geometry having larger offset fin length. As a result, the pressure drops and colburn j factor tends to increase. As indicated in the figure 9, the functions of f and j factor increases with increase in δ . In this study, the δ was varied by changing the fin uninterrupted length l . So, for large values of δ , the offset fin length was small resulting in higher values of f and j factors. The deviation of friction factor data obtained from FLUENT deviated from the existing values by about 8% and the deviation in case of colburn factor was found to be 10%.

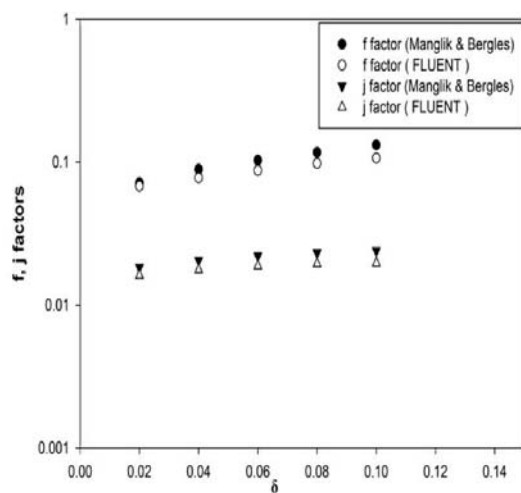


Figure 9: Variation of f and j factors with dimensionless parameter δ

4. Conclusions

In this study, a three dimensional parametric analysis of a rectangular offset strip fin heat exchanger using ANSYS FLUENT 14.0 was carried out. The analysis was carried out for Reynolds number ≤ 1000 . A three-dimensional computational domain was created and suitable boundary conditions were defined. The heat

transfer characteristics and pressure drop characteristics were analysed by varying dimensionless parameters such as Reynolds number, $\alpha = s/h$, $\delta = t/l$. The results show that f & j factors decrease with respect to increase in Reynolds number and $\alpha = s/h$. On the other hand, f & j factors increase with respect to increase in $\delta = t/l$. It was also found that the main factors influencing the design of a compact heat exchanger are Colburn j factor and Fanning friction factor.

Nomenclature

A_{ff}	free flow area
D_h	hydraulic diameter
f	friction factor
h	fin height
\bar{h}	mean heat transfer coefficient
j	colburn factor
l	offset fin length
L_m	length of computational module
Pr	Prandtl number
Re	Reynolds number
s	fin spacing
t	fin thickness
U_m	mean velocity
U_c	velocity at minimum free flow area
μ	dynamic viscosity
ν	kinematic viscosity
ρ	density
P	pressure
u	velocity component in x direction
v	velocity component in y direction
w	velocity component in z direction

References

- Asadi M., Nadali A., 2013, Study on the functions of friction and colburn factors in compact heat exchanger, *Wyno Academic Journal of Engineering & Technology Research*, 4, 37-48.
- Bhowmik H., Kwan-Soo Lee, 2009, Analysis of heat transfer and pressure drop characteristics in an offset strip fin heat exchanger, *International Communications in Heat and Mass Transfer*, 36, 259 – 263.
- Dong J.Q., Chen J.P., Chen Z.J., Zhou Y.M., 2007, Air-side thermal hydraulic performance of offset strip fin aluminum heat exchangers, *Applied Thermal Engineering*, 27, 306–313. DOI: 10.1016/j.applthermaleng.2006.08.005
- Joshi H.M., Webb R.L., 1987, Heat transfer and friction in the offset strip fin heat exchangers, *International Journal of Heat and Mass Transfer*, 30, 69 – 84.
- Kays W.M., London A.L., 1984, *Compact Heat Exchangers*, 3rd ed. McGraw-Hill, New York.
- Manglik. R.M., Bergles A.E., 1995, Heat transfer and pressure drop correlations for the rectangular offset strip fin compact heat exchanger, *Experimental Thermal Fluid Science*, 10, 171–180. DOI: 10.1016/0894-1777(94)00096-Q
- Muzychka Y.S., Kenway G., 2009, A model for thermal-hydraulic characteristics of offset strip fin arrays for large Prandtl number liquids, *Journal of Enhanced Heat Transfer*, 16, 73–92.
- Saad S.B., Clément P., Fourmigué J.F., Gentric C., Leclerc J.P., 2012, Single phase pressure drop and two-phase distribution in an offset strip fin compact heat exchanger, *Applied Thermal Engineering*, 49, 99–105. DOI: 10.1016/j.applthermaleng.2011.09.022
- Saidi A., Sunden B., 2001, A numerical investigation of heat transfer enhancement in offset strip fin heat exchangers in self-sustained oscillatory flows, *International Journal of Numerical Methods for Heat & Fluid Flow*, 11, 699-716. DOI: 10.1108/eum000000005984
- Wieting A.R., 1975, Empirical correlations for heat transfer and flow friction characteristics of rectangular offset-fin plate – fin heat exchangers, *International Journal of Heat and Mass Transfer*, 97, 488–490.

Effect of Copper Slag and Granite Powder on the Mechanical Properties of Reclaimed Asphalt Pavement Aggregate Concrete

T.Mahitha¹, J. Aswini²

^{1,2} Department of civil engineering, APJ Abdul Kalam Technological University, Calicut, India

*Corresponding E-mail: mahi.thodiyil@gmail.com

Received 24 May 2018; Revised 20 November 2018; Accepted 5 December 2018

DOI: <https://10.30880/ijscet.2018.09.02.001>

Abstract

The replacement of natural gravel aggregate with reclaimed asphalt as coarse aggregate would help in reduction of environmental and ecological effects. Researches were rarely performed by replacing fine aggregate in reclaimed asphalt pavement aggregate concrete. This project aims to investigate the feasibility of improving the strength of recycled asphalt aggregate concrete in which recycled asphalt aggregate is used as a partial replacement of coarse aggregate at 30%. Abrasion and attrition technique is used to modify or roughen the surface of RAP aggregates. Granite powder and copper slag are used as a partial replacement of sand at 5, 10, 15, 20 and 25% in Abrasion and attrition Treated Reclaimed Asphalt Pavement Aggregate Concrete (ABTRAPC). Thirty cubes, twenty cylinders and twenty beams of concrete with granite powder and thirty cubes, twenty cylinders and ten beams of concrete with copper slag were made and tested. The 7th and 28th day strengths were found out at these replacements. It was observed that the compressive strength, split tensile strength and flexural strength was found to be maximum at 15% replacement of sand by copper slag. The compressive strength was increased about 29.8% compared to ABTRAPC. Flexural strength similar to normal concrete and about 12.8% greater compared to ABTRAP concrete. The compressive strength and flexural strength was also increased to a maximum at 15% replacement of sand by granite powder and split tensile strength at 20% replacement of granite powder. The results showed that the potential of reclaimed asphalt aggregates as a partial replacement of coarse aggregates in concrete could be effectively enhanced with its a combination with granite powder or copper slag. The increase in compressive strength values and the increase in flexural strength values similar to normal concrete proved that this concrete has its potential to be used in pavement applications.

Keywords: *Reclaimed asphalt pavement aggregate, Abrasion, and attrition, Copper slag, Granite powder, Compressive strength, Flexural strength, Split tensile strength, Sustainability*

1.0 Introduction

The current concrete construction practice is thought unsustainable due to the consumption of enormous quantities of stone, sand, drinking water and cement. To move towards ecological sustainability, we must move on to low cost and highly durable concrete mixtures containing largest possible amounts of industrial and urban byproducts that could be suitable as a partial replacement of Portland cement, aggregate and drinking water. Natural aggregate accounts for more than 70% of the volume of concrete. The increasing demand for quality natural aggregates and the subsequent effects on the environment led to the need to consider locally and cheaply available materials in concrete.

India has the second largest road network in the world. Reclaimed Asphalt Pavement (RAP) is the removed pavement materials composed of asphalt and aggregates. These materials are produced when asphalt pavements are removed during reconstruction and resurfacing. The replacement of gravel aggregate with reclaimed asphalt would also help in reducing the quantity of reclaimed asphalt which would otherwise be disposed of in landfill sites. The applications of concrete containing recycled asphalt have been very limited due to its low strength. Thus there is a need to find methods to improve the properties of concrete containing RAP as partial replacement of coarse aggregate. Partial replacement of fine aggregate of this concrete containing RAP with a suitable cheap and recyclable material is an interesting area of study. Granite powder is obtained as

a by-product from granite cutting or polishing industries. Granite powder is also generated from recycling marble tops, granite pavers and stone scraps. This powder is deposited in large amounts causing a threat to the environment. Inhalation of fine dust of granite powder causes lung diseases. The use of granite powder in concrete would minimize its effect on the environment. Copper slag is an industrial by-product material produced from the process of manufacturing copper. Approximately 24.6 million tons of slags are estimated to be generated from the copper industries in the world. Some amount of copper slag is mainly used in the sand blasting industry and in the manufacturing of abrasive tools and the remaining is disposed of in the ecosystem without any reuse.

2.0 Literature Review

Reference [1] studied on fine fraction of Reclaimed Asphalt Pavement (RAP) aggregates as an alternative to natural fine aggregates. Cement mortar samples were prepared with 25%, 50%, 75% and 100% replacement of natural aggregates. The decrease in strength of cement mortar may be due to the increase in the porosity of Interfacial Transition Zone (ITZ) and the predominance of asphalt-cohesion failure in comparison to asphalt adhesion failure. It also opens up the scope to incorporate mineral admixtures in mortar mixes to improve the strength of the same with a higher percentage of RAP content. Reference [2] investigated the effect of using copper slag replacement by preparing eight concrete mixes with different proportions of copper slag (0-100%). The compressive, tensile and flexural strength of concrete was comparable to the control mix using up to 50% copper slag. Copper slag, in the range of 40–50%, could potentially replace sand in concrete mixtures. Al-Mufti et al. [3] investigated improving the strength properties of recycled asphalt aggregate concrete. Replacement of 20 mm gravel with recycled asphalt aggregate at 25%, 50%, 75% were compared with 100% recycled asphalt aggregate concrete and control concrete. A replacement of 25% reduces 28 days strength by 27%. Further increase in replacement results in further reduction in strength but at a more reduced rate. Roughening of aggregate prior to mixing for 3 hour increases the strength reaching similar strength to normal concrete. Roughening of recycled asphalt aggregate alone for 3 hours made a limited improvement in concrete strength. The treatment of recycled asphalt aggregate with solvent turpentine has no effect on strength development of concrete.

Reference [4] studied bonding properties in cementitious materials with asphalt-coated particles. Interfacial Transition Zone (ITZ) properties and phase distribution with age of reclaimed asphalt showed high porosity, larger ITZ size, low CH and CSH contents near the interface. This caused a reduction in concrete strength and bulk modulus. Hydrophobic nature of asphalt prevented hydration products from growing around aggregate in larger and porous ITZ. Mortars with RAP showed a decreasing trend in the CH content near the aggregate interface suggesting that somehow asphalt is preventing CH growth. Even though the silica fume decreased the porosity to some extent, the CH content is found to reduce with age due to the pozzolanic reaction of silica fume. Reference [5] studied the nature of the cement-asphalt bond. The interfacial cement-asphalt bond energy was found to improve by several chemical oxidative treatments of the asphalt without affecting the porosity and size factors in the ITZ. Asphalt cohesion is found out to be as the preferential failure mode than the cement-asphalt adhesion or ITZ cohesion. A lower bulk modulus is produced due to the higher porosity in ITZ which allows for easier crack initiation, and the preferential asphalt cohesion failure. An improvement in the concrete the mechanical properties in concrete with RAP aggregates would be improved by increasing the cohesive strength of the asphalt coating thus driving the failure mode to an asphalt-cement adhesive and decreasing the ITZ porosity. Reference [6] studied the use of fractionated reclaimed asphalt pavement (FRAP) as a partial replacement (0%, 20%, 35%, and 50%) of coarse aggregate in a ternary blend concrete containing cement, slag, and fly ash. The increase in the percentage of FRAP in concrete resulted in a decrease in the compressive, split tensile, and flexural strength. The elastic and dynamic moduli also decreased with increasing FRAP content. The results of the study indicated that up to 35% FRAP can be replaced as coarse aggregates while still meeting the sufficient fresh, strength, and durability

specifications of conventional concrete. Dirty FRAP without washing was found to meet the IDOT compressive strength requirements up to 50% replacement. Reference [7] studied on the potential of blasted copper slag as fine aggregate in Portland cement concrete. The greatest reductions of compressive strength were found when the replacement was over 40%.

Reference [8] conducted studies on soft and hard bitumen from unaged, aged recycled asphalt concrete mixtures for rheological, thermal, microstructural aspects. Bitumen with 50% weight of virgin bitumen and 50% from recycled asphalt pavements were studied. Aging and recycling changed rheological properties of soft bitumen by increasing complex modulus and decreasing phase angle. Recycled asphalt pavement bitumen has an adverse effect on adhesion properties. Reference [9] conducted an experimental study of concrete made with granite and iron powders as partial replacement of sand. The test resulted showed that for 10% ratio of granite powder in concrete, the increase in compressive strength was about 30% compared to normal concrete. Similar results were obtained for flexure. For replacement, up to 20% of sand by weight with iron powder in concrete resulted in an increase in compressive and flexural strength.

Reference [10] conducted studies on experiments with control concrete with natural sand and gravel, concrete with reclaimed coarse and reclaimed fine aggregate, concrete with reclaimed coarse and natural sand, and concrete mix with reclaimed coarse and natural sand where 30% OPC replaced with flash. Concrete made with reclaimed coarse asphalt aggregates and sand showed less reduction in strength compared to others. Reference [11] studied on RAP aggregate materials treated with different dosages of portland type I/II cement and with alkali-resistant glass fibers. Reference [12] investigated on portland cement concrete containing recycled asphalt aggregate. Soft asphalt binder induces stress concentration and microcracking in concrete matrix causing a reduction in strength. Concrete made with only coarse RAP showed the least reduction in strength and a significant increase in toughness. Compared with rubber, RAP had a better chance of replacement in concrete. Reference [13] studied the durability of copper slag contained concrete exposed to sulfate attack. Replacement of cement with copper slag up to 15% led to more than 50% decrease in sulfate expansion. Reference [14] experimentally investigated the feasibility of granite powder waste as a possible replacement in manufacturing concrete. At 0.5 water to cement ratio, experiments were done for 10, 25, 40, 55 and 70% sand replacement by granite powder. Compressive strength results for 7, 28, and 56 days were highest at 25% replacement and lowest at 70% replacement.

Reference [15] studied the effect of incorporating Dirty RAP (DRAP) Washed RAP (WRAP), and Abrasion and Attrition (AB&AT) treated RAP on the fresh, mechanical and durability properties of concrete and compared with each other as well as normal aggregate concrete. Beneficiation of RAP by AB&AT method increased the compressive strength of concrete by 9.74% and 12.21% and flexural strength by 6.05% and 8.55% as compared to WRAP and DRAP inclusive concrete. ABTRAP aggregates were found to possess both the desirable properties of RAP as well as natural aggregates. Aggregates processed with both washing and AB&AT method resulted in better workability than natural aggregate concrete. Reference [16] studied on improving the properties of ABTRAP (Beneficiated RAP aggregates by Abrasion & Attrition technique) inclusive concrete by incorporating mineral admixtures such as Silica Fume (SF), Fly ash (FA) and Sugarcane Bagasse Ash (SCBA). 6 mixes were prepared by partially replacing Ordinary Portland Cement (OPC) by SF (5% & 10%), FA (10% & 20%) and SCBA (5% & 10%). Maximum improvement in compressive, flexural and split tensile strength of ABTRAPC mix was found when 10% OPC was partially replaced by SF followed by 20% replacement by FA and 5% replacement by SCBA.

Reference [17] found out that replacement of 10% cement by BGA was found to increase the compressive strength by 15%, modulus of rupture by 12%, and splitting strength by 13% compared to concrete containing 100% RAP aggregates. Shi et al. [18] investigated the viability of partial replacement of virgin coarse aggregate by coarse RAP to formulate PCC paving mixtures. Replacing virgin coarse aggregate by RAP in a typical PCC pavement mix has caused a reduction in strength and modulus of elasticity. The coarse RAP with sufficient intermediate size particles can help to make dense graded RAP-PCC mixtures which can show better workability and

mechanical properties compared to other gap-graded RAP-PCC mixtures. Reference [19] studied the strength and durability properties of concrete made with granite industry waste. The obtained test results were indicated that the replacement of natural sand by GP waste up to 15% of any formulation is favorable for the concrete making without adversely affecting the strength and durability criteria.

Reference [21] investigated the effect of using alternatives for both fine and coarse aggregates with copper slag (30%, 40% and 50%), iron slag (30%, 40% and 50%) and recycled concrete aggregate (20%, 25% and 30%) with various proportions of mix by the partial replacement of sand and gravel respectively. From the study, it has been concluded that 40% of copper slag, 40% iron slag and 25% of recycled concrete aggregate possess more strength than a conventional concrete mix. Reference [22-23] studied the interactions between granites and asphalts based on theology. Different granite powders and asphalt showed significant differences in their interactions and this compatibility problem between asphalt and granite should be considered during the choice of materials.

3.0 Research Significance

Granite powder and copper slag are industrial by-products obtained from the granite cutting and copper manufacturing industries. These can be used as partial replacement of sand in concrete. RAP aggregates are obtained during the reconstruction or resurfacing of pavements. These aggregates, when used as coarse aggregate in concrete, have shown to decrease the mechanical properties of concrete. The modification of RAP coarse aggregates by abrasion and attrition and the partial replacement of sand in the concrete by granite powder or copper slag is an interesting area of research. The use of RAP aggregates, granite powder and copper slag in concrete will reduce the consumption of natural resources in the construction process. The health hazards and the effects on the ecosystem will also be reduced by the recycling of these byproducts.

4.0 Experimental Investigation

The experimental investigation comprised of preparing specimens of normal concrete, concrete with RAP aggregate replaced as coarse aggregate at 100%, concrete with RAP aggregate replaced as coarse aggregate at 30%, concrete with RAP aggregate replaced as coarse aggregate at 30% after abrasion, and abrasion treated RAP concrete with granite powder or copper slag replacement. The specimens comprised of concrete cubes, beams, and cylinders for testing the compressive strength, flexural strength and split tensile strength respectively. The concrete mix consists of Portland Pozzolana Cement, coarse aggregates, RAP aggregates, m-sand, granite powder or copper slag, superplasticizer and water.

4.1. Materials

The materials used for the study included Portland Pozzolana Cement coarse aggregates (gravel) RAP aggregates, fine aggregates (m-sand), granite powder, copper slag, superplasticizer, and water. Portland Pozzolana Cement (PPC) conforming to (IS 1489 part1) fly ash based is used for the experimental work. The specific gravity of cement is 2.89 found using le chatelier flask method as per IS 2720 part3. Reclaimed Asphalt Pavement aggregates and natural aggregates are used as coarse aggregates in this experiment. Reclaimed Asphalt Pavement Aggregates were collected from the highway works in Calicut. Dirty Reclaimed Asphalt Pavement Aggregates were used for the work without washing. Natural coarse aggregates of size passing through 20 mm sieve and retained on 12.5 mm sieve are taken. Reclaimed Asphalt Pavement aggregates of size passing through 20 mm sieve and retained on 12.5 mm sieve are taken. The specific gravity of coarse aggregates and RAP aggregates are 2.66 and 2.35 respectively. M-Sand, granite powder and copper slag are used as fine aggregates. Granite powder is collected from Cemal Gems & Minerals,

Bangalore. Copper slag is collected from Blastine private Limited, Koratty, Kerala. Chemical composition analysis results for granite powder and copper slag were obtained from their suppliers i.e. Cemal Gems & Minerals and Blastine private limited respectively. The chemical composition of granite powder and copper slag are given in Table 1 and Table 2 respectively. Specific gravities of m-sand, granite powder, and copper slag are 2.6, 2.5 and 3.2 respectively found out using a pycnometer test as per IS-2386 part-3. Fineness modulus of m-sand, granite powder, and copper slag are 3.44, 2.64 and 3.43 respectively. Sieve analysis test was conducted according to IS 2386 part-1. Gradation curves for fine aggregates are shown in Fig.1. High range water reducing super plasticizer Glenium B233 of specific gravity 1.09 is used for the experiment.

Table 1: Chemical composition of granite powder

Particulars	Values
SiO ₂	72.04%
Al ₂ O ₃	14.42%
K ₂ O	4.12%
Na ₂ O	3.69%
CaO	1.82%
FeO	1.68%
Fe ₂ O ₃	1.22%
MgO	0.71%
TiO ₂	0.3%
P ₂ O ₅	0.12%
MnO	0.05%

Source: Batch Inspection Certificate, Cemal Gems, and Minerals, Bangalore

Table 2: Chemical composition of copper slag

Constituent	Percentage weight
Silica, SiO ₂	26- 30 %
Free Silica	< 5%
Alumina, Al ₂ O ₃	2%
Iron Oxide, FeO	42-47%
Calcium Oxide, CaO	1-2 %
Magnesium Oxide, MgO	1.04 %
Copper Oxide, CuO	6.1 % max
Sulfates	0.13 %

Source: Batch Inspection Certificate, Blastline Pvt.Ltd

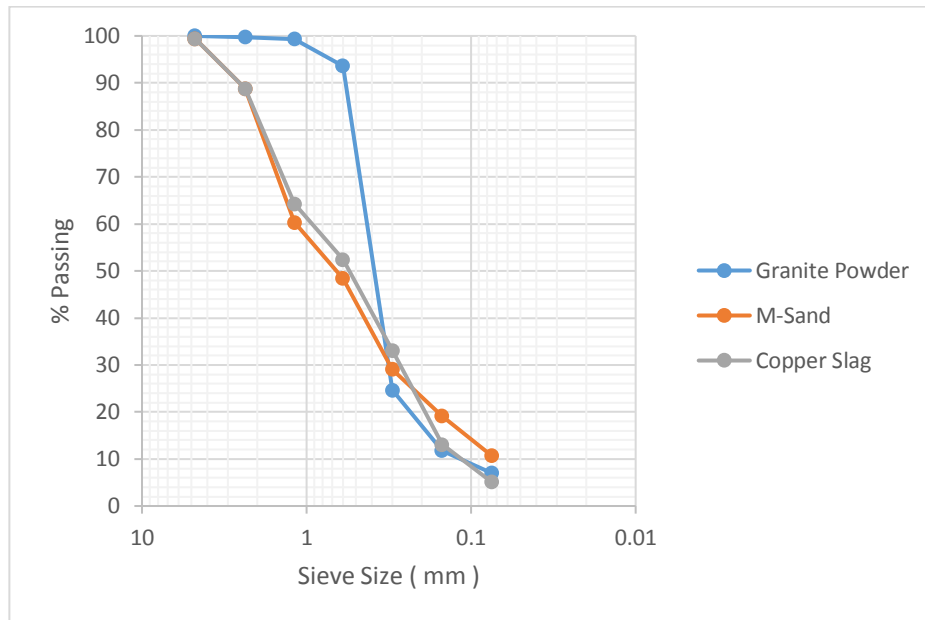


Figure 1: Particle size distribution curves of fine aggregates

4.2 Mix Design of Concrete

Concrete mixtures were prepared with recycled asphalt pavement aggregates as coarse aggregates and granite powder or copper slag as partial replacement of fine aggregate at various percentages i.e. 0% (for the control mix), 5%, 10%, 15%, 20%, and 25%. The control mixture was designed to have a target 28 day compressive strength of 30 N/mm² (M-30). The mix design obtained is 1:0.43:2.13:2.89 as per IS 10262-2009. Slump test was conducted at admixture dosages of 0.4, 0.45 and 0.5% by mass of cementitious material. As better slump value and mix was obtained at 0.4% dosage, admixture dosage is fixed as 0.4% by mass of cementitious material for all mixes except for the abrasion treated RAP aggregate concrete mix with granite powder replaced as fine aggregate at 20 and 25% in which the dosage is increased to 0.42 and 0.43% by mass of cementitious material.

4.3 Reference Specimens and Abrasion Process

Reference specimens like Normal Aggregate Concrete (NAC), concrete with RAP aggregate replaced as coarse aggregate at 100% (RAPC), concrete with RAP aggregate replaced as coarse aggregate at 30% (R-APC) and concrete with RAP aggregate replaced as coarse aggregate at 30% after abrasion (ABTRAPC) were cast. Los Angeles abrasion test was conducted according to IS 2386 part-4.

The principle of Los Angeles abrasion test is to produce abrasive action by use of standard steel balls which when mixed with aggregates and rotated in a drum for a specific number of revolutions also cause an impact on aggregates. In the modification process, Los Angeles Abrasion Testing Machine is used to do the abrasion process. The machine consists of a hollow cylinder, mounted on a steady frame on ball bearings. It has a detachable shelf which extends throughout the inside length of the drum. The drum is rotated at a speed of 30-33 rpm by an electric motor through a heavy reduction gear. Abrasive charge i.e., cast iron or steel balls, approximately 48mm in diameter and each weighing between 390 to 445 g of twelve numbers are used. Optimum duration time for the abrasion process is fixed at 10 minutes as longer duration resulted in fractured aggregates which might cause a loss in load transfer efficiency. As a number of abrasive charge increases, reduction in asphalt content also increases. Therefore 10 steel balls were selected for the abrasion process. Input quantity of Reclaimed Asphalt Pavement (RAP) Aggregates in the machine

was selected based on the materials passing 4.75 mm sieve after the abrasion process as per Table 3. When the number of aggregates was 30 kg, maximum attrition took place and hence the input quantities of aggregates were fixed as 30 kg. Bitumen content was found to reduce about 40.4% by centrifugal extraction method.

Table 3: Percentage passing through 4.75 mm sieve

RAP (kg)	15	20	25	30	35
Passing 4.75 mm Sieve (%)	4.02	5.15	6.2	6.63	6.38

4.4. Preparation of Test Specimens with Granite Powder and copper slag

Granite powder and m-sand were mixed thoroughly. Natural coarse aggregate and RAP aggregates modified by abrasion were mixed thoroughly and added to the mix. Once all materials were mixed thoroughly, superplasticizer was added to water and this water is added to the concrete mix. Hand mixing was done thoroughly. Specimens like 150X150X150 mm cubes, 100X100X500 mm beams, 150 mm X 300 mm cylinders were prepared using the concrete mix. After pouring into molds compaction of 25 blows was done using compaction rod in three layers. After finishing the surface, molds are dried for 24 hrs. After the removal from molds, the specimens are cured in an open water tank for a period of 28 days. The percentages of granite powder used were 5%, 10%, 15%, 20% and 25 of sand by weight designated by GP05, GP10, GP15, GP20, and GP25 respectively. Preparation of concrete specimens with copper slag was similar to those of granite powder specimens. The percentages of copper slag used were 5%, 10%, 15%, 20% and 25 of sand by weight designated by CS05, CS10, CS15, CS20 and CS25 respectively.

5.0 Testing of Fresh and Hardened Properties in Concrete

Slump test is done to check the workability of freshly made concrete. Concrete cubes, beams, and cylinders were used for testing the compression tests, flexural tests and split tensile strength tests into cubes, beams, and cylinders respectively. Compressive strength test, Flexural strength test and split tensile strength test were done according to IS 516-1959 at the 7th and 28th day. 24 cubes, 16 beams, and 16 cylinders were prepared as the reference specimens. Thirty cubes, twenty cylinders, and twenty beams were prepared each for granite powder and copper slag concrete mix in total. Slump variations for concrete mixes are given in Fig.2.

6.0 Slump Test Results

Reclaimed Asphalt Pavement Aggregate Concrete mixes were more workable compared to normal concrete mixes and are high due to its small particle size and larger fineness. These mixes were less workable at higher percentage replacements, especially above 15%. Concrete mixes with copper slag were highly workable and the problem of bleeding occurred at replacements above 15%.

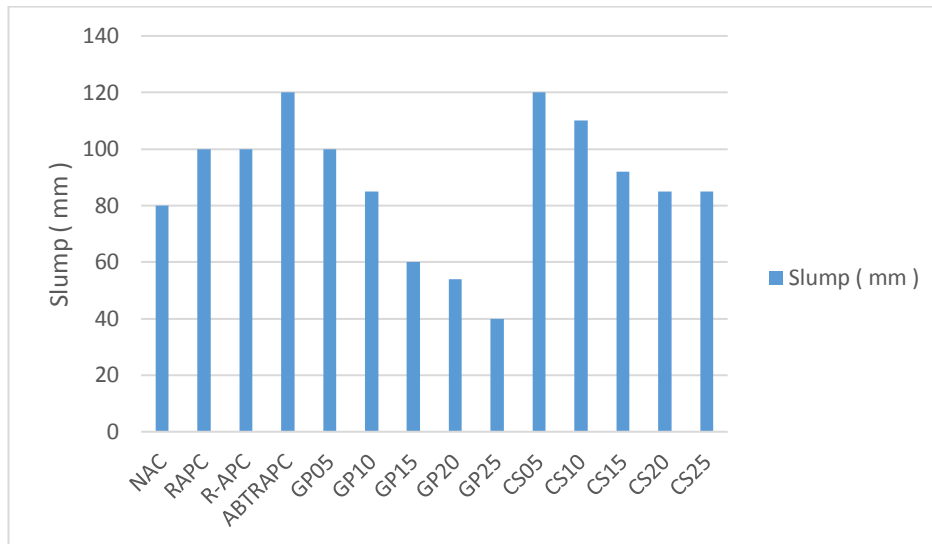


Figure 2: Slump variations for concrete mixes

7.0 Hardened Concrete Test Results

Strength tests were performed at the 7th and 28th day. Hardened concrete test results were obtained as an average of three specimens for each mix. A Compressive strength of 37.55 N/mm² is obtained for the NAC at 28 days. RAPC showed a reduction in strength of 62.13% (14.22 N/mm²) compared to NAC. R-APC showed a reduction in strength of 34.32% (24.66 N/mm²) compared to NAC. ABTRAPC showed a reduction in strength of 33.44% (24.99 N/mm²) compared to NAC and it exhibits the least reduction in strength. Fig.3 and Fig.4 show the compressive strength of cubes with different proportions of (GP) and (CS) respectively. A Flexural strength of 7.62 N/mm² is obtained for the NAC at 28 days. RAPC showed a reduction in strength of 40.94% (4.5 N/mm²) compared to NAC. R-APC showed a reduction in strength of 32.15% (5.17 N/mm²) compared to NAC. ABTRAPC showed a reduction in strength of 11.41% (6.75 N/mm²) compared to NAC and it exhibits the least reduction in strength. A split tensile strength of 2.63 N/mm² is obtained for the NAC at 28 days. RAPC showed a reduction in strength of 61.21% (1.02 N/mm²) compared to NAC. R-APC showed a reduction in strength of 28.89% (1.87 N/mm²) compared to NAC. ABTRAPC showed a reduction in strength of 24.33% (1.99 N/mm²) compared to NAC and it exhibits the least reduction in strength. Split tensile strength of ABTRAPC mixes (1.99 MPa) were 6.41% greater than R-APC mixes. Strength values of reference specimens are given in Table 4. Strength values of specimens with granite powder and copper slag are given in Table 5 and Table 6 respectively.

Table 4: Strength values of reference specimens

MIX	Average Compressive Strength (N/mm ²)		Average Flexural Strength (N/mm ²)		Average Tensile Strength (N/mm ²)	
	7 days	28 days	7 days	28 days	7 days	28 days
NAC	24.22	37.55	5	7.62	2.13	2.63
RAPC	6.505	14.22	0.17	4.5	0.78	1.02
R-APC	18.75	24.66	5.12	5.17	1.52	1.87
ABTRAPC	20.10	24.99	6	6.75	1.71	1.99

Table 5: Strength values of specimens with granite powder

MIX	Average Compressive Strength (N/mm ²)		Average Flexural Strength (N/mm ²)		Average Tensile Strength (N/mm ²)	
	7 days	28 days	7 days	28 days	7 days	28 days
GP05	14.99	18.55	3.87	4.75	1.83	1.96
GP10	17.22	19.66	4.55	4.92	1.93	1.98
GP15	23.12	30.99	5.87	6.12	1.96	1.99
GP20	19.56	25.37	4.55	6	1.8	2.08
GP25	14.48	17.82	3.77	4.25	1.2	1.37

Table 6: Strength values of specimens with copper slag

MIX	Average Compressive Strength (N/mm ²)		Average Flexural Strength (N/mm ²)		Average Tensile Strength (N/mm ²)	
	7 days	28 days	7 days	28 days	7 days	28 days
CS05	16.37	30.77	4.62	6.37	1.95	2.41
CS10	22.21	31.84	5.00	6.67	1.94	2.46
CS15	23.19	32.46	5.05	7.62	1.99	2.67
CS20	20.26	24.31	5.00	6.87	1.95	2.59
CS25	17.45	22.71	4.87	6.8	1.92	2.38

A maximum strength of 30.99 MPa is achieved by granite powder mixes at 15 % replacements at 28th day and it is equal to an increase of 24% compared to ABTRAPC mix. At 20% replacement it showed an increase of 1.52 % compared to ABTRAPC and at 25% replacement, strength decreased to 17.82 MPa.

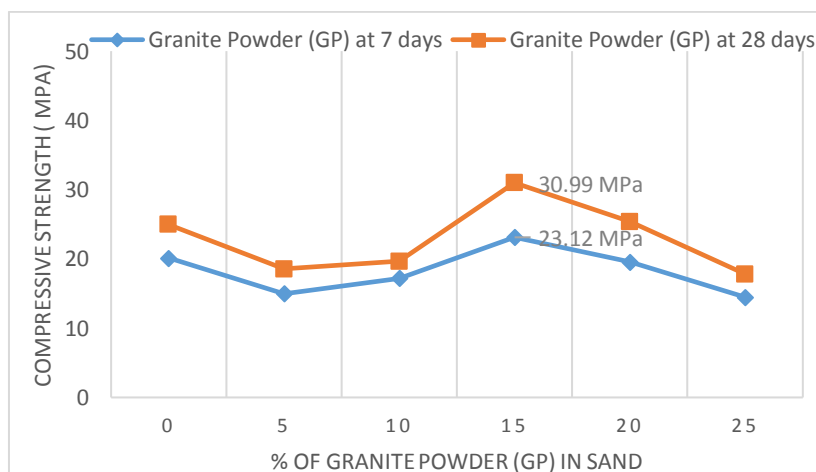


Figure 3: Compressive strength of cubes with different proportions of (GP)

Copper slag at 5% replacement itself shows an increase of 23.12% (30.77 MPa) compared to ABTRAPC mix. A maximum strength of 32.46 MPa is achieved by copper slag mixes at 15 % replacements at 28th day and it is equal to an increase of 29.89% compared to ABTRAPC mix. At 20% strength decreases to 24.31 MPa and decreases further.

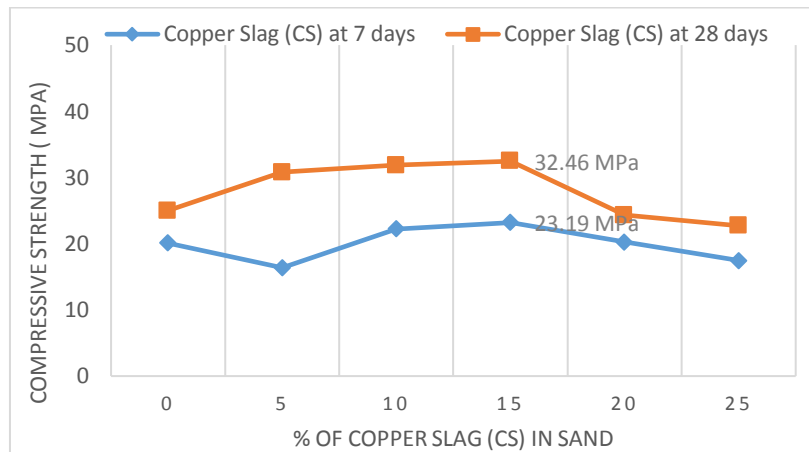


Figure 4: Compressive strength of cubes with different proportions of (CS)

Fig.5 and Fig.6 shows the flexural strength of beams with different proportions of (GP) and (CS) respectively.

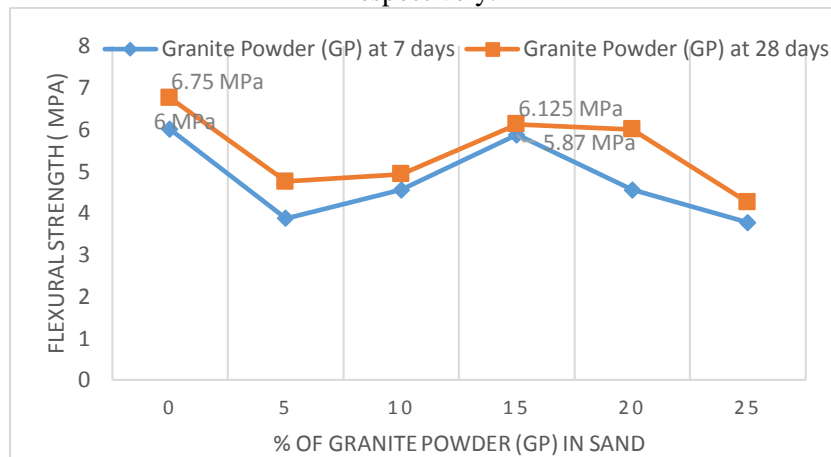


Figure 5: Flexural strength of a beam with different proportions of (GP)

Abrasion process increased the bending strength (5.17MPa) by 30.5% comparing to non-abrasion treated aggregates (6.75 MPa) at 28 days. At 15% replacement of fine aggregate with granite powder, a flexural strength of 6.12 MPa is obtained which shows a reduction of 9.3% compared to abrasion treated RAP aggregates (6.75 MPa) at 28 days. At 15% replacement of fine aggregate with copper slag, a flexural strength of 7.62 MPa is obtained which is similar to that of normal concrete and about 12.8% greater compared to ABTRAP concrete mix at 28 days. All mixes with copper slag exhibited greater flexural strength than granite powder mixes and all other reference mixes.

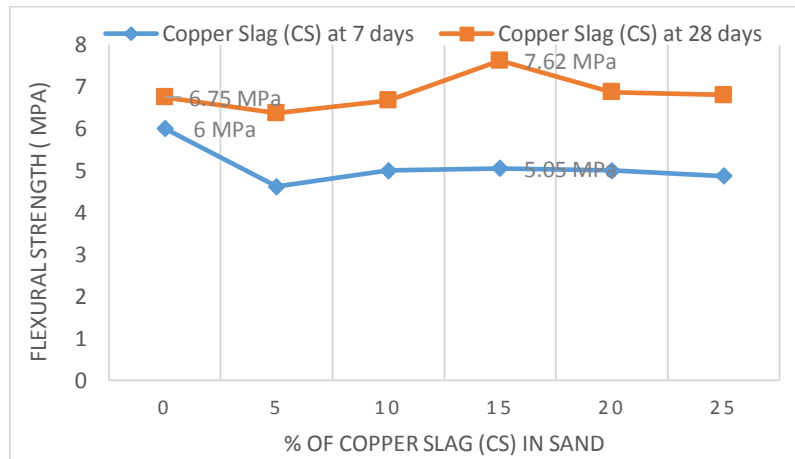


Figure 6: Flexural strength of a beam with different proportions of (CS)

Split tensile strength increased with an increase in the percentage of granite powder replacements up to 20% with a maximum of 2.08 MPa at 20% replacement and decrease further. A maximum split tensile strength of 2.67 MPa is obtained at 15% replacement of fine aggregate with copper slag which shows an increase of 1.52% compared to normal concrete and 34.17% compared to ABTRAP mixes. Fig.7 and Fig.8 shows the split tensile strength of cylinders with different proportions of (GP) and (CS) respectively.

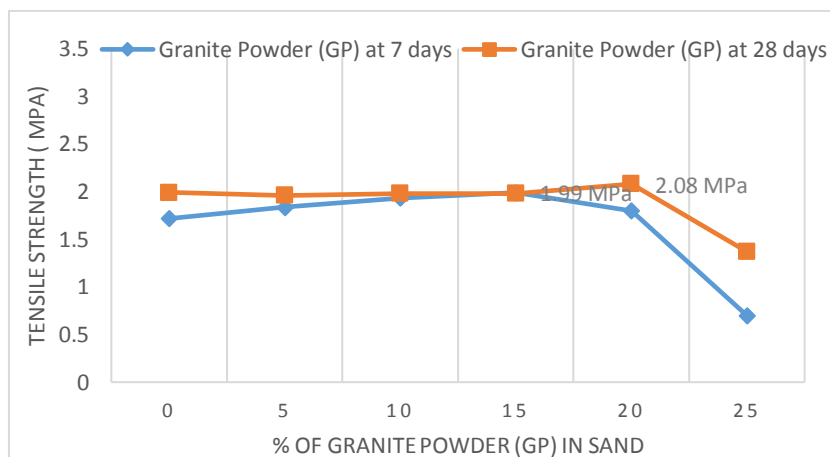


Figure 7: Split tensile strength of cylinders with different proportions of (GP)

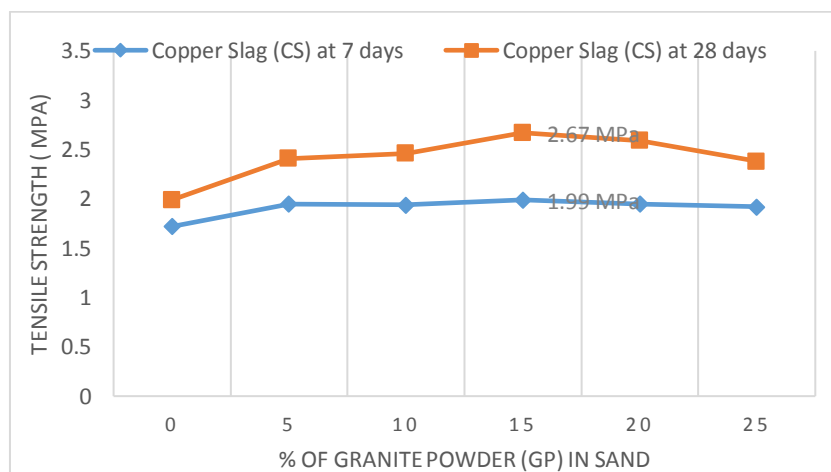


Figure 8: Split tensile strength of cylinders with different proportions of (CS)

8.0 Comparison of Test Results

Compressive strength increased with an increase in the percentage of replacement of granite powder up to 15% compared to ABTRAPC and increase in this case was 24%. Maximum flexural strength was obtained at 15% replacement even though it exhibited a reduction of 9.3% compared to ABTRAPC. Maximum split tensile strength is obtained at 20% and the increase was 4.52% compared to ABTRAPC. Compressive strength increased with an increase in the percentage of replacement of copper slag up to 15% and there was an increase of 29.89% compared to ABTRAPC. Maximum flexural strength was obtained at 15% replacement similar to normal concrete and 12.8% compared to ABTRAPC. Maximum split tensile strength is obtained at 15% and the increase was 1.52% compared to normal aggregate concrete and 34.17% compared to ABTRAPC. Replacements at 25% showed the least water absorption and more resistance to acid attack.

Fig.9 shows a comparison of compressive strength of concrete with granite powder and copper slag. Comparing the results of GP and CS, it is observed that up to 15% replacements, CS exhibited a higher compressive strength. At 20%, the compressive strength of GP increases and at 25% maximum strength was exhibited by CS.

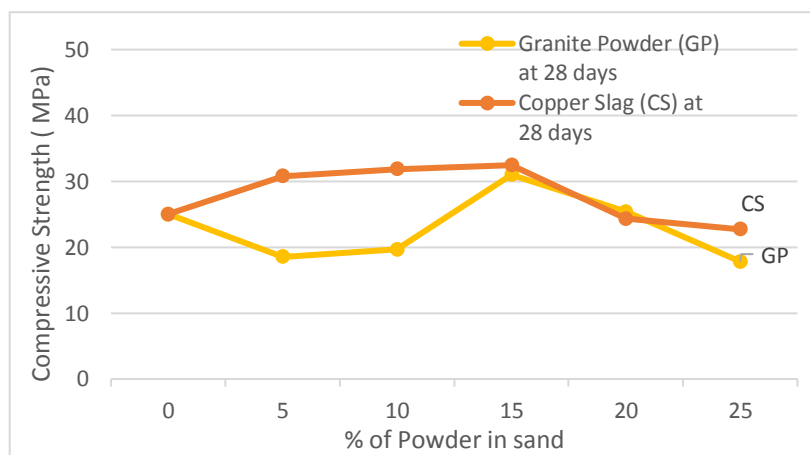


Figure 9: Effect of % of (GP) and (CS) on the Compressive Strength of Concrete

Fig.10 shows a comparison of flexural strength of concrete with granite powder and copper slag. Comparing the results of GP and CS, it is observed that at all replacements, CS exhibited a higher flexural strength comparing to GP.

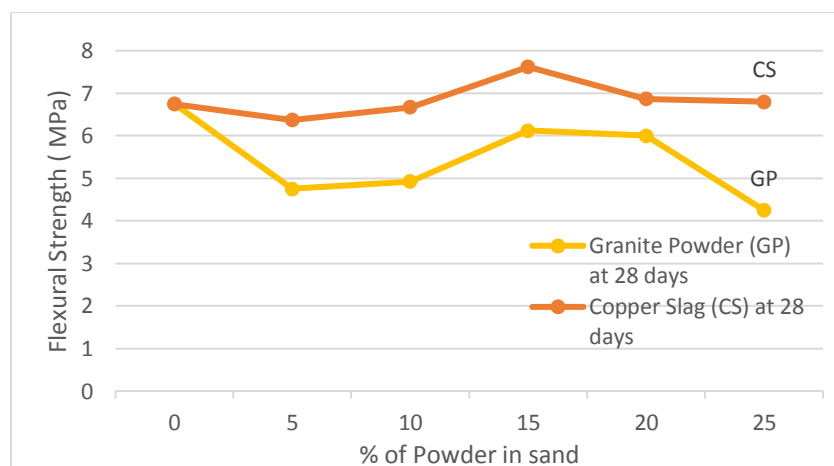


Figure 10: Effect of % of (GP) and (CS) on the Flexural Strength of Concrete

Fig.11 shows a comparison of the split tensile strength of concrete with granite powder and copper slag. Comparing the results of GP and CS, it is observed that at all replacements, CS exhibited a higher split tensile strength comparing to GP.

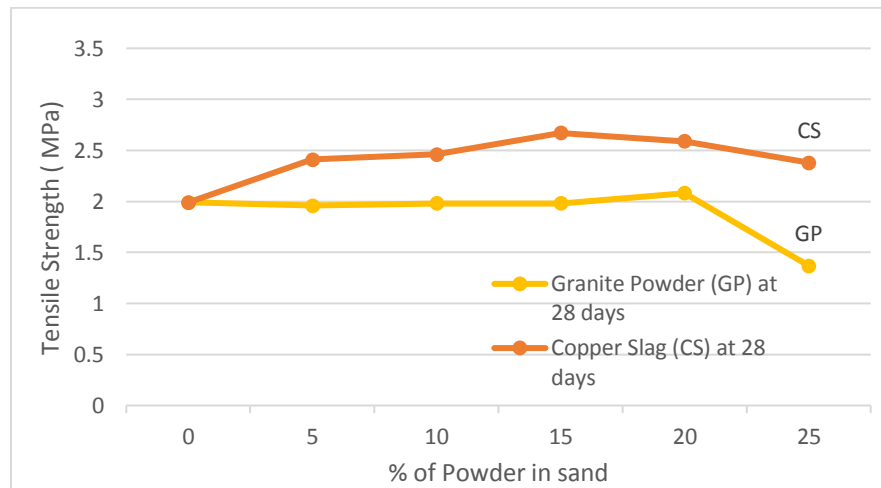


Figure 11: Effect of % of (GP) and (CS) on the Tensile Strength of Concrete

9.0 Conclusions

Based on the test results, the following conclusions can be made.

1. Abrasion and attrition improved the workability, mechanical and durability properties in concrete than the concrete with reclaimed pavement aggregates without abrasion since now the aggregate surface is more available to bonding with mortar and aggregates.
2. Workability of concrete mixes with granite powder and copper slag were good up to 15% of replacement. High water absorption of granite powder caused poor compactness and porosity and low water absorption property of copper slag caused bleeding above the replacement rates.
3. M30 grade concrete mix was developed by using reclaimed asphalt pavement aggregates as a partial replacement of coarse aggregate and granite powder as a fine aggregate at 15% and copper slag as a fine aggregate at 5, 10 and 15%.
4. Granite powder replaced at 15% showed a compressive strength of 23.12 MPa at 7th day and a maximum strength of 30.99 MPa at 28th day. Compressive strength gain of 34.03% was attained in the 28th day. Strength at 15% replacement is about 24% greater than the ABTRAPC specimens and strength at 20% replacement is 1.52% greater than the ABTRAPC specimens. Granite powder specimens developed strength ranging from 18.55MPa, 19.66 MPa, 30.99 MPa, 25.37 MPa, and 17.82 MPa at 5, 10, 15, 20 and 25 % replacements respectively.
5. Copper slag replaced at 5% itself showed a compressive strength similar to that attained by granite powder at 15% and it is 23.12% greater than ABTRAPC. Copper slag replaced at 15% showed a maximum strength 29.89% greater than ABTRAPC of 23.12 MPa at 7th day and a maximum strength of 30.99 MPa at 28th day. Compressive strength gain of 34.03% was attained in the 28th day. Strength at 15% replacement is about 24% greater than the ABTRAPC specimens and strength at 20% replacement is 1.52% greater than the ABTRAPC specimens. Copper slag specimens developed strength ranging from 30.77MPa, 31.84 MPa, 32.46 MPa, 24.3 MPa, and 22.7 MPa at 5, 10, 15, 20 and 25 % replacements respectively.
6. At 15% replacement of fine aggregate with granite powder, a flexural strength of 6.12 MPa is obtained which shows a reduction of 9.3% compared to abrasion treated RAP aggregates (6.75 MPa) at 28 days.
7. At 15% replacement of fine aggregate with copper slag, a flexural strength of 7.62 MPa is obtained which is similar to that of normal concrete and about 12.8% greater compared to

ABTRAP concrete mix at 28 days. All mixes with copper slag exhibited greater flexural strength than granite powder mixes and all other reference mixes.

8. Split tensile strength increased with an increase in the percentage of granite powder replacements up to 20% with a maximum of 2.08 MPa at 20% replacement which is 4.52% greater than ABTRAPC and decrease further. A maximum split tensile strength of 2.67 MPa is obtained at 15% replacement of fine aggregate with copper slag which shows an increase of 1.52% compared to normal concrete and 34.17% compared to ABTRAP mixes.

Conflict of Interest Statement

On behalf of all authors, the corresponding author states that there is no conflict of interest.

References

- [1] S. Abraham and G. Ransinchung, "Strength and permeation characteristics of cement mortar with Reclaimed Asphalt Pavement Aggregates", *Construction and Building Materials*, vol. 167, pp. 700-706, 2018.
- [2] K. Al-Jabri, A. Al-Saidy, and R. Taha, "Effect of copper slag as a fine aggregate on the properties of cement mortars and concrete", *Construction and Building Materials*, vol. 25, no. 2, pp. 933-938, 2011.
- [3] R. Al-Mufti and A. Fried, "Improving the strength properties of recycled asphalt aggregate concrete", *Construction and Building Materials*, vol. 149, pp. 45-52, 2017.
- [4] Brand and J. Roesler, "Bonding in cementitious materials with asphalt-coated particles: Part I – The interfacial transition zone", *Construction and Building Materials*, vol. 130, pp. 171-181, 2017.
- [5] A. Brand and J. Roesler, "Bonding in cementitious materials with asphalt-coated particles: Part II – Cement-asphalt chemical interactions", *Construction and Building Materials*, vol. 130, pp. 182-192, 2017.
- [6] Brand, A, fractionated reclaimed asphalt pavement as a coarse aggregate replacement in a ternary blended concrete pavement, Report ICT-12-008, Illinois State Toll Highway Authority, Downers Grove, 2012.
- [7] Dos Anjos, M. A. G., Sales, A. T. C., and Andrade, N. "Blasted Copper Slag as Fine Aggregate in Portland Cement Concrete", *Journal of environmental management*, vol. 96, 607-613, 2017.
- [8] Dos Santos, S., Party, M. N., and Poulikakos, L. D. "From Virgin to Recycled Bitumen: A Microstructural View", *Composites Part B: Engineering*, vol. 80, pp. 177-185, 2015.
- [9] Ghannam, S., Najm, H., and Vasconez, R. "Experimental Study of Concrete made with Granite and Iron Powders as Partial Replacement of Sand", *Sustainable Materials and Technologies*, vol. 9, pp. 1-9, 2016.
- [10] Hassan, K. E., Brooks, J. J., and Erdman, M. "The Use of Reclaimed Asphalt Pavement (RAP) Aggregates in Concrete", *Waste management series*, (Vol. 1, pp. 121-128), 2000.
- [11] M. S. Shahbaz, R. Z. R. M. Rasi, M. F. Bin Ahmad, and F. Rehman, "What is supply chain risk management? A review," *Adv. Sci. Lett.*, vol. 23, no. 9, pp. 9233–9238, 2017.
- [12] Hoyos, L. R., Puppala, A. J., and Ordonez, C. A. "Characterization of Cement-Fiber-Treated Reclaimed Asphalt Pavement Aggregates: Preliminary Investigation", *Journal of Materials in Civil Engineering*, vol. 23, pp. 977-989, 2017.
- [13] Huang, B., Shu, X., and Li, G. "Laboratory Investigation of Portland Cement Concrete Containing Recycled Asphalt Pavements", *Cement and Concrete Research*, vol. 35, pp. 2008-2013, 2005.
- [14] Najimi, M., Sobhani, J., and Pourkhorshidi, A. R. "Durability of Copper Slag Contained Concrete Exposed to Sulfate Attack", *Construction and Building materials*, vol. 25, pp. 1895-1905, 2011.

- [15] M. S. Shahbaz, R. Z. RM Rasi, M. F. Bin Ahmad, and S. Sohu, "The impact of supply chain collaboration on operational performance: Empirical evidence from manufacturing of Malaysia," *Int. J. Adv. Appl. Sci.*, vol. 5, no. 8, pp. 64–71, 2018.
- [16] Singh, S., Nande, N., Bansal, P., and Nagar, R. "Experimental Investigation of Sustainable Concrete Made with Granite Industry By-Product, *Journal of Materials in Civil Engineering*", vol. 29, 2017.
- [17] Singh, S., Ransinchung, G. D., and Kumar, P. "An Economical Processing Technique to Improve RAP Inclusive Concrete Properties", *Construction and Building Materials*, vol. 148, pp. 734-747, 2017.
- [18] Singh, S., Ransinchung, G. D., and Kumar, P. "Effect of Mineral Admixtures on Fresh, Mechanical and Durability Properties of RAP Inclusive Concrete", *Construction and Building Materials*, vol. 156, pp. 19-27, 2017.
- [19] Singh, S., Debbarma, S., and Kumar, P. "Utilization of Reclaimed Asphalt Pavement Aggregates Containing Waste from Sugarcane Mill for Production of Concrete Mixes", *Journal of Cleaner Production*, vol. 74, pp. 42-52, 2018.
- [20] Shi, X., Mukhopadhyay, A., and Liu, K. W. "Mix Design Formulation and Evaluation of Portland Cement Concrete Paving Mixtures Containing Reclaimed Asphalt Pavement", *Construction and Building Materials*, vol. 152, pp. 756-768, 2018.
- [21] Vijayalakshmi, M., and Sekar, A. S. S. "Strength and Durability Properties of Concrete made with Granite Industry Waste, *Construction, and Building Materials*", vol. 46, pp. 1-7, 2013.
- [22] Vijayaraghavan, J., Jude, A. B., and Thivya, J. "Effect of Copper Slag, Iron Slag, and Recycled Concrete Aggregate on the Mechanical Properties of Concrete", *Resources Policy*, vol. 53, pp. 2019-225, 2017.
- [23] Yi-qiu, T., Li, X., and Zhou, X. "Interactions of Granite and Asphalt based on the Rheological Characteristics", *Journal of Materials in Civil Engineering*, vol. 22, pp. 820-825, 2013.



A machine learning based approach to detect malicious android apps using discriminant system calls

Vinod P.^a  , Akka Zemhari^b, Mauro Conti^c

^a Department of Mathematics, University of Padua, Italy



^b LaBRI, Univ. Bordeaux, CNRS, France

^c Department of Mathematics, University of Padua, Italy

Received 20 March 2018, Revised 31 August 2018, Accepted 12 November 2018, Available online 27 November 2018, Version of Record 13 December 2018.



Show less 

 Share  Cite

<https://doi.org/10.1016/j.future.2018.11.021> 

[Get rights and content](#) 

Abstract

The openness of Android framework and the enhancement of users trust have gained the attention of malware writers. The momentum of downloaded applications (app for short) from numerous app stores has stimulated the proliferation of mobile malware. Now the threat is due to the sophistication in malware being written to bypass signature-based detectors. In this paper, we investigate system calls to tackle mobile malware on Android operating system. To do so, we first employed machine learning to extract system calls. We then performed the empirical estimation of system calls derived from diverse datasets employing human interaction and random inputs. After accomplishing intensive experiments on synthesized system calls with two feature selection approach, namely Absolute Difference of Weighted System Calls (ADWSC) and Ranked System Calls using Large Population Test (RSLPT), we validated the results on five datasets. All classifiers generated in Area Under Curve of 1.0 with an accuracy exceeding 99.9% suggest the appropriateness and efficacy of the proposed approach. Finally, we evaluated the effectiveness of classifier against adversarial attacks and found that the classifiers are vulnerable to data poisoning and label flipping attacks. Adversarial examples created by poisoning malware samples resulted in the significant drop of classifier performance on perturbing 12–18 prominent attributes. Moreover, we implemented class label poisoning attacks which brought down the classification accuracy by 50% on altering labels of 50 malicious training instances.

Introduction

The Gartner's report summarizes global sales of smartphones over a year. It reports the global sales of smartphones in the year 2017 as 380 million units with a 9.1% increase over first quarter of 2016. The plethora of Android applications and the openness of Android markets have added to the popularity of smartphones. Further, this has created an opportunity for the malware authors to sneak in and cause copious instances where malware is hidden behind benign applications threatening the privacy and security of users.

To protect the users from malware threats, security vendors offer different tools which are usually based on signature matching approach. Signature-based detection is prone to several challenges such as database with patterns of known threats, frequent update of the signature repository and intervention of experienced personnel in the signature generation process. In the present scenario, where malware attack is tremendously increasing, it is an extremely difficult for a pattern matching based scanners to detect new variants of existing malicious programs. As a result, there arises the need for devising alternate methods to detect malware.

Malware analysis approaches are broadly classified as static, dynamic and hybrid. Static analysis involves extracting features from malware after installing the app on a device or emulator. Such systems investigate the presence of known patterns, permissions, APIs and perform control flow analysis of an application without their execution using tool such as Apktool [1]. The approach is fast, however, unavailability of complete source code does not reveal malicious behavior. Anti-malware scanners employing static analysis can be evaded by transformation attacks involving code obfuscation and reflection. Moreover, control flow analysis adds computational overhead and is thus not recommended to be performed on the device. In dynamic analysis, malware samples are executed in an emulated environment such as a sandbox. Certain dynamic behavioral based anti-virus engine [2], observes the presence of sensitive APIs(such as read contacts, Internet, sending SMS), and assumes it as the malicious artifacts. Later, these malware detectors alert the user of suspicious behavior. However, benign messaging, travel and tourism apps also make use of these APIs for legitimate reasons. Therefore, these systems may raise the false alarm and make them less predictable.

New malware samples evolve by employing code obfuscation, manifest cheating, and loading malicious code while in execution. Even if the fingerprint of original malware sample is available with the anti-malware engine, new derivatives of the parents hide from detection. Although these techniques can help malware to remain stealth, the runtime behavior in-terms of OS interaction using system calls can be used reliably to identify them. Malware scanners using machine learning techniques constructed with robust features and classifiers are surely a solution to fight attacks. Machine learning algorithms are thus used to build classification models by training classifiers with prominent features mined from datasets consisting of a large number of examples. Consequently learned models are used to identify unseen samples. This paper utilizes the machine learning techniques accompanied by dynamic analysis to distinguish between malware and benign behaviors. The study was conducted on five datasets; here system calls are considered as features for analysis. System calls were selected as they represent the activities related to battery consumption, memory accesses, incoming and outgoing traffic and sensor status of a smartphone. Extraction of features was performed in two ways (a) using Android Monkey and also (b) by human interaction. Android Monkey is a utility which is a part of Android SDK and simulates human interaction with the application. Independent as well as a sequence of system calls were derived from the extracted call logs.

The extracted features space containing noise do not contribute towards the detection process. Hence, an optimal feature vector must be derived. Generally, use of feature selection methods reduces the high-dimensional feature space by identifying subsets of qualitative attributes enhancing the performance of classifiers. This paper thus proposes two feature selection methods Absolute Difference of Weighted System Calls(ADWSC) and Ranked System Calls using Large Population Test(RSLPT) for pruning higher dimensional system call set. An optimized feature occurrence matrix with each element representing the Term Frequency and Inverse Document(TF-IDF) value is built and, classification is carried out using ensemble algorithms. Furthermore, we investigate the viability of malware scanners by subjecting it to adversarial examples. These instances are created by (a) poisoning malicious input vectors and (b) altering the class labels to mislead the classification algorithm. Evaluation also validates the robustness of the different solution and open the research community to develop secure classification model resistant to adversarial attacks. Through our work, we make following contributions.

- We demonstrated the effectiveness of feature selection in Android malware classification system. To our knowledge, most of the prior work in the domain of malware detection utilizes conventional approaches such as information gain, chi square attribute ranking, correlation-based filters, Fischer's score etc. We focused predominantly on synthesizing relevant attributes for creating qualitative classification models fruitful for real-time analysis of malicious code. Hence, we implemented two new methods *Absolute Difference of Weighted System Calls(ADWSC)* and *Ranked System calls using Large Population Test(RSLPT)* that exhibited in an exceptional performance in the identification of malicious applications.
- With exhaustive experimentation considering variable feature length, we showed that a sub-optimal feature space can be extracted that minimizes false positives. We also conclude that representation of feature vector plays an important role in classifier performance. Thus, comparative analysis of different categories of feature vectors was performed. Finally, we concluded that application vector where each element represented as TF-IDF weight excelled compared to their counterpart. By doing so diversity between feature vector was enhanced and subsequently resulted in higher prediction accuracies ranging from 99.81% to 100% with AUC of 1.0.
- We empirically show the significance of system calls based scanners in comparison to other attributes such as permissions and APIs. Also, we evaluate the performance of proposed feature selection methods with symmetric uncertainty, information gain and principal component analysis(PCA). We show the improved performance of proposed feature selection over conventional methods.
- We evaluate the effectiveness of classifier against adversarial attacks. More specifically to the best of our knowledge, we are the first to implement data poisoning and label flipping attack on the system call feature set. Also, none of the prior work except one(discussed in Section2) considers attacks on the developed classification model. Moreover, we experimentally conclude that carefully created adversarial samples can easily evade detection, suggesting the development of security aware classification model.

The rest of the paper has been organized as follows. In Section2 we introduce the prior work conducted by researchers and compare different approaches based on features, attribute selection methods, classifiers. Section3 outlines the methodology that has been implemented. Section4 presents the experiments and results. Attacks on machine learning based scanners are covered in Section5. Also, we evaluate the performance of poisoning samples and class labels. Section6 discuss the outcome of the study and validity of threats respective to our proposed approach. Comparative analysis is covered in Section7. Finally, in Section8 we conclude the paper with directions for future work.

Section snippets

Related work

Android malware analysis using machine learning can be categorized into (a) static (b) dynamic and (c) hybrid approaches. In the following subsection we introduces the aforementioned methods....

Methodology

In this section, we outline our proposed methodology. Following are the steps used in the identification of malicious samples, also refer to Fig. 1:

- Dataset collection and cleaning(preprocessing)....
- System call extraction with the help of automated tool and human interaction....
- Elimination of irrelevant attributes by employing feature selection algorithms....
- Construction of feature occurrence matrix using prominent attributes....
- Evaluation of classification model using cross-validation....

...

Experiments and results

The experiment was conducted on Ubuntu 14.04 platform with the support of Intel Core i7-4510U CPU @ 2.0GHz with 16 GB RAM. In order for an emulator to mimic real devices, we added an adequate number of contacts, periodically modifying battery status with random values and finally created the sufficient number of messages and call logs. To evaluate the consistency of our approach, experiments were initially performed on two datasets, later the scalability is estimated on three more datasets.

- ...

...

Adversarial attacks on system call based scanner

The fundamental idea of any classifier is to estimate a boundary/decision surface that separates the training examples. In [55], authors introduced a notion of mimicry attack against anomaly-based detector, the attack was created by introducing sequence of legitimate call sequence. In our paper, we refer to such attack as poisoning attack. An adversary can launch *poisoning attack* either have limited or complete knowledge of the system. By limited knowledge (i.e.,the classification system is a...

Discussions and future work

Exhaustive experiments on the dataset gave insight to some of the important findings. We observed that sequence of system call were effective in identifying malicious apps. In order to further show the effectiveness of system call-centric detector over scanners using static attributes, we created a similar set of the experiment after extracting subset of critical permissions and APIs. With Random forest algorithm learned with 70 permissions an accuracy of 92.37%, FPR value of 0.076 and AUC of...

Comparative analysis

In this section, we provide a comparative evaluation of our approach with similar studies previously conducted. The summary of analysis is presented in Table 13. We also implemented similar feature selection methods reported by authors in[3] and[20] for

synthesizing system call set derived using our dataset. As we had no access to dataset in [3] and [20], hence we experimented on the derived system call set from the collected samples. Refer to Table 12 for the outcome of results. We observe...

Conclusion

In this paper, the application of feature selection approaches and their performance was investigated. Evaluation was performed in two different experimental settings (a) using input generator and (b) employing human interaction. Impact of feature selection methods such as ADWSC and RSLPT on classifier performance was assessed. The assessment metrics for different settings of experiments exhibited an AUC in range of 0.99–1.0. To affirm the scalability of proposed machine learning approach...

Vinod P., is Post Doc at Department of Mathematics, University of Padua, Italy. Prior to joining Padua he was working as Professor in SCMS School of Engineering & Technology, Cochin, India. He holds his Ph.D. in Computer Engineering from Malaviya National Institute of Technology, Jaipur, India. He has more than 50 research articles published in peer reviewed Journals and International Conferences. He is reviewer of number of security journals, and is also serving as programme committee member...

References (61)

WangWei *et al.*

[Detecting Android malicious apps and categorizing benign apps with ensemble of classifiers](#)

Future Gener. Comput. Syst. (2018)

IdreesF. *et al.*

[Pndroid: A novel Android malware detection system using ensemble learning methods](#)

Comput. Secur. (2017)

MilosevicN. *et al.*

[Machine learning aided android malware classification](#)

J. Comput. Electr. Eng. (2017)

SheenShina *et al.*

[Android based malware detection using a multifeature collaborative decision fusion approach](#)

Neurocomputing (2015)

ZhuHui-Juan *et al.*

[DroidDet: effective and robust detection of android malware using static analysis along with rotation forest model](#)

Neurocomputing (2018)

TongFei *et al.*

[A hybrid approach of mobile malware detection in Android](#)

J. Parallel Distrib. Comput. (2017)

BhandariShweta *et al.*

[SWORD: semantic aware android malware detector](#)

J. Inf. Secur. Appl. (2018)

FeizollahAli *et al.*

[A review on feature selection in mobile malware detection](#)

Int. J. Digit. Forensics Incident Response (2015)

ChandrashekarG. *et al.*

[A survey on feature selection methods](#)

J. Comput. Electr. Eng. (2014)

Apktool,...

View more references

Data poisoning attacks against machine learning algorithms

2022, Expert Systems with Applications

[Show abstract](#) 

On the relativity of time: Implications and challenges of data drift on long-term effective android malware detection

2022, Computers and Security

Citation Excerpt :

...The vast majority of literature regarding Android malware detection neglects the existence of concept drift. The models and proposed solutions are generally trained and validated on static snapshots of Android historical data, usually with the same well-known data sets (Abderrahmane et al., 2019; Afonso et al., 2015; Ahsan-Ul-Haque et al., 2018; Alzaylaee et al., 2017; 2020; Amin et al., 2016; Bhatia and Kaushal, 2017; Burguera et al., 2011; Canfora et al., 2015; Casolare et al., 2021; Da et al., 2016; Dimjašević et al., 2016; Feng et al., 2018; Ferrante et al., 2016; Frenklach et al., 2021; Guerra-Manzanares et al., 2019a; 2019b; 2019c; Hei et al., 2021; Hou et al., 2016; Isohara et al., 2011; Jaiswal et al., 2018; Jang et al., 2014; Kapratwar et al., 2017; Lin et al., 2013; Lindorfer et al., 2015; Liu et al., 2021; Mahindru and Sangal, 2021; Malik and Khatter, 2016; McLaughlin et al., 2017; Naval et al., 2015; Rathore et al., 2021; Saif et al., 2018; Saracino et al., 2018; Sasidharan and Thomas, 2021; Sihag et al., 2021; Singh and Hofmann, 2017; Surendran et al., 2020; Tchakounté and Dayang, 2013; Tong and Yan, 2017; Vidal et al., 2017; Vinod et al., 2019; Wahanggara and Prayudi, 2015; Wang and Li, 2021; Xiao et al., 2015; 2016; 2019; Yu et al., 2013; Yuan et al., 2014). In this regard, MalGenome (Zhou and Jiang, 2012) and Drebin (Arp et al., 2014) are the most used data sets for Android malware research....

[Show abstract](#) 

An in-depth review of machine learning based Android malware detection

2022, Computers and Security

Citation Excerpt :

...From the evaluation results provided by Burguera et al. (2011), Vinod et al. (2019), Xiao et al. (2019), system calls do seem to produce high accuracy rates when used to classify applications as benign or malware. The results reported in Vinod et al. (2019) showed that the usage of independent or sequences of system calls did not affect the accuracy rates significantly. API calls are one of the most extracted features in dynamic analysis....

[Show abstract](#) 

Concept drift and cross-device behavior: Challenges and implications for effective android malware detection

2022, Computers and Security

[Show abstract](#) 

Security analysis of menstruation cycle tracking applications using static, dynamic and machine learning techniques

2022, Journal of Information Security and Applications

[Show abstract](#) 

Malicious application detection in android - A systematic literature review

2021, Computer Science Review

Citation Excerpt :

...Generative adversarial networks (GAN) is also discussed in latest research studies [51,258,376] used to evaluate the performance of malware detector. Adversarial samples are generated to mislead the detection process that is used to find out the vulnerabilities in the machine learning classification system [258,360,361]. According to previous research there are a number of datasets available for the experiments....

[Show abstract](#) 



[View all citing articles on Scopus](#)

Recommended articles (6)

Research article

A stacking model using URL and HTML features for phishing webpage detection

Future Generation Computer Systems, Volume 94, 2019, pp. 27-39

[Show abstract](#) ✓

Research article

[Detecting Android malicious apps and categorizing benign apps with ensemble of classifiers](#)

Future Generation Computer Systems, Volume 78, Part 3, 2018, pp. 987-994

[Show abstract](#) ✓

Research article

[Detection of app collusion potential using logic programming](#)

Journal of Network and Computer Applications, Volume 105, 2018, pp. 88-104

[Show abstract](#) ✓

Research article

[Visualizing the outcome of dynamic analysis of Android malware with VizMal](#)

Journal of Information Security and Applications, Volume 50, 2020, Article 102423

[Show abstract](#) ✓

Research article

[A scalable and extensible framework for android malware detection and family attribution](#)

Computers & Security, Volume 80, 2019, pp. 120-133

[Show abstract](#) ✓

Research article

[Similarity-based Android malware detection using Hamming distance of static binary features](#)

Future Generation Computer Systems, Volume 105, 2020, pp. 230-247

[Show abstract](#) ✓



Vinod P., is Post Doc at Department of Mathematics, University of Padua, Italy. Prior to joining Padua he was working as Professor in SCMS School of Engineering & Technology, Cochin, India. He holds his Ph.D. in Computer Engineering from Malaviya National Institute of Technology, Jaipur, India. He has more than 50 research articles published in peer reviewed Journals and International Conferences. He is reviewer of number of security journals, and is also serving as programme committee member in the International Conferences related to Computer and Information Security. Vinod's area of interest is Adversarial Machine Learning, Malware Analysis, Context aware privacy preserving Data Mining, Ethical Hacking and Natural Language Processing.



Dr. Akka Zemhari has received his Ph.D. degree from the University of Bordeaux, France, in 2000. He is an Associate Professor in computer science since 2001 at University of Bordeaux, France. He has more than 100 research articles published in peer reviewed Journals and International Conferences, and also serves as programme committee member in the International Conferences. His research interests include distributed algorithms and systems, graphs, randomized algorithms, machine learning and security.



Mauro Conti (SM'14) received the Ph.D. degree from the Sapienza University of Rome, Italy, in 2009. He is currently an Associate Professor at the University of Padua, Italy. After his Ph.D., he was a Postdoctoral Researcher with Vrije Universiteit Amsterdam, The Netherlands. In 2011, he joined the University of Padua, where he became an Associate Professor in 2015. He was a Visiting Researcher with GMU (2008), UCLA (2010), UCI (2012, 2013, and 2014), and TU Darmstadt (2013). He received a Marie Curie Fellowship (2012) from the European Commission, and a Fellowship from the German DAAD (2013). His main research interest is in the area of security and privacy. In this area, he has authored over 100 papers in topmost international peer-reviewed journals and conference. He is an Associate Editor of several journals, including the IEEE COMMUNICATIONS SURVEYS AND TUTORIALS. He was the Program Chair of TRUST 2015, and the General Chair of Secure Comm 2012 and ACM SACMAT 2013.

[View full text](#)

© 2018 Elsevier B.V. All rights reserved.



Copyright © 2023 Elsevier B.V. or its licensors or contributors.
ScienceDirect® is a registered trademark of Elsevier B.V.



Identification of Android malware using refined system calls

Deepa K., Radhamani G., Vinod P., Mohammad Shojafar ✉, Neeraj Kumar, Mauro Conti

First published: 09 May 2019

<https://doi.org/10.1002/cpe.5311>

Citations: 2

Summary

The ever increasing number of Android malware has always been a concern for cybersecurity professionals. Even though plenty of anti-malware solutions exist, we hypothesize that the performance of existing approaches can be improved by deriving relevant attributes through effective feature selection methods. In this paper, we propose a novel two-step feature selection approach based on Rough Set and Statistical Test named as RSST to extract refined system calls, which can effectively discriminate malware from benign apps. By refined set of system call, we mean the existence of highly relevant calls that are uniformly distributed thought target classes. Moreover, an optimal attribute set is created, which is devoid of redundant system calls. To address the problem of higher dimensional attribute set, we derived suboptimal system call space by applying the proposed feature selection method to maximize the separability between malware and benign samples. Comprehensive experiments conducted on three datasets resulted in an accuracy of 99.9%, Area Under Curve (AUC) of 1.0, with 1% False Positive Rate (FPR). However, other feature selectors (Information Gain, CFSSubsetEval, ChiSquare, FreqSel, and Symmetric Uncertainty) used in the domain of malware analysis resulted in the accuracy of 95.5% with 8.5% FPR. Moreover, the empirical analysis of RSST derived system calls outperformed other attributes such as permissions, opcodes, API, methods, call graphs, Droidbox attributes, and network traces.

REFERENCES

- 1 Smartphones Industry: Statistics & Facts. <http://www.statista.com/topics/840/smartphones/>. Accessed March 2019.
[Google Scholar](#)
- 2 Sophos. <http://www.sophos.com/en-us/security-news-trends/whitepapers.aspx>. Accessed March 2019.
[Google Scholar](#)
- 3 Faruki P, Bharmal A, Laxmi V, et al. Android security: a survey of issues, malware penetration, and defenses. *IEEE Commun Surv Tutor*. 2015; **17**(2): 998-1022.
View | [Web of Science®](#) | [Google Scholar](#)
- 4 Amos B, Turner H, White J. Applying machine learning classifiers to dynamic Android malware detection at scale. Paper presented at: 9th International Wireless Communications and Mobile Computing Conference; 2013; Sardinia, Italy.
[Google Scholar](#)
- 5 Gardiner J, Nagaraja S. On the security of machine learning in malware C&C detection: a survey. *ACM Comput Surv*. 2016; **49**(3): 59:1-59:39.
View | [Web of Science®](#) | [Google Scholar](#)
- 6 Android Monkey. <http://developer.android.com/studio/test/monkey.html>. Accessed March 2019.
[Google Scholar](#)
- 7 Feizollah A, Anuar NB, Salleh R, Wahab AWA. A review on feature selection in mobile malware detection. *Digit Investig*. 2015; **13**: 22-37.
View | [Web of Science®](#) | [Google Scholar](#)
- 8 Zhang M, Yao JT. A rough sets based approach to feature selection. Paper presented at: IEEE Annual Meeting of the Fuzzy Information; 2004; Banff, Canada.
[Google Scholar](#)
- 9 Świniarski RW. Rough sets methods in feature reduction and classification. *Int J Appl Math Comput Sci*. 2001; **11**: 565-582.
[Google Scholar](#)
- 10 Massey A, Miller SJ. Tests of Hypotheses Using Statistics. Providence, RI: Brown University; 2006.
[Google Scholar](#)

11 Freund Y, Schapire R, Abe N. A short introduction to boosting. *Jpn Soc Artif Intell.* 1999; **14**(771-780): 1612.

[Google Scholar](#)

12 Breiman L. Random forests. *Mach Learn.* 2001; **45**(1): 5-32.

View | [Web of Science®](#) | [Google Scholar](#)

13 Kuncheva LI, Rodríguez JJ. An experimental study on rotation forest ensembles. Paper presented at: International Workshop on Multiple Classifier Systems; 2007; Prague, Czech Republic.

[Google Scholar](#)

14 Droidbox. <http://github.com/pjlantz/droidbox>. Accessed March 2019.

[Google Scholar](#)

15 Arp D, Spreitzenbarth M, Hubner M, Gascon H, Rieck K, Siemens C. DREBIN: Effective and explainable detection of Android malware in your pocket. Paper presented at: Network and Distributed System Security Symposium; 2014; San Diego, CA.

[Google Scholar](#)

16 Zhou Y, Jiang X. Dissecting Android malware: Characterization and evolution. Paper presented at: 33rd IEEE Symposium on Security and Privacy; 2012; San Francisco, CA.

[Google Scholar](#)

17 Glodek W, Harang R. Rapid permissions-based detection and analysis of mobile malware using random decision forests. Paper presented at: Military Communications Conference; 2013; San Diego, CA.

[Google Scholar](#)

18 Cen L, Gates CS, Si L, Li N. A probabilistic discriminative model for android malware detection with decompiled source code. *IEEE Trans Dependable Secure Comput.* 2015; **12**(4): 400-412.

View | [Web of Science®](#) | [Google Scholar](#)

19 Talha KA, Alper DI, Aydin C. APK auditor: permission-based Android malware detection system. *Digit Investig.* 2015; **13**: 1-14.

View | [Web of Science®](#) | [Google Scholar](#)

20 Wang W, Li Y, Wang X, Liu J, Zhang X. Detecting Android malicious apps and categorizing benign apps with ensemble of classifiers. *Future Gener Comput Syst.* 2018; **78**: 987-994.

View | [Web of Science®](#) | [Google Scholar](#)

21 Zhao K, Zhang D, Su X, Li W. Fest: A feature extraction and selection tool for Android malware detection. Paper presented at: IEEE Symposium on Computers and Communication; 2015; Larnaca, Cyprus.

[Google Scholar](#)

22 Wang W, Wang X, Feng D, Liu J, Han Z, Zhang X. Exploring permission-induced risk in android applications for malicious application detection. *IEEE Trans Inf Forensics Secur.* 2014; **9**(11): 1869-1882.

View | [Web of Science®](#) | [Google Scholar](#)

23 Ham H-S, Choi MJ. Analysis of Android malware detection performance using machine learning classifiers. Paper presented at: International Conference on ICT Convergence; 2013; Jeju, South Korea.

[Google Scholar](#)

24 Amamra A, Robert J-M, Abraham A, Talhi C. Generative versus discriminative classifiers for android anomaly-based detection system using system calls filtering and abstraction process. *Secur Commun Netw.* 2016; **9**(16): 3483-3495.

View | [Web of Science®](#) | [Google Scholar](#)

25 Kim H-H, Choi M-J. Linux kernel-based feature selection for Android malware detection. Paper presented at: 16th Asia-Pacific Network Operations and Management Symposium; 2014; Hsinchu, Taiwan.

[Google Scholar](#)

26 Shabtai A, Tenenboim-Chekina L, Mimran D, Rokach L, Shapira B, Elovici Y. Mobile malware detection through analysis of deviations in application network behavior. *Comput Secur.* 2014; **43**: 1-18.

View | [Web of Science®](#) | [Google Scholar](#)

27 Narudin FA, Feizollah A, Anuar NB, Gani A. Evaluation of machine learning classifiers for mobile malware detection. *Soft Computing*. 2016; **20**(1): 343-357.

View | [Web of Science®](#) | [Google Scholar](#)

28 Chekina L, Mimran D, Rokach L, Elovici Y, Shapira B. Detection of Deviations in Mobile Applications Network Behavior. 2012. <http://arxiv.org/abs/1208.0564>

[Google Scholar](#)

29 Shabtai A, Kanonov U, Elovici Y, Glezer C, Weiss Y. Andromaly: a behavioral malware detection framework for android devices. *J Intell Inf Syst*. 2012; **38**(1): 161-190.

View | [Web of Science®](#) | [Google Scholar](#)

30 Tong F, Yan Z. A hybrid approach of mobile malware detection in Android. *J Parallel Distributed Comput*. 2017; **103**: 22-31. Special Issue on Scalable Cyber-Physical Systems.

View | [Web of Science®](#) | [Google Scholar](#)

31 Damshenas M, Dehghantanha A, Choo K-KR, Mahmud R. M0droid: an android behavioral-based malware detection model. *J Inf Priv Secur*. 2015; **11**(3): 141-157.

[Google Scholar](#)

32 Xiao X, Wang Z, Li Q, Xia S, Jiang Y. Back-propagation neural network on Markov chains from system call sequences: a new approach for detecting Android malware with system call sequences. *IET Inf Secur*. 2016; **11**(1): 8-15.

View | [Web of Science®](#) | [Google Scholar](#)

33 Canfora G, Medvet E, Mercaldo F, Visaggio CA. Detecting Android malware using sequences of system calls. Paper presented at: 3rd International Workshop on Software Development Lifecycle for Mobile; 2015; Bergamo, Italy.

[Google Scholar](#)

34 Xin Su, Chuah M, Tan G. Smartphone dual defense protection framework: Detecting malicious applications in Android markets. Paper presented at: 8th International Conference on Mobile Ad-hoc and Sensor Networks; 2012; Chengdu, China.

[Google Scholar](#)

35 Canfora G, Mercaldo F, Visaggio CA. A classifier of malicious Android applications. Paper presented at: 8th International Conference on Availability, Reliability and Security; 2013; Regensburg, Germany.

[Google Scholar](#)

36 Rocha BPS, Conti M, Etalle S, Crispo B. Hybrid static-runtime information flow and declassification enforcement. *IEEE Trans Inf Forensics Secur*. 2013; **8**(8): 1294-1305.

View | [Web of Science®](#) | [Google Scholar](#)

37 Feldman S, Stadther D, Wang B. Manalyzer: Automated Android malware detection through manifest analysis. Paper presented at: IEEE 11th International Conference on Mobile Ad Hoc and Sensor Systems; 2014; Philadelphia, PA.

[Google Scholar](#)

38 Lin Y-D, Lai Y-C, Lu C-N, Hsu P-K, Lee C-Y. Three-phase behavior-based detection and classification of known and unknown malware. *Secur Commun Netw*. 2015; **8**(11): 2004-2015.

View | [Web of Science®](#) | [Google Scholar](#)

39 Google Play Store. <http://play.google.com/store?hl=en>. Accessed March 2019.

[Google Scholar](#)

40 AppInChina. <http://www.appinchina.co/market/>. Accessed March 2019.

[Google Scholar](#)

41 Koodous. <http://koodous.com/>. Accessed March 2019.

[Google Scholar](#)

42 1Mobile Market. <http://m.1mobile.com/me.onemobile.android.html>. Accessed March 2019.

[Google Scholar](#)

43 9apps. <http://www.9apps.com/>. Accessed March 2019.

44 VirusTotal. <http://www.virustotal.com/>. Accessed March 2019.

[Google Scholar](#)

45 Ransomware. <http://ransom.mobi/>. Accessed March 2019.

[Google Scholar](#)

46 strace. <http://linux.die.net/man/1/strace>. Accessed March 2019.

[Google Scholar](#)

47 Ramos J. Using TF-IDF to determine word relevance in document queries. Paper presented at: 1st Instructional Conference on Machine Learning; 2003; Banff, Canada.

[Google Scholar](#)

48 Hu X. Knowledge Discovery in Databases: An Attribute-Oriented Rough Set Approach [dissertation]. Regina, Canada: University of Regina; 1995.

[Google Scholar](#)

49 Jensen R, Shen Q. Rough set based feature selection: A review. In: AE Hassanien, Z Suraj, D Slezak, P Lingras, eds. *Rough Computing: Theories, Technologies and Applications*. Hershey, PA: Information Science Reference; 2007: 70-107.

View | [Google Scholar](#)

50 Hall M, Frank E, Holmes G, Pfahringer B, Reutemann P, Witten IH. The WEKA data mining software: an update. *ACM SIGKDD Explor. Newsl.* 2009; **11**(1): 10-18.

View | [Google Scholar](#)

51 AV-Test. <http://goo.gl/Rg6NDN>. Accessed March 2019.

[Google Scholar](#)

52 WEKA. <http://www.cs.waikato.ac.nz/ml/weka/>. Accessed March 2019.

[Google Scholar](#)

53 Idrees F, Rajarajan M, Conti M, Chen TM, Rahulamathavan Y. Plndroid: a novel Android malware detection system using ensemble learning methods. *Comput Secur.* 2017; **68**: 36-46.

View | [Web of Science®](#) | [Google Scholar](#)

54 Bhandari S, Panihar R, Naval S, Laxmi V, Zemmari A, Gaur MS. SWORD: Semantic aWare andrOid malwaRe Detector. *J Inf Secur Appl.* 2018; **42**: 46-56.

View | [Web of Science®](#) | [Google Scholar](#)

55 Alam Mohammed S, Vuong Son T. Random forest classification for detecting Android malware. Paper presented at: 2013 IEEE International Conference on Green Computing and Communications and IEEE Internet of Things and IEEE Cyber, Physical and Social Computing; 2013; Beijing, China.

[Google Scholar](#)

56 Bhatia T, Kaushal R. Malware detection in Android based on dynamic analysis. Paper presented at: 2017 International Conference on Cyber Security and Protection of Digital Services; 2017; London, United Kingdom.

[Google Scholar](#)

57 Goyal R, Spognardi A, Dragoni N, Argyriou M. Safedroid: A distributed malware detection service for Android. Paper presented at: 2016 IEEE 9th International Conference on Service-Oriented Computing and Applications (SOCA); 2016; Macau, China.

[Google Scholar](#)

58 Moonsamy V, Batten L. Zero permission Android applications-attacks and defenses. Paper presented at: 3rd International Conference on Applications and Techniques for Information Security; 2012; Melbourne, Australia.

[Google Scholar](#)

59 Narain S, Vo-Huu TD, Block K, Noubir G. Inferring user routes and locations using zero-permission mobile sensors. Paper presented at: 2016 IEEE Symposium on IEEE Security and Privacy; 2016; San Jose, CA.

[Google Scholar](#)

60 Google TCP Dump. <https://sites.google.com/site/christians310/tcpdump>. Accessed March 2019.

[Google Scholar](#)

61 Ruta D, Gabrys B. An overview of classifier fusion methods. *Comput Inf Syst.* 2000; 7(1): 1-10.

[Google Scholar](#)

62 Goodfellow I, Pouget-Abadie J, Mirza M, et al. Generative adversarial nets. Paper presented at: 27th International Conference on Neural Information Processing Systems; 2014; Montreal, Canada.

[Google Scholar](#)

63 Felt AP, Chin E, Hanna S, Song D, Wagner D. Android permissions demystified. Paper presented at: 18th ACM conference on Computer and Communications Security; 2011; Chicago, IL.

[Google Scholar](#)

64 Rastogi V, Chen Y, Jiang X. Droidchameleon: Evaluating Android anti-malware against transformation attacks. Paper presented at: 8th ACM SIGSAC Symposium on Information, Computer and Communications Security; 2013; Hangzhou, China.

[Google Scholar](#)

65 Rastogi V, Chen Y, Jiang X. Catch me if you can: evaluating android anti-malware against transformation attacks. *IEEE Trans Inf Forensics Secur.* 2014; 9(1): 99-108.

View | [Web of Science®](#) | [Google Scholar](#)

66 Dong S, Li M, Diao W, et al. Understanding Android obfuscation techniques: A large-scale investigation in the wild. Paper presented at: International Conference on Security and Privacy in Communication Systems; 2018; Singapore.

[Google Scholar](#)

67 Proguard. <http://developer.android.com/tools/help/proguard.html>. Accessed March 2019.

[Google Scholar](#)

68 Dasho. <http://www.preemptive.com/solutions/android-obfuscation/>. Accessed March 2019.

[Google Scholar](#)

69 Du P, Samat A, Waske B, Liu S, Li Z. Random forest and rotation forest for fully polarized SAR image classification using polarimetric and spatial features. *ISPRS J Photogramm Remote Sens.* 2015; 105: 38-53.

View | [Web of Science®](#) | [Google Scholar](#)

Citing Literature

Number of times cited according to CrossRef: 2

Ke Shao, Qiang Xiong, Zhiming Cai, FB2Droid: A Novel Malware Family-Based Bagging Algorithm for Android Malware Detection, Security and Communication Networks, 10.1155/2021/6642252, 2021, (1-13), (2021).

[View](#)

Xin Su, Lijun Xiao, Wenjia Li, Xuchong Liu, Kuan-Ching Li, Wei Liang, DroidPortrait: Android Malware Portrait Construction Based on Multidimensional Behavior Analysis, Applied Sciences, 10.3390/app10113978, 10, 11, (3978), (2020).

[View](#)

[Download PDF](#)

ABOUT WILEY ONLINE LIBRARY

[Privacy Policy](#)
[Terms of Use](#)
[About Cookies](#)
[Manage Cookies](#)
[Accessibility](#)

[Wiley Research DE&I Statement and Publishing Policies](#)
[Developing World Access](#)

HELP & SUPPORT

Contact Us
Training and Support
DMCA & Reporting Piracy
OPPORTUNITIES

Subscription Agents
Advertisers & Corporate Partners

CONNECT WITH WILEY

The Wiley Network
Wiley Press Room



IN SEARCH OF A SELF IN THE NOVELS *THE BLUEST EYE* BY TONI MORRISON AND *THE GOD OF SMALL THINGS* BY ARUNDHATI ROY

JANE THERESA

Assistant Professor,

English,

SSET, SCMS Ernakulam.

(KERALA) INDIA

ABSTRACT

*There is a quoting in the Holy bible by St Mark, stating that the stones which the builders rejected became the cornerstone of the building, that was the Lord's doing and it's amazing in our eyes .The one who is oppressed, the rejected stone, due to the policies and systems that are developed on the needs of the elite will become the corner stone of the world. All are God's creation and people should realize that even the most marginalized bear the image of God. Everybody has the right to live the life in its fullness. This paper compares the Afro American oppression in Toni Morrison's *The Bluest Eye* and Indian dalit oppression in Arundhati Roy's *The God of small things*. Both the novels use the themes of racism and oppression to underscore the effects of post-slavery. Oppression of the downtrodden is seen in every corner of the world. The literature of Afro American is similar to dalit literature as both are records of the tragedy of their respective histories .The different setting and era in each novel suggest that the oppression and inequality had changed very little even after years later. Dalit literature and African American literature makes the readers understand their respective society and gives the answers of the fundamental questions of life and dignity. The paper also focuses on the oppression of many women who consider them as marginalized. Because of their gender, women are not valued and not respected in the society all over the world. This tragedy is examined through the works of Toni Morrison's *The Bluest Eye* and Arundhati Roy's *The God of Small Things*. Given that the two societies are different in terms of place and time, it is understandable that there should be certain limitations and differences in their literatures. On the other hand, there are similarities too. This paper is the study of similarities in Toni Morrison's *The Bluest Eye* and Arundhati Roy's *The God of Small Things*.*

INTRODUCTION

JANE THERESA

1P age



Arundhati Roy born on 18th February 1931 is a Nobel Prize and Pulitzer Prize winner. Her novels are known for their epic themes, vivid dialogue and richly detailed black characters. Her novels reflect the experience of the black community. *The Bluest Eye* is a novel which focuses on the experience of black women, the existence of the black women's desperate bid for survival in a white man's world. For Toni Morrison, the black artist has a responsibility to the black community, a quality of hunger and disturbance that never ends. Her novels bear witness to the reality of the black community and the reality of the blacks who survived under different circumstances. Morrison's novel is the true voice of the blacks in its original power. Morrison leads her readers to an understanding of racism. Even after the abolition of slavery, the whites have still continued to treat black women under subjection in the matter of the concept of beauty arising self hatred among the black women. The characters of both Alice Walker and Morrison show that they don't exist and always compared them to the whites.

The Bluest Eye deals mainly with the predominant idea of beauty of whites upon the blacks. This novel shows the reader that the concept of beauty is socially constructed.

"Here is the house. It is green and white. It has a red door. It is very pretty."(Morrison 18)

Mother, Father, Dick and Jane live in a pretty green house. The green symbolises that there is life and soul in the house. The red door symbolises the mystery in the story. White symbolises innocence and virginity. In the prologue the author focuses on Jane who wishes to play. Jane sees a cat, but the cat did not play with her. Jane's mother laughs but does not play with her. Her father smiles, but does not play with her. At last a friend comes to play along with Jane. The prologue is repeated word for word, a second time without punctuation. The paragraph is repeated a third time without punctuation and spaces between the words, which transforms the narrative into a rambling and disorienting block of text. The shift from oriented text to the rambling text makes the reader feel that the situation of isolation among the black girl is getting intense and torturous.

"Our house is old, cold and green. At night a kerosene lamp lights one large room. The others are braced in darkness peopled by roaches and mice."(Morrison 26)

A nine year old Claudia serves Morrison as the narrator of the story who is confused but sensitive witness to Pecola's tragedy. The central story is about eleven years old Pecola who is raped by her father and bears his child. The baby dies as it was premature and Pecola sinks into madness, with a notion that she has been granted her wish to have blue eyes and believes that now she is the most beautiful in the eyes of White Americans.

JANE THERESA

2P a g e



When we compare the novels *The Bluest Eye* by Toni Morrison and *The God of Small Things* by Arundhati Roy, both blacks and dalits have remained outside their culture excommunicated and exile. Afro Americans were brought directly from Africa to America to become slaves. Forced into slavery all that was left to the black man was his African soul. The blacks were vastly different from the white races. The black Americans are very concerned about the land of his origins. As the years went by legislatures abolished slavery and thereby the black gained freedom. But the inferiority was witnessed in every field they interacted.

The dalit in India is in similar situation. They were excluded from the society. They have been stripped of their dignity and denied basic human rights. They were considered untouchables implying that anybody touching them would be polluted. They were denied access to roads, temples, schools, etc to avoid pollution of other castes. Arundhati Roy's *The God of Small Things* is one such remarkable work which shows the sufferings and sorrows of the Dalits in a unique style. Booker Prize winner and activist-author Arundhati Roy is usually praised for her efforts in trying to represent the marginalised in her writing. All over the world every society has two categories of people, the higher level and the lower level. The people belonging to the higher level are at the top and they govern and exploit the people belonging to the lower level. Even though many political and economical changes have happened all over the world, the mindset of the people has not changed across the different cultures as well as the social discrimination against them even continue today. If the Dalit is the subjective of India's boycotted society, the African American is the self of Black America. One is abandoned and degraded by the White society and the other by Savarna society. One is brought and sold from their own home land and the other was called untouchable by birth. The women who belong to these outcastes are treated as marginalized. In both Dalit and Afro American society girls have a debased self image. Marginalised women discover themselves in both race and gender discrimination. The aim of this paper is to analyze the suppressed people's state in Arundhati Roy's *The God of Small Things* and Toni Morrison's *The Bluest Eye*. In both novels, the women struggle to survive in the world they live in because of their womanhood. A cross cultural study of both dalit and the black shows the cruel enslavement of both these two groups. The cruel oppression based on caste and race is responsible for the deprivation of the lives of the blacks and dalits.

When we look into Toni Morrison's *The Bluest Eye*, the blacks have to suffer a lot for their identity.

"We know she is offering us something precious and that our pride must be arrested by refusing to accept." (Morrison 25)



The black characters in the novel consider themselves as inferior when they interact with whites. The story centres on the lives of two black families, the Mac Teers and the Breedloves. The story is based on the children Claudia, Freeda and Pecola, their happy and painful experiences in growing up. The girls often had a loving conversation about how cute Shirley Temple was. Shirley Temple had golden curls, pink cheeks and blue eyes. Everyone loved her. Pecola had black skin. She was so poor and ugly.

“The Breedloves did not live in a storefront because they were having temporary difficulty adjusting to the cutbacks at the plant. They lived there because they were poor and black, and they stayed there because they believed they were ugly.”(Morrison 53)

The blacks believed that their poverty was traditional and stultifying, it was not unique. But their ugliness they believed that was unique. No one can convince them that they were not relentlessly and aggressively ugly. In her eleven years, no one had ever noticed Pecola. Each night Pecola prayed for blue eyes.

“Frieda brought her four graham crackers on a saucer and some milk in a blue and white Shirley Temple cup. She was long time with the milk, and gazed fondly at the Silhouette of Shirley Temple’s dimpled face.”(Morrison 35)

The whole novel explores the psychological and sociological changes in the protagonist, Pecola. Claudia was younger than both Frieda and Pecola. She had not yet arrived at the turning point in the development of psyche which would allow loving white dolls. During Christmas all exchanged gifts of big, special, blue eyed baby dolls.

“I was physically revolted by and secretly frightened of those round moronic eyes, the pancake face and orange worm’s hair.” (Morrison 36)

Pecola is the character who wants herself to look like the whites and wishes for the blue eyes. She believes that the symbol of white beauty is the blue eyes. She was having a wrong notion that only blue eyes would make her beautiful and believed that only blue eyes will help her in gaining her self-respect. As her eyes can never be altered into blue eyes in reality, her quest for blue eyes ends in madness. She cannot even look at a white girl as she believes that whiteness is the only standard of beauty and satisfies her envy by destroying white dolls.

“I fingered the face wondering at the single stroke eyebrows picked at the pearly teeth stuck like two piano keys between red bowline lips. Traced the turned –up nose, poked the glarcy blue eyeballs, and twisted the yellow hair. I

JANE THERESA

4Page



could not love it. But I could examine it to see what it was that all the world said was lovable.”(Morrison 37)

“I destroyed white baby dolls.”(Morrison 38)

The truly horrifying thing was the transference of the same impulses to little white girls. Black females possess hatred towards white women because of the set beauty concept by the society. The staring looks of the whites towards the blacks make them feel that they are ugly and unworthy.

“I saw a pair of fascinated eyes in a dough- white face.” (Morrison 46)

Toni Morrison shows that not all African Americans mindset are dominated by an oppressive culture. Some are very bold enough to survive in the midst of these oppressions. For example, the characters Claudia, the nine year old who is the narrator of the story is against the notion of the white standards of beauty. An independent and strong-minded nine-year-old, Claudia is a fighter and rebels against adults’ tyranny over children and against the black community’s idealization of white beauty standards. She has not yet learned the self-hatred that plagues her peers. She consciously deconstructs the ideology of the dominant society and understands the fact that a doll is a consumer item and tries to constrict Pecola by her destruction of white dolls.

“Younger than both Frieda and Pecola , I had not yet arrived at the turning point in the development of my psyche which would allow me to love her.”(Morrison 35)

In the novel Toni Morrison challenges the white standards of beauty and demonstrates that the concept of beauty is socially constructed.

“Cholly, whose ugliness (the result of despair, dissipation and violence direct toward petty things and weak people) was behaviour, the rest of the family – Mrs.Breedlove, Sammy Breedlove and Pecola Breedlove wore their ugliness, put it on, so to speak, although it did not belong to them.” (Morrison 54)

The Breedlove family are blacks who can never be like whites. Even though human beings look different, the soul is same. This realisation can bring some changes in the beauty concept. The whites looked at the blacks and wondered why they are so ugly. They observed them carefully to find the source of this ugliness which the blacks considered as staring. The realisation was that the ugliness came from conviction. They began to believe that some mysterious all knowing master had given each one a choke of ugliness to wear and they had

JANE THERESA

5P a g e



each accepted it without question. In the novel we can see that ugliness is something which can never be altered or changed, it is inherited from a powerful master.

“You are ugly people. And they took ugliness in their hands, threw it as a mantle over them, and went about the world with it.” (Morrison 55)

The novel helps the readers to understand that the standard of beauty is created by oneself. If the blacks value their blackness; they can subvert the ideology put forward by the white society. The background of the novel is racism, sexism and classicism which signifies the traumatic condition under which African Americans lived in White America. The restrictions upon the blacks affected their lives especially the women. They were always marginalised. The reason for the backwardness black people is because of the self hatred persuaded by white domination. Many of them considered themselves as inferior to the white women which ended in self hatred. They trust in their own unworthiness which is interpreted into ugliness. They considered themselves as unworthy for the society.

Throughout the novel, there are many incidents which show the feeling of separation and pain faced by Pecola Breedlove because of being black.

“If those eyes of her’s were different, that is to say, beautiful, she herself would be different. Her teeth were good and at least her nose was not big and flat like some of those was thought so cute.” (Morrison 62)

The novel shows several incidents which depicts the kind of world into which Pecola has been born. Pecola’s mother, who works as a house keeper in a white family, loves her employer’s children, ignoring her own daughter. No one expresses pity on her. Pecola is hurt not only because of her race but also because of her gender. Each night without fail she prayed for blue eyes. She has seen the hatred in the eyes of all white people. So she believed that the distaste must be for her blackness.

“A picture of little Mary Jane, for whom the candy is named. Smiling white face, blonde hair in gentle disarray, blue eyes looking at her out of a world of clean comfort. The eyes are petulant and mischievous”. (Morrison 66)

For the three girls to eat the candy was to eat Mary Jane. Throughout the novel, the author describes the mentally agonizing thoughts of these girls battling with the cultural standards of beauty that have been impaired upon them.

When we read the novels *The God of Small Things* by Arundhati Roy and *The Bluest Eye* by Toni Morrison, a lot of similarities in the mental thoughts of the characters can be observed.

JANE THERESA

6P a g e



Just like racism which is a prominent factor in dividing people in Western history, the caste system, a deep-rooted factor which is a shame for Indian culture, affects the socio-economic and socio-cultural systems of Indian society. Untouchables are the most exploited and unwanted ones. Some scholars believe that the Aryans, a fair-skinned race which invaded India had controlled and subjugated the dark-skinned aborigines placing them at the lower strata of society. Both the Dalits and the African Americans are distinctive groups that occupy a similar position in their respective societies- the bottom of the socio-economic hierarchy. In the famous essay, *Can the Subaltern speak?* By Gayathri Spivak, the writer suggests that the subaltern cannot have a history of his or her own and cannot have a voice if the subaltern is a female. She cannot be heard at all because she exists in absolute silence.

“The subaltern as female is even more deeply in shadow.” (Spivak 28)

In *The God of Small Things*, small things referred in the title are the subaltern people who are considered as small worthless creatures by most of the upper caste people. In reality these small people are the big ones who can bring a change to the whole system created by the society. These are the voice that should be given their voice, the voice that should be heard against the unreasonable hate, revenge and violence. The characters in the novel have their unfulfilled desires and are punished and silenced by the system in various ways. The women in *The God of Small things* are mostly confronted with marital and family problems. Estha and Rahel’s mother Ammu married Babu; however Babu turns out to be an alcoholic and even urges her to sleep with his boss, Mr. Hollick. After this incident Ammu leaves him and returns with the twins Estha and Rahel. Although a divorced daughter is a disgrace to a traditional Indian society, a divorcee son is not. Chacko, Ammu’s brother, is also a divorced but he returned to take charge of the family pickle business. The patriarchal privilege disproportionately over the other in the lives of the brother and sister. Ammu then falls into a love affair with Velutha, an untouchable.

“Ammu travelled upwards through a dream in which a cheerful man with one arm held her close by the light of an oil lamp. He had no other arm with which to fight the shadows that flickered around him on the floor.” (Roy, 215)

Ammu defies patriarchal domination, class and caste prejudice in public and pays with her life. Roy’s protagonists suffer from lack of parental love, disturbed infancy, broken homes. They are dissatisfied with their existence. They often choose to go out of the mainstream of life. This alienation generally manifests in immoral ties and activities. Alienation from their selves leads to a frantic search for their identity in the milieu through self-discovery and self-identification. She is banished from home and society because of this secret relation and she dies in another place because of this abandonment. Her relationship with Velutha is



considered to be a sin, as it is extra-marital and a crime as it is between the members of two different classes in the caste system.

“If he held her, he couldn’t kiss her. If he kissed her, he couldn’t see her. If he saw her, he couldn’t feel her.” (Roy, 215)

A related inferiority complex is evident in the interactions between untouchables and touchable in Ayemenem. Vellya Paapen is an example of an Untouchable so grateful to the touchable class. He is willing to kill his son, Velutha, when he discovers that Velutha has broken the most important rule of class segregation that there be no inter-caste sexual relations. A love-affair between Ammu and Velutha results in his brutal beating by a group of policemen. The beating takes place in front of the twins. This results in his death.

“If they hurt Velutha more than they intended to, it was only because any kinship, any connection between themselves and him, any implication that if nothing else, at least biologically he was a fellow creature had been served long ago. They had no instrument to calibrate how much punishment he could take. No means of gauging how much or how permanently they had damaged him.” (Roy, 309)

In part, this reflects how many untouchables have internalized caste segregation. Nearly all of the relationships in the novel are somehow coloured by cultural and class tension. Roy’s women characters in the novel are exploited. They are torn between their individuality and social obligations. Ammu sacrifices her life in her quest for identity. Estha is described as occupying very little space in the world. Ammu dies alone and sad, beaten by the world. Shadows gathered like bats in the steep hollows near her collarbone. Rahel never quite fits in, especially in such rigid confines as boarding schools. Velutha is the smallest of the small, as Ammu points out, calling her Ammukutty, ‘Little Ammu’, though she was so much less little than he was.

“If he touched her, he couldn’t talk to her, if he loved her he couldn’t leave, if he spoke he couldn’t listen, if he fought he couldn’t win.” (Roy ,330)

Ammu, on the other hand, defies the notion of the male-oriented society. She emerges as a rebel, voicing her suppressed voice. The capitalist society always treated women figures as commodity. They have no right over their body. Before marriage, they are under parental guidance and after marriage, under husband’s care. That’s why; we see that Ammu is denied of her college education whereas Chacko goes to Oxford. Even Ammu has no right in her father’s property. Mammachi, Baby Kochamma all accepted the female role-model imposed on them by the society – docile, submissive, ungrudging, stoic resignation. In the novel,

JANE THERESA

8P a g e



Velutha becomes the central and essential character and a sort of divinity in the eyes of the twins. Velutha is the children's only father figure and a true friend. Mammachi, Baby Kochamma, the policemen, in their realms of power, see to it that Ammu, Velutha, Rahel and Estha who hold no power in the social hierarchies remain vulnerable and overruled. Ammu, Velutha and the Twins, who get together for mutual love and warmth and not for any material gains are crudely acted upon and destroyed. The children who are the small things in the novel go against the rule and make Velutha their God, The God of Small Things.

The caste and gender hierarchies in India are equally relevant to the race and class as seen in *The Bluest Eye*. In both the novels, the children become victims of the communal response of the oppressed. By employing child narrators, both Morrison and Arundhati Roy explore how children negotiate different binaries between the beauty concepts, between male and female privileges, between higher and lower economic classes' and between upper and lower caste. The painful stories of Ammu and Pecola shows the authors concern for the silences that illustrates self destruction.

WORKS CITED

1. Morrison, Toni. "The Bluest Eye", New York: Rinehart and Winston, 1970. Print
2. Roy, Arundhati. "The God of Small Things". London: Penguin Books, 1997. Print.
3. Spivak, Gayatri. "Can the Subaltern Speak?" Marxism and the Interpretation of Culture. Eds. Cary Nelson and Lawrence Grossberg. London: Macmillan, 1988. Print

ACCEPTED MANUSCRIPT

An Experimental Investigation on Wear and Corrosion Characteristics of Mg-Co nanocomposites

To cite this article before publication: Raghav G R *et al* 2018 *Mater. Res. Express* in press <https://doi.org/10.1088/2053-1591/aac862>

Manuscript version: Accepted Manuscript

Accepted Manuscript is “the version of the article accepted for publication including all changes made as a result of the peer review process, and which may also include the addition to the article by IOP Publishing of a header, an article ID, a cover sheet and/or an ‘Accepted Manuscript’ watermark, but excluding any other editing, typesetting or other changes made by IOP Publishing and/or its licensors”

This Accepted Manuscript is © **2018 IOP Publishing Ltd.**

During the embargo period (the 12 month period from the publication of the Version of Record of this article), the Accepted Manuscript is fully protected by copyright and cannot be reused or reposted elsewhere.

As the Version of Record of this article is going to be / has been published on a subscription basis, this Accepted Manuscript is available for reuse under a CC BY-NC-ND 3.0 licence after the 12 month embargo period.

After the embargo period, everyone is permitted to use copy and redistribute this article for non-commercial purposes only, provided that they adhere to all the terms of the licence <https://creativecommons.org/licenses/by-nc-nd/3.0>

Although reasonable endeavours have been taken to obtain all necessary permissions from third parties to include their copyrighted content within this article, their full citation and copyright line may not be present in this Accepted Manuscript version. Before using any content from this article, please refer to the Version of Record on IOPscience once published for full citation and copyright details, as permissions will likely be required. All third party content is fully copyright protected, unless specifically stated otherwise in the figure caption in the Version of Record.

View the [article online](#) for updates and enhancements.

An Experimental Investigation on Wear and Corrosion Characteristics of Mg-Co nanocomposites

G.R.Raghav¹, A.N.Balaji^{2*}, D.Muthukrishnan³, V.Sruthi⁴, E.Sajith⁵

^{1,2,3}Department of Mechanical Engineering, KLN College of Engineering, Pottapalayam, Sivagangai Dt. Tamilnadu, India630612

⁴Department of Basic Science and Humanities, SCMS School of Engineering & Technology, Cochin, Kerala, India 683582

⁵Department of Mechanical Engineering, SCMS School of Engineering & Technology, Cochin, Kerala, India 683582

* Corresponding author: A.N.Balaji, E-mail: balajime@yahoo.com

Abstract:

In this research, Mg-Co nanocomposites were synthesized using powder metallurgy process. The impact of Co nanoparticle reinforcements on the hardness, wear and corrosion characteristics of Mg-Co nanocomposites were investigated. The dry sliding wear of the Mg-Co nanocomposites was examined using pin-on-disc apparatus under various loading conditions. The results substantiate that the hardness (70 HV) and wear resistance of Mg-25Co were higher than pure Mg (25 HV). The morphological analysis of Mg-based nanocomposites has been carried out using Scanning Electron Microscope and Atomic Force Microscope. The electrochemical corrosion analysis reveals that the increase in Co content in Mg matrix decreases the corrosion rate. The Mg-25Co nanocomposites shows better corrosion resistance ($I_{corr} = 0.397 \times 10^{-3} \mu A/cm^2$) than that of Pure Mg ($I_{corr} = 0.544 \times 10^{-3} \mu A/cm^2$). An increase in Polarization resistance (R_p) also authenticates the increase in corrosion resistance of Mg-25Co nanocomposites. The EIS spectroscopy results reveal that the charge transfer resistance (R_{ct}) has enhanced from $14.44 \Omega cm^2$ for the pure Mg to $42.50 \Omega cm^2$ for the Mg-25Co nanocomposites.

Keywords: Wear, Corrosion, Dental implants, SEM, EDAX

1. Introduction

Generally, the orthopaedic implants are made up of metals because of their substantial mechanical properties such as ductility and formability. The potential biodegradable material which is attracting more potential research is Mg and its alloys because of its biocompatibility, physical and mechanical properties[1–5]. The Mg with a density of about 1.74 g/cm^3 makes it much lighter than of other biodegradable metals and is appropriate for dental and orthopaedic implants. Besides the Mg has poor corrosion resistance which limits the application of Mg alloys in dental and orthopaedic implants[6–8].

Another such kind of metal is cobalt and cobalt-based alloys which are most potent and widely suited for dental and orthopaedic implants owing to its high corrosion and wear resistance along with its high strength[9–15]. The most common alloying element of Mg-based composites is Cr, Mo, Ni, etc. so as to improve the wear and corrosion resistance properties. The major concerns of Cr, Mo, and Ni reinforcements are the development of Carbides which in turn reduces the ductile property of the composite. The other major entanglement is the release of dangerous ions and particles which can result in adverse effects such as allergy, toxicity and carcinogenic issues[13,14,16–19].

AjithKumar.K. K et al [3]studied the dry sliding behaviour of Mg-Si alloys prepared using gravity casting method. The results show that the wear rate decreases with the increase in Si Content in Mg matrix. Renqi Ma et al investigated the effect of Co reinforcement in WC using spark plasma sintering the results shows that the fracture toughness increases with increase in Co content[10].

So by considering the important properties of Mg andCo, it is proposed to study the effect of reinforcement of Cobalt in the Mg-based composite. The studies on Mg-Co alloys have been rather limited especially on tribological and corrosion behaviours[20,21]. In this work,Mg-Co nanocomposites for potential dental implants were prepared using powder metallurgy process. The various wear mechanisms were studied using pin-on-disc apparatus under different loading and sliding conditions. The corrosion characteristics of the composites were analyzed using electrochemical methods.

2. Materials and Methods

2.1 Materials:

The magnesium (600 μm) and cobalt (100 μm) powders (research grade) of purity levels 99.5% and 99% respectively were used as matrix and reinforcements in this work. The particle size, microstructures and presence of Mg and Co are analyzed using SEM and EDAX.

2.2 Preparation of Composite materials:

Table.1 shows the different proportions of composites that were prepared in this work. The various proportions of Mg and Co were milled under the presence of Toluene in high energy ball mill [Fritsch pulverisette, Germany] at 300 rpm for 5h with Tungsten Carbide balls so as to obtain a homogeneous composite mixture. The Toluene was used in order to provide uniform, perfect mixing and also to avoid unwanted reactions. The powder to ball ratio was maintained at about 1:20. The Blended composite mixtures are then fed into a cylindrical die of 10 mm diameter and compacted using the hydraulic press at a load of 500 Mpa. The green compacts are then sintered at the temperature of about 550^o C for 1h in a muffle furnace under argon atmosphere in Contemplation of obtaining a composite pellet.

2.3 Micro hardness:

The contact surfaces of the sintered composites were polished using abrasive papers of grades 600, 800 and 1000 in order to remove any impurities present at the contact surfaces. The microhardness of the composite pellets was studied using Vickers hardness tester at a uniform load of 5 kg. The dwell time was maintained at about 20 sec.

2.4 Characterization

The surface topographies of Mg–Co nanocomposites were studied using Atomic Force Microscopy (XE70, Park System, South Korea). The morphological characterization of the Mg-Co nanocomposite was done using SEM (Hitachi SU1510, Secondary Electron Mode, 10 KV, the emission current of 96 μA). The compositional analysis of specimens was analyzed using EDX (QUANTAX - Bruker).

2.5 Wear analysis:

The Mg-Co composite pellets of 10 mm diameter and 30 mm in height were used as the test specimen. The dry sliding wear analysis was performed according to ASTM: G99 standards

1
2
3 using pin-on-disc apparatus (DUCOM, Bangalore). The tribological studies of the composite
4 pellets were analyzed considering the criteria's such as applied load, sliding distance and sliding
5 speed for five respective trials (n=5) and the mean values were considered. The composite pellets
6 were measured before and after the wear analysis using an electronic weighing scale to
7 determine the weight loss due to wear mechanism.
8
9

10 11 12 **2.6 Potentiometric Polarization test:**

13
14 The potentiometric polarization analysis was used to explore the electrochemical
15 corrosion behaviour of Mg-Co nanocomposites. The potentiometric tests were premeditated
16 using Biologic SP-150 potentiostat. The investigations were performed using three electrode cell
17 consists of platinum wire counter electrode Ag/AgCl reference electrode and the Magnesium-
18 Cobalt nano composite pellet as a working electrode. The polarization tests were carried out at
19 room temperature with the 5 wt. % NaCl solution. The composite pellets were polished with
20 emery paper which was rinsed with acetone and double distilled water prior to the
21 electrochemical tests. The Mg-Co nanocomposite working electrodes were immersed in the
22 electrolytic solution of 5 wt. % NaCl for 1 h in order to reach steady state open circuit potential
23 and the OCP was measured. The scan rate was maintained at 5 mV/s. The corrosion potential
24 E_{corr} and current density I_{corr} were calculated using EC lab software through Tafel fit
25 extrapolation.
26
27
28
29
30
31
32
33

34 35 **2.7 Electro Chemical Impedance Spectroscopy:**

36
37 The electrochemical impedance spectroscopy (EIS) for the composite specimens was
38 executed at the range of 100 kHz to 100 MHz and 10 mV initial sinusoidal voltage. The Biologic
39 SP-150 electrochemical workstation was used to carry out experiments with open circuit
40 potential. The EC-lab software was then utilized for fitting and analyzing the raw EIS
41 data.[22,23]
42
43
44
45

46 47 **3 Results and Discussion:**

48 49 **3.1 Microhardness:**

50 The Fig. 1 shows the mean hardness values of Mg-Co composite samples for a sample
51 size of n = 10. From the figure, it is evident that the hardness of the composites increase hugely
52 with an increase in Co content owing to its inherent hard nature. The Mg-25Co composite has a
53 hardness of about 70 HV compared to that of pure Mg which has a hardness of 25 HV.
54
55
56
57
58
59
60

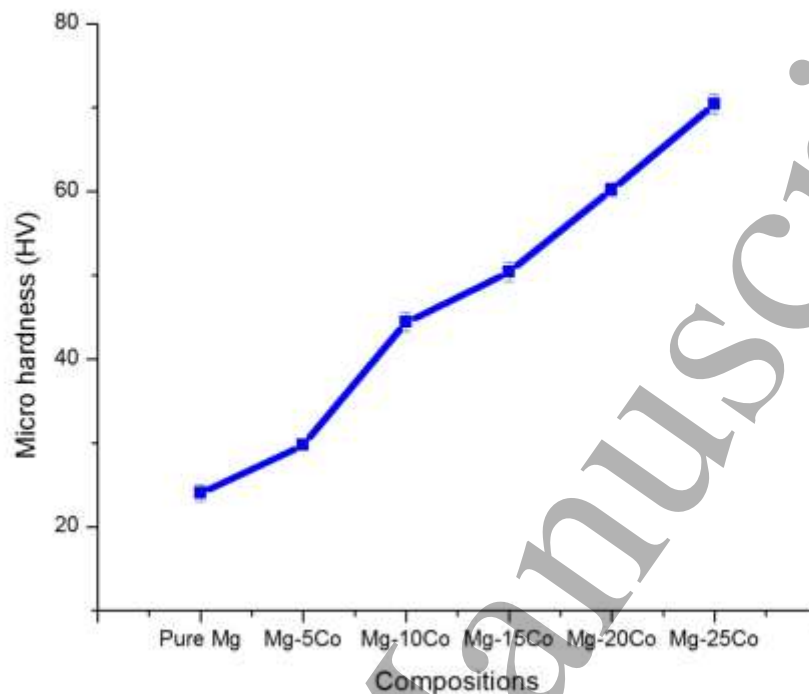
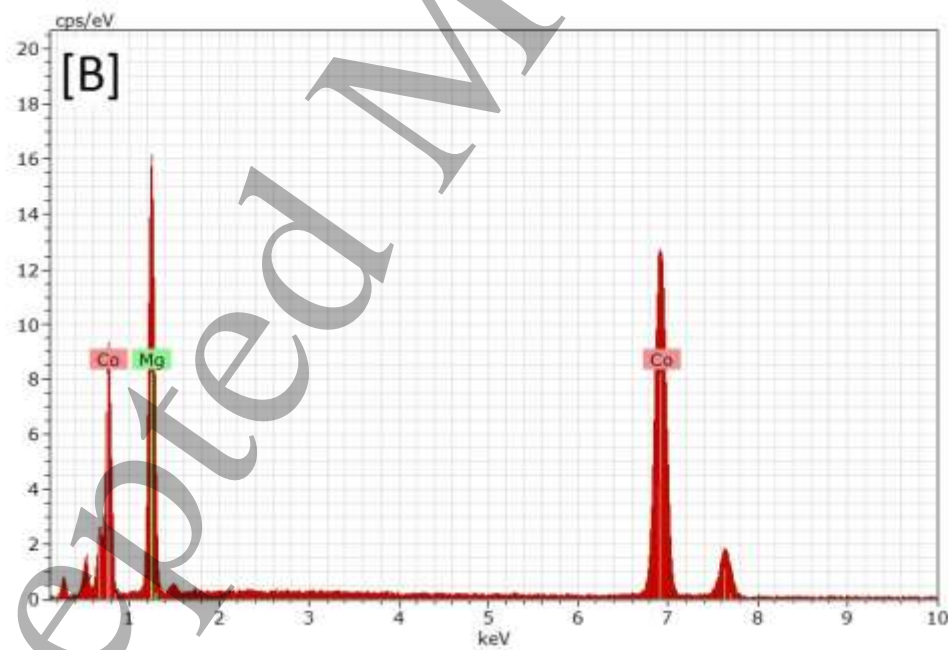


Fig.1 Graphical representation of micro hardness values of different composition of Mg-Co nanocomposites (Standard deviation σ).

3.2 SEM Analysis:

Fig 2.A& 2B shows the morphological structure and EDAX spectrum of Magnesium-Cobalt nanocomposites. The SEM image noticeably reveals the unvarying mixture of Mg-Co composites. The EDAX spectrum substantiates the presence of magnesium, cobalt and oxides in the composite material. The particle size of Mg and Cobalt were found to be in the range of 500 microns and 80-150 nm respectively. The Co nanoparticles were seen to be agglomerated.



52 Fig.2 SEM image [A] and EDAX Spectrum [B] of Mg-Co nanocomposite

53
54
55
56
57
58
59
60

3.3 AFM Analysis

Atomic force microscopy is one of the important tools in studying the topography of materials, with demonstrated resolution in the order of a nanometer. Fig 3, illustrate the 3D AFM Image which shows the stature and breadth of the Cobalt nanoparticles which is recognized to be around 10 – 20 nm and 300 nm respectively.

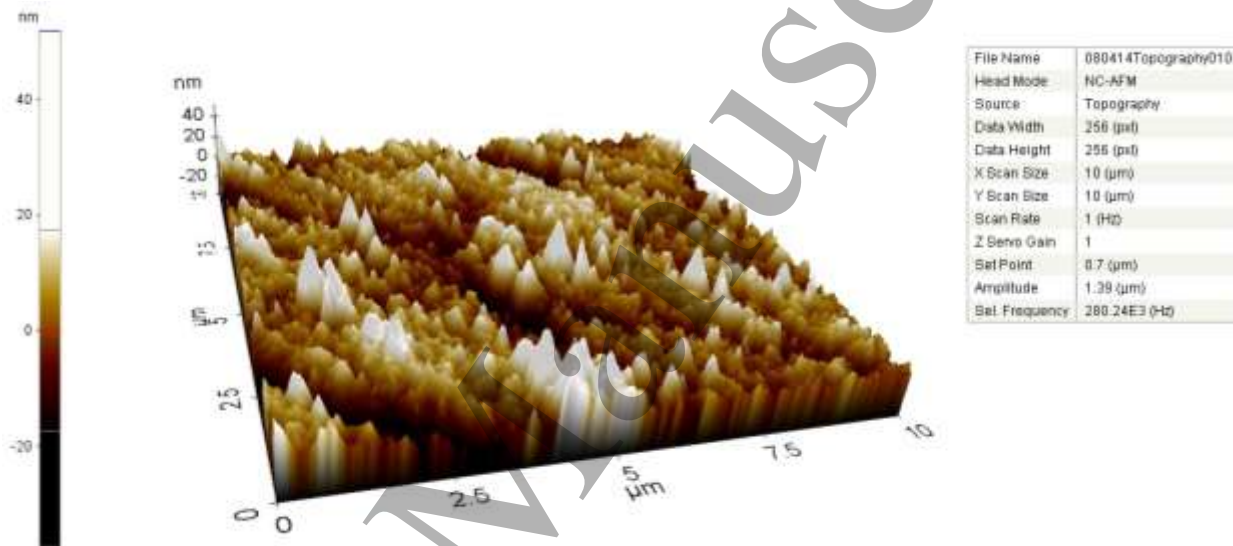
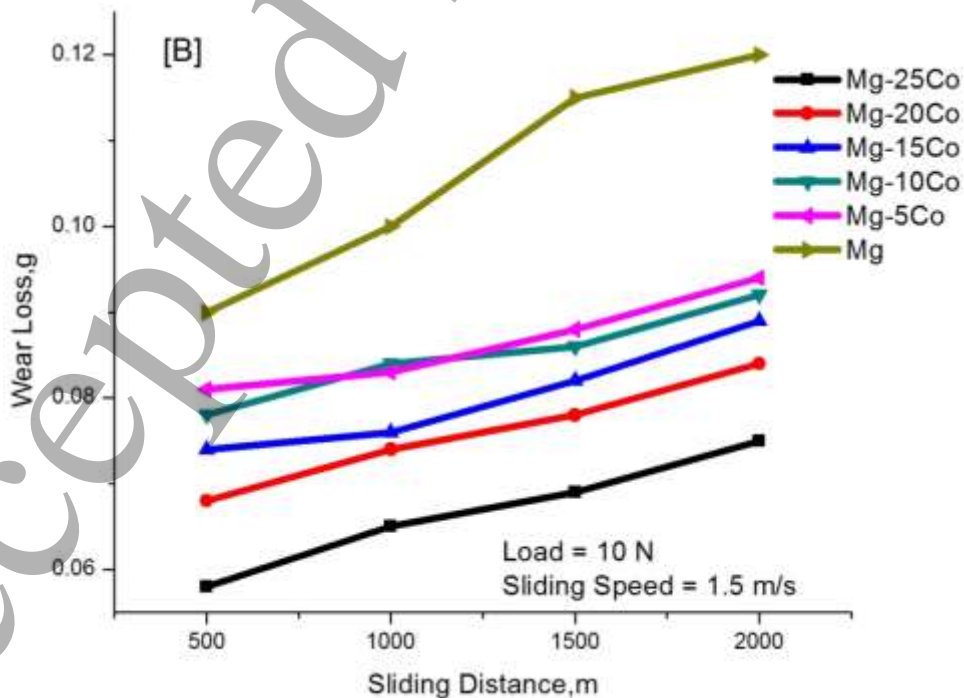
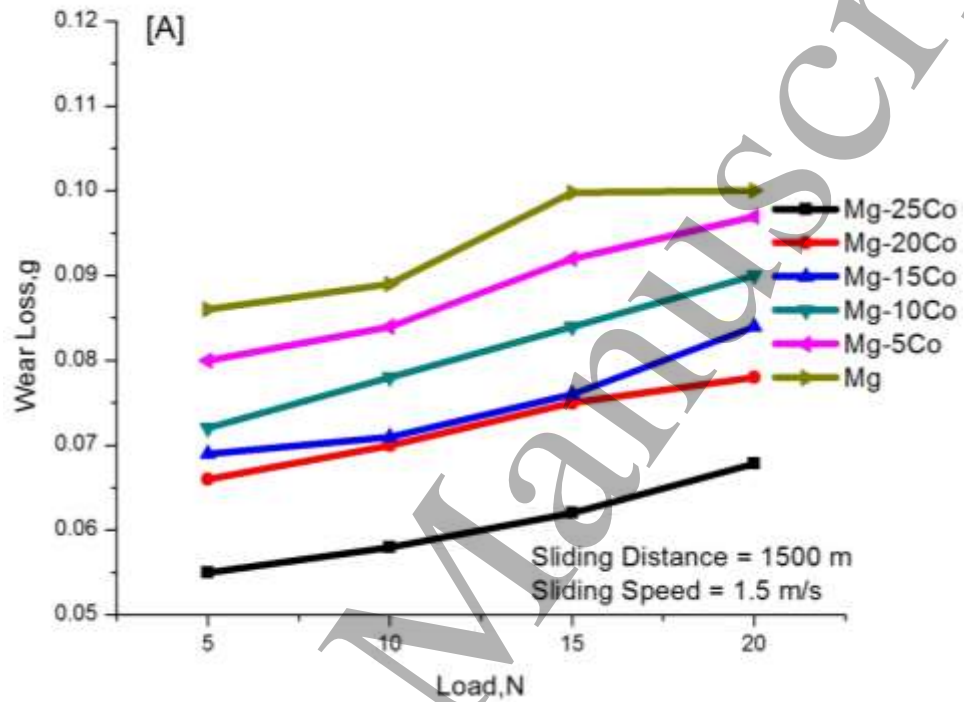


Fig.3 3D AFM Image of cobalt nanoparticles

3.4 Sliding Wear Analysis:

The investigation on wear is done using Pin-on-disc apparatus for the study of the Tribological behaviour of Mg-Co nanocomposites. From the Fig.4 we can add fact that the addition of Co decreases the wear loss of the composites as compared to that of pure Mg pellets. The outcome discloses that increase in the percentage of Cobalt in Mg matrix has further improved the wear resistance. The Mg-25Co nanocomposites have less wear loss than Mg-5Co. Fig.4 (A) shows the wear loss sustained by specimens at various loads ranging from 5 N to 20 N. From the graphs, it is perceptible that the Mg-Co composites show an increase in wear resistance at different loads and also with an increase in the percentage of Co. This may be due to hardening of composites due to the presence of Co in the composite pellets. The wear loss experience ranging from 500 m to 2000 m is shown in the Fig. 4(B). It can be noted that increase of Co content in nanocomposites decreases the wear loss which may be due to the hard nature of

Co reinforcements. The Fig.4(C) characterizes the trend of wear loss of composite materials at various sliding speed. From the figure, it is evident that the wear loss decreases with increase in sliding speed.



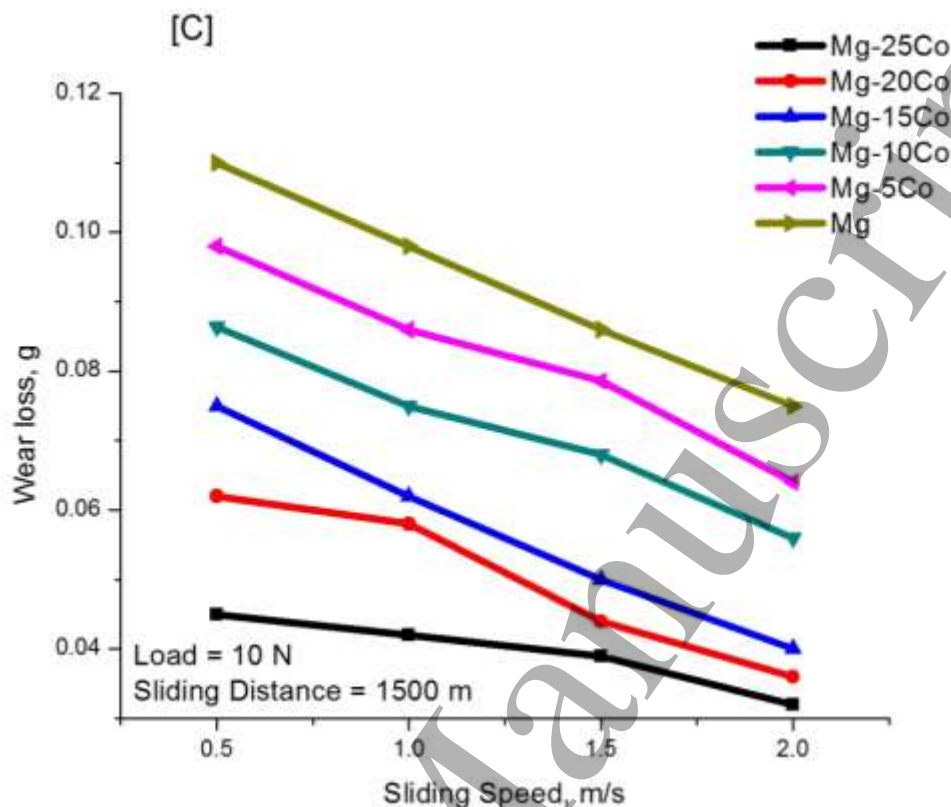
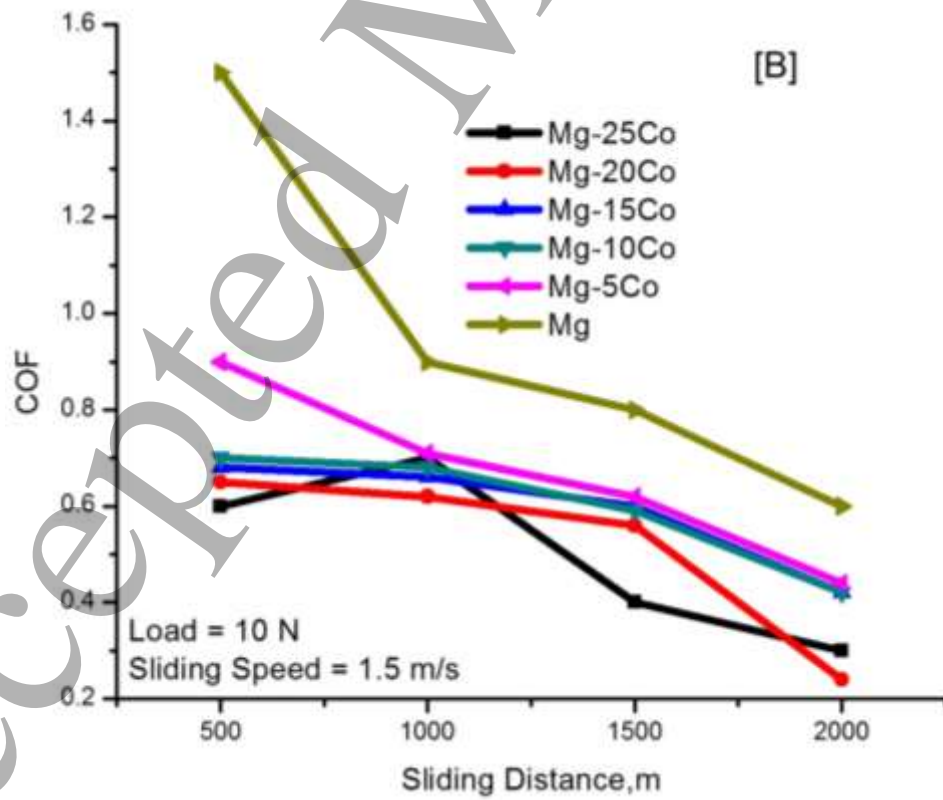
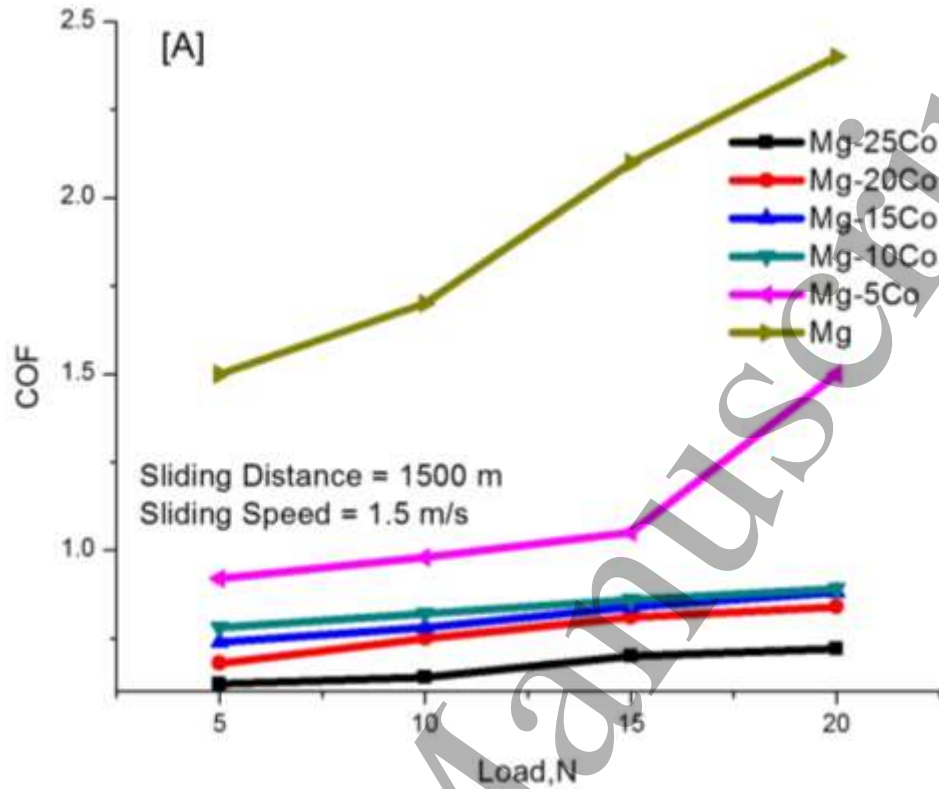


Fig.4 Wear Loss ($n = 5$) of Mg and Mg-Co nanocomposites (A) Applied Load, (B) Sliding Distance, (C) Sliding Speed

3.5 Coefficient of Friction Analysis (COF):

The Fig. 5 gives you an idea about the various trends of Coefficient of friction of Mg-Co composites. The COF decreases with increase in Co reinforcements; this is because of the inherent hard nature Co particles. The results uncover that the COF of Mg-25Co is lesser compared to that of pure Mg pellet. The Coefficient of friction of composite specimens is revealed in the Fig.5 (A) which discloses that the pure Mg has the higher COF with an increase in load but the COF of the composites remains more or less unwavering at various loading conditions. From the fig. 5(B) it is unmistakable that the COF values of Mg-Co composites show a considerable decline with the rise in sliding distance whereas the Mg has higher COF values. The evaluation of Fig.5(C) states that there is a linear decrement in COF values with a boost in sliding speed.



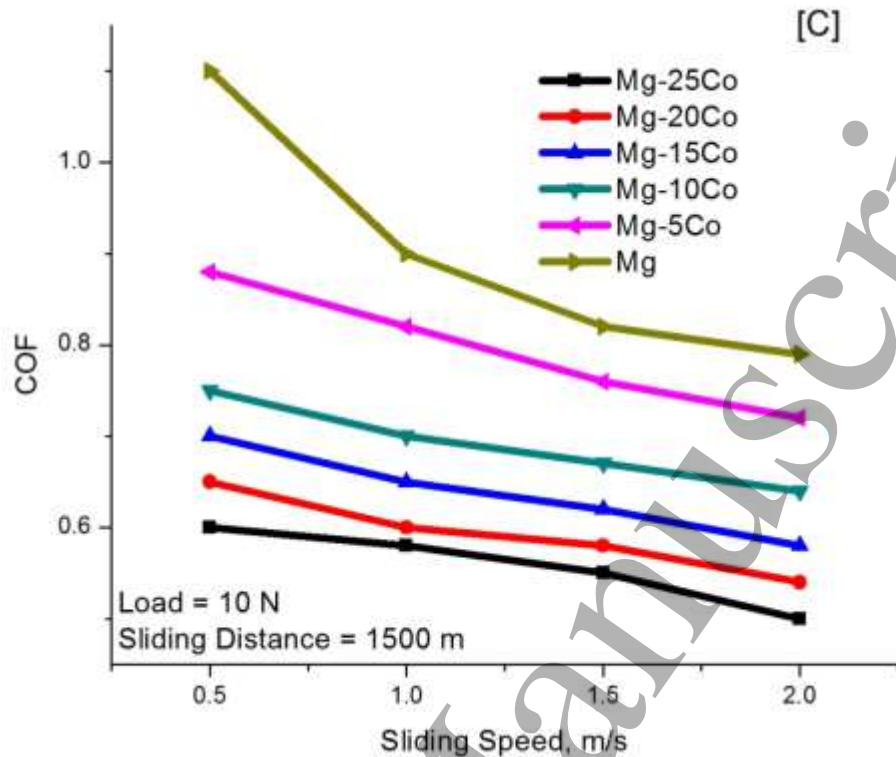


Fig.5 COF ($n = 5$) of Mg and Mg-Co nanocomposites (A) Applied Load, (B) Sliding Distance, (C) Sliding Speed

3.6 Worn out surface Analysis:

Fig 6 shows the surface morphology of Mg- 25Co nanocomposite pellet before the test, which shows the homogeneous diffusion of Cobalt in Mg matrix. Fig 7 A & B unveil the worn out surfaces of the Pure Mg and Mg-25Co nanocomposite pellets after sliding wear test. The scratches and grooves were formed in the direction of sliding which confirms the mechanism of wear due to abrasive wear involving the composite pellet and rotating disc. The SEM micrograph shows the formation of grooves in the subsurface microstructure of the pure Mg pellets which attributes to the abrasive wear as compared to Mg-Co pellets.

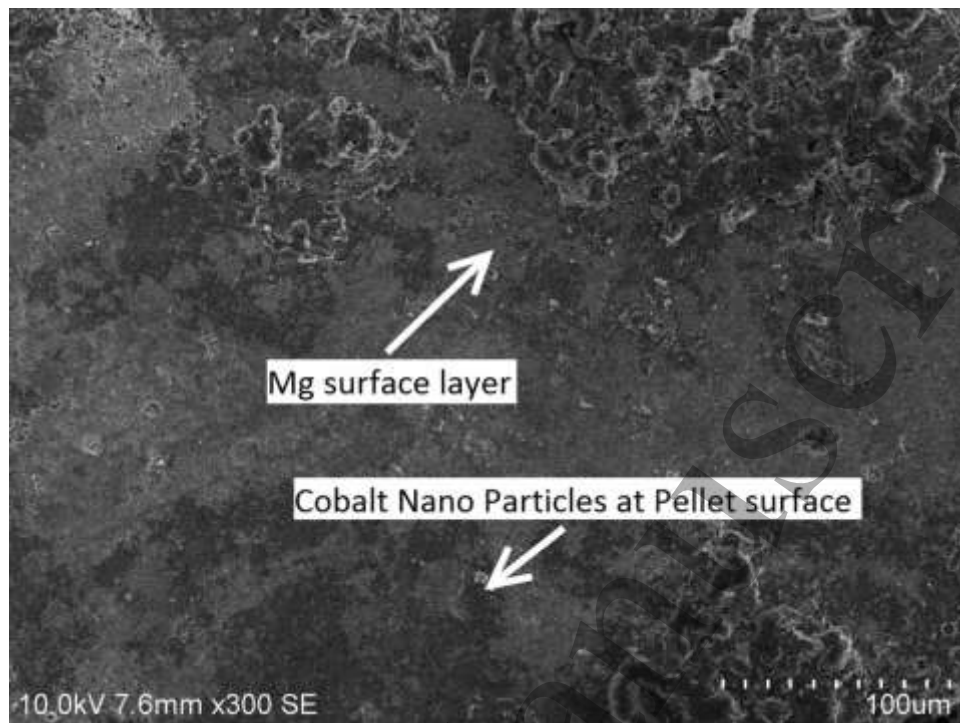


Fig. 6 SEM Micrograph of Mg- 25 Co nanocomposite pellet before Wear Test

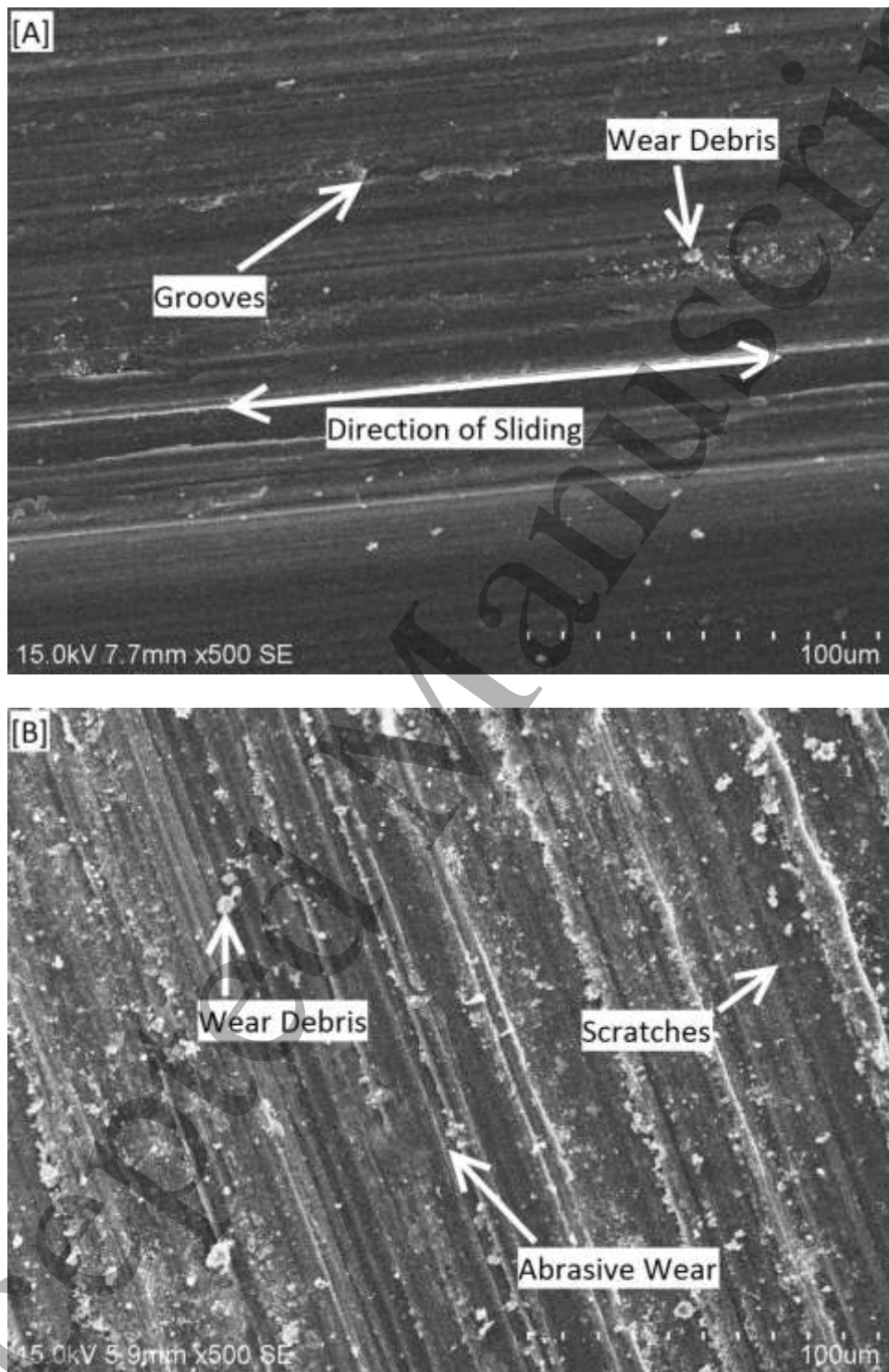


Fig.7 SEM Micrograph of Pure Mg (A) and Mg-25Co (B) nanocomposite pellet after the wear test

3.7 Potentiometric Polarization Analysis:

The potentiometric polarization investigation of the pure Mg and various compositions of Mg-Co composites in a 5 wt % NaCl solution is plotted in Fig.8; the graphs scheme against potential voltage and current density. The composite materials show unpassivated anodic and cathodic curves. The current density declines with increased potential voltage. This observable fact is due to the formation of Magnesium oxide layers at the facade of the specimen. The corrosion characteristics such as corrosion potential (E_{corr}), Current density (I_{corr}) and polarization resistance (R_p) are determined by Tafel extrapolation method. From the Table: 1 it can be comprehended that corrosion potential (E_{corr}) of Mg-25Co nanocomposites (-0.813 V vs Ag/AgCl) is decreased than that of pure Mg (-0.940 V vs Ag/AgCl) which confirms the increase in corrosion resistance of the composites. The Current density of the Mg-25Co nanocomposites ($0.397 \times 10^{-3} \mu\text{A}/\text{cm}^2$) has reduced considerably when compared to pure Mg ($0.544 \times 10^{-3} \mu\text{A}/\text{cm}^2$). The drop in current density reduces the intensity of the corrosion in composite specimens which in turn diminishes the rate of the corrosion. The polarization resistance (R_p) rises with accumulation in Co content in Mg matrix composites which also substantiate the reduction in corrosion rate of the Mg-Co nanocomposites [17,24–27]. The one way ANOVA statistical analysis for the corrosion potential (E_{corr}) of pure Mg and composite pellets confirm that there is a considerable increase in corrosion potential (E_{corr}) of the Mg-25Co nanocomposites when compared to pure Mg ($p < 0.05$) is shown in Fig.9. Further, the statistical analysis of the composite specimens has shown significant variation in corrosion current (I_{corr}). Fig.10 depicts the comparative variations in the corrosion current for each composite.

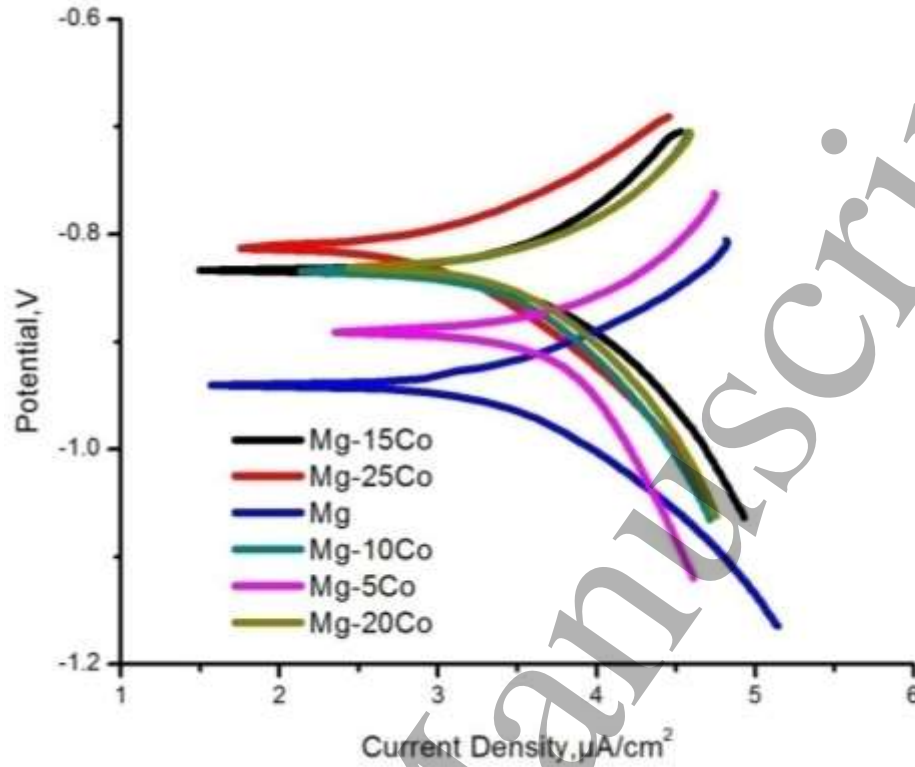


Fig.8 Potentiometric Polarization Curves of Mg and Mg-Co nanocomposites

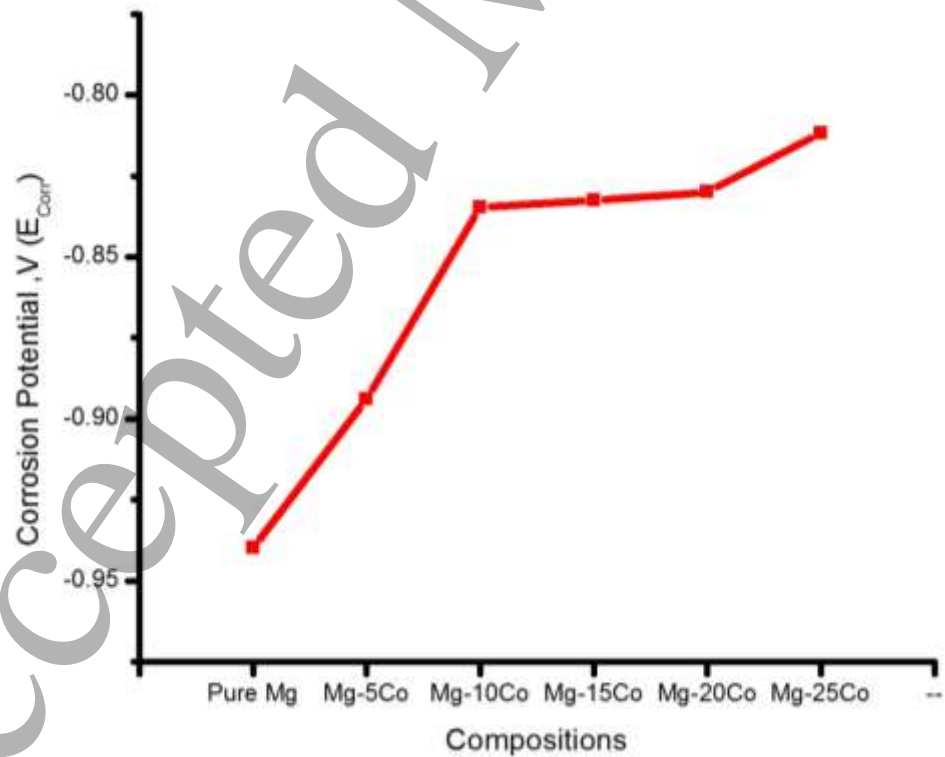


Fig.9 Statistical analysis of the corrosion potential (E_{corr}) of Mg and Mg-Co nanocomposites

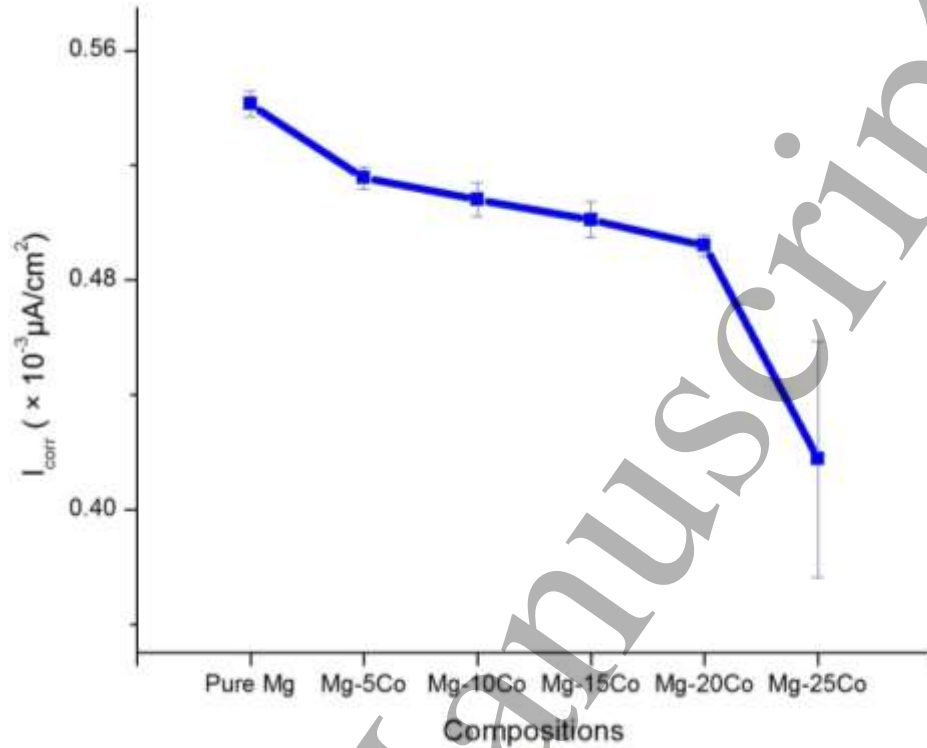


Fig.10 Statistical analysis of the corrosion current (I_{corr}) of Mg and Mg-Co nanocomposites

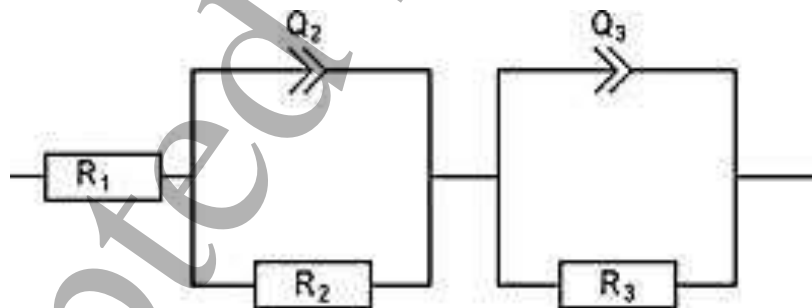
Table 1: Electrochemical corrosion Characteristics of the Pure Mg and Mg-Co nanocomposites

S.No	Specimen	E_{corr} (V)	$I_{corr} (\times 10^{-3} \mu A/cm^2)$	Polarization resistance, R_p ($\times 10^{-4} \Omega cm^2$)
1	Pure Mg	-0.940 ± 0.001	0.544 ± 0.004	2.79 ± 0.04
2	Mg-5Co	-0.894 ± 0.153	0.511 ± 0.004	2.80 ± 0.02
3	Mg-10Co	-0.834 ± 0.153	0.510 ± 0.006	2.87 ± 0.04
4	Mg-15Co	-0.833 ± 0.100	0.505 ± 0.006	2.90 ± 0.02
5	Mg-20Co	-0.830 ± 0.129	0.491 ± 0.004	2.93 ± 0.02
6	Mg-25Co	-0.813 ± 0.001	0.397 ± 0.041	3.61 ± 0.5

3.8 Electrochemical Impedance Spectroscopy Analysis:

EIS spectroscopy was employed to study the corrosion resistance properties of Mg-Co nanocomposites. Fig.11 shows the equivalent circuit used for fitting the Nyquist impedance for the Mg-Co nanocomposites. R_1 corresponds to the resistance of the electrolytic solution (NaCl)

1
2
3 at room temperature. The R_2 can be judged as charge transfer resistance which is inversely
4 proportional to the corrosion rate [28,29]. The Q_2 and Q_3 are interpreted as constant phase
5 elements which are used to calculate the true capacitance of the nanocomposite specimens. The
6
7 resistance R_3 is related to the effect of Co nanoparticle reinforcement. The Fig.12 shows two
8
9 characteristic arcs at higher and lower frequency region. The larger arc is due to the electron
10
11 transfer within the Mg-Co nanocomposite working electrode and the smaller arc at the lower
12
13 frequency region is due to the diffusion at the interface of Mg-Co nanocomposite electrode and
14
15 the electrolyte [30]. The perfect capacitance behaviour is not seen in this study and for this
16
17 reason, a constant phase element (CPE) is introduced in the equivalent circuit[23,31].The
18
19 measured resistance and CPE values of the Mg-Co nanocomposites are shown in Table.2. From
20
21 the table, it is evident that the charge transfer resistance (R_{ct1}) of the Mg-25Co nanocomposites
22
23 ($R_{ct1}= 42.50 \Omega \text{ cm}^2$) has improved than the pure Mg ($R_{ct1}= 14.44 \Omega \text{ cm}^2$) which confirms the
24
25 improvement in corrosion resistance of Mg-25Co nanocomposites. The charge transfer
26
27 capacitance of the Mg-Co nanocomposites decreases with increase in Co content which may be
28
29 attributed due to the double layer capacitance. The true capacitance calculated from the constant
30
31 phase elements and resistance values also confirm that the Mg-25Co nanocomposite ($C= 0.0198$
32
33 Fcm^{-2}) have lesser Capacitance value compared to pure Mg ($C = 0.4729 \text{ Fcm}^{-2}$).



45 *Fig.11 The Equivalent circuit for fitting EIS*

46
47
48
49
50
51
52
53
54
55
56
57
58
59
60

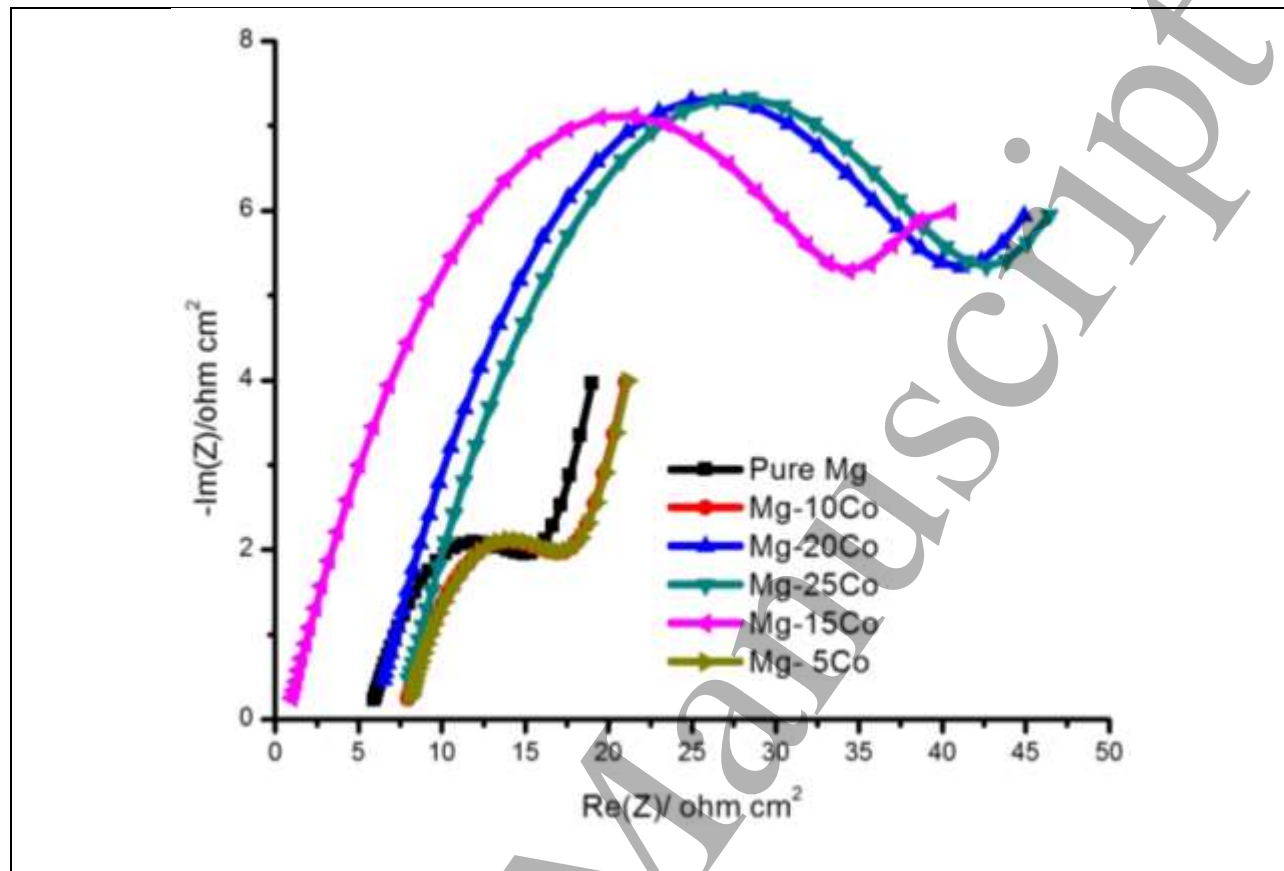


Fig.12 EIS Spectra of Mg-Co nano composites

Table 2: Charge transfer resistance obtained from EIS data fitting by equivalent circuit model (Standard deviation σ)

S.No	Specimen	R_s ($\Omega \text{ cm}^2$)	Q_2 ($\text{F.s}^2 \text{ cm}^{-2}$)	C_{dl1} (F cm^{-2})	R_{ct1} ($\Omega \text{ cm}^2$)	Q_3 ($\text{F.s}^2 \text{ cm}^{-2}$)	C_{dl2} (F cm^{-2})	R_{ct2} ($\Omega \text{ cm}^2$)
1	Mg	5.647 ± 1.65	0.4565	0.4729	14.44 ± 7.02	0.2952	4.619	10.13 ± 5.10
2	Mg-5Co	7.650 ± 2.50	0.4550	0.4521	17.45 ± 8.12	0.2842	4.213	12.76 ± 1.23
3	Mg-10Co	7.659 ± 1.60	0.4540	0.4489	17.48 ± 5.50	0.2750	3.890	13.21 ± 3.25
4	Mg-15Co	1.240 ± 0.50	0.1732	0.2409	35.16 ± 6.00	0.2598	0.014	11.73 ± 0.50
5	Mg-20Co	5.980 ± 1.80	0.1722	0.0205	40.10 ± 5.45	0.2540	0.013	08.01 ± 5.60
6	Mg-25Co	7.462 ± 1.45	0.1697	0.0198	42.50 ± 2.15	0.2359	0.013	10.00 ± 3.45

4. Conclusions:

The Mg-Co nanocomposites were synthesized by utilizing high energy ball mill and hydraulic compacting process. The wear and corrosion resistance of the composites are considered in different conditions.

- The wear analysis on a pin on disc apparatus shows Mg-25Co nanocomposite has healthier wear resistance and coefficient of friction.
- The potentiometric polarization analysis shows that the Mg-25Co nanocomposite has enhanced corrosion resistance due to the existence of Co nanoparticles.
- The electrochemical impedance spectroscopy (EIS) also authenticates that the Mg-25Co nanocomposite has higher charge transfer resistance value compared to that of pure Mg.
- The Microhardness of the Mg-25Co nanocomposite is superior to that of Pure Mg.
- From the findings of this study, it can be concluded that the Mg-25Co nanocomposite has better wear and corrosion resistance.

References:

- [1] J. Zhang, X. Zhang, Q. Liu, S. Yang, Z. Wang, Effects of Load on Dry Sliding Wear Behavior of Mg–Gd–Zn–Zr Alloys, *J. Mater. Sci. Technol.* 33 (2017) 645–651. doi:10.1016/j.jmst.2016.11.014.
- [2] H. Sharifi, K. Ostovan, M. Tayebi, A. Rajaei, Dry sliding wear behavior of open-cell Al-Mg/Al₂O₃ and Al-Mg/SiC-Al₂O₃ composite preforms produced by a pressureless infiltration technique, *Tribol. Int.* 116 (2017) 244–255. doi:10.1016/j.triboint.2017.07.023.
- [3] K.K. Ajith Kumar, U.T.S. Pillai, B.C. Pai, M. Chakraborty, Dry sliding wear behaviour of Mg-Si alloys, *Wear.* 303 (2013) 56–64. doi:10.1016/j.wear.2013.02.020.
- [4] J. Dai, X. Zhang, Q. Yin, S. Ni, Z. Ba, Z. Wang, Friction and wear behaviors of biodegradable Mg-6Gd-0.5Zn-0.4Zr alloy under simulated body fluid condition, *J. Magnes. Alloy.* 5 (2017) 448–453. doi:10.1016/j.jma.2017.11.002.
- [5] K. Soorya Prakash, P. Balasundar, S. Nagaraja, P.M. Gopal, V. Kavimani, Mechanical and wear behaviour of Mg–SiC–Gr hybrid composites, *J. Magnes. Alloy.* 4 (2016) 197–206. doi:10.1016/j.jma.2016.08.001.
- [6] F. Toptan, A.C. Alves, I. Kerti, E. Ariza, L.A. Rocha, Corrosion and tribocorrosion behaviour of Al-Si-Cu-Mg alloy and its composites reinforced with B₄C particles in 0.05M NaCl solution, *Wear.* 306 (2013) 27–35. doi:10.1016/j.wear.2013.06.026.
- [7] M.E. Turan, Y. Sun, Y. Akgul, Mechanical, tribological and corrosion properties of fullerene reinforced magnesium matrix composites fabricated by semi powder metallurgy, *J. Alloys Compd.* 740 (2018) 1149–1158. doi:10.1016/j.jallcom.2018.01.103.
- [8] M.S. Kabir, T.I. Minhaj, M.D. Hossain, A. Kurny, Effect of Mg on the Wear Behaviour of as-cast Al-4.5Cu-3.4Fe in-situ Composite, *Am. J. Mater. Eng. Technol.* 3 (2015) 7–12.

- 1
2
3 doi:10.12691/MATERIALS-3-1-2.
4
5
6 [9] F. Ren, W. Zhu, K. Chu, Fabrication and evaluation of bulk nanostructured cobalt
7 intended for dental and orthopaedic implants, *J. Mech. Behav. Biomed. Mater.* 68 (2017)
8 115–123. doi:10.1016/j.jmbbm.2017.01.039.
9
10
11
12 [10] R. Ma, S. Ju, H. Chen, C. Shu, Effect of Cobalt Content on Microstructures and Wear
13 Resistance of Tungsten Carbide-Cobalt-Cemented Carbides Fabricated by Spark Plasma
14 Sintering, *IOP Conf. Ser. Mater. Sci. Eng.* 207 (2017). doi:10.1088/1757-
15 899X/207/1/012019.
16
17
18
19
20
21 [11] G. Manivasagam, D. Dhinasekaran, A. Rajamanickam, Biomedical Implants: Corrosion
22 and its Prevention - A Review, *Recent Patents Corros. Sci.* 2 (2010) 40–54.
23 doi:10.2174/1877610801002010040.
24
25
26
27
28 [12] L.M. Vilhena, C.M. Fernandes, E. Soares, J. Sacramento, A.M.R. Senos, A. Ramalho,
29 Abrasive wear resistance of WC-Co and WC-AISI 304 composites by ball-cratering
30 method, *Wear.* 346–347 (2016) 99–107. doi:10.1016/j.wear.2015.11.005.
31
32
33
34
35 [13] Y. Liu, J. Cheng, B. Yin, S. Zhu, Z. Qiao, J. Yang, Study of the tribological behaviors and
36 wear mechanisms of WC-Co and WC-Fe₃Al hard materials under dry sliding condition,
37 *Tribol. Int.* 109 (2017) 19–25. doi:10.1016/j.triboint.2016.12.023.
38
39
40
41
42 [14] N. Elkhoshkhany, A. Hafnway, A. Khaled, Electrodeposition and corrosion behavior of
43 nano-structured Ni-WC and Ni-Co-WC composite coating, *J. Alloys Compd.* 695 (2017)
44 1505–1514. doi:10.1016/j.jallcom.2016.10.290.
45
46
47
48
49 [15] H.W. Liu, X.J. Xu, M.H. Zhu, P.D. Ren, Z.R. Zhou, High temperature fretting wear
50 behavior of WC₂₅Co coatings prepared by D-gun spraying on TiAlZr titanium alloy,
51 *Tribol. Int.* 44 (2011) 1461–1470. doi:10.1016/j.triboint.2011.01.002.
52
53
54
55
56
57
58
59
60

- 1
2
3 [16] X. Zhang, J. Ma, J. Yang, Q. Bi, W. Liu, Dry-sliding tribological behaviour of Fe–28Al–
4 5Cr/TiC composites, *Wear*. 271 (2011) 881–888. doi:10.1016/j.wear.2011.03.020.
5
6
7 [17] C. Jiang, Y. Xing, F. Zhang, J. Hao, Microstructure and corrosion resistance of Fe/Mo
8 composite amorphous coatings prepared by air plasma spraying, *Int. J. Miner. Metall.*
9 *Mater.* 19 (2012) 657–662. doi:10.1007/s12613-012-0609-z.
10
11
12 [18] R. Mousavi, M.E. Bahrololoom, F. Deflorian, Preparation, corrosion, and wear resistance
13 of Ni-Mo/Al composite coating reinforced with Al particles, *Mater. Des.* 110 (2016) 456–
14 465. doi:10.1016/j.matdes.2016.08.019.
15
16
17 [19] L. Zhang, X. Qu, B. Duan, X. He, M. Qin, Effect of porosity on wear resistance of SiC p /
18 Cu composites prepared by pressureless infiltration, *Trans. Nonferrous Met. Soc. China.*
19 18 (2008) 1076–1082. doi:10.1016/S1003-6326(08)60184-3.
20
21
22 [20] M.G. Verón, F.C. Gennari, G.O. Meyer, Role of MgCo compound on the sorption
23 properties of the Mg-Co milled mixtures, *J. Power Sources.* 195 (2010) 546–552.
24 doi:10.1016/j.jpowsour.2009.07.047.
25
26
27 [21] E.M. Kirkpatrick, D.L. Leslie-Pelecky, S.H. Kim, R.D. Rieke, Magnetic and structural
28 properties of Mg–Co nanostructures fabricated by chemical synthesis, *J. Appl. Phys.* 85
29 (1999) 5375–5377. doi:10.1063/1.369982.
30
31
32 [22] W.R. Osório, L.C. Peixoto, P.R. Goulart, A. Garcia, Electrochemical corrosion parameters
33 of as-cast Al-Fe alloys in a NaCl solution, *Corros. Sci.* 52 (2010) 2979–2993.
34 doi:10.1016/j.corsci.2010.05.011.
35
36
37 [23] M. Hosseini, L. Fotouhi, A. Ehsani, M. Naseri, Enhancement of corrosion resistance of
38 polypyrrole using metal oxide nanoparticles: Potentiodynamic and electrochemical
39 impedance spectroscopy study, *J. Colloid Interface Sci.* 505 (2017) 213–219.
40
41
42
43
44
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59
60


- 1
2
3 doi:10.1016/j.jcis.2017.05.097.
4
5
6 [24] W.X. Zhang, Z.H. Jiang, G.Y. Li, Q. Jiang, J.S. Lian, Electroless Ni-Sn-P coating on
7 AZ91D magnesium alloy and its corrosion resistance, *Surf. Coatings Technol.* 202 (2008)
8 2570–2576. doi:10.1016/j.surfcoat.2007.09.023.
9
10
11
12 [25] J.F. Marco, a C. Agudelo, J.R. Gancedo, D. Hanzel, Corrosion resistance of single TiN
13 layers, Ti/TiN bilayers and Ti/TiN/Ti/TiN multilayers on iron under a salt fog spray
14 (phohesion) test: an evaluation of XPS, *Surf. Interface Anal.* 27 (1999) 71–75.
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59
60
- [26] J. Yuan, X. Luan, R. Riedel, E. Ionescu, Preparation and hydrothermal corrosion behavior of C_f/SiCN and C_f/SiHfBCN ceramic matrix composites, *J. Eur. Ceram. Soc.* 35 (2015) 3329–3337. doi:10.1016/j.jeurceramsoc.2014.12.009.
- [27] R. Liu, J. Yao, Q. Zhang, M.X. Yao, R. Collier, Effects of molybdenum content on the wear/erosion and corrosion performance of low-carbon Stellite alloys, *Mater. Des.* 78 (2015) 95–106. doi:10.1016/j.matdes.2015.04.030.
- [28] S.A. Umoren, Y. Li, F.H. Wang, Influence of iron microstructure on the performance of polyacrylic acid as corrosion inhibitor in sulfuric acid solution, *Corros. Sci.* 53 (2011) 1778–1785. doi:10.1016/j.corsci.2011.01.052.
- [29] A. Ehsani, M.G. Mahjani, M. Hosseini, R. Safari, R. Moshrefi, H. Mohammad Shiri, Evaluation of *Thymus vulgaris* plant extract as an eco-friendly corrosion inhibitor for stainless steel 304 in acidic solution by means of electrochemical impedance spectroscopy, electrochemical noise analysis and density functional theory, *J. Colloid Interface Sci.* 490 (2017) 444–451. doi:10.1016/j.jcis.2016.11.048.
- [30] E. Angelini, S. Grassini, F. Rosalbino, F. Fracassi, R. D'Agostino, Electrochemical

1
2
3 impedance spectroscopy evaluation of the corrosion behaviour of Mg alloy coated with
4 PECVD organosilicon thin film, *Prog. Org. Coatings*. 46 (2003) 107–111.
5
6 doi:10.1016/S0300-9440(02)00217-5.
7
8

- 9
10 [31] E. Kowsari, S.Y. Arman, M.H. Shahini, H. Zandi, A. Ehsani, R. Naderi, A.
11 PourghasemiHanza, M. Mehdipour, In situ synthesis, electrochemical and quantum
12 chemical analysis of an amino acid-derived ionic liquid inhibitor for corrosion protection
13 of mild steel in 1M HCl solution, *Corros. Sci.* 112 (2016) 73–85.
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59
60

Article

Numerical Study on the Influence of Mass and Stiffness Ratios on the Vortex Induced Motion of an Elastically Mounted Cylinder for Harnessing Power

Vidya Chandran ¹, Sekar M. ², Sheeja Janardhanan ^{3,*} and Varun Menon ⁴ 

¹ Department of Mechanical Engineering, Karunya Institute of Technology and Sciences, Coimbatore, Tamil Nadu 600018, India; vidya.rudn@gmail.com

² Department of Mechanical Engineering, AAA College of Engineering and Technology, Sivakasi, Tamil Nadu 600018, India; mailtosekar@gmail.com

³ Department of Mechanical Engineering, SCMS School of Engineering and Technology, Ernakulam, Kerala 673307, India

⁴ Department of Computer Science and Engineering, SCMS School of Engineering and Technology, Ernakulam, Kerala 673307, India; varungmenon46@gmail.com

* Correspondence: sheejajanardhanan@scmsgroup.org; Tel.: +91-828-194-3531

Received: 10 September 2018; Accepted: 25 September 2018; Published: 27 September 2018



Abstract: Harnessing the power of vortices shed in the wake of bluff bodies is indeed a boon to society in the face of fuel crisis. This fact serves as an impetus to develop a device called a hydro vortex power generator (HVPG), comprised of an elastically mounted cylinder that is free to oscillate in the cross-flow (CF) direction even in a low velocity flow field. The oscillatory motions in turn can be converted to useful power. This paper addresses the influence of system characteristics viz. stiffness ratio (k^*) and mass ratio (m^*) on the maximum response amplitude of the elastically mounted cylinder. Computational fluid dynamics (CFD) simulations have been used here to solve a two way fluid–structure interaction (FSI) problem for predicting the trend of variation of the non-dimensional amplitude Y/D with reduced velocity U_r through a series of simulations. Maximum amplitude motions have been attributed to the lowest value of m^* with $U_r = 8$. However, the maximum lift forces correspond to $U_r = 4$, providing strong design inputs as well as indicating the best operating conditions. The numerical results have been compared with those of field tests in an irrigation canal and have shown reasonable agreement.

Keywords: computational fluid dynamics (CFD); flow around cylinder; fluid structure interaction (FSI); hydrodynamic response; numerical methods; simulation and modeling; vortex induced vibration (VIV) ratio

1. Introduction

As the sources of fossil fuels are depleting at a faster pace, energy scientists all over the world are keen on the search for new technologies that can provide renewable and clean energy. Hydroelectric power generation is of course a clean source of energy, but considering the capital investment and the effects of dams on natural ecosystems, the need for a much cleaner energy source becomes more important. This paper discusses the design and manufacture of the hydro vortex power generator (HVPG) model, which when scaled up can be viewed as one such cleaner source of electricity. Also, the paper discusses a numerical method to optimize the design parameters of HVPG model. The principle behind the working of HVPG is vortex shedding in the wake of bluff bodies in fluid flow. The phenomenon of vortex shedding behind bluff bodies has been an extensively researched topic [1,2]. The presence of such vortex shedding has been considered undesirable and researchers had been in

search of methods to suppress vortex shedding [3]. Vortex power was proved useful to mankind by the researchers at Michigan University, who first converted vortex power into electricity [4,5]. HVPG works on the principle of vortex induced vibration of bluff bodies subjected to fluid current. The power of vortices shed in the wake of these bluff bodies are converted into vibration energy and then into electricity. HVPG can be made useful as a single standing power unit that can provide electricity to remote locations; and also as a multiunit module which can supply power to the grid [6]. The paper discusses the design optimization of a single, power-generating, scaled-down module, harnessing power from vortices. In this paper, an attempt has been made to optimize the design based on the major influencing parameters, oscillating mass ratio (m^*) and stiffness ratio (k^*). Griffin consolidated experimental results and plotted them to show the dependence of maximum amplitude on system characteristics [7]. However, the drawback of Griffin's plot was its considerable scatter which could be attributed to the inclusion of mode shapes also as an influencing parameter. Later researchers could successfully reduce the scatter in Griffin's plot and establish a simple relationship between maximum amplitude and mass damping parameter by eliminating mode shapes from the list of variables [7,8]. The simplified mass damping parameter as in [8] was applicable for cylinders of high and low mass ratios equally. Many researchers have formulated empirical formulae to express the parametric relationship and experimentally verified the correlations [9,10]. Later in the experiments, however, it has been observed that with variation in the damping ratio, U_r and the Strouhal number (St) varies [11]. Also, these experiments revealed relatively larger response amplitude compared to other studies. Recently researchers have also succeeded in theoretically proving the effectiveness of harnessing VIV energy for powering underwater mooring platforms [12].

The present work studies the influence of k^* and m^* on maximum response amplitude of an elastically mounted cylinder with a single DOF. It also provides a detailed insight into the vortex shedding pattern at various U_r . The simulations are carried out at Re of the order 10^4 which corresponds to the realistic flow regime encountered by power generating vortices [13]. The numerical results have been verified using field tests conducted at Palissery irrigation canal (Palissery irrigational canal is one of the irrigation projects by Government of Kerala located in Thrissur district, Kerala, India).

Previous studies in the same domain had only considered the effect of complex and coupled parameters such as the Skop Griffin parameter [14]. The novelty in the present work is the effort made to represent the influence of tangible parameters viz the stiffness coefficient and mass of the cylinder. These parameters are easily controllable from a designer's point of view. A non-dimensional approach has been used here to generalize the results for the design of power harnessing devices of any scale.

2. The Concept of HVPG

HVPG works on the principle of vortex induced vibration (VIV). If a bluff body is not completely secured with at least one degree of freedom motion, and the frequency of vortex shedding matches the natural frequency of the structure, the structure begins to resonate, vibrating with harmonic oscillations of large amplitude. This phenomenon is known as 'lock-in'. During lock-in, vortex shedding frequency shifts to the natural frequency of the structure, leading to large amplitude vibrations. Vortex shedding in the wake of a cylinder is shown in Figure 1.

The vortex shedding occurs at a discrete frequency and is a function of the Reynolds number (Re), defined by Equation (1)

$$Re = \frac{\rho V D}{\mu} \quad (1)$$

The dimensionless frequency of the vortex shedding, $St = f_v D/V$, is approximately equal to 0.2 when the Reynolds number is greater than 1000 [15]. When vortices are shed from the cylinder, uneven pressure distribution develops around the upper and lower surfaces of the cylinder, generating an

oscillating hydrodynamic lift force on the cylinder. This unsteady force given by Equation (2) can induce significant cross flow vibrations on a structure, especially if the resonance condition is met.

$$F_L = C_L \frac{1}{2} \rho A V^2. \quad (2)$$

where F_L is the lift force and C_L is the coefficient of lift. ρ is the density of water, A the projected area in the direction of flow, and V is the velocity of flowing water. The cylinder also experiences a net force along the flow direction and is called the drag force and is given by the Equation (3).

$$F_D = C_D \frac{1}{2} \rho A V^2 \quad (3)$$

where F_D is the drag force and C_D is the drag coefficient.

The oscillating lift force acting on the cylinder makes the cylinder oscillate in the cross flow (CF) direction at the frequency of vortex shedding. For the making of HVPG, the cylinder has been mounted elastically, which enables the entire module to be considered as a spring-mass system with the cylinder considered as the mass and the elastic supports as springs. When the natural frequency of spring-mass system matches the vortex shedding frequency, the cylinder oscillates with large amplitudes. The linear motion of the mass can then be converted to rotary motions through a slider-crank mechanism and the crank rotations can be used to drive a generator unit.

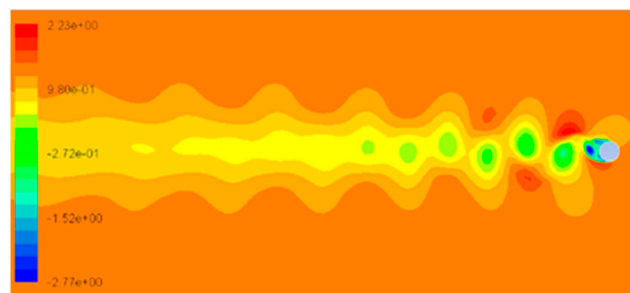


Figure 1. Shedding of alternate vortices behind a cylinder represented as pressure (N/m^2) contours. (Von Kármán Vortex Street).

3. Mathematical Model

A single power module of HVPG has been modeled as a spring mass system undergoing instability induced vibration. The instability is caused by the shedding of vortices in the wake of the cylinder when the flow encounters a bluff body. Alternate vortex shedding causes oscillatory forces that induce structural vibrations, where the rigid cylinder is now similar to a spring-mass system with a harmonic forcing term. This phenomenon is referred to as heave motion [14]. Equation of motion [16] for this system can be written as

$$m\ddot{Y} + c\dot{Y} + kY = F(t) \quad (4)$$

where Y is the displacement of the cylinder under VIV in the cross-flow direction; m is the sum of mass of the oscillating system or body mass, m_b and added mass of the system, m_a . m_a is defined as $m_a = C_A m_b$, where C_A is the added mass coefficient. c is the damping coefficient and k is the coefficient of stiffness of the spring mass system. $F(t)$ is the time varying force acting on the cylinder due the flow instability. Relatively small oscillation amplitudes are approximated by

$$F(t) = F_L \sin(\omega_v t + \varphi) \quad (5)$$

where ω_v is the circular frequency of vortex shedding and φ the phase difference between the force and cylinder displacement. F_L is the maximum value of oscillating hydrodynamic lift force acting on the cylinder and is given by Equation (2).

The amplitude of oscillation of the system depends on the mass (m^*) ratio of the oscillating cylinder given by

$$m^* = \frac{m}{m_{fd}} \quad (6)$$

where m_{fd} is the mass of fluid displaced by the oscillating mass. The maximum possible response amplitude at any Re , Y_{max} can be calculated from the empirical relation between non-dimensional amplitude ($A_y = \frac{Y_{max}}{D}$) and Re [10] as given by Equation (7).

$$A_Y = -0.4435 \left[\log \frac{\alpha}{Re} \right] - 1.5 \quad (7)$$

where α is defined as

$$\alpha = (m^* + C_A)\zeta \quad (8)$$

where C_A is the added mass coefficient and ζ is the damping ratio.

Maximum amplitude of oscillation occurs when shedding frequency locks on to the natural frequency of the oscillating system (f_n). This condition is known as lock-in. Amplitude of oscillation of a spring mass system can also be obtained from Equation (9)

$$Y = \frac{F_L}{k} \left[\frac{1}{\sqrt{(1 - \eta^2)^2 + (2\zeta\eta)^2}} \right] \quad (9)$$

where η is the frequency ratio represented by Equation (10)

$$\eta = \frac{f_n}{f_v} \quad (10)$$

where f_v is the vortex shedding frequency. During lock-in $\eta = 1$ and Equation (9) simplifies as shown by Equation (11).

$$Y = \frac{F_L}{2k\zeta} \quad (11)$$

The paper discusses effect of mass and stiffness ratios of the oscillating cylinder on the maximum response amplitude. The structural damping variations are not considered as it is observed to be less significant compared to its inertia and elastic counterparts. Also, mass and stiffness of the system are more tangible parameters from design point of view compared to damping. Moreover, the study focuses on non-dimensionalizing the influencing parameters so that results hold applicable for prototypes and models equally. Many researchers have considered the combined effect of mass and damping through mass damping parameter $m^*\zeta$. In such analysis also ζ is kept constant and m^* is varied independently [17].

4. Numerical Determination of Hydrodynamic Lift Forces and Motions

Vortex induced vibration, a two-way fluid structure interaction phenomenon, is complex in nature due to the fact that the cylinder displacement is capable of changing the vortex shedding pattern behind it leading to a variation in the hydrodynamic load acting on the cylinder. Parameters k^* , m^* , and c have significant influence on the oscillation amplitude. A significant amount of research has been carried out to bring clarity on the influence of these parameters on the maximum cylinder response amplitude. Experiments conducted by [18] could capture lock-in phenomenon for a cylinder with a single degree of freedom. It was observed that cylinder oscillation frequency matches with vortex shedding frequency for cylinders having low mass ratios [19]. For mass ratios below critical mass ratio, m^*_{cr} , the range of U_r over which resonance occurs tend to extend towards infinity. The following section of the paper is an effort to understand the effect of mass and stiffness coefficient on the response

of cylinder numerically in a simpler and economic way, and the results of the numerical study is verified using a field test.

4.1. Modeling the Flow

Numerically this problem has been treated as a case of two-way fluid structure interactions (two-way FSI). Modeling and meshing has been performed in ANSYS ICEM CFD (version 12) [20] and solving using ANSYS FLUENT (version 12) [21]. Flow around the cylinder is modeled using the transient, incompressible Navier–Stokes equation based RANS solver with $k-\omega$ SST as the turbulence model. The RANS solver does the virtual averaging of velocities over an interval of time and hence for a specific interval the velocity vector appears to be constant in a RANS solver. In the present work, an optimized fine grid is used to compensate for this drawback of the solver enabling it to capture the physics of von Kármán street eddies. RANS solver for transient two-dimensional analysis can be explained as follows [21]

$$\frac{\partial \rho}{\partial t} + \frac{\partial}{\partial x_i}(\rho u_i) = 0 \quad (12)$$

$$\frac{\partial}{\partial t}(\rho u_i) + \frac{\partial}{\partial x_i}(\rho u_i u_j) = -\frac{\partial p}{\partial x_i} + \frac{\partial}{\partial x_j} \left[\mu \left(\frac{\partial u_i}{\partial x_j} + \frac{\partial u_j}{\partial x_i} - \frac{2}{3} \delta_{ij} \frac{\partial u_l}{\partial x_l} \right) \right] + \frac{\partial}{\partial x_j}(-\rho \overline{u'_i u'_j}) \quad (13)$$

where u_i and u'_i are mean and fluctuating velocity components for $i = 1, 2$, and 3.

The velocities and other solution variables in the above equation represent the time averaged values. Equation (12) is solved by modeling Reynolds stresses $\overline{\rho u'_i u'_j}$, effectively using $k-\omega$ SST as turbulence model [22]. $k-\omega$ SST is capable of accurately predicting the commencement and the intensity of flow separation at fixed boundaries while the standard $k-\epsilon$ model has proved its efficacy in predicting the wake characteristics accurately. This fact has been established after extensive studies conducted by the authors. $k-\omega$ SST turbulence model demands a very high near wall grid resolution and hence the maximum element size is fixed to be less than 1×10^{-4} , which satisfies CFL criterion and near wall y^+ values.

The above governing equations are discretized using finite difference method. Non iterative time advancement (NITA) scheme with fractional time stepping method (FSM) has been chosen for pressure-velocity coupling of the grid. A Least Squares Cell Based scheme is used for gradient in spatial discretization and a second order upwind scheme as convective scheme.

NITA

For capturing the physics of the flow with accuracy in the boundary as well as in the wake of the cylinder, the computational grid needs to be extremely fine. Solving a dynamic mesh case with such extreme grid fineness using iterative time advancement scheme demands a considerable number of iterations to be performed using a very small time step size to satisfy the dynamic mesh criteria. This in turn leads to huge computational cost and effort. As an alternative and computationally economic method, in the present work, NITA with FSM has been implemented. NITA scheme assures the same time accuracy by reducing the splitting error, which occurs while solving the discretized Navier–Stokes equation to the same order as the truncation error. Splitting error need not be reduced to zero in NITA scheme, saving a lot of computational effort.

4.2. Structural Modeling

An elastically mounted cylinder can be mathematically represented by Equation (4). This equation of motion is solved using six degrees of freedom solver (6DOF), an integral part of the main solver by defining the cylinder as an object with one degree of freedom (1DOF) in transverse direction. A user defined function (UDF) compiled in C programming language has been hooked to the cylinder dynamic boundary conditions. The governing equation for the motion of the center of gravity of

the cylinder in the transverse direction is solved in the inertial coordinate system. Velocity in the transverse direction is obtained by performing integration on Equation (14).

$$\ddot{Y} = \frac{1}{m} \sum F \quad (14)$$

where \ddot{Y} , is the translational acceleration in the transverse direction, m is the mass of the cylinder and F , resultant fluid force acting on the cylinder. Position of the center of gravity of the cylinder (CG) is updated after solving the equation of motion of a spring mass system.

$$m\ddot{Y} + c\dot{Y} + kY = F(t) \quad (15)$$

The inertial force term on the left-hand side of Equation (15) is computed by the 6DOF solver for each time step from Equation (14) and the UDF hooked to the moving cylinder inputs the restoring force term as 6DOF load acting on the cylinder. Mass of the cylinder is given in the UDF as

$$m = m_b + m_a \quad (16)$$

$$m_a = (1 + C_A)m_b \quad (17)$$

Added mass coefficient C_A for the aspect ratio of the present model is found to be equal to 0.7 [13].

4.3. Mesh Deformation

Mesh motion to adapt to the movement of the cylinder is achieved by using displacement based smoothing algorithm. The governing equation for mesh motion is represented by Equation (18).

$$\nabla \cdot (\gamma \nabla \vec{u}) = 0 \quad (18)$$

where \vec{u} is the velocity of mesh displacement. The boundary conditions for Equation (18) are computed by the 6DOF solver and the boundary mesh motion diffuses into the interior of the deforming mesh according to the Laplace equation, Equation (18). Diffusion coefficient, γ is calculated using boundary distance formulation given by Equation (19).

$$\gamma = \frac{1}{d^\tau} \quad (19)$$

where τ is the diffusion parameter and d is the normalized boundary distance. Diffusion parameter is set as unity to avoid excessive deformation of the near cylinder elements.

4.4. Fluid Structure Interaction

In this paper, a two-way implicit approach is used to study the effect of m^* and k^* on the response of cylinder under VIV. Flow equations and structural equations are solved simultaneously in iterations with a time step. A flow chart for the solution procedure is shown in Figure 2.

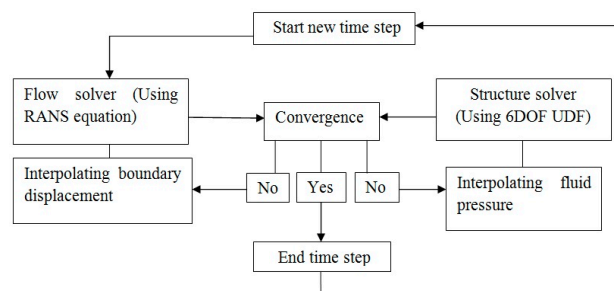


Figure 2. Flow chart of two-way implicit FSI solution procedure.

5. Problem Description

5.1. Simulation Parameters

In the present study, geometrically identical cylinders of different masses are considered for VIV of an elastically mounted horizontal cylinder. Based on the present study, a basic model of HVPG as in [5] was fabricated and a field study was carried out on it for verifying the numerical results. The main parameters of the model are summarized in Table 1. The model has an aspect ratio of 13.12 and an outer diameter of 0.0762 m. The structural damping is considered to be zero in the present study. The computational domain for the study is shown in Figure 3a. The representation of the present problem as a spring-mass system is depicted in Figure 3b. The mesh fineness is indicated in Figure 3c and the grid used for the present computation is represented by Figure 3d.

Table 1. Properties of the elastically mounted cylinder model.

Properties	Values	Units
Diameter of the cylinder (D)	0.0762	m
Aspect ratio of the cylinder (L/D)	13.12	-
Flow velocity (V)	0.5	m/s
Reynolds Number of flow (Re)	3.8×10^4	-
Mass ratio (m^*)	0.66	-

A simple representation of the two-dimensional computational domain for the cylinder is displayed in Figure 3a. The flow direction is parallel to the global x -axis and the flow velocity is set to be 0.5 m/s. Domain size is fixed based on previously published analysis and allowance is given to accommodate the vertical motion of cylinder boundary [23]. Simulations are performed for three different values of mass ratio, $m^* = 0.66, 1.32,$ and 1.98 which correspond to moderate mass ratios above m^*_{cr} , for which maximum response is confined to the range of $U_r = 4-12$. For fixed mass, influence of stiffness ratio k^* is studied by varying the reduced velocity value which is defined as

$$U_r = \frac{V}{f_n D} \quad (20)$$

$$f_n = \frac{1}{2\pi} \sqrt{\frac{k}{m}} \quad (21)$$

Each case has been analyzed over a range of reduced velocity, $U_r = 4-12$, over which the cylinder is predicted to have maximum amplitude of oscillation [24]. $U_r = 5$ has also been analyzed since the case corresponds to $\eta = 1$ where one might expect resonance. The incoming flow velocity is fixed as 0.5 m/s to maintain the flow regime uniform at $Re = 3.8 \times 10^4$. The mass ratio, stiffness ratio, and other parameters for each case are summarized in Table 2. Stiffness coefficient of the cylinder has been non-dimensionalized to generalize the applicability of the analysis. Stiffness ratio is defined as

$$k^* = \frac{k}{mg/L} \quad (22)$$

Table 2. Reduced velocity, stiffness ratio, and frequency ratio at $Re = 3.8 \times 10^4$, for $m^* = 0.66, 1.32,$ and 1.98 .

U_r	k^*	η
4	11.17	1.3
5	6.9	1.0
6	4.81	0.84
8	2.7	0.63
10	1.73	0.51
12	1.21	0.42

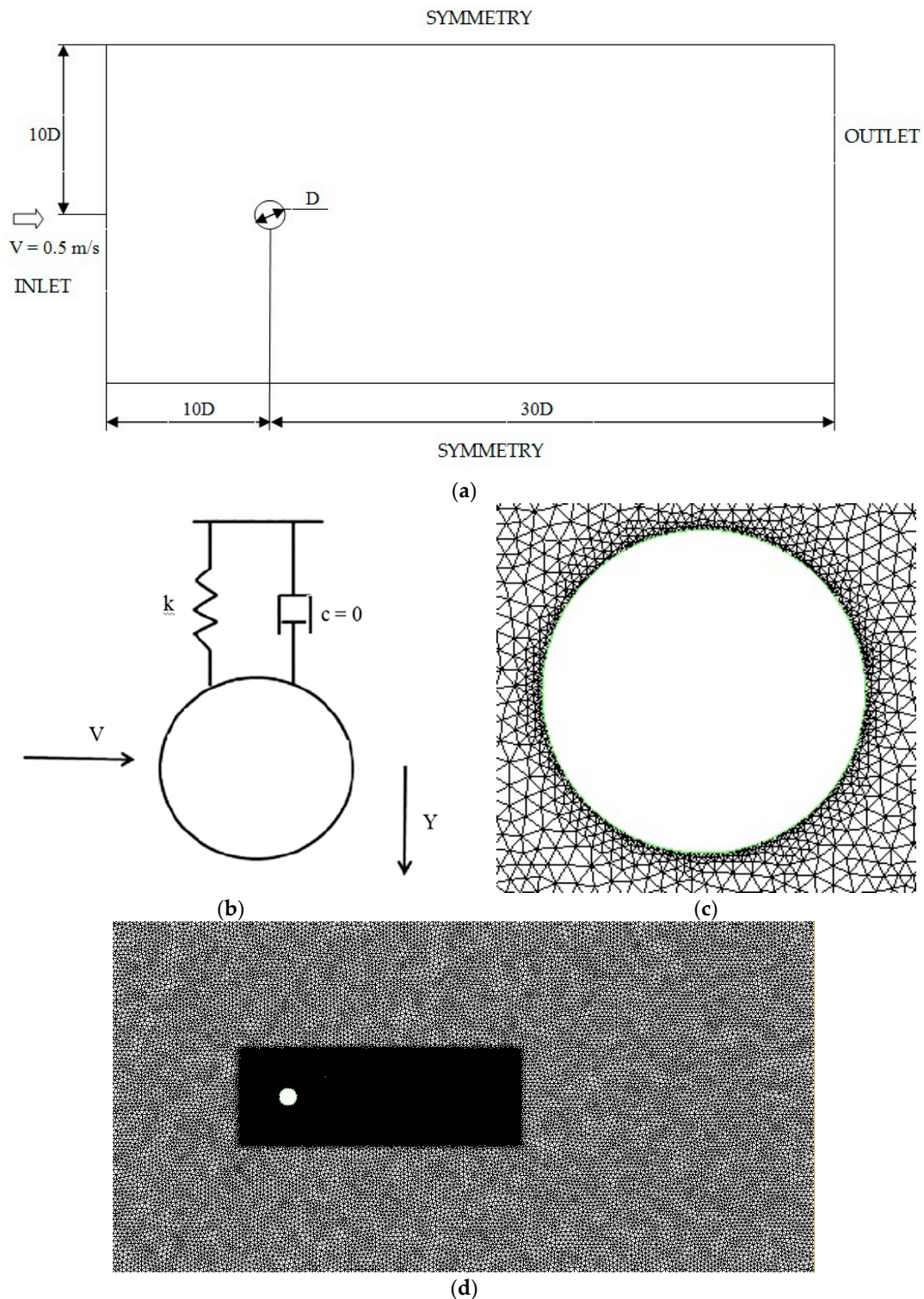


Figure 3. (a) Computational domain; (b) representation of elastically mounted cylinder model; (c) mesh around the cylinder; (d) computational mesh.

5.2. Fluid Domain and Boundary Conditions

Figure 3a shows the computational domain for the CFD simulation of VIV of an elastically mounted horizontal cylinder. The origin of the Cartesian coordinate system is located at the center of the cylinder. The length of the domain is $40D$ with the cylinder located at $10D$ away from the inlet boundary. The cross-flow width of the domain is $20D$ with the center of the cylinder at the

middle. Detailed views of the mesh around the cylinder along with the computational domain after meshing have been shown in Figure 3c,d respectively. There are 307 nodes around the circumference of the cylinder and the minimum element size near the rigid wall boundary has been computed from boundary layer theory to be $0.0001D$. The non-dimensional element size represented as y^+ , next to the cylinder surface is found to be less than unity. For the cylinder wall, a no slip boundary condition has been applied assuming the surface to be smooth. Inlet boundary has been treated as velocity-inlet with inflow velocity, $V = 0.5$ m/s. Outlet boundary has been treated as pressure outlet, the gradients of fluid velocity are set to zero and the pressure with zero reference pressure. On the two transverse boundaries a symmetry boundary condition has been applied.

5.3. Mesh Independence Study

An unstructured 2D mesh has been used in the present CFD simulation to facilitate computationally economic platform for dynamic mesh simulation. The three dimensionality of the wake reduces as a result of the motion of the cylinder [16]. Hence it is possible to get a reasonably accurate result from a 2D analysis saving much computational cost and effort. The meshing strategy is that finer mesh is used in the vicinity of the moving cylinder with extra fine meshing in the boundary layer. Boundary layer thickness and the near wall element size have been calculated from boundary layer theory. The thickness of laminar sub-layer is obtained from Equation (23) [25]

$$\delta' = \frac{11.6\vartheta}{V^*} \quad (23)$$

where V^* is the frictional velocity given by

$$V^* = \sqrt{\frac{\tau_0}{\rho}} \quad (24)$$

and τ_0 , the wall shear stress is obtained as

$$\tau_0 = \frac{0.664}{\sqrt{Re_D}} \cdot \frac{\rho V^2}{2} \quad (25)$$

Increased mesh density has been adopted in the near cylinder and its wake in order to capture the physics of vortex shedding accurately. For ensuring that the results are independent of the grid size, a mesh independence study has been carried out. Three different grids have been used to simulate a specific case $m^* = 2.45$ and $U_r = 8$ and has been verified using results of experiments conducted at a towing tank facility in the Department of Ocean Engineering, Indian Institute of Technology Madras, India [10]. The details of the mesh independency study are given in Table 3. The last three grids give almost similar results and experiments, and [10] shows a 4.9% deviation from the present results. This can be assumed to be due to not accounting for damping in the present study. It can be concluded that the variation in the numerical results given by Meshes II, III, and IV are in the acceptable range and considering the computational economy Grid II with 49,995 nodes has been chosen for further analysis.

Table 3. Mesh independency study results

	Re	m^*	U_r	Nodes	Y_{max}/D
Grid I				35,487	1.241
Grid II	3.8×10^4	2.45	8	49,995	1.220
Grid III				70,857	1.219
Grid IV				98,475	1.219
Narendran et al. (2015)				0.3–2.4 $\times 10^5$	2.45

While due steps like mesh independence studies have been carried out in this investigation, we acknowledge that the use of eddy-viscosity based turbulence models introduces a small amount of discrepancy in the final results. The errors of the $k-\omega$ SST model in flow separation and wakes has been documented comprehensively in prior studies [26,27].

6. Results and Discussion

Numerical simulations have been carried out for three different mass ratios over reduced velocities ranging from 4 to 12. The cylinder is modeled to be having only single degree of freedom (SDOF) in the transverse or CF direction. Influence of m^* and k^* on both hydrodynamic force coefficient in the CF direction and the response of the cylinder have been studied in detail. The CF response results can be verified with experimental [17,28]. Time history of coefficient of lift, C_L and non-dimensional CF response Y/D over the range of U_r for $m^* = 0.66, 1.32,$ and 1.98 are displayed in Figures 4–6 respectively.

6.1. Case I

Under Case I, the response of cylinder is studied for $m^* = 0.66$. The mass of the cylinder is taken as 3 kg and added mass coefficient $C_A = 0.7$. U_r is varied in the analysis by varying the coefficient of stiffness k and in turn the natural frequency f_n of the oscillating system. Details of the simulation parameters have been given in Table 2. For a stationary cylinder, it was observed from numerous experimental and numerical works [29–31] that C_L oscillates in a symmetrical fashion about zero due to vortex shedding [13]. In the present study for lower values of U_r , C_L is not oscillating about zero symmetrically. However, the response of the cylinder is observed to be symmetrical for all values of U_r at $m^* = 0.66$. At $U_r = 8$, C_L becomes almost symmetrical with an effective lift coefficient 0.18. Beat phenomenon is captured in the response of the cylinder at $U_r = 8$. Results for different cases are presented in Table 4. Maximum lift force is observed at $U_r = 4$ with $C_L = 1.12$ and maximum response at $U_r = 8$ with $Y/D = 1.26$. With increase in U_r response amplitude of the cylinder decreases beyond $U_r = 8$. Time histories of C_L and Y/D for $m^* = 0.66$ is presented in Figure 4.

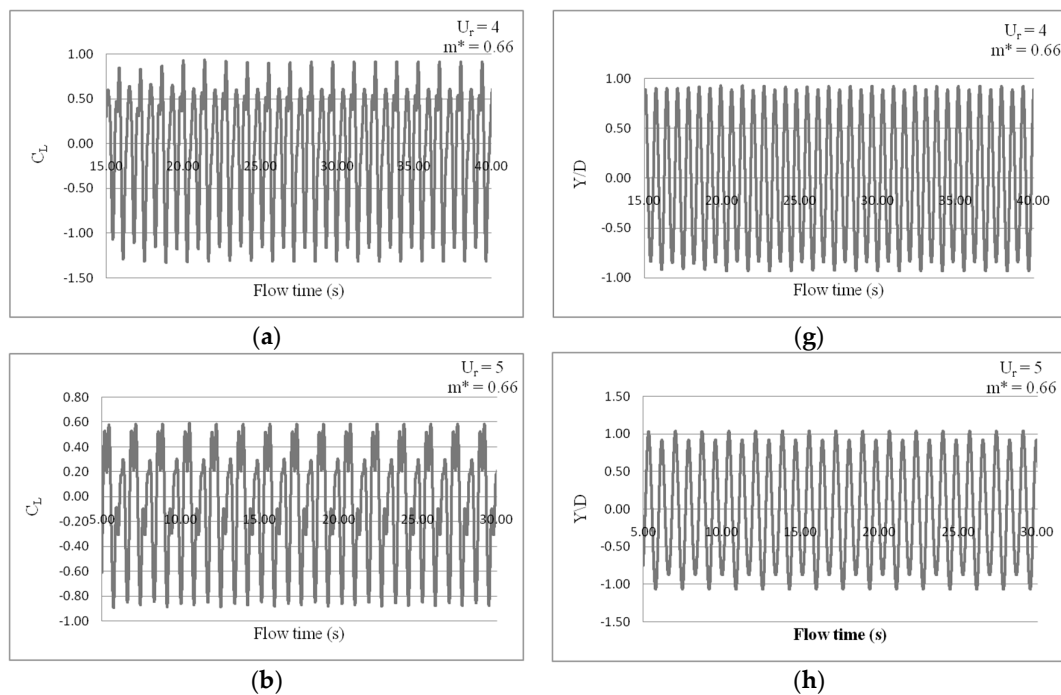


Figure 4. Cont.

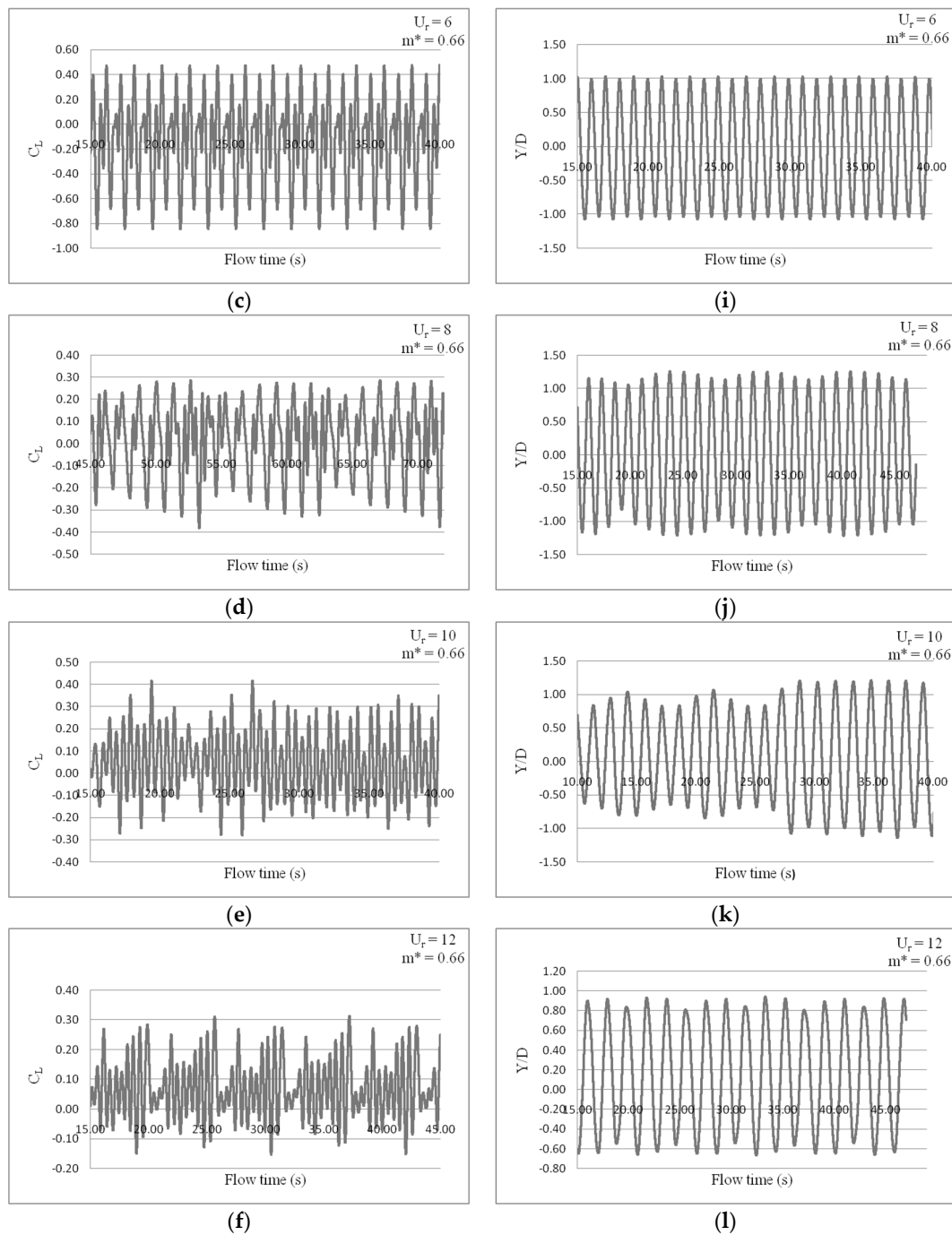


Figure 4. Time histories of hydrodynamic and structural response parameters at $m^* = 0.66$: (a) C_L for $U_r = 4$; (b) C_L for $U_r = 5$; (c) C_L for $U_r = 6$; (d) C_L for $U_r = 8$; (e) C_L for $U_r = 10$; (f) C_L for $U_r = 12$; (g) Y/D for $U_r = 4$; (h) Y/D for $U_r = 5$; (i) Y/D for $U_r = 6$; (j) Y/D for $U_r = 8$; (k) Y/D for $U_r = 10$; (l) Y/D for $U_r = 12$.

6.2. Case II

Under Case II, the response of cylinder is studied for $m^* = 1.32$. Mass of the cylinder is taken as 6 kg and added mass coefficient $C_A = 0.7$. Time histories of C_L and Y/D for $m^* = 1.32$ is presented in Figure 5. At $m^* = 1.32$, the cylinder exhibits similar response characteristics as in the previous case with maximum response at $U_r = 8$ with $Y/D = 1.17$. As the mass ratio increases, a slight decrease in the cross flow response amplitude is observed. Unlike the previous case, beat phenomenon is observed at $U_r = 10$.

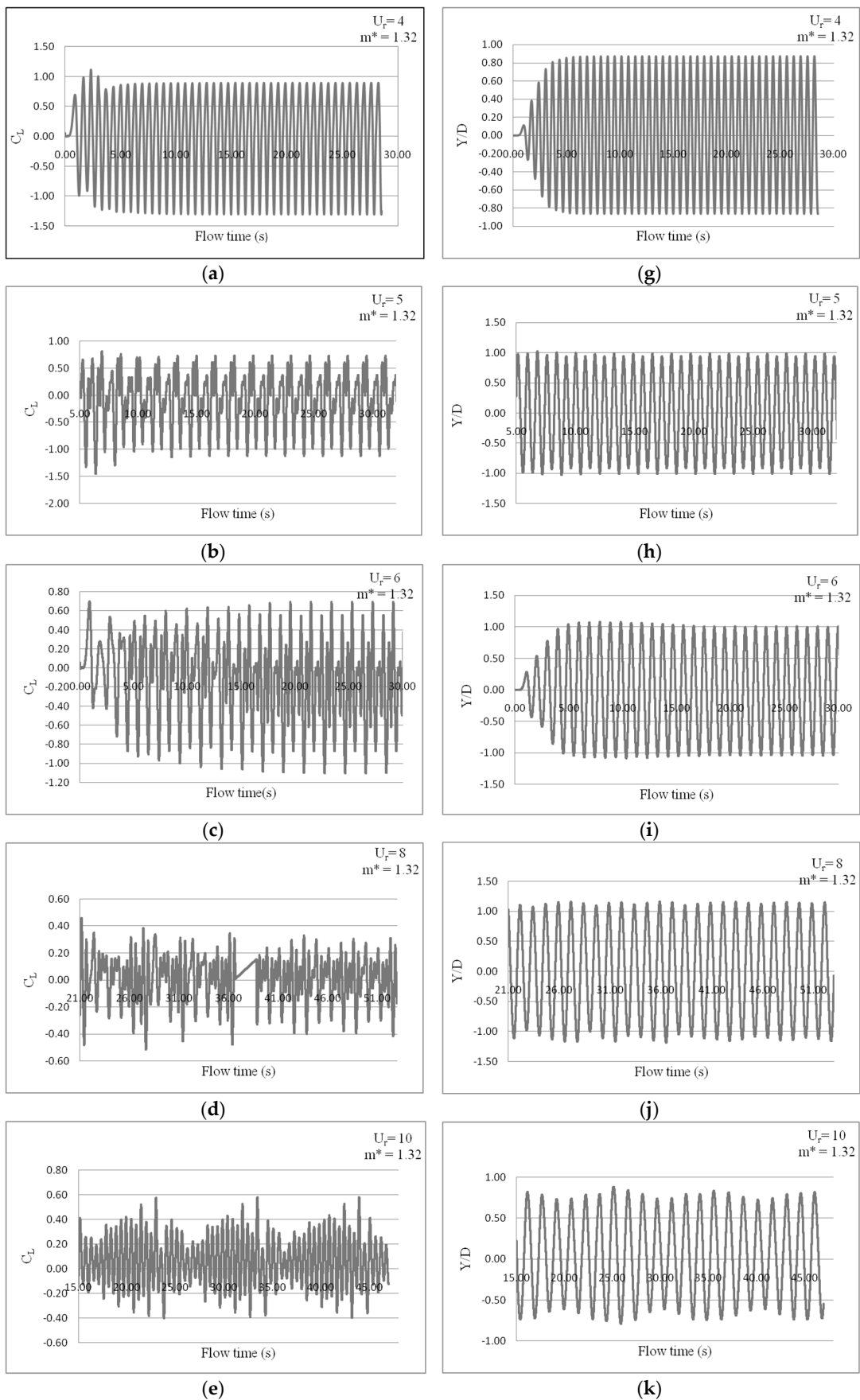


Figure 5. Cont.

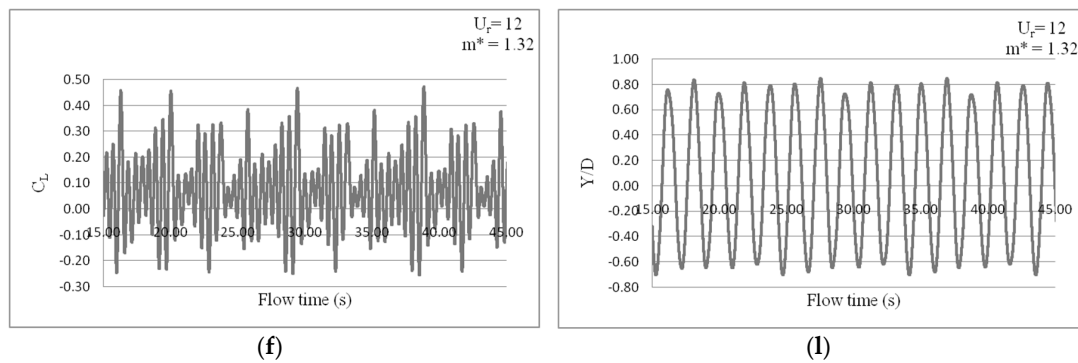


Figure 5. Time histories of hydrodynamic and structural response parameters at $m^* = 1.32$: (a) C_L for $U_r = 4$; (b) C_L for $U_r = 5$; (c) C_L for $U_r = 6$; (d) C_L for $U_r = 8$; (e) C_L for $U_r = 10$; (f) C_L for $U_r = 12$; (g) Y/D for $U_r = 4$; (h) Y/D for $U_r = 5$; (i) Y/D for $U_r = 6$; (j) Y/D for $U_r = 8$; (k) Y/D for $U_r = 10$; (l) Y/D for $U_r = 12$.

6.3. Case III

Under Case III, the response of cylinder is studied for $m^* = 1.98$. The mass of the cylinder is taken as 9 kg and added mass coefficient $C_A = 0.7$. Time histories of C_L and Y/D for $m^* = 1.98$ is presented in Figure 6. Maximum amplitude is observed at $U_r = 8$ with $Y/D = 1.13$ which is slightly less than the previous two cases. Here also prominent beat is observed at $U_r = 10$.

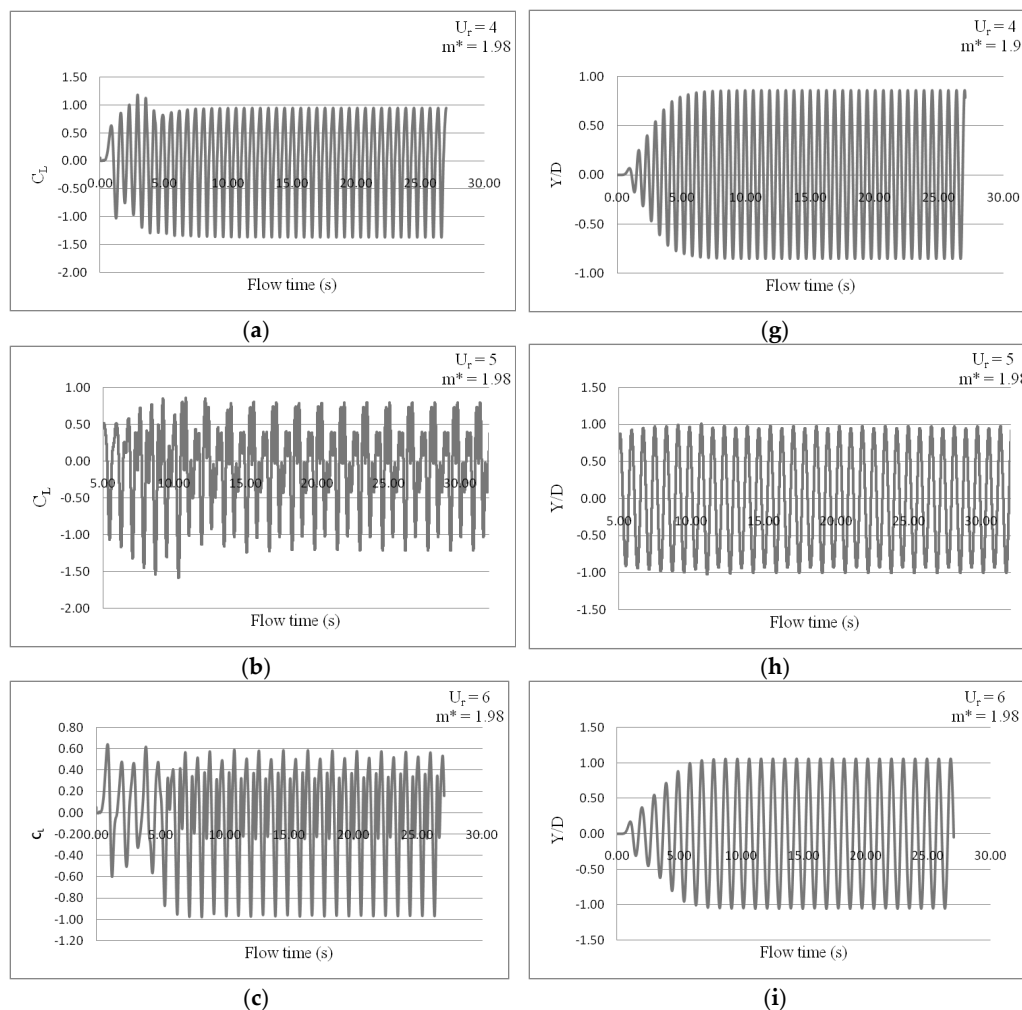


Figure 6. Cont.

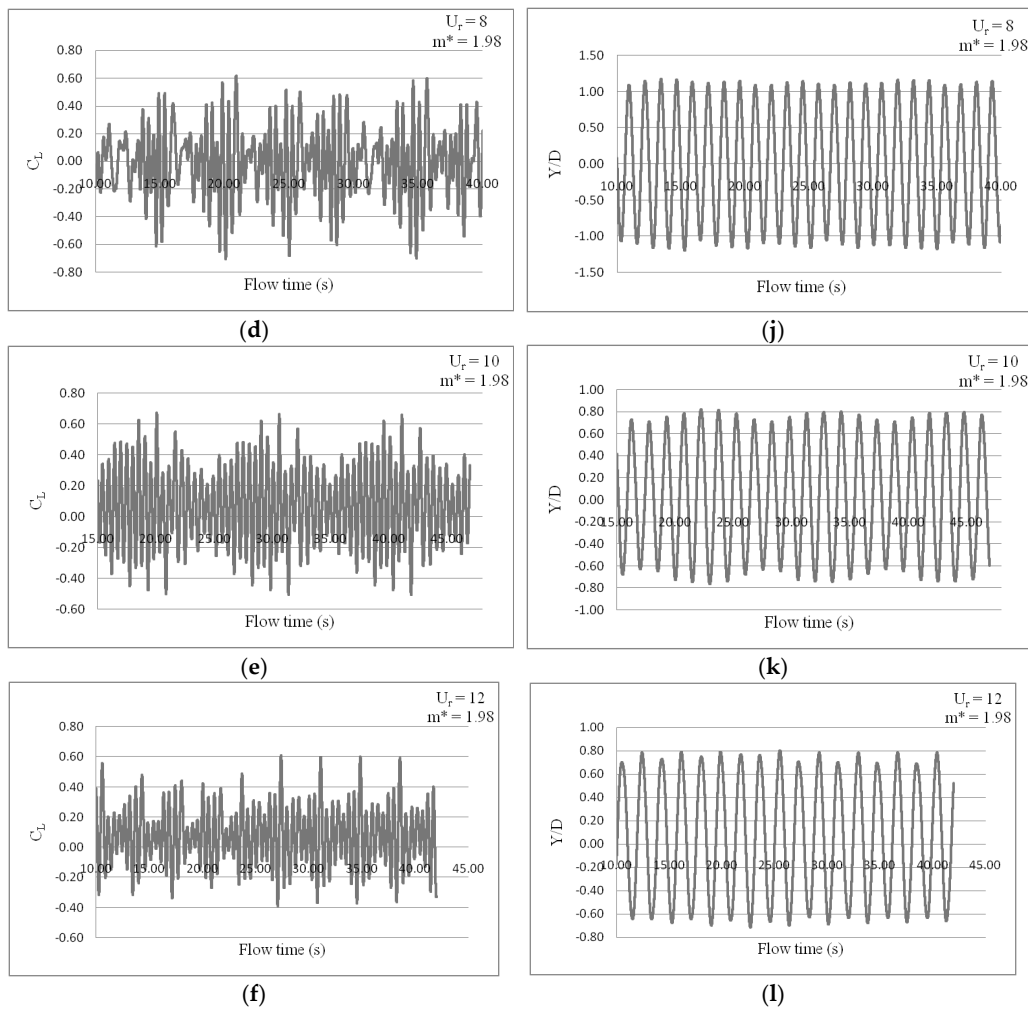


Figure 6. Time histories of hydrodynamic and structural response parameters at $m^* = 1.98$: (a) C_L for $U_r = 4$; (b) C_L for $U_r = 5$; (c) C_L for $U_r = 6$; (d) C_L for $U_r = 8$; (e) C_L for $U_r = 10$; (f) C_L for $U_r = 12$; (g) Y/D for $U_r = 4$; (h) Y/D for $U_r = 5$; (i) Y/D for $U_r = 6$; (j) Y/D for $U_r = 8$; (k) Y/D for $U_r = 10$; (l) Y/D for $U_r = 12$.

6.4. Shedding Characteristics

Numerical simulations for each case show that the shedding pattern and the characteristic variation of C_L strongly depend on the natural frequency of the oscillating mass. A more detailed history of C_L and Y/D for $m^* = 0.66$, 1.32, and 1.98 are presented in Figures 7–9 respectively.

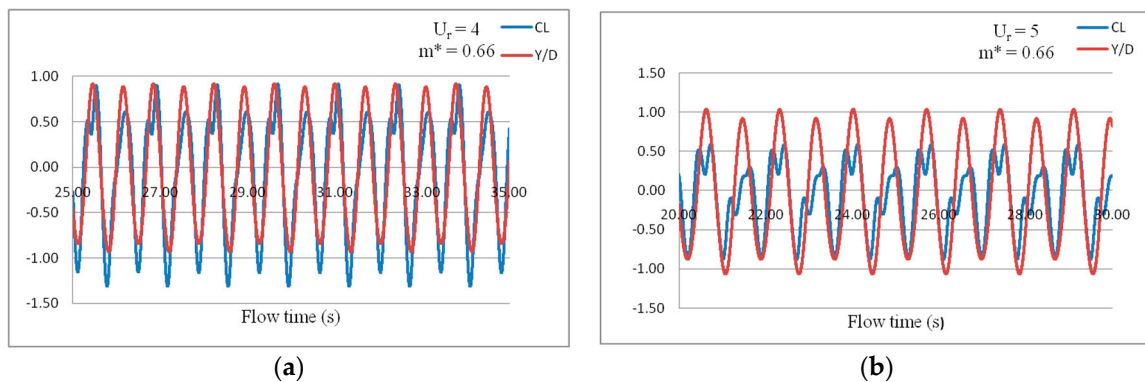


Figure 7. Cont.

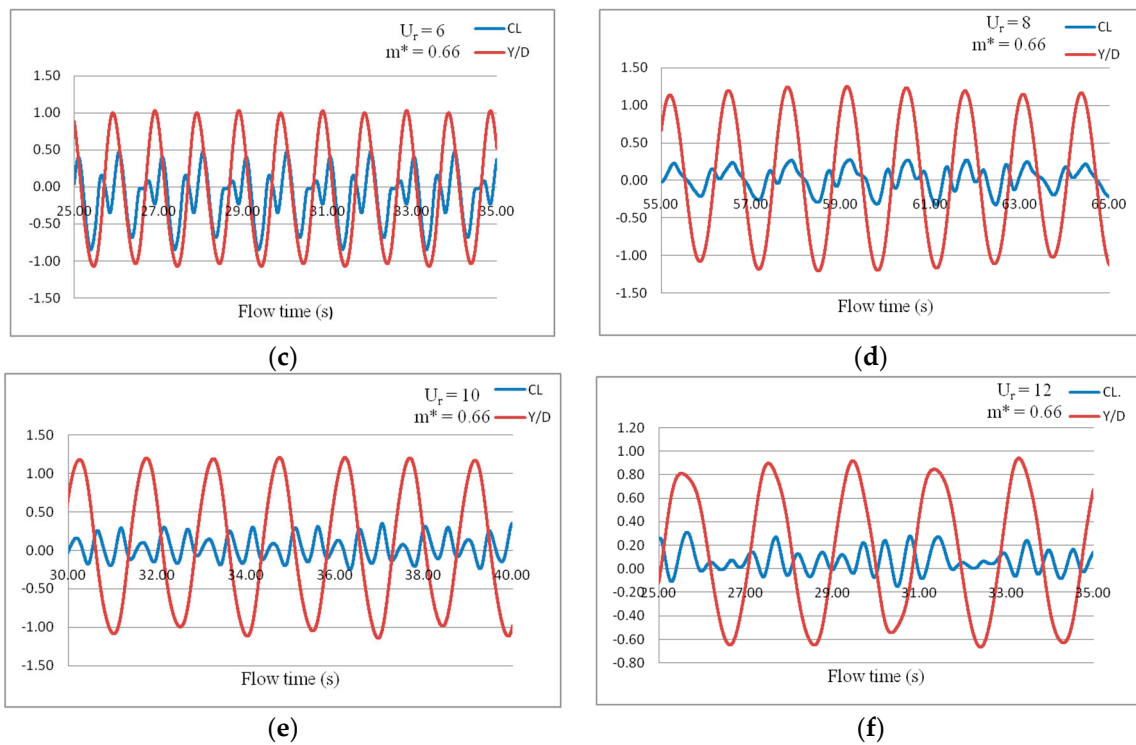


Figure 7. Variation of C_L with Y/D for $m^* = 0.66$ (a) $U_r = 4$; (b) $U_r = 5$; (c) $U_r = 6$; (d) $U_r = 8$; (e) $U_r = 10$; (f) $U_r = 12$.

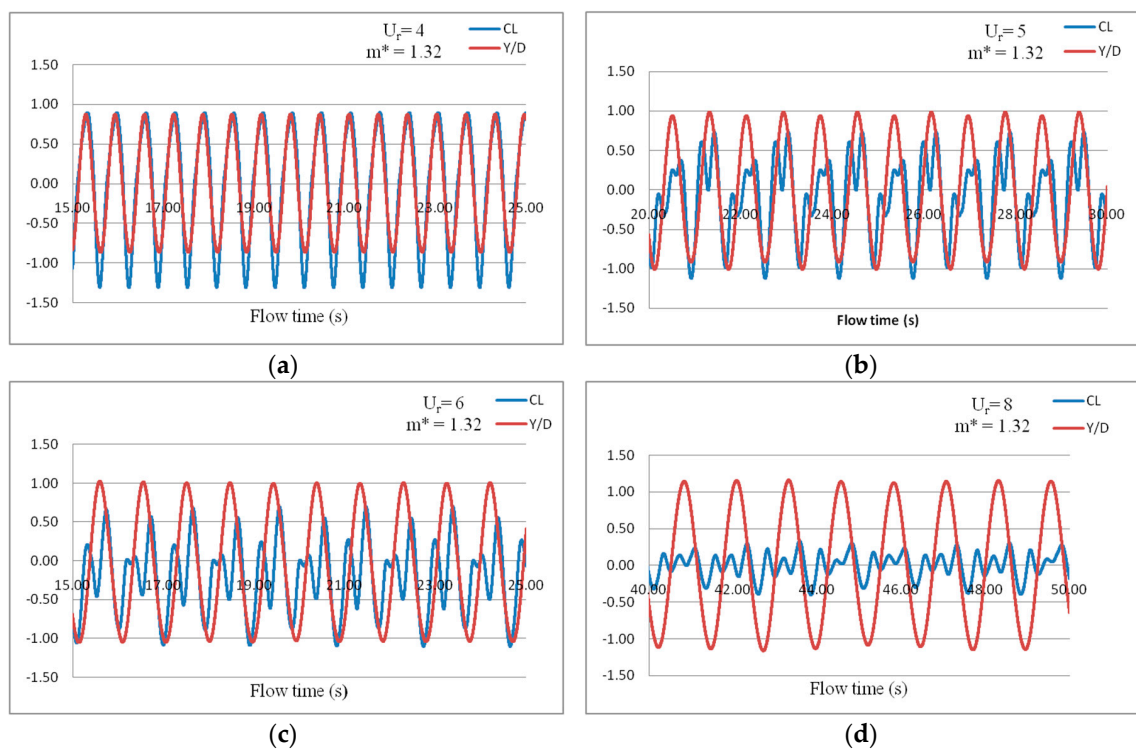


Figure 8. Cont.

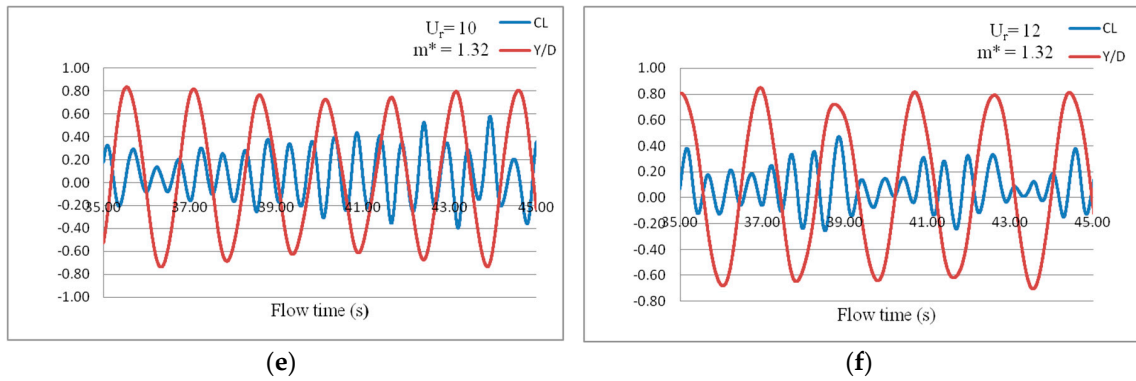


Figure 8. Variation of C_L with Y/D for $m^* = 1.32$: (a) $U_r = 4$; (b) $U_r = 5$; (c) $U_r = 6$; (d) $U_r = 8$; (e) $U_r = 10$; (f) $U_r = 12$.

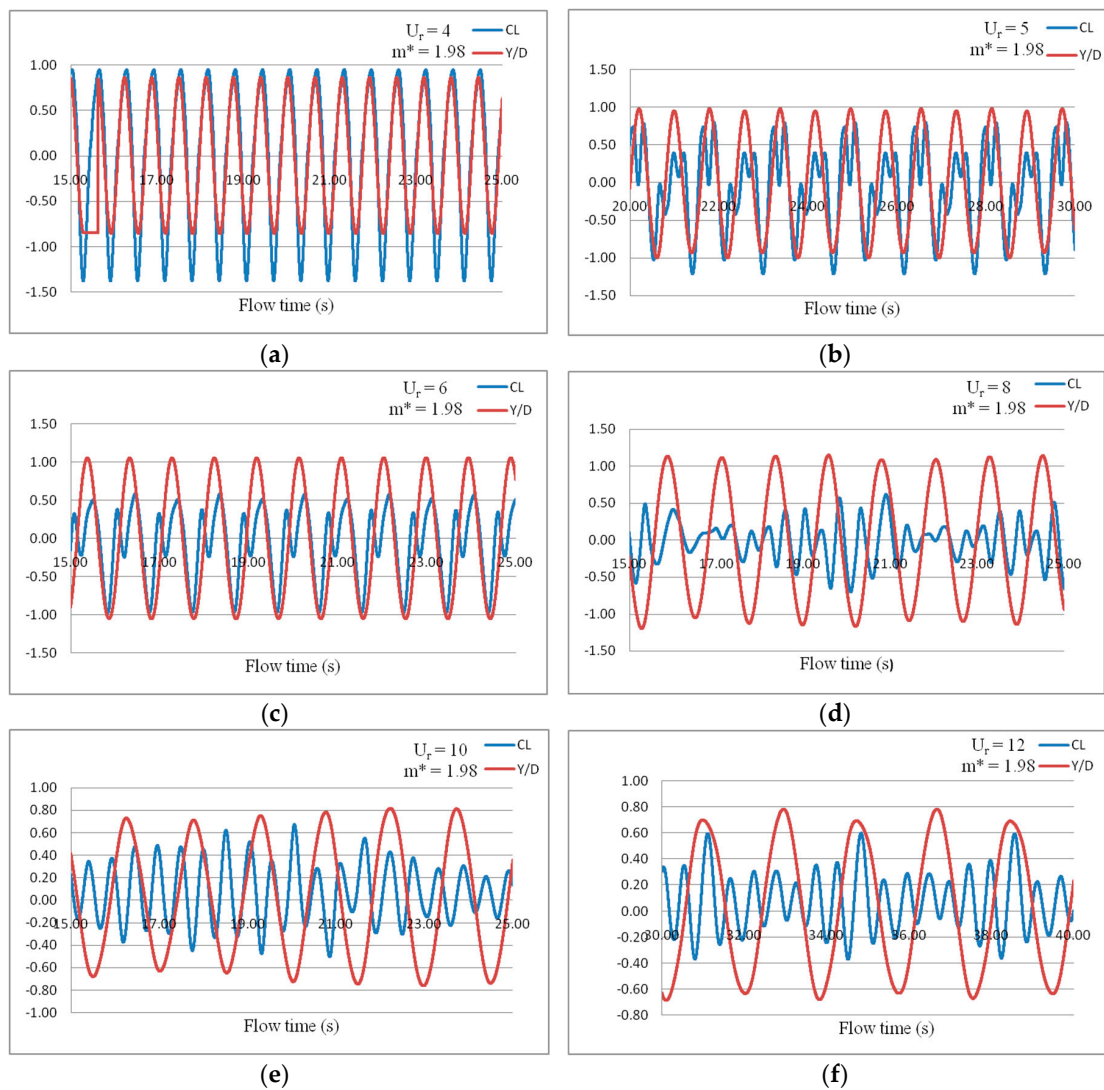


Figure 9. Variation of C_L with Y/D for $m^* = 1.98$: (a) $U_r = 4$; (b) $U_r = 5$; (c) $U_r = 6$; (d) $U_r = 8$; (e) $U_r = 10$; (f) $U_r = 12$.

From a detailed analysis of amplitude of variation of lift coefficient, it is observed that the characteristics of hydrodynamic load causing the cylinder to oscillate varies with U_r and in turn with frequency ratio, η . For all the three cases, a similarity can be observed in the shedding characteristics which are reflected in the pattern of lift coefficient variation. In each case, a single oscillation of the

cylinder is actuated by a single oscillation of lift force when $U_r = 4$. For $U_r = 6$, double oscillation of lift coefficient is observed for each oscillation of Y/D . The first oscillation is of relatively low amplitude and the second one of larger amplitude. $U_r = 8$ and 10 which is more prone to beating phenomenon displays three separate C_L oscillations for each oscillation of the cylinder. $U_r = 12$ is observed to have an additional half oscillation. For all mass ratios, a 2P mode of vortex shedding is observed in the range of $U_r = 4$ –12 which corresponds to synchronization.

A single beat sustains for a time period of 10.53 and 10.42 seconds for $m^* = 1.98$ and 1.32, respectively. Differently for $m^* = 0.66$, single beat sustains at $U_r = 8$ for 7.84 s which is significantly lesser than the other two cases, showing the highest value of cross flow response amplitude. Also, at the lowest mass ratio, $m^* = 0.66$, it is observed from the response amplitude history that the cylinder initially shows a tendency to beat at $U_r = 10$ with a significantly larger response amplitude with $Y/D = 1.08$ compared to 0.82 and 0.80 for $m^* = 1.32$ and 1.98 respectively at same U_r . Further study on the influencing parameters led to a trend showing a relationship between m^* and U_r , through which they have proved that the range of reduced velocity over which cylinder under VIV shows maximum cross flow response widens as m^* decreases [10]. The relationship put forward by [14] is shown in Figure 11. Results of the present study also show that Y/D increases with decreasing mass ratio and the range of U_r over which the maximum amplitude of response to be expected widens.

The effect of U_r on various simulation parameters is illustrated in Figure 10. A comparison of various hydrodynamic and structural parameters at different k^* values for each case is given in Figure 11a,b. Present simulation results matches well with the values represented in Figure 11b. In all cases maximum response occurs at $U_r = 8$. Even though the response amplitude is high in the range $U_r = 4$ –12, as it deviates away from $U_r = 8$, amplitude decreases. A similar result was reported by [19] is represented in the modified Griffin’s plot.

The numerical simulation could successfully reproduce the response behavior depicted by the lower branch of response. Figure 11b shows the response of a cylinder of mass ratio $m^* = 2.4$ which is comparable with the present study.

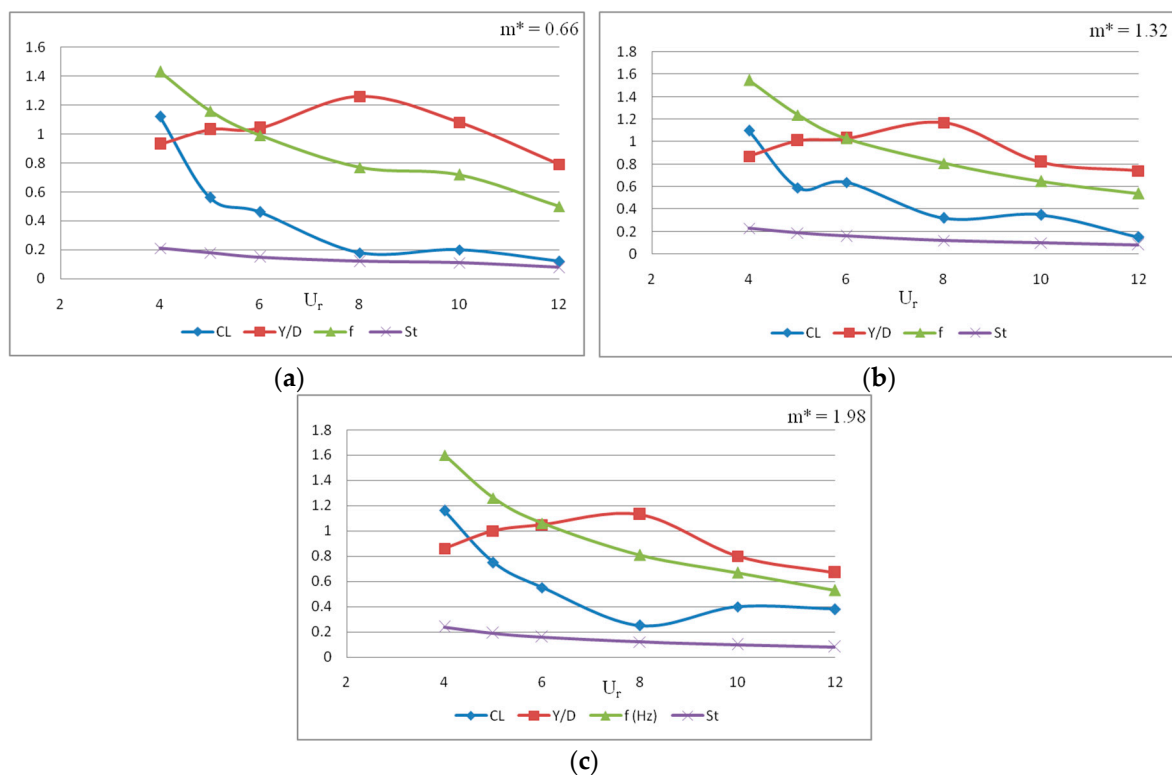


Figure 10. Effect of U_r on various hydrodynamic and structural parameters for VIV of a cylinder (a) $m^* = 0.66$; (b) $m^* = 1.32$; (c) $m^* = 1.98$.

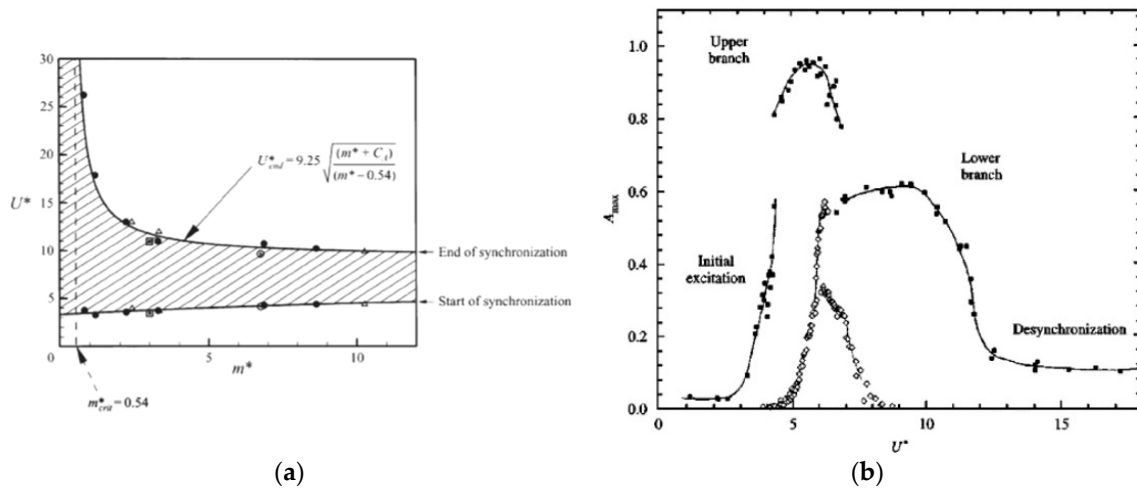


Figure 11. (a) Relationship between U_r and m^* presented by Williamson and Govardhan [23]; (b) maximum response amplitudes A_{max} as functions of the reduced velocity U_r for $m^* = 2.4$ and $m^* = 248$ [19].

It was previously observed that 2P mode shedding is the reason for synchronized response [20]. Since detailed analysis of physics of the flow is not in the scope of this paper, shedding pattern is not further discussed. A representation of 2P mode of vortex shedding in the synchronization range of U_r is shown in Figure 12. A detailed study to analyze this phenomenon is pending. Shedding characteristics at different m^* and k are listed in Table 4.

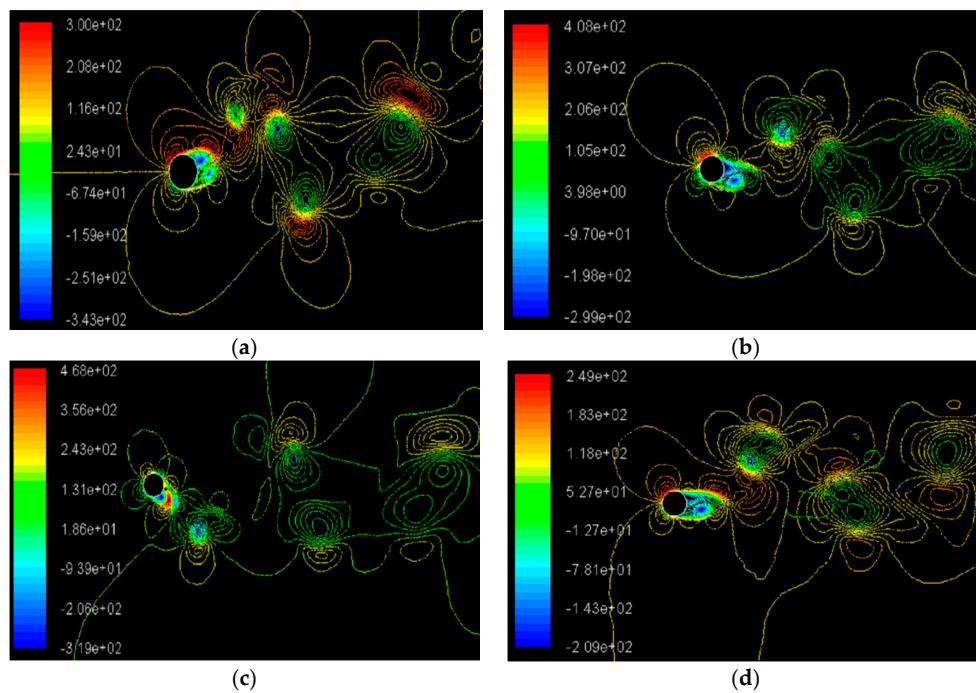


Figure 12. Cont.

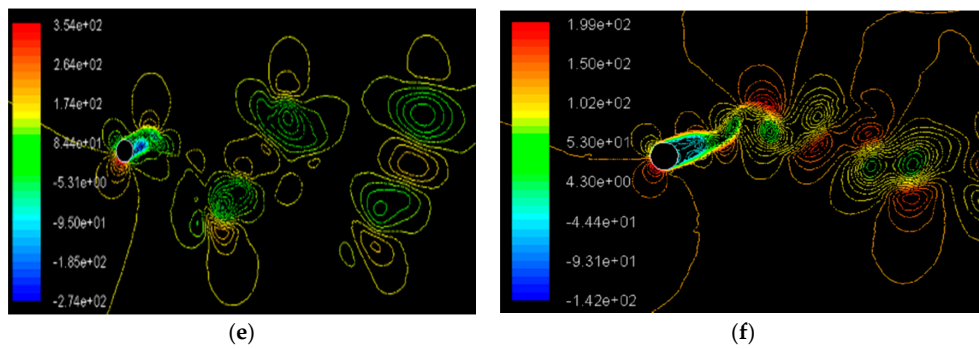


Figure 12. Representation of pressure (N/m²) contours in 2P mode of vortex shedding for $m^* = 0.66$ (a) $U_r = 4$; (b) $U_r = 5$; (c) $U_r = 6$; (d) $U_r = 8$; (e) $U_r = 10$; (f) $U_r = 12$.

Table 4. Hydrodynamic and structural response characteristics for $m^* = 0.66, 1.32,$ and 1.98 .

Mass Ratio, m^*	U_r	C_L	Y/D	f_v (Hz)	η	St	Shedding Characteristics
$m^* = 1.98$	4	1.16	0.86	1.6	1.04	0.24	2P Lift force oscillates about zero value once during one time period of oscillation of the cylinder.
	5	0.75	1.0	1.26	1.04	0.19	2P Lift force oscillates twice during one time period of oscillation of the cylinder.
	6	0.55	1.05	1.06	1.03	0.16	2P Lift force oscillates twice during one time period of oscillation of the cylinder.
	8	0.25	1.13	0.81	1.01	0.12	2P Lift force oscillates thrice during one time period of oscillation of the cylinder.
	10	0.4	0.8	0.67	0.98	0.1	2P Lift force oscillates thrice during one time period of oscillation of the cylinder. Beat phenomenon is observed with time period 10.53 s.
	12	0.38	0.67	0.53	1.04	0.08	2P Lift force oscillates 3.5 times during one time period of oscillation of the cylinder.
$m^* = 1.32$	4	1.1	0.87	1.55	1.07	0.23	2P Lift force oscillates about zero value once during one time period of oscillation of the cylinder.
	5	0.59	1.01	1.24	1.06	0.19	2P Lift force oscillates twice during one time period of oscillation of the cylinder.
	6	0.64	1.03	1.03	1.06	0.16	2P Lift force oscillates twice during one time period of oscillation of the cylinder.
	8	0.32	1.17	0.81	1.01	0.12	2P Lift force oscillates thrice during one time period of oscillation of the cylinder.
	10	0.35	0.82	0.65	1.02	0.1	2P Lift force oscillates thrice during one time period of oscillation of the cylinder. Beat phenomenon is observed with time period 10.42 s.
	12	0.15	0.74	0.54	1.01	0.082	2P Lift force oscillates 3.5 times during one time period of oscillation of the cylinder.
$m^* = 0.66$	4	1.12	0.93	1.43	1.14	0.21	2P Lift force oscillates about zero value once during one time period of oscillation of the cylinder.
	5	0.56	1.03	1.16	1.13	0.18	2P Lift force oscillates twice during one time period of oscillation of the cylinder.
	6	0.46	1.04	0.99	1.10	0.15	2P Lift force oscillates twice during one time period of oscillation of the cylinder.
	8	0.18	1.26	0.77	1.06	0.12	2P Lift force oscillates thrice during one time period of oscillation of the cylinder. Beat phenomenon is observed with time period 7.84 s.
	10	0.2	1.08	0.72	1.1	0.11	2P Lift force oscillates thrice during one time period of oscillation of the cylinder. No beat is observed.
	12	0.12	0.79	0.5	1.1	0.08	2P Lift force oscillates 3.5 times during one time period of oscillation of the cylinder.

Energy possessed by a spring mass system undergoing oscillation can be represented as the sum of its kinetic and potential energies as given by Equation (26).

$$E = \frac{1}{2}m\dot{Y}^2 + \frac{1}{2}kY^2 \quad (26)$$

When the position of the mass corresponds to maximum amplitude, the entire kinetic energy of the system will be converted into potential energy and Equation (26) reduces to

$$E = \frac{1}{2}kY^2 \quad (27)$$

At zero amplitude position of the mass, the entire potential energy is converted into kinetic energy. Since the total energy of the system is conserved energy balance can be written as Equation (28).

$$E = \frac{1}{2}kY^2 = \frac{1}{2}m\dot{Y}^2 \quad (28)$$

Hence the maximum possible velocity with which the system oscillates can be expressed as

$$\dot{Y} = \sqrt{\frac{k}{m}}Y \quad (29)$$

Which may be also represented in non-dimensional form represented by Equation (30)

$$\dot{Y} = \sqrt{\frac{Dk^*g}{L/D}} \frac{Y}{D} \quad (30)$$

For the optimum condition proven numerically, V_{max} is obtained as 0.5 m/s. Power associated with the oscillatory motion can be expressed by Equation (31)

Maximum velocity has been calculated using the above expression and a comparison of average power output estimated is represented in Table 5. Even though the maximum amplitude of oscillation is obtained for each m^* at $U_r = 8$, power output is maximum at $U_r = 4$, suggesting the best operating conditions.

$$P_{avg} = F_L \dot{Y} = C_L \frac{1}{2} \rho AV^2 \dot{Y} \quad (31)$$

Table 5. Cylinder velocity and calculated average power for different configurations.

Re	m^*	U_r	k^*	C_L	Y/D	\dot{Y}	P_{avg} (W)
3.8×10^4	0.66	4	11.17	1.12	0.93	0.74	7.90
		5	6.9	0.56	1.03	0.65	3.44
		6	4.81	0.46	1.04	0.54	2.38
		8	2.7	0.18	1.26	0.49	0.85
		10	1.73	0.2	1.08	0.34	0.64
		12	1.21	0.12	0.79	0.21	0.24
	1.32	4	11.17	1.1	0.87	0.69	7.26
		5	6.9	0.59	1.01	0.63	3.55
		6	4.81	0.64	1.03	0.54	3.28
		8	2.7	0.32	1.17	0.46	1.40
		10	1.73	0.35	0.82	0.26	0.86
		12	1.21	0.15	0.74	0.19	0.28
	1.98	4	11.17	1.16	0.86	0.69	7.57
		5	6.9	0.75	1	0.63	4.47
		6	4.81	0.55	1.05	0.55	2.87
		8	2.7	0.25	1.13	0.44	1.05
		10	1.73	0.4	0.8	0.25	0.95
		12	1.21	0.38	0.67	0.18	0.64

7. Field Test Validation of Numerical Results

The HVPG module with specifications as given in Table 1 has been used for a field test in the Palissery irrigation canal. The flow velocity in the canal was measured to be 0.5 m/s. The model has been tested for different k^* values. Cylinder displacement was measured by attaching a pantograph to the side vanes. As the cylinder oscillates, the marking pencil attached to the spring side of the module marks its impression on the paper attached on the vane side. The results are tabulated in Table 6. $U_r = 4, 8,$ and $12,$ but the effect of k^* is observed to follow the same trend as predicted numerically. An average deviation of 30% is observed between numerical method and field tests. Over prediction of the response amplitude by the numerical method may be attributed to not accounting for structural damping. Also, friction in the sliding parts of the guide vane contributes to lowering the response. Components of the HVPG and field test set up are shown in Figure 13.

Table 6. Results of field test conducted at Palissery irrigation canal.

Re	m^*	U_r	k^*	Y_{field} (cm)	Y/D_{field}	$Y/D_{numerical}$
3.8×10^4	0.66	4	11.17	5.5	0.72	0.93
		8	2.7	7.5	0.98	1.26
		12	1.21	4.5	0.59	0.79



Figure 13. (a) Model of HVPG; (b) field test at Palissery irrigation canal for $m^* = 0.66$ and $U_r = 4, 8,$ and $12.$

8. Conclusions

Extensive research carried out to understand and interpret the intrinsic vortex shedding phenomenon has brought out several correlations to estimate response amplitude Y/D [32], but most of these expressions define the non-dimensional oscillation amplitude Y/D as a function of complex parameters like the Skop–Griffin parameter [14]. The present study is an effort to understand the hydrodynamic response of the cylinder from a designers' perspective by considering the effect of tangible system parameters only. Optimum response is obtained at $m^* = 0.66$ and $U_r = 8,$ but optimum estimated power output for the same mass ratio is obtained at $U_r = 4.$ It is observed that maximum power output can be derived from an HVPG operating at low mass ratio and in the lowest regime of reduced velocity in the synchronization range irrespective of amplitude of cylinder response. The reduced power output at $U_r = 8$ is due to the lower value of C_L which in turn is due to several oscillations of lift force within one time period of oscillation of the cylinder. The true values of frequency ratio, η obtained from the simulations are indicative of synchronized response for the range of U_r considered. Hence it is observed that the developed numerical method could successfully simulate the flow around an oscillating cylinder. The numerical method developed is capable of predicting the trend of variation of Y/D which is verified using the results of field test. At $m^* = 0.66$ where maximum response is observed, η significantly exceeds over unity compared to the higher mass ratio cases. It can

be concluded that maximum amplitude of response is observed at mass ratios corresponding to η values greater than unity rather than at unity η values. Even though hydrodynamic lift force acting on the cylinder is proportional to the incoming flow velocity, C_L strongly depends on the natural frequency of the oscillating system and the shedding pattern. Response amplitude of the cylinder also depends on stiffness ratio k^* and in turn on natural frequency of the oscillating system f_n . Response amplitude increases with decreasing mass ratio and the range of U_r over which the response is high (resonance) widens. Occurrence of beat phenomenon also depends on m^* and k^* and the relationship is more pronounced at lower values of m^* . The mode of vortex shedding depends only on U_r at a constant flow velocity and is independent of m^* . On the whole, the work provides strong design inputs to the construction of the envisaged HVPG model.

9. Scope for Future Research

The discussions and conclusions from Sections 7 and 8 respectively indicate an immense scope for future research. Authors are in the process of improving the present design by incorporating structural damping in the studies. Inclusion of a greater number of rollers in the guide vanes is also being aimed at for eliminating the friction between sliding parts. The influence of these additional parameters in the equation of motion can reduce the errors in the subsequent numerical prediction, leading the design parameters closer to those of practical values. Improvised designs are also being devised for minimizing the transmission losses during power generation.

Author Contributions: Conceptualization, V.C., S.M., and S.J.; Data curation, V.C. and S.J.; Formal analysis, V.C. and S.J.; Funding acquisition, S.J. and V.M.; Investigation, V.C.; Methodology, S.M. and S.J.; Project administration, S.M. and S.J.; Resources, S.J. and V.M.; Software, V.M.; Supervision, S.M. and S.J.; Validation, V.C. and S.J.; Visualization, V.C. and S.J.; Writing—original draft, V.C. and S.J.; Writing—review & editing, V.C., S.J., and V.M.

Funding: This research was partially funded by Energy Management Center, Government of Kerala, India specifically for the development of Hydro Vortex Power Generator module with grant no. EMC/ET&R/18/R&D/SCMS/01.

Acknowledgments: The authors would like to thank the management and principal of SCMS School of Engineering and Technology for all the support offered for the research and development. The authors would also like to thank Energy Management Center, Government of Kerala for all the support.

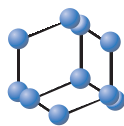
Conflicts of Interest: The authors declare no conflict of interest.

References

- Gerrard, J.H. The mechanics of the formation region of vortices behind bluff bodies. *J. Fluid Mech.* **1966**, *25*, 401–413. [[CrossRef](#)]
- Gao, Y.; Fu, S.; Xiong, Y.; Zhao, Y.; Liu, L. Experimental study on response performance of vortex-induced vibration on a flexible cylinder. *Ships Offshore Struct.* **2016**, *12*, 116–134. [[CrossRef](#)]
- Bimbato, A.M.; Pereira, L.A.; Hirata, M.H. Suppression of vortex shedding on a bluff body. *J. Wind Eng. Ind. Aerodyn.* **2013**, *122*, 16–18. [[CrossRef](#)]
- Bernitsas, M.; Raghavan, K.; Ben-Simon, Y.; Garcia, E. VIVACE (Vortex Induced Vibration Aquatic Clean Energy): A New Concept in Generation of Clean and Renewable Energy from Fluid Flow. *J. Offshore Mech. Arct. Eng.* **2006**, *130*, 041101. [[CrossRef](#)]
- An, X.; Song, B.; Tian, W.; Ma, C. Design and CFD Simulations of a Vortex-Induced Piezoelectric Energy Converter (VIPEC) for Underwater Environment. *Energies* **2018**, *11*, 330. [[CrossRef](#)]
- Janardhanan, S.; Chandran, V.; Varghese, C.; Achuth, D.; Devassy, D.; Mathews, D.C. Hydro vortex power generator design and construction. In Proceedings of the Kerala Technological CONGRESS, KETCON 2018—Human Computer Interface, Thrissur, India, 24 February 2018.
- Griffin, O.M. Vortex-Excited Cross-Flow Vibrations of a Single Cylindrical Tube. *ASME J. Press. Vessel Technol.* **1980**, *102*, 158–166. [[CrossRef](#)]
- Khalak, A.; Williamson, C.H.K. Dynamics of a hydroelastic cylinder with very low mass and damping. *J. Fluids Struct.* **1996**, *10*, 455–472. [[CrossRef](#)]

9. Narendran, K.; Murali, K.; Sundar, V. Vortex-induced vibrations of elastically mounted circular cylinder at Re of the O(105). *J. Fluids Struct.* **2015**, *54*, 503–521. [[CrossRef](#)]
10. Govardhan, R.; Williamson, C.H.K. Defining the ‘modified Griffin plot’ in vortex-induced vibration: Revealing the effect of Reynolds number using controlled damping. *J. Fluid Mech.* **2006**, *561*, 147–180. [[CrossRef](#)]
11. Bernitsas, M. Out of the Vortex. *Mech. Eng.* **2010**, *132*, 22–27. [[CrossRef](#)]
12. Tian, W.; Mao, Z.; Zhao, F. Design and Numerical Simulations of a Flow Induced Vibration Energy Converter for Underwater Mooring Platforms. *Energies* **2017**, *10*, 1427. [[CrossRef](#)]
13. Khan, N.B.; Ibrahim, Z.; Tuan, L.; Javed, M.F.; Jameel, M. Numerical investigation of the vortex-induced vibration of an elastically mounted circular cylinder at high Reynolds number ($Re = 104$) and low mass ratio using the RANS code. *PLoS ONE* **2017**, *12*, e0185832. [[CrossRef](#)] [[PubMed](#)]
14. Williamson, C.H.K.; Govardhan, R. Vortex induced vibrations. *Annu. Rev. Fluid Mech.* **2004**, *36*, 413–455. [[CrossRef](#)]
15. Achenbach, E.; Heinecke, E. On Vortex Shedding from Smooth and Rough Cylinders in the Range of Reynolds Numbers 6×10^3 to 5×10^6 . *J. Fluid Mech.* **1981**, *109*, 239–251. [[CrossRef](#)]
16. Blevins, R.D. *Flow-Induced Vibration*, 2nd ed.; Van Nostrand Reinhold: New York, NY, USA, 1990; pp. 163–164, ISBN 1-57524-183-8.
17. Gabbai, R.D.; Benaroya, H. An overview of modeling and experiments of vortex-induced vibration of circular cylinders. *J. Sound Vib.* **2005**, *282*, 575–616. [[CrossRef](#)]
18. Anagnostopoulos, P.W.; Bearman, P.W. Response characteristics of a vortex excited cylinder at low Reynolds number. *J. Fluids Struct.* **1992**, *6*, 39–50. [[CrossRef](#)]
19. Khalak, A.; Williamson, C.H.K. Investigation of the relative effects of mass and damping in vortex induced vibration of a circular cylinder. *J. Wind Eng. Ind. Aerodyn.* **1997**, *69–71*, 341–350. [[CrossRef](#)]
20. IcemCfd, A. *12.0 User’s Ma*; Ansys Inc.: Canonsburg, PA, USA, 2009; Volume 5.
21. Fluent, A. *12.0 Theory Guide*; Ansys Inc.: Canonsburg, PA, USA, 2009; Volume 6.
22. Menter, F.R. Two-equation eddy-viscosity turbulence models for engineering applications. *AIAA J.* **1994**, *32*, 1598–1605. [[CrossRef](#)]
23. Anton, G. Analysis of Vortex-Induced Vibration of Risers. Master’s Thesis, Applied Mechanics, Chalmers University of Technology, Gothenburg, Sweden, 2012.
24. Vandiver, J.K. Damping parameters for flow-induced vibration. *J. Fluids Struct.* **2012**, *35*, 105–119. [[CrossRef](#)]
25. Schlichting, H. *Boundary Layer Theory*, 8th ed.; McGraw-Hill Book Company: New York, NY, USA, 1979; ISBN 13 978-3540662709.
26. Iaccarino, G.; Mishra, A.A.; Ghili, S. Eigenspace perturbations for uncertainty estimation of single-point turbulence closures. *Phys. Rev. Fluids* **2017**, *2*, 024605. [[CrossRef](#)]
27. Mishra, A.A.; Gianluca, I. Uncertainty Estimation for Reynolds-Averaged Navier Stokes Predictions of High-Speed Aircraft Nozzle Jets. *AIAA J.* **2017**, *55*, 3999–4004. [[CrossRef](#)]
28. Govardhan, R.; Williamson, C.H.K. Modes of vortex formation and frequency response for a freely-vibrating cylinder. *J. Fluid Mech.* **2000**, *420*, 85–130. [[CrossRef](#)]
29. Chen, W.; Zhang, Q.; Li, H.; Hu, H. An experimental investigation on vortex induced vibration of a flexible inclined cable under a shear flow. *J. Fluids Struct.* **2015**, *54*, 297–311. [[CrossRef](#)]
30. Feng, C.C. The Measurements of Vortex Induced Effects in Flow Past a Stationary and Oscillating Circular and D-Section Cylinders. Master’s Thesis, The University of British Columbia, Vancouver, BC, Canada, 1968.
31. Naudascher, E.; Rockwell, D. *Flow Induced Vibration—An Engineering Guide*; Dover Publications Inc.: Mineola, NY, USA, 2005; pp. 37–38, ISBN 13 978-0-486-44282-2.
32. Domal, V.; Sharma, R. An experimental study on vortex-induced vibration response of marine riser with and without semi-submersible. *J. Eng. Marit. Environ.* **2017**, *232*, 176–198. [[CrossRef](#)]





A Secure Reversible Data Hiding and Encryption System for Embedding EPR in Medical Images

Sonal Ayyappan¹, C. Lakshmi² and Varun Menon^{3,*}

¹Department of Software Engineering, SRM University Chennai, Chennai, India; ²Department of Computer Science and Engineering, SRM University, Chennai, India; ³Department of Computer Science and Engineering, SCMS School of Engineering and Technology, Kochi, India

Abstract: Background: Recent advances in medical associated technologies have drastically increased the amount of electronic medical records collected, stored and transferred through the network. Considering the significance and level of sensitivity of the collected medical data, the security of the transmitted data has become a very vital and challenging task for researchers. The protection of these medical images with embedded data is usually guaranteed using encryption or data hiding techniques. Conventional techniques that employ encryption or data hiding are often insecure and also time-consuming during transmission through the network.

Materials and Methods: A method combining encryption and data hiding together can result in compression of data that reduces the transmission time and increases the security level. Reversible data hiding in images can reestablish the cover image after extracting the hidden embedded data exclusive of alterations. Here a new reversible crypto-watermarking system is proposed using cryptographic algorithms that encrypts and hides an Electronic Patient Record (EPR) into an image corresponding to that patient using Rhombus Prediction Scheme. It embeds a big amount of encrypted data into an image with hardly noticeable modification using spatial pixel manipulations based on prediction errors. The marked image is hashed using SHA-256 algorithm.

Results and Conclusion: Hashing and cryptography increases the robustness and guarantees authenticity with integrity. The proposed method results in improved safety with a lower transmission time than the existing methods.

ARTICLE HISTORY

Received: November 01, 2018
Revised: January 14, 2019
Accepted: January 29, 2019

DOI:
10.2174/1574362414666190304162411



CrossMark

Keywords: Crypto-watermarking, Diffie-Hellman, image security, medical images, RC4 encryption, rhombus prediction scheme, SHA-256.

1. INTRODUCTION

Crypto-watermarking has great significance in the area of research related to medical associated technologies. Patient's medical reports are transferred among health care institutions to get opinions from experts. Storage and locked transmission of the medical images [1] are carried out using well-organized crypto-watermarking systems. Crypto-watermarking helps to provide suitable information embedded in medical images without any chance of defaming an institution by providing the proposed owner with legal medical images. Encryption is done to protect image while transferring through channel. Once the images are decrypted on the receiver side, they are prone to breaches of security, which can be met by watermarking.

Crypto-watermarking is a method used to combine cryptography with watermarking. These techniques have recently

become important in areas such as health, military interaction and law administration and have also been widely employed to securely transmit data between devices in Internet of Things and fog networks [2-6]. Web application for data transmission has created a security call. The protection of privacy can be guaranteed by encrypting and embedding the symmetrical key that forms the encrypted domain. Hiding the encrypted data ensures confidentiality and the authentication in the transmission of medical images. One important difference between text and image data is that the text data is much lesser than image data when considering size. While transmitting an encoded image with hidden data, the unidentified source attempts to compress this encoded image. Time taken, which is also a major concern, can be found on two levels, one for encryption and the other for image transfer. To minimize it, the first step is to choose a robust, fast and easy cryptosystem implementation method. Another key concern is the compression method, which reduces the size of the images deprived of losing the characteristics of the image. Partial encryption is a method for reducing computer resources for large amounts of multimedia data in low power networks. In order to transfer images se-

*Address correspondence to this author at the Department of Computer Science and Engineering, SCMS School of Engineering and Technology, Ernakulam 683582, India; E-mail: varunmenon@scmsgroup.org

curely with confidential data embedded, encryption of EPR (Electronic Patient Record) that includes patient id, current diagnostic and Region of Interest is done. This avoids the need to encrypt image to be transferred that saves much of time and computational resources.

A medical practitioner requires the data to be sent securely to a medical expert. In order to preserve the ethics regarding the broadcast of medical images along with the patient record, the combination of encryption and data hiding is made. The encryption of medical data with the area of interest preserves the image detail, also privacy along with confidentiality is ensured. This hiding scheme is used for grayscale image based on prediction error or local standard deviation to encode the encrypted data securely. This preserves the attacker from taking the data. Works previously done in this area are discussed in Section II. The planned technique and its features are described in Section III. Results from the experiments are presented and discussed in Section IV and Section V concludes the paper with Future scope.

2. RELATED WORKS

Reversible Data Hiding (RDH) is widely considered by researchers worldwide as one of the major research problems. Various techniques are proposed to achieve host images reversibility classified with compression, histogram equalization and differential expansion. The general method for compressing data [7-11] is embedding the relevant information in the watermarked host image. This is done by compressing a small amount of the cover image. Histogram equalization is an additional method for hiding reversible information as in [12-23]. The initial reported technique was to embed 1/0 bit by moving the highest / lowest bin [24]. It was reported that only the peak bin pixels were used even when it had overflow and underflow problems. As the number of peak points of the cover image is inadequate, the implanting capacity is low in almost all stated works [25-27].

Tian [28], based on Difference Expansion (DE) proposed a Reversible Watermarking (RW) technique. DE has an advantage of increasing the data hiding capacity and reducing the cost of computing compared to the earlier work [29-33]. Thodi *et al.* [34] as an extension, proposed Prediction Error Expansion (PEE) also implemented in [35-39]. Interpolation of images is another idea used to protect the reversibility of the image cover. In this case, $2M \times 2N$ sized image is first sized down to $M \times N$ dimension known as the seed pixels. The final cover image of the size $2M \times 2N$ is obtained from the seed pixels. The different interpolation methods (IM) are Neighbour Mean Interpolation (NMI) [40-42], Interpolation by Neighbouring Pixels (INP) [43], Interpolation by Maximizing the difference values between Neighbouring Pixels (IMNP) [44] and Pixel Repetition Technique (PRT).

A novel approach to image interpolation was given in [44, 45] using Neighbour Mean Interpolation (NMI). In [35], Luo *et al.* used IM using neighbouring pixels to implement reversibility. The algorithm does not have underflow and overflow problems and embedding does not use border pixels. Abadi *et al.* [46] used Histogram shifting method to intensify the embedding volume. The boundary pixels were

used for embedding, thus surging the payload. Naheed *et al.* [47] improved reversibility by approximating misplaced pixels with Particle Swarm Optimization (PSO). In [48], Lee and Huang suggested an INP to provide a reversible high-capacity hiding algorithm for pixel differential values which was maximum. Jie *et al.* [49] suggested another technique based on prolonged interpolation of images using the highest difference among adjacent pixels. Poor perception of watermarked images was the result. Tang *et al.* [50] reported immense capacity RDH approach for a group of standard images, ranging from 1.20 bits per pixel (bpp) to 2.45 bpp.

In [51], Arsalan reported an RW algorithm for medical pictures using the various approaches along with Genetic Algorithm (GA). For a payload of 0.5 bpp the average arrived PSNR was 45 dB. Hiraik *et al.* [52] suggested an RDH algorithm, considering the different modes of capturing and sizes of DICOM images. It replaces usual Reversible Watermarking (RW) with reversible contrast mapping (RCM) from Colcut, which ensures low computer difficulty. Tsai *et al.* [27] proposed an RDH system for medical pictures with huge payloads using the neighbouring pixel residual histogram prediction technique. Naheed *et al.* [53] gave a technique which worked on the expansion of cumulative interpolation-error for medical pictures. In order to achieve reversibility in watermarking and huge payload, the authors worked with GA and PSO. For 38,545 bits of data the authors testified a PSNR of 49 dB. The key attribute of any hiding system is the ability to detect and locate tampering [54, 55]. Hiding systems are gaining wide popularity in data transmission in areas like underwater sensor networks [56-58], swarm robots [59], ad hoc networks [60].

The authors of [55] have proposed an RDH scheme using Distributed Source Code (DSC) in encoded images. When the receiver has the encryption key only, the original cover image can be recovered with almost the same quality with the help of an image estimation algorithm. Authors of [61] proposed a new crypto-watermarking system to recognize the original data with illegitimate distribution. In [62], a new method along with traditional RDH method is proposed by reserving the room before encryption. The procedure described by authors of [63] embeds EPR in the cover image using discrete cosine transform (DCT) watermarking and RSA cryptographic algorithm. The technique proposed in [64] is built on the combination of public-private key encryption, secret keys and watermarking. The author of [65] proposed a new scheme for the hiding of reversible information in encrypted pictures. When the receiver has data hiding and encryption keys, it takes advantage of the natural image spatial correlation to obtain extra data and claim the error-free original content.

The work presented in [66] shows a system with integrity checking of images using the Fast Johnson Linden-Strauss Transform (FJLT) image hashing method and a blind DCT watermarking method. It is robust with JPEG compression with a quality level of more than 60 and can be distinguished from any other possible handling. The system proposed in [67] is built on an approach that combines the Quantization Index Modulation watermarking algorithm (QIM) with an encryption algorithm. Medical watermarking must maintain the superiority of the image for medicinal diagnosis and

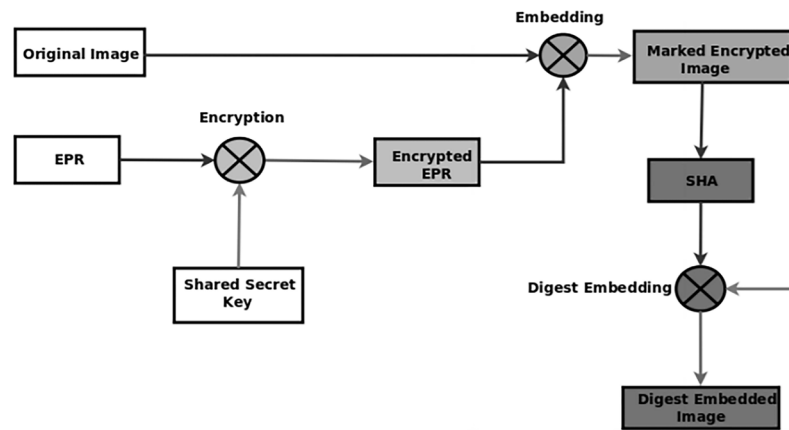


Fig. (1). Proposed methodology for medical specialist. (A higher resolution/colour version of this figure is available in the electronic copy of the article).

treatment. The paper [68] highlights the need for medical watermarking with an evaluation of advances since 2000. It simulates tests to determine the importance of watermarking in managing health information.

The science involving the collaboration of secret data in a suitable multimedia carrier is steganography. In the paper [69], the author examines the distinctive existing approaches of steganography and some common benchmarks derived from the literature. In order to improve the sharing of medical images in e-learning or remote diagnostic aids applications, the authors of [70] suggested watermarking it with a summary of its use of the image. In [71-76], application in acoustic, multimedia and radar systems could be followed. Using interpolation-based reversible watermarking has been suggested in [77-79] for medical and RS images. The paper [80] addresses this issue and a block image encryption has been suggested to get a hidden EPR data encrypted image. It also uses support vector machine based classification for extracting data from the encrypted image. In [81], Authors proposed an RDH algorithm for images exclusive of the use of a location map in the paper. This algorithm incorporates data into the image that exploits the forecast error and then encrypts it. The authors of paper [82] used the method of hiding data based on bit substitution to implant the secret data. The secret key k is used for each block Y_i as the initial start of the Pseudo-Random Number Generator (PRNG) to replace a pixel bit with a bit of data to be implanted.

Various methodologies have been suggested to safeguard the authenticity of multimedia images. These methods include traditional cryptography, watermarking and digital signatures created on relevant image content. The authors of [83] aim to survey and present a comparison of developing image authentication methods based on their service, detection, location and restoration abilities and toughness versus various anticipated image-processing processes. The authors of paper [84] present an RDH algorithm that can recapture the original image from the encoded image without any distortion after extracting the secret data. This method uses the zero or minimum points in the histogram of an image and marginally alters the values of grayscale to include data in the image.

The authors in [85] use pixel to block conversion instead of interpolation ensuring reversibility. They also included a fragile watermark and block checksum in order to facilitate

content authentication at the receiver. Intermediate Significant Bit Substitution has been used to insert the EPR, watermark and checksum data. In addition to providing complete reversibility of high quality and high capacity watermark, this also detects and localizes tamper if any. Use of robots in telemedicine is becoming popular these days hence the authentication of the data collected by robots has to be ensured.

3. MATERIALS AND METHODS

The proposed method is a combination of encryption and data hiding with integrity verification using hashing technique. A medical image with the help of a medical specialist is nominated for transmission. Prior to transmission, steps to be done systematically are as follows. The EPR data is encrypted using the Diffie Hellman key initialization technique for ensuring authentication using the RC4 method. Then hiding is done on the encrypted data. The data-hiding scheme used is built on prediction errors manipulating the features of local variance. The watermarked image is finally transmitted after calculating its digest based on SHA hashing scheme and appending it to the image with hidden data. The suggested method is shown in Fig. (1) from the transmission perspective and in (Fig. 2) from the receptive perspective.

The asymmetric methods are not appropriate for encrypting images due to their computational complexity. So an encryption of secret key with transmission channel for transferring the key is used. Key is confirmed based on Diffie-Hellman key algorithm (DH). The proposed method combines a symmetric encryption algorithm for EPR data, data hiding scheme for embedding encrypted data and a hashing scheme for integrity verification of the marked image in transit.

If a specialist M wants to safely send another specialist S a medical image of concern, M will encrypt the EPR data using a symmetrical algorithm. For this purpose, M generates its secret key to encrypt the EPR data, which is then inserted into the cover image using spatial pixel manipulation based on prediction errors to obtain a watermarked image. As in space, the capacity of data embedding is more comparable to the frequency domain. After that, the digest is calculated using a hashing scheme for the integrity check and attached at the end of the image. Finally, send the picture marked to specialist S . S on receiving the image, checks the

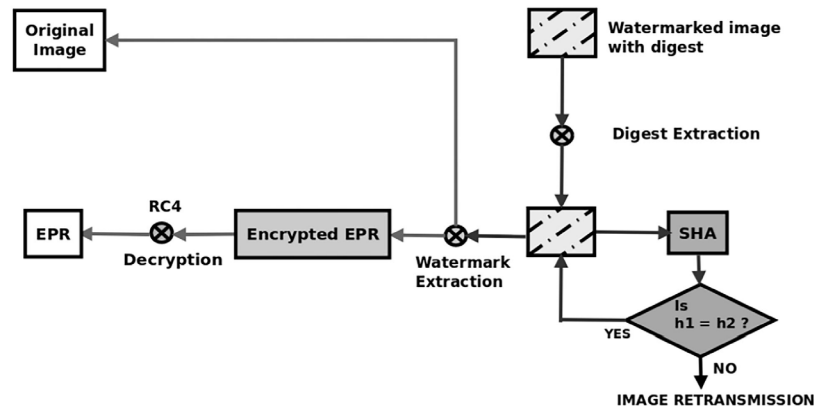


Fig. (2). Proposed methodology for the receiver specialist. (A higher resolution/colour version of this figure is available in the electronic copy of the article).

digest to verify the integrity of the image and extracts the hidden key k by which he can decrypt and view the data M received by him.

Basically, the RDH scheme for EPR data in medical images involve EPR data encryption, and embedding the encrypted data using a robust scheme based on spatial/frequency domain characteristics and the image authentication with integrity check is done using hashing scheme which can be SHA- 256. The next sections offer a detailed explanation of the proposed work. The brief points involved in the proposed scheme before the transmission of biomedical images and the EPR data include the enumerated items: -

1. Encryption of EPR data.
2. RDH scheme for embedding the encrypted data
3. Image authentication and integrity verification using hashing technique.

The steps are reversed during the reception of the medical image as shown in Fig. (2).

3.1. EPR Encryption

Section headings should be numbered sequentially, left aligned and have the first letter capitalized, starting with the introduction. Sub-section headings, however, should be in lower-case and italicized with their initials capitalized. They should be numbered as 1.1, 1.2, etc.

EPR data includes various types of data, such as notes from the medical specialist, MRIs and clinical laboratory results. The data of the patient can be transferred to doctors, to the home patient and to other healthcare providers. The advantages of these technologies must be balanced with security and privacy. Access regulator mechanisms are thus used in encryption to protect EPR data. In order to meet this demand, various messaging encryption techniques have been developed. The encryption process can be symmetrical, asymmetrical or hybrid in blocks or streams. Three problems can be encountered; one is when all blocks in regions with same color are encrypted in the same way. The second is that it is not hard to noise block encryption methods, whether symmetrical or asymmetrical. And data integrity is the third. These problems can be solved by grouping encryption and data hiding [8]. Combining encryption and watermarking can

therefore eliminate these problems. The RC4 stream cipher algorithm is applied to X consisting of ERP data with N characters. The general equation for encryption is given below Eq. (1):

$$Y = E_k(X) \tag{1}$$

Where $E_k()$ is the encryption function done with the secret key k and Y is equivalent X cipher text.

3.1.1. Stream Cipher - RC4

RC4 is a symmetric variable key sized stream cipher algorithm. Mostly symmetric stream cipher algorithms are utilized to group the plain text bits/bytes along with secret key bits/bytes supplied from a Pseudo Random Number Generator (PRNG) and an XOR operation is done. The key streams origination depends on one key.

The RC4 PRNG consists of two steps:

- Initialization - A 256-byte table is filled in here by repeating the encryption key.
- Byte key stream generation - Here permutation and addition is applied to the elements of the table to generate the key stream.

When each key stream value is produced, the records in the S-box are permuted, and XORed for encryption on the next byte of plaintext. The reverse is done by XORing the encryption value with the next cipher byte. Image encryption is based on the RC4 algorithm.

3.1.2. Key Scheduling Algorithm

The S items are set from 0 to 255 in ascending order, i.e. $S[0]=$ zero, $S[1]=$ 1, $S[255]=$ 255. If the key with K length is 256 bytes, then K is assigned to a newly created vector T . Otherwise, for a key with length, $keylen$ bytes, the first $keylen$ elements of T is traced from K and then K is iterated number of times so as necessary to fill T .

3.1.3. Byte Stream Generation

The input key is used only till S has been initialized. The stream origination starts from $S[0]$ to $S[255]$ and keeps on replacing $S[i]$ with another byte as configured by S . This process repeats the procedure.

The EPR data is shown below as a sample example and its corresponding RC4 encryption is done. It is converted to a binary format and then incorporated into the medical image.

3.1.4. Electronic Patient Record

Patient Name: Ghosh (m)
 Patient ID: 12005
 Diagnostic: TB
 ROI: (142, 87) (97,151).

Binary Encrypted Electronic Patient Record
11111100100010101
000000010000010100000
00000011010110011
0110111.....00111000.

3.2. Data Embedding

The converted data is incorporated in the host image by sorting local variances μ based on prediction errors. The local variance $\mu_{i,j}$ is used to measure data embedding feature. It should be unaffected even after data hiding in the cover image is done. It is also related to the magnitude of cell error under consideration.

Cell is a pixel unit in which data must be embedded. Efficient embedding of low distortion data can be achieved using the prediction scheme. Each picture element of the host image is used to hide data, which significantly increases the capacity. Techniques for hiding data prefer prediction error values that are low. The reversible data hiding after EPR data encryption is the main emphasis of this methodology. The data safety is ensured by RC4 encryption and this respective data is then secreted in the medical copy using prediction error scheme. The use of prediction errors in spatial domain is effective where the correlation factor is high and distortion resulted in embedding is less. The method makes use of histogram shifting method and local variance determination. The ratio of local variance within a set of pixels in medical image before and after embedding remains the same. This feature enables the extraction of elec-

tronic data fast and with less error induced. After the embedding, hash of watermarked image is found to get a digest, which is used to verify the legitimacy of medical data.

At receiver end, the image obtained from the practitioner is checked for its authenticity and integrity while taking the hash of the image and comparing it with the respective hash digest sent via email. When the hash is found to be same, the image is worked upon for extraction of the electronic patient record. Otherwise, the image is regarded as manipulated during transmission and is requested for retransmission. The extraction method is followed as the same prediction error scheme used while embedding data.

3.2.1. EPR Data Embedding in DCT Domain

The EPR data embedding method in the DCT domain systematically ensures ERP data encryption and image watermarking in medical field with guaranteed privacy and security. In the presence of a medical specialist, a medical image is chosen for transmission. The following steps are done thoroughly before the transmission. This comprises encryption of EPR record for a patient account associated with the corresponding scan or other biomedical image sets. The encryption is done after the secret key is agreed on securely using convenient stream cipher algorithm RC4. The encrypted electronic patient record is then embedded in the DCT domain by watermarking. The key is encrypted by a public-private crypto system by itself. Finally, the watermarked image with the patient's encrypted record is transmitted for specialist opinion derivation. The EPR data embedding methodology in DCT is depicted in Fig. (3).

Digital watermarking is a tool for copyright defense and to prevent the illegally intended access to reliable multimedia data, including images. The watermarking can be performed in the domain of space and frequency [24]. As the frequency domain was harder to attack, discrete cosine transformation was selected. The spread spectrum approach, which is a traditional method [68], is used to embed encrypted data as the fundamental watermarking principle in the DCT domain. The DCT frequency components are calculated for an input image. In this case, $N \times M$ pixels are taken in consideration. $x(m,n)$ is the spatial component at an image position and $y(u, v)$ is the DCT frequency coefficients at the respective discrete cosine transform position.

The reverse DCT operation is achieved on the watermarked image so as to reestablish the image. This protects the

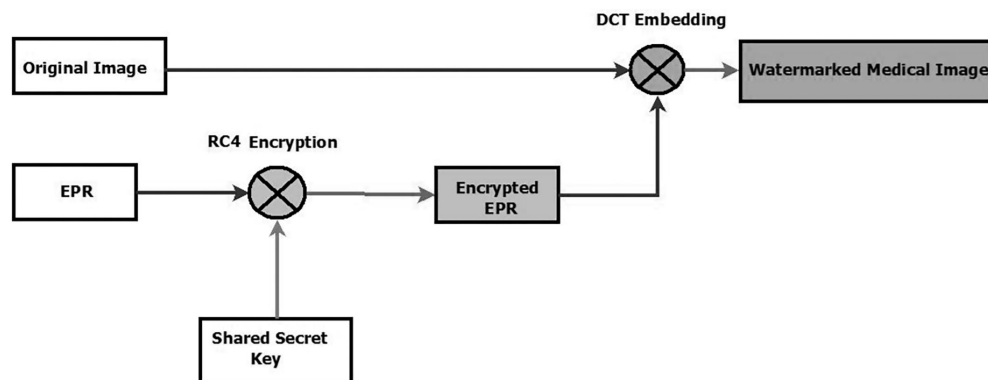


Fig. (3). Methodology for Embedding in DCT. (A higher resolution/colour version of this figure is available in the electronic copy of the article).

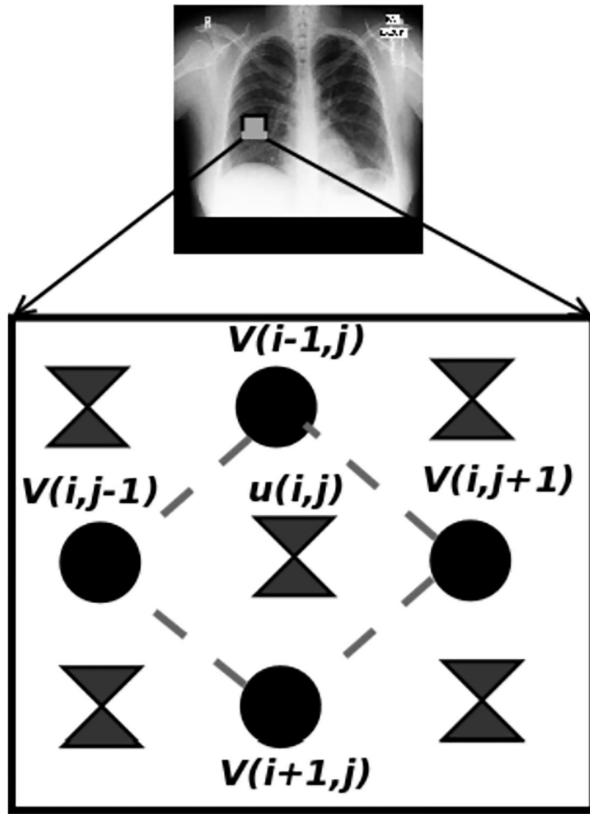


Fig. (4). Cross set. (A higher resolution/colour version of this figure is available in the electronic copy of the article).

watermark information too. The low frequency sub band contains important image details and high frequency image coefficients are easily removed by geometric modification compression. The low frequency sub band contains important image details and high frequency image coefficients are easily eliminated by geometric modification compression.

3.2.2. Spread Spectrum Watermarking

The watermarking algorithm proposed in the DCT field is the spread spectrum technique. First, the position is determined to inject the bits to be watermarked by index classification. Index classification provides an account of high frequency coefficients. The watermark is distributed over several bins, so as to keep the energy negligent and that it cannot be identified in any bin. Therefore, the watermark should be placed in significant regions and hence referred to as frequency domain signal. The explicit placement of the watermark in the most important image coefficients ensures that the watermark is robust and safe. DCT coefficients are calculated for N x N image in order to place watermarks of length n in it. Then the watermark is placed in high coefficients magnitudes.

A watermark is created by independently choosing x_i . A sequence of values V_i is extracted from the host image in which the watermark x_i is inserted to get a series of values W_i as shown in Eq. 2. The insertion of the watermark results in watermarked image W , along a scaling parameter α used to specify the extent to which the watermark alters the cover image. A higher value of α can cause degradation of the watermarked image Eq. (2).

$$W_i = V_i + \alpha x_i \tag{2}$$

where V_i is the DCT image coefficient and α is the scaling factor indicating the degree of imperceptibility. The watermark extraction reverses the above-mentioned process, including analysis of deviation. For each Y_i watermarked chip text, the decoding function is applied to 0 or 1, the probable values and the local standard deviation is analyzed. The value for the bit is selected with the least standard deviation.

3.2.3. Spatial EPR Embedding using Rhombus Prediction Scheme

In the rhombus prediction scheme, image is partitioned into a dot set and a cross set as shown in Fig. (4). The cross set includes a single cross pixel and four dot pixel. The dot pixels are used to evaluate the predicted value of cross pixel where the embedding is done. The embedding method in which modified predicted value of cross pixel in cross set is used for hiding data bits is called cross embedding scheme. Here dot pixels are not changed and this independence of dot pixels with that of cross pixels help in the extraction of data bits reversibly. The dot embedding process is used to significantly increase the embedding rate once the cross embedding is done. Cross embedding and dot embedding methods follow the same process for hiding and it is done consecutively. So for convenience cross-embedding scheme is taken for explanation.

Following are the steps followed for data embedding scheme using rhombus prediction scheme.

1. The image is classified into two sets - cross set and dot set.
2. For individual set, predicted value of pixel, local variance and prediction error is found.
3. Prediction error is sorted based on local variance.
4. First 34 prediction error values after sorting are reserved in order to hide the threshold, load length and location map length.
5. Histogram shifting data hiding method is done checking the overflow and underflow condition. 6. Overflow and underflow condition for a set is done using two-pass testing and location map is updated accordingly.
6. After data hiding is done, the threshold values, the payload and location map length is embedded in first 34-pixel set reserved for it.
7. Same procedure is followed for dot set pixels - this is subsequently called the dot-embedding scheme.

At decoding phase, the independence feature enables the extraction of embedded bits promptly as the dot set pixels is independent of cross set pixel. The diagrammatic representation of the Rhombus prediction scheme is shown in Fig. (5), Eq. (3-5).

Cell definition Predicted Value ($u'_{i,j}$) :

$$u'_{i,j} = \frac{v_{i,j-1} + v_{i+1,j} + v_{i,j+1} + v_{i-1,j}}{4} \tag{3}$$

Prediction Error ($d_{i,j}$)

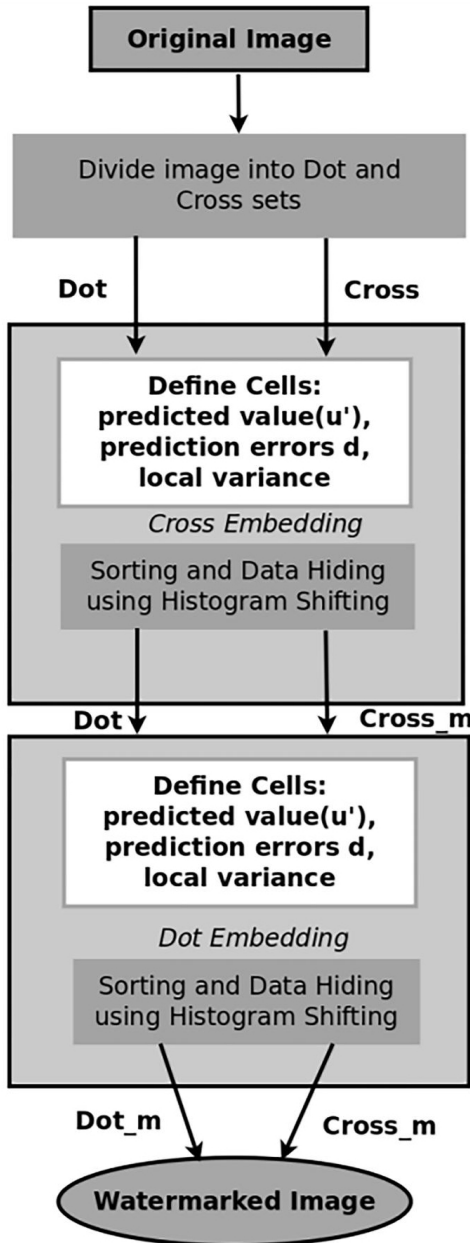


Fig. (5). Proposed rhombus embedding scheme. (A higher resolution/colour version of this figure is available in the electronic copy of the article).

$$d_{i,j} = u_{i,j} - u'_{i,j} \quad (4)$$

Local Variance

$$\mu_{i,j} = \frac{1}{4} \sum_{k=1}^4 (\Delta v_k - \Delta v'_k)^2 \quad (5)$$

where $\Delta v_1 = |v_{i,j-1} - v_{i-1,j}|$

and $\Delta v'_k = \frac{\Delta v_1 + \Delta v_2 + \Delta v_3 + \Delta v_4}{4}$

3.2.4. Histogram Shifting Technique Encoding

Encoding using Histogram Shifting method follows Eq. (6):

$$D_{i,j} = \begin{cases} 2 * d_{i,j} + \text{bit } d_{i,j} \in [T_n; T_p] \\ d_{i,j} + T_p + 1 & \text{if } d_{i,j} > T_p \text{ and } T_p \geq 0 \\ d_{i,j} + T_n & \text{if } d_{i,j} < T_n \text{ and } T_n < 0 \end{cases} \quad (6)$$

Decoder reverses the original prediction errors and bits embedded Eq.(7,8).

$$d_{i,j} = \begin{cases} \frac{D_{i,j}}{2} & \text{if } D_{i,j} \in [2T_n; 2T_p + 1] \\ D_{i,j} - T_p - 1 & \text{if } D_{i,j} > 2T_p \text{ and } T_p \geq 0 \\ D_{i,j} - T_n & \text{if } D_{i,j} < 2T_n \text{ and } T_n < 0 \end{cases} \quad (7)$$

Bit embedded can be extracted by

$$b = D_{i,j} \text{ mod } 2 \text{ where } D_{i,j} \in [2 * T_n; 2 * T_p + 1] \quad (8)$$

3.2.5. Problems of Overlapping and Under Lapping

To locate the overlapping and underlapping problems the following condition must be met Eq. (9):

$$0 \leq u_{i,j} + D_{i,j} \leq 255 \quad (9)$$

- Two-Pass Testing is done. (With test bits 1 or 0 depending on prediction error)
- Overlapping problems are resolved by location map.
 1. If the cell can be modified at least once, the cell on the map should be '0'.
 2. If the cell cannot be modified at all, the cell on the map should be '1'.

3.3. Authentication

The authentication and integrity of the transmitted image are verified using hashing scheme. The digest of the watermarked image is computed and its one time only. This digest is appended to the watermarked image and sent to the specialist where the extracted digest is verified using the same scheme with the currently calculated digest. Hash functions are deterministic mathematical algorithms that map arbitrary bits in a hash result of a fixed, limited length. The primary use of hash functions in cryptography is the integrity of messages. The hash value provides a digital fingerprint of the content of a message that does not alter the message by an intruder, virus or other means. MD5 and SHA-1 designed by Ronald Rivest and the National Safety Agency (NSA) respectively are the most commonly used hash functions.

3.3.1. Secure Hash Algorithm

The SHA family is a set of associated cryptographic hash functions with 16 bits and above. SHA-2 includes a set of 2 hash functions with 256, 512 bits of digest. SHA-1 algorithm is based on similar principles to the digest algorithm for MD4 messages. It works on 512-bit messaging blocks for which a 160-bit digest is generated. Since the SHA-1 digest is 32 bits longer than the MD5, it is much stronger against attacks 256 converts an input message into a 256-bit digest message. The SHA-256 compression algorithm then repeats



Fig. (6.1). Chest Image.

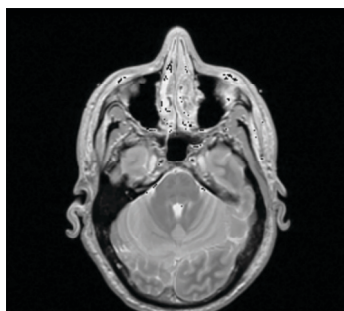


Fig. (6.2). MRI Image.

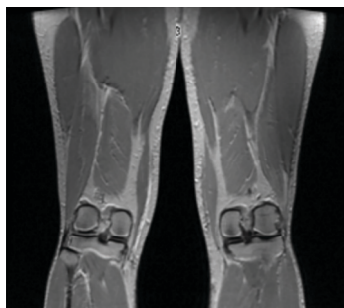


Fig. (6.3). Feet Image.

Fig. (6). Input Images. (A higher resolution/colour version of this figure is available in the electronic copy of the article).

and processes a further 512-bit message block until all data blocks are processed.

3.3.2. Transmissions and Reception

The ERP encrypted data is implanted into the original document with a secret key-ensuring authentication. This encrypted data is transferred to the network after appending the digest evaluated with SHA hashing scheme. When the image is received at the receiver end, the encrypted data has to be reversibly extracted. Before extracting, the hash value is calculated and compared to the hash value extracted. This is carried out to perform integrity check. The algorithm should be a lossless system for the correct removal of the encrypted data.

4. RESULTS

The reversible crypto watermarking system in python was implemented using the Open CV library running on the Ubuntu 14.04 platform with Intel i5 and 4 GB RAM support. The performance of each step in combined spatial embed-



Fig. (7.1). Chest Image.

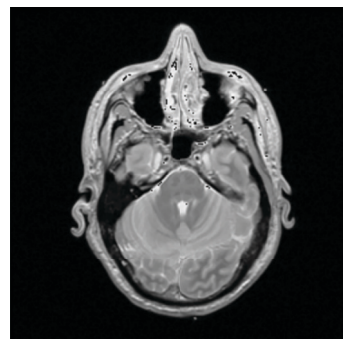


Fig. (7.2). MRI Image.

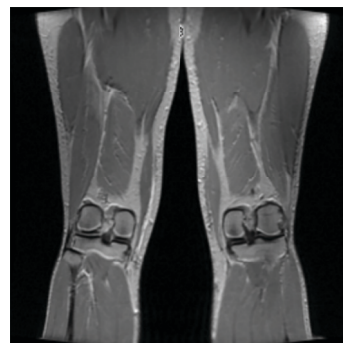


Fig. (7.3). Feet Image

(PSNR = 80.58dB) (PSNR = 79.73dB) (PSNR = 79.88dB

Fig. (7). Watermarked Images. (A higher resolution/colour version of this figure is available in the electronic copy of the article).

ding and frequency embedding crypto watermarking techniques is evaluated using the dataset.

4.1. Dataset

The method proposed is practiced to a chest image (396x 400 pixels), MRI scan and Feet X - Ray image (512x 512 pixels), as shown in Fig. (6.1). The encrypted electronic patient record of variable length is watermarked in the host image and is shown in Fig. (6.2). Mean-Square-Error (MSE) and Peak-Signal-to-Noise Ratio (PSNR) is used to estimate results (Fig. 6.3). Data sets of medical images are collected from (Fig. 7.1-7.3):

- open.nlm.nih.gov/gridquery.php/
- MHealth Database: <https://archive.ics.uci.edu/ml/>
- Montgomery County chest X-ray set [76].

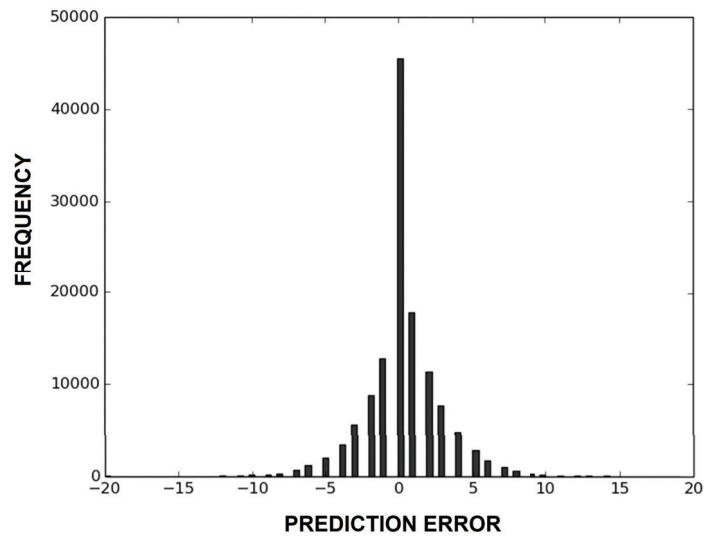


Fig. (8). Prediction Error Histogram ($T_n = -9$, $T_p = 10$). (A higher resolution/colour version of this figure is available in the electronic copy of the article).

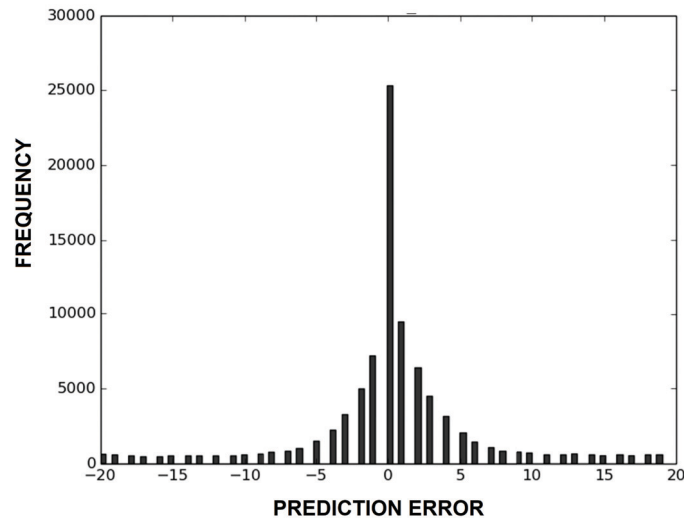


Fig. (9). Prediction error histogram ($T_n = -19$, $T_p = 20$). (A higher resolution/colour version of this figure is available in the electronic copy of the article).

4.2. Results - DCT Crypto-watermarking System

Interpretation of results obtained using histogram analysis, entropy analysis and PSNR ratios calculate the differences among host image and EPR embedded image. The image under consideration has 256 gray scales and the theoretical entropy value is 8 bits. Entropy is a factor for understanding the safety and robustness of image encryption process. The performance of crypto-watermarking techniques with (i) RC4 EPR encryption (ii) DCT- Spread spectrum coding is tested and evaluated with the same dataset. The input images and their respective watermarked images are displayed together with their PSNR values. Since the embedding rates vary, the image quality is reduced in comparison with the spatial embedding system.

4.3. Histogram Analysis

Histogram is a graphic representation, which shows the underlying frequency distribution for a set of uninterrupted data. The spatial embedding method of Rhombus Prediction

Scheme accomplishes the use of histogram shifting and sorting based on predicted values, histogram based on threshold values are used for shifting the bins making room for embedding. For higher efficiency the values of threshold are varied to get more qualified images after embedding. Histograms, the graph between the prediction error and the frequency are shown in Figs. (8 and 9) for 2 sets of threshold values.

4.3.1. D. Quality Check

The crypto-watermarking system proposed is used for medical images. Peak Signal to Noise Ratio is the quality measure utilized to match the original image and embedded data. PSNR should be high in order to obtain a good image. PSNR for $M \times N$ image is provided as below Eq.(10).

$$\text{obtain } PSNR = 10 \log_{10} \left(\frac{\sum_{x=1}^M \sum_{y=1}^N E_{max}^2}{\sum_{x=1}^M \sum_{y=1}^N (f(x,y) - f'(x,y))^2} \right) \quad (10)$$

where, $f(x, y)$ is the original image gray values. $F'(x, y)$ is watermarked image gray values. $M \times N$ is the dimension of the image. The resulting PSNR value for the embedded image tends to be high and decreases as the embedded bits increase.

These results demonstrate an enhancement in the functioning of the crypto-watermarking technique with rhombus prediction. In addition, the use of the digital watermarking and encryption hybrid system resists various types of attacks in a very good way. It ensures confidentiality and robustness. The value of these quality metrics can be concluded to validate the efficiency of the projected crypto-marking.

These results demonstrate an enhancement in the functioning of the crypto-watermarking technique with rhombus prediction. In addition, the use of the digital watermarking and encryption hybrid system resists various types of attacks in a very good way. It ensures confidentiality and robustness. The value of these quality metrics can be concluded to validate the efficiency of the projected crypto-marking technique (Tables 1-3).

Table 1. PSNR value for different bits embedded into chest image.

Bits (Capacity)	PSNR (dB)
216	80.58
888	74.63
3016	69.84
7712	65.77
15242	62.84

Table 2. PSNR value for different bits embedded into MRI image.

Bits (Capacity)	PSNR (dB)
216	79.73
888	74.03
3016	69.22
7712	65.19
15242	62.21

Table 3. PSNR value for different bits embedded into feet image.

Bits (Capacity)	PSNR (dB)
216	79.88
888	73.78
3016	69.91
7712	64.86
15242	61.87

CONCLUSION

For the benign communication of EPR data embedded in a cover image, the method combining encryption and data hiding with integrity verification is proposed and analyzed. The cipher data ensures the robustness of reasonable noise and has a high quality factor. Data hiding based on the rhombus prediction error scheme that compares the standard local deviation is used. The prediction error is used to insert the key due to geometric distortions imperceptibility. Hash scheme SHA is used to calculate an authentication image digest for integrity verification. The EPR embedding with a Rhombus prediction pattern, therefore, applies to the hiding of nil distortion data. In addition, the use of sorting results in a good relationship with capacity and distortion. Numerous works in data hiding of medical images are currently under study and we are working towards an optimal solution modifying and combining the innovative concepts from for future developments in other imaging systems like SAR images and core networks.

ETHICS APPROVAL AND CONSENT TO PARTICIPATE

Not applicable.

HUMAN AND ANIMAL RIGHTS

No animals/humans were used for studies that are basis of this research.

CONSENT FOR PUBLICATION

Not applicable.

AVAILABILITY OF DATA AND MATERIALS

The authors confirm that the data supporting the findings of this research are available within the article.

FUNDING

None.

CONFLICT OF INTEREST

The authors confirm that this article content has no conflict of interest.

ACKNOWLEDGEMENTS

Declared none.

REFERENCES

- [1] Diffie W, Hellman M. New directions in cryptography. IEEE Trans Inf Theory 1976; 22(6): 644-54. <http://dx.doi.org/10.1109/TIT.1976.1055638>
- [2] Philip V, Suman VK, Menon VG, Dhanya KA. A review on latest Internet of things based healthcare applications. Int J Comp Sci Inf Secur 2017; 15(1): 248.
- [3] Vinoj PG, Jacob S, Menon VG. Hybrid brain actuated muscle interface for the physically disabled. Basic Clint Pharmacol Toxicol 2018; 123(S3): 8-9.
- [4] Deshkar S, Thanseeh RA, Menon VG. A review on IoT based m-health systems for diabetes. Int J Comp Sci Tel 2017; 8(1): 13-8.
- [5] Menon VG, Prathap J. Vehicular fog computing: Challenges, applications and future directions. Fog computing: Breakthroughs in research and practice. IGI Global 2018; pp. 220. <http://dx.doi.org/10.4018/978-1-5225-5649-7.ch011>

- [6] Menon VG, Joe Prathap PM. Moving from vehicular cloud computing to vehicular fog computing: Issues and challenges. *Int J Comp Sci Eng* 2017; 9(2).
- [7] Yang B, Schmucker M, Funk W, Busch C, Sun S. Integer DCT based reversible watermarking for images using companding technique. *Proceedings of the SPIE, Security, Steganography, and Water-marking of Multimedia Contents VI*. 2004; pp. 405-15. <http://dx.doi.org/10.1117/12.527216>
- [8] Xuan G, Yang C, Zhen Y, Shi YQ, Ni Z. Reversible data hiding using integer wavelet transform and companding technique. *Digital watermarking IWDW 2004. Lecture Notes in Computer Science Berlin, Heidelberg: Springer* 2005; 3304: pp. 115-24.
- [9] Celik MU, Sharma G, Tekalp AM, Saber E. Lossless generalized LSB data embedding. *IEEE Trans Image Process* 2005; 14(2): 253-66. <http://dx.doi.org/10.1109/TIP.2004.840686> PMID: 15700530
- [10] Memon N, Khan A, Gilani S, Ahmad M. Reversible water-marking method based on adaptive thresholding and companding technique. *Int J Comp Math* 2011; 88(8): 1573-94. <http://dx.doi.org/10.1080/00207160.2010.509429>
- [11] Arsalan M, Malik S, Khan A. Intelligent reversible watermarking in integer wavelet domain for medical images. *J Syst Soft* 2012; 85(4): 883-94. <http://dx.doi.org/10.1016/j.jss.2011.11.005>
- [12] Gao X, An L, Li X, Tao D. Reversibility improved lossless data hiding. *Signal Processing* 2009; 89(10): 2053-65. <http://dx.doi.org/10.1016/j.sigpro.2009.04.015>
- [13] Hu Y, Heung-Kyu Lee, Jianwei Li. DE-based reversible data hiding with improved overflow location map. *IEEE Trans Circ Syst Video Tech* 2009; 19(2): 250-60. <http://dx.doi.org/10.1109/TCSVT.2008.2009252>
- [14] Juang Y, Ko L, Chen J, Shieh Y, Sung T, Hsin H. Histogram modification and wavelet transform for high performance watermarking. *Math Prob Eng* 2012; 2012: 1-14. <http://dx.doi.org/10.1155/2012/164869>
- [15] Kamran KA, Malik S. A high capacity reversible water-marking approach for authenticating images: Exploiting down-sampling, histogram processing, and bloc selection. *Inf Sci* 2014; 256: 162-83. <http://dx.doi.org/10.1016/j.ins.2013.07.035>
- [16] Kim K, Lee M, Lee H, Lee H. Reversible data hiding exploiting spatial correlation between sub-sampled images. *Pattern Recognit* 2009; 42(11): 3083-96. <http://dx.doi.org/10.1016/j.patcog.2009.04.004>
- [17] Lee S, Suh Y, Ho Y. Reversible image authentication based on watermarking. *IEEE International Conference on Multimedia and Expo. Toronto, Canada*. 2006; pp. 1321-4.
- [18] Li X, Li B, Yang B, Zeng T. General framework to histogram shifting- based reversible data hiding. *IEEE Trans Image Process* 2013; 22(6): 2181-91. <http://dx.doi.org/10.1109/TIP.2013.2246179> PMID: 23399962
- [19] Li X, Zhang W, Gui X, Yang B. A novel reversible data hiding scheme based on two-dimensional difference-histogram modification. *IEEE Trans Inf Forensics Security* 2013; 8(7): 1091-100. <http://dx.doi.org/10.1109/TIFS.2013.2261062>
- [20] Ni Z, Shi Y, Ansari N, Su W, Sun Q, Lin X. Robust lossless image data hiding designed for semi-fragile image authentication. *IEEE Trans Circ Syst Video Tech* 2008; 18(4): 497-509. <http://dx.doi.org/10.1109/TCSVT.2008.918761>
- [21] Pan JS, Yang CN, Lin CC, Wang ZH, et al. Multi- dimensional and multi-level histogram-shifting-imitated reversible data hiding scheme *Adv Intell Syst Appl*. 2013; pp. 149-58.
- [22] Tai W-L, Chia-Ming Yeh, Chin-Chen Chang. Reversible data hiding based on histogram modification of pixel differences. *IEEE Trans Circ Syst Video Tech* 2009; 19(6): 906-10. <http://dx.doi.org/10.1109/TCSVT.2009.2017409>
- [23] De Vleeschouwer C, Delaigle J, Macq B. Circular interpretation of bijective transformations in lossless watermarking for media asset management. *IEEE Trans Multimed* 2003; 5(1): 97-105. <http://dx.doi.org/10.1109/TMM.2003.809729>
- [24] De-Vleeschouwer C, Delaigle JF, Macq B. Circular interpretation of histogram for reversible watermarking *IEEE Fourth Workshop on Multimedia Signal Processing*. 345-50.
- [25] Lin C, Tai W, Chang C. Multilevel reversible data hiding based on histogram modification of difference images. *Pattern Recognit* 2008; 41(12): 3582-91. <http://dx.doi.org/10.1016/j.patcog.2008.05.015>
- [26] Ni Z, Shi Y, Ansari N, Su W. Reversible data hiding. *IEEE Trans Circ Syst Video Tech* 2006; 16(3): 354-62. <http://dx.doi.org/10.1109/TCSVT.2006.869964>
- [27] Tsai P, Hu Y, Yeh H. Reversible image hiding scheme using predictive coding and histogram shifting. *Signal Processing* 2009; 89(6): 1129-43. <http://dx.doi.org/10.1016/j.sigpro.2008.12.017>
- [28] Tian J. Reversible data embedding using a difference expansion. *IEEE Trans Circ Syst Video Tech* 2003; 13(8): 890-6. <http://dx.doi.org/10.1109/TCSVT.2003.815962>
- [29] Al-Qershi O, Khoo B. High capacity data hiding schemes for medical images base on difference expansion. *J Syst Soft* 2011; 84(1): 105-12. <http://dx.doi.org/10.1016/j.jss.2010.08.055>
- [30] Alattar AM. Reversible watermark using the difference expansion of a generalized integer transform. *IEEE Trans Image Process* 2004; 13(8): 1147-56. <http://dx.doi.org/10.1109/TIP.2004.828418> PMID: 15326856
- [31] Hsu F, Wu M, Wang S, Huang C. Reversibility of image with balanced fidelity and capacity upon pixels differencing expansion. *J Supercomput* 2013; 66(2): 812-28. <http://dx.doi.org/10.1007/s11227-013-0896-9>
- [32] Jawad K, Khan A. Genetic algorithm and difference expansion based reversible watermarking for relational databases. *J Syst Soft* 2013; 86(11): 2742-53. <http://dx.doi.org/10.1016/j.jss.2013.06.023>
- [33] Hyoung Joong Kim, Sachnev V, Yun Qing Shi, Jeho Nam, Hyoung-Gon Choo. A novel difference expansion transform for reversible data embedding. *IEEE Trans Inf Forensics Security* 2008; 3(3): 456-65. <http://dx.doi.org/10.1109/TIFS.2008.924600>
- [34] Ni R, Cheng HD, Zhao Y, Hou Y. High capacity reversible watermarking for images based on classified neural network. *Lect Notes Comp Sci, Image Anal*. 2013; pp. 697-706. http://dx.doi.org/10.1007/978-3-642-38886-6_65
- [35] Pei Q, Wang X, Li Y, Li H. Adaptive reversible watermarking with improved embedding capacity. *J Syst Soft* 2013; 86(11): 2841-8. <http://dx.doi.org/10.1016/j.jss.2013.06.055>
- [36] Peng F, Lei Y, Long M, Sun X. A reversible watermarking scheme for two-dimensional CAD engineering graphics based on improved difference expansion. *Comp Aided Des* 2011; 43(8): 1018-24. <http://dx.doi.org/10.1016/j.cad.2011.03.011>
- [37] Tseng H, Chang C. An extended difference expansion algorithm for reversible watermarking. *Image Vis Comp* 2008; 26(8): 1148-53. <http://dx.doi.org/10.1016/j.imavis.2007.12.005>
- [38] Thodi DM, Rodriguez JJ. Prediction-error based reversible watermarking *International Conference on Image Processing*. 1549-52.
- [39] Chen M, Chen Z, Zeng X, Xiong Z. Reversible image watermarking based on full context prediction. *16th IEEE International Conference of Image Processing. Cairo, Egypt*. 2009; pp. 4253-6.
- [40] Chen X, Sun X, Sun H, Zhou Z, Zhang J. Reversible watermarking method based on asymmetric-histogram shifting of prediction errors. *J Syst Soft* 2013; 86(10): 2620-6. <http://dx.doi.org/10.1016/j.jss.2013.04.086>
- [41] Sachnev V, Hyoung Joong Kim, Jeho Nam, Suresh S, Yun Qing Shi. Reversible watermarking algorithm using sorting and prediction. *IEEE Trans Circ Syst Video Tech* 2009; 19(7): 989-99. <http://dx.doi.org/10.1109/TCSVT.2009.2020257>
- [42] Shi X, Xiao D. A reversible watermarking authentication scheme for wireless sensor networks. *Inf Sci* 2013; 240: 173-83. <http://dx.doi.org/10.1016/j.ins.2013.03.031>
- [43] Tseng H, Hsieh C. Prediction-based reversible data hiding. *Inf Sci* 2009; 179(14): 2460-9. <http://dx.doi.org/10.1016/j.ins.2009.03.014>
- [44] Jung K, Yoo K. Data hiding method using image interpolation. *Comp Stand Interfaces* 2009; 31(2): 465-70. <http://dx.doi.org/10.1016/j.csi.2008.06.001>
- [45] Lixin L, Zhenyong C, Ming C, Xiao Z, Zhang X. Reversible image watermarking using interpolation technique. *IEEE Trans Inf Forensics Security* 2010; 5(1): 187-93. <http://dx.doi.org/10.1109/TIFS.2009.2035975>
- [46] Abadi M A M, Danyali H, Helfroush MS. Reversible watermarking based on interpolation error histogram shifting. *5th International Symposium on Telecommunications (IST)*. Kish Island, Iran. 2010; pp. 840-5.
- [47] Naheed T, Usman I, Dar A. Lossless data hiding using optimized interpolation error expansion. *Front. Inform. Technol* 2011; pp. 281-6.

- [48] Lee C, Huang Y. An efficient image interpolation-increasing payload in reversible data hiding. *Expert Syst Appl* 2012; 39(8): 6712-9. <http://dx.doi.org/10.1016/j.eswa.2011.12.019>
- [49] Hu J, Li T. Reversible steganography using extended image interpolation technique. *Comput Electr Eng* 2015; 46: 447-55. <http://dx.doi.org/10.1016/j.compeleceng.2015.04.014>
- [50] Tang M, Hu J, Song W. A high capacity image steganography using multi-layer embedding. *Optik (Stuttg)* 2014; 125(15): 3972-6. <http://dx.doi.org/10.1016/j.ijleo.2014.01.149>
- [51] Hirak KM, Santi PM. Joint robust and reversible watermarking for medical images. 2nd International Conference on Communication, Computing Security [ICCCS-2012], Elsevier, Procedia Technology. 6: 275-82.
- [52] Naheed T, Usman I, Khan T, Dar A, Shafique M. Intelligent reversible watermarking technique in medical images using GA and PSO. *Optik (Stuttg)* 2014; 125(11): 2515-25. <http://dx.doi.org/10.1016/j.ijleo.2013.10.124>
- [53] Ou B, Zhao Y, Ni R. Reversible watermarking using optional prediction error histogram modification. *Neurocomputing* 2012; 93: 67-76. <http://dx.doi.org/10.1016/j.neucom.2012.04.021>
- [54] Wang X, Chang C, Nguyen T, Li M. Reversible data hiding for high quality images exploiting interpolation and direction order mechanism. *Digit Signal Process* 2013; 23(2): 569-77. <http://dx.doi.org/10.1016/j.dsp.2012.06.015>
- [55] Menon VG, Joe Prathap PM. comparative analysis of opportunistic routing protocols for underwater acoustic sensor networks. Proceedings of the IEEE International Conference on Emerging Technological Trends. Kerala, India. 2016. <http://dx.doi.org/10.1109/ICETT.2016.7873733>
- [56] Menon VG. Opportunistic routing protocols in underwater acoustic sensor networks: Issues, challenges, and future directions magnetic communications: From theory to practice. CRC Press 2018; pp. 127-48.
- [57] Menon V G. Survey on latest energy based routing protocols for under-water wireless sensor networks. *Sensors* 2016; 6(6): 52-5.
- [58] Keerthi KS. Bandana Mahapatra and Menon V G. Into the world of underwater swarm robotics: Architecture, communication, applications and challenges. *Recent Pat Comp Sci* 2019; 12: 1.
- [59] Menon VG, Joe Prathap PM. Analyzing the behavior and performance of opportunistic routing protocols in highly mobile wireless ad hoc networks. *IACSIT Int J Eng Technol* 2016; 8(5): 1916-24. <http://dx.doi.org/10.21817/ijet/2016/v8i5/160805409>
- [60] Bouslimi D, Coatrieux G, Cozic M, Roux C. Combination of watermarking and joint watermarking-decryption for reliability control and traceability of medical images. Annual International Conference of the IEEE Engineering in Medicine and Biology Society 2014; 4495-8.
- [61] Ma K, Zhang W, Zhao X, Yu N, Li F. Reversible data hiding in encrypted images by reserving room before encryption. *IEEE Trans Inf Forensics Security* 2013; 8(3): 553-62. <http://dx.doi.org/10.1109/TIFS.2013.2248725>
- [62] Koushik P, Subhajt K, Goutam G, Mahua B. A new combined crypto-watermarking technique using RSA algorithm and discrete cosine transform to retrieve embedded EPR from noisy bio-medical images. IEEE 1st International Conference on Condition Assessment Techniques in Electrical Systems (CATCON). 368-73.
- [63] Lakrissi Y, Mohammed E, Fakir M. A joint encryption/watermarking algorithm for secure image transfer. *Int J Comp Net Commun IJCNAC* 2013; p. 1.
- [64] Zhang X. Separable reversible data hiding in encrypted image. *IEEE Trans Inf Forensics Security* 2012; 7(2): 826-32. <http://dx.doi.org/10.1109/TIFS.2011.2176120>
- [65] Subeesh V, Sudhish NG, Deepthi P. An integrity verification system for image using hashing and watermarking. International Conference on Image Processing, Applications and Systems 2020; 85-9.
- [66] Bouslimi D, Coatrieux G, Cozic M, Roux C. A joint encryption/watermarking system for verifying the reliability of medical images. *IEEE Trans Inf Technol Biomed* 2012; 16(5): 891-9. <http://dx.doi.org/10.1109/TITB.2012.2207730> PMID: 22801525
- [67] Rao N, Kumari V. Watermarking in medical imaging for security and authentication. *Inf Sec J: Glo Percep* 2011; 20(3): 148-55. <http://dx.doi.org/10.1080/19393555.2011.561154>
- [68] Cheddad A, Condell J, Curran K, Mc Kevitt P. Digital image steganography: Survey and analysis of current methods. *Signal Processing* 2010; 90(3): 727-52. <http://dx.doi.org/10.1016/j.sigpro.2009.08.010>
- [69] Coatrieux G, Le Guillou C, Cauvin JM, Roux C. Reversible watermarking for knowledge digest embedding and reliability control in medical images. *IEEE Trans Inf Technol Biomed* 2009; 13(2): 158-65. <http://dx.doi.org/10.1109/TITB.2008.2007199> PMID: 19272858
- [70] Basri H. Efficient routing for dense UWSNs with high-speed mobile nodes using spherical divisions. *J Super Comp* 2018; 74: 696-716. <http://dx.doi.org/10.1007/s11227-017-2148-x>
- [71] Basri H. Distributed random cooperation for VBF-based routing in high-speed dense underwater acoustic sensor networks. *J Super Comp* 2018; 74: 6184-200. <http://dx.doi.org/10.1007/s11227-018-2532-1>
- [72] Basri H. Energy efficient spherical divisions for vbf-based routing in dense UWSNs. The International Conference on Knowledge-Based Engineering and Innovations 2015; pp. 961-5.
- [73] Tavallali P, Yazdi M, Khosravi MR. Robust cascaded skin detector based on Ada- Boost. *Multimedia Tools App* 2018; 78: 2599-2620. <http://dx.doi.org/10.1007/s11042-018-6385-7>
- [74] Basri H. A novel fake color scheme based on depth protection for MR passive/optical sensors. The International Conference on Knowledge-Based Engineering and Innovations. 362-7.
- [75] Samadi S. Determining the optimal range of angle tracking radars. *IEEE International Conference on Power, Control, Signals and Instrumentation Engineering*. 3132-5.
- [76] Yazdi M. A lossless data hiding scheme for medical images using a hybrid solution based on IBRW error histogram computation and quartered interpolation with greedy weights. *Neural Comp Appl* 2018; 30(7): 2017-28. <http://dx.doi.org/10.1007/s00521-018-3489-y>
- [77] Sharif-Yazdi M. MRF-based multispectral image fusion using an adaptive approach based on edge-guided interpolation. *J Geogr Inf Syst* 2017; 09(02): 114-25. <http://dx.doi.org/10.4236/jgis.2017.92008>
- [78] Rostami H. enhancing the binary watermark-based data hiding scheme using an interpolation-based approach for optical remote sensing images. *Int J Agric Environ Inf Syst* 2018; 9(2): 53-71. <http://dx.doi.org/10.4018/IJAEIS.2018040104>
- [79] Manikandan V, Masilamani V. Reversible data hiding scheme during encryption using machine learning. *Procedia Comp Sci* 2018; 133: 348-56. <http://dx.doi.org/10.1016/j.procs.2018.07.043>
- [80] Sachnev V, Hyoung Joong Kim, Jeho Nam, Suresh S, Yun Qing Shi. Reversible watermarking algorithm using sorting and prediction. *IEEE Trans Circ Syst Video Tech* 2009; 19(7): 989-99. <http://dx.doi.org/10.1109/TCSVT.2009.2020257>
- [81] Haouzia A, Noumeir R. Methods for image authentication: A survey. *Multimedia Tools Appl* 2007; 39(1): 1-46. <http://dx.doi.org/10.1007/s11042-007-0154-3>
- [82] Puech W. A reversible data hiding method for encrypted images, electronic imaging. *International Society for Optics and Photonics* 2008; pp. 68191E-E.
- [83] Loan NA, Parah SA, Sheikh JA, Akhoon JA, Bhat GM. Hiding Electronic Patient Record (EPR) in medical images: A high capacity and computationally efficient technique for e-healthcare applications. *J Biomed Inform* 2017; 73: 125-36. <http://dx.doi.org/10.1016/j.jbi.2017.08.002> PMID: 28782602
- [84] Akbarzadeh O. An introduction to envi tools for Synthetic Aperture Radar (sar) image despeckling and quantitative comparison of denoising filters. *IEEE International Conference on Power, Control, Signals and Instrumentation Engineering*. 2012-15.
- [85] Alhihi M. Determining the optimum number of paths for realization of multi-path routing in MPLS-TE networks. *TELKOMNIKA* 2017; 15: 1701-9. <http://dx.doi.org/10.12928/telkomnika.v15i4.6597>

Comparison of Classifier Strength for Detection of Retinal Hemorrhages

Sreeja K.A., S.S. Kumar

Abstract: Diabetes Mellitus(DM) which is the root cause of diabetic retinopathy(DR) diseases such as occlusion, microaneurysms, retinal hemorrhage, etc. Hemorrhage is considered the most dangerous among these, as it can accelerate the occurrence of vision loss. Hence, the severity of hemorrhages is analyzed in most of the recent studies of diabetic retinopathy detection. This paper focusses on the best classification approach by comparing different machine learning approach using supervised classifiers. Fundus image collected from publically available database are preprocessed and enhanced. Using splat based method, ground truth is established with the help of a retinal expert. Supervised classifiers are trained from the GLCM features extracted from the segmented images and validated on clinical images. The experimental results were verified by the Area Under Curve(AUC) for the three classifiers that were trained and results are verified and tabulated.

I. INTRODUCTION

DR detection is usually done from the analysis of fundus images. The fundus image of a person with the retinal hemorrhage compared with a normal retina is shown in Fig. 1. Image segmentation is the technique used to extract the features and analyze retinal images. This method is non-invasive and cost effective and that is the reason we chose Image based method for our analysis.

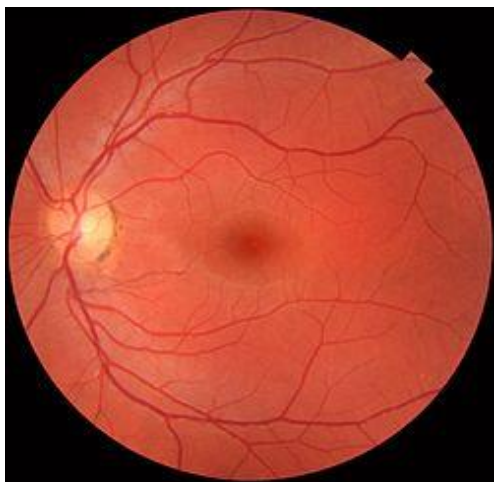


Figure 1 a

Figure 1 a. Fundus Image of a Normal Retina.



Figure 1 b

Figure 1 b. DR Fundus image with Hemorrhages.

II. LITERATURE REVIEW

Recent developments in DR studies suggest an increase in the number of diabetic patients as well as new methods to detect the retinopathy symptoms like retinal hemorrhage. A systematic review has been described using PRISMA guidelines in [1] based on meta-analysis. In order to discern between DR and glaucoma Rommel et. al [2] proposed a work using statistical texture analysis for retinal disease screening. The implementation of a digital tool that facilitates ophthalmologist to what extent the DR has affected is proposed in [3]. The implementation is based on Gabor transform and uses digital filters for a quality retinography tool. Detection of all the DR symptoms such as Microaneurysms, exudates, hemorrhages, etc. has been reviewed in [4]. Alongside several blood vessel detection technique for retinal fundus images have been described in [4]. Recent studies on Diabetic Neuropathy is presented by R. B. Kakkeri. et. al. [5] where the phenomenon called neovascularization is explained. Machine learning algorithm based retinopathy diagnosis in [6] predicts the presence of diabetic retinopathy using alternating decision tree, adaBoost, Naive Bayes, Random Forest and SVM classifiers. Exudate detection using artificial neural network algorithm was presented in [7].

III. FUNDUS IMAGE SEGMENTATION

Image segmentation techniques, as already said is the effective method to extract features from a retinal fundus image. There are several image segmentation techniques

Revised Manuscript Received on April 12, 2019.

Sreeja K.A., Asst. Professor, Dept. Of Electronics and Communication Engg., SCMS School of Engineering & Technology, Karukutty, Ernakulam, Kerala, India. (ka.sreeja@gmail.com)

S.S. Kumar, Associate Professor, Dept. of Electronics and Instrumentation Engg., Noorul Islam University, Kanyakumari, Tamil Nadu, India.

available over literature which



Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

can be utilized to segment the required region in an image. All segmentation methods share some of the common stages, such as pre-processing, processing and post-processing stages. Retinal segmentation techniques are broadly classified into two [8] as rule based methods and machine based methods. In this paper, machine based methods are preferred that utilizes ground truth and has a labelled dataset to train the classifiers. An irregular segmentation technique employing a high level entity called splat is the method[9] utilized here. Pixels that share the same structural and spatial properties are partitioned into a non-overlapping entity known as splat. Since, Hemorrhages contain blood, those hemorrhage pixels have similar properties such as color, intensity, spatial locations etc. These pixels are delineated from the whole image to form hemorrhage splats. Before segmentation of the fundus image to generate splats, the blood vessels are to be removed so that the they should not be misinterpreted as hemorrhages since both have similar structural properties.

III a. Blood vessels removal

Inorder to make the splat based method more effective, the blood vessels are removed using a **Kirsch compass kernel**. [10]The Kirsch’s operator takes a single kernel mask and turns it in 45° increments over all 8 compass courses such as: N, NW, W, SW, S, SE, E, and NE. The maximum magnitude across all directions is the value of edge magnitude of the Kirsch operator. It is calculated as

$$h_{n,m} = \max_{z=1,\dots,8} \sum_{i=-1}^1 \sum_{j=-1}^1 g_{i,j}^{(z)} \cdot f_{n+i,m+j} \quad (1)$$

Where g^z is the 8 different compass direction kernels.

III b. Splat Generation

Using edge detection, the vessels are delineated and the image is segmented to generate splats. Meaningful splats, are created by a scale specific over segmentation which is done in two steps. Initially, gradient scale of contrast enhanced bright-dark opponent image is taken using diverse gradations(scales), as the appearance of hemorrhages varies in different locations. The values of the scales are grouped and the highest of the gradient value with its scale of interest(SOI) is taken to accomplish watershed segmentation. [11]

The gradient magnitude is computed using the equation

$$|\nabla I(x, y; s)| = \sqrt{I_x(x, y; s)^2 + I_y(x, y; s)^2} \quad (2)$$

where $I(x, y; s)$ is the image. Now creating a scale-space depiction of the image using Gaussian kernels G_s , the gradient magnitude is computed from its derivatives –the horizontal and vertical ones as:

$$|\nabla I(x, y; s)| = \sqrt{\left[\frac{\partial}{\partial x} (G_s * I(x, y)) \right]^2 + \left[\frac{\partial}{\partial y} (G_s * I(x, y)) \right]^2} \quad (3)$$

$$|\nabla I(x, y; s)| = \sqrt{\left[\frac{\partial G_s}{\partial x} * I(x, y) \right]^2 + \left[\frac{\partial G_s}{\partial y} * I(x, y) \right]^2} \quad (4)$$

where the symbol * signify convolution and $\frac{\partial G_s}{\partial x}$ and $\frac{\partial G_s}{\partial y}$ are the 1° derivatives of Gaussian in the x axis and y axis direction using the scale s

The highest of the gradient magnitude is

$$|\nabla I(x, y)| = \max_i |\nabla I(x, y; s_i)| \quad (5)$$

While the field surface in watershed algorithm is essential [11] to attain meaningful splats, the greatest of the gradient magnitude is taken for a definite scale of Interest (SOI). The splats are generated based on Algorithm 1.

Algorithm 1. Splat Generation

```

1: function SPLAT_GEN(gradientoutputimage)
2:   nSeg ← Number of segments required
3:   thresGrad ← Gradient threshold
4:   top:
5:   finSeg ← Number of segments generated after
6:   watershed segmentation
7:   if nSeg > finSeg then
8:     thresGrad ← thresGrad+1
9:     loop:
10:    if imageGrad(a)(b) > thresGrad then
11:      newimageGrad(a)(b) ← imageGrad(a)(b)
12:      p=a+1
13:      q=b+1
14:      goto loop.
15:    imageGrad = newimageGrad
16:    goto top.
return finalimage ← watershed(imageGrad)

```

Thus the image can be portioned as non-overlapping splats having similar intensity over the entire image[9]. Some of the Splats formed by means of diverse scales exploiting the same watershed algorithm is shown in the figure 2.

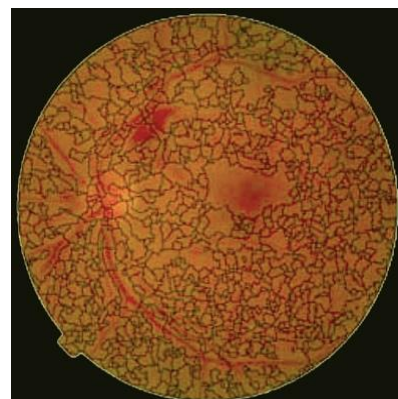


Figure 2a



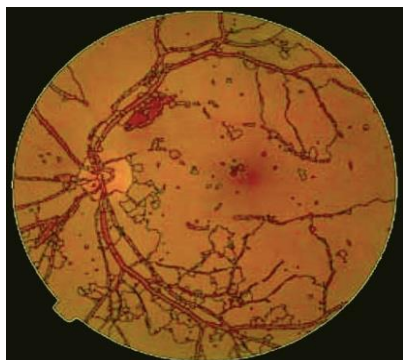


Figure 2b

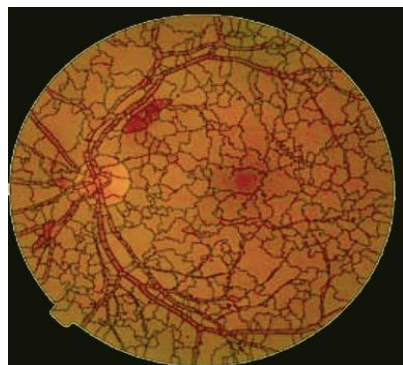


Figure 2c

Fig. 2a has smaller splats which are generated with scales outside the desired SOI for hemorrhage splats. The range of scales used in Fig. 2a can be used for optic disc removal and blood vessel detection. Fig. 2b uses a fine scale and also less than the desired SOI. These range of scales can be used in the detection of Microaneurysms and exudates. Figure 2c is the required scale for hemorrhages detection as the retinal background is represented by larger splats and blood regions are represented as smaller splats.

The total number of splats generated is kept under a threshold without compromising the accuracy and speed of computation.

IV. GOLD STANDARD LABELLING BY OPHTHALMOLOGIST

The splats obtained by segmentation are labelled with the help of an ophthalmologist in order to train the supervised classifiers for the clinical images. For the DIARETDB1 database, ground truth's confidence level is kept as 0.75 based on the evaluation done in [12]. This level is the certainty of the decision that a splat is accurate.

Feature Extraction and Feature Subset Selection:

The classifiers can be trained to detect the target objects after assigning reference labels for splats. An overall 352 possibly relevant features are taken from each splats to train the classifiers.

They are:

1) Color: Colors of each splat is obtained in RGB color space and dark-bright (db), red-green (rg), and blue-yellow (by) opponency images [13], which derives to six colour components.

2) Difference Of Gaussian (DoG Filter): Difference of Gaussian (DoG) kernels are employed at five distinct

smoothing scales with one baseline scale to take advantage of Gaussian scale space. [14][15]

3) Responses from Gaussian Filter Bank[13]: A Gaussian filter bank which include a first order derivative and a second order derivative with at two orientations and three orientations respectively are applied to the green channel.

4) Responses from Schmid Filter Bank: 13 kernels of Schmid filter banks which are rotationally invariant is applied to the dark bright opponency image.

5) Responses from Local Texture Filter Banks: Local texture filter bank contains local entropy filter, local range filter and local standard deviation filter which calculate the entropy, standard deviation and intensity range of a single pixel in a given region [16].

The above features are combined to obtain a meaningful response image that has small inter splat similarity and large intra splat similarity[13] [15] [16] [17]. These features mentioned above are called pixel- based responses. Alongside these features, we take splat wise features according to Gray-Level Co-occurrence Matrix (GLCM)[16] [18] [19] [20] statistics. These are splat area, extent, texture, solidity and orientations. After sequential forward feature selection subset(SFS) insignificant and redundant ones were removed from the feature set and only the relevant features were considered. The 19 features considered for training the classifiers are shown in Table I

TABLE I

Features	Number	Description
DoG filter bank	s2 - s0.5	from Green channel
DoG filter bank	s4 - s0.5	from db and rg opponency
DoG filter bank	s8 - s 0.5	from db opponency
Gaussian Filter Bank	s=8 orientation:2,3	Mean of second order Gaussian derivative from green channel
Gaussian Filter Bank	s=1,2,4 orientation:1,2,3	Mean of second order Gaussian derivative from green channel
Schmid filter bank	response=11 s=8,16	Mean of second order Gaussian derivative from green channel
Mean of Gaussian		from db opponency from Green channel

V. CLASSIFICATION USING DIFFERENT CLASSIFIERS

In order to do the classification, several machine learning algorithms are available over literature. Among them, three classifiers are used to train our experiment and evaluate the result. They are: Neural Network Classifier, Naïve Bayes Classifier and kNN Classifier.

A. Neural Network classifier:

Artificial neurons or nodes which are biliogically inspired from the functionality of



human brain forms the key part of a neural network. Individually nodes have their own scope of intelligence concerning rules and functionalities to improve it-self through knowledges learned from previous methods which is called backpropagation. Neural networks are suitable to identify non-linear patterns, where there isn't a one-to-one relationship between the input and output[21]. The neural network consists of input layers, hidden layers and a threshold function. All the nodes are interconnected to form a network.

Neural networks are characterized by holding adaptive weights along paths between neurons that can be adjusted by a backpropagation algorithm that learns from perceived data in order to improve the learning model. The inputs to the neural network classifier are the relevant feature set and they are transformed using the desired weights from the hidden layer. Finally, using a sigmoid transfer function the output class is determined.

B. Naïve Bayes Classifier:

The naive Bayes classifier [22] uses the principle of Bayesian maximum a posteriori (MAP) classification: measure a finite set of features $x = (x_1, \dots, x_n)$ then select the class

$$\hat{y} = \underset{y}{\operatorname{arg\,max}} P(y|x) \tag{6}$$

where

$$P(y|x) \propto P(x|y)P(y)$$

$P(y|x)$ is the likelihood of feature vector x given class y , and $P(y)$ is the priori probability of class y . Naive Bayes classifier assumes that the features are independent of the condition. For the class:

$$P(y|x) = \prod_i P(x_i|y) \tag{7}$$

The parameters $P(x_i|y)$ and $P(y)$ are obtained from the training data.

C. kNN Classification

The kNN algorithm allocates soft class labels. The two output classes defined are hemorrhage splat or non-hemorrhage splat. Euclidean distance is the measure by which the classifier decides whether a particular splat belongs to hemorrhage or normal class in an optimized feature space. As the value of k is increased the computation time increases and the splats are more accurately identified. But since all the k nearest neighbors are not near, an optimum value of k is chosen instead of an arbitrary value.

VI. EXPERIMENT AND RESULTS

A. Data acquisition and Pre-processing

The fundus images were acquired from two sources. Clinical images were obtained from Dr. Bhejan Singh's eye hospital. The clinical image was captured using a "Remidio Non-Mydriatic Fundus On Phone (FOP-NM10)"

[23] Camera with FOV 40°, working distance of 33mm and an ISO range from ISO 100 to 400. The images used for training was acquired from the publically available database DIARETDB1

(<http://www.it.lut.fi/project/imageret/diaretdb1/index.html>).

An overall 1500 images were taken among which 1050 images were taken for training, 225 images for testing and 225 for validation. The gold standard reference observations were accomplished by an ophthalmologist expert using the splat-based interpretation. Overall 1200 (950 from training set 150 from testing) images were marked by the expert from a total of 1500. Preprocessing is done in order to adapt the color variation throughout the dataset and also to equalize the intensity of the image. Histogram equalization is done using Contrast limited Adaptive Histogram Equalization(CLAHE)[24]. Also Each image is normalized according to its prevailing pixel value at the three colour channels. The pixel values that occur frequently are shifted to the beginning of RGB colour space.

B. Classification and result

From the 1050 training images. 10100 splats were formed. In this there were approximately 300 hemorrhage splats. This amounts to a very low hemorrhage splat density. So images having at least 6 splats are taken for training, where the value 6 is arbitrarily chosen. After sequential forward feature selection subset(SFS) 19 unique features were considered and the insignificant and redundant features were omitted from the feature set. The set of features are already shown in Table I.

For the neural network classifier, the network protocols used for detection are as shown in table II.

TABLE II

Features	Hemorrhage splats
Learning rule base	Delta rule
Transfer function	Sigmoid
Hidden Layer Elements	30
Preprocessing filter	Feature set
Number of training iterations	1000
Training algorithm	Bayesian
Neural network	Fitting network
Training time- Core i5, 4.10 GHz	10 min
Number of training splats	7350
Number of testing splats	3150

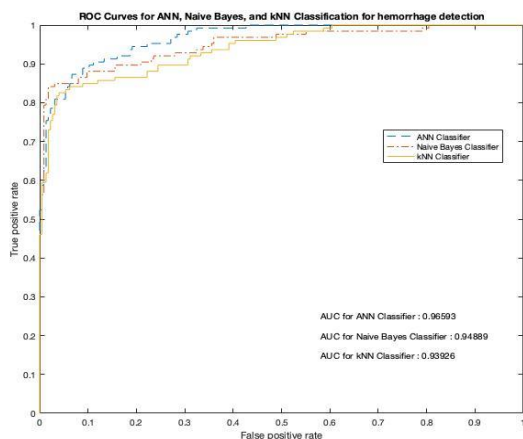
For the kNN Classifier, the value of k was chosen between 15 to 160 that involves both feature selection as well classification. After repeated calculations, the value of k was fixed at 105 without compromising and prediction accuracy and computation period. For the Naïve Bayes classification in addition to the above features, six Difference of Gaussian (DoG) filter responses were taken. The DoG filter deducts one distorted version of an original image from another distorted version of the image [25]. The convolution was done with seven different Gaussian kernels with SD of 0.75, 1.5, 3, 6, 12, 24, and 48. We used DoG1,



DoG2, DoG3, DoG4, DoG5 and DoG6 to state the features attained by subtracting the image at scale $\sigma = 0.75$ from $\sigma = 1.5$, scale $\sigma = 1.5$ from $\sigma = 3$, scale $\sigma = 3$ from $\sigma = 6$, scale $\sigma = 6$ from $\sigma = 12$, scale $\sigma = 12$ from $\sigma = 24$, and scale $\sigma = 24$ from $\sigma = 48$, respectively.

The results were obtained for the fundus image shown in Fig 2. The Area Under Curve(AUC) for the Receiver Operator Characteristics (ROC) curve is shown in Fig. III

Figure III



The Obtained accuracy, sensitivity and specificity for the three different classifiers are tabulated in Table III. From this the maximum AUC is attained for the Neural Network Classifier of AUC= 0.96 followed by the Naïve Bayes classifier of AUC = 0.94 and finally the kNN Classifier with AUC= 0.93.

TABLE III

Classifier	Sensitivity	Specificity	AUC for test data
ANN	87.651	87.145	0.96
Naïve Bayes	84.476	83.791	0.94
kNN	80.872	82.137	0.93

VII. CONCLUSION

From the above test results, it is clear that a promising sensitivity and specificity is provided by the neural network classifier. From literature it is understood that, a more sensitive result can be acquired using an advanced Convolutional neural network classifier(CNN). A new algorithm using CNN network is the future scope of this work.

REFERENCES

1. R. Cheloni, S. A. Gandolfi, C. Signorelli, and A. Odone, "Global prevalence of diabetic retinopathy: protocol for a systematic review and meta-analysis.," *BMJ Open*, vol. 9, no. 3, p. e022188, Mar. 2019.
2. R. M. Anacan *et al.*, "Retinal Disease Screening through Statistical Texture Analysis and Local Binary Patterns using Machine Vision," in *2018 IEEE 10th International Conference on Humanoid, Nanotechnology, Information*

3. Y. Morales, R. Nuñez, J. Suarez, and C. Torres, "Digital tool for detecting diabetic retinopathy in retinography image using gabor transform," in *Journal of Physics: Conference Series*, 2017.
4. J. Amin, M. Sharif, and M. Yasmin, "A Review on Recent Developments for Detection of Diabetic Retinopathy," *Scientifica (Cairo)*, vol. 2016, pp. 1–20, Sep. 2016.
5. V. D. R. B. Kakkeri, Sayali Surve, Shahrulkh Shaikh, "Detection of Diabetic Retinopathy," *Int. J. Innov. Technol. Explor. Eng(IJITEE)*, vol. 5, no. 12, 2016.
6. K. Bhatia, S. Arora, and R. Tomar, "Diagnosis of diabetic retinopathy using machine learning classification algorithm," in *2016 2nd International Conference on Next Generation Computing Technologies (NGCT)*, 2016, pp. 347–351.
7. S. W. Franklin and S. E. Rajan, "Diagnosis of diabetic retinopathy by employing image processing technique to detect exudates in retinal images," *IET Image Process.*, vol. 8, no. 10, pp. 601–609, Oct. 2014.
8. J. Almotiri, K. Elleithy, and A. Elleithy, "Retinal Vessels Segmentation Techniques and Algorithms: A Survey," *Appl. Sci.*, 2018.
9. L. Tang, M. Niemeijer, J. M. Reinhardt, S. Member, M. K. Garvin, and M. D. Abramoff, "Splat Feature Classification With Application to Retinal Hemorrhage Detection in Fundus Images," vol. 32, no. 2, pp. 364–375, 2013.
10. R. A. Kirsch, "Computer determination of the constituent structure of biological images," *Comput. Biomed. Res.*, 1971.
11. Yung-Chieh Lin, Yu-Pao Tsai, Yi-Ping Hung, and Zen-Chung Shih, "Comparison between immersion-based and toboggan-based watershed image segmentation," *IEEE Trans. Image Process.*, vol. 15, no. 3, pp. 632–640, Mar. 2006.
12. T. Kauppi *et al.*, "the DIARETDB1 diabetic retinopathy database and evaluation protocol," in *Proceedings of the British Machine Vision Conference 2007*, 2007.
13. M. D. Abramoff *et al.*, "Automated Segmentation of the Optic Disc from Stereo Color Photographs Using Physiologically Plausible Features," *Investig. Ophthalmology Vis. Sci.*, vol. 48, no. 4, p. 1665, Apr. 2007.
14. B. M. ter Haar Romeny, *Front-end vision and multi-scale image analysis: multi-scale computer vision theory and applications*, written in Mathematica. Kluwer Academic, 2003.
15. L. Tang, M. Niemeijer, and M. D. Abramoff, "Splat feature classification: Detection of the presence of large retinal hemorrhages," in *2011 IEEE International Symposium on Biomedical Imaging: From Nano to Macro*, 2011, pp. 681–684.
16. O. Engler, *Introduction to Texture Analysis: Macrotecture, Microtexture, and Orientation Mapping*, Second Edition. CRC Press LLC, 2017.
17. M. Varma and A. Zisserman, "A Statistical Approach to Texture Classification from Single Images," *Int. J. Comput. Vis.*, vol. 62, no. 1/2, pp. 61–81, Apr. 2005.
18. H. Tamura, S. Mori, and T. Yamawaki, "Textural Features Corresponding to Visual Perception," *IEEE Trans. Syst. Man. Cybern.*, vol. 8, no. 6, pp. 460–473, 1978.
19. M. Niemeijer, J. Staal, B. van Ginneken, M. Loog, and M. D. Abramoff, "Comparative study of retinal vessel segmentation methods on a new publicly available database," 2004, vol. 5370, p. 648.
20. M. Niemeijer, M. D. Abramoff, and B. van Ginneken, "Segmentation of the Optic Disc, Macula and Vascular Arch in Fundus Photographs," *IEEE Trans. Med. Imaging*, vol. 26, no. 1, pp. 116–127, Jan. 2007.
21. G. G. Gardner, D. Keating, T. H. Williamson, and A. T.



- Elliott, "Automatic detection of diabetic retinopathy using an artificial neural network: A screening tool," *Br. J. Ophthalmol.*, 1996.
22. J. J. Cochran, L. A. Cox, P. Keskinocak, J. P. Kharoufeh, J. C. Smith, and M. Goldszmidt, "Bayesian Network Classifiers," in *Wiley Encyclopedia of Operations Research and Management Science*, 2011.
 23. "Remidio Non-Mydriatic Fundus On Phone (FOP-NM10)."
 24. Kee Yong Pang, I. Lila Iznita, M. H. Ahmad Fadzil, A. N. Hanung, N. Hermawan, and S. A. Vijanth, "Segmentation of retinal vasculature in colour fundus images," in *2009 Innovative Technologies in Intelligent Systems and Industrial Applications*, 2009, pp. 398–401.
 25. M. W. D. Kenneth R. Spring, John C. Russ, Matthew J. Parry-Hill, Thomas J. Fellers, "Molecular Expressions Microscopy Primer: Digital Image Processing - Difference of Gaussians Edge Enhancement Algorithm - Interactive Tutorial." [Online]. Available: <https://micro.magnet.fsu.edu/primer/java/digitalimaging/processing/diffgaussians/index.html>. [Accessed: 06-May-2019].

Article

A Secure and Efficient Lightweight Symmetric Encryption Scheme for Transfer of Text Files between Embedded IoT Devices

Sreeja Rajesh ¹, Varghese Paul ², Varun G. Menon ^{3,*} and Mohammad R. Khosravi ⁴ 

¹ Department of Computer Science, Bharathiar University, Coimbatore 641046, Tamil Nadu, India; m.sreeja79@gmail.com

² Department of Information Technology, Cochin University of Science and Technology, Ernakulam 682022, Kerala, India; vp.itcusat@gmail.com

³ Department of Computer Science and Engineering, SCMS School of Engineering and Technology, Ernakulam 683582, Kerala, India

⁴ Department of Electrical and Electronic Engineering, Shiraz University of Technology, Shiraz 71555-313, Iran; m.khosravi@sutech.ac.ir

* Correspondence: varunmenon@scmsgroup.org; Tel.: +918714504684

Received: 29 January 2019; Accepted: 20 February 2019; Published: 24 February 2019



Abstract: Recent advancements in wireless technology have created an exponential rise in the number of connected devices leading to the internet of things (IoT) revolution. Large amounts of data are captured, processed and transmitted through the network by these embedded devices. Security of the transmitted data is a major area of concern in IoT networks. Numerous encryption algorithms have been proposed in these years to ensure security of transmitted data through the IoT network. Tiny encryption algorithm (TEA) is the most attractive among all, with its lower memory utilization and ease of implementation on both hardware and software scales. But one of the major issues of TEA and its numerous developed versions is the usage of the same key through all rounds of encryption, which yields a reduced security evident from the avalanche effect of the algorithm. Also, the encryption and decryption time for text is high, leading to lower efficiency in IoT networks with embedded devices. This paper proposes a novel tiny symmetric encryption algorithm (NTSA) which provides enhanced security for the transfer of text files through the IoT network by introducing additional key confusions dynamically for each round of encryption. Experiments are carried out to analyze the avalanche effect, encryption and decryption time of NTSA in an IoT network including embedded devices. The results show that the proposed NTSA algorithm is much more secure and efficient compared to state-of-the-art existing encryption algorithms.

Keywords: avalanche effect; efficiency; encryption time; key confusions; NTSA; symmetric encryption; tiny encryption algorithm

1. Introduction

Internets of things (IoT) includes millions of connected devices that can sense, compute and communicate data [1–6]. Every second, large amounts of data are transferred among these devices. Considering the sensitivity of applications in the IoT network, such as connected vehicles or wearable health devices, security of transmitted information has remained a major area of concern [7–9]. The increasing number of intruders and hackers has made this task very challenging. Over the years, numerous cryptographic algorithms have been used to ensure the security of transmitted data. The strength of the cryptographic algorithms depended on the techniques used for managing, establishing and distributing the secret keys. Secret keys that are poorly maintained make the

cryptographic algorithm useless, even if the algorithm is theoretically and also, practically ideal [10,11]. Cryptographic algorithms proposed for IoT networks can be classified into the symmetric and asymmetric algorithms. Symmetric algorithms use the same key for both encryption and decryption. The strength of the symmetric algorithms truly depends on how the key is securely exchanged between the sender and receiver. Asymmetric algorithms indeed avail two different keys including the public and private keys. The private key is never transmitted through the network and hence it is secure. The public key is sent through the network to the receiver. During encryption, the sender encrypts the plaintext using the public key of the receiver and sends the resultant cipher text to the receiver using the network. Even if the public key is known to the hacker, he cannot read the scrambled (or hashed) message because secret key is not known for him. During decryption, the receiver will use his private key to decrypt the cipher text. Asymmetric algorithms are more complex to implement and utilize more resources than symmetric algorithms [12,13]. Thus, most of the modern applications in IoT networks use symmetric algorithms to provide security to the transmitted information. Further, they are easy to implement, utilize fewer resources with low overhead and are secure as long as the key is kept secret.

Symmetric algorithms are classified into block and stream ciphers. Encryption of plaintext is done bit-by-bit in case of stream cipher [14] and a group of bits (i.e., 64 bits) is taken for encryption in block cipher as a unit. The block cipher algorithm is preferred to the stream cipher for faster computations. Most of the symmetric algorithms use Feistel ciphers [15,16]. In the Feistel cipher, the encrypted plaintext is decomposed into two parts. A transformation function known as the round function is applied to one half using a sub-key and the output of the round function is XOR'ed with the other half. These two parts are then swapped with each other. This step is performed iteratively on the number of times specified in the algorithm. The Feistel cipher is an efficient method for implementing block symmetric algorithms. So, we focus on improving the security of symmetric algorithms that use the Feistel ciphers for encryption of text files.

With numerous IoT devices having different computational capabilities, one of the major requirements for an efficient security protocol in IoT networks is that it should be light weight. The processing time taken by the protocol should be minimal for less delay and better performance. Also, the security algorithm needs to be less complex with minimal overhead. Because of these reasons many protocols used with normal computer networks do not give good performance in IoT networks and are not preferred. Considering these features, tiny encryption algorithm (TEA) [17–19] is the most widely used symmetric algorithm with a Feistel cipher for secure transmission of data through the IoT network. The popularity of TEA is mainly due to the ease of implementation and less memory utilization compared to all other encryption algorithms. But one of the major issues with TEA is the usage of the same keys through all the rounds of encryption which leads to reduced security. This is undoubtedly observed from the avalanche effect of TEA. Moreover, the time taken for encryption and decryption is high, leading to reduced efficiency of TEA. Although many versions of TEA have been proposed over these years [20–23], none of them have given concrete solutions to the above problems.

This paper proposes an algorithm named NTSA (novel tiny symmetric encryption algorithm) that improves the security features of TEA by introducing more key confusions. Most of the works with TEA and its variations has focused only on decreasing the delay in delivery. Very few researches have been done on key alteration as a method to enhance the security of the transmission algorithm. In the proposed method we introduce multiple key alterations dynamically and secure the key from intruders. Since the key is computed dynamically, the key values are changed during the execution time and cannot be pre-computed. Furthermore, our proposed algorithm (NTSA) takes less time for encryption and decryption compared to TEA and thus provides both better security and efficiency for all the modern applications in IoT networks. The rest of the research is organized into four sections as follows. Section 2 discusses different existing encryption mechanisms for the secure transmission of data through IoT networks. This section further explains the implementation of the TEA algorithm in detail. Few variations of the TEA algorithm are also discussed in this section. Our proposed NTSA is

explained in the Section 3. Section 4 presents the experimental results of the NTSA algorithm and we conclude in Section 5 and express some potential future works.

2. Related Work

In here, we discuss the major encryption algorithms proposed for transmission of data in IoT networks. Specifically, we discuss the design and implementation of these algorithms and highlight their issues and drawbacks. We also discuss the design, implementation and issues with the TEA and its latest versions in detail.

One of the earliest works in this area was the RC5 symmetric key block cipher [24]. RC5 uses variable sized blocks, 32, 64, 128 bits etc. The rounds used are 0–255 with key size of 0 to 2040 bits. The case RC5 is determined suitable for wireless sensor network (WSN) applications, but the key schedule must be calculated a priori based on 104 additional bytes of RAM for each key. Also, the variable-bit rotation instruction used by RC5 is rarely supported by the embedded systems [24]. Skipjack algorithm is another block cipher algorithm developed by the US National Security Agency. Skipjack and its variants, TinySec and MiniSec, are used for transmission of data in WSNs. But the algorithm is not efficient in embedded IoT devices with multiple issues in implementation [25–27]. Standaert et al. gave the scalable encryption algorithm (SEA) [28] generated for processing units that have limited the instruction set. It provides cost-effective encryption and authentication, but does not address secure search of the substring. Hong et al. proposed the HIGHT algorithm [29] that is very useful for pervasive computing devices like devices of a wireless sensory system or network. It uses Feistel network and basic operations like addition mod 2^8 or XOR. There are 32 rounds with 128-bit key and 64-bit block size. But the noted algorithm is vulnerable to saturation attack. Usman et al. proposed SIT—a lightweight encryption algorithm [30] that provides enhanced security for data transmission between IoT devices. SIT uses a combinational form of Feistel structure and network with a uniform substitution-permutation. But the detailed study on performance evaluation and cryptanalysis for possible attacks have not been performed. Liang C et al. [31] proposed the hybrid encryption algorithm for lightweight data in cloud storage. This was an improved method on the RSA algorithm and it combined with advanced encryption standard (AES) to introduce a hybrid encryption algorithm. The proposed algorithm improves the efficiency of generating large primes. But the algorithm was mainly focused on enhancing the data confidentiality in the cloud. M-SSE proposed by Chongzhi Gao et al. [32] is different from existing searchable symmetric encryption algorithms as it provides privacy in both forward and backward directions using a technique of multi-cloud computing. But the algorithms and its variations are prone to information leakage. International data encryption algorithm (IDEA) [33] is a block symmetric algorithm that uses 64-bit plain text and a key size of 128 permuted into 52 sub-keys of 128 bits. It includes a Feistel structure and has eight rounds. The degree of diffusion and non-linearity properties of the round function decides the strength of the Feistel structure. IDEA does not use substitution and permutation boxes and is based on operations like XOR, addition and multiplication, thus reducing the memory overhead. The use of the multiplication operation provides diffusion. IDEA does not support any change in the Feistel structure and hence is not flexible. MARS [34] is another symmetric block algorithm that uses 128-bit plaintext with key size varying between 128–448 bits. It follows Feistel structure and has only one substitution box. This algorithm is faster than DES and it is susceptible to many attacks. The involvement of various components makes MARS very complex to analyze and implement in hardware. Abdelhalim et al. proposed the modified TEA algorithm (MTEA) [35], which improves the security of TEA and power consumption. The linear feedback shift register (LFSR) is used as a pseudo-random number generator to improve the security of the TEA and power utilization. The pseudo-random number generator frequently changes the MTEA key in each round. Zhdanov and Sokolov proposed an algorithm [36] based on the principles of many-valued logic and variable block length. The encryption process is performed iteratively with five rounds. The number of rounds can be varied, with round 1 consisting of gamma and permutations procedures, remaining rounds include substitution and gamma procedures.

The proposed method can process binary information after representing as a ternary vector. But there is no method developed that does this conversion directly. LEA (lightweight encryption algorithm) is a block encryption algorithm [37] that is designed to provide confidentiality in lightweight environment like mobile devices. This algorithm uses plain text of 128 bits and varying modes can be selected depending on the size of the key (128, 192, or 256 bits). Based on the modes, the number of rounds can be changed between 24, 28, and 32 bits. This algorithm does not use S-box, instead addition, rotation and XOR arithmetic operation is processed in 32-bit unit [38]. Abdullah et al. proposed a super-encryption cryptography [39] with IDEA (international data encryption algorithm) and WAKE (word auto key encryption) algorithm. The technique of super encryption combines two or more symmetric cryptographic algorithms so as to provide more security to data. Anderson et al. proposed the serpent algorithm [40] that was an AES candidate. The main aim of this algorithm is to maximize the avalanche effect within the cipher text. Serpent has substitution permutation structure that uses 128-bit plain text and accepts keys of 128, 192, or 256 bits. The 32 rounds of serpent make it a bit slower and complex to implement on small blocks. Data encryption standard (DES) is one of the widely used symmetric key block cipher that uses the Feistel structure. The plaintext of 64-bit and a key size of 56 bits are used for the encryption process that includes 16 rounds. The DES algorithm does not allow flexibility in Feistel structure and hence does not support any changes in it [41].

Tiny encryption algorithm (TEA) developed by David Wheeler and Roger Needham [42] is the most efficient for use with embedded devices in IoT networks compared to all the discussed encryption algorithms. Some of the interesting features of TEA are ease of implementation, the absence of specialized tables, good performance and short enough to integrate into any embedded device. The main focus of TEA is reduced memory usage and maximized speed. Encryption routine of TEA is shown in Figure 1 and the decryption routine is shown in Figure 2.

TEA uses Feistel structure with 64 rounds or 32 cycles where one cycle is composed of two rounds [43]. The plaintext block size is 64 bits (operate on two 32-bit unsigned integers and stored in $v[0]$ and $v[1]$). The recommended key size is 128 bits. The key is split into four 32-bit blocks, $k[0]$ to $k[3]$. The XOR and AND operations are used alternatively. Also repeated mixing of all the bits of plaintext and key is achieved by the dual shift operation. A simple key schedule is used for both encryption and decryption and the four 32-bit blocks of the key are mixed exactly the same way for each cycle. Magic constant is used to compute the key. For preventing the attacks caused by the symmetry of rounds, each cycle (one cycle constitutes of two rounds) uses different multiples of magic constants. Magic constant is 2,654,435,769 or $9E3779B9_{16}$ and would be selected as $2^{31} / \phi$ (ϕ is named the golden ratio). During the encryption process, the plaintext is partitioned into two parts Left[0] and Right[0]. Each of the parts utilizes another half part for doing the encryption process. There will be 64 rounds along with two other rounds that constitute one cycle, so there are 32 cycles. After the 64th round, both parts will be composed to create the cipher text. In each of the rounds, all the inputs include "Left[$i - 1$]" and "Right[$i - 1$]" which is derived from the previous round and sub-key K_i extracted from the 128-bit key K . The constant $\delta = 0 \times 9E3779B9$ is chosen to be $2^{31} / \phi$. This is to confirm that the sub-keys are distinct and that the accurate value of it does not have a cryptographic significance. In each round, the integer "addition" modulo of 2^{32} is applied instead of XOR. The round function F uses addition, bitwise XOR, left and right shift operation.

For the i -th cycle,

$$\text{Left}[i] = \text{Left}[i - 1] + F(\text{Right}[i - 1], \text{key}[0, 1], \text{delta}[i]),$$

$$\text{Right}[i] = \text{Right}[i - 1] + F(\text{Left}[i - 1], \text{key}[2, 3], \text{delta}[i]),$$

$$\text{Delta}[i] = \text{Floor}((i + 1)/2) * \text{delta}$$

Round function F is

$$F(M, K[a, b], \text{delta}[i]) = ((M \ll 4) \text{AND } k[a]) \text{ XOR } (M \text{ AND } \text{delta}[i]) \text{ XOR } ((M \gg 5) \text{AND } k[b]).$$

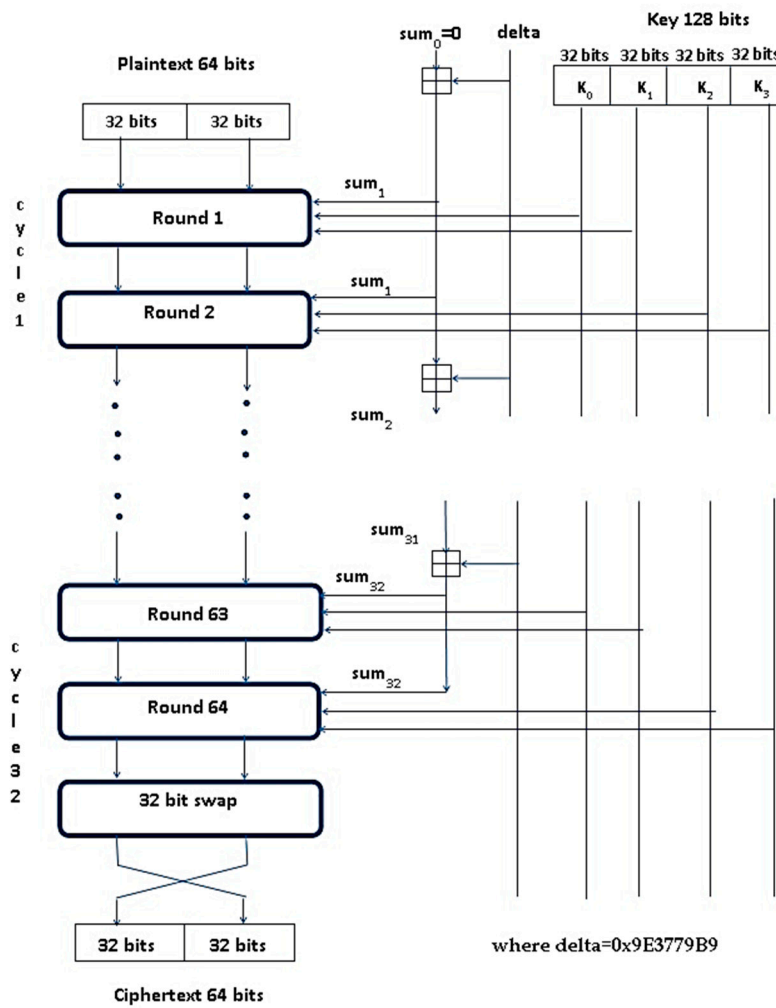


Figure 1. Encryption routine of the tiny encryption algorithm (TEA).

The 128-bit key is divided into four 32-bit blocks $K=(k[0], k[1], k[2], k[3])$ where odd rounds use keys $k[0]$ and $k[1]$ and even rounds use $k[2]$ and $k[3]$. One cycle constitutes two rounds and the i -th round is shown in Figure 3.

Many variations of the TEA algorithm have been proposed recently. Dian Rachmawati et al. proposed an algorithm [44] that uses a combined asymmetric and symmetric encryption for secure file transfer. The security of the file is taken care by the symmetric algorithm TEA and security of the key by the asymmetric algorithm LUC based on Lucas function. But the method used the same key for all rounds of encryption leading to reduced security. Novelan et al. developed an SMS security system for mobile devices using the Tiny Encryption algorithm [45]. This system ensures that the confidential messages are encrypted in the presence of a key to obtain the encrypted SMS message that is sent to the destination mobile number. Cipher text at the receiver side can be decrypted using the same key to get the SMS. The drawback with this method is that the size of the SMS decides the encryption and decryption time taken for the process. XTEA is a block symmetric encryption algorithm that uses the Feistel structure [46]. This algorithm uses 64-bit block plaintext, 128-bit key and 64 rounds of encryption. This algorithm uses a more complex key-schedule than TEA with rearrangements of the shifts, XOR's and additions [47]. XXTEA, also called block TEA uses the same round function as XTEA but applies it cyclically across an entire message for several iterations [48]. Table 1 presents a summary of all the existing security algorithms.

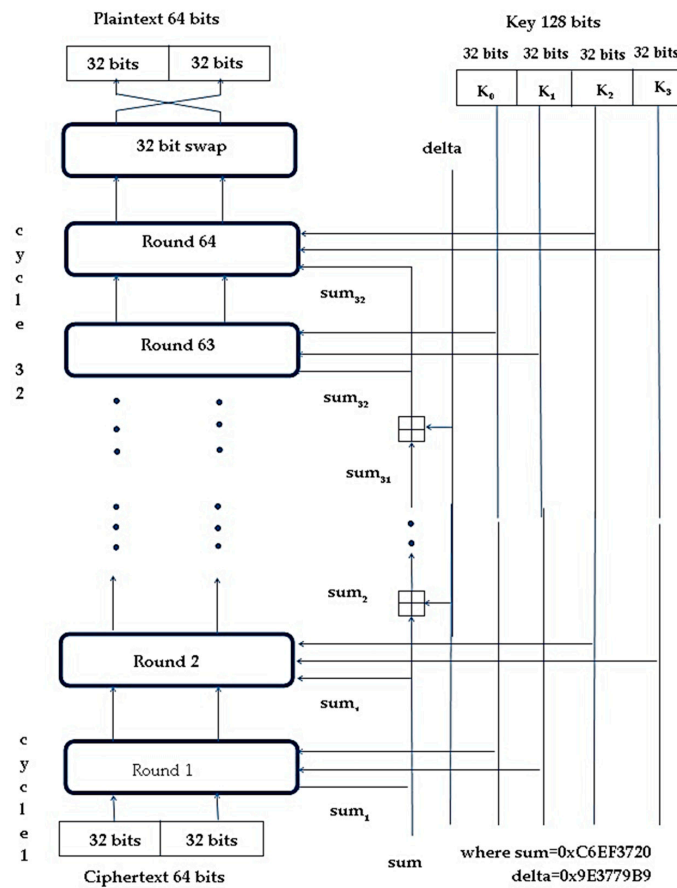


Figure 2. Decryption routine of TEA.

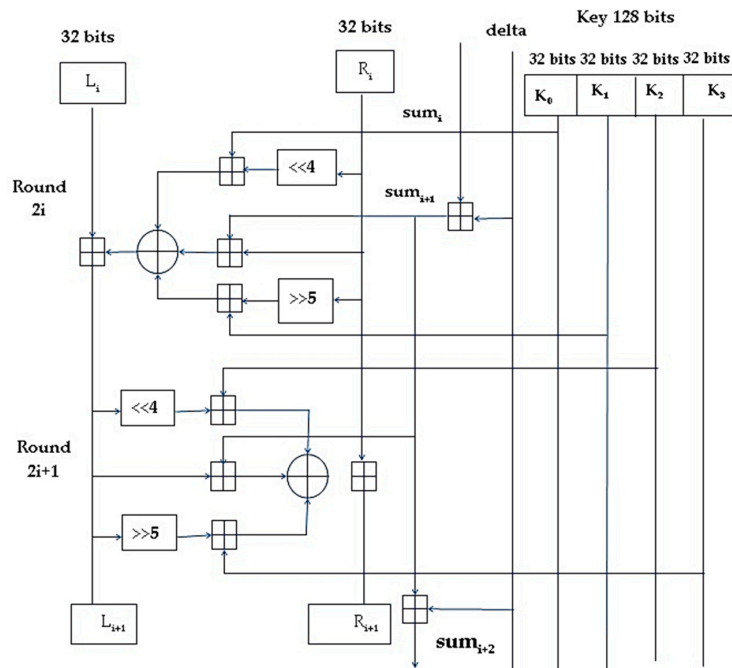


Figure 3. The i -th cycle of TEA.

Of all the discussed algorithms, TEA remains the most efficient for use in IoT networks for secure and quick transfer of text files between simple embedded devices. But one of the major issues with

TEA and its latest variations is the usage of same keys through all rounds of encryption, resulting in reduced security, which is evident from the avalanche effect of the algorithm. Also, the encryption and decryption time for text is high, leading to lower efficiency in IoT networks with embedded devices. This paper proposes a NTSA which provides enhanced security for the transfer of text files through the IoT network by introducing additional key confusions dynamically for each round of encryption.

Table 1. Summary of the symmetric encryption techniques.

Algorithm	Developer	Block/Stream Cipher	Key Size	Attack	Algorithm Structure
DES [41]	IBM	Block cipher (64 bits)	56 bits	Brute Force Attack	16 rounds Feistel Structure
3DES [49]	IBM	Block cipher (64 bits)	112 or 168 bits	chosen-plaintext attack	48 rounds Feistel Structure
IDEA [33]	Lai and James	Block cipher (64 bits)	128 bits	weak keys	8 rounds Feistel Structure
RC5 [24]	Ron Rivest	Block cipher (32,64,128 bits)	0–2040 bits	differential attack	(12 round suggested) Feistel Structure
TEA [45]	Wheeler and Needham	Block cipher (64 bits)	128 bits	equivalent key attack	Variable round Feistel Structure
XTEA [46]	Wheeler and Needham	Block cipher (64 bits)	128 bits	related key differential attack	Variable round nested Feistel Structure
XXTEA [47]	Wheeler and Needham	Block cipher (64 bits)	128 bits	chosen-plaintext attack	unbalanced Feistel Network
SKIPJACK [50]	National Security Agency (NSA)	Block cipher (64 bits)	80 bits	slide attack	32 rounds, unbalanced Feistel Structure
AES [40]	Daemen and Rijmen	Block cipher (128 bits)	128, 192, 256 bits	known plaintext	20 rounds Feistel Structure
MARS [34]	IBM	Block cipher (128 bits)	128, 192, 256 bits	meet-in-the-middle	32 rounds Feistel Structure
HIGHT [29]	Hong et al.	Block cipher (64 bits)	128 bits	Impossible Differential attack	light weight block algorithm, effective in hardware

3. Novel Tiny Symmetric Encryption Algorithm (NTSA)

The TEA algorithm and its variations use the same key in all rounds of encryption and are thus more prone to relative key attack where the attacker tries to realize some relationship between different keys used by the user. The proposed NTSA algorithm is intended to provide more confusion to the keys in each round dynamically. It uses 64-bit plaintext and key of 128 bits. There are 32 cycles and each cycle is composed of two rounds, resulting in 64 rounds. The plaintext is divided into two halves, v_0 and v_1 , with 32 bits each. The round function op is applied to each half of plaintext. The 128-bit key is divided into four 32-bit partial keys k_1 , k_2 , k_3 , and k_4 . Partial keys k_1 and k_3 are applied to the odd numbered round and partial keys k_2 and k_4 are applied to even numbered round. Compute key schedule constant $ksc = \text{floor}(2^{31}/\phi)$ where ϕ is the golden ratio. The golden ratio ϕ is 1.618033988749895 and computed as $(1 + \sqrt{5})/2$.

NTSA round function is as follows:

Round i (i is odd):

$$v_0 += ((v_1 \text{ LSHIFT } 4) \text{ AND } k_0) \text{ XOR } (v_1 \text{ AND } k_c) \text{ XOR } ((v_1 \text{ RSHIFT } 5) \text{ AND } k_1)$$

Round i (i is even):

$$v_1 += ((v_0 \text{ LSHIFT } 4) \text{ AND } k_2) \text{ XOR } (v_0 \text{ AND } k_c) \text{ XOR } ((v_0 \text{ RSHIFT } 5) \text{ AND } k_3)$$

For 1st cycle: the partial keys are k_0 , k_1 , k_2 and k_3 .

From 2nd cycle onwards:

For odd round k_0 is kept constant but k_1 changes for all odd rounds as follows,

$$k_1 = k_1 + (k_0 \text{ XOR}(\text{xtract}(v_0)))$$

For even round k_2 is kept constant but k_3 changes for all even rounds as follows,

$$k_3 = k_3 + (k_2 \text{ XOR}(\text{xtract}(v_1)))$$

The function $\text{xtract}()$ will compute an integer in the range 0 to 32 from v_0 or v_1 depending upon the parameter being passed. This integer value is an index to an array that is generated dynamically based on the key value selection. The $\text{xtract}()$ function will return the value from the array that is pointed by the index value computed. Thus, the key confusion is created dynamically and cannot be predicted prior to execution and the value changes on each execution of the algorithm. The NTSA encryption and decryption model is shown in Figure 4.

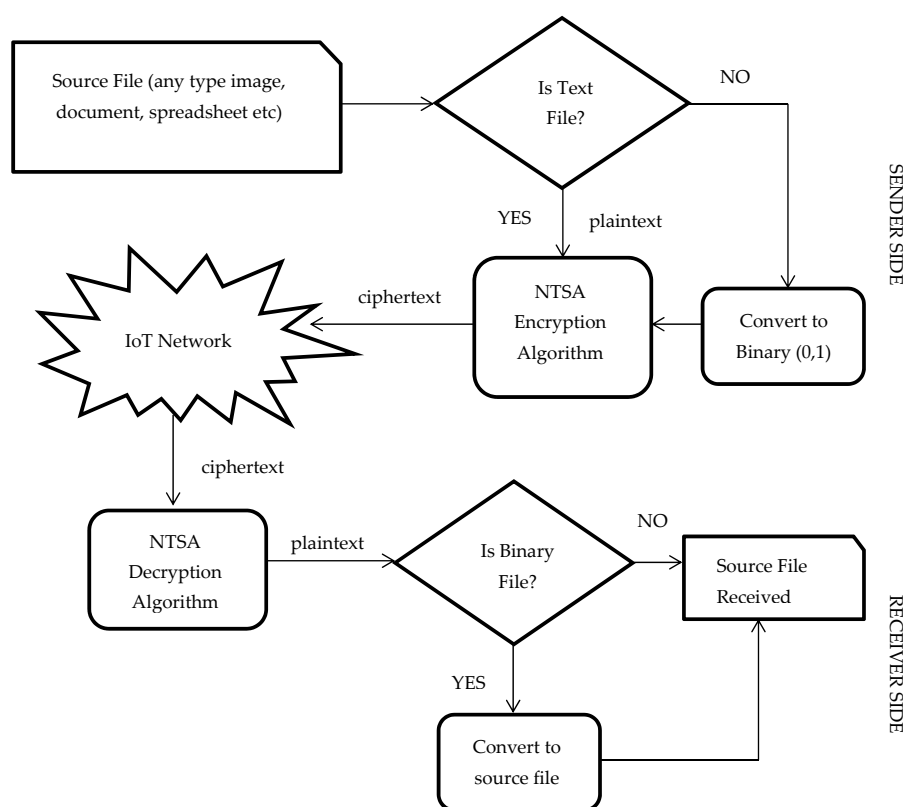


Figure 4. System model: novel tiny symmetric encryption algorithm (NTSA) encryption and decryption.

The source file can be a file of any type such as a document, spreadsheet, pdf, presentation, image, text file etc. The text file can be sent directly to the NTSA encryption algorithm to obtain the cipher text. All the other types of files are converted into binary, the streams of ones and zeros. This binary stream is sent to the NTSA encryption algorithm to get the cipher text using the secret key which has already been agreed upon by the sender and the receiver. On reception of cipher text at the receiver end, the NTSA decryption algorithm converts the cipher text to plaintext. If the converted file is binary (that is streams of zeros and ones) the file is converted to the respective source file, otherwise the plaintext is already received. The NTSA Encryption technique is presented as Algorithm 1 and Decryption technique is presented as Algorithm 2.

Algorithm 1 Novel tiny symmetric encryption algorithm (NTSA) symmetric encryption algorithm

Encrypt (plaintext v , key k):

1: Start

2: Assign key constant $kc = 0$

3: Assign cycle = 0

4: $kc = kc + ksc$

5: 32-bit block $v0$ is recomputed as

$v0 += ((v1 \text{ LSHIFT } 4) \text{ AND } k0) \text{ XOR } (v1 \text{ AND } kc) \text{ XOR } ((v1 \text{ RSHIFT } 5) \text{ AND } k1)$

6: Partial key $k1$ is recomputed as

$k1 += (k0 \text{ XOR } (xtract(v0)))$ where function $xtract()$ returns value of array indexed $v0$.

7: 32-bit block $v1$ is recomputed as

$v1 += ((v0 \text{ LSHIFT } 4) \text{ AND } k2) \text{ XOR } (v0 \text{ AND } kc) \text{ XOR } ((v0 \text{ RSHIFT } 5) \text{ AND } k3)$

8: Partial key $k3$ is recomputed as

$k3 += (k2 \text{ XOR } (xtract(v1)))$ where function $xtract()$ returns value of array indexed $v1$.

9: Increment cycle by 1

10: Repeat step 4 through step 9 until cycle = 32

11: Assign value of $k1$ to $newk1$ and $k3$ to $newk3$

12: Return $newk1$ and $newk3$

The NTSA symmetric encryption algorithm uses the plaintext to encrypt with the key that was already agreed upon by the two parties in communication. The key constant is initialized to zero. The key schedule constant ksc is computed as $\text{floor}(2^{31}/\phi)$ where ϕ is the golden ratio. The golden ratio ϕ is 1.618033988749895. The 32-bit block plaintext $v0$ and $v1$ are recomputed each time for 32 cycles and partial keys $k1$ and $k3$ are recomputed for even and odd rounds respectively to induce key confusion. The computation of $v0$, $k1$, $v1$, $k3$ are shown in the following equations.

$$v0 += ((v1 \text{ LSHIFT } 4) \text{ AND } k0) \text{ XOR } (v1 \text{ AND } kc) \text{ XOR } ((v1 \text{ RSHIFT } 5) \text{ AND } k1)$$

$$k1 += (k0 \text{ XOR } (xtract(v0))) \text{ where function } xtract() \text{ returns value of array indexed } v0.$$

$$v1 += ((v0 \text{ LSHIFT } 4) \text{ AND } k2) \text{ XOR } (v0 \text{ AND } kc) \text{ XOR } ((v0 \text{ RSHIFT } 5) \text{ AND } k3)$$

$$k3 += (k2 \text{ XOR } (xtract(v1))) \text{ where function } xtract() \text{ returns value of array indexed } v1.$$

$$kc \text{ is recomputed each time as } kc = kc + ksc$$

This process is repeated for 32 cycles and after the last cycle the values of partial keys $k1$ and $k3$ are the new values computed and these new partial keys and the cipher text are sent to the decryption process. The NTSA symmetric decryption algorithm uses the cipher text, the key that was already agreed upon by the two parties in communication and the newly computed partial keys $k1$ and $k3$ for the decryption purpose. The key constant is initialized to 0XC6EF3720. The key schedule constant ksc is computed as $\text{floor}(2^{31}/\phi)$. The golden ratio ϕ is 1.618033988749895. The 32-bit blocks $v1$ and $v0$ are recomputed each time for 32 cycles and partial keys $k3$ and $k1$ are recomputed for odd and even rounds respectively to induce key confusion. The computation of $k3$, $v1$, $k1$ and $v0$ are shown in the following equations.

$$k3 - = (k2 \text{ XOR } (xtract(v1))) \text{ where function } xtract() \text{ returns value of array indexed } v1$$

$$v1 - = ((v0 \text{ LSHIFT } 4) \text{ AND } k2) \text{ XOR } (v0 \text{ AND } kc) \text{ XOR } ((v0 \text{ RSHIFT } 5) \text{ AND } k3)$$

$$k1 - = (k0 \text{ XOR } (xtract(v0))) \text{ where function } xtract() \text{ returns value of array indexed } v0$$

$$v0 - = ((v1 \text{ LSHIFT } 4) \text{ AND } k0) \text{ XOR } (v1 \text{ AND } kc) \text{ XOR } ((v1 \text{ RSHIFT } 5) \text{ AND } k1)$$

$$kc \text{ is recomputed each time as } kc = kc - ksc$$

This process is repeated for 32 cycles and after the last cycle the 32-bit block v0 and v1 contains the decrypted contents.

Algorithm 2. NTSA symmetric decryption algorithm

Encrypt (plaintext v, key k):

- 1: Start
- 2: Assign key constant $kc = 0XC6EF3720$
- 3: Assign $k1 = newk1$ and $k3 = newk3$
- 4: Assign $cycle=0$
- 5: Partial key $k3$ is recomputed as
 $k3 = (k2 \text{ XOR}(\text{xtract}(v1)))$ where function $\text{xtract}()$ returns value of array indexed v1.
- 6: 32-bit block v1 is recomputed as
 $v1 = ((v0 \text{ LSHIFT } 4) \text{ AND } k2) \text{ XOR } (v0 \text{ AND } kc) \text{ XOR } ((v0 \text{ RSHIFT } 5) \text{ AND } k3)$
- 7: Partial key $k1$ is recomputed as
 $k1 = (k0 \text{ XOR}(\text{xtract}(v0)))$ where function $\text{xtract}()$ returns value of array indexed v0.
- 8: 32-bit block v0 is recomputed as
 $v0 = ((v1 \text{ LSHIFT } 4) \text{ AND } k0) \text{ XOR } (v1 \text{ AND } kc) \text{ XOR } ((v1 \text{ RSHIFT } 5) \text{ AND } k1)$
- 9: $kc = kc - ksc$
- 10: Increment cycle by 1
- 11: Repeat step 5 through step 10 until $cycle=32$
- 12: Return

Figures 5 and 6 show the structure of NTSA encryption and decryption algorithm.

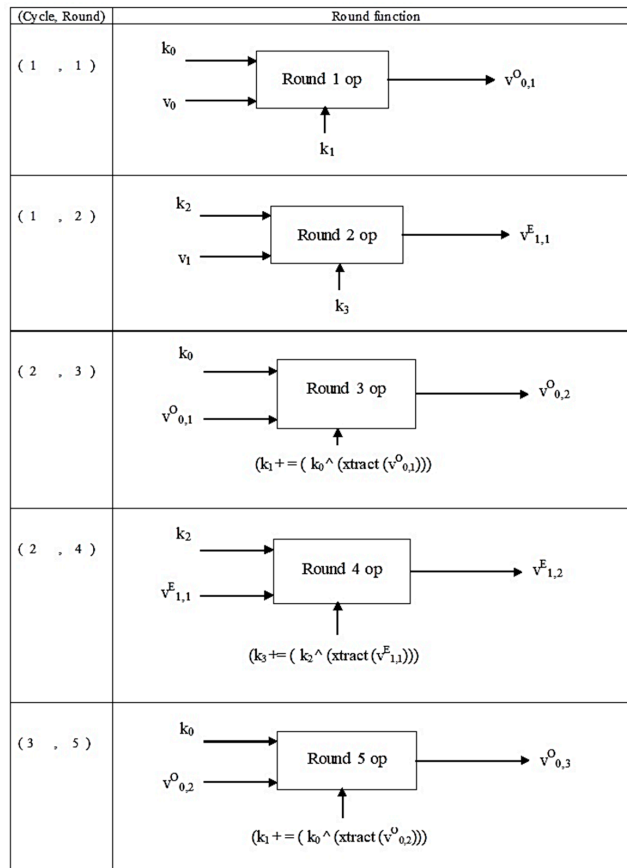


Figure 5. Cont.

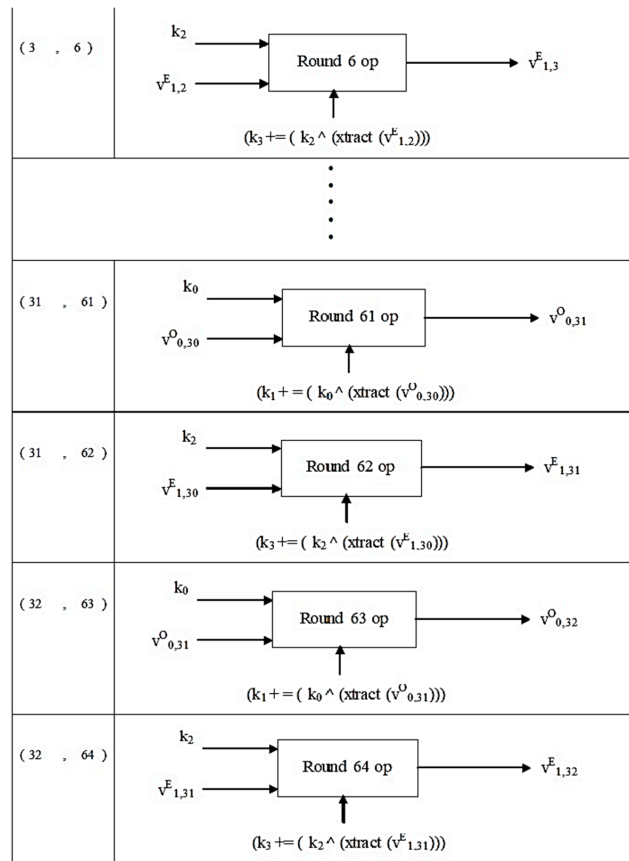


Figure 5. Structure of NTSA encryption algorithm.

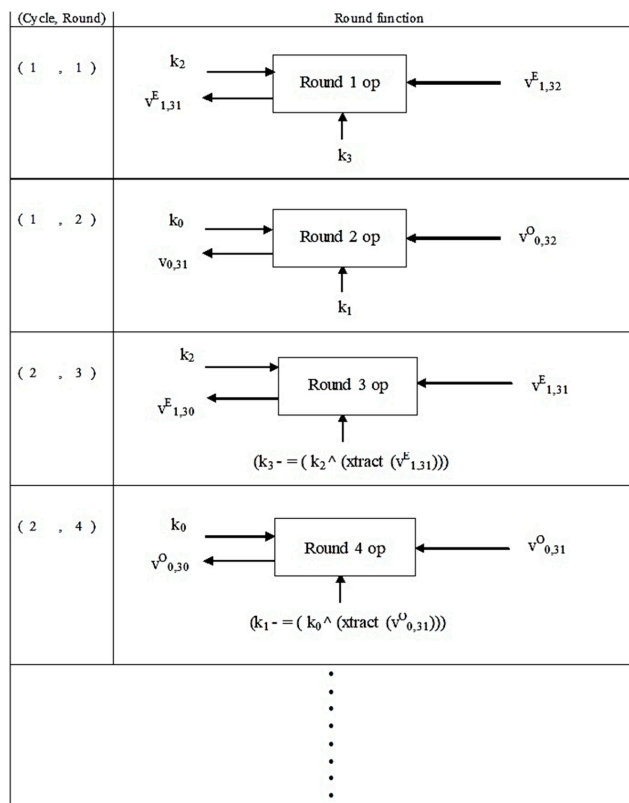


Figure 6. Cont.

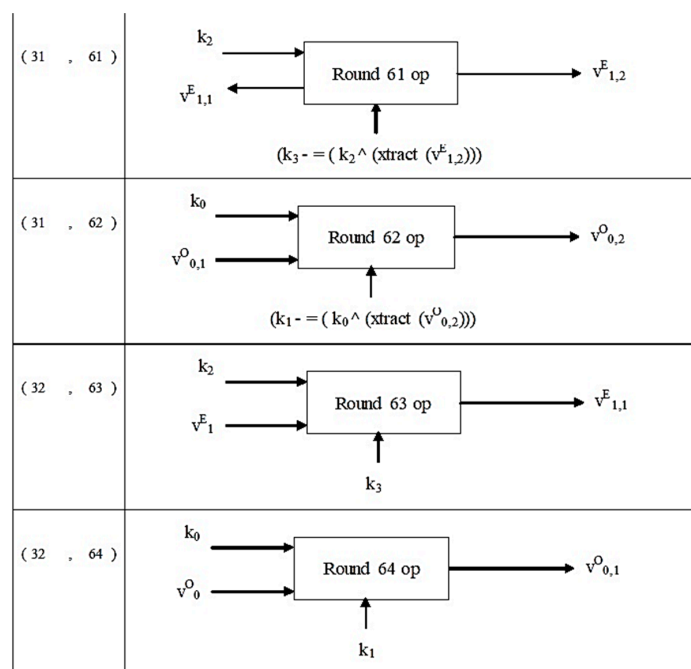


Figure 6. Structure of NTSA decryption algorithm.

The notation:

in $v^{O,1}$; O indicates an odd round, and 0,1 indicate the 0th cycle, round 1;

in $v^{E,1}$; E indicates an even round, and 1,1 indicate the 1st cycle, round 1.

For computing $v^{O,1}$, the second half of the plaintext v_1 is used and shift, AND, and XOR operations are performed on v_1 . Similarly, for computing $v^{E,1}$, the first half (32 bits) of plain text v_0 is used and shift, AND and XOR operations are performed on v_0 .

4. Experimental Results and Discussion

In this section we discuss the results obtained with our experiments. The performance of NTSA is analyzed and compared with TEA and its latest variations XTEA and XXTEA. A network with LPWAN and IoT infrastructures was set up in our lab. NTSA, TEA, XTEA and XXTEA algorithms were implemented in embedded devices. System architecture similar to [51] was used for the experimental set up. IoT configured mobile devices connected with LPWAN and interfaced with IoT cloud via the IoT gateway was set up. The text files were then transmitted from these devices to the IoT cloud configured in a mobile device through the IoT gateway platform. The text files were then stored in the database in the cloud server. The text files were then encrypted using the four algorithms separately in four different scenarios and were send to the IoT configured mobile devices. The encryption and decryption times for each algorithm was measured for varying file sizes and key sizes.

4.1. Performance Comparison of NTSA with TEA, XTEA and XXTEA

Table 2 and 3 presents the encryption and decryption times of the various security algorithms for 48-bit key with varying file sizes from 0.37 kilobytes to 26.7 kilobytes. It is evident from Table 2 that the encryption time for text files using the proposed method NTSA was lower than the other existing security algorithms. NTSA achieved an encryption time of 0.041 ms for a 0.37 kB text file which is much lower compared to 0.059 ms obtained by the TEA algorithm. The two other variations of TEA, XTEA and XXTEA had much higher encryption times because of their complexity in design and implementation. It is observed from the results that, even when the text file size increased, NTSA maintained a lower encryption time compared to the other existing security encryption schemes. NTSA achieved a much lower encryption time of 0.857 ms, 1.211 ms and 1.603 ms for text file size

12.2 kB, 16.2 kB, and 26.7 kB, respectively. This asserts the excellent performance of NTSA even with higher text file sizes.

Table 2. Encryption time for key size of 48 bits.

FILE SIZE (IN KILO BYTES)	ENCRYPTION TIME (in milliseconds)			
	TEA	XTEA	BLOCK TEA (XXTEA)	NTSA
0.37	0.059	0.174	0.083	0.041
0.95	0.125	0.244	0.155	0.112
1.6	0.214	0.451	0.271	0.201
2.6	0.351	0.683	0.429	0.289
6.8	0.771	1.384	1.768	0.551
8.6	0.817	2.120	1.192	0.801
12.2	0.916	2.306	1.379	0.857
16.2	1.544	3.744	1.981	1.211
26.7	1.802	4.176	2.712	1.603

From the results presented in Table 3, it is evident that NTSA achieved a lower decryption time for various text file sizes compared to the other three existing security algorithms in IoT networks. NTSA achieved a decryption time of 0.055 ms for a 0.37 kB text file, which is much lower than the decryption time achieved by other algorithms. For higher file sizes of 12.2 kB, 16.2 kB and 26.7 kB, NTSA achieved 0.890 ms, 1.234 ms, and 1.645 ms decryption times, respectively. So even with higher text file sizes, NTSA achieved lower decryption times similar to the results obtained during encryption. Lower encryption and decryption times are a very important parameter determining the efficiency of a security algorithm in an IoT network. With most of the devices having limited computational capabilities, it is very much required to have a security algorithm that can provide maximum security with less complexity and minimum encryption and decryption times. Thus, the results obtained from our experiments with 48-bit key encryption confirms that the proposed method achieves much lower encryption and decryption times compared to the existing security algorithms in IoT networks. This result is achieved, especially due to the simplicity in design of the proposed algorithm, without compromising the strength in security. The improved strength in security of the algorithm was later verified using the avalanche effect parameter. With lower encryption and decryption time, this algorithm would be highly beneficial for the users to transmit text files through the IoT networks more efficiently.

Table 3. Time for key size of 48 bits.

FILE SIZE (IN KILO BYTES)	DECRYPTION TIME (in milliseconds)			
	TEA	XTEA	BLOCK TEA (XXTEA)	NTSA
0.37	0.058	0.136	0.068	0.055
0.95	0.123	0.289	0.156	0.112
1.6	0.209	0.474	0.254	0.201
2.6	0.332	0.691	0.371	0.323
6.8	0.753	1.369	1.73	0.655
8.6	0.806	2.095	1.16	0.789
12.2	0.903	2.228	1.365	0.890
16.2	1.537	3.698	1.959	1.234
26.7	1.78	4.241	2.799	1.645

Tables 4 and 5 present the comparison of encryption and decryption time of NTSA with TEA, XTEA and XXTEA for a 128-bit key with varying file sizes from 0.37 kilobytes to 26.7 kilobytes. It is interesting to observe from the results presented in Table 4 that with a larger key size, NTSA achieved lower encryption time compared to all the existing security algorithms in IoT networks. The encryption time for a text file of size 0.37 kB with 128-bit key is 0.51 ms for NTSA which was much lower compared

to the encryption time achieved by TEA, XTEA and XXTEA algorithms. The simplicity in design of NTSA helped the algorithm to achieve lower encryption time with varying key and file sizes.

Table 4. Time for key size of 128 bits.

FILE SIZE (IN KILO BYTES)	ENCRYPTION TIME (in milliseconds)			
	TEA	XTEA	BLOCK TEA (XXTEA)	NTSA
0.37	0.059	0.125	0.068	0.51
0.95	0.126	0.264	0.158	0.109
1.6	0.198	0.423	0.232	0.189
2.6	0.332	0.686	0.384	0.221
6.8	0.696	1.584	0.743	0.548
8.6	0.948	1.669	1.171	0.899
12.2	1.277	2.807	1.535	1.02
16.2	1.12	3.263	1.864	1.10
26.7	2.209	5.207	2.224	1.983

Table 5. Time for key size of 128 bits.

FILE SIZE (IN KILO BYTES)	DECRYPTION TIME (in milliseconds)			
	TEA	XTEA	BLOCK TEA (XXTEA)	NTSA
0.37	0.058	0.143	0.068	0.49
0.95	0.125	0.276	0.179	0.101
1.6	0.195	0.43	0.233	0.174
2.6	0.324	0.673	0.388	0.311
6.8	0.678	1.57	0.75	0.556
8.6	0.936	1.641	1.21	0.889
12.2	1.241	2.764	1.538	1.03
16.2	1.111	3.184	1.956	1.10
26.7	2.179	5.178	2.193	1.989

This scenario was also observed with the decryption times presented in Table 5. With decryption also, NTSA achieved lower times compared to its compatriots with a 128-bit key and varying file sizes. NTSA achieved a decryption time of 0.49 ms for a 0.37 kB text file compared to 0.058 ms, 0.143 ms and 0.068 ms achieved by TEA, XTEA and XXTEA respectively for similar text file size. For higher file sizes of 12.2 kB, 16.2 kB, and 26.7 kB, NTSA achieved 1.03 ms, 1.10 ms, and 1.989 ms decryption times, respectively. So even with higher text file sizes, NTSA achieved lower decryption times similar to the results obtained during encryption. With lower encryption and decryption times at 128-bit key, NTSA can become the preferred security algorithm for hand held devices and other embedded IoT devices with different computational capabilities for efficiently transferring text files.

Tables 6 and 7 show the encryption and decryption times of the security algorithms for the transfer of a text file with size 0.95 kB. The better performance of NTSA compared to all the existing security algorithms is evident from the obtained results. This is because the NTSA algorithm has a very simple implementation strategy. The TEA and its different variations use complex computations with the key and hence the encryption and decryption time is greater. In Table 6, the encryption time obtained by NTSA for a file size of 0.95 kB with varying key size is compared with the existing algorithms. The key size is varied from 32 bits to 240 bits and the corresponding encryption time is observed. TEA achieved an encryption time of 0.125 ms for a key size of 32 bits while XTEA and XXTEA achieved 0.287ms and 0.145 ms, respectively. For the same key size, NTSA had an encryption time of 0.07 ms which was much lower compared to all the other security algorithms. For the 96-bit key, XTEA had an encryption time of 0.126 ms, while XTEA and XXTEA had encryption times of 0.265 ms and 0.158 ms, respectively. The encryption time obtained by NTSA for similar key size was 0.093 ms which was much lower than the time achieved by the existing algorithms. This demonstrates the better performance of the

proposed approach NTSA, compared to all the existing security algorithms in IoT networks with varying key sizes.

Table 6. Encryption time for file size 0.95 kB.

KEY SIZE (IN BITS)	ENCRYPTION TIME (in milliseconds)			
	TEA	XTEA	BLOCK TEA (XXTEA)	NTSA
32	0.125	0.287	0.145	0.07
48	0.125	0.264	0.162	0.083
64	0.125	0.246	0.17	0.088
96	0.126	0.265	0.158	0.093
128	0.126	0.264	0.158	0.097
160	0.114	0.271	0.154	0.100
192	0.125	0.279	0.144	0.100
240	0.125	0.279	0.145	0.113

Table 7. Time for file size 0.95 kB.

KEY SIZE (IN BITS)	DECRYPTION TIME (in milliseconds)			
	TEA	XTEA	BLOCK TEA (XXTEA)	NTSA
32	0.124	0.281	0.146	0.068
48	0.136	0.257	0.15	0.087
64	0.123	0.214	0.152	0.088
96	0.123	0.259	0.158	0.091
128	0.125	0.276	0.179	0.090
160	0.113	0.267	0.155	0.101
192	0.126	0.26	0.159	0.119
240	0.123	0.259	0.157	0.119

Tables 8 and 9 show the encryption and decryption times of the security algorithms for the transfer of a text file with size 12.2 kB with varying key sizes. The encryption time achieved by TEA, XTEA and XXTEA for a key size of 32 bits was 1.173 ms, 2.287 ms, and 1.649 ms, respectively, which was much higher compared to 1.009 ms obtained by NTSA for a similar key size. Even for a key size of 96 bits, NTSA achieved an encryption time of 1.10 ms which is lower than the values obtained by all the other existing security algorithms for similar file size. For a key size of 240 bits, NTSA had an encryption time of 1.2 ms which was much lower compared to all the existing algorithms. Thus, for smaller and larger key sizes, NTSA achieved lower encryption time compared to all the existing security algorithms in IoT networks. This scenario is also observed with the decryption times presented in Table 9. NTSA achieved a decryption time of 1.025 ms, 1.155 ms, and 1.388 ms for a key size 160 bits, 192 bits, and 240 bits, respectively. This time achieved by NTSA was lower than the times obtained by TEA, XTEA and XXTEA for similar key sizes in the IoT network. This assures the better performance of NTSA compared to all the existing algorithms with varying key sizes in IoT networks.

Tables 10 and 11 presents the results obtained in encryption and decryption time with NTSA, TEA, XTEA and XXTEA for a text file size of 26.7 kB with varying key sizes from 32 bits to 240 bits. The encryption time achieved by TEA, XTEA and XXTEA for a key size of 32 bits is 2.253 ms, 4.459 ms, and 2.339 ms, respectively, which is much higher compared to 1.772 ms obtained by NTSA for a similar key size. Even for a key size of 96 bits, NTSA achieved an encryption time of 1.856 ms which was lower than the values obtained by all the other existing security algorithms for similar file size. NTSA also achieved an encryption time of 1.887 ms, 1.662 ms, and 1.912 ms for 160 bits, 192 bits and 240 bits' key sizes. Thus, from the results it is evident that NTSA achieved much lower encryption times compared to all the existing algorithms in IoT networks. This scenario is also verified in Table 11 which presents the decryption time obtained by these algorithms for varying key sizes. The simplicity in design enables NTSA to achieve much lower encryption and decryption times in IoT networks. This would

definitely enable IoT devices with varying computational and storage capabilities to efficiently and securely transmit text files through the network.

Table 8. Time for file size 12.2 kB.

KEY SIZE (IN BITS)	ENCRYPTION TIME (in milliseconds)			
	TEA	XTEA	BLOCK TEA (XXTEA)	NTSA
32	1.173	2.287	1.649	1.009
48	1.178	2.572	1.393	1.010
64	1.248	2.089	1.178	1.006
96	1.208	2.32	1.502	1.10
128	1.067	2.301	1.534	1.04
160	1.137	2.608	1.076	1.03
192	1.39	2.327	1.148	1.11
240	1.439	2.866	1.413	1.2

Table 9. Decryption time for file size 12.2 kB.

KEY SIZE (IN BITS)	DECRYPTION TIME (in milliseconds)			
	TEA	XTEA	BLOCK TEA (XXTEA)	NTSA
32	1.127	2.249	1.641	1.08
48	1.195	2.572	1.396	1.083
64	1.241	2.084	1.179	1.112
96	1.226	2.299	1.477	1.117
128	1.029	2.265	1.583	1.020
160	1.093	2.645	1.074	1.025
192	1.363	2.278	1.163	1.155
240	1.402	2.827	1.414	1.388

Table 10. Time for file size 26.7 kB.

KEY SIZE (IN BITS)	ENCRYPTION TIME (in milliseconds)			
	TEA	XTEA	BLOCK TEA (XXTEA)	NTSA
32	2.253	4.459	2.339	1.772
48	1.883	3.734	2.111	1.789
64	1.933	3.349	2.485	1.812
96	2.812	4.856	2.246	1.856
128	2.209	5.207	2.224	1.825
160	2.925	3.687	2.731	1.887
192	1.869	4.562	1.958	1.662
240	1.989	4.213	2.43	1.912

Table 11. Time for file size 26.7 kB.

KEY SIZE (IN BITS)	DECRYPTION TIME (in milliseconds)			
	TEA	XTEA	BLOCK TEA (XXTEA)	NTSA
32	2.212	4.422	2.387	1.701
48	1.854	3.713	2.136	1.746
64	1.888	3.307	2.516	1.777
96	2.726	4.892	2.289	1.834
128	2.179	5.178	2.193	1.820
160	2.883	3.668	2.711	1.811
192	1.853	4.498	1.935	1.812
240	1.934	4.073	2.456	1.936

From the results presented in Tables 2–11, it is very evident that the NTSA algorithm give better performance compared to all the existing algorithms with variable file sizes and key sizes. NTSA gave much lower encryption and decryption times for variable size text files using multiple key sizes in IoT networks. This is due to the simple and efficient design of NTSA. One of the most important features of NTSA is that it provides enhanced security to all the applications in IoT devices with lower encryption and decryption times. Thus, the proposed approach NTSA can be used for efficient and secure transfer of text files between devices in IoT networks.

Avalanche Effect

The avalanche effect is the property wherein a very small change in input results in significant changes on the output. An encryption algorithm is considered good if a one-bit change in key results in significant changes in the cipher text. With reference to the avalanche effect, we compared the strength of NTSA and TEA algorithms.

Experiment 1: an encryption was performed for NTSA and TEA algorithms using keys with varying key sizes of 48, 64 and 128 bits and same plaintext. Then one bit was changed on the key and the experiment was repeated. It is observed that for every 64-bit block, a one-bit change in key resulted in significant changes on the cipher text. Drastic changes were observed for the NTSA algorithm when compared to TEA. Figure 7 shows, for every 64-bit block, a change in one bit of the key with various key sizes and the corresponding change in cipher text for NTSA and TEA.

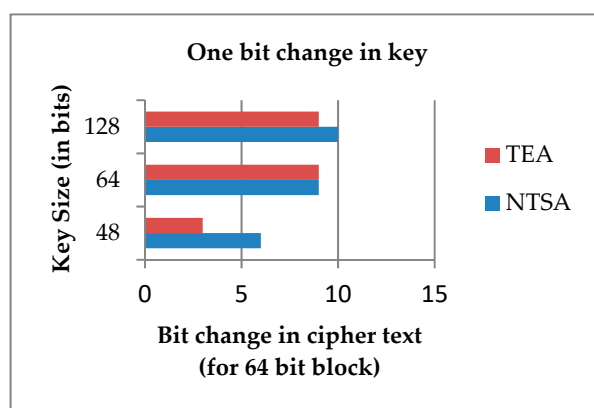


Figure 7. Change in key and the corresponding change in cipher text for a 64-bit block.

From Figure 7, it is very evident that when a bit in the key was changed, the cipher text generated using NTSA algorithm had more drastic change than the cipher text created using TEA. This shows the increased security offered by the NTSA algorithm compared to TEA.

Experiment 2: an encryption was performed for NTSA and TEA algorithms using keys with varying key sizes 48, 64 and 128 bits. Then one bit was changed on the plaintext and the experiment is repeated. It was observed that for every 64-bit block, one-bit change in plaintext resulted in significant changes on the cipher text. Drastic changes were observed for the NTSA algorithm when compared to the tiny encryption algorithm. Figure 8 shows that for every 64-bit block a change in one bit of key with various key sizes and the corresponding change in cipher text for NTSA and TEA.

From Figure 8 it is very evident that when a bit in the plaintext was changed, the cipher text generated using NTSA algorithm had more drastic change than the cipher text created using TEA. This verifies the increased security offered by the NTSA algorithm compared to TEA. Thus, the proposed method NTSA is more efficient and secure than all previously proposed encryption schemes for transfer of text files between embedded devices in IoT network.

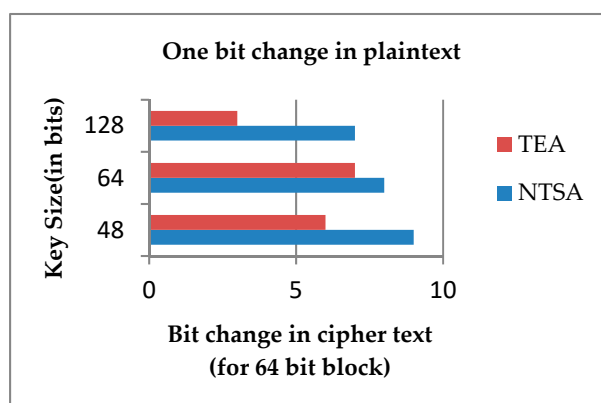


Figure 8. One-bit change in plaintext corresponding change in cipher text for 64-bit block.

5. Conclusions

TEA showed better performance in terms of both encryption and decryption execution times than XTEA and XXTEA. The XTEA was proposed to set the key schedule and XXTEA was proposed in order to present the key material slowly. The proposed algorithm NTSA does the same, and experiments performed proved that the performance of NTSA is better than TEA. In addition to this, NTSA created more confusion on the key than the tiny encryption algorithm. The avalanche effect showed a positive result to NTSA when compared to TEA. Thus, NTSA can be used by all the latest applications in IoT devices with different computational and storage facilities to transfer text files efficiently and securely through the network. The NTSA algorithm security can be further increased by encrypting the compressed file. In future we also aim to integrate and implement this algorithm for data transfer in ad hoc, sensor and fog networks [8,52–57].

Author Contributions: Conceptualization, S.R.; formal analysis, S.R. and V.M.; funding acquisition, V.M.; investigation, S.R.; methodology, S.R.; project administration, V.P., V.M. and M.K.; resources, V.P. and V.M.; software, M.K.; supervision, V.P.; validation, S.R. and M.K.; visualization, S.R.; writing—original draft, S.R., V.P. and V.M.; writing—review and editing, V.M. and M.K.

Acknowledgments: Authors would like to thank the Management and Principal of SCMS School of Engineering and Technology for providing the infrastructure and facilities to carry out the research. Authors would also like to thank Linda Cui, Assistant Editor for all the support handling the manuscript and the reviewers for providing valuable suggestions and comments in improving the manuscript.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Porambage, P.; Okwuibe, J.; Liyanage, M.; Ylianttila, M.; Taleb, T. Survey on Multi-Access Edge Computing for Internet of Things Realization. *IEEE Commun. Surv. Tutor.* **2018**, *20*, 2961–2991. [CrossRef]
2. Ploennigs, J.; Cohn, J.; Stanford-Clark, A. The Future of IoT. *IEEE Internet Things Mag.* **2018**, *1*, 28–33. [CrossRef]
3. Philip, V.; Suman, V.K.; Menon, V.G.; Dhanya, K. A Review on latest Internet of Things based Healthcare Applications. *Int. J. Comput. Sci. Inf. Secur.* **2017**, *15*, 248–254.
4. Deshkar, S.; Thanseeh, R.A.; Menon, V.G. A Review on IoT based m-Health Systems for Diabetes. *Int. J. Comput. Sci. Telecommun.* **2017**, *8*, 13–18.
5. Vinoj, P.G.; Jacob, S.; Menon, V.G. Hybrid brainactuated muscle interface for the physically disabled. In *Basic and Clinical Pharmacology and Toxicology*; Wiley: Hoboken, NJ, USA, 2018; Volume 123.
6. Keerthi, K.S.; Mahapatra, B.; Menon, V.G. Into the World of Underwater Swarm Robotics: Architecture, Communication, Applications and Challenges. *Recent Pat. Comput. Sci.* **2019**, *12*, 1.
7. Bordel, B.; Alcarria, R.; De Andres, D.M.; You, I.; Martin, D. Securing Internet-of-Things Systems through Implicit and Explicit Reputation Models. *IEEE Access* **2018**, *6*, 47472–47488. [CrossRef]

8. Menon, V.G.; Prathap, J. Vehicular Fog Computing: Challenges applications and future directions. *Int. J. Veh. Telemat. Infotain. Syst.* **2017**, *1*, 15–23. [[CrossRef](#)]
9. Frustaci, M.; Pace, P.; Aloï, G.; Fortino, G. Evaluating Critical Security Issues of the IoT World: Present and Future Challenges. *IEEE Internet Things J.* **2018**, *5*, 2483–2495. [[CrossRef](#)]
10. Wang, B.; Zhan, Y.; Zhang, Z. Cryptanalysis of a Symmetric Fully Homomorphic Encryption Scheme. *IEEE Trans. Inf. Forensics Secur.* **2018**, *13*, 1460–1467. [[CrossRef](#)]
11. Maimuț, D.; Reyhanitabar, R. Authenticated Encryption: Toward Next-Generation Algorithms. *IEEE Secur. Privacy* **2014**, *12*, 70–72. [[CrossRef](#)]
12. Ahmad, S.; Alam, K.M.R.; Rahman, H.; Tamura, S. A comparison between symmetric and asymmetric key encryption algorithm based decryption mixnets. In Proceedings of the 2015 International Conference on Networking Systems and Security (NSysS), Dhaka, Bangladesh, 5–7 January 2015; pp. 1–5.
13. Yassein, M.B.; Aljawarneh, S.; Qawasmeh, E.; Mardini, W.; Khamayseh, Y. Comprehensive study of symmetric key and asymmetric key encryption algorithms. In Proceedings of the 2017 International Conference on Engineering and Technology (ICET), Antalya, Turkey, 21–23 August 2017; pp. 1–7.
14. Lamba, C.S. Design and Analysis of Stream Cipher for Network Security. In Proceedings of the 2010 Second International Conference on Communication Software and Networks, Singapore, 26–28 February 2010; pp. 562–567.
15. Baker, S.I.B.; Al-Hamami, A.H. Novel Algorithm in Symmetric Encryption (NASE): Based on Feistel Cipher. In Proceedings of the 2017 International Conference on New Trends in Computing Sciences (ICTCS), Amman, Jordan, 9–11 October 2017; pp. 191–196.
16. Rebeiro, C.; Nguyen, P.H.; Mukhopadhyay, D.; Poschmann, A. Formalizing the Effect of Feistel Cipher Structures on Differential Cache Attacks. *IEEE Trans. Inf. Forensics Secur.* **2013**, *8*, 1274–1279. [[CrossRef](#)]
17. Wheeler, D.; Needham, R. TEA, a tiny encryption algorithm. In Proceedings of the 1995 Fast Software En-Cryption Workshop, Leuven, Belgium, 14–16 December 1995; Springer: Berlin/Heidelberg, Germany, 1995; pp. 97–110.
18. Amrutha George, A.; Riyadh, M.; Prajitha, M.V. Secure image transferring using KBRP and TEA algorithms. In Proceedings of the 2015 International Conference on Innovations in Information, Embedded and Communication Systems (ICIIECS), Coimbatore, India, 19–20 March 2015; pp. 1–5.
19. Abdelhalim, M.B.; El-Mahallawy, M.; Ayyad, M.; Elhennawy, A. Implementation of a modified lightweight cryptographic TEA algorithm in RFID system. In Proceedings of the 2011 International Conference for Internet Technology and Secured Transactions, Abu Dhabi, UAE, 11–14 December 2011; pp. 509–513.
20. Shepherd, S.J. The Tiny Encryption Algorithm. *Cryptologia* **2007**, *31*, 233–245. [[CrossRef](#)]
21. Sima, I.; Tarmurean, D.; Greu, V.; Diaconu, A. XXTEA, an alternative replacement of KASUMI cipher algorithm in A5/3 GSM and f8, f9 UMTS data security functions. In Proceedings of the 2012 9th International Conference on Communications (COMM), Bucharest, Romania, 21–23 June 2012; pp. 323–326.
22. Lu, J. Related-key rectangle attack on 36 rounds of the XTEA block cipher. *Int. J. Inf. Sec.* **2009**, *8*, 1–11.
23. Holden, J. Demitasse: A “Small” Version of the Tiny Encryption Algorithm and Its Use in a Classroom Setting. *Cryptologia* **2013**, *37*, 74–83. [[CrossRef](#)]
24. De Dormale, G.M.; Bass, J.; Quisquater, J.-J. On Solving RC5 Challenges with FPGAs. In Proceedings of the 15th Annual IEEE Symposium on Field-Programmable Custom Computing Machines (FCCM 2007), Napa, CA, USA, 23–25 April 2007; pp. 281–282.
25. Li, T.; Wu, H.; Wang, X.; Bao, F. *SenSec Design Technical Report-TR v1.1*; InfoComm Security Department, Institute for Infocomm Research: Singapore, 2005.
26. Karlof, C.; Sastry, N.; Wagner, D. TinySec: A link layer security architecture for wireless sensor networks. In Proceedings of the 2nd International Conference on Embedded Networked Sensor Systems (SenSys '04), Baltimore, MD, USA, 3–5 November 2004; pp. 162–175.
27. Luk, M.; Mezzour, G.; Perrig, A.; Gligor, V. MiniSec: A secure sensor network communication architecture. In Proceedings of the 6th International Symposium on Information Processing in Sensor Networks (IPSN '07), Cambridge, MA, USA, 25–27 April 2007; pp. 479–488.
28. Standaert, F.-X.; Piret, G.; Gershenfeld, N.; Quisquater, J.-J. SEA: A scalable encryption algorithm for small embedded applications. In Proceedings of the Workshop on RFIP and Light weight Crypto, Graz, Austria, 14–15 July 2005.

29. Hong, D.; Sung, J.; Hong, S.; Lim, J.; Lee, S.; Koo, B.-S.; Lee, C.; Chang, D.; Lee, J.; Jeong, K.; et al. HIGHT: A new block cipher suitable for low-resource device. In *Cryptographic Hardware and Embedded Systems—CHES 2006: 8th International Workshop, Yokohama, Japan, 10–13 October 2006*; Volume 4249 of Lecture Notes in Computer Science; Springer: Berlin, Germany, 2006; pp. 46–59.
30. Usman, M.; Ahmed, I.; Aslam, M.I.; Khan, S.; Shah, U.A. SIT: A Lightweight Encryption Algorithm for Secure Internet of Things. *Int. J. Adv. Comput. Sci. Appl.* **2017**, *8*. [[CrossRef](#)]
31. Liang, C.; Ye, N.; Malekian, R.; Wang, R. The hybrid encryption algorithm of lightweight data in cloud storage. In *Proceedings of the 2016 2nd International Symposium on Agent, Multi-Agent Systems, and Robotics (ISAMSR), Bangi, Malaysia, 23–24 August 2016*; pp. 160–166.
32. Gao, C.; Lv, S.; Wei, Y.; Wang, Z.; Liu, Z.; Cheng, X. M-SSE: An Effective Searchable Symmetric Encryption with Enhanced Security for Mobile Devices. *IEEE Access* **2018**, *6*, 38860–38869. [[CrossRef](#)]
33. Schneier, B. The IDEA Encryption Algorithm. *Dr. Dobbs's J.* **1990**, *18*, 50–56.
34. Burwick, C.; Coppersmith, D.; D'Avignon, E.; Gennaro, R.; Halevi, S.; Jutla, C.; Matyas, S.M.; O'Connor, L.; Peyravian, M.; Safford, D.; et al. MARS—A candidate cipher for AES. 1998. Available online: <http://www.research.ibm.com/security/mars.html> (accessed on 29 April 2018).
35. Abdelhalim, M.B.; El-Mahallawy, M.; Elhennawy, M.A.A. Design and Implementation of an Encryption Algorithm for use in RFID System. *Int. J. RFID Secur. Cryptogr.* **2013**, *2*. [[CrossRef](#)]
36. Zhdanov, O.N.; Sokolov, A.V. Block Symmetric Cryptographic Algorithm based on Principles of variable block length and many-valued logic. *Far East J. Electron. Commun.* **2016**, *16*, 573–589. [[CrossRef](#)]
37. Korea Telecommunication Technology Association. *128 Bit Light Weight Block Cipher LEA*, Information Telecommunication Organization Standard (Korean Standard). 2013.
38. Park, J.H. 128 bit block cipher LEA. *TTA J.* **2015**, *157*.
39. Abdullah, D.; Rahim, R.; Siahaan, A.P.U.; Ulva, A.F.; Fitri, Z.; Malahayati, M.; Harun, H. Super-Encryption Cryptography with IDEA and WAKE Algorithm. *J. Phys. Conf. Ser.* **2018**, *1019*, 012039. [[CrossRef](#)]
40. Anderson, R.; Biham, E.; Knudsen, L. Serpent: A Proposal for the Advanced Encryption Standard. In *Proceedings of the First Advanced Encryption Standard (AES) Conference, Ventura, CA, USA, 20–22 August 1998*.
41. Ren, W.; Miao, Z. A Hybrid Encryption Algorithm Based on DES and RSA in Bluetooth Communication. In *Proceedings of the 2010 Second International Conference on Modeling, Simulation and Visualization Methods, Sanya, China, 15–16 May 2010*; pp. 221–225.
42. Wheeler, D.; Needham, R. TEA, A Tiny Encryption Algorithm. Available online: <http://www.cix.co.uk/~klockstone/tea.pdf> (accessed on 22 April 2018).
43. Andem, V.R. *A Cryptanalysis of the Tiny Encryption Algorithm*; The University of Alabama: Tuscaloosa, AL, USA, 2003.
44. Rachmawati, D.; Sharif, A.; Jaysilen; Budiman, M.A. Hybrid Cryptosystem Using Tiny Encryption Algorithm and LUC Algorithm. *IOP Conf. Ser. Mater. Sci. Eng.* **2018**, *300*, 012042. [[CrossRef](#)]
45. Novelan, M.S.; Husein, A.M.; Harahap, M.; Aisyah, S. SMS Security System on Mobile Devices Using Tiny Encryption Algorithm. *IOP Conf. Ser. J. Phys. Conf. Ser.* **2018**, *1007*, 012037. [[CrossRef](#)]
46. Needham, R.M.; Wheeler, D.J. *TEA Extensions*; Technical Report; Computer Laboratory, University of Cambridge: Cambridge, MA, USA, 1997.
47. Kaps, J.-P. Chai-tea, Cryptographic Hardware Implementations of XTEA. In *Proceedings of the INDOCRYPT 08 Proceedings of the 9th International Conference on Cryptology in India: Progress in Cryptology, Kharagpur, India, 14–17 December 2008*.
48. Wheeler, D.; Needham, R. *XXTEA: Correction to XTEA*; Technical report; Computer Laboratory, University of Cambridge: Cambridge, MA, USA, 1998.
49. Coppersmith, D.; Johnson, D.B.; Matyas, S.M. A proposed mode for triple-DES encryption. *IBM J. Res. Dev.* **1996**, *40*, 253–262. [[CrossRef](#)]
50. Milad, A.A.; Muda, H.Z.; Noh, Z.A.; Algaet, M.A. Comparative Study of Performance in Cryptography Algorithms (Blowfish and Skipjack). *J. Comput. Sci.* **2012**, *8*, 1191–1197.
51. Wu, F.; Wu, T.; Yuce, M.R. An Internet-of-Things (IoT) Network System for Connected Safety and Health Monitoring Applications. *Sensors* **2019**, *19*, 21. [[CrossRef](#)] [[PubMed](#)]
52. Menon, V.G.; Prathap, J.; Priya, J. Ensuring reliable communication in disaster recovery operations with reliable routing technique. *Mobile Inf. Syst.* **2016**, *2016*, 9141329. [[CrossRef](#)]

53. Menon, V.G.; Prathap, J. Comparative analysis of opportunistic routing protocols for underwater acoustic sensor networks. In Proceedings of the 2016 International Conference on Emerging Technological Trends (ICETT), Kollam, India, 21–22 October 2016.
54. Menon, V. Optimized Opportunistic Routing in Highly Dynamic Ad hoc Networks. *Preprints* **2019**, *2019*, 020130.
55. Menon, V.G.; Prathap, J. Performance of various Routing Protocols in Mobile Ad Hoc Networks-A Survey. *Res. J. Appl. Sci. Eng. Technol.* **2013**, *6*, 4181–4185. [[CrossRef](#)]
56. Menon, V.G.; Prathap, J. Analyzing the behavior and performance of opportunistic routing protocols in highly mobile wireless ad hoc networks. *Int. J. Eng. Technol.* **2016**, *8*, 1916–1924. [[CrossRef](#)]
57. Menon, V.G.; Prathap, P.M.J. Opportunistic routing with virtual coordinates to handle communication voids in mobile ad hoc networks. In *Advances in Signal Processing and Intelligent Recognition Systems*; Springer: Cham, Switzerland, 2016; pp. 323–334.



© 2019 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<http://creativecommons.org/licenses/by/4.0/>).

001 | Computerized fragment reduction and evaluation for distal femur fractures

Yu-Ching Hsiao; Jing-Jing Fang

Department of Mechanical Engineering, National Cheng Kung University, Tainan, Taiwan

Objectives:: Distal femur fractures usually involve the articular surface and the size of its fragments are irregular. To minimize post-surgical complications associated with the knee joint function of patients, the accuracy of fragment reduction is critical. There are some simulation software available for fracture fragment reduction; however, the simulation process usually takes a long time and there is also no valid verification to prove the accuracy of the reduction result. Therefore, we developed a surgical planning software for fracture reduction simulation, particularly for distal femur, by applying the techniques of semi-automatic fragments identification, segmentation and reduction. We provide surgeons a useful tool to pre-plan on computers in order to find suitable placements for fragments in a short time. Moreover, an experimental evaluation method was proposed to reveal the simulation error.

Methods: We separated the digital model of patients into many single objects by placing the seed points with the region growing method. We then set the single segmented bone fragments as subjects and mirrored the contralateral normal side of the patient as the target. In the case where contralateral femur is unavailable, a built-in template of the intact femur was replaced as the target. Finally, an iterative closet point algorithm was applied for reduction simulation. In order to investigate whether the simulation is feasible, we set up a verifying experiment to find the reduction error of the simulation. We invoked nine physical artificial femurs as a test bed where fiducial markers (piecewise k-wire) were embedded in. Nine femur physical models were then destructed to create distal femur fracture fragments in advance based on the AO/OTA classification. Initially, the whole nine physical femurs with fiducial markers are sent for computed tomography (CT) scan. After femur fracture fragments were generated, a second scan was performed. Reconstructed fragments of the second CT scan were given for reduction simulation. We then compared both the fiducial markers placements between the outcomes

of reduction simulation and the whole femur model from the first CT scan.

Results: Outcomes of the nine reduction simulations were evaluated, from which the animated reduction error of the entry point deviation and the included angles of the k-wire markers were found to be 0.4475 ± 0.2938 mm and 1.6366 ± 1.2716 , respectively. The maximum deviation error and the maximum angular error of the reduction simulation are 1.4352 mm and 6.5203, respectively.

Conclusions: In this study, we proposed an evaluation method for reduction simulation software by examining the distal femur fracture reduction. The proposed semi-automatic reduction method includes the whole process of fragment segmentation and reduction, which effectively reduces the simulation time. The whole simulation process takes 6 minutes, compared to other proposed methods, which takes 20 minutes in average. Based on clinical orthopedic literatures from the AO Foundation, a 1-2 mm displacement in reduction surgery is acceptable. The maximum deviation in our study was 1.4352 mm which is less than the clinical requirement, 2 mm. The result shows that the error in reduction simulation is reasonable for reduction planning in distal femur fractures.

002 | Facial acne detection system using deep convolution neural network

C.L. Chin¹; M.C. Chin^{1,2}; C.H. Yang¹; W.E. Chen¹; Z.Y. Yang¹; R.C. Su¹; T.Y. Tsai¹

¹Department of Medical Informatics, Chung Shan Medical University, Taichung, Taiwan; ²E-mail: kobe61201321@gmail.com

Objectives: People clearly understand the condition of the facial skin combining facial skin care or medical cosmetology to make improvements. Many experts and scholars are aware of the possibility of applying machine learning to the judgment of facial skin condition. Among the facial skin problems such as acne, wrinkle and so on, the acne problem is difficult to recognize has because it has different size and shape. And, it is easily affected by various environment light. The acne color is similar to skin color, hence the problem is proper to use deep learning approach for recognition. According to these reasons, we use deep

(c) Insertion, (d) Drug injection, (e) Ablation. After removing the handle part, we only measured precision of operating mechanism. The test results, the error for the resulting target position is measured to within 2 mm.

Conclusions: Automatic injection and puncture device joining ultrasound probe is a device that is possible with just one hand ultrasonic imaging diagnosis and drug injection treatment to combine an automatic injection and puncture device to probe for ultrasound diagnosis. This device has a function that puncture guide service coupled with ultrasound image transmitted via a probe, automatic puncture to the target point in ultrasound image and drug injection and blood inhalation after needle insertion to the target point. In use benefits of this device are shorter operation time that the operation can be alone without assistance person and that puncture can be in the exact point, regardless of the skill of the surgeon.

Acknowledgements: This work was supported by the National Research Foundation of Korea (NRF) grant funded by the Korea government. (NRF-2016R1C1B2008460).

009 | Non-contact autonomic nervous system response measurement for psychiatric trauma treatment

Kun Ha Suh; Kunyoung Lee; Dongkeun Kim; Eui Chul Lee
Intelligent Engineering Informatics for Human, Sangmyung University, Seoul, South Korea

Objectives: To psychiatric treat trauma, a method to grasp the condition of a patient through a physiological reaction during psychiatric treatment and induce a therapeutic effect through feedback on the condition is widely used. Autonomic nervous system responses such as heart rate, respiration, and skin temperature are used as important objective indicators of the patient's emotional and psychological state. Traditionally, it is a method of attaching a sensor to the surface of a patient's skin and measuring the signal, but it can cause a sense of discomfort and unpleasantness

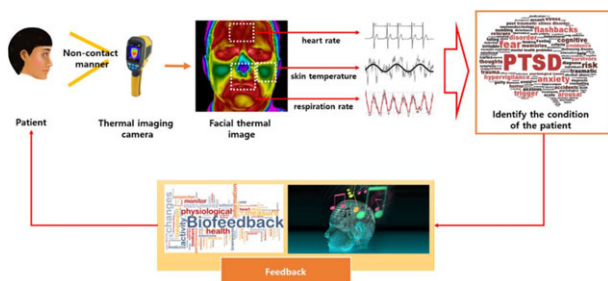


Figure 1 Overall flow of proposed method for measuring autonomic nervous system response using single thermal imaging camera.

due to the attachment of the sensor. These disadvantages can be more lethal for psychiatric patients.

Methods: In order to solve the problems, remote sensing methods without attaching sensors have been actively studied. In previous studies, there have been studies to measure heart rate and respiration without attaching sensors [1], but there has been no way to simultaneously analyze heart rate, respiration, and body temperature with a single sensor. In this study, we proposed a method which estimate the heart rate by observing the minute temperature change of the carotid artery, respiration rate by analyzing the temperature change due to the nostril inspiratory/exhalation, and skin temperature by analyzing facial thermal image as shown in Figure 1.

Results: The measurement accuracy of the skin temperature depends on the sensitivity of the thermal imaging camera, but the temperature of the surface of the skin can be continuously measured. The accuracy of the heart rate measurement method using the carotid artery blood vessel detection was about 98% of that of the ground-truth sensor. Respiration measurement by observing changes in the inspiratory/expiratory temperature of the nostrils was about 99%.

Conclusions: Our method will be used to identify the condition of trauma patients and can be used as a means of self-healing and tele-healthcare. Future studies will improve to be a robust measure of facial pose variation. In addition, we will develop a comprehensive emotion measurement system that considers the facial expression and voice analysis results together.

Acknowledgement: This study was funded by the Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Science, ICT and Future Planning (grant number NRF-2016R1C1B2014345). Also, this work was supported by the Industrial Strategic Technology Development Program (10073159, Developing mirroring expression based interactive robot technique by non-contact sensing and recognizing human intrinsic parameter for emotion healing through heart-body feedback) funded By the Ministry of Trade, industry & Energy (MI, Korea).

010 | Hybrid brainactuated muscle interface for the physically disabled

P.G. Vinoj¹; Sunil Jacob²; Varun G. Menon³

¹Electronics and Communication Engineering Department, APJ Abdul Kalam Technological University, India; ²Centre for Robotics, SCMS School of Engineering and Technology, India; ³Computer Science Engineering Department, SCMS School of Engineering and Technology, India

Objectives: According to Reeve Foundation 29% of paralysis is due to stroke followed by injury in the spinal cord.

Sometimes it may be difficult for a person to move the paralyzed person's body part as it may be too stiff. Our research focuses on actuating the paralyzed person's body part through his own thought process using Brain-Muscle Interface. The system uses Novel Technique which avoids the use of Exo-Skeleton.

Methods: In our current work, we propose a Hybrid Brain-Muscle Interface (HBMI) for the paralyzed person. The HBMI interface should have the provision for pre-processing, classifying, recording and training multidimensional EEG signals. The classifier module and the pre-processor module were implemented separately for easy testing and modification of different phases. The electrical signal from brain is captured using EEG and must be recorded during voluntary movement. When the brain does real time activities it must be detected and categorized into two dimensional movements. The non-invasive technique of recording EEG from the scalp is used for analyzing brain activity. This technique reduces the human mental workload and cost compared to invasive Technique. The excitation of the neurons is done using External audio and video feedback. The accuracy of the system is improved by combining Steady State Visually Evoked Potential (SSVEP) and Event Related Desynchronization (ERD) signals.

Results: The person suffering with Amyotrophic Lateral Sclerosis (ALS) is interfaced with HBMI. The HBMI generate electrical stimulation based on the subject's thought processing and in response to the stimulus the subject under test perform the desired movements of his/her body part. During the operation, the HBMI record the EEG signals, process it and classify it to different desired movements. The recorded operation is compared with the actual operations. The performance accuracy is measured. The performance accuracy is the number of correct classification divided by number of physical operations. A pair of EMG Electrodes must be placed on the identified body part. If the result is not satisfactory a Bio-feedback is given and the process is repeated till the performance accuracy is achieved.

Conclusions: The Hybrid brain muscle Interface (HBMI) will bypass the brain clotting and help the paralyzed person to move their paralyzed parts using brain stimulation without any Exo-skeleton. It is non-invasive and it does not require any exoskeleton for the motion. In it there is wireless connection between the brain and the controlled parts. Hybridization helps to classify the brain signals more accurately. Our findings will assist paralyzed person, and provide a better interface for the families, friends, and caretaker of the paralyzed person.

Acknowledgements: The part of the research was funded by EPICS in IEEE (Grant No. 2016-12).

011 | Seismocardiography system based on micromechanical sensors

Alexander Levkovich¹; Vladimir Achildiev¹; Viktor Soldatenkov¹; Mikhael Basarab²; Nicolay Bedro¹; Yury Gruzevich^{1,2}; Yuliya Evseeva¹; Natalya Konnova²; Mariya Komarova¹

¹Scientific Production Unity "GEOPHIZIKA-NV", St. Company, Moscow, Russia; ²Bauman Moscow State Technical University, Moscow, Russia

Objectives: The purpose is to develop new equipment and algorithm for non-invasive diagnostics based on the seismocardiography (SCG) method.

Methods: SCG method is based on the recording of mechanical vibrations of the chest that are associated with the activity of the heart and is used to investigate the *strength* of the heartbeat and perform the analysis of the cardiac cycle.

Results: The SCG signal is significantly different in its view from the electrocardiogram and carries much more information. As supposed, SCG will significantly increase the number of diagnosed diseases with higher accuracy. The basis of the *SCG system* is a micro-vibration sensor based on microelectromechanical (MEMS) accelerometers. To eliminate the effect of angular vibrations on the data samples from accelerometers a new design of SCG system is proposed that include MEMS gyroscopes for the angular rate measurement in addition to MEMS accelerometers. The design of the *SCG system* includes a three-axis MEMS accelerometer unit and a three-axis MEMS angular velocity unit, a microcontroller and other necessary chips and elements. To provide high performance and small processing time, a microcontroller with high clock frequency is selected, and commands and data are received and transmitted via the built-in RS-422/485 interface or bluetooth interface if wireless communication is required.

The result of data processing is the modulus of the acceleration vector of the heartbeat and the attitude angles in the wander frame. The SCG system algorithm uses three frames and initial data about relationships between them: the body frame related to the body of the SCG system, the anatomical frame related to the heart and human body and the wander frame.

During the signal processing, pulse waves are extracted by digital filtering of *discrete* in *time* and quantized in *amplitude* signals, amplitude selection of pulse signals, their temporal analysis and calculation of the pulse vector module from its three projections on the axis of the body frame and the angles of the direction of the vector. Digital signal processing includes the implementation of fast wave approximation algorithms with subsequent analysis of approximating functions key parameters. As functional bases, both global (polynomials) and local (splines, wavelets, etc.) systems are tested. The error of the

approximation is estimated depending on the dimension of the approximating space.

Conclusions: The result of the research is the experimental sample of SCG system based on MEMS accelerometer and angular velocity sensors. The conducted research confirms the correctness of the selected circuit and constructive solutions and operation algorithm. The algorithm of secondary filtration by using Chebyshev polynomials of the first kind is tested.

Acknowledgements: This work was supported by the Russian Fund of Fundamental Researches of the Russian Academy of Sciences (Grants No. 18-29-02019 mk).

012 | A remote diagnostic system for screening and early diagnostics of internals diseases

Vyacheslav Uspenskiy^{1,2}; Vladimir Achildiev¹; Viktor Soldatenkov¹; Alexander Baldin³; Nicolay Bedro¹; Yury Gruzevich^{1,3}; Natalie Konnova³; Roman Shabaev¹; Dmitry Zhuk³

¹Scientific Production Unity "GEOPHIZIKA-NV", St. Company, Moscow, Russia; ²Mandryka Medical Study-Scientific Clinical Centre, Moscow, Russia; ³Bauman Moscow State Technical University, Moscow, Russia

Objectives: The aim is to develop a new medicine concept, equipment and algorithms of non-invasive diagnostics based on the heart information function.

Methods: The method is based on the recording and information analysis of the electrocardiogram (ECG) signals, as the heart carries out information function, that is directly connected with the formation and maintenance of the information media of a human body, including a set of information entities of the norm, diseases and various conditions.

Results: The technology of information analysis of the ECG signals for diagnostics of internals diseases consists in simultaneous record by the ECG unit of 300-600 cardiac cycles in 1, 2, and 3 standard Einthoven assignments and subsequent analysis as it is described below.

Changes of the information entities of the norm and diseases, generated by the heart, reveal themselves in two ways. The first way is through changing activity of the information entities of the norm and diseases, which is based on the changing frequency of occurrence in a codified pattern of the man of symbol combinations included in the codified reference pattern. The second way is through the impermanence of information entity of certain diseases and the formation of the diseases report.

The conclusion about the presence of a norm or disease is taken out after, summarizing diagnostics data from the three assignments. The presence of norm or disease for each assignment measurement data is defined in the presence of a full character set of the appropriate standard.

For this purpose a new ECG unit was designed with an amplitude accuracy of 5 μV and a time intervals accuracy of 0.25 ms, that provides the expansion of the application scope and the opportunity of diagnostics of the bigger numbers of various internals diseases at any stage of development. A new remote diagnostic system for screening and early diagnostics of internals diseases is based on the high resolution ECG unit equipped with the special wireless interface. The system includes ECG unit providing signal compression, recording and transmission to the remote server. The remote server carries out the diagnostic algorithm using the set of informative attributes from initial ECG. Each type of disease corresponds to a code combination is compared to that of a healthy condition to define the probability and presence of a norm or diseases and generate the report.

Conclusions: The developed method, equipment and algorithm for non-invasive diagnostics of internals diseases based on the method of the information analysis of the ECG signals allows to diagnose more than 40 various diseases.

Acknowledgements: This work was supported by the Russian Fund of Fundamental Researches of the Russian Academy of Sciences (Grants No. 18-29-02019 mk).

013 | A new method of oncological diseases treatment with high reliability

Yury Gruzevich^{1,2}; Viktor Soldatenkov¹; Vyacheslav Shiryaev¹

¹Scientific Production Unity "GEOPHIZIKA-NV", St. Company, Moscow, Russia; ²Bauman Moscow State Technical University, Moscow, Russia

Objectives: The aims are development of a new equipment and algorithms for the distant high frequency electromagnetic low lever radiation system with automatic control for cancer patients named "Nadezhda".

Methods: The achieved medical effect is based on the selective influence on the cancer patient by the spectrum of high-frequency electromagnetic radiation of low intensity generated from nine frequencies discretely chosen in a determined combination of a radio range (100-1300 MHz), with the usage of second and third harmonics of the basic frequencies, with density of the electromagnetic energy less than 10 $\mu\text{W}/\text{cm}^2$ and directivity varied frequency modulation in limits from 0 to 200 Hz.

Results: The principle of therapeutic modality and achievement of the curative effect is provided due to the selective bimolecular absorption of the high-frequency electromagnetic radiation that leads to the change of its energetic state and in the future that doesn't permit these molecules gone in high-grade to take a full part in the process of cells proliferation. On the base of this method

medical equipment (named “Nadezhda”) was designed. Now equipment “Nadezhda” is used for the following effects achievement: tumor growth retardation; localization of generalized processes; reduction of pain syndrome within the 1-2 stages; improvement of immunological status; reduction of inflammatory processes and forming of the favorable situation for the acceleration of the anagenesis process; reduction of the weight of complications caused by chemotherapy and radial therapy; forming of the sedation. Besides in case of the medical equipment “Nadezhda” using it in combination with other methods of the treatment, it provides the mentioned above results, and also allows reducing used doses of radiation therapy to reduce negative effects of radial and chemotherapy and to get radio modifying effect in the case of radial therapy.

Clinical trials of medical equipment “Nadezhda” were carried out within nine years in 5 leading Russian oncological centers. In clinical trials have taken part more than 300 patients. During the clinical trials, the influence efficiency of the device on a condition of patients with clinical symptoms was estimated by antitumoral, wound healing, anesthetic and immunomodulatory effects, forming of the sedation, localization of generalized processes. In the report the main results of the objective and subjective effects after the therapeutic influence of the medical equipment “Nadezhda” will be given.

Conclusions: The influences of the medical equipment “Nadezhda” retards of the tumor and its metastasis approximately to 20%-25%, and also this equipment is perspective with regard to extension of the possibilities of its use for treatment of various diseases, including cancer, AIDS and tuberculosis, after realization of additional clinical tests and improvement of the treatments methods.

Acknowledgements: This work was supported by the Russian Fund of Fundamental Researches of the Russian Academy of Sciences (Grants No. 18-29-02019 mk).

014 | Piper betle formulated emulsion (O/W) effectiveness towards oral bacteria

W.F. Lee¹; S. Eraricar¹; J. Khairunadwa²

¹Bioprocess & Polymer Engineering Department, Faculty of Chemical and Energy Engineering, Universiti Teknologi Malaysia, Johor Bahru, Johor, Malaysia; ²Biosciences & Health Sciences Department, Faculty of Biosciences and Medical Engineering, Universiti Teknologi Malaysia, Johor Bahru, Johor, Malaysia

Background: *Piper betle* is a well-known traditional medicinal plant. Many natural antibacterial compounds can be found among extracted compounds from *Piper betle* plant. *Piper betle* leaves is widely used for medicinal purposes, and the extract and essential oils of *Piper betle*

leaves possess antibacterial activity. The purpose of this research was to investigate antibacterial activity of oil-in-water (O/W) *Piper betle* emulsions against dental cariogenic bacteria, *Streptococcus mutans* and *Staphylococcus aureus*. Emulsion with Tween 80 can solve the poor water solubility problem of hydrophobic bioactive compound in water based antimicrobial formulations.

Methods: The *Piper betle* emulsion was formulated using 20 kHz probe type ultrasonic processor. The emulsions was prepared by mixing 1 g *Piper betle* oil, Tween 80 with final volume 200 mL distilled water. The antibacterial activity of formulated emulsion was evaluated in vitro and the minimal inhibitory concentration (MIC) was determined by the macrodilution method. The bacterial killing kinetic was also evaluated for this formulated emulsion.

Results: The minimum inhibition concentration (MIC) of the *Piper betle* emulsion for *Streptococcus mutans* was 2.5 mg/mL and *Staphylococcus aureus* was 5 mg/mL. The time kill kinetics study showed that the formulated emulsion can act as microbiostatic agents. The time-kill curves clearly showed the ability of the *Piper betle* emulsion can reduce the bacterial population with time. The area under the curve (AUC) for *Piper betle* emulsion against *Streptococcus mutans* and *Staphylococcus aureus* revealed that the number of bacterial cells was significantly ($P < 0.05$) reduced when compared to the control sample.

Conclusions: The results proposed that, this formulated O/W *Piper betle* emulsion have a potential to be used as an antibacterial drug against *Streptococcus mutans* and *Staphylococcus aureus* for example use for the treatment of oral diseases. Further study should be conduct to investigate the cytotoxicity effect for this *Piper betle* emulsion.

015 | A MICCA-Based Clustering System for Rodent and Lagomorph Species Gene Sequence Clustering and Habitat Tracking

Eunjeong Choi¹; Dongkeun Kim²

¹Department of Computer Science, Sangmyung University, Seoul, Korea; ²Department of Intelligent Engineering Informatics for Human, Sangmyung University, Seoul, Korea

Objectives: Because of the recently increased interest in next-generation sequencing (NGS) technology research, it has become possible to analyze tens to thousands of gene pairs in a relatively short period of time. In addition, the frequency of reports on the clustering of the gene sequences of biological organisms continues to increase. Thus, this study aims to design a clustering system that can analyze the gene sequences, and then cluster and compare them to those of the actual species. This will provide the

Effect of Copper Slag and Granite Powder on the Mechanical Properties of Reclaimed Asphalt Pavement Aggregate Concrete

T.Mahitha¹, J. Aswini²

^{1,2} Department of civil engineering, APJ Abdul Kalam Technological University, Calicut, India

*Corresponding E-mail: mahi.thodiyil@gmail.com

Received 24 May 2018; Revised 20 November 2018; Accepted 5 December 2018

DOI: <https://10.30880/ijscet.2018.09.02.001>

Abstract

The replacement of natural gravel aggregate with reclaimed asphalt as coarse aggregate would help in reduction of environmental and ecological effects. Researches were rarely performed by replacing fine aggregate in reclaimed asphalt pavement aggregate concrete. This project aims to investigate the feasibility of improving the strength of recycled asphalt aggregate concrete in which recycled asphalt aggregate is used as a partial replacement of coarse aggregate at 30%. Abrasion and attrition technique is used to modify or roughen the surface of RAP aggregates. Granite powder and copper slag are used as a partial replacement of sand at 5, 10, 15, 20 and 25% in Abrasion and attrition Treated Reclaimed Asphalt Pavement Aggregate Concrete (ABTRAPC). Thirty cubes, twenty cylinders and twenty beams of concrete with granite powder and thirty cubes, twenty cylinders and ten beams of concrete with copper slag were made and tested. The 7th and 28th day strengths were found out at these replacements. It was observed that the compressive strength, split tensile strength and flexural strength was found to be maximum at 15% replacement of sand by copper slag. The compressive strength was increased about 29.8% compared to ABTRAPC. Flexural strength similar to normal concrete and about 12.8% greater compared to ABTRAP concrete. The compressive strength and flexural strength was also increased to a maximum at 15% replacement of sand by granite powder and split tensile strength at 20% replacement of granite powder. The results showed that the potential of reclaimed asphalt aggregates as a partial replacement of coarse aggregates in concrete could be effectively enhanced with its a combination with granite powder or copper slag. The increase in compressive strength values and the increase in flexural strength values similar to normal concrete proved that this concrete has its potential to be used in pavement applications.

Keywords: Reclaimed asphalt pavement aggregate, Abrasion, and attrition, Copper slag, Granite powder, Compressive strength, Flexural strength, Split tensile strength, Sustainability

1.0 Introduction

The current concrete construction practice is thought unsustainable due to the consumption of enormous quantities of stone, sand, drinking water and cement. To move towards ecological sustainability, we must move on to low cost and highly durable concrete mixtures containing largest possible amounts of industrial and urban byproducts that could be suitable as a partial replacement of Portland cement, aggregate and drinking water. Natural aggregate accounts for more than 70% of the volume of concrete. The increasing demand for quality natural aggregates and the subsequent effects on the environment led to the need to consider locally and cheaply available materials in concrete.

India has the second largest road network in the world. Reclaimed Asphalt Pavement (RAP) is the removed pavement materials composed of asphalt and aggregates. These materials are produced when asphalt pavements are removed during reconstruction and resurfacing. The replacement of gravel aggregate with reclaimed asphalt would also help in reducing the quantity of reclaimed asphalt which would otherwise be disposed of in landfill sites. The applications of concrete containing recycled asphalt have been very limited due to its low strength. Thus there is a need to find methods to improve the properties of concrete containing RAP as partial replacement of coarse aggregate. Partial replacement of fine aggregate of this concrete containing RAP with a suitable cheap and recyclable material is an interesting area of study. Granite powder is obtained as

a by-product from granite cutting or polishing industries. Granite powder is also generated from recycling marble tops, granite pavers and stone scraps. This powder is deposited in large amounts causing a threat to the environment. Inhalation of fine dust of granite powder causes lung diseases. The use of granite powder in concrete would minimize its effect on the environment. Copper slag is an industrial by-product material produced from the process of manufacturing copper. Approximately 24.6 million tons of slags are estimated to be generated from the copper industries in the world. Some amount of copper slag is mainly used in the sand blasting industry and in the manufacturing of abrasive tools and the remaining is disposed of in the ecosystem without any reuse.

2.0 Literature Review

Reference [1] studied on fine fraction of Reclaimed Asphalt Pavement (RAP) aggregates as an alternative to natural fine aggregates. Cement mortar samples were prepared with 25%, 50%, 75% and 100% replacement of natural aggregates. The decrease in strength of cement mortar may be due to the increase in the porosity of Interfacial Transition Zone (ITZ) and the predominance of asphalt-cohesion failure in comparison to asphalt adhesion failure. It also opens up the scope to incorporate mineral admixtures in mortar mixes to improve the strength of the same with a higher percentage of RAP content. Reference [2] investigated the effect of using copper slag replacement by preparing eight concrete mixes with different proportions of copper slag (0-100%). The compressive, tensile and flexural strength of concrete was comparable to the control mix using up to 50% copper slag. Copper slag, in the range of 40–50%, could potentially replace sand in concrete mixtures. Al-Mufti et al. [3] investigated improving the strength properties of recycled asphalt aggregate concrete. Replacement of 20 mm gravel with recycled asphalt aggregate at 25%, 50%, 75% were compared with 100% recycled asphalt aggregate concrete and control concrete. A replacement of 25% reduces 28 days strength by 27%. Further increase in replacement results in further reduction in strength but at a more reduced rate. Roughening of aggregate prior to mixing for 3 hour increases the strength reaching similar strength to normal concrete. Roughening of recycled asphalt aggregate alone for 3 hours made a limited improvement in concrete strength. The treatment of recycled asphalt aggregate with solvent turpentine has no effect on strength development of concrete.

Reference [4] studied bonding properties in cementitious materials with asphalt-coated particles. Interfacial Transition Zone (ITZ) properties and phase distribution with age of reclaimed asphalt showed high porosity, larger ITZ size, low CH and CSH contents near the interface. This caused a reduction in concrete strength and bulk modulus. Hydrophobic nature of asphalt prevented hydration products from growing around aggregate in larger and porous ITZ. Mortars with RAP showed a decreasing trend in the CH content near the aggregate interface suggesting that somehow asphalt is preventing CH growth. Even though the silica fume decreased the porosity to some extent, the CH content is found to reduce with age due to the pozzolanic reaction of silica fume. Reference [5] studied the nature of the cement-asphalt bond. The interfacial cement-asphalt bond energy was found to improve by several chemical oxidative treatments of the asphalt without affecting the porosity and size factors in the ITZ. Asphalt cohesion is found out to be as the preferential failure mode than the cement-asphalt adhesion or ITZ cohesion. A lower bulk modulus is produced due to the higher porosity in ITZ which allows for easier crack initiation, and the preferential asphalt cohesion failure. An improvement in the concrete the mechanical properties in concrete with RAP aggregates would be improved by increasing the cohesive strength of the asphalt coating thus driving the failure mode to an asphalt-cement adhesive and decreasing the ITZ porosity. Reference [6] studied the use of fractionated reclaimed asphalt pavement (FRAP) as a partial replacement (0%, 20%, 35%, and 50%) of coarse aggregate in a ternary blend concrete containing cement, slag, and fly ash. The increase in the percentage of FRAP in concrete resulted in a decrease in the compressive, split tensile, and flexural strength. The elastic and dynamic moduli also decreased with increasing FRAP content. The results of the study indicated that up to 35% FRAP can be replaced as coarse aggregates while still meeting the sufficient fresh, strength, and durability

specifications of conventional concrete. Dirty FRAP without washing was found to meet the IDOT compressive strength requirements up to 50% replacement. Reference [7] studied on the potential of blasted copper slag as fine aggregate in Portland cement concrete. The greatest reductions of compressive strength were found when the replacement was over 40%.

Reference [8] conducted studies on soft and hard bitumen from unaged, aged recycled asphalt concrete mixtures for rheological, thermal, microstructural aspects. Bitumen with 50% weight of virgin bitumen and 50% from recycled asphalt pavements were studied. Aging and recycling changed rheological properties of soft bitumen by increasing complex modulus and decreasing phase angle. Recycled asphalt pavement bitumen has an adverse effect on adhesion properties. Reference [9] conducted an experimental study of concrete made with granite and iron powders as partial replacement of sand. The test resulted showed that for 10% ratio of granite powder in concrete, the increase in compressive strength was about 30% compared to normal concrete. Similar results were obtained for flexure. For replacement, up to 20% of sand by weight with iron powder in concrete resulted in an increase in compressive and flexural strength.

Reference [10] conducted studies on experiments with control concrete with natural sand and gravel, concrete with reclaimed coarse and reclaimed fine aggregate, concrete with reclaimed coarse and natural sand, and concrete mix with reclaimed coarse and natural sand where 30% OPC replaced with flash. Concrete made with reclaimed coarse asphalt aggregates and sand showed less reduction in strength compared to others. Reference [11] studied on RAP aggregate materials treated with different dosages of portland type I/II cement and with alkali-resistant glass fibers. Reference [12] investigated on portland cement concrete containing recycled asphalt aggregate. Soft asphalt binder induces stress concentration and microcracking in concrete matrix causing a reduction in strength. Concrete made with only coarse RAP showed the least reduction in strength and a significant increase in toughness. Compared with rubber, RAP had a better chance of replacement in concrete. Reference [13] studied the durability of copper slag contained concrete exposed to sulfate attack. Replacement of cement with copper slag up to 15% led to more than 50% decrease in sulfate expansion. Reference [14] experimentally investigated the feasibility of granite powder waste as a possible replacement in manufacturing concrete. At 0.5 water to cement ratio, experiments were done for 10, 25, 40, 55 and 70% sand replacement by granite powder. Compressive strength results for 7, 28, and 56 days were highest at 25% replacement and lowest at 70% replacement.

Reference [15] studied the effect of incorporating Dirty RAP (DRAP) Washed RAP (WRAP), and Abrasion and Attrition (AB&AT) treated RAP on the fresh, mechanical and durability properties of concrete and compared with each other as well as normal aggregate concrete. Beneficiation of RAP by AB&AT method increased the compressive strength of concrete by 9.74% and 12.21% and flexural strength by 6.05% and 8.55% as compared to WRAP and DRAP inclusive concrete. ABTRAP aggregates were found to possess both the desirable properties of RAP as well as natural aggregates. Aggregates processed with both washing and AB&AT method resulted in better workability than natural aggregate concrete. Reference [16] studied on improving the properties of ABTRAP (Beneficiated RAP aggregates by Abrasion & Attrition technique) inclusive concrete by incorporating mineral admixtures such as Silica Fume (SF), Fly ash (FA) and Sugarcane Bagasse Ash (SCBA). 6 mixes were prepared by partially replacing Ordinary Portland Cement (OPC) by SF (5% & 10%), FA (10% & 20%) and SCBA (5% & 10%). Maximum improvement in compressive, flexural and split tensile strength of ABTRAPC mix was found when 10% OPC was partially replaced by SF followed by 20% replacement by FA and 5% replacement by SCBA.

Reference [17] found out that replacement of 10% cement by BGA was found to increase the compressive strength by 15%, modulus of rupture by 12%, and splitting strength by 13% compared to concrete containing 100% RAP aggregates. Shi et al. [18] investigated the viability of partial replacement of virgin coarse aggregate by coarse RAP to formulate PCC paving mixtures. Replacing virgin coarse aggregate by RAP in a typical PCC pavement mix has caused a reduction in strength and modulus of elasticity. The coarse RAP with sufficient intermediate size particles can help to make dense graded RAP-PCC mixtures which can show better workability and

mechanical properties compared to other gap-graded RAP-PCC mixtures. Reference [19] studied the strength and durability properties of concrete made with granite industry waste. The obtained test results were indicated that the replacement of natural sand by GP waste up to 15% of any formulation is favorable for the concrete making without adversely affecting the strength and durability criteria.

Reference [21] investigated the effect of using alternatives for both fine and coarse aggregates with copper slag (30%, 40% and 50%), iron slag (30%, 40% and 50%) and recycled concrete aggregate (20%, 25% and 30%) with various proportions of mix by the partial replacement of sand and gravel respectively. From the study, it has been concluded that 40% of copper slag, 40% iron slag and 25% of recycled concrete aggregate possess more strength than a conventional concrete mix. Reference [22-23] studied the interactions between granites and asphalts based on theology. Different granite powders and asphalt showed significant differences in their interactions and this compatibility problem between asphalt and granite should be considered during the choice of materials.

3.0 Research Significance

Granite powder and copper slag are industrial by-products obtained from the granite cutting and copper manufacturing industries. These can be used as partial replacement of sand in concrete. RAP aggregates are obtained during the reconstruction or resurfacing of pavements. These aggregates, when used as coarse aggregate in concrete, have shown to decrease the mechanical properties of concrete. The modification of RAP coarse aggregates by abrasion and attrition and the partial replacement of sand in the concrete by granite powder or copper slag is an interesting area of research. The use of RAP aggregates, granite powder and copper slag in concrete will reduce the consumption of natural resources in the construction process. The health hazards and the effects on the ecosystem will also be reduced by the recycling of these byproducts.

4.0 Experimental Investigation

The experimental investigation comprised of preparing specimens of normal concrete, concrete with RAP aggregate replaced as coarse aggregate at 100%, concrete with RAP aggregate replaced as coarse aggregate at 30%, concrete with RAP aggregate replaced as coarse aggregate at 30% after abrasion, and abrasion treated RAP concrete with granite powder or copper slag replacement. The specimens comprised of concrete cubes, beams, and cylinders for testing the compressive strength, flexural strength and split tensile strength respectively. The concrete mix consists of Portland Pozzolana Cement, coarse aggregates, RAP aggregates, m-sand, granite powder or copper slag, superplasticizer and water.

4.1. Materials

The materials used for the study included Portland Pozzolana Cement coarse aggregates (gravel) RAP aggregates, fine aggregates (m-sand), granite powder, copper slag, superplasticizer, and water. Portland Pozzolana Cement (PPC) conforming to (IS 1489 part1) fly ash based is used for the experimental work. The specific gravity of cement is 2.89 found using le chatelier flask method as per IS 2720 part3. Reclaimed Asphalt Pavement aggregates and natural aggregates are used as coarse aggregates in this experiment. Reclaimed Asphalt Pavement Aggregates were collected from the highway works in Calicut. Dirty Reclaimed Asphalt Pavement Aggregates were used for the work without washing. Natural coarse aggregates of size passing through 20 mm sieve and retained on 12.5 mm sieve are taken. Reclaimed Asphalt Pavement aggregates of size passing through 20 mm sieve and retained on 12.5 mm sieve are taken. The specific gravity of coarse aggregates and RAP aggregates are 2.66 and 2.35 respectively. M-Sand, granite powder and copper slag are used as fine aggregates. Granite powder is collected from Cemal Gems & Minerals,

Bangalore. Copper slag is collected from Blastine private Limited, Koratty, Kerala. Chemical composition analysis results for granite powder and copper slag were obtained from their suppliers i.e. Cemal Gems & Minerals and Blastine private limited respectively. The chemical composition of granite powder and copper slag are given in Table 1 and Table 2 respectively. Specific gravities of m-sand, granite powder, and copper slag are 2.6, 2.5 and 3.2 respectively found out using a pycnometer test as per IS-2386 part-3. Fineness modulus of m-sand, granite powder, and copper slag are 3.44, 2.64 and 3.43 respectively. Sieve analysis test was conducted according to IS 2386 part-1. Gradation curves for fine aggregates are shown in Fig.1. High range water reducing super plasticizer Glenium B233 of specific gravity 1.09 is used for the experiment.

Table 1: Chemical composition of granite powder

Particulars	Values
SiO ₂	72.04%
Al ₂ O ₃	14.42%
K ₂ O	4.12%
Na ₂ O	3.69%
CaO	1.82%
FeO	1.68%
Fe ₂ O ₃	1.22%
MgO	0.71%
TiO ₂	0.3%
P ₂ O ₅	0.12%
MnO	0.05%

Source: Batch Inspection Certificate, Cemal Gems, and Minerals, Bangalore

Table 2: Chemical composition of copper slag

Constituent	Percentage weight
Silica, SiO ₂	26- 30 %
Free Silica	< 5%
Alumina, Al ₂ O ₃	2%
Iron Oxide, FeO	42-47%
Calcium Oxide, CaO	1-2 %
Magnesium Oxide, MgO	1.04 %
Copper Oxide, CuO	6.1 % max
Sulfates	0.13 %

Source: Batch Inspection Certificate, Blastline Pvt.Ltd

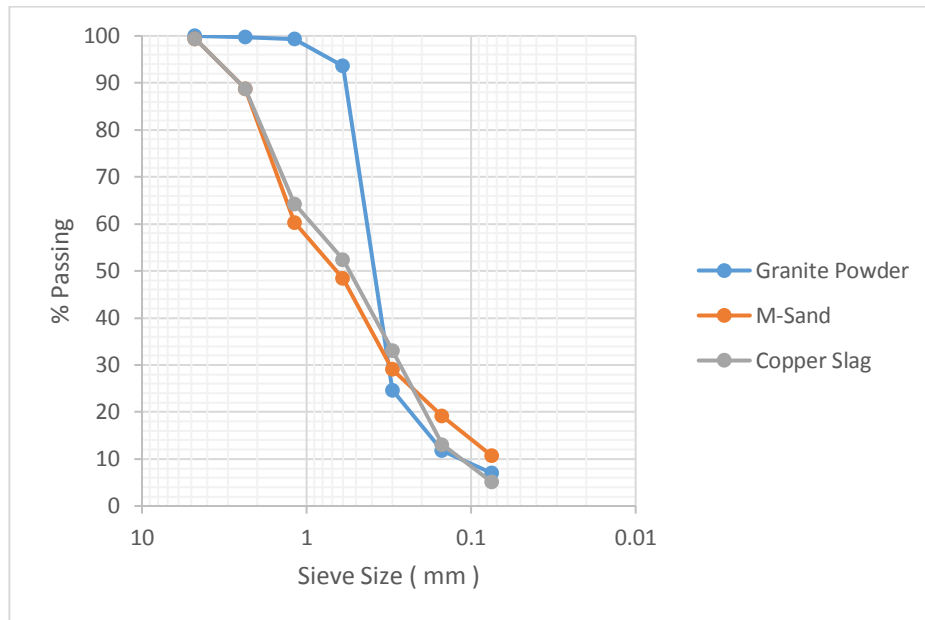


Figure 1: Particle size distribution curves of fine aggregates

4.2 Mix Design of Concrete

Concrete mixtures were prepared with recycled asphalt pavement aggregates as coarse aggregates and granite powder or copper slag as partial replacement of fine aggregate at various percentages i.e. 0% (for the control mix), 5%, 10%, 15%, 20%, and 25%. The control mixture was designed to have a target 28 day compressive strength of 30 N/mm² (M-30). The mix design obtained is 1:0.43:2.13:2.89 as per IS 10262-2009. Slump test was conducted at admixture dosages of 0.4, 0.45 and 0.5% by mass of cementitious material. As better slump value and mix was obtained at 0.4% dosage, admixture dosage is fixed as 0.4% by mass of cementitious material for all mixes except for the abrasion treated RAP aggregate concrete mix with granite powder replaced as fine aggregate at 20 and 25% in which the dosage is increased to 0.42 and 0.43% by mass of cementitious material.

4.3 Reference Specimens and Abrasion Process

Reference specimens like Normal Aggregate Concrete (NAC), concrete with RAP aggregate replaced as coarse aggregate at 100% (RAPC), concrete with RAP aggregate replaced as coarse aggregate at 30% (R-APC) and concrete with RAP aggregate replaced as coarse aggregate at 30% after abrasion (ABTRAPC) were cast. Los Angeles abrasion test was conducted according to IS 2386 part-4.

The principle of Los Angeles abrasion test is to produce abrasive action by use of standard steel balls which when mixed with aggregates and rotated in a drum for a specific number of revolutions also cause an impact on aggregates. In the modification process, Los Angeles Abrasion Testing Machine is used to do the abrasion process. The machine consists of a hollow cylinder, mounted on a steady frame on ball bearings. It has a detachable shelf which extends throughout the inside length of the drum. The drum is rotated at a speed of 30-33 rpm by an electric motor through a heavy reduction gear. Abrasive charge i.e., cast iron or steel balls, approximately 48mm in diameter and each weighing between 390 to 445 g of twelve numbers are used. Optimum duration time for the abrasion process is fixed at 10 minutes as longer duration resulted in fractured aggregates which might cause a loss in load transfer efficiency. As a number of abrasive charge increases, reduction in asphalt content also increases. Therefore 10 steel balls were selected for the abrasion process. Input quantity of Reclaimed Asphalt Pavement (RAP) Aggregates in the machine

was selected based on the materials passing 4.75 mm sieve after the abrasion process as per Table 3. When the number of aggregates was 30 kg, maximum attrition took place and hence the input quantities of aggregates were fixed as 30 kg. Bitumen content was found to reduce about 40.4% by centrifugal extraction method.

Table 3: Percentage passing through 4.75 mm sieve

RAP (kg)	15	20	25	30	35
Passing 4.75 mm Sieve (%)	4.02	5.15	6.2	6.63	6.38

4.4. Preparation of Test Specimens with Granite Powder and copper slag

Granite powder and m-sand were mixed thoroughly. Natural coarse aggregate and RAP aggregates modified by abrasion were mixed thoroughly and added to the mix. Once all materials were mixed thoroughly, superplasticizer was added to water and this water is added to the concrete mix. Hand mixing was done thoroughly. Specimens like 150X150X150 mm cubes, 100X100X500 mm beams, 150 mm X 300 mm cylinders were prepared using the concrete mix. After pouring into molds compaction of 25 blows was done using compaction rod in three layers. After finishing the surface, molds are dried for 24 hrs. After the removal from molds, the specimens are cured in an open water tank for a period of 28 days. The percentages of granite powder used were 5%, 10%, 15%, 20% and 25 of sand by weight designated by GP05, GP10, GP15, GP20, and GP25 respectively. Preparation of concrete specimens with copper slag was similar to those of granite powder specimens. The percentages of copper slag used were 5%, 10%, 15%, 20% and 25 of sand by weight designated by CS05, CS10, CS15, CS20 and CS25 respectively.

5.0 Testing of Fresh and Hardened Properties in Concrete

Slump test is done to check the workability of freshly made concrete. Concrete cubes, beams, and cylinders were used for testing the compression tests, flexural tests and split tensile strength tests into cubes, beams, and cylinders respectively. Compressive strength test, Flexural strength test and split tensile strength test were done according to IS 516-1959 at the 7th and 28th day. 24 cubes, 16 beams, and 16 cylinders were prepared as the reference specimens. Thirty cubes, twenty cylinders, and twenty beams were prepared each for granite powder and copper slag concrete mix in total. Slump variations for concrete mixes are given in Fig.2.

6.0 Slump Test Results

Reclaimed Asphalt Pavement Aggregate Concrete mixes were more workable compared to normal concrete mixes and are high due to its small particle size and larger fineness. These mixes were less workable at higher percentage replacements, especially above 15%. Concrete mixes with copper slag were highly workable and the problem of bleeding occurred at replacements above 15%.

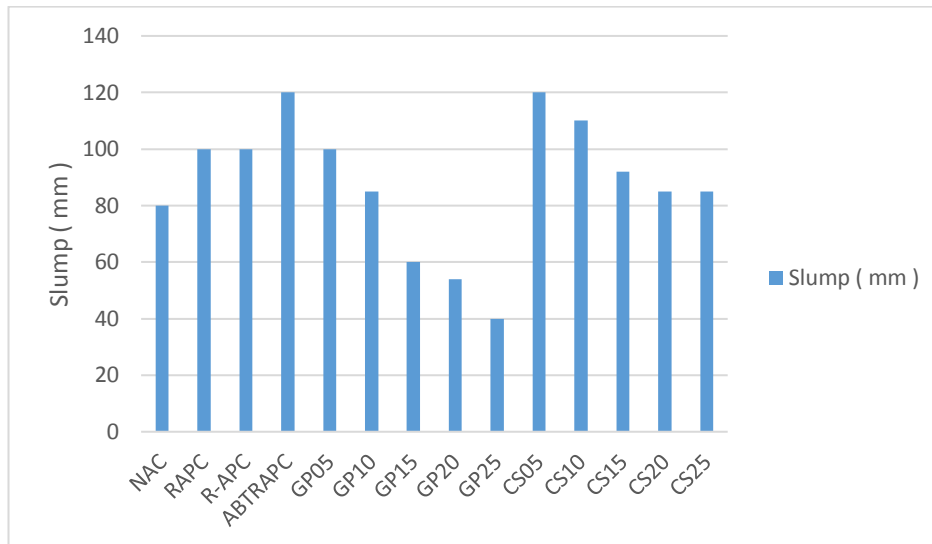


Figure 2: Slump variations for concrete mixes

7.0 Hardened Concrete Test Results

Strength tests were performed at the 7th and 28th day. Hardened concrete test results were obtained as an average of three specimens for each mix. A Compressive strength of 37.55 N/mm² is obtained for the NAC at 28 days. RAPC showed a reduction in strength of 62.13% (14.22 N/mm²) compared to NAC. R-APC showed a reduction in strength of 34.32% (24.66 N/mm²) compared to NAC. ABTRAPC showed a reduction in strength of 33.44% (24.99 N/mm²) compared to NAC and it exhibits the least reduction in strength. Fig.3 and Fig.4 show the compressive strength of cubes with different proportions of (GP) and (CS) respectively. A Flexural strength of 7.62 N/mm² is obtained for the NAC at 28 days. RAPC showed a reduction in strength of 40.94% (4.5 N/mm²) compared to NAC. R-APC showed a reduction in strength of 32.15% (5.17 N/mm²) compared to NAC. ABTRAPC showed a reduction in strength of 11.41% (6.75 N/mm²) compared to NAC and it exhibits the least reduction in strength. A split tensile strength of 2.63 N/mm² is obtained for the NAC at 28 days. RAPC showed a reduction in strength of 61.21% (1.02 N/mm²) compared to NAC. R-APC showed a reduction in strength of 28.89% (1.87 N/mm²) compared to NAC. ABTRAPC showed a reduction in strength of 24.33% (1.99 N/mm²) compared to NAC and it exhibits the least reduction in strength. Split tensile strength of ABTRAPC mixes (1.99 MPa) were 6.41% greater than R-APC mixes. Strength values of reference specimens are given in Table 4. Strength values of specimens with granite powder and copper slag are given in Table 5 and Table 6 respectively.

Table 4: Strength values of reference specimens

MIX	Average Compressive Strength (N/mm ²)		Average Flexural Strength (N/mm ²)		Average Tensile Strength (N/mm ²)	
	7 days	28 days	7 days	28 days	7 days	28 days
NAC	24.22	37.55	5	7.62	2.13	2.63
RAPC	6.505	14.22	0.17	4.5	0.78	1.02
R-APC	18.75	24.66	5.12	5.17	1.52	1.87
ABTRAPC	20.10	24.99	6	6.75	1.71	1.99

Table 5: Strength values of specimens with granite powder

MIX	Average Compressive Strength (N/mm ²)		Average Flexural Strength (N/mm ²)		Average Tensile Strength (N/mm ²)	
	7 days	28 days	7 days	28 days	7 days	28 days
GP05	14.99	18.55	3.87	4.75	1.83	1.96
GP10	17.22	19.66	4.55	4.92	1.93	1.98
GP15	23.12	30.99	5.87	6.12	1.96	1.99
GP20	19.56	25.37	4.55	6	1.8	2.08
GP25	14.48	17.82	3.77	4.25	1.2	1.37

Table 6: Strength values of specimens with copper slag

MIX	Average Compressive Strength (N/mm ²)		Average Flexural Strength (N/mm ²)		Average Tensile Strength (N/mm ²)	
	7 days	28 days	7 days	28 days	7 days	28 days
CS05	16.37	30.77	4.62	6.37	1.95	2.41
CS10	22.21	31.84	5.00	6.67	1.94	2.46
CS15	23.19	32.46	5.05	7.62	1.99	2.67
CS20	20.26	24.31	5.00	6.87	1.95	2.59
CS25	17.45	22.71	4.87	6.8	1.92	2.38

A maximum strength of 30.99 MPa is achieved by granite powder mixes at 15 % replacements at 28th day and it is equal to an increase of 24% compared to ABTRAPC mix. At 20% replacement it showed an increase of 1.52 % compared to ABTRAPC and at 25% replacement, strength decreased to 17.82 MPa.

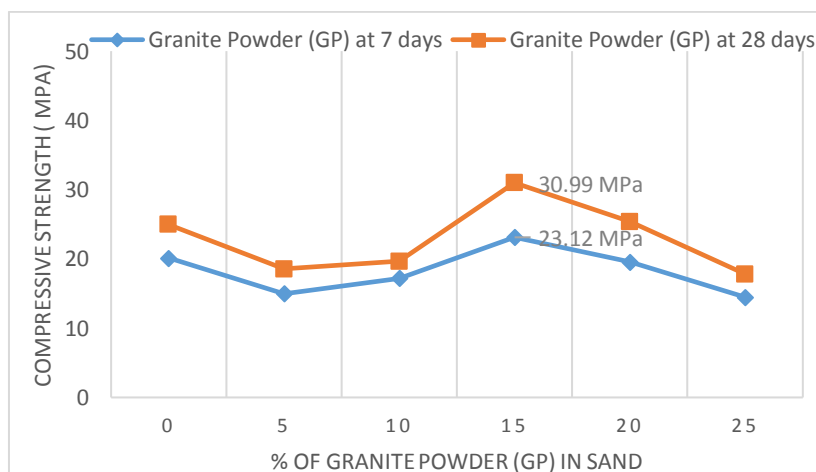


Figure 3: Compressive strength of cubes with different proportions of (GP)

Copper slag at 5% replacement itself shows an increase of 23.12% (30.77 MPa) compared to ABTRAPC mix. A maximum strength of 32.46 MPa is achieved by copper slag mixes at 15 % replacements at 28th day and it is equal to an increase of 29.89% compared to ABTRAPC mix. At 20% strength decreases to 24.31 MPa and decreases further.

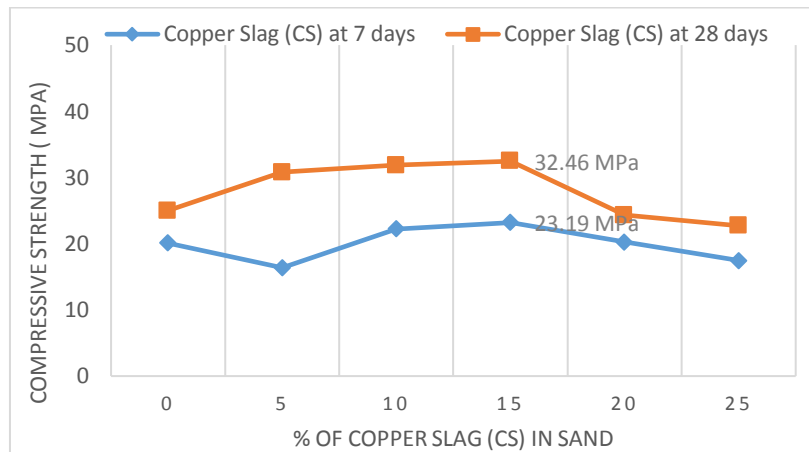


Figure 4: Compressive strength of cubes with different proportions of (CS)

Fig.5 and Fig.6 shows the flexural strength of beams with different proportions of (GP) and (CS) respectively.

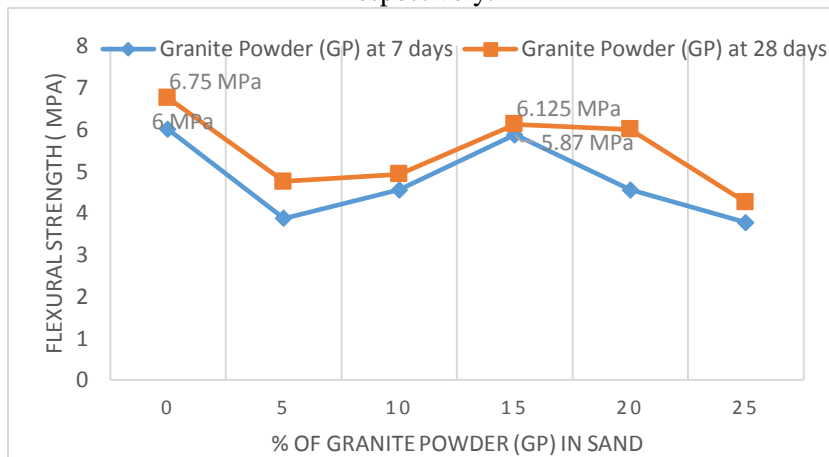


Figure 5: Flexural strength of a beam with different proportions of (GP)

Abrasion process increased the bending strength (5.17MPa) by 30.5% comparing to non-abrasion treated aggregates (6.75 MPa) at 28 days. At 15% replacement of fine aggregate with granite powder, a flexural strength of 6.12 MPa is obtained which shows a reduction of 9.3% compared to abrasion treated RAP aggregates (6.75 MPa) at 28 days. At 15% replacement of fine aggregate with copper slag, a flexural strength of 7.62 MPa is obtained which is similar to that of normal concrete and about 12.8% greater compared to ABTRAP concrete mix at 28 days. All mixes with copper slag exhibited greater flexural strength than granite powder mixes and all other reference mixes.

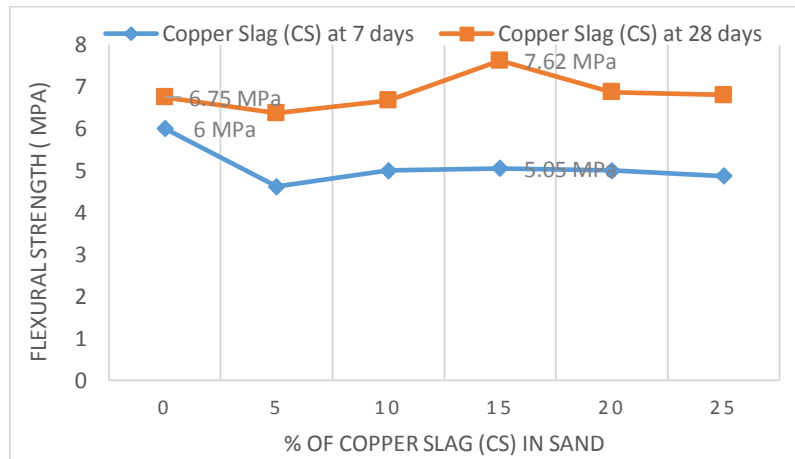


Figure 6: Flexural strength of a beam with different proportions of (CS)

Split tensile strength increased with an increase in the percentage of granite powder replacements up to 20% with a maximum of 2.08 MPa at 20% replacement and decrease further. A maximum split tensile strength of 2.67 MPa is obtained at 15% replacement of fine aggregate with copper slag which shows an increase of 1.52% compared to normal concrete and 34.17% compared to ABTRAP mixes. Fig.7 and Fig.8 shows the split tensile strength of cylinders with different proportions of (GP) and (CS) respectively.

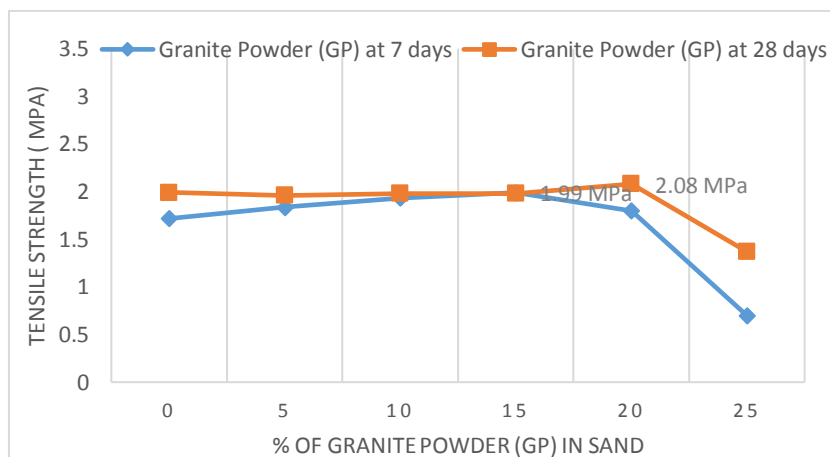


Figure 7: Split tensile strength of cylinders with different proportions of (GP)

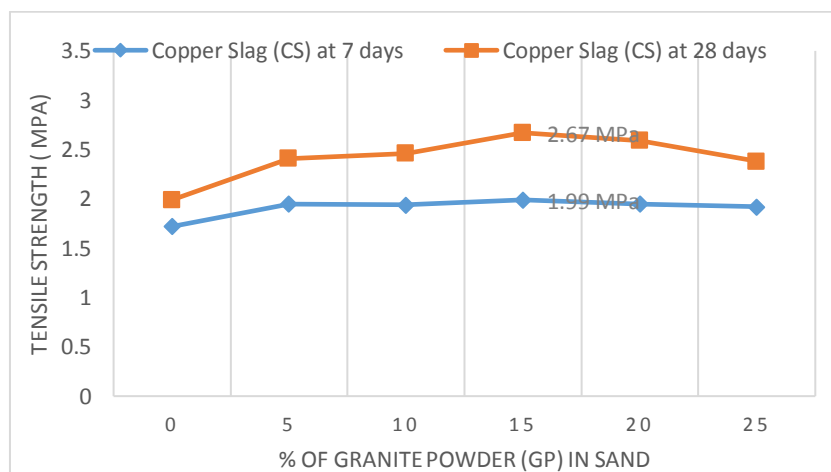


Figure 8: Split tensile strength of cylinders with different proportions of (CS)

8.0 Comparison of Test Results

Compressive strength increased with an increase in the percentage of replacement of granite powder up to 15% compared to ABTRAPC and increase in this case was 24%. Maximum flexural strength was obtained at 15% replacement even though it exhibited a reduction of 9.3% compared to ABTRAPC. Maximum split tensile strength is obtained at 20% and the increase was 4.52% compared to ABTRAPC. Compressive strength increased with an increase in the percentage of replacement of copper slag up to 15% and there was an increase of 29.89% compared to ABTRAPC. Maximum flexural strength was obtained at 15% replacement similar to normal concrete and 12.8% compared to ABTRAPC. Maximum split tensile strength is obtained at 15% and the increase was 1.52% compared to normal aggregate concrete and 34.17% compared to ABTRAPC. Replacements at 25% showed the least water absorption and more resistance to acid attack.

Fig.9 shows a comparison of compressive strength of concrete with granite powder and copper slag. Comparing the results of GP and CS, it is observed that up to 15% replacements, CS exhibited a higher compressive strength. At 20%, the compressive strength of GP increases and at 25% maximum strength was exhibited by CS.

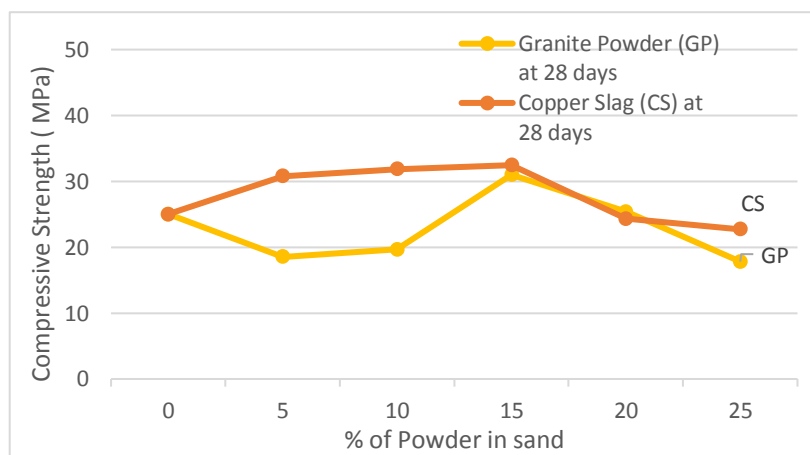


Figure 9: Effect of % of (GP) and (CS) on the Compressive Strength of Concrete

Fig.10 shows a comparison of flexural strength of concrete with granite powder and copper slag. Comparing the results of GP and CS, it is observed that at all replacements, CS exhibited a higher flexural strength comparing to GP.

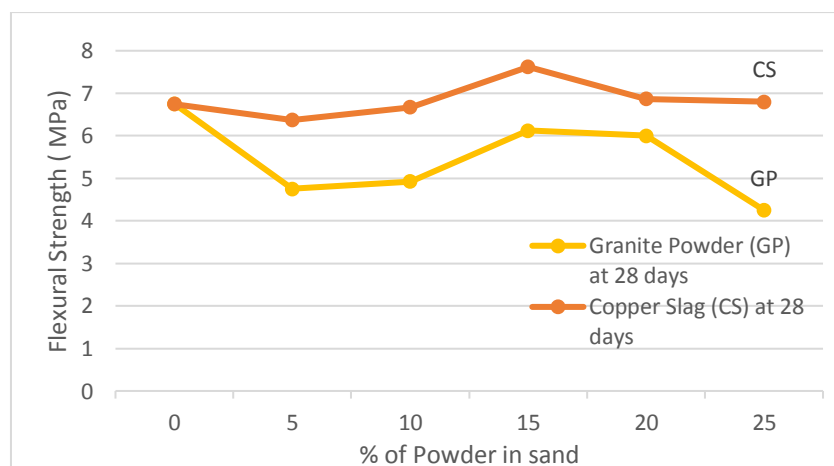


Figure 10: Effect of % of (GP) and (CS) on the Flexural Strength of Concrete

Fig.11 shows a comparison of the split tensile strength of concrete with granite powder and copper slag. Comparing the results of GP and CS, it is observed that at all replacements, CS exhibited a higher split tensile strength comparing to GP.

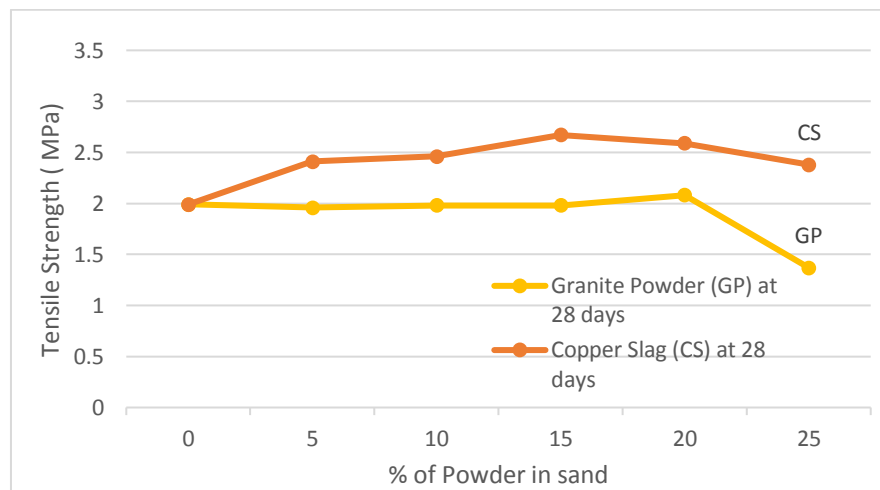


Figure 11: Effect of % of (GP) and (CS) on the Tensile Strength of Concrete

9.0 Conclusions

Based on the test results, the following conclusions can be made.

1. Abrasion and attrition improved the workability, mechanical and durability properties in concrete than the concrete with reclaimed pavement aggregates without abrasion since now the aggregate surface is more available to bonding with mortar and aggregates.
2. Workability of concrete mixes with granite powder and copper slag were good up to 15% of replacement. High water absorption of granite powder caused poor compactness and porosity and low water absorption property of copper slag caused bleeding above the replacement rates.
3. M30 grade concrete mix was developed by using reclaimed asphalt pavement aggregates as a partial replacement of coarse aggregate and granite powder as a fine aggregate at 15% and copper slag as a fine aggregate at 5, 10 and 15%.
4. Granite powder replaced at 15% showed a compressive strength of 23.12 MPa at 7th day and a maximum strength of 30.99 MPa at 28th day. Compressive strength gain of 34.03% was attained in the 28th day. Strength at 15% replacement is about 24% greater than the ABTRAPC specimens and strength at 20% replacement is 1.52% greater than the ABTRAPC specimens. Granite powder specimens developed strength ranging from 18.55MPa, 19.66 MPa, 30.99 MPa, 25.37 MPa, and 17.82 MPa at 5, 10, 15, 20 and 25 % replacements respectively.
5. Copper slag replaced at 5% itself showed a compressive strength similar to that attained by granite powder at 15% and it is 23.12% greater than ABTRAPC. Copper slag replaced at 15% showed a maximum strength 29.89% greater than ABTRAPC of 23.12 MPa at 7th day and a maximum strength of 30.99 MPa at 28th day. Compressive strength gain of 34.03% was attained in the 28th day. Strength at 15% replacement is about 24% greater than the ABTRAPC specimens and strength at 20% replacement is 1.52% greater than the ABTRAPC specimens. Copper slag specimens developed strength ranging from 30.77MPa, 31.84 MPa, 32.46 MPa, 24.3 MPa, and 22.7 MPa at 5, 10, 15, 20 and 25 % replacements respectively.
6. At 15% replacement of fine aggregate with granite powder, a flexural strength of 6.12 MPa is obtained which shows a reduction of 9.3% compared to abrasion treated RAP aggregates (6.75 MPa) at 28 days.
7. At 15% replacement of fine aggregate with copper slag, a flexural strength of 7.62 MPa is obtained which is similar to that of normal concrete and about 12.8% greater compared to

ABTRAP concrete mix at 28 days. All mixes with copper slag exhibited greater flexural strength than granite powder mixes and all other reference mixes.

8. Split tensile strength increased with an increase in the percentage of granite powder replacements up to 20% with a maximum of 2.08 MPa at 20% replacement which is 4.52% greater than ABTRAPC and decrease further. A maximum split tensile strength of 2.67 MPa is obtained at 15% replacement of fine aggregate with copper slag which shows an increase of 1.52% compared to normal concrete and 34.17% compared to ABTRAP mixes.

Conflict of Interest Statement

On behalf of all authors, the corresponding author states that there is no conflict of interest.

References

- [1] S. Abraham and G. Ransinchung, "Strength and permeation characteristics of cement mortar with Reclaimed Asphalt Pavement Aggregates", *Construction and Building Materials*, vol. 167, pp. 700-706, 2018.
- [2] K. Al-Jabri, A. Al-Saidy, and R. Taha, "Effect of copper slag as a fine aggregate on the properties of cement mortars and concrete", *Construction and Building Materials*, vol. 25, no. 2, pp. 933-938, 2011.
- [3] R. Al-Mufti and A. Fried, "Improving the strength properties of recycled asphalt aggregate concrete", *Construction and Building Materials*, vol. 149, pp. 45-52, 2017.
- [4] Brand and J. Roesler, "Bonding in cementitious materials with asphalt-coated particles: Part I – The interfacial transition zone", *Construction and Building Materials*, vol. 130, pp. 171-181, 2017.
- [5] A. Brand and J. Roesler, "Bonding in cementitious materials with asphalt-coated particles: Part II – Cement-asphalt chemical interactions", *Construction and Building Materials*, vol. 130, pp. 182-192, 2017.
- [6] Brand, A, fractionated reclaimed asphalt pavement as a coarse aggregate replacement in a ternary blended concrete pavement, Report ICT-12-008, Illinois State Toll Highway Authority, Downers Grove, 2012.
- [7] Dos Anjos, M. A. G., Sales, A. T. C., and Andrade, N. "Blasted Copper Slag as Fine Aggregate in Portland Cement Concrete", *Journal of environmental management*, vol. 96, 607-613, 2017.
- [8] Dos Santos, S., Party, M. N., and Poulikakos, L. D. "From Virgin to Recycled Bitumen: A Microstructural View", *Composites Part B: Engineering*, vol. 80, pp. 177-185, 2015.
- [9] Ghannam, S., Najm, H., and Vasconez, R. "Experimental Study of Concrete made with Granite and Iron Powders as Partial Replacement of Sand", *Sustainable Materials and Technologies*, vol. 9, pp. 1-9, 2016.
- [10] Hassan, K. E., Brooks, J. J., and Erdman, M. "The Use of Reclaimed Asphalt Pavement (RAP) Aggregates in Concrete", *Waste management series*, (Vol. 1, pp. 121-128), 2000.
- [11] M. S. Shahbaz, R. Z. R. M. Rasi, M. F. Bin Ahmad, and F. Rehman, "What is supply chain risk management? A review," *Adv. Sci. Lett.*, vol. 23, no. 9, pp. 9233–9238, 2017.
- [12] Hoyos, L. R., Puppala, A. J., and Ordonez, C. A. "Characterization of Cement-Fiber-Treated Reclaimed Asphalt Pavement Aggregates: Preliminary Investigation", *Journal of Materials in Civil Engineering*, vol. 23, pp. 977-989, 2017.
- [13] Huang, B., Shu, X., and Li, G. "Laboratory Investigation of Portland Cement Concrete Containing Recycled Asphalt Pavements", *Cement and Concrete Research*, vol. 35, pp. 2008-2013, 2005.
- [14] Najimi, M., Sobhani, J., and Pourkhorshidi, A. R. "Durability of Copper Slag Contained Concrete Exposed to Sulfate Attack", *Construction and Building materials*, vol. 25, pp. 1895-1905, 2011.

- [15] M. S. Shahbaz, R. Z. RM Rasi, M. F. Bin Ahmad, and S. Sohu, "The impact of supply chain collaboration on operational performance: Empirical evidence from manufacturing of Malaysia," *Int. J. Adv. Appl. Sci.*, vol. 5, no. 8, pp. 64–71, 2018.
- [16] Singh, S., Nande, N., Bansal, P., and Nagar, R. "Experimental Investigation of Sustainable Concrete Made with Granite Industry By-Product, *Journal of Materials in Civil Engineering*", vol. 29, 2017.
- [17] Singh, S., Ransinchung, G. D., and Kumar, P. "An Economical Processing Technique to Improve RAP Inclusive Concrete Properties", *Construction and Building Materials*, vol. 148, pp. 734-747, 2017.
- [18] Singh, S., Ransinchung, G. D., and Kumar, P. "Effect of Mineral Admixtures on Fresh, Mechanical and Durability Properties of RAP Inclusive Concrete", *Construction and Building Materials*, vol. 156, pp. 19-27, 2017.
- [19] Singh, S., Debbarma, S., and Kumar, P. "Utilization of Reclaimed Asphalt Pavement Aggregates Containing Waste from Sugarcane Mill for Production of Concrete Mixes", *Journal of Cleaner Production*, vol. 74, pp. 42-52, 2018.
- [20] Shi, X., Mukhopadhyay, A., and Liu, K. W. "Mix Design Formulation and Evaluation of Portland Cement Concrete Paving Mixtures Containing Reclaimed Asphalt Pavement", *Construction and Building Materials*, vol. 152, pp. 756-768, 2018.
- [21] Vijayalakshmi, M., and Sekar, A. S. S. "Strength and Durability Properties of Concrete made with Granite Industry Waste, *Construction, and Building Materials*", vol. 46, pp. 1-7, 2013.
- [22] Vijayaraghavan, J., Jude, A. B., and Thivya, J. "Effect of Copper Slag, Iron Slag, and Recycled Concrete Aggregate on the Mechanical Properties of Concrete", *Resources Policy*, vol. 53, pp. 2019-225, 2017.
- [23] Yi-qiu, T., Li, X., and Zhou, X. "Interactions of Granite and Asphalt based on the Rheological Characteristics", *Journal of Materials in Civil Engineering*, vol. 22, pp. 820-825, 2013.