



SCMS SCHOOL OF ENGINEERING & TECHNOLOGY

BOOKS/CONFERENCE DETAILS 2021

| Sl No: | Name | First Author | Second Author | Third Author | Fourth Author | INDEXING |
|--|---------------------|--------------|--------------------|-----------------------|-------------------|-----------------|
| 1 | Remya Y K | CCE2101 | | | | CONFERENCE-BOO |
| 2 | Dr.Akhila M | CCE2102 | | | | CONFERENCE-BOO |
| 3 | Dr.Sanju Sreedharan | CCE2103 | | | | CONFERENCE-BOO |
| 4 | Sonal Ayyappan | CCSE2103 | | | | CONFERENCE-BOOK |
| 6 | Dhanya K.A. | BCSE2108 | | | CCSE2102, CSE2109 | BOOK CHAPTER |
| 7 | Gayathry S Warriar | CCSE2110 | CSE2114, CSE2122 | | | CONFERENCE-BOOK |
| 8 | Josna Philomina | CCSE2104 | | | | CONFERENCE-BOOK |
| 9 | Susmi Jacob | | | CCSE2112 | | CONFERENCE-BOOK |
| 10 | Arshey M | | | CCSE2114, CCSE2122 | | CONFERENCE-BOOK |
| 11 | Bini Omman | | CSE2116 | | | CONFERENCE-BOOK |
| 12 | Litty Koshy | CCSE2101 | | | | CONFERENCE-BOOK |
| 13 | Neenu Sebastian | CCSE2119 | | | | CONFERENCE-BOOK |
| 14 | Blessy Antony | | CCSE2120, CCSE2121 | | | CONFERENCE-BOOK |
| 16 | Shilpa P C | CCSE2112 | | | | CONFERENCE-BOOK |
| 17 | Rosebell Paul | CCSE2119 | | | | CONFERENCE-BOOK |
| 18 | Binu John | CCSE2109 | | | | CONFERENCE-BOOK |
| 19 | Asha S | CCSE2105 | | CSE2116 | | CONFERENCE-BOOK |
| 20 | Sreeja Rajesh | CCSE2106 | | CCSE2123, | | BOOK CHAPTER |
| 21 | Geethu S Kumar | CCSE2123 | | | | CONFERENCE-BOOK |
| 22 | Deepasreevarma | CCSE2107 | | | | CONFERENCE-BOOK |
| 23 | Koshy P Joseph | CAU2101 | | | | CONFERENCE-BOOK |
| Total BOOKS/CONFERENCE for the calender year 2021 | | | | | | 21 |




DR. PRAVEENSAL C.J.
 PRINCIPAL
 SCMS SCHOOL OF ENGINEERING & TECHNOLOGY

A Review on Studies Based on Vehicle Stability and Safety on Rural Horizontal Curves

Y K Remya^{1*}, Anitha Jacob², E A Subaida³

¹ Department of Civil Engineering, SCMS School of Engineering and Technology, Karukutty, APJ Abdul Kalam Technological University, India 683576

² Department of Civil Engineering, Government Polytechnic College, Chelakkara, Thrissur, 680586, India

³ Department of Civil Engineering, Government Engineering College, Thrissur, APJ Abdul Kalam Technological University, India 680009

*Corresponding author: remyayk@scmsgroup.org

doi: <https://doi.org/10.21467/proceedings.112.62>

ABSTRACT

All over the world India bangs the top most position in crash deaths. Nearly 1.2 lakh people die every year on Indian roads. Crashes involving rollover and lateral skidding are now responsible for almost 1/3 of all highway vehicle occupant fatalities. So, rollovers and skidding are more serious than other types of crashes. One of the major reasons for such incidents is vehicle instability at curves due to its inconsistent geometric design. This necessitates a review on current design guidelines followed in India. Many researchers have pointed out drawbacks of current design approach and a few have identified various influential factors which are significant in curve design to reduce rollover and lateral skidding. When some researchers conducted field studies to measure vehicle stability at selected curves, some carried out computer simulations. There are efforts to incorporate vehicular characteristics in curve design which is much appreciable. This paper aims to project efforts made by researchers to reduce vehicle instability at horizontal curves. Moreover, gaps in these research works and scope for further research are highlighted.

Keywords: crash, rollover, skidding, vehicle stability

1 Introduction

As per Ministry of Road Transport and Highways, New Delhi (MORTH), about 15% of road crashes on highways occur at horizontal curves among which 8% is due to vehicle overturning or lateral skidding. A closer look at the crash statistics records of a few years reveals that road crashes involving vehicle overturning and lateral skidding are increasing drastically, especially heavy vehicle crashes. Several studies are conducted to identify the factors causing road crashes and prevent them. Crashes are multi causal and are affected by numerous factors like geometric design, traffic volume, traffic composition, variation in speed between vehicles of the same class and different classes, weather, motivation for travelling, driver's attentiveness and so on (Aljanahi et al., 1999).

James McKnight et al., 2008 conducted 'Large Truck Crash Causation Study' for 967 crashes, with 1,127 large trucks, 959 non-truck motor vehicles, 251 fatalities, and 1,408 injuries. The identified causes are misjudged speed, insecure loading, inattentiveness, loss of steering control, vehicle characteristics like tire, brake and suspension. Numerous research works are carried out by researchers across the world to identify influence of geometry on crash rate. Yingxue Zhang et al, 2009 identified curve radius, width, superelevation, transition curve and sight distance have important effect on traffic accidents. According to Sunanda Dissanayake and



Bio-reactor Landfill for Sustainable Waste Management – A Review

Akhila M

Dept. of Civil Engineering
SCMS School of Engineering and Technology
Ernakulam, India
akhila144@gmail.com

Anjali A M

Dept. of Civil Engineering
SCMS School of Engineering and Technology
Ernakulam, India
am.anjalianju@gmail.com

Abstract - To improve personal satisfaction in any country, the strategies for strong waste management should be reinforced. In India, the concept of engineered landfilling is not fully utilized. On the off chance that enough land is usable, it is viewed as a savvy practice. Aside from certain progressions, for example, reusing and source moderation methodologies, it has been found that garbage removal in landfills will stay an unavoidable piece of the strong waste administration framework. The bioreactor landfill concept changes the purpose of landfilling from storage to treatment of waste. The working hypothesis is that they encourage and speed up the natural exploitation of waste by safeguarding ideal dampness content inside the cells where the squanders are handled. The distribution of leachate assists with controlling dampness and microorganisms help to settle natural waste. The development of Bioreactor landfills can give natural and monetary advantages, and it is a promising strong waste administration framework for a thickly populated and emerging nation like India. This paper examines the possibility of a Bioreactor landfill for waste handling in the Indian context. The main features, types, operations, advantages, disadvantages and differences to the conventional landfills are discussed in detail.

Keywords—bioreactor landfill, waste disposal, sustainability

I. INTRODUCTION

Attributable to different sources of strong waste with quick development in the populace worldwide, maintainable metropolitan strong waste administration has become a necessity. The age of MSW has become an inexorably significant worldwide issue throughout the most recent decade. The expanded age of strong waste has provoked the execution of coordinated MSW the board, which incorporates reusing, fertilizing the soil, incineration and landfilling. About 80% to 90% of metropolitan waste is discarded in landfills without proper administration strategies or open copying, as indicated by gauges prompting air, water, soil contamination. Natural substances and actual cycles in landfill conditions encourage the biodegradation of natural squanders in MSW. Natural boundaries, like landfill liners and covers, are regularly utilized in ordinary landfills to keep dampness out, which is essential for waste biodegradation. Therefore, wastes are caught in a "dry burial place" and stay unharmed for extensive stretches going from 30 to 200 years, possibly outliving the landfill obstructions and covers. Liner disappointment in customary dry landfills is a chance, later on, representing a critical danger of groundwater and surface water pollution. Today, one idea that has got a ton of

consideration is the "Bioreactor landfill." Within 5 to 10 years of presenting the bioreactor interaction, a bioreactor landfill is a sterile landfill that utilizes improved microbiological cycles to change over and balance out the promptly and respectably decomposable natural waste constituents. In contrast with what might somehow occur in a landfill, the bioreactor landfill incredibly builds the level of natural waste decay, transformation rates, and cycle adequacy. The expansion of leachate or other fluid revisions, the expansion of sewage muck or different alterations, temperature control, and a "bioreactor landfill" give control and cycle streamlining, mostly through the expansion of leachate or other fluid changes, temperature control, and supplement supplementation. Additionally, the activity of a bioreactor landfill can require the option of air. Various types of "bioreactor landfills, for example, anaerobic bioreactors, oxygen-consuming bioreactors, and vigorous anaerobic bioreactors have been created and worked around the planet dependent on waste biodegradation mechanisms.

This paper means to raise peruse consciousness of the bioreactor landfill as a possibly reasonable waste management tool. It is required to be an essential commitment to future conversations among landfill proprietors and administrators, lawmakers, controllers, preservationists, and the overall population.

II. WASTE MANAGEMENT IN INDIA

It has been found that MSW, which ordinarily contains half biodegradable materials, 20% recyclable materials, and 30% dormant and inorganic materials including sands, rocks, and rock, has enormous energy potential. The metropolitan urban communities and towns of India's different states produce about 0.5 kg of MSW per capita each day. Only 12–14 % of MSW is formally taken care of in India, with the rest going to open unloading and landfill removal choices. As per the Planning Commission Report (2014), around 377 million individuals living in metropolitan territories produce 62 million tons of MSW each year, with 165 million tons each year and 436 million tons each year projected later on. The MSWM rules are set up to decrease the measure of waste that winds up in landfills by reusing likely material and assets from MSW. The various waste management methods for Indian MSW are listed below (Nandan et al., 2017; Pujara et al., 2019)



All



ADVANCED SEARCH

Conferences > 2021 Smart Technologies, Comm... ?

Video Forgery Detection using CNN

Publisher: IEEE

Cite This

PDF

Litty Koshy; Ajay S; Akhil Paul; Hariharan V; Ashil Basheer All Authors

3 Paper Citations

171 Full Text Views



Alerts

Manage Content Alerts Add to Citation Alerts

Abstract



Document Sections

- I. Introduction
- II. Literature Survey
- III. Proposed Architecture
- IV. Results and Discussion
- V. Conclusion

Abstract:With the widespread use of digitally interactive multimedia such as audio, images, and video, there has been a significant increase in the mode and motivation to create d... **View more**

Metadata

Abstract:

With the widespread use of digitally interactive multimedia such as audio, images, and video, there has been a significant increase in the mode and motivation to create digital forgeries. The widespread availability of video information and services, as well as the low cost of devices such as cameras, camcorders, and CCTVs, has led to widespread use of video information and services in our society for a variety of purposes such as video surveillance, forensics investigation, and entertainment. Previously, video editing techniques were mostly employed to improve digital information. However, as the popularity of low-cost, easy-to-use video editing software has grown, so has the number of negative repercussions and risks associated with such editing procedures. By merging, changing, or synthesising new footage, video forgery is a technique for creating changed or fraudulent videos. A method based on deep learning is given in the proposed system for classifying videos as tampered or original. The video clip that is used as input is divided into two categories: original and modified. The video is segmented into non-overlapping frames, and the authenticity of the movie is determined by whether or not all of the frames are genuine. The suggested method uses a deep CNN model that has two types of layers: (1) CNN layers which involve convolutional, pooling and fully connected layers and (2) Parasitic layers.

Authors

Figures

References

Citations

Keywords

Metrics

IEEE websites place cookies on your device to give you the best user experience. By using our websites, you agree to the placement of these cookies. To learn more, read our Privacy Policy.

Accept & Close

Date of Conference: 09-10 October 2021

INSPEC Accession Number: 21297365

Date Added to IEEE Xplore: 10 November 2021

DOI: 10.1109/STCR51658.2021.9588860

► ISBN Information:

Publisher: IEEE

Conference Location: Sathyamangalam, India

☰ Contents

I. Introduction

In the present digital age of internet and social media, our day to day life is permeated with digital video content as one of the prominent means for communication. Developments in video technologies such as generation, transmission, storage and retrieval along with applications like Video sharing platforms, Video-conferencing etc. have reached people and society in many ways. Applications such as the entertainment business, video surveillance, legal evidence, political films, video tutorials, ads, and other social networking platforms, such as YouTube, Facebook, and Instagram, demonstrate their unparalleled role in today's context.

| | |
|------------|---|
| Authors | ▼ |
| Figures | ▼ |
| References | ▼ |
| Citations | ▼ |
| Keywords | ▼ |
| Metrics | ▼ |

More Like This

Deep Learning-Based Person Detection and Classification for Far Field Video Surveillance
2018 IEEE 13th Dallas Circuits and Systems Conference (DCAS)
Published: 2018

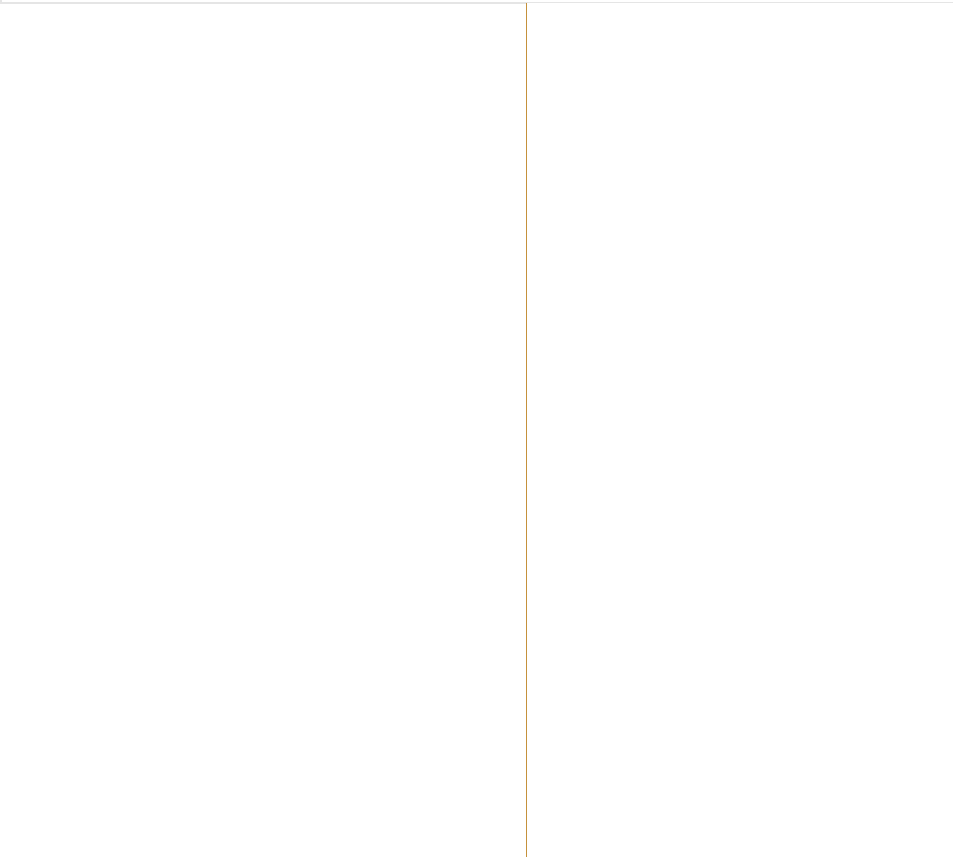
Characterizing Animal Behavior through Audio and Video Signal Processing

Published: 2007

IEEE websites place cookies on your device to give you the best user experience. By using our websites, you agree to the placement of these cookies. To learn more, read our Privacy Policy.

Accept & Close

Show More



IEEE Personal Account

CHANGE USERNAME/PASSWORD

Purchase Details

PAYMENT OPTIONS
VIEW PURCHASED DOCUMENTS

Profile Information

COMMUNICATIONS PREFERENCES
PROFESSION AND EDUCATION
TECHNICAL INTERESTS

Need Help?

US & CANADA: +1 800 678 4333
WORLDWIDE: +1 732 981 0060
CONTACT & SUPPORT

Follow



[About IEEE Xplore](#) | [Contact Us](#) | [Help](#) | [Accessibility](#) | [Terms of Use](#) | [Nondiscrimination Policy](#) | [IEEE Ethics Reporting](#) | [Sitemap](#) | [IEEE Privacy Policy](#)

A not-for-profit organization, IEEE is the world's largest technical professional organization dedicated to advancing technology for the benefit of humanity.

© Copyright 2023 IEEE - All rights reserved.

IEEE Account

- » Change Username/Password
- » Update Address

Purchase Details

- » Payment Options

» View Purchased Documents

IEEE websites place cookies on your device to give you the best user experience. By using our websites, you agree to the placement of these cookies. To learn more, read our Privacy Policy.

Accept & Close

- » [Communications Preferences](#)
- » [Profession and Education](#)
- » [Technical Interests](#)

Need Help?

- » **US & Canada:** +1 800 678 4333
- » **Worldwide:** +1 732 981 0060
- » [Contact & Support](#)

[About IEEE Xplore](#) | [Contact Us](#) | [Help](#) | [Accessibility](#) | [Terms of Use](#) | [Nondiscrimination Policy](#) | [Sitemap](#) | [Privacy & Opting Out of Cookies](#)

A not-for-profit organization, IEEE is the world's largest technical professional organization dedicated to advancing technology for the benefit of humanity.
© Copyright 2023 IEEE - All rights reserved. Use of this web site signifies your agreement to the terms and conditions.

IEEE websites place cookies on your device to give you the best user experience. By using our websites, you agree to the placement of these cookies. To learn more, read our [Privacy Policy](#).

Accept & Close



All



ADVANCED SEARCH

Conferences > 2021 Third International Conf... ?

A study on various thermographic methods for the detection of diseases

Publisher: IEEE

Cite This



Geethu S Kumar ; Rony George Roy ; Sreeja Rajesh All Authors

1 Paper Citation

365 Full Text Views



Alerts

Manage Content Alerts
Add to Citation Alerts

Free

Abstract



Downl
PDF

Document Sections

- I. Introduction
- II. Background
- III. Literature Survey
- IV. Analysis and Discussions
- V. Conclusion

Abstract:Fever is a common symptom for various infectious diseases that are reporting nowadays in a massive amount like COVID-19, Ebola and so on that will directly affect our who... **View more**

Metadata

Abstract:

Fever is a common symptom for various infectious diseases that are reporting nowadays in a massive amount like COVID-19, Ebola and so on that will directly affect our whole human cells and are showing a lot of chromosomal aberrations too. Since there was not a unique way are to predict how these diseases will affect our body both physically and mentally, since they can create some aftereffects in future too, there should be a suitable system which will efficiently detect these type of pandemic. In all these situations thermal screening had emerged as a remedial method for the detection of temperature variations. Among this Infrared thermography had been used as the best and effective method for fever screening. This survey presents some of the important papers which discussed how Infrared thermography can be effectively utilized for the detection of these epidemics by analyzing the temperature variations done in fever screening. Infrared thermography (IRT) is a method which uses an imaging scheme that gives you an image which is a thermal diagram that shows the temperature variations of various intensities. IRT uses the basic working principle from Stefan- Boltzmann Law, where the relationship between the temperature and the emissive power is established and the camera which is the infrared camera will capture this infrared energy and is converted into corresponding electronic signals. This paper gives a brief idea about various techniques used for fever screening which can be used to detect various diseases.

Authors

Figures

References

Citations

Keywords

IEEE websites place cookies on your device to give you the best user experience. By using our websites, you agree to the placement of these cookies. To learn more, read our Privacy Policy.

Accept & Close

Published in: 2021 Third International Conference on Intelligent Communication Technologies and Virtual Mobile Networks (ICICV)

Date of Conference: 04-06 February 2021

INSPEC Accession Number: 20607698

Date Added to IEEE Xplore: 31 March 2021

DOI: 10.1109/ICICV50876.2021.9388617

► ISBN Information:

Publisher: IEEE

Conference Location: Tirunelveli, India

 Contents

SECTION I. Introduction



In December 2019, COVID has vanquished our everyday life measure by detailing its first case from the Huanan fish market in Wuhan, Hubei, China. Scientists had recognized a novel Covid (SARS-CoV-2, additionally alluded to as COVID-19) from affirmed contaminated pneumonia patients [1]. Also, later on, COVID has changed its structure to extremely intense respiratory conditions (SARS) and the Middle East respiratory disorder (MERS). By April 13, 2020, instances of COVID-19 which was affirmed had surpassed 1,800,000. The World Health Organization (WHO) has proclaimed COVID-19 as both a pandemic just as a general wellbeing crisis of worldwide concern. By April 13, 2020, cases of COVID-19 which was confirmed had exceeded 1,800,000. The World Health Organization (WHO) has declared COVID-19 as both a pandemic as well as a public health emergency of international concern.

Infrared Thermography had wide range of applications like Non-Destructive Material Testing for interior analysis of material layers, Thermography in Aerospace where making high end machines, in Chemical industries for monitoring chemical reactions and so many other areas. Where the area focussed by this research paper was Thermography in Medicine.

In like manner, fever is the key manifestation of a few pestilences like extreme intense respiratory disorder (SARS) in 2003, flu A (H1N1) in 2009, Ebola infection sickness (EVD) in 2014, and Covid illness 2019 (COVID-19). As a safety measure government has implemented fever screening as a countermeasure for preventing these disease to its extreme for the people who are crossing international as well as national borders and in places like hospitals, malls, railway stations, and in all places where the crowd assembles fever screening is the one and only remedial measure to detect these diseases.

This research paper provides an idea regarding the momentum situation, where how to focus viably and productively utilize image processing techniques for the recognition of different ailments which contribute to COVID19 detection. Secondly, since the virus was showing variations of symptoms a single symptom called fever cannot be relayed for identifying the virus. So the research paper gives a comparative study of different types of disease symptoms that can be a cause for the detection of corona virus. Third factor was the sensors, since the images were captured by IR cameras an equal focus was given on various sensors used by different methods. The disease mainly focused by the research paper are fever detection, respiratory infections, thyroid, osteo based problems, diabetes, blood flow analysis and cancer detection.

SECTION II. Background

IEEE websites place cookies on your device to give you the best user experience. By using our websites, you agree to the placement of these cookies. To learn more, read our Privacy Policy.

Accept & Close

Image Processing is one of the recent trends in analyzing a digital image where the images were grouped as pixels. In this survey the images were concentrated mainly to thermal images. Thermal images were obtained using a thermal camera in which an array of thermophile sensors were embedded in the lens of camera. These sensors will be of varying resolutions which captures the image. The thermal images obtained will be gray scale images and the RGB coloring model was incorporated to identify each areas based on thermal variations. Infrared Thermography (IRT) comes under infrared imaging science. Radiation in the long-infrared scope of the electromagnetic range (about 9,000–14,000 nanometers or 9–14 μm) is identified by thermographic cameras and produces pictures of that radiation which are named as thermograms. There is a wide scope of utilizations for thermography which can be utilized in a few conditions as an analytic instrument, for arranging the treatment and assessing the impacts of treatment. Thermography can be joined with other imaging strategies and Artificial Intelligence ideas, play a vital role essentially in the adaptation of numerous ailments [2]. Infrared radiations are emitted by all objects above absolute zero, which is stated in black body radiation law. These infrared radiations lie in the range of 0.75–1000 micrometers [3]. Thermography utilizes a non-obtrusive, non-contact strategy that utilizes the warmth from your body to help in making the conclusion of a large group of medical care conditions. So this method was completely safe since it uses no radiations.

SECTION III. Literature Survey

A. Clinical evaluation of fever-screening thermography

In the research paper, a clinical study of over 596 subjects has been conducted [4]. They made an experimental set up to capture the thermal image where they used a tripod to obtain a full face. The graphical user interface was developed with MATLAB and two IRTs. The analysis was for the duration of fifteen minutes, where four measurement readings were taken. For limiting the impact of outside temperature each subject was asked to meet a relaxation time of 15 minutes and all initial humidity factors were defined properly. Temperature readings were taken on each stage, focusing on the region's facial and forehead so that two IRTs were used. In each round of capturing the image, the webcam acquires a standard color image and the IRTs will acquire three consecutive frames that were reduced to the midpoint from which a solitary mean temperature image was obtained. As the last stage, thermal images of sublingual tissue were captured by instructing them to open their mouth. To establish a reference temperature, oral thermometry was used and the corresponding temperature readings were taken from the region of study. The two temperature measurements will help to modulate two models, a fast model and a monitor model were formulated. The monitor model had an accuracy of ± 1 . From the monitor mode, the oral temperature measurements average value was calculated and the final reference temperature was developed. As a subsequent stage facial district depiction and temperature counts were finished. Here temperature from several facial areas was compressed. For the delineation of facial key points, a new approach called image registration was done. This technique uses a matching method by which facial landmarks are mapped to thermal images which will give the main facial points whose temperature measurements are to be recorded.

The calculated values of temperature which are recorded from the selected regions were compared with the reference and from this, the pairwise differences were recorded. Based on this data, the final result was generated which shows the temperature measurement values of the five regions of interest.

Advantages: Gives an efficient method for monitoring temperature especially in the region inner canthi region. Provides a better system performance.

Further enhancement: The effect of puzzling elements identifying with between subject and ecological fluctuation can be remembered for clinical investigation.

This study aims at establishing a modest and efficient temperature screening instrument. The methodology uses an AMG8833 thermal camera. The camera is connected to an Arduino by a 12C bus. The picture caught by the camera which is essentially the IR camera is in the form of 64 individual pixels and the pixel values are stored in the Random Access Memory (RAM) of the camera. The IR camera and its in-constructed sensor, which is corresponding to the surrounding temperature and sensor work in sustained, uninterrupted mode. Numerous methods were done to obtain the temperature of the subject which is under study like considering the normal room temperature, pixel offset cancelling, and normalization and thereby compensating the emissivity of the object. The temperature values in the form of an 8X8 matrix were generated which will give the resultant values for analysis by running an Arduino program. And an efficient image can be developed by adding an extra feature, a thin film transistor LED to the original setup.

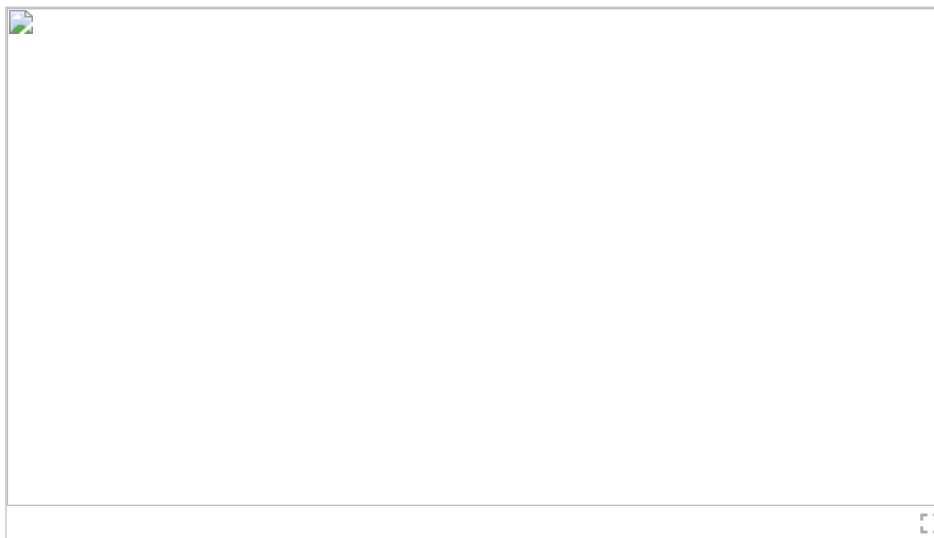


Fig. 1. Steps in Development of Low-cost Thermal Imaging System as a Preliminary Screening Instrument.

In a microcontroller, a sensor and display module is attached, which senses thermal data by AMG8833. An Arduino IDE captures the thermal images and the images are saved in an SD card which is inserted in the display module. Fig. 1, demonstrate the general working of the proposed method. To this image processing operations are carried out to detect abnormalities in image regions [5].

Advantages: Able to develop an economical, compact easily carrying thermal camera.

Further enhancement: Uses a low pixel ratio when compared to other high quality thermal imaging cameras. The analysis can be made more understandable if the resolution can be increased to 64X64 pixels.

C. A low cost thermal imaging system for medical diagnostic applications

This system uses an infrared sensor which belongs to Melexis IR sensors and it is a thermophile based one. It also constitutes a microcontroller and other hardware related components. The infrared sensor is a completely aligned 16x4 pixels industry-standard IR cluster. It has two chips: an IR array and the 24AA02 (256x8 EEPROM) chip which are embedded into a single sensor. The sensor has a committed low noise chopper-settled enhancer and is quick ADC incorporated which contains 64 IR pixels. By employing a Proportional to Absolute temperature sensor, ambient temperature measurement of the chip is integrated. The temperature sensations in the form of recorded thermal values of both the infrared and proportional to absolute temperature sensors are stored on an internal RAM. The pixel array had a versatile frame rate and every pixel is designed in such a manner that they are cohesively combined with an amplifier and an Analog to Digital converter. The remaining hardware part consists of a sensor module which is connected with a microcontroller and an adjustable digital interface [6].

The thermal sensor captures the image as a 16X4 matrix, which is an array of pixels. A microcontroller module calculates the temperature value of each pixel and it will read the calibration values and raw temperature data from the sensor's EEPROM and RAM. With these calculated values microcontrollers calculate the corresponding temperature values of each pixel. A PC will read the serial data and divide the temperature values into different ranges which is an RGB value. During analysis, different variants of temperature recordings were taken, from which an average temperature value was calculated as a unique measurement [7].

Advantages: This framework there use no direct contact with the object so it is safe. It has no radiation too.

Further enhancement: This mechanism can be improved to be used for certain diagnostic applications.

D. Screening for Fever by Remote-sensing Infrared Thermographic Camera

In this model, three different infrared cameras were used. In all these cameras they use a similar system such that they can detect a temperature difference of 0.1. For the measurement of accurate temperature readings, a program was designed in such a way that the parameters for taking correct readings are incorporated in this program like, the object whose temperature has to recorded was at which particular distance from the infrared camera and the surrounding environmental parameters for each dataset. The temperature readings from several points were recorded and the maximum infrared temperature was taken from all these measured temperature values. Six different regions in the body were taken for temperature measurements and two referential measurements were taken. For every person, the IRT measurements and normal body temperature were taken and the same process was repeated after fifteen minutes where they are asked to do exercise. Then by using correlation and regression analysis the two readings, the IRT and ambient body temperatures were analyzed. Finally, the classification was done as false-positive in which the temperature shows a considerable change above the reference value and as false-negative where the temperature is within the normal range [8].

Advantages: This method give an accurate result even if the person whose temperature has been captured was moving. Further enhancement: Additional research can be done for various factors like texture, the application of external makeup and other biological factors.

E. Multi-person fever screening using a thermal and a visual camera

This method involves the fusion of an ordinary visual camera, which gives a clear identifiable image, and an infrared camera that can record the correct temperature measurements of the object which was under investigation. The existing system uses a Forward-looking Infrared Camera (FLIR) of 640x512 pixels resolution and an image capturing camera which belongs to Microsoft LifeCam Studio. The visual camera selected was of higher resolution and has a very high frame rate. Recognized appearances where set apart with rectangular boxes that make use of various inclinations of shadings. Three colors are selected in which each has its own temporal meanings and they are yellow, red, and green. If the measured temperature value shows not much robustness it was recorded with a yellow color gradient. Green is for ordinary ambient temperature and if the recorded temperature was above a referential value that should be considered as a high-risk zone hence indicated in red color. By using a sliding window technique and Random Forest classification the face detection was done smoothly.

The basic working of the proposed system is depicted in Fig.2. In the face, the main area of focus was the corners of the eyes and these features where extracted using random forest repressors. Thermal image coordinators are obtained from the thermal image coordinates of the transformed visual images of corner positions of the eye. For face detection, a modified version of standard Viola-Jones faces detection is used [9]. Then the image is processed with a course of binary classifiers at all sensible positions and scales. If all these stages were fulfilled completely the image will be identified as a face. After the detection of faces, a multi-face tracker was used that will detect faces in a new frame, irrespective of what happens before. And a multi-target tracker will associates

of rectangle where the calculation was conducted. A rectangle selection of small dimension would reduce the risk factor than with large dimensions even though the localization was more stable. In this view the eye corner detection algorithm was prominent where a key point dimension selection of window can be selected. This method was performed on a recursive basis till the output was obtained. The orientations of camera were focused to obtain a high orientation image. The actual orientations and speed of objects were detected using Kalman filters. By analyzing the assignment matrix, the auction algorithm which is an association method was developed [10]. Thus, the estimation of temperature is generally insensitive toward a wrong surrounding temperature. A bias factor was estimated to consider if the ambient temperature shows a variation than the referential value [11].

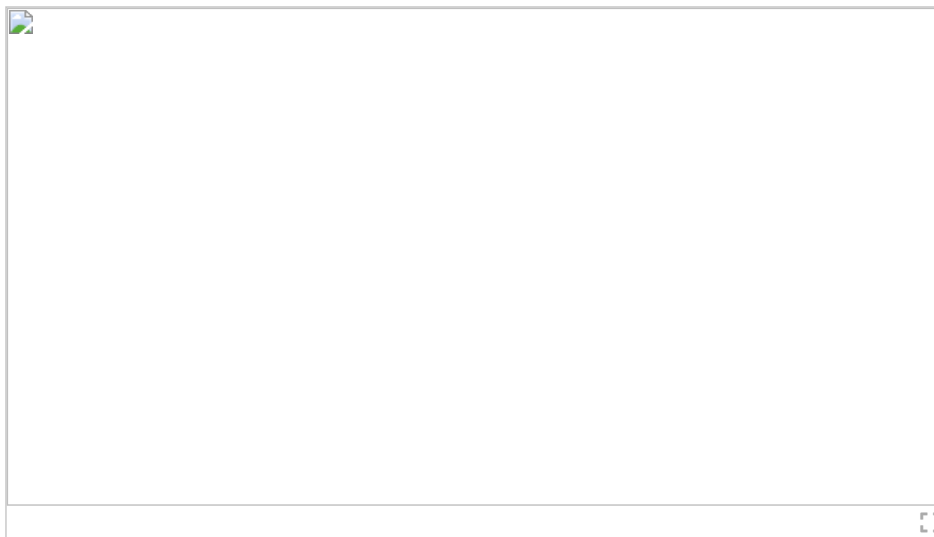


Fig. 2. Steps in Multi-person fever screening using a thermal and a visual camera

Advantages: Multiple persons can be fever screened at the same time. This method can be used at the airport thus saving a lot of time.

Further enhancement: For identifying glasses in the images obtained by IR camera, a detection algorithm can be developed. Cameras can be properly calibrated to produce a single optical axis.

F. Combining Visible Light and Infrared Imaging for Efficient Detection of Respiratory Infections Such As Covid-19 on Portable Device

This research paper [12] discuss an aberrant breathing detection which uses a deep learning technique. The method incorporates the combination of RGB and thermal videos which are acquired using a dual-mode camera. With the aid of a portable and intelligent screening device, RGB and thermal videos were obtained. For achieving this a FLIR one thermal camera was used which collaborate two cameras one is for taking RGB and the other for thermal. As a part of the respiratory study, the face regions of the videos were focussed, and by a face detection method, the nose and forehead areas were extracted. By using a time series analysis of the breathing data the respiratory patterns of test cases are obtained. There is a chance of occurring temperature fluctuations due to the normal breathing process and the usage of a mask may hide many of the facial features. For avoiding those defects a method where two parallel placed RGB and infrared cameras are placed which capture the images of face and mask regions. An algorithm for the detection of face which is covered by a mask is based on the pyramid box model suggested by Tang et al. [13]. This method makes use of the tactics like the Gaussian pyramid box in deep learning and by implementing a Gaussian pyramid algorithm. After this, the masked areas are extracted and the area from RGB is portrayed as thermal. As most of the calculations are based on the region of interest, as the next step of developing a tracking method was used which analyses the images which is having a mask and that without a mask as the temperature variations cannot be effectively captured while having a mask. As a foremost step for the final classification which systematizes the respiratory condition between a healthy and infected person, a BiGRU-AT neural network is used.

Being a time series data the classification uses a bidirectional Gated Recurrent Unit with an attention layer is used. For processing time-series data a Recurrent Neural Network (RNN) was

IEEE websites place cookies on your device to give you the best user experience. By using our websites, you agree to the placement of these cookies. To learn more, read our Privacy Policy.

Accept & Close

used. RNN is a feed-forward neural network that had an internal memory. Since RNN can remember past data it encounters a problem of vanishing gradient problem. So as a remedy another network called Long Short Term Memory (LSTM) will resolve this problem [14]. The bidirectional recurrent neural network will intensify the interrelation between the context of sequence and a bidirectional GRU will provide more statistics regarding periodic sequence. While performing the respiratory data analysis, the complete waveform in time sequence is considered and there may be a chance of immediate acceleration occurring. So by the discussed networks, these features may be feeble because the time series data are given one by one which can generate a larger error. To avoid that an attention layer is affixed.

Advantages: Accurate and robust respiratory data detection algorithm was obtained.

Disadvantages: Limitation in the angle of the camera during measurement.

Further enhancement: Can use a more efficient algorithm that reduces the effect on breathing conditions by wearing various masks. To ensure high detection accuracy on respiratory infections.

G. Non-contact monitoring of human respiration using infrared thermography and machine learning

The Respiration Rate (RR) varies under different contexts. So the breathing waveforms under varying circumstances were obtained. As the first step volunteers were selected for study [15] and with the support of an A325 Infrared camera [16] thermal images were captured. The ROI was nostrils and they were selected by a FLIR software [17]. For efficient tracking of nostrils, Vahid Kazemi et al., proposed a tracking algorithm and this was used [18]. This algorithm uses an ensemble of Regression tree which gives decisions by comparing the threshold differences between the intensities of two pixels. But this will spawn the drawback that pixel differences may be large. Due to the influence of numerous environmental conditions, the breathing waveform obtained was having a low signal to noise ratio. Since the signals involve a number of noise contents, it has to be filtered with the help of a low pass IIR filter. Breaths per minute (BPM) is an important variable for tracking our health. For this calculation, this work proposes a Breath detection algorithm where two counters are initialized to zero in which one counter will count the number of abnormal breaths and the other will count the normal breath. Here a normal and abnormal breath was obtained by analyzing the actual signal with the measurement of background noise ratio where the duration of the breath cycle is compared with a threshold value. For the classification between a normal and abnormal breath, a K-Nearest Neighbour (k-NN) classifier was used [19]. And the analysis of data points that are given to the k-NN classifier is tracked using the t-Stochastic Neighbour embedding algorithm. The information which is getting looked at was separated into training and testing information and the training dataset was again partitioned with the help of a cross-validation technique as training and validation datasets.

Advantages: Efficient Breath detection algorithm was implemented.

Disadvantage: For checking the validation accuracy it uses different k values.

Further enhancement: Instead of checking for different k values other classifiers can be considered such as Support Vector Machines and so on.

H. Detecting Fever in Polish Children by Infrared Thermography

Since the immune system of children is under development they may be more prone to sickness. So there should be an efficient method to detect fever in children. So this research paper gives a method in fever detection especially in children who were within an age span from 1 to 17 years [20]. In this research, three types of FLIR IR cameras were used. The temperature from four regions of interest was considered axilla, ear, eye, and forehead. For the analysis, both temperatures taken from an ordinary clinical thermometer and thermographic measurements were considered. During the analysis, the forehead temperature and the temperature taken from the ear especially focussing on the tympanic region are not reliable because of various factors. Physical exercise can cause a huge impact on the variation of forehead temperature and for ear, the variations in the ear channel,

the occurrence of ear pain and ear fluid affect the temperature but there occurs a good immunity between the eyes especially the inner canthus region and axilla region. So by using software the region of interest was located. The temperature readings were taken which can trigger an audible alarm. During the analysis, the temperature values from different recordings should be considered

by taking an average value and the temperature value of single pixel should not be considered. But the parameters that affect the temperature measurement should be optimal so some standardization technique is very crucial. Also, to acquire the greatest number of pixels inside the located interested regions the picture should fit the frame.

Advantages: Accuracy is more especially in the axilla and eye areas.

Disadvantages: For optimizing the parameters, standardization techniques are required.

I. Early Detection of Diabetes using Thermography and Artificial Neural Networks

This work will confer a method for early identification of diabetes by combining thermal imaging with a neural network technique where the training of the network was in the similar way the human brain will function [21]. Thermography is an effective tool in the diagnosis of many diseases like diabetics, fever screening, breast cancer detection, and so on [22, 23]. Initially pre-processing of thermal images were done to reduce noise and regions of interest were extracted to which a neural network model was applied to obtain the status of the patient. Thermal imaging has emerged as a prominent tool in the field of medicine for the early detection of various diseases as most of the diseases will start with a variation in temperature as the beginning symptom [24, 25]. This study makes use of a FLIR thermal camera which will record the images of thermal distributions on the patient foot. The temperature values obtained from various points from the patient's foot are mapped to a matrix representation and were later stored on a personal computer for data analysis. As the thermal images are captured and data is given to a personal computer the next step is the implementation of the Artificial Intelligence (AI) model which has a data-driven approach. An artificial neural network [26] is an efficient way of computation which consists of different number of layers like input, hidden and output layers. And by an activation function which is a mathematical function the inputs which are given to hidden and output layers are summed to generate the desired output [27]. For data analysis, MATLAB was used which can provide more accuracy by using different MATLAB functions. Two sets of data was used in the case study analysis of which one can be used for training and the other for testing. This method uses an artificial neural network where the number of hidden layers were three and the input layer uses four input variables. For analyzing different ANN model Root Mean Square Error was used.

Advantages: Early detection of diabetes.

Disadvantages: Used a three hidden layer network since it fits the model.

Further enhancement: Can use improved artificial intelligence tools for improving the performance of the existing system.

J. A Non-Invasive Human Temperature Screening System with Multiple Detection Points

By using a 2D thermal imaging camera there are some limitations in identifying the temperature in periorbital areas which makes it difficult to compare with the reference values [28, 29]. So to avoid this difficulty the research paper [30] suggests several image processing techniques that select human faces for the maximum skin temperature. This system proposes a non-contact temperature screening system on a real-time basis. By using an inherent 2D space a quite number of people can be maintained from the infrared thermal camera at a considerable distance. And the others will be directed to stand a few distances behind the currently analyzing people. Then the focal length of the lens will be adjusted that focus the maximum number of people whose temperature is screened. And the camera will be able to capture thermal images of people who are walking at a normal speed. For monitoring the fluctuations of surrounding temperature an outside temperature and humidity sensors are interfaced with the existing system. For the good capturing of images the thermal imaging camera of the FLIR system was used and the lens should be focussed at a particular degree along the vertical and horizontal axes. So the selection of camera lens is an issue. Then by restricting the number of people in front of the camera the thermal images are captured and the next step is face detection. So a face searching technique in one image frame is used to detect the faces [31]. For

morphological processing, hole filling, and so on and coordinates of the face were obtained. A field test was used to capture the efficiency of the camera for detecting multiple faces at a time. The result shows that the system can trace the real-time display of the maximum skin temperature.

Furthermore, on remunerating, the worries it was evident that on the core body temperature once the aggravation from the general climate, the temperature esteem got from the thermal imaging camera has less variation. At the point when the temperature limit level and the balance temperature esteem are fittingly picked Hyperthermic patients can be related to 100% accuracy. The choice of the number of human countenances on the thermal image marginally influences the framework speed which has a rate of 7 milliseconds for one face, and up to 10 milliseconds for four appearances.

Advantages: System introduces a real-time display system in which the maximum skin temperature can be monitored. There is less fluctuation in the temperature value obtained from the thermal imaging camera.

For febrile detection the proposed system can give 100% efficiency.

Future works: By embedding an outside temperature and relative humidity sensor to the ThermScreen framework, the estimation connection with aural temperature information can be improved.

K. Thermographic analysis of thyroid diseases

In this work [32], a FLIR infrared camera which is of the model ThermaCAM S65 system was used for handling thermal images. The camera was working in a programmed self-adjustment mode and the patients were treated under conducive conditions [33, 34]. For the detection of the thyroid, the region of interest was captured by considering the camera calibrations and proper orientations. The cytological study was conducted and the smears were identified and these results were compared with the results of ultrasonography. The result analysis gives a massive contribution to the detection of disease based on detecting hyperthyroid and hypothyroid by the temperature variations. The analysis clearly shows that the comparison of thyroid disease type with the mean skin temperature shows the pieces of evidence of temperature variations. By using this method a clear classification of good and affected thyroid nodules can be detected [35].

Advantages: Uses the least invasive and low cost method for the detection of thyroid nodules.

Further enhancement: For predicting thyroid pathologies, the temperature gradient of thermograms can be used.

L. Dynamic Infrared Thermography Study of Blood Flow Relative to Lower Limb Position

For the proper heat distribution within the body, blood flow plays a very crucial role. This research paper discusses how infrared thermography can be used in the analysis of blood flow in the lower limb positions [36]. For the easy understanding of the temperature behaviour of skin, dynamic infrared thermography is used [37]. And for relating the vascularity of tissues, temperature measurements of the human leg were acquired [38]. By using a FLIR T440 thermographic camera, dynamic thermography of lower limb was obtained. It has a focal plane array of 320X240 pixels and for absolute temperature measurements depends on emissivity, ambient temperature, relative humidity, and distance [39]. Temperature variations of five distinct points of limb were recorded. During analysis, the average temporal temperature restorations of the foot from both vertical and horizontal positions were considered. The spots which show a temperature difference gives a faster return to thermal balance.

Advantages: Dynamic thermographic study gives a clear detection of temperature variations in lower limb regions. Disadvantages: The heat transfer mechanism was affected by the opposite gravity of blood flow.

M. A Study on Implementing Physiology-Based Approach and Optical Flow Algorithm to Thermal Screening System for Flu Detection

In this method [40] a physiology-based approach was used so that the area of selection was the human face. The face consists of hot and cold tissues which can be modelled as a collection of these two normal distributions [41]. In this study, using a thermal camera five different angular positions on your device to give you the best User experience. By using our websites area of the human face and the temperature variations were recorded. For detecting a minor flow of motion of the object an Optical Flow Algorithm was used which provides higher accuracy for temperature

detection [42]. For better performance, this method makes use of a Parabolic Regression and Radial Basis Function Network. An algorithm known as the Adaptive Network-Based Fuzzy Interferences System has been used for this purpose [43]. Then the thermal images will be classified using the Image Classification Pre-processing module. Fig. 3 shows the basic working model of the discussed system.

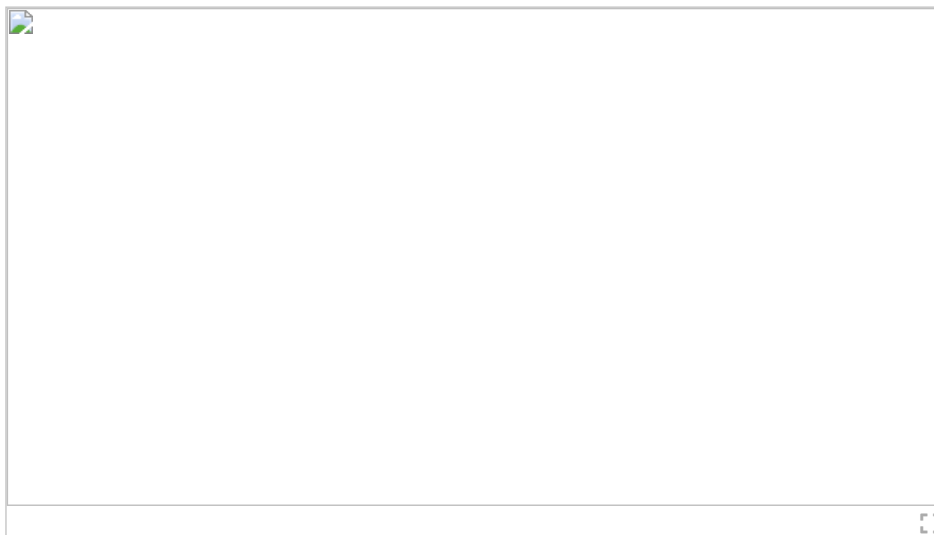


Fig. 3. Flow diagram of A Study on Implementing Physiology-Based Approach and Optical Flow Algorithm to Thermal Screening System for Flu Detection.

Advantages: This system gives a good performance especially in hospitals, airports and other places where huge crowd assembles for effectively recording the temperature of person who are in motion.

Further enhancement: Can integrate more crowd, for thermal screening system which can be utilized in public areas like airports and hospitals to reduce the rate of transmissible infectious diseases.

N. Supportive Noninvasive Tool for the Diagnosis of Breast Cancer Using a Thermographic Camera as Sensor

This research paper provides a tool for breast cancer detection by Infrared thermography [44]. For establishing the method the image acquisition basically the thermogram images were taken using the thermographic sensors. To this captured image, image processing algorithms were applied to obtain the breast area segmentation. Thermographic image acquisition will in either static or dynamic form and the different images of a single patient from different orientations were taken [45, 46]. The image acquired was processed for the avoidance of background noises and thresholding using Otsu's method was done to the required thermogram [47]. From the preprocessed image the area of interest was segmented and since the paper focused on breast cancer detection, two regions where the right and left breast images were segmented from the initial thermographic image. The automatic segmentation module does all the related task of segmenting the images into different separate independent images so that the temperature variations can be done more effectively. For identifying the temporal variations on the right and left breast it was necessary to convert the grayscale values to their corresponding thermal intensities. The thermographic values are represented in a matrix format. Average temperature values are estimated, and the region with a temperature greater than the referential temperature was detected as infected areas. For detecting the tumor areas, regions with the highest temperature values were used and segmentation of these regions using the watershed technique was used [48]. By using the same segmentation technique apart from the cancer detection another phenomenon called Angiogenesis was also able to be detected.

Further enhancement: The automatic segmentation method used can be modified to set the target values for attaining thermal stabilization.

O. Automated Analysis Method for Screening Knee Osteoarthritis using Medical Infrared Thermography

Osteoarthritis is a common degenerative disease that is most frequently occurring in people nowadays [49, 50]. This research paper presents an idea for identifying knee osteoarthritis with the aid of IR thermography [51]. This disease will be affecting knees, so they are the region of interest. Images of the knee were captured using an infrared thermal imaging system. Based on certain predefined parameter settings, the thermographic image obtained was later processed for the patella-centering procedure. During the first step, the left and right knees were compared and in the second step, the sub-regions temperature variations were obtained. After the segmentation and sub-regional segmentation then the feature extraction and classification were done. During the feature extraction module, the sub-regions were evaluated and the defective portions and normal portions were identified. The statistical features were calculated using histogram analysis and the entropy features were calculated [52]. By using the feature extraction method the features were extracted and these were given as the input to the classification module and the classifier used in the proposed method is a classification by Support Vector Machine (SVM) [53]. SVM gives an efficient classification for the diagnosis of knee Osteoarthritis.

Advantages: Method was a cost-effective tool that can easily detect various diseases that too the chronic ones.

When compared to other medical imaging techniques the proposed method was especially desirable to be highly useful in the detection of rheumatism and most geriatric-related issues.

Further enhancement: Further analysis should also be carried out to ensure the accurate quantitative portrayal of specific anatomical positions in a thermal image using techniques such as CT and MRI multi-image fusion, which would dramatically increase the precision of the screening procedure.

SECTION IV. **Analysis and Discussions**

As a comparative study most research papers give a better explanation for detection of diseases in an efficient way. The major classification tools used were K-means classifiers, artificial neural networks and in common most of the research papers used thermal sensors for disease detection. An important factor which influence the performance of temperature measurement was the thermal camera resolution. As the resolution varies the thermal image capture was influenced. Fig. 4 describes the influence of pixel resolution on thermal distributions.

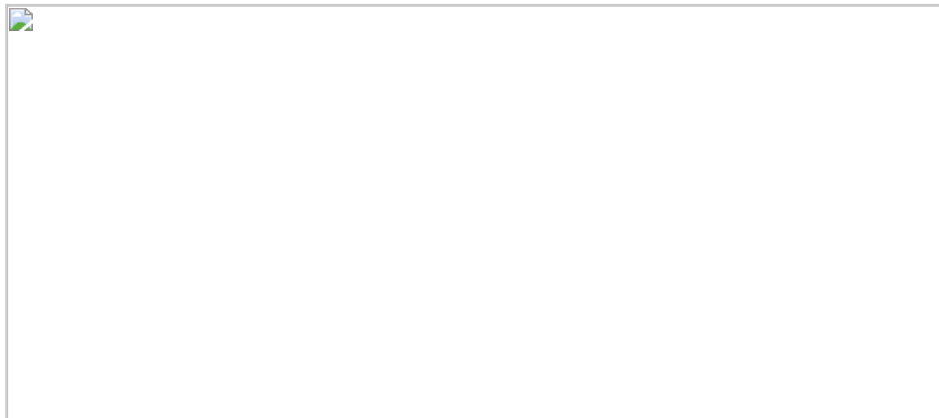


Fig. 4.
Pixel ratio and efficiency

Performance analysis of various research work based on sensitivity and specificity was depicted by TABLE I. Based on the selection of various sensors and the number of sensors the efficiency of thermal detection was also improving.

TABLE I Comparison of Various Methods Based On Sensitivity and Specificity

TABLE II Gives a comparative study on various methods discussed and the advantages, disadvantages and various methods used by different research papers. so in all the research works, the thermal images were captured and various image processing techniques were used for the efficient detection of diseases where the focus was on thermal screening. this survey will give a better study for covid-19 detection since the primary symptoms were fever, osteo-based problems and thyroid variations. based on the selection of various sensors and the number of sensors the efficiency of thermal detection was also improving.

TABLE II Comparison of Various Methods

So based on the relevance of the application to be developed, the sensors can be chosen. For critical application where the minute details are to be captured focus should be placed on the selection of

IEEE websites place cookies on your device to give you the best user experience. By using our websites, you agree to the placement of these cookies. To learn more, read our Privacy Policy.

Accept & Close

SECTION V.

Conclusion

Here a comparative study of various thermometric methods is done to find an effective system especially in the fever screening scenario that can be used for COVID-19 detection. So when two separate cameras were used in the analysis, a thermal camera for temperature measurements and an ordinary visual camera for image capture most of the system face synchronization problems. And the correct correlation of the optical axis is also a factor that affects efficient calculations. Thus by considering all these factors a low cost, easy to use thermal imaging system was hence developed so that with the help of image processing techniques combined with other detection and classification methods an efficient disease detection method can be developed.

| | |
|------------|---|
| Authors | ▼ |
| Figures | ▼ |
| References | ▼ |
| Citations | ▼ |
| Keywords | ▼ |
| Metrics | ▼ |

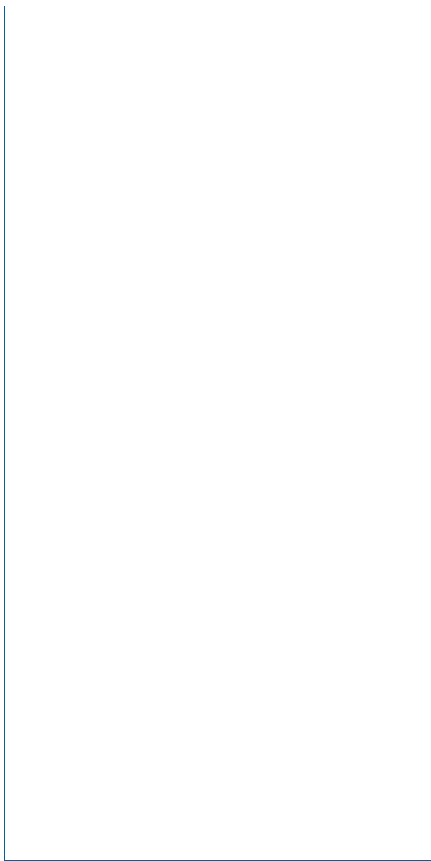
More Like This

Medical Image Processing in Collaboration with Medical Researchers--Imaging and Image Processing of Cardiovascular Disease Dynamic Images
Second International Conference on Informatics Research for Development of Knowledge Society Infrastructure (ICKS'07)
Published: 2007

The effects of medical image processing techniques on the computational haemodynamics
2012 IEEE 2nd Portuguese Meeting in Bioengineering (ENBENG)
Published: 2012

IEEE websites place cookies on your device to give you the best user experience. By using our websites, you agree to the placement of these cookies. To learn more, read our [Privacy Policy](#).

Show More
Accept & Close



IEEE Personal Account

CHANGE USERNAME/PASSWORD

Purchase Details

PAYMENT OPTIONS
VIEW PURCHASED DOCUMENTS

Profile Information

COMMUNICATIONS PREFERENCES
PROFESSION AND EDUCATION
TECHNICAL INTERESTS

Need Help?

US & CANADA: +1 800 678 4333
WORLDWIDE: +1 732 981 0060
CONTACT & SUPPORT

Follow



[About IEEE Xplore](#) | [Contact Us](#) | [Help](#) | [Accessibility](#) | [Terms of Use](#) | [Nondiscrimination Policy](#) | [IEEE Ethics Reporting](#) | [Sitemap](#) | [IEEE Privacy Policy](#)

A not-for-profit organization, IEEE is the world's largest technical professional organization dedicated to advancing technology for the benefit of humanity.

© Copyright 2023 IEEE - All rights reserved.

IEEE Account

- » Change Username/Password
- » Update Address

Purchase Details

- » Payment Options
- » Order History
- » View Purchased Documents

Profile Information

IEEE websites place cookies on your device to give you the best user experience. By using our websites, you agree to the placement of these cookies. To learn more, read our Privacy Policy.

- » Communications Preferences
- » Profession and Education

Accept & Close

» [Technical Interests](#)

Need Help?

» **US & Canada:** +1 800 678 4333

» **Worldwide:** +1 732 981 0060

» [Contact & Support](#)

[About IEEE Xplore](#) | [Contact Us](#) | [Help](#) | [Accessibility](#) | [Terms of Use](#) | [Nondiscrimination Policy](#) | [Sitemap](#) | [Privacy & Opting Out of Cookies](#)

A not-for-profit organization, IEEE is the world's largest technical professional organization dedicated to advancing technology for the benefit of humanity.

© Copyright 2023 IEEE - All rights reserved. Use of this web site signifies your agreement to the terms and conditions.

IEEE websites place cookies on your device to give you the best user experience. By using our websites, you agree to the placement of these cookies. To learn more, read our [Privacy Policy](#).

Accept & Close



All



ADVANCED SEARCH

Conferences > 2021 7th International Confer... ?

Excavation of Time sliced and Cost based KDD for the lead generation and promotion on B2C/B2B Sales

Publisher: IEEE

Cite This

PDF

Jency Rena NM ; Gayathry S Warriar ; M Arshney All Authors



76 Full Text Views

Alerts

Manage Content Alerts Add to Citation Alerts

Abstract



Document Sections

- I. Introduction
- II. Related
- III. Literature Review
- IV. Research Methodology
- V. Results and Discussion

Show Full Outline

Authors

Figures

References

Keywords

Metrics

More Like This

Abstract:Fast advances in information gathering and capacity have empowered associations to collect huge measures of information and hence extracting the only relevant and useful ... **View more**

Metadata

Abstract:

Fast advances in information gathering and capacity have empowered associations to collect huge measures of information and hence extracting the only relevant and useful information from large volumes of data is a challenging task. The conventional techniques for data analysis and evaluation cannot be utilized subsequently on the huge measure of the data-set and-so new methods were developed for mining data. Frequent pattern mining algorithms like Apriori, FP-Growth, etc. may sometimes miss the rare but important patterns of a database since they are dealing only with the number of times an item appears in the database. In business environments like retail shops or online markets, identifying the profit-generating items is more important than finding the items which are sold many times. The high utility item set mining with the time cube concept helps us to find the relevant, profit-generating item sets from the transactional data set by performing the calculations using the quantity that is purchased, total cost and unit gain of each item in the database. The concept of time cubes implemented here helps to efficiently deal with the temporal parts of the transactional data set. Considering total cost decides the frequent customer of particular product set. The proposed system is mainly applicable in online markets, FMCG Sectors, large retail stores, and manufacturing plants for improving the revenue by promoting the profit-generating item sets.

Published in: 2021 7th International Conference on Advanced Computing and Communication Systems (ICACCS)**Date of Conference:** 19-20 March 2021**INSPEC Accession Number:** 20799984**Date Added to IEEE Xplore:** 03 June 2021**DOI:** 10.1109/ICACCS51430.2021.9441949**► ISBN Information:****Publisher:** IEEE**► ISSN Information:****Conference Location:** Coimbatore, India

 **Contents****I. Introduction**

Data mining is the process of extracting relevant and appropriate data from huge databases. Data mining is also known as 'Knowledge Discovery' or 'Data Discovery'. The traditional data analysis methods are blended with sophisticated algorithms to process large volumes of data. [3] In data mining, previously unknown, interesting patterns and co-relations are identified. Data mining is also related to classical statistics, artificial intelligence, and machine learning in many aspects. It comes under the field of computer science and statistics intending to analyze data. After that, the extracted data is presented to humans for an easy understanding. In general, the data mining task includes data pre-processing, data transformation, data mining, and data post-processing steps

Authors



Figures



References



Keywords



Metrics



More Like This

Data analysis with empirical probability functions as a data mining method: Employing CF-miner and pattern difference quantifiers

2018 Smart City Symposium Prague (SCSP)

Published: 2018

Churn Prediction of Customers in a Retail Business using Exploratory Data Analysis

2022 International Conference on Frontiers of Information Technology (FIT)

Published: 2022

Show More

IEEE Personal Account

CHANGE
USERNAME/PASSWORD

Purchase Details

PAYMENT OPTIONS
VIEW PURCHASED
DOCUMENTS

Profile Information

COMMUNICATIONS
PREFERENCES
PROFESSION AND
EDUCATION
TECHNICAL INTERESTS

Need Help?

US & CANADA: +1 800
678 4333
WORLDWIDE: +1 732
981 0060
CONTACT & SUPPORT

Follow



[About IEEE Xplore](#) | [Contact Us](#) | [Help](#) | [Accessibility](#) | [Terms of Use](#) | [Nondiscrimination Policy](#) | [IEEE Ethics Reporting](#) | [Sitemap](#) | [IEEE Privacy Policy](#)

A not-for-profit organization, IEEE is the world's largest technical professional organization dedicated to advancing technology for the benefit of humanity.

© Copyright 2023 IEEE - All rights reserved.

IEEE Account

- » Change Username/Password
- » Update Address

Purchase Details

- » Payment Options
- » Order History
- » View Purchased Documents

Profile Information

- » [Communications Preferences](#)
- » [Profession and Education](#)
- » [Technical Interests](#)

Need Help?

- » **US & Canada:** +1 800 678 4333
- » **Worldwide:** +1 732 981 0060
- » [Contact & Support](#)

[About IEEE Xplore](#) | [Contact Us](#) | [Help](#) | [Accessibility](#) | [Terms of Use](#) | [Nondiscrimination Policy](#) | [Sitemap](#) | [Privacy & Opting Out of Cookies](#)

A not-for-profit organization, IEEE is the world's largest technical professional organization dedicated to advancing technology for the benefit of humanity.

© Copyright 2023 IEEE - All rights reserved. Use of this web site signifies your agreement to the terms and conditions.

Chapter

Analysis of Sybil Attacks in Online Social Networks Using SyPy

January 2021

DOI: [10.1007/978-981-16-0980-0_16](https://doi.org/10.1007/978-981-16-0980-0_16)

In book: Computer Communication, Networking and IoT (pp.155-167)

Authors:



Christina Roseline



Blessy Antony



Bijitha Balakrishnan



C. V. Chaithra

[Show all 5 authors](#)

Request full-text

Download citation

Copy link



To read the full-text of this research, you can request a copy directly from the authors.

[Citations \(1\)](#)

[References \(18\)](#)

Discover the world's research

- 25+ million members
- 160+ million publication pages
- 2.3+ billion citations

[Join for free](#)

Sponsored videos

No full-text available



To read the full-text of this research, you can request a copy directly from the authors.

Request full-text PDF

Citations (1)

[References \(18\)](#)

... A recommender based on content can already make recommendations based on data from one single user. Supported science publishing systems often employ user-profiles focusing on publications [27,28] or clicks [29]. Alternatively, we build user profiles on things related to social media. ...

... The discrepancy between the prediction operators defines prediction errors ϵ_2 (29) where $\|\cdot\|_2$ stands for the spectral norm of a matrix, considering that ...

Trust management and data protection for online social networks

[Article](#)

[Full-text available](#)

May 2022

Shehab Thabit · Yan Lianshan · Yao Tao · AL-badwi Abdullah

[View](#) [Show abstract](#)

Article [Full-text available](#)

Is it Really Easy to Detect Sybil Attacks in C-ITS Environments: A Position Paper

October 2022 · IEEE Transactions on Intelligent Transportation Systems

● Badis Hammi · Yacine Mohamed Idir · Sherali Zeadally · [...] · ● Nebhen Jamel

In the context of current smart cities, Cooperative Intelligent Transportation Systems (C-ITS) represent one of the main use case scenarios that aim to improve peoples' daily lives. Thus, during the last few years, numerous standards have been adopted to regulate such networks. Within a C-ITS, a large number of messages are exchanged continuously in order to ensure that the different applications ... [\[Show full abstract\]](#)

[View full-text](#)

Article [Full-text available](#)

Detecting sybil attacks using heterogeneous topologies in static wireless sensor network

August 2018 · Journal of Theoretical and Applied Information Technology

● Sohail Abbas · ● Muhammad Haqqad · S. Begum · [...] · ● Muhammad Zahid Khan

Wireless Sensor Network (WSN) is composed of few to several hundred nodes that coordinate to perform a specific action. Data is propagated in multihop fashion from sources to sink(s). Security is an important issue in WSNs, especially when they are used to protect or monitor critical situations. The WSNs require a unique identity per node in order to function properly. However an attack called ... [\[Show full abstract\]](#)

[View full-text](#)

Article [Full-text available](#)

Secure Vehicular Platoon Management against Sybil Attacks

November 2022 · Sensors

Danial Ritzuan Junaidi · ● Maode Ma · [...] · ● R. Su

The capacity of highways has been an ever-present constraint in the 21st century, bringing about the issue of safety with greater likelihoods of traffic accidents occurring. Furthermore, recent global oil prices have inflated to record levels. A potential solution lies in vehicular platooning, which has been garnering attention, but its deployment is uncommon due to cyber security concerns. One ... [\[Show full abstract\]](#)

[View full-text](#)

Conference Paper

Evaluating Sybil Attacks in P2P Infrastructures for Online Social Networks

August 2015

● Francisco Lopez-Fuentes · [...] · Salvador Balleza-Gallegos

[Read more](#)



Chapter

Study on Data Transmission Using Li-Fi in Vehicle to Vehicle Anti-Collision System

June 2021

DOI:10.1007/978-981-16-0965-7_41

In book: Computer Networks, Big Data and IoT (pp.519-540)

Authors:



Rosebell Paul
SCMS Group of Educational Institutions



Neenu Sebastian
SCMS Group of Educational Institutions



P. S. Yadukrishnan



Parvathy Vinod

Request full-text

Download citation

Copy link



To read the full-text of this research, you can request a copy directly from the authors.

Citations (4)

References (16)

Abstract

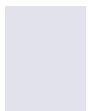
This paper examines the relevance of a fast approaching highly secure and fast data transmission technique using Li-Fi. It describes the upcoming technology Li-Fi and its applications as well as the developments made in it so far. It enlightens on the new era that will soon be used in almost all domains like health sector, school, bank and so on. An application framework design has been studied to analyze the role of Li-Fi in the process of communication. © The Author(s), under exclusive license to Springer Nature Singapore Pte Ltd. 2021.

Discover the world's research

- 25+ million members
- 160+ million publication pages
- 2.3+ billion citations [Join for free](#)

Sponsored videos

No full-text available



To read the full-text of this research, you can request a copy directly from the authors.

Request full-text PDF

Citations (4)

[References \(16\)](#)

... The advent of 5G is envisioned to boost the performance of C-V2X. There have been several other communication protocols suggested for data transmission in vehicular environments [19, 20]. These technologies would enable the infrastructures to become smarter and eventually self-capable of detecting incidents. ...

Traffic Event Reporting Framework Using Mobile Crowdsourcing and Blockchain

Chapter

Jan 2022

● Abin Philip · RA. K. Saravanaguru · P. A. Abhay

[View](#) [Show abstract](#)

Li-Fi based human health monitoring system

Conference Paper

Jan 2023

● Kanagaraj Venusamy · D. David Neels Ponkumar · ● B. Sumathy · P. Malathi

[View](#) [Show abstract](#)

Indoor Navigation using Li-Fi & IoT Technologies

Conference Paper

Apr 2022

Bharanidharan N · Darshan Kalyan B S · K Bala Vishnu Vardhan Reddy · Dharnesh Kumar B

[View](#)

Li-Fi: A Novel Stand-In for Connectivity and Data Transmission in Toll System

Chapter

Jan 2023

● Rosebell Paul · M. Neeraj · P. S. Yadukrishnan

[View](#) [Show abstract](#)

Article

Research on Evasion Control of Vehicle Anti-Collision Warning System

August 2013 · Applied Mechanics and Materials

Jian Hua Wang · Yun Cheng Wang · Hai Feng Ding · [...] · Fei Xie

This paper put forward a kind of vehicle anti-collision warning system and put the emphasis on the research of active control. It introduced the function and composition of the system and expounded its working principle. First the safety distance model was studied based on the vehicle kinetic theory. This model contained longitudinal and lateral safety distance model. And the longitudinal safety ... [\[Show full abstract\]](#)

[Read more](#)

Article

A highway vehicle anti-collision protocol based on broadcasting feedback mechanism

January 2015

Yang Yang · [...] · Nannan Cheng

This paper proposed a vehicle anti-collision protocol using on highways, This protocol is based on broadcast mechanism, and vehicles could broadcast the warning messages to all adjacent nodes in the network as fast as possible. Once the adjacent nodes received the broadcasting warning messages, they will forward the messages to the next hop nodes and the previous node will recognized it as the ... [\[Show full abstract\]](#)

[Read more](#)

Conference Paper

Research on Safety Classification for Vehicle Anti-collision Data by Improved Interval Fuzzy Reasoni...

August 2021

Lijuan Qin · [...] · Yingying Shen

[Read more](#)

Conference Paper

Pulse Laser Ranging Design for Vehicle Anti-collision System

April 2012

Ping Liao · Ruiming Ding · [...] · Yuxin Wu

The most commonly used anti-collision technology in vehicle electronics system is introduced. According to requirements of the vehicle rear-end collision system on ranging module, the pulsed laser ranging is selected to achieve the front distance detection. The laser energy transfer during the flight is analyzed which is the basis for selecting opto electronic devices. Transmitter uses 12V DC ... [\[Show full abstract\]](#)

[Read more](#)





All



ADVANCED SEARCH

Conferences > 2021 International Conference... ?

Pedestrian Counting Using Yolo V3

Publisher: IEEE

Cite This

PDF

Aiswarya Menon ; Bini Omman ; Asha S All Authors

5 Paper Citations

565 Full Text Views



Alerts

Manage Content Alerts Add to Citation Alerts

Abstract



Download PDF

Document Sections

- I. Introduction
- II. Related Techniques
- III. Methodology
- IV. Experimental Result
- V. Conclusion

Show Full Outline

Authors

Figures

References

Citations

Keywords

Abstract: Object detection is the process of determining the presence, location, and type or class of at least one object using a bounding box. The person detection process produce... [View more](#)

Metadata

Abstract:

Object detection is the process of determining the presence, location, and type or class of at least one object using a bounding box. The person detection process produces a bounding box and allot a class label as a person based on YOLO v3. In YOLO v3 the features are learned, divides the image cells and each cell says a bounding box and entity classification directly. There could be more than one bounding box per person, but the system makes use of non-maximum suppression to reduce the number of bounding boxes to one per person. Finally, the number of persons in the image and video are calculated using the count of the bounding boxes. The dataset used for static pedestrian detection is the INRIAdataset and ShanghaiTech dataset. Yolo_Mark is used for marking bounding boxes of persons and gets its annotation files using 243 images from the INRIA dataset. Darknet is used as the framework for implementing YOLOv3. From INRIA Dataset 120 images are used for testing purposes. Testing on the INRIA dataset resulted in an accuracy of 96.1%. From the Shanghai tech-B, dataset 56 images are used for testing. Testing resulted in an accuracy of 87.3%.

Published in: 2021 International Conference on Innovative Trends in Information Technology (ICITIT)

IEEE websites place cookies on your device to give you the best user experience. By using our websites, you agree to the placement of these cookies. To learn more, read our Privacy Policy.

Date of Conference: 11-12 February 2021

INSPEC Accession Number: 2065135

Accept & Close

Date Added to IEEE Xplore: 14 April 2021

DOI: 10.1109/ICITIT51526.2021.9399607

► ISBN Information:

Publisher: IEEE

Conference Location: Kottayam, India

☰ Contents

I. Introduction

Computer vision is the region of study that expects to build up a technique that upholds computers to watch and comprehend the substance of advanced pictures, for example, photos and recordings. Computer vision has a number of multidisciplinary applications like military human-computer interaction, mobile robot navigation, industrial inspection, and medical image analysis. Many popular computer vision applications like object classification, object identification, object verification, object detection [3], and object recognition recognize objects in images or videos.

| | |
|------------|---|
| Authors | ▼ |
| Figures | ▼ |
| References | ▼ |
| Citations | ▼ |
| Keywords | ▼ |
| Metrics | ▼ |

Sign in to Continue Reading

More Like This

A Combined Object Detection Method With Application to Pedestrian Detection

IEEE Access

Published: 2020

Person Re-Identification (Pre-id) in Blur, Low Light, Low Resolution Surveillance Videos: Object Detection and Characterization of Sequences

2021 International Conference on Smart Generation Computing, Communication and Networking (SMART GENCON)

Published: 2021

Show More

IEEE websites place cookies on your device to give you the best user experience. By using our websites, you agree to the placement of these cookies. To learn more, read our Privacy Policy.

Accept & Close



IEEE Personal Account

CHANGE USERNAME/PASSWORD

Purchase Details

PAYMENT OPTIONS
VIEW PURCHASED DOCUMENTS

Profile Information

COMMUNICATIONS PREFERENCES
PROFESSION AND EDUCATION
TECHNICAL INTERESTS

Need Help?

US & CANADA: +1 800 678 4333
WORLDWIDE: +1 732 981 0060
CONTACT & SUPPORT

Follow



[About IEEE Xplore](#) | [Contact Us](#) | [Help](#) | [Accessibility](#) | [Terms of Use](#) | [Nondiscrimination Policy](#) | [IEEE Ethics Reporting](#) | [Sitemap](#) | [IEEE Privacy Policy](#)

A not-for-profit organization, IEEE is the world's largest technical professional organization dedicated to advancing technology for the benefit of humanity.

© Copyright 2023 IEEE - All rights reserved.

IEEE Account

- » Change Username/Password
- » Update Address

Purchase Details

- » Payment Options
- » Order History
- » View Purchased Documents

Profile Information

IEEE websites place cookies on your device to give you the best user experience. By using our websites, you agree to the placement of these cookies. To learn more, read our Privacy Policy.

- » Communications Preferences
- » Profession and Education

Accept & Close

» [Technical Interests](#)

Need Help?

» **US & Canada:** +1 800 678 4333

» **Worldwide:** +1 732 981 0060

» [Contact & Support](#)

[About IEEE Xplore](#) | [Contact Us](#) | [Help](#) | [Accessibility](#) | [Terms of Use](#) | [Nondiscrimination Policy](#) | [Sitemap](#) | [Privacy & Opting Out of Cookies](#)

A not-for-profit organization, IEEE is the world's largest technical professional organization dedicated to advancing technology for the benefit of humanity.
© Copyright 2023 IEEE - All rights reserved. Use of this web site signifies your agreement to the terms and conditions.

IEEE websites place cookies on your device to give you the best user experience. By using our websites, you agree to the placement of these cookies. To learn more, read our [Privacy Policy](#).

Accept & Close



Search & Download more than 27000 research papers



ICCIDT - 2021 (VOLUME 09 - ISSUE 07)

Bio-inspired Metaheuristic Optimization Technique for the Detection of Phishing Emails

DOI : 10.17577/IJERTCONV9IS07022

DOWNLOAD FULL-TEXT PDF

CITE THIS PUBLICATION

- **Open Access**
- Article Download / Views: 217
- **Authors** : Arshey M, Dr. Angel Viji K S
- **Paper ID** : IJERTCONV9IS07022
- **Volume & Issue** : [ICCIDT – 2021 \(Volume 09 – Issue 07\)](#)
- **Published (First Online)**: 04-06-2021
- **ISSN (Online)** : 2278-0181
- **Publisher Name** : IJERT
- **License**: This work is licensed under a [Creative Commons Attribution 4.0 International License](#)

∨ PDF Version

∧ **Text Only Version**

Bio-inspired Metaheuristic Optimization Technique for the Detection of Phishing Emails

Arshey M

Department Of Computer Science and Engineering Noorul Islam Centre for Higher Education, Thuckalay

Dr. Angel Viji K S Department Of Computer Science and Engineering College of Engineering,

Kidangoor

AbstractThe most trending cybersecurity threat all over the world is Phishing, which uses the public through various media especially e-mail, to gather the individuals private particulars. This rapid rise of undesired information needs to be coped with, raising the need to develop suitable and efficient anti-phishing methods. This paper emphasizes a process to detect email phishing based on optimization algorithms using deep belief networks. At the first, the emails are subjected to pre-processing using stemming and stop word removal mechanisms are implemented to assure that the significant words are identified for further processing. Term-Frequency (TF) is used for feature extraction from the significant words, followed by the Bhattacharya distance for feature selection. The features selected are fed as input to the deep belief neural network (DBN), which is then trained using the proposed Earth Worm optimization (EWA) Algorithm. The analysis of the spam mail detection is performed using the datasets and found that the accuracy, sensitivity, and specificity of the proposed EWA DBN are found to be a maximal value of 0.671, 0.814, and 0.804, respectively.

Index TermsE-mail, Phishing, Optimization, deep learning, spam mails, Deep Belief Network(DBN)

1. INTRODUCTION

Technology enhancement brings out fresh criminal ways and many new types of crimes. The Web is upright for developing and refining worldwide commerce to already far-fetched statures, cultivating momentous headways in instruction, and inspiring round-the-world communication that was once seen to be constrained and exorbitant. Regardless, the Web, with its boundless measure and as of now unimaginable capacities, remembers a despairing side for that it has opened windows of effectively dark criminal openings that not in a manner of speaking test, but rather too transcend every actual limit, boundaries, and limitations to detect, rebuke and lessen what appears at being a creating social issue of overall degrees. Cybercrime is

an offense to data, the public, associations, or governments. The idea of digital infringement isn't radically different from the idea of standard bad behavior. Both fuse directly whether act or prohibition, which causes a break of rules of law counterbalanced by the support of the state. [1] Computer-based wrongdoing insinuates any bad behavior that incorporates a system and an organization.

Phishing is the technique for delicate data, similar to pass- words, usernames, and credit card data for noxious purposes, through dissimulating as a dependable individual in electronic correspondence. Phishing messages consist of sites linked with malware. Phishing is subsequently performed utilizing

texting or email parodying, which makes the clients give their subtleties in any phony site that looks and seems indistin- guishable from the real site. Phishing remains an occurrence for social designing strategies that misleads clients, and ad- ventures helpless convenience of present security advances in the web. Phishing is a danger that forces huge negative effects on online media, similar to Twitter, Facebook, and Google+. Programmers clone a site and demand the web clients to give the individual data that is at last sent to the programmers [2]. Additionally, there are various anti-phishing procedures to perform phishing and smishing is a consolidation of Phishing assaults that use a basic instant message or Short Messaging Service (SMS) on mobiles to claim the individual credentials

[3] [4]. Accordingly, it is outstanding that phishing irritated the clients as well as caused financial damage for people and associations [5].

Spam is the undesirable message of a sender sent elec- tronically to a beneficiary, who doesn't have any relationship with the individual [6]. Email spam alludes to a subset of electronic spam that takes enormous time since the clients participate in recognizing and eliminating the undesired mes- sages. The common issues on the web are in regards to email spam. [7]Spamming is the consistently enduring issue that is accessible from the hour of the presence of mailboxes. The methods utilized for separating are progressing with time and the level of spam messages are rising definitely with time, causing tremendous traffic in the messages. In this way, a successful spam channel is utilized for upgrading the efficiency of the client and limits the utilization of the assets related to the data innovation, similar to help work areas.

There are various spam filters utilized alongside the AI techniques, similar to decision trees, Naive Bayes classifiers, k-closest neighbor algorithm, SVM, K-means algorithm, and many more⁸. Machine Learning techniques consequently build up the word records alongside their weights for arranging the messages as two classes. The input

messages could be either spam or not. Also, there are various strategies utilized for identifying spam.

The main aim of this research is to develop an approach for eliminating phishing by recommending an optimization algorithm. The proposed method involves four steps, which include pre-processing, feature extraction, feature selection, and classification of phishing emails. Initially, the stop word elimination and stemming of the input dataset is performed

in the pre-processing stage followed by the feature extraction process. The features are selected based on extracting the keyword frequency from the output of the pre-processing. The next step is the feature selection using Bhattacharya distance to identify the significant features for the classification stage. The selected features are subject to classification using the Deep Belief Network and trained using the proposed EWA.

2. RELATED WORKS

The review of various methods is deliberated in this section. Smadi, S et al. [9] developed an algorithm to detect the zero- day phishing attacks using 2 techniques namely Feature Evaluation and Reduction algorithm and (DENNuRL) Dynamic Evolving Neural Network using a Reinforcement learning algorithm. As per the algorithm, the result revealed a higher performance and provided reasonable error rates. The main drawback of this technique was due to the insufficient amount of dataset chosen for classification, which was critical to group the spam mails.

Barushka. A and Hajek P [10] designed an algorithm to effectively handle the class distributions which shows the imbalance and misclassification costs with some difficult forms of text patterns. The Algorithm namely Distribution-based balancing along with the regularized deep multi-layer perceptrons NN model with rectified linear units (DBB-RDNN-ReL) can help in effectively tackling the class distributions with imbalance. The disadvantage of the method is that it makes use of numerous hidden layers and the units in the model would exhibit noise in the data, which leads to unsatisfactory performance.

Kovalluri, S.S et al. [11] designed a system based on Artificial Intelligence using LSTM. This helped in reducing the application of fake mails to sneak the data, proliferate, and made it difficult to track the victims. The disadvantage of this technique was that this model had errors during sentence generation.

Ruano-Orda's et al. [12] designed a model using the Genetic programming algorithm to be used for datasets that were large and also identified the patterns which improved the accuracy to great extent. However, it further helped in the reduction of the computational overhead related to the e-mail filter server. The main drawback of this technique was the requirement of security features to prevent False Positive errors.

Sonowal, G and Kuppusamy, K.S [13] designed an algorithm that used the Spishing Detection based on the Correlation Algorithm (SmiDCA) that accomplished higher efficiency to confront datasets based on both the English and non-English. However, to improve the accuracy the system had to depend on deep learning technologies.

3. DBN BASED SPAM MAIL CLASSIFICATION

An Email Spam causes affliction in the digital world and it imprints the loss of time, space, and communication bandwidth. Almost more than 40% of the mails are fake nowadays that implies that more than 15 billion emails a day, thereby increasing the price of cyberspace users. This research

work focused on the spam mail classification technique using the Deep Belief Network classifier, tuned perfectly using the Earthworm Algorithm. The dataset is first pre-processed based on which the keywords are identified and followed by feature extraction. This is then followed by feature selection. The selection of features is performed using the Bhattacharya distance. The features retrieved using the Bhattacharya distance are then subjected to spam mail classification in which Deep Belief Network is used which identifies the spam mails. Fig

1. shows the proposed plan for spam mail detection.

Fig. 1. Proposed plan of Email Phishing Detection

1. Pre-processing

Pre-processing is the first step in the identification of phishing attacks. [14] This phase involves 2 processes which include the elimination of stop words and stemming. The dataset for the email is chosen from UCI and Enron and the mail has words as a sentence or a paragraph. The stop words mainly a, an, in, and so on searched are eliminated from the mail. This is followed by stemming in which certain words in the mail document are changed

to their root word. The output of the pre-processing step is known as dictionary words. This in turn acts as input to the feature extraction.

2. Feature extraction

The dictionary words are then put through the feature extraction using Term Frequency which identifies the frequency of the dictionary words used in the particular mail. TF is an arithmetic method of retrieving the significant word from a dataset. Term frequency is an efficient algorithm to extract the frequency of terms from dictionary words and also in the method of assigning word weights. Therefore Term Frequency expresses the total number of times an individual word appears in an email.

3. Feature selection

Feature selection is the method of selecting prominent features from the identified dictionary words. The Bhattacharya distance is computed between the individual feature

and the class and the feature with the maximal Bhattacharya distance is selected as the effective features for the classification using the DBN. The Bhattacharya distance is calculated based on,

(1)

where $BD(g_k, C_l)$ refers to the Bhattacharya distance between the k th feature and the l th class. The mean of the k th feature and the l th class is denoted as $\hat{\mu}_k$ and $\hat{\mu}_l$, and variance of the k th feature and the l th class is denoted as σ_k and σ_l .

4. Classification using Deep Belief Neural Networks

The features identified from the feature selection are classified using the DBN. The classified data are first given as input to the classifier and then trained using the proposed Earthworm Algorithm which in turn tunes the optimal weights of DBN. This helps in differentiating spam mails from relevant mails.

1. Deep Belief Neural networks (DBN):

Deep Belief Network is a generative network and it is implemented by stacking several layers with each middle layer consisting of the visible and hidden neurons [15]. The DBN layers include Restricted Boltzmann Machine (RBM) layers and a Multilayer perceptron (MLP) layer. Each RBM layer in turn consists of its input and hidden layers and the MLP layer comprises the input, hidden, and output layers [16]. The effectiveness of DBN is the interconnection between the hidden and the input neurons that are interlinked by a set of tunable weights. The architecture of the DBN network is shown in Fig 2.

Step 1: Train the 2 layers RBM1 and RBM2. Step 2: Train the MLP layer

The first step involves providing an RBM1 layer with the input data and then subjected to a probability distribution. The data is then encoded using weights to compose an output which forms the input to the RBM2 layer.

The process of training the DBN can be further repeated to retrieve the input to the MLP layer.

- Initialization of MLP weights
- Determine the output of the MLP layer
- Determine the error of the network
- Weight calculation in the MLP layer
- Termination

The following steps are repeated for a maximum number of iterations till a globally optimal solution is obtained.

3) Determination of weights of DBN based on Optimization algorithm: Earthworm Algorithm is a bio-inspired metaheuristic algorithm based on the reproducing pattern of the earthworms [17]. This can be viewed as 2 types of reproduction and the new obtained solutions are calculated by counting the weights for producing new earthworms. The searching tendency in EWA was enhanced by the use of Cauchy op-

erators. In the reproductive capability of the Earthworm, the type-1 Reproduction produces only 1 offspring and the type-2 Reproduction produces 2 or more offspring.

Type-1 Reproduction: In this type of reproduction, the single earthworm is involved in reproduction as earthworms are known as hermaphrodites.

Type-2 Reproduction: This type of reproduction produces two or more two offspring. Crossovers are considered as parents can be changed accordingly to produce the offspring to ensure that offspring produced is not less than zero. The crossover mentioned is single-point, multi-point, and uniform crossover. The parents selected for crossover are based on the strategy named roulette wheel selection.

Case 1: With 2 parents and 1 offspring and it follows a single-point crossover. The multipoint crossover with 2 parents is based on two random numbers generated.

Case 2: With 2 parents and 2 offspring

Case 3: With 3 parents and 3 offspring

The position of the earthworm based on the 2 types of offspring generated can be calculated as,

$$u_{t+1} = \alpha u_t + (1 - \alpha) u_{t+2} \quad (2)$$

Fig. 2. Proposed plan of Email Phishing Detection p, q, p, q, p, q

where, $u_{p,q}$ is the q th element of u_p , which is the position

2) Training phase of DBN:

The DBN classifier has to be trained to acquire the correct weights and biases that help to reveal the spam mails.

of p th the earthworm and is the proportional factor.

The Cauchy operator gives the position of the earthworm based on the formula,

This phase points at fine-tuning the RBM and MLP layers,

$u_1 u$

* R

(3)

which entirely depends on the optimal weights derived using the proposed EWA algorithm.

p, q

p, q q

The newly enhanced optimization algorithm helps in fine-tuning the optimal weights and biases and therefore ensures a minimal level of error values. The following steps are followed in the training of DBN are:

p,q

p,q

where, R indicates the random number obtained by performing the Cauchy distribution and q denotes the weight assigned for the qth position, and u+1 determines the qth position of the pth earthworm at time .

4. EXPERIMENTAL SETUP

The proposed algorithm is implemented using JAVA and the datasets utilized for the analysis include Enron and UCI. The effectiveness of the proposed algorithm for spam mail de- tection is computed based on three metrics, namely accuracy, specificity, and sensitivity. The datasets like Enron and UCI have the original messages which include both ham and spam mails in non-Latin encodings.

1. Performance metrics

The algorithm is analyzed based on the performance met- rics, mainly accuracy, specificity, and sensitivity. The accuracy can be determined by calculating the accurate number of spam mails, Specificity is the metric to determine the negatives which are correctly detected and sensitivity determines the positives correctly identified.

Fig. 3. Comparative analysis based on the training percentage using dataset accuracy

$$\text{Accuracy} = \frac{Tn + Tp}{Tn + Tp + Fn + Fp}$$

$$Tn + Tp + Fn + Fp$$

$$Tn$$

(4)

$$\text{Specificity} = \frac{Tn}{Tn + Fp}$$

$$\text{Sensitivity} = \frac{Tp}{Tp + Fn}$$

$$Tn + Fp$$

$$Tp + Fn$$

(5)

(6)

where Tn refers to the values as true positive, Tp refers to true negative, Fn denotes the false negative values, and Fp denotes the values as false positive.

2. Comparative Analysis

The proposed algorithm is being compared with the following methods namely Naive Bayes (NB) [18], Deep Belief Networks (DBN), and Neural Networks (NN). The proposed EWA-DBN algorithm is employed for the detection of email phishing and compared with the above methods to determine its effectiveness.

1. Analysis of Dataset by varying the data percentage : The figure below denotes the comparative analysis based on the data chosen for training. Fig 3 denotes the comparative analysis based on the accuracy of the algorithm chosen. When the percentage of the data is 50, the accuracy of the methods, NB, DBN, NN and EWA-DBN is 0.5333, 0.5455, 0.5556 and 0.5714, respectively. Fig 4 denotes the comparative analysis on the sensitivity of the algorithm chosen. When the percentage of the data is 50, the sensitivity of the methods, NB, DBN, NN and EWA-DBN, is 0.4558, 0.5531, 0.7035 and 0.7223 respectively. Fig 5 denotes the comparison based on

the specificity of the algorithm chosen. When the data percentage is 50, the specificity of the methods, NB, DBN, NN and EWA- DBN, is 0.5052, 0.5631, 0.7028 and 0.7104, respectively.

3. Comparative discussion

Table 1 shows the comparative results based on the various methods chosen depending on the performance metrics from the dataset ENRON [19] and UCI [20]. The accuracy value of the methods, NB, DBN, NN and EWA-DBN is 0.5233, 0.5465, 0.5568 and 0.6714. The sensitivity range of the

Fig. 4. Comparative analysis based on the training percentage using dataset Sensitivity

Fig. 5. Comparative analysis based on the training percentage using dataset Specificity

methods, NB, DBN, NN and EWA-DBN is 0.4978, 0.5642,

0.7235 and 0.8145 respectively. Similarly, the specificity value of the methods, NB, DBN, NN and EWA-DBN is 0.5152, 0.5845, 0.7238 and 0.8040 respectively. It is evident from the comparison that the proposed new algorithm has accomplished the maximum value with regards to accuracy, sensitivity, and specificity in comparison with the already existing methods.

TABLE I COMPARATIVE DISCUSSION

| Metrics | NN | DBN | NN | EWA-DBN |
|-------------|--------|--------|--------|---------|
| Accuracy | 0.5233 | 0.5465 | 0.5568 | 0.6714 |
| Sensitivity | 0.4978 | 0.5642 | 0.7235 | 0.8145 |
| Specificity | 0.5152 | 0.5845 | 0.7238 | 0.8040 |

5. CONCLUSION

The email phishing has created a havoc among the internet users. The phishing detection is carried out using the optimization-based deep learning networks. The mail

received are first pre-processed to furnish only the selected words to the next step namely feature extraction. The extracted features are then provided to feature selection using the method of Bhat-tacharya distance. This is in turn fed to the classification algorithm based on the deep belief neural networks. The classifier after fine tuning based on the proposed EWA aims at detecting the spam mails effectively. The comparison is performed using the datasets, UCI and Enron, which is analyzed based on the performance metrics, such as accuracy, sensitivity, and specificity, which is 0.671, 0.814, and 0.804, respectively. The research can be further extended by performing hybrid optimizations so as to enhance the phishing detection ratio.

REFERENCES

1. J. Ma, Y. Zhang, Z. Wang, and B. Chen, A new fine-grain sms corpus and its corresponding classifier using probabilistic topic model., *TIIS*, vol. 12, no. 2, pp. 604625, 2018.
2. P. Patil, R. Rane, and M. Bhalekar, Detecting spam and phishing mails using svm and obfuscation url detection algorithm, in *2017 International Conference on Inventive Systems and Control (ICISC)*, pp. 14, IEEE, 2017.
3. S. J. Delany, M. Buckley, and D. Greene, Sms spam filtering: Methods and data, *Expert Systems with Applications*, vol. 39, no. 10, pp. 9899 9908, 2012.
4. L. Zhang, J. Zhu, and T. Yao, An evaluation of statistical spam filtering techniques, *ACM Transactions on Asian Language Information Processing (TALIP)*, vol. 3, no. 4, pp. 243269, 2004.
5. G. DalklcÂ, and D. Sipahi, Spam filtering with sender authentication network, *Computer Communications*, vol. 98, pp. 7279, 2017.
6. B. Zhou, Y. Yao, and J. Luo, Cost-sensitive three-way email spam filtering, *Journal of Intelligent Information Systems*, vol. 42, no. 1, pp. 1945, 2014.
7. G. V. Cormack, *Email spam filtering: A systematic review*, 2008.
8. C. Laorden, X. Ugarte-Pedrero, I. Santos, B. Sanz, J. Nieves, and P. G. Bringas, Study on the effectiveness of anomaly detection for spam filtering, *Information Sciences*, vol. 277, pp. 421444, 2014.

9. S. Smadi, N. Aslam, and L. Zhang, Detection of online phishing email using dynamic evolving neural network based on reinforcement learning, *Decision Support Systems*, vol. 107, pp. 88102, 2018.
10. A. Barushka and P. Hajek, Spam filtering using integrated distribution- based balancing approach and regularized deep neural networks, *Applied Intelligence*, vol. 48, no. 10, pp. 35383556, 2018.
11. S. S. Kovalluri, A. Ashok, and H. Singanamala, Lstm based self- defending ai chatbot providing anti-phishing, in *Proceedings of the first workshop on radical and experiential security*, pp. 4956, 2018.
12. D. Ruano-Orda's, F. Fdez-Riverola, and J. R. Me'ndez, Using evolution- ary computation for discovering spam patterns from e-mail samples, *Information Processing & Management*, vol. 54, no. 2, pp. 303317, 2018.
13. G. Sonowal and K. Kuppusamy, Smidca: an anti-smishing model with machine learning approach, *The Computer Journal*, vol. 61, no. 8, pp. 11431157, 2018.
14. R. M. Silva, T. C. Alberto, T. A. Almeida, and A. Yamakami, Towards filtering undesired short text messages using an online learning approach with semantic indexing, *Expert Systems with Applications*, vol. 83, pp. 314325, 2017.
15. E. Benavides, W. Fuertes, S. Sanchez, and M. Sanchez, Classification of phishing attack solutions by employing deep learning techniques: A systematic literature review, *Developments and advances in defense and security*, pp. 5164, 2020.
16. G. Tzortzis and A. Likas, Deep belief networks for spam filtering, in *19th IEEE International Conference on Tools with Artificial Intelligence (ICTAI 2007)*, vol. 2, pp. 306309, IEEE, 2007.
17. G.-G. Wang, S. Deb, and L. D. S. Coelho, Earthworm optimisation algorithm: a bio- inspired metaheuristic algorithm for global optimisation problems, *International Journal of Bio-Inspired Computation*, vol. 12, no. 1, pp. 122, 2020.
18. I. Androutsopoulos, J. Koutsias, K. V. Chandrinou, and C D. Spyropou- los, An experimental comparison of naive bayesian and keyword-based anti-spam filtering with personal e-mail messages, in *Proceedings of the 23rd annual international ACM SIGIR conference on Research and development in information retrieval*, pp. 160167, 2000.

19. <http://nlp.cs.aueb.gr/softwareanddatasets/Enron>

[Spam/index.html](#), 2021 (accessed Marcp02021).

20. <https://archive.ics.uci.edu/ml/machine-learning-databases/00228>, 2021 (accessed March 20 2021).



[← Fire Detection Approaches for the Modern World: A Review](#)

[Improving Requirement Specification by Prototype Generation from Requirement Models >](#)

Leave a Reply

You must be [logged in](#) to post a comment.

CURRENT ISSUE new



Publish your Paper

Call for Papers

July 2023

Last Date 31 Jul '23

Journal Indexing UPDATED



RECENT POSTS

[Studies on morpho-dynamics of the Coastal Environment and Management using remote sensing technology on some part of the Prakasam district coastal zone , Andhra Pradesh, East Coast of India](#)

[Real Time Object Detection based on YOLOv3 using Python](#)

[A Review on Developments in Catalytic Filters for Production of Bio-Syngas As Green Fuel](#)

[A Review on a Web-Based Hybrid Encryption System for Secure Data Communication](#)

[Influence of Cooling Time and Colorants During Injection Molding of Plastic Closures in a Typical Processing Plant](#)

RECENT COMMENTS

Sreejith on [How To Improve Performance of High Traffic Web Applications](#)

Peter on [Cost and Waste Evaluation of Expanded Polystyrene \(EPS\) Model House in Kenya](#)

Ushus Maria Joseph on [Real Time Detection of Phishing Attacks in Edge Devices](#)

motsoko on [Structural Design of Interlocking Concrete Paving Block](#)

Priya on [The Role and Potential of Information Technology in Agricultural Development](#)

Copyright 2023 © IJERT.ORG





All



ADVANCED SEARCH

Conferences > 2021 7th International Confer... ?

Thwarting Cyber Crime and Phishing Attacks with Machine Learning: A Study

Publisher: IEEE

Cite This

PDF

M Arshey ; K S Angel Viji All Authors

4 Paper Citations

436 Full Text Views



Alerts

Manage Content Alerts
Add to Citation Alerts

Abstract



Document Sections

- I. Introduction
- II. Fundamental Elements of Cyber Crime:
- III. Types of Cyber Crime
- IV. MI Based Cyber Crime Mitigation
- V. Cyber Crime Detection Techniques

Show Full Outline

- Authors
- Figures
- References
- Citations
- Keywords

Abstract:Almost over 4 billion people are currently making rampant usage of the internet. The massive utilization of mobile technology along with the rise of the digital era cause... [View more](#)

Metadata

Abstract:

Almost over 4 billion people are currently making rampant usage of the internet. The massive utilization of mobile technology along with the rise of the digital era caused a socio-technical threat to the Government and to the public. Many new developments in the internet and modern technologies give rise to new illegal and unethical opportunities among which some of them are crime. Cyber crime is an unlawful means which makes use of a digital media either as a tool or as a target or both. Cyber crime cases, which includes mainly the Phishing attacks and many other attacks in the prevailing COVID -19 situation, have reached an alarming rate with the outburst of numerous forms of crime. This paper focuses on various types of cyber crime and targets some of the present day cyber crime attacks based on Phishing, Artificial Intelligence, Cloud technology and Block chain. The principal objective of this work is to identify how Machine Learning can be deployed in detection of diversified fields of cyber crime. The application of various Machine Learning models in the prediction, identification and mitigation of complex threats is also discussed.

Published in: 2021 7th International Conference on Advanced Computing and Communication Systems (ICACCS)

Date of Conference: 19-20 March 2021

INSPEC Accession Number: 20800083

Date Added to IEEE Xplore: 03 June 2021

DOI: 10.1109/ICACCS51430.2021.9441925

Metrics

More Like This

► ISBN Information:

Publisher: IEEE

► ISSN Information:

Conference Location: Coimbatore, India

 Contents



| | |
|------------|---|
| Authors | ▼ |
| Figures | ▼ |
| References | ▼ |
| Citations | ▼ |
| Keywords | ▼ |
| Metrics | ▼ |

IEEE Personal Account

CHANGE
USERNAME/PASSWORD

Purchase Details

PAYMENT OPTIONS
VIEW PURCHASED
DOCUMENTS

Profile Information

COMMUNICATIONS
PREFERENCES
PROFESSION AND
EDUCATION
TECHNICAL INTERESTS

Need Help?

US & CANADA: +1 800
678 4333
WORLDWIDE: +1 732
981 0060
CONTACT & SUPPORT

Follow



[About IEEE Xplore](#) | [Contact Us](#) | [Help](#) | [Accessibility](#) | [Terms of Use](#) | [Nondiscrimination Policy](#) | [IEEE Ethics Reporting](#) | [Sitemap](#) | [IEEE Privacy Policy](#)

A not-for-profit organization, IEEE is the world's largest technical professional organization dedicated to advancing technology for the benefit of humanity.

© Copyright 2023 IEEE - All rights reserved.

IEEE Account

- » [Change Username/Password](#)
- » [Update Address](#)

Purchase Details

- » [Payment Options](#)
- » [Order History](#)
- » [View Purchased Documents](#)

Profile Information

- » [Communications Preferences](#)
- » [Profession and Education](#)

» Technical Interests

Need Help?

» **US & Canada:** +1 800 678 4333

» **Worldwide:** +1 732 981 0060

» Contact & Support

[About IEEE Xplore](#) | [Contact Us](#) | [Help](#) | [Accessibility](#) | [Terms of Use](#) | [Nondiscrimination Policy](#) | [Sitemap](#) | [Privacy & Opting Out of Cookies](#)

A not-for-profit organization, IEEE is the world's largest technical professional organization dedicated to advancing technology for the benefit of humanity.

© Copyright 2023 IEEE - All rights reserved. Use of this web site signifies your agreement to the terms and conditions.



All



ADVANCED SEARCH

Conferences > 2021 Third International Conf... ?

Sentiment Analysis Using Deep Learning

Publisher: IEEE

Cite This

PDF

P C Shilpa ; Rissa Shereen ; Susmi Jacob ; P Vinod All Authors

8 Paper Citations

346 Full Text Views



Alerts

Manage Content Alerts Add to Citation Alerts

Abstract



Download PDF

Document Sections

- I. Introduction
- II. Background and Related Work
- III. System Architecture
- IV. Methodology
- V. Experiments

Show Full Outline

Authors

Figures

References

Citations

Keywords

Abstract: Emotion recognition from text is crucial Natural Language Processing task which can contribute enormous benefits to different areas such as artificial intelligence, human... **View more**

Metadata

Abstract:

Emotion recognition from text is crucial Natural Language Processing task which can contribute enormous benefits to different areas such as artificial intelligence, human interaction with computers etc. Emotions are physiologic thoughts engendered in human reactions to the events. Analysis of these emotions without facial and voice modulation are critical and requires a supervisory approach for proper interpretation of emotions. In spite of these challenges, it's essential to acknowledge the human emotions as they progressively communicate using mistreatment text through social media applications such as Facebook, Twitter etc. In this paper, we propose a sentimental classification of multitude of tweets. Here, we use deep learning techniques to classify the sentiments of an expression into positive or negative emotions. The positive emotions are further classified into enthusiasm, fun, happiness, love, neutral, relief, surprise and negative emotions are classified into anger, boredom, emptiness, hate, sadness, worry. We experimented and evaluated the method using Recurrent Neural Networks and Long short-term memory on three different datasets to show how to achieve high emotion classification accuracy. A through evaluation shows that the system gains emotion prediction on LSTM model with 88.47% accuracy for positive/negative classification and 89.13% and 91.3% accuracy for positive and negative subclass respectively.

IEEE websites place cookies on your device to give you the best user experience. By using our websites you agree to the placement of these cookies. To learn more, read our Privacy Policy.

Published in: 2021 Third International Conference on Intelligent Communication Technologies and Virtual Mobile Networks (ICICV) **Accept & Close**

More Like This

Date of Conference: 04-06 February 2021

INSPEC Accession Number: 20513093

Date Added to IEEE Xplore: 31 March 2021

DOI: 10.1109/ICICV50876.2021.9388382

► **ISBN Information:**

Publisher: IEEE

Conference Location: Tirunelveli, India

☰ Contents

I. Introduction

Twitter is a social networking web site where members can post messages in the form of "tweets". This is a platform where individuals can share ideas or sentiments on diverse subjects, fields or themes. It is a collection of user thoughts and sentiments spanning across various topics including standard net articles and net blogs. The quantity of pertinent data is bigger for twitter, when contrasted with former social media and blogging platforms. When compared to other blogging sites, the response rate on Twitter is much more quicker. Sentiment analysis is widely utilized by different parties such as shoppers or marketers to gain insights into merchandise or understand the market trends [1].

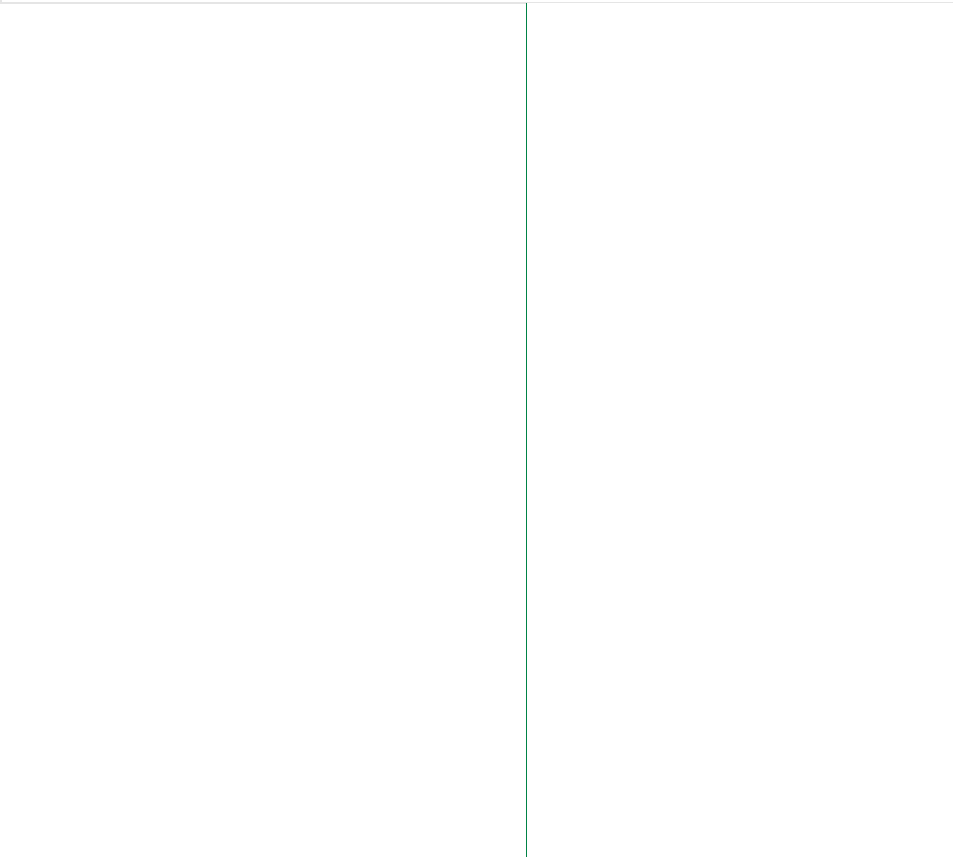
| | |
|------------|---|
| Authors | ▼ |
| Figures | ▼ |
| References | ▼ |
| Citations | ▼ |
| Keywords | ▼ |
| Metrics | ▼ |

More Like This

Text Mining and Emotion Classification on Monkeypox Twitter Dataset: A Deep Learning-Natural Language Processing (NLP) Approach
 IEEE Access
 Published: 2023

2019 Sixth International Conference on Social Networks Analysis, Management and Security (SNAMS)
 Published: 2019
 IEEE websites place cookies on your device to give you the best user experience. By using our websites, you agree to the placement of these cookies. To learn more, read our Privacy Policy.

Accept & Close



IEEE Personal Account

CHANGE USERNAME/PASSWORD

Purchase Details

PAYMENT OPTIONS
VIEW PURCHASED DOCUMENTS

Profile Information

COMMUNICATIONS PREFERENCES
PROFESSION AND EDUCATION
TECHNICAL INTERESTS

Need Help?

US & CANADA: +1 800 678 4333
WORLDWIDE: +1 732 981 0060
CONTACT & SUPPORT

Follow



[About IEEE Xplore](#) | [Contact Us](#) | [Help](#) | [Accessibility](#) | [Terms of Use](#) | [Nondiscrimination Policy](#) | [IEEE Ethics Reporting](#) | [Sitemap](#) | [IEEE Privacy Policy](#)

A not-for-profit organization, IEEE is the world's largest technical professional organization dedicated to advancing technology for the benefit of humanity.

© Copyright 2023 IEEE - All rights reserved.

IEEE Account

- » Change Username/Password
- » Update Address

Purchase Details

» Payment Options

» Order History

IEEE websites place cookies on your device to give you the best user experience. By using our websites, you agree to the placement of these cookies. To learn more, read our Privacy Policy.

» View Purchased Documents
Profile Information

Accept & Close

- » [Communications Preferences](#)
- » [Profession and Education](#)
- » [Technical Interests](#)

Need Help?

- » **US & Canada:** +1 800 678 4333
- » **Worldwide:** +1 732 981 0060
- » [Contact & Support](#)

[About IEEE Xplore](#) | [Contact Us](#) | [Help](#) | [Accessibility](#) | [Terms of Use](#) | [Nondiscrimination Policy](#) | [Sitemap](#) | [Privacy & Opting Out of Cookies](#)

A not-for-profit organization, IEEE is the world's largest technical professional organization dedicated to advancing technology for the benefit of humanity.
© Copyright 2023 IEEE - All rights reserved. Use of this web site signifies your agreement to the terms and conditions.

IEEE websites place cookies on your device to give you the best user experience. By using our websites, you agree to the placement of these cookies. To learn more, read our [Privacy Policy](#).

Accept & Close



All



ADVANCED SEARCH

Conferences > 2021 Seventh International co... ?

Segmentation of Spinal Canal using Active Contour Model

Publisher: IEEE

Cite This

PDF

Gayathry S Warriar; K.S. Angel Viji All Authors

102 Full Text Views



Alerts

Manage Content Alerts Add to Citation Alerts

Abstract



Document Sections

- I. Introduction
- II. Literature Review
- III. Proposed System
- IV. Experimental Results
- V. Conclusion

Abstract: Today, the lifestyle of people has paved the way for rise in spinal cord disorders. Severe cases have been reported which could be treated if diagnosed early. Scoliosis i... **View more**

Metadata

Abstract:

Today, the lifestyle of people has paved the way for rise in spinal cord disorders. Severe cases have been reported which could be treated if diagnosed early. Scoliosis is a deformity to spine and ribs which is the primary cause of spinal curvature. The major challenge of scoliosis disease is the unnoticeable change in the orientation of spinal column at its early stage. Moreover, it is visually detectable only in the prodromal stage. The early diagnosis could help cure the disease through exercises and minor surgeries. Depending on manual diagnosis techniques is a tiring task as it can deliver inaccurate results. An automatic segmentation method which helps in the early diagnosis is proposed in this paper. Initially, CT image which is the input is fed into the system. CT images have high contrast between bone and adjacent tissues. Sagittal view datasets have been chosen in order to calculate the cob angle for the measurement of scoliosis intensity. Further, distortions are removed from the image and pre processing is performed followed by K-means clustering which detects the spinal canal. In order to segment the required features, the output of clustering is loaded to Active Contour Model. Finally, segmentation of spinal canal is completed. Experimental results prove the accuracy of 95%,86.86%,92.22% for Lumbar Vertebrae CT , Lumbar spine CT, Lumbar spine CT with multiple compression fractures respectively for the proposed system which is greater than traditional diagnosis methods. Subsequently, this would be a revolutionary study which assists the doctors for the early diagnosis of the disease.

- Authors
- Figures
- References
- Keywords
- Metrics

IEEE websites place cookies on your device to give you the best user experience. By using our websites, you agree to the placement of these cookies. To learn more, read our Privacy Policy.

Accept & Close

Date of Conference: 25-27 March 2021**INSPEC Accession Number:** 20727875**Date Added to IEEE Xplore:** 04 June 2021**DOI:** 10.1109/ICBSII51839.2021.9445160**► ISBN Information:****Publisher:** IEEE**Conference Location:** Chennai, India

☰ Contents

I. Introduction

The progress in technology has altered the lifestyle of people which resulted in spinal disorders. People hardly identify the disease at its early stage. Subsequently, the disease becomes the part of their life as it cannot be cured as whole. Early diagnosis could save the patient affected with the disorders and give a complete cure. The major challenge in disease detection is the unnoticeable change in early stages. Today, various techniques are available for the early diagnosis. Relying on manual detection techniques could provide inaccurate results. Spinal curvature defects refer to the deformity in the column. The vertebrae in human body constitute thoracic, cervical, lumbar and sacro coccygeal vertebrae. The deformities in these vertebrae results in spinal disorders which further affects the posture and body movement. The paper mainly focuses on the patients affected by scoliosis disease. The experiment is conducted based on the various stages of scoliosis disease. Scoliosis is a disease affecting spine which cannot be cured if not diagnosed early. It is commonly observed in thoracolumbar region.

Authors



Figures



References



Keywords



Metrics



More Like This

Computer aided monitoring of fibrous dysplasia disease in craniofacial bones

2004 2nd IEEE International Symposium on Biomedical Imaging: Nano to Macro (IEEE Cat No. 04EX821)

Published: 2004

IEEE websites place cookies on your device to give you the best user experience. By using our websites, you agree to the placement of these cookies. To learn more, read our Privacy Policy.

[Accept & Close](#)

Published: 2012

Show More

IEEE Personal Account

CHANGE USERNAME/PASSWORD

Purchase Details

PAYMENT OPTIONS
VIEW PURCHASED DOCUMENTS

Profile Information

COMMUNICATIONS PREFERENCES
PROFESSION AND EDUCATION
TECHNICAL INTERESTS

Need Help?

US & CANADA: +1 800 678 4333
WORLDWIDE: +1 732 981 0060
CONTACT & SUPPORT

Follow



[About IEEE Xplore](#) | [Contact Us](#) | [Help](#) | [Accessibility](#) | [Terms of Use](#) | [Nondiscrimination Policy](#) | [IEEE Ethics Reporting](#) | [Sitemap](#) | [IEEE Privacy Policy](#)

A not-for-profit organization, IEEE is the world's largest technical professional organization dedicated to advancing technology for the benefit of humanity.

© Copyright 2023 IEEE - All rights reserved.

IEEE Account

- » Change Username/Password
- » Update Address

Purchase Details

IEEE websites place cookies on your device to give you the best user experience. By using our websites, you agree to the placement of these cookies. To learn more, read our [Privacy Policy](#).

Accept & Close

» View Purchased Documents

Profile Information

» Communications Preferences

» Profession and Education

» Technical Interests

Need Help?

» **US & Canada:** +1 800 678 4333

» **Worldwide:** +1 732 981 0060

» Contact & Support

[About IEEE Xplore](#) | [Contact Us](#) | [Help](#) | [Accessibility](#) | [Terms of Use](#) | [Nondiscrimination Policy](#) | [Sitemap](#) | [Privacy & Opting Out of Cookies](#)

A not-for-profit organization, IEEE is the world's largest technical professional organization dedicated to advancing technology for the benefit of humanity.
© Copyright 2023 IEEE - All rights reserved. Use of this web site signifies your agreement to the terms and conditions.

IEEE websites place cookies on your device to give you the best user experience. By using our websites, you agree to the placement of these cookies. To learn more, read our [Privacy Policy](#).

Accept & Close



All



ADVANCED SEARCH

Conferences > 2021 Third International Conf...

Twitter Sentiments: A Machine Learning Approach

Publisher: IEEE

Cite This

PDF

Binu John ; C Vishnu ; Rebecca Joshua ; KA Dhanya All Authors

71 Full Text Views



Alerts

Manage Content Alerts Add to Citation Alerts

Abstract



Document Sections

- I. Introduction
- II. Related Works
- III. Proposed Method
- IV. Results and Discussions
- V. Conclusion

Abstract:Sentiment evaluation is the problem of examining texts,critiques, mind and conditioned emotional response published with the aid of various users in microblogging systems... **View more**

Metadata

Abstract:

Sentiment evaluation is the problem of examining texts,critiques, mind and conditioned emotional response published with the aid of various users in microblogging systems. Twitter is one of the maximum extensively used micro running a blog systems and has proved to be the biggest source of statistics.Twitter can give a clear cut view about the current trends. A big dataset of tweets is used to perform sentiment evaluation. The tweets are labeled into two classes, positive and negative. There are various techniques which can be utilised to perform this task. In this paper we aim to perform a comparison between a multilayer perceptron and a factorization machine for classification of tweets in the Sentiment 140 dataset. We apply this approach using two different lexical resources namely AFFIN dictionary and SentiWordNet. The generated models are compared based on the lexicon used as well as the classifier adopted (multilayer perceptron or factorization machine) for their accuracy and training time.

Published in: 2021 Third International Conference on Intelligent Communication Technologies and Virtual Mobile Networks (ICICV)

Authors

Figures

References

Keywords

Metrics

More Like This

IEEE websites place cookies on your device to give you the best user experience. By using our websites, you agree to the placement of these cookies. To learn more, read our Privacy Policy.

Accept & Close

► ISBN Information:

Publisher: IEEE

Conference Location: Tirunelveli, India

☰ Contents

I. Introduction

Artificial Intelligence (AI) deals with making computers work like humans. This is accomplished by observing human ways of thinking and decision making and applying the outcomes to develop software and systems comparable to human capabilities. AI has been utilized in numerous fields like speech recognition, hand writing recognition, gaming and robotics. Natural Language Processing (NLP) which is a subfield of AI has a range of techniques for the purpose of obtaining human-like language processing for different tasks or applications [1]. It is an effort to get computers closer to human level understanding of language. Sentiment Analysis falls under NLP. It is a process by which all the content can be evaluated to represent the ideas, beliefs and opinions of the public. It can be accomplished at various degrees like document, section, paragraph and phrase level. With the upward push of social networking tendencies there was a surge of online generated content material. Many people sign up for online readings and opinions on microblogging websites. Twitter is one of the broadly followed micro blogging platform for expression of opinion and experience. It was created and launched in the year 2006 [2]. It evolved as a golden platform for companies to disclose about their brands and success. Twitter users include a variety of users ranging from regular users, celebrities, politicians, entrepreneurs, veterans and other persons of influence. The primary advantages of performing sentiment analysis encompass scalability and real time evaluation. Efficiency and cost effectiveness of processing large huge data contributes to scalability. Real time analysis is performing analysis on real time data which can be tweets that are tweeted in a certain scenarios or even critical situations. Sentiment analysis systems help the companies to get meaning of the sea of data by automating business process which saves long hours of manual data processing.

| | |
|------------|---|
| Authors | ▼ |
| Figures | ▼ |
| References | ▼ |
| Keywords | ▼ |
| Metrics | ▼ |

More Like This

IEEE websites place cookies on your device to give you the best user experience. By using our websites,

you agree to the placement of these cookies. To learn more, read our Privacy Policy.

Accept & Close

IEEE Access
Published: 2023

Blockchain-Based Event Detection and Trust Verification Using Natural Language Processing and Machine Learning

IEEE Access
Published: 2022

Show More

IEEE Personal Account

CHANGE
USERNAME/PASSWORD

Purchase Details

PAYMENT OPTIONS
VIEW PURCHASED
DOCUMENTS

Profile Information

COMMUNICATIONS
PREFERENCES
PROFESSION AND
EDUCATION
TECHNICAL INTERESTS

Need Help?

US & CANADA: +1 800
678 4333
WORLDWIDE: +1 732
981 0060
CONTACT & SUPPORT

Follow



About IEEE Xplore | Contact Us | Help | Accessibility | Terms of Use | Nondiscrimination Policy | IEEE Ethics Reporting | Sitemap | IEEE Privacy Policy

A not-for-profit organization, IEEE is the world's largest technical professional organization dedicated to advancing technology for the benefit of humanity.

© Copyright 2023 IEEE - All rights reserved.

IEEE Account place cookies on your device to give you the best user experience. By using our websites, you agree to the placement of these cookies. To learn more, read our Privacy Policy.

Accept & Close

» Update Address

Purchase Details

» Payment Options

» Order History

» View Purchased Documents

Profile Information

» Communications Preferences

» Profession and Education

» Technical Interests

Need Help?

» **US & Canada:** +1 800 678 4333

» **Worldwide:** +1 732 981 0060

» Contact & Support

[About IEEE Xplore](#) | [Contact Us](#) | [Help](#) | [Accessibility](#) | [Terms of Use](#) | [Nondiscrimination Policy](#) | [Sitemap](#) | [Privacy & Opting Out of Cookies](#)

A not-for-profit organization, IEEE is the world's largest technical professional organization dedicated to advancing technology for the benefit of humanity.

© Copyright 2023 IEEE - All rights reserved. Use of this web site signifies your agreement to the terms and conditions.

IEEE websites place cookies on your device to give you the best user experience. By using our websites, you agree to the placement of these cookies. To learn more, read our [Privacy Policy](#).

Accept & Close




Symposium on Machine Learning and Metaheuristics Algorithms, and Applications

SoMMA 2020: **Machine Learning and Metaheuristics Algorithms, and Applications** pp 221–231

[Home](#) > [Machine Learning and Metaheuristics Algorithms, and Applications](#) > [Conference paper](#)

Detection of Obfuscated Mobile Malware with Machine Learning and Deep Learning Models

[K. A. Dhanya](#) , [O. K. Dheesha](#), [T. Gireesh Kumar](#) & [P. Vinod](#)

Conference paper | [First Online: 06 February 2021](#)

1081 Accesses | **4** Citations

Part of the [Communications in Computer and Information Science](#) book series (CCIS, volume 1366)

Abstract

Obfuscation techniques are used by malware authors to conceal malicious code and surpass the antivirus scanning. Machine Learning techniques especially deep learning techniques are strong enough to identify obfuscated malware samples. Performance of

deep learning model on obfuscated malware detection is compared with conventional machine learning models like Random Forest (RF), Classification and Regression Trees (CART) and K Nearest Neighbour (KNN). Both Static (hardware and permission) and dynamic features (system calls) are considered for evaluating the performance. The models are evaluated using metrics which are precision, recall, F1-score and accuracy. Obfuscation transformation attribution is also addressed in this work using association rule mining. Random forest produced best outcome with F1-Score of 0.99 with benign samples, 0.95 with malware and 0.94 with obfuscated malware with system calls as features. Deep learning network with feed forward architecture is capable of identifying benign, malware, obfuscated malware samples with F1-Score of 0.99, 0.96 and 0.97 respectively.

Keywords

Obfuscated malware detection

Machine learning Deep learning

Random forest

Classification and regression trees

K nearest neighbor

This is a preview of subscription content, [access via](#)

[your institution.](#)

▼ Chapter

EUR 29.95

Price includes VAT (India)

- Available as PDF
- Read on any device
- Instant download
- Own it forever

Buy Chapter

▼ eBook

EUR 42.79

Price includes VAT (India)

- Available as EPUB and PDF
- Read on any device
- Instant download
- Own it forever

Buy eBook

▼ Softcover Book

EUR 49.99

Price excludes VAT (India)

- Compact, lightweight edition
- Dispatched in 3 to 5 business days
- Free shipping worldwide - [see info](#)

Buy Softcover Book

Tax calculation will be finalised at checkout

Purchases are for personal use only

[Learn about institutional subscriptions](#)

References

1. Kaspersky Lab. <https://securelist.com/it-threat-evolution-q3-2018-statistics/88689/>. Accessed 4 May 2019

2. McAfee Labs Threats Report. <https://www.mcafee.com/enterprise/en-us/assets/reports/rp-quarterly-threats-sep-2018.pdf>. Accessed 20 May 2020

3. Gartner Report. <https://www.gartner.com/en/newsroom/press-releases>. Accessed 15 Apr 2019

4. Scott, J.: Signature Based Malware Detection is Dead. Institute for Critical Infrastructure Technology, Illinois (2017)

5. Mirzaei, O., de Fuentes, J.M., Tapiador, J., Gonzalez-Manzano, L.: AndrODet: an adaptive Android obfuscation detector. Future Gener. Comput. Syst. **90**, 240–261 (2019)

6. Mohammadinooshan, A., Ulf, K., Nahid, S.: Comment on “AndrODet: an adaptive Android obfuscation detector”. arXiv preprint [arXiv:1910.06192](https://arxiv.org/abs/1910.06192) (2019)

7. Ikram, M., Beaume, P., Kâafar, M.A.: DaDiDroid: an obfuscation resilient tool for detecting android malware via weighted directed call graph modelling. arXiv preprint [arXiv:1905.09136](https://arxiv.org/abs/1905.09136) (2019)

8. Suarez-Tangil, G., Dash, S.K., Ahmadi, M., Kinder, J., Giacinto, G., Cavallaro, L.: DroidSieve: fast and accurate classification of obfuscated Android malware. In: Proceedings of the Seventh ACM on Conference on Data and Application Security and Privacy, pp. 309–320 (2017)

9. Wang, Y., Atanas, R.: Who changed you? Obfuscator identification for Android. In: 2017 IEEE/ACM 4th International Conference on Mobile Software Engineering and Systems (MOBILESoft), pp. 154–164. IEEE (2017)

10. Garcia, J., Hammad, M., Malek, S.: Lightweight, obfuscation-resilient detection and family identification of Android malware. ACM Trans. Softw. Eng. Methodol. (TOSEM) **26**(3), 1–29 (2018)

11. Google Play Store.
<https://play.google.com/store?hl=en>. Accessed 25 Feb 2019

12. Virustotal. <https://developers.virustotal.com>.

Accessed 25 Feb 2019

13. Arp, D., Spreitzenbarth, M., Hubner, M., Gascon, H., Rieck, K., Siemens, C.E.R.T.: Drebin: effective and explainable detection of android malware in your pocket. In: NDSS, vol. 14, pp. 23–26 (2014)

14. PRAGard Dataset.

[http://pralab.diee.unica.it/en/AndroidPRAGuard Dataset](http://pralab.diee.unica.it/en/AndroidPRAGuardDataset). Accessed 5 Mar 2019

15. Android Asset Packaging Tool.

<https://developer.android.com/studio/command-line/aapt2>. Accessed 15 Mar 2019

16. Android Debug Bridge.

<https://developer.android.com/studio/command-line/adb>. Accessed 15 Mar 2019

17. Android Monkey Runner.

<https://developer.android.com/studio/test/monkey>. Accessed 15 Mar 2019

18. Gościak, J., Łukaszuk, T.: Application of the recursive feature elimination and the relaxed linear separability feature selection algorithms to

gene expression data analysis. *Adv. Comput. Sci. Res.* **10**, 39–52 (2013)

19. Zakharov, R., Dupont, P.: Ensemble logistic regression for feature selection. In: Loog, M., Wessels, L., Reinders, M.J.T., de Ridder, D. (eds.) *PRIB 2011. LNCS*, vol. 7036, pp. 133–144. Springer, Heidelberg (2011).
https://doi.org/10.1007/978-3-642-24855-9_12

20. Biau, G.: Analysis of a random forests model. *J. Mach. Learn. Res.* **13**(1), 1063–1095 (2012)

21. Loh, W.-Y.: Classification and regression trees. *Wiley Interdiscip. Rev.: Data Min. Knowl. Discov.* **1**(1), 14–23 (2011)

22. Cunningham, P., Delany, S.: K-nearest neighbour classifiers. Technical report. UCD School of Computer Science and Informatics (2007)

23. Srivastava, N., Hinton, G., Krizhevsky, A., Sutskever, I., Salakhutdinov, R.: Dropout: a simple way to prevent neural networks from overfitting. *J. Mach. Learn. Res.* **15**(1), 1929–1958 (2014)

24. Nwankpa, C., Ijomah, W., Gachagan, A., Marshall, S.: Activation functions: comparison of trends in practice and research for deep learning. arXiv preprint [arXiv:1811.03378](https://arxiv.org/abs/1811.03378) (2018)

25. Hossin, M., Sulaiman, M.N.: A review on evaluation metrics for data classification evaluations. *Int. J. Data Min. Knowl. Manag. Process* **5**(2), 1 (2015)

26. Agarwal, R., Srikant, R.: Fast algorithms for mining association rules. In: *Proceedings of the 20th VLDB Conference*, pp. 487–499 (1994)

27. Alzaylaee, M.K., Yerima, S.Y., Sezer, S.: DL-Droid: deep learning based Android malware detection using real devices. *Comput. Secur.* **89**, 101663 (2020)

Author information

Authors and Affiliations

TIFAC CORE in Cyber Security, Amrita School of Engineering, Amrita University, Coimbatore, India

K. A. Dhanya & T. Gireesh Kumar

SCMS School of Engineering and Technology, Cochin, India

O. K. Dheesha & P. Vinod

Corresponding author

Correspondence to [K. A. Dhanya](#).

Editor information

Editors and Affiliations

**Indian Institute of Information Technology and
Management - Kerala, Trivandrum, India**

Prof. Sabu M. Thampi

University of Florida, Gainesville, FL, USA

Selwyn Piramuthu

Providence University, Taichung, Taiwan

Dr. Kuan-Ching Li

Università degli Studi di Firenze, Florence, Italy

Prof. Stefano Berretti

**Wrocław University of Technology, Wrocław,
Poland**

Prof. Michal Wozniak

**Hankuk University of Foreign Studies, Yongin,
Korea (Republic of)**

Dr. Dhananjay Singh

Rights and permissions

[Reprints and Permissions](#)

Copyright information

© 2021 Springer Nature Singapore Pte Ltd.

About this paper

Cite this paper

Dhanya, K.A., Dheesha, O.K., Gireesh Kumar, T., Vinod, P. (2021). Detection of Obfuscated Mobile Malware with Machine Learning and Deep Learning Models. In: Thampi, S.M., Piramuthu, S., Li, K.C., Berretti, S., Wozniak, M., Singh, D. (eds) Machine Learning and Metaheuristics Algorithms, and Applications. SoMMA 2020. Communications in Computer and Information Science, vol 1366. Springer, Singapore. https://doi.org/10.1007/978-981-16-0419-5_18

[.RIS](#) [.ENW](#) [.BIB](#)

| DOI | Published | Publisher Name |
|---|------------------|---------------------|
| https://doi.org/10.1007/978-981-16-0419-5_18 | 06 February 2021 | Springer, Singapore |

| Print ISBN | Online ISBN | eBook Packages |
|-------------------|-------------------|--|
| 978-981-16-0418-8 | 978-981-16-0419-5 | Computer Science Computer Science (R0) |



All



ADVANCED SEARCH

Conferences > 2021 International Conference...

Analysing Gender and Age Aspects of Cyberbullying through Online Social Media

Publisher: IEEE

Cite This

PDF

Mariya Raphael ; P J Parvathi ; Rizwana Yasmin Hashim ; Rohan J Thevara ; P Deepasree Varma. All Authors

108 Full Text Views



Alerts

Manage Content Alerts Add to Citation Alerts

Abstract



Download PDF

Document Sections

- I. Introduction
- II. Literature Survey
- III. Research Question
- IV. Dataset
- V. Research Methodology

Show Full Outline

Authors

Figures

References

Keywords

Metrics

Abstract:In this paper, we focus at tracking down cyberbullies and categorize them based on their age and gender. The dataset that we use to analyze this information is provided b... [View more](#)

Metadata

Abstract:

In this paper, we focus at tracking down cyberbullies and categorize them based on their age and gender. The dataset that we use to analyze this information is provided by the MySpace group data labeled for cyberbullying. Machine learning classifiers are trained using this data to detect cyberbullies and later we analyze the age and gender patterns of those cyberbullies. We look for features that are simple to extract as well as yield good outcomes. As appropriate training data is often tough to obtain in machine learning-specially in the domain of cyberbullying detection - we also examine to what extend does lesser amounts of training data would contribute to better outcomes by performing cross-validation. Our findings show that employing a few yet expressive features has a significant benefit in detecting cyberbullies, particularly when size of training data is small.

Published in: 2021 International Conference on Advances in Computing and Communications (ICACC)

Date of Conference: 21-23 October 2021

INSPEC Accession Number: 21623484

Date Added to IEEE Xplore: 15 February 2022

DOI: 10.1109/ICACC-202152719.2021.9708197

IEEE websites place cookies on your device to give you the best user experience. By using our websites, you agree to the placement of these cookies. To learn more, read our Privacy Policy.

Accept & Close

 Contents

I. Introduction

Social networking sites are the platforms where a person can interact with other users despite any location and physical limitations. Billions of users are part of the ever-changing and ever-evolving social media. Individuals have completely accepted the web for mingling and conveying. Throughout the most recent decade, advancements in the internet have empowered everybody across topographical partitions. Along with these technological improvements, the negative impact of cyber activity has also received a lot of attention.

Sign in to Continue Reading

| | |
|------------|---|
| Authors | ▼ |
| Figures | ▼ |
| References | ▼ |
| Keywords | ▼ |
| Metrics | ▼ |

More Like This

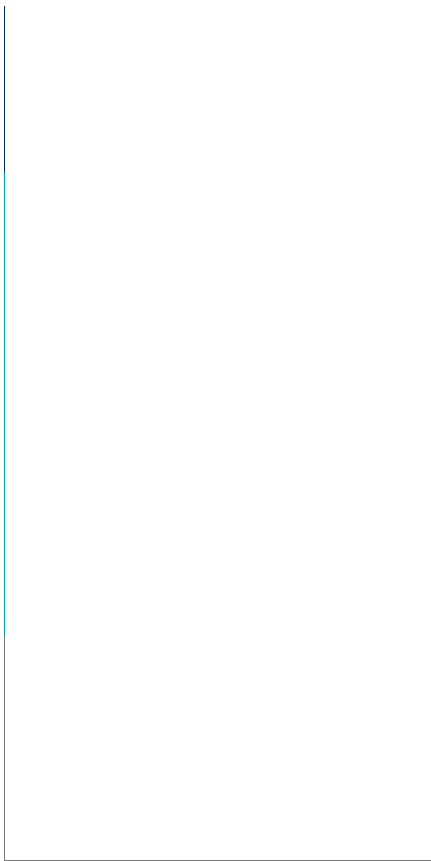
Sentiment Assessment of Brand Advertising on Gender Issues on Social Network: A Case Study of Femvertising on Sina Weibo in China
2021 4th International Conference on Artificial Intelligence and Big Data (ICAIBD)
Published: 2021

Towards a gold standard dataset for Open Information Extraction in Italian
2019 Sixth International Conference on Social Networks Analysis, Management and Security (SNAMS)
Published: 2019

Show More

IEEE websites place cookies on your device to give you the best user experience. By using our websites, you agree to the placement of these cookies. To learn more, read our Privacy Policy.

Accept & Close



IEEE Personal Account

CHANGE USERNAME/PASSWORD

Purchase Details

PAYMENT OPTIONS
VIEW PURCHASED DOCUMENTS

Profile Information

COMMUNICATIONS PREFERENCES
PROFESSION AND EDUCATION
TECHNICAL INTERESTS

Need Help?

US & CANADA: +1 800 678 4333
WORLDWIDE: +1 732 981 0060
CONTACT & SUPPORT

Follow



[About IEEE Xplore](#) | [Contact Us](#) | [Help](#) | [Accessibility](#) | [Terms of Use](#) | [Nondiscrimination Policy](#) | [IEEE Ethics Reporting](#) | [Sitemap](#) | [IEEE Privacy Policy](#)

A not-for-profit organization, IEEE is the world's largest technical professional organization dedicated to advancing technology for the benefit of humanity.

© Copyright 2023 IEEE - All rights reserved.

IEEE Account

- » Change Username/Password
- » Update Address

Purchase Details

- » Payment Options
- » Order History
- » View Purchased Documents

Profile Information

IEEE websites place cookies on your device to give you the best user experience. By using our websites, you agree to the placement of these cookies. To learn more, read our Privacy Policy.

- » Communications Preferences
- » Profession and Education

Accept & Close

» [Technical Interests](#)

Need Help?

» **US & Canada:** +1 800 678 4333

» **Worldwide:** +1 732 981 0060

» [Contact & Support](#)

[About IEEE Xplore](#) | [Contact Us](#) | [Help](#) | [Accessibility](#) | [Terms of Use](#) | [Nondiscrimination Policy](#) | [Sitemap](#) | [Privacy & Opting Out of Cookies](#)

A not-for-profit organization, IEEE is the world's largest technical professional organization dedicated to advancing technology for the benefit of humanity.

© Copyright 2023 IEEE - All rights reserved. Use of this web site signifies your agreement to the terms and conditions.

IEEE websites place cookies on your device to give you the best user experience. By using our websites, you agree to the placement of these cookies. To learn more, read our [Privacy Policy](#).

Accept & Close



Smart Computing Techniques and Applications pp 415–424

[Home](#) > [Smart Computing Techniques and Applications](#) > Conference paper

Real-Time Proximity Sensing Module for Social Distancing and Disease Spread Tracking

[Sreeja Rajesh](#), [Varghese Paul](#), [Abdul Adil Basheer](#) & [Jibin Lukose](#)

Conference paper | [First Online: 14 July 2021](#)

444 Accesses | 1 Citations

Part of the [Smart Innovation, Systems and Technologies](#) book series (SIST, volume 224)

Abstract

Low energy proximity sensing devices are being used in our daily life for various purposes. The concept of making a dedicated hardware module for measuring the distance arose from this concept, so as to provide reliable and accurate measurements for various applications. Analysing the need and severity of the present situation due to the spread of COVID-19, the proposed hardware and software architecture can be tuned for the efficient practice of social distancing. It also provides an effective measure to track the disease spread by the integration of a secure database. NTSA—a cryptographic algorithm that is specifically designed and developed to run on low energy microcontrollers can protect the identity of every user. Since the encryption is done by the embedded device, NTSA can ensure enhanced privacy protection compared to any algorithm run on the server. This also ensures the reliability of the collected data. The hardware module actively transmits and receives signals from similar hardware modules. The proximity or distance between the two modules is measured by analysing the signal strength received by each module. To achieve disease spread tracking the users can track their status or level of exposure on a scale of 4 and hence would provide a metric for having external interactions like first-hand contact with COVID-19 patients, secondary contact, tertiary contact, and so on.

Keywords

COVID-19 **NTSA** **Proximity sensing device**

Disease spread tracking

| | |
|--|--|
| <p>▼ Chapter</p> <p>EUR 29.95</p> <p>Price includes VAT (India)</p> <ul style="list-style-type: none">• Available as PDF• Read on any device• Instant download• Own it forever <p>Buy Chapter</p> | <p>> eBook</p> <p>EUR 160.49</p> |
| <p>> Softcover Book</p> <p>EUR 199.99</p> | <p>> Hardcover Book</p> <p>EUR 199.99</p> |

Tax calculation will be finalised at checkout

Purchases are for personal use only

[Learn about institutional subscriptions](#)

References

1. Stalling, W.: Text Book: Cryptography and Network Security, Principles and Practices (2006). Retrieved on 8 Dec 2006
2. Schneier, B.: Applied Cryptography, 2nd edn. Wiley, New York (1996)
3. Wheeler, D., Needham, R.: TEA, a tiny encryption algorithm.
<https://www.cl.cam.ac.uk/ftp/papers/djw-rmn/djw-rmn-tea.html>;
<https://www.cix.co.uk/~klockstone/tea.pdf>. Accessed 21 May 2007
4. Needham, R.M., Wheeler, D.J. (1997). TEA extensions. Technical Report, Computer Laboratory. Cambridge: University of Cambridge
5. Wheeler, D., Needham, R.: XXTEA: correction to XTEA. Technical Report, Computer Laboratory. University of Cambridge (1998)
6. Tang, H., Sun, Q.T., Yang, X., Long, K.: A Network coding and DES based dynamic encryption scheme for moving target defense. IEEE Access **6**, 26059–26068 (2018). <https://doi.org/10.1109/ACCESS.2018.2832854>
7. Banik, S., Bogdanov, A., Regazzoni, F.: Atomic-AES: a compact implementation of the aes encryption/decryption core. In: Dunkelman, O., Sanadhya, S.K. (eds) INDOCRYPT 2016, 10095. LNCS. Springer, Heidelberg, pp. 173–190 (2016). https://doi.org/10.1007/978-3-319-49890-4_10

8. Hoffman, N.: A simplified IDEA algorithm. *Cryptologia* **31**(2), 143–151 (2007)

9. Standaert, F.X., Piret, G., Gershenfeld, N., Quisquater, J.J.: SEA: a scalable encryption algorithm for small embedded applications. In: Workshop on RFID and Light weight Crypto, Graz, Austria (2005)

10. Choi, J., Kim, Y.: An improved LEA block encryption algorithm to prevent side-channel attack in the IoT system. In: 2016 Asia-Pacific Signal and Information Processing Association Annual Summit and Conference (APSIPA), Jeju, pp. 1–4 (2016).
<https://doi.org/10.1109/APSIPA.2016.7820845>

11. Abdullah, D., et al.: Super-encryption cryptography with IDEA and WAKE algorithm. In: 1st International Conference on Green and Sustainable Computing (ICoGeS) 2017. *J. Phys. Conf. Ser.* **1019**, 012039 (2018)

12. Ramakrishna Murthy, M., Murthy, J.V.R., Prasad Reddy, P.V.G.D., et al.: Homogeneity separateness: a new validity measure for clustering problems. In: International Conference and Published the Proceedings in AISC and Computing. Springer (indexed by SCOPUS, ISI proceeding DBLP etc), vol. 248, pp. 1–10 (2014). ISBN 978-3-319-03106

Author information

Authors and Affiliations

Bharathiar University, Coimbatore, 641046, India

Sreeja Rajesh

CUSAT, Kochi, Kerala, India

Varghese Paul

Beurokrat Business Management Solutions, Thrissur, Kerala, India

Abdul Adil Basheer & Jibin Lukose

Editor information

Editors and Affiliations

School of Computer Engineering, KIIT University, Bhubaneswar, Odisha, India

Dr. Suresh Chandra Satapathy

Department of Electronics and Communication Engineering, Shri Ramswaroop Memorial Group of Professional Colleges (SRMGPC), Lucknow, Uttar Pradesh, India

Dr. Vikrant Bhateja

Informatics and Computer Techniques, Reshetnev Siberian State

University of Science and Technologies, Krasnoyarsk, Russia

Prof. Margarita N. Favorskaya

Department of Computer Science and Engineering, Vasavi College of

Engineering, Hyderabad, India

Dr. T. Adilakshmi

Rights and permissions

[Reprints and Permissions](#)

Copyright information

© 2021 The Author(s), under exclusive license to Springer Nature Singapore Pte Ltd.

About this paper

Cite this paper

Rajesh, S., Paul, V., Basheer, A.A., Lukose, J. (2021). Real-Time Proximity Sensing Module for Social Distancing and Disease Spread Tracking. In: Satapathy, S.C., Bhateja, V., Favorskaya, M.N., Adilakshmi, T. (eds) Smart Computing Techniques and Applications. Smart Innovation, Systems and Technologies, vol 224. Springer, Singapore.
https://doi.org/10.1007/978-981-16-1502-3_42

[.RIS](#) [.ENW](#) [.BIB](#)

| | | |
|---|--------------|---------------------|
| DOI | Published | Publisher Name |
| https://doi.org/10.1007/978-981-16-1502-3_42 | 14 July 2021 | Springer, Singapore |

| | | |
|-------------------|-------------------|---|
| Print ISBN | Online ISBN | eBook Packages |
| 978-981-16-1501-6 | 978-981-16-1502-3 | Intelligent Technologies and Robotics Intelligent Technologies and Robotics (R0) |



All



ADVANCED SEARCH

Conferences > 2021 IEEE/ACS 18th Internatio... ?

Downsampling Attack on Automatic Speaker Authentication System

Publisher: IEEE

Cite This

PDF

Asha S ; Vinod P ; Varun G Menon ; Akka Zemmari All Authors

89 Full Text Views



Alerts

Manage Content Alerts Add to Citation Alerts

Abstract



Document Sections

- I. Introduction
- II. Literature Review
- III. Speaker Recognition System
- IV. Results and discussions
- V. Conclusion

Abstract:Recent years have observed an exponential growth in the popularity of audio-based authentication systems. The benefit of a voice-based authentication system is that the p... **View more**

Metadata

Abstract: Recent years have observed an exponential growth in the popularity of audio-based authentication systems. The benefit of a voice-based authentication system is that the person need not be physically present. Voice biometric system provides effective authentication in various domains like remote access control, authentication in mobile applications, customer care centers for call attests. Most of the existing authentication systems that recognize speakers formulate deep learning models for better classification. At the same time, research studies show that deep learning models are highly vulnerable to adversarial inputs. A breach in security on authentication systems are not generally acceptable. This paper exposes the vulnerabilities of audio-based authentication systems. Here, we propose a novel downsampling attack to the speaker recognition system. This attack can effectively trick the speaker recognition framework by causing inaccurate predictions. The proposed threat model achieved remarkable attack effectiveness of 75%. This system employs a custom human voice dataset recorded in real-time conditions to achieve real-time effectiveness during classification. We compare the attack accuracy of the proposed attack against the adversarial audios generated using the CleverHans toolbox. The proposed attack being a black box attack, is transferable to other deep learning systems also.

Authors

Figures

References

Keywords

Metrics

IEEE websites place cookies on your device to give you the best user experience. By using our websites you agree to the placement of these cookies. To learn more, read our Privacy Policy.

Published in: 2021 IEEE/ACS 18th International Conference on Computer Systems and Applications (AICCSA)

Accept & Close

Date of Conference: 30 November 2021 - 03 December 2021

INSPEC Accession Number: 21593091

DOI: 10.1109/AICCSA53542.2021.9686767

Date Added to IEEE Xplore: 25 January 2022

Publisher: IEEE

► ISBN Information:

Conference Location: Tangier, Morocco

► ISSN Information:

☰ Contents

I. Introduction

Recent research trends witnessed tremendous advancement in the area of voice authentication. Nowadays various applications such as smart speakers, personal digital assistants, biometric frameworks, and forensics, enforce voice-based commands for authentication. Voice biometric system is more convenient to use as it is a contactless means of authentication. Voice biometric system incorporates identifying the human voice and finally verifying the speaker of the audio. As the use of voice-command-based applications are increasingly rising, the need to endorse security in such systems has become a demanding issue. The limitations in uniquely recognizing the owner of the voice brings the possibility of malpractices. Any person who is aware of specific voice commands can operate such systems. Hence these voice-command-based systems should also incorporate a voice recognition system that identifies and verifies genuine speakers from voice.

Authors



Figures



References



Keywords



Metrics



More Like This

Deep Speaker Recognition: Process, Progress, and Challenges

IEEE Access

Published: 2021

IEEE websites place cookies on your device to give you the best user experience. By using our websites, you agree to the placement of these cookies. To learn more, read our Privacy Policy and Applications (TPS-ISA) 2020. Agree to the placement of these cookies, To learn more, read our Privacy Policy

Accept & Close

Published: 2020

Show More

IEEE Personal Account

CHANGE USERNAME/PASSWORD

Purchase Details

PAYMENT OPTIONS
VIEW PURCHASED DOCUMENTS

Profile Information

COMMUNICATIONS PREFERENCES
PROFESSION AND EDUCATION
TECHNICAL INTERESTS

Need Help?

US & CANADA: +1 800 678 4333
WORLDWIDE: +1 732 981 0060
CONTACT & SUPPORT

Follow



About IEEE Xplore | Contact Us | Help | Accessibility | Terms of Use | Nondiscrimination Policy | IEEE Ethics Reporting | Sitemap | IEEE Privacy Policy

A not-for-profit organization, IEEE is the world's largest technical professional organization dedicated to advancing technology for the benefit of humanity.

© Copyright 2023 IEEE - All rights reserved.

IEEE Account

- » Change Username/Password
- » Update Address

Purchase Details

IEEE websites place cookies on your device to give you the best user experience. By using our websites, you agree to the placement of these cookies. To learn more, read our Privacy Policy.

Accept & Close

» [View Purchased Documents](#)

Profile Information

» [Communications Preferences](#)

» [Profession and Education](#)

» [Technical Interests](#)

Need Help?

» **US & Canada:** +1 800 678 4333

» **Worldwide:** +1 732 981 0060

» [Contact & Support](#)

[About IEEE Xplore](#) | [Contact Us](#) | [Help](#) | [Accessibility](#) | [Terms of Use](#) | [Nondiscrimination Policy](#) | [Sitemap](#) | [Privacy & Opting Out of Cookies](#)

A not-for-profit organization, IEEE is the world's largest technical professional organization dedicated to advancing technology for the benefit of humanity.
© Copyright 2023 IEEE - All rights reserved. Use of this web site signifies your agreement to the terms and conditions.

IEEE websites place cookies on your device to give you the best user experience. By using our websites, you agree to the placement of these cookies. To learn more, read our [Privacy Policy](#).

Accept & Close



All



ADVANCED SEARCH

Conferences > 2021 8th International Confer... ?

A Study on the Effect of Hardware Trojans in the Performance of Network on Chip Architectures

Publisher: IEEE

Cite This

PDF

Josna Philomina All Authors



1 Paper Citation

103 Full Text Views

Alerts

Manage Content Alerts Add to Citation Alerts

Abstract



Document Sections

- I. Introduction
- II. Background
- III. Case Study and Analysis
- IV. Issues challenges and research future directions
- V. Conclusion and Future Work

Abstract:Network on chip (NoC) is the communication infrastructure used in multicores which has been subject to a surfeit of security threats like degrading the system performance... [View more](#)

Metadata

Abstract:

Network on chip (NoC) is the communication infrastructure used in multicores which has been subject to a surfeit of security threats like degrading the system performance, changing the system functionality or leaking sensitive information. Because of the globalization of the advanced semiconductor industry, many third-party vendors take part in the hardware design of system. As a result, a malicious circuit, called Hardware Trojans (HT) can be added anywhere into the NoC design and thus making the hardware untrusted. In this paper, a detailed study on the taxonomy of hardware trojans, its detection and prevention mechanisms are presented. Two case studies on HT-assisted Denial of service attacks and its analysis in the performance of network on Chip architecture is also presented in this paper.

Published in: 2021 8th International Conference on Smart Computing and Communications (ICSCC)

Date of Conference: 01-03 July 2021

INSPEC Accession Number: 21137841

Date Added to IEEE Xplore: 06 September 2021

DOI: 10.1109/ICSCC51290.2021.9528249

IEEE websites place cookies on your device to give you the best user experience. By using our websites, you agree to the placement of these cookies. To learn more, read our Privacy Policy.

Accept & Close

Metrics

► ISBN Information:

Publisher: IEEE

More Like This

Conference Location: Kochi, Kerala, India

☰ Contents

I. Introduction

Mobiles and handheld devices are becoming part and parcel of our day today life. More number of applications have to be executed concurrently and the performance of the device cannot be compromised at any level. Also, we are signing to continue learning where more computation intensive tasks have to be performed. In all these scenarios the prior requirement is that performance of the processor must be high enough to get the expected work done.

Authors



Figures



References



Citations



Keywords



Metrics



More Like This

Networks on Chip with Provable Security Properties

IEEE Micro

Published: 2014

Electronic, Wireless, and Photonic Network-on-Chip Security: Challenges and Countermeasures

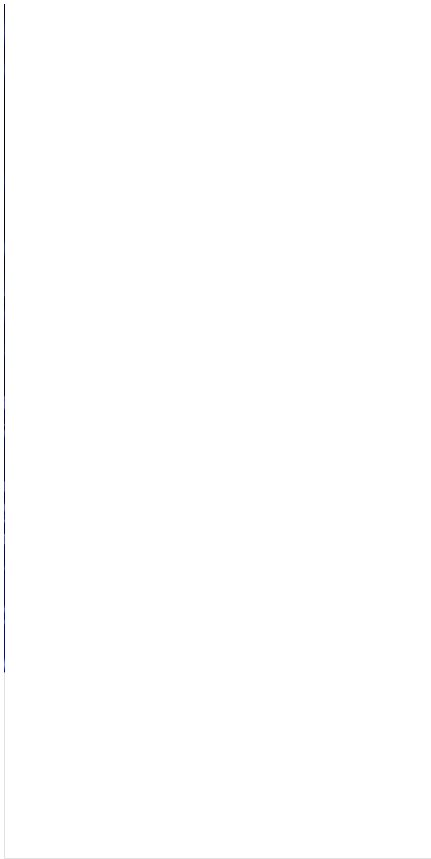
IEEE Design & Test

Published: 2022

Show More

IEEE websites place cookies on your device to give you the best user experience. By using our websites, you agree to the placement of these cookies. To learn more, read our Privacy Policy.

Accept & Close



IEEE Personal Account

CHANGE USERNAME/PASSWORD

Purchase Details

PAYMENT OPTIONS
VIEW PURCHASED DOCUMENTS

Profile Information

COMMUNICATIONS PREFERENCES
PROFESSION AND EDUCATION
TECHNICAL INTERESTS

Need Help?

US & CANADA: +1 800 678 4333
WORLDWIDE: +1 732 981 0060
CONTACT & SUPPORT

Follow



[About IEEE Xplore](#) | [Contact Us](#) | [Help](#) | [Accessibility](#) | [Terms of Use](#) | [Nondiscrimination Policy](#) | [IEEE Ethics Reporting](#) | [Sitemap](#) | [IEEE Privacy Policy](#)

A not-for-profit organization, IEEE is the world's largest technical professional organization dedicated to advancing technology for the benefit of humanity.

© Copyright 2023 IEEE - All rights reserved.

IEEE Account

- » Change Username/Password
- » Update Address

Purchase Details

- » Payment Options
- » Order History
- » View Purchased Documents

Profile Information

IEEE websites place cookies on your device to give you the best user experience. By using our websites, you agree to the placement of these cookies. To learn more, read our Privacy Policy.

- » Communications Preferences
- » Profession and Education

Accept & Close

» Technical Interests

Need Help?

» **US & Canada:** +1 800 678 4333

» **Worldwide:** +1 732 981 0060

» Contact & Support

[About IEEE Xplore](#) | [Contact Us](#) | [Help](#) | [Accessibility](#) | [Terms of Use](#) | [Nondiscrimination Policy](#) | [Sitemap](#) | [Privacy & Opting Out of Cookies](#)

A not-for-profit organization, IEEE is the world's largest technical professional organization dedicated to advancing technology for the benefit of humanity.

© Copyright 2023 IEEE - All rights reserved. Use of this web site signifies your agreement to the terms and conditions.

IEEE websites place cookies on your device to give you the best user experience. By using our websites, you agree to the placement of these cookies. To learn more, read our [Privacy Policy](#).

Accept & Close



All



ADVANCED SEARCH

Conferences > 2021 International Conference... ?

Age and Spoof Detection from Fingerprints using Transfer Learning

Publisher: IEEE

Cite This

PDF

Sonal Ayyappan ; Navaneeth Asok ; Nandu Shaji All Authors

62 Full Text Views



Alerts

Manage Content Alerts Add to Citation Alerts

Abstract



Document Sections

- I. Introduction
- II. Related Works
- III. Dataset
- IV. Methodology
- V. Experiment

Show Full Outline

Authors

Figures

References

Keywords

Metrics

Abstract:The use of biometric authentication has seen an exponential increase in recent years ranging from smartphones to even forensic analyses. Fingerprints are obtained and use... **View more**

Metadata

Abstract:

The use of biometric authentication has seen an exponential increase in recent years ranging from smartphones to even forensic analyses. Fingerprints are obtained and used in crime scenes, old monuments and excavated relics and to the day-to-day authentication including attendance marking. Determination of age has always been an ardent task as they experience virtually zero changes as a person ages. Also, with the increased attacks and bypassing on the fingerprint authentication systems, it is also important to confirm the genuineness of the fingerprints. This brings forth a need for a spoof detection for fingerprints. Since fingerprints have been used as an effective method for authentication, their correlation with the age of a person is to be identified, if any. This paper aims in using Convolutional Neural Networks and other machine learning techniques to estimate age of a person from fingerprints and also spoof detection. The models we compare include three pre-trained CNNs which are fine-tuned with the fingerprint images, and a classical Local Binary Pattern approach. It is found that pre-trained CNNs along with Dataset Augmentation can produce good results with no need for any hyperparameter selection. NIST dataset was used for age detection and LiveDet 2013 dataset was used for spoof detection. It was able to achieve a top accuracy of 84% for age detection and 94% for spoof detection. The paper also focuses on identifying the best scanner for our purposes and also the possible materials used for spoofing.

IEEE websites place cookies on your device to give you the best user experience. By using our websites, you agree to the placement of these cookies. To learn more, read our Privacy Policy.

Accept & Close

Date of Conference: 21-23 October 2021

INSPEC Accession Number: 21623492

Date Added to IEEE Xplore: 15 February 2022

DOI: 10.1109/ICACC-202152719.2021.9708286

► ISBN Information:

Publisher: IEEE

Conference Location: Kochi, Kakkanad, India

☰ Contents

I. Introduction

Individuals can be identified and verified using their bio-metric characteristics such as the finger prints, palm prints, vein, and iris and these traits have been widely used in the modern day to day life. Fingerprints are generally used for the identification or verification of a person and for official documentation. It is one of the most matured biometric technologies and is considered as a legitimate proof of evidence for judiciary purposes. The demand for increased security and better authentication techniques has pushed fingerprint biometrics to be developed into a key technology, especially in this age of computerised access control systems. [13].

Authors



Figures



References



Keywords



Metrics



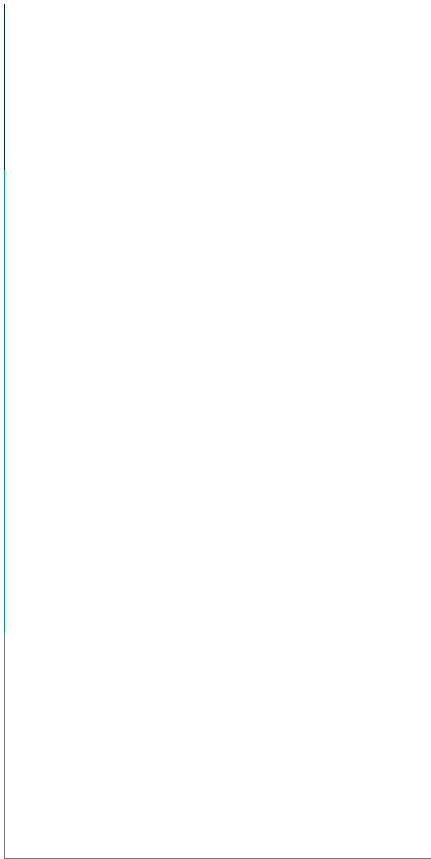
More Like This

A Novel Deep Learning Framework by Combination of Subspace-Based Feature Extraction and Convolutional Neural Networks for Hyperspectral Images Classification
IGARSS 2018 - 2018 IEEE International Geoscience and Remote Sensing Symposium
Published: 2018

Hyperspectral Image Classification via Object-Oriented Segmentation-Based Sequential Feature Extraction and Recurrent Neural Network
IGARSS 2020 - 2020 IEEE International Geoscience and Remote Sensing Symposium
Published: 2020

IEEE websites place cookies on your device to give you the best user experience. By using our websites, you agree to the placement of these cookies. To learn more, read our Privacy Policy.

Accept All Cookies



IEEE Personal Account

CHANGE USERNAME/PASSWORD

Purchase Details

PAYMENT OPTIONS
VIEW PURCHASED DOCUMENTS

Profile Information

COMMUNICATIONS PREFERENCES
PROFESSION AND EDUCATION
TECHNICAL INTERESTS

Need Help?

US & CANADA: +1 800 678 4333
WORLDWIDE: +1 732 981 0060
CONTACT & SUPPORT

Follow



[About IEEE Xplore](#) | [Contact Us](#) | [Help](#) | [Accessibility](#) | [Terms of Use](#) | [Nondiscrimination Policy](#) | [IEEE Ethics Reporting](#) | [Sitemap](#) | [IEEE Privacy Policy](#)

A not-for-profit organization, IEEE is the world's largest technical professional organization dedicated to advancing technology for the benefit of humanity.

© Copyright 2023 IEEE - All rights reserved.

IEEE Account

- » Change Username/Password
- » Update Address

Purchase Details

- » Payment Options
- » Order History

IEEE websites place cookies on your device to give you the best user experience. By using our websites, you agree to the placement of these cookies. To learn more, read our [Privacy Policy](#).

Accept & Close

» Profession and Education

» Technical Interests

Need Help?

» **US & Canada:** +1 800 678 4333

» **Worldwide:** +1 732 981 0060

» Contact & Support

[About IEEE Xplore](#) | [Contact Us](#) | [Help](#) | [Accessibility](#) | [Terms of Use](#) | [Nondiscrimination Policy](#) | [Sitemap](#) | [Privacy & Opting Out of Cookies](#)

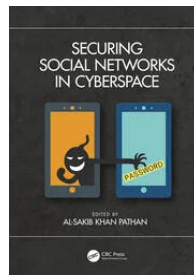
A not-for-profit organization, IEEE is the world's largest technical professional organization dedicated to advancing technology for the benefit of humanity.

© Copyright 2023 IEEE - All rights reserved. Use of this web site signifies your agreement to the terms and conditions.

IEEE websites place cookies on your device to give you the best user experience. By using our websites, you agree to the placement of these cookies. To learn more, read our [Privacy Policy](#).

Accept & Close

Chapter



A Deep Learning-Based Model for an Efficient Hate-Speech Detection in Twitter

By [P. R. Vishnu](#) (/search?contributorName=P. R. Vishnu&contributorRole=author&redirectFromPDP=true&context=ubx), [Basant Agarwal](#) (/search?contributorName=Basant Agarwal&contributorRole=author&redirectFromPDP=true&context=ubx), [P. Vinod](#) (/search?contributorName=P. Vinod&contributorRole=author&redirectFromPDP=true&context=ubx), [K. A. Dhanya](#) (/search?contributorName=K. A. Dhanya&contributorRole=author&redirectFromPDP=true&context=ubx), [Alice Baroni](#) (/search?contributorName=Alice Baroni&contributorRole=author&redirectFromPDP=true&context=ubx)

Book [Securing Social Networks in Cyberspace \(https://www.taylorfrancis.com/books/mono/10.1201/9781003134527/securing-social-networks-cyberspace?refId=737bdf44-834c-4057-a330-d8885f4f5f78&context=ubx\)](https://www.taylorfrancis.com/books/mono/10.1201/9781003134527/securing-social-networks-cyberspace?refId=737bdf44-834c-4057-a330-d8885f4f5f78&context=ubx)

| | |
|-----------------|---------------|
| Edition | 1st Edition |
| First Published | 2021 |
| Imprint | CRC Press |
| Pages | 16 |
| eBook ISBN | 9781003134527 |

ABSTRACT



[< Previous Chapter \(chapters/edit/10.1201/9781003134527-7/steganographic-botnet-channel-using-twitter-nicholas-pantic-mohammad-husain?context=ubx\)](#)

[Next Chapter > \(chapters/edit/10.1201/9781003134527-10/cyberbullying-cyberstalking-online-social-networks-umit-bilal-alatas?context=ubx\)](#)



(<https://www.taylorfrancis.com>)

Policies



[Back to Top](#)

Journals



Corporate



Help & Contact



Connect with us



(<https://www.linkedin.com/company/taylor-&-francis-group/>)



(<https://twitter.com/tandfnewsroom?lang=en>)



(<https://www.facebook.com/TaylorandFrancisGroup/>)



(<https://www.youtube.com/user/TaylorandFrancisGroup>)

Registered in England & Wales No. 3099067
5 Howick Place | London | SW1P 1WG

© 2023 Informa UK Limited

Browse » Publications » Technical Papers » 2021-28-0150

2021-09-15

Parked Car Thermal Management and Air Quality System 2021-28-0150

The motivation of this work is to respond to high cabin temperatures within a parked/stationary vehicle which may cause discomfort and lead to vehicular heatstroke. The system also intends to ensure sufficient limits of oxygen within the vehicle cabin to prevent asphyxiation to the cabin occupants. The rise in global temperature is affecting the quality of air and comfort of occupants inside a parked car. There have been several cases reported of pets and children being left unattended or unsupervised in a parked car for a long period of time which have led to their deaths due to asphyxiation. The use of cost-effective materials like high density plastics for interior cabin trim have also been proven to contribute to cancer because of the emission of benzene a carcinogen by these plastics when exposed to extreme temperatures for long periods of time. This paper proposes a system where an oxygen sensor is used to measure oxygen levels within the cabin and an arrangement to lower the windows when a low level of oxygen is detected. The system also includes a temperature sensor with a suction and blower fan arrangement where the suction fan pulls the hot air out and the blower fan pushes fresh air in. This air flow will ensure air circulation in a parked car and prevent the stagnation of hot air within the vehicle cabin. It was also a crucial factor that this system should not interfere or hinder with any other workings of the car. This system will be powered by a compact solar system.

DOI: <https://doi.org/10.4271/2021-28-0150>

Citation: **Joseph, K. and Antony, M.**, "Parked Car Thermal Management and Air Quality System," SAE Technical Paper 2021-28-0150, 2021, <https://doi.org/10.4271/2021-28-0150>.

[Download Citation](#)

Author(s): Koshy P Joseph, Manu Antony

Affiliated: **SCMS School Of Engineering and Technology**

Pages: 4

Event: Thermal Management Systems Conference 2021

ISSN: 0148-7191

e-ISSN: 2688-3627

Related Topics:

AIR POLLUTION

FANS

THERMAL MANAGEMENT