



SCMS SCHOOL OF ENGINEERING AND TECHNOLOGY



ENIGMA



DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

Vision

To achieve academic excellence in creating globally competent professionals and ethically strong global workforce in the field of Computer Science & Engineering, facilitating research activities, catering to the ever changing industrial demands and societal needs.

Mission

1. Creating excellence in Computer Science & Engineering through academic professionalism for the changing needs of the society.
2. Establishing centre of excellence for research and for technical development in the area of Computer Science & Engineering.
3. Developing communication skill, team work and leadership qualities for continuing education among the students, through project based and team based learning.
4. Inculcating ethics and human values for sustainable societal growth and environmental protection.
5. Empowering students for employability, aspiring higher studies and to become entrepreneur.

Program Educational Objectives

1. Apply computer science theory blended with mathematics and engineering to model computing systems.
2. Nurture strong understanding in logical, computing and analytical reasoning among students coupled with problem solving attitude that prepares them to productively engage in research and higher learning.
3. Communicate effectively with team members, engage in applying technologies and lead teams in industry.
4. Engage in lifelong learning, career enhancement and adapt to changing professional and societal needs.

EDITORIAL



Asha .S
Assistant Professor



Jency Rena NM
Assistant Professor



Isham Mohamed
Student



Sara Abraham
Student



Prashant G
Student



Naijith Gopal
Student



Sherin Phillip
Student



Navaneeth Asok
Student

CONTENTS

01

DRIVING IN THE FAST LANE :
5G AND AUTONOMOUS VECHILES

02

AGE INVARIANT FACE
RECONGNITION : USING 3D
AGLIE MODEL

03

INTERNET OF BODIES :
FUTURE OF BIONIC
EMBEDDED SYSTEMS

04

DEALING WITH SPAM AS A
MACHINE LEARNING
PROGRAMMER : EXPLORE,
PLOT AND VISUALIZE YOUR
DATA

05

IMAGE FORGERY



DRIVING IN THE FAST LANE

5G AND AUTONOMOUS VEHICLES

-Sreelakshmi S

“In this era of digitalisation and smart technologies, the use of autonomous vehicles as a mode of transport is not a question of 'if' but 'when'.”
- Chen Tsuhan

The automobile industry is experiencing exponential growth of self-driving features, and this trend is expected to continue. 5G network connections will have a major influence on the development of self-driving cars making them faster, smarter, and safer.

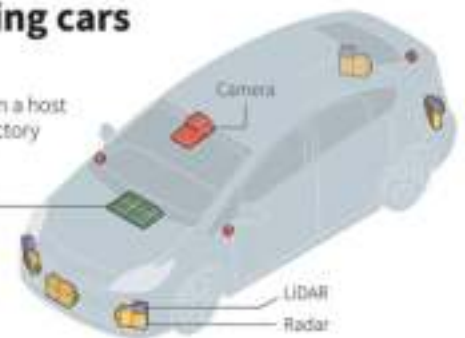
Companies such as Tesla and Toyota are now testing self driving vehicles on the roads in places like Pittsburgh, Boston, and Phoenix. But while many people already had grave concerns surrounding driverless cars, a recent fatal accident by an autonomous Uber vehicle has many questioning if autonomous cars will ever be safe enough to feel confident with them sharing our roads.

Still, with self-driving features already in widespread use, it does appear that fully autonomous cars will be appearing on our roads, and perhaps sooner than people realize. Even more surprising, they will also be considered much safer than human-controlled vehicles.

How self-driving cars see the road

Autonomous vehicles rely on a host of sensors to plot their trajectory and avoid accidents.

• **Multi-domain controller**
Manages inputs from camera, radar, and LIDAR. With mapping and navigation data, it can confirm decisions in multiple ways.



• **Camera**
Takes images of the road that are interpreted by a computer. Limited by what the camera can "see".



• **Radar**
Radio waves are sent out and bounced off objects. Can work in all weather but cannot differentiate objects.



• **LIDAR**
Light pulses are sent out and reflected off objects. Can define lines on the road and works in the dark.

Source: Delphi





For autonomous car technology to be unlocked, many experts agree that large-scale adoption of 5G, the next-generation wireless technology—is required. The current 4G network is fast enough to online stream full HD content and play online games, but it can't support safer and smarter autonomous cars. We need to look at how long it takes for the message to be transmitted between sensors and then get to the computer in each car, and then how long it takes for the computer to make a decision, and all of this has to be in less time than a human would take to make a decision, 2 milliseconds. We need a network supporting this, and 5G is that network. The current 4G network is simply not fast enough to provide the capability to give autonomous vehicles human-like reflexes that may have prevented the Uber vehicle fatality.

Why 5G is Crucial for Autonomous Cars?

Self-driving cars use hundreds of sensors to make vehicles faster and smarter. These sensors generate unprecedented amounts of data, much more than any other IoT adoption would. Handling, processing, and analysing this amount of data requires a much faster network than the existing 4G technology. Autonomous cars, systems require incredible data processing capabilities and speeds needed to mimic the timing of human reflexes.

Future autonomous cars will generate nearly 2 petabits of data, which is equivalent of 2 million gigabits.

With an advanced Wi-Fi connection, it will take 230 days to transfer a week-worth of data from a self-driving car, and that is why we need much faster ASIC processing technology and products. The world's leading semiconductor companies, such as Intel and Qualcomm, are advancing toward an ASICs revolution, combining large available bandwidth at 5G frequencies with new innovative digital radio and antenna architectures. Simply put, these companies are creating chips to turn autonomous vehicles into mobile data centers, allowing driverless cars to make real-time, complex decisions.

Market watchers say that 5G, when adopted at the full scale, will offer internet speeds up to 100 times faster than 4G. It will present exciting possibilities for the automobile industry used for vehicle-to-vehicle (V2V) and vehicle-to-everything (V2X) connectivity. Furthermore, the technology's low latency will make these vehicles extraordinarily safe and reliable on the roads safer than vehicles today that are operated by people.



Edge Computing Powered by 5G

Offering a range of advantages, edge computing is recognized by many experts as one of the latest significant enterprise trends. Edge computing refers to infrastructure that allows data processing as close to the source as possible, enabling faster processing of data, reduced latency, and overall better outcomes. When it comes to edge computing, there are many challenges in terms of network reliability.

With autonomous cars comes the responsibility of managing the infrastructure which processes massive amounts of unstructured data and privacy protection when collecting sensitive data at the edge. Edge computing will allow lightning fast response time because of 5G's promise of lower latency and ability to offload computing tasks and better location awareness.

Remote Pilots

Another key reason why 5G is crucial for autonomous cars is the inclusion of specific safety measures in the vehicle. For example, suppose a self-driving car fails to navigate due to a traffic jam caused by a road accident.

The autopilot feature might hand the reins over to the driver. However, it would not be possible in case of an elderly or a disabled rider. For this reason, many tech companies have been testing remote pilots, who are trained drivers sitting miles away in a simulator that can take over instantly. However, to achieve it, a stable and fast connection offered by 5G would be crucial. Additionally, 5G will provide passengers in self-driving cars with high-quality infotainment services. It will make communications service provider an important partner for autonomous cars, whether for data analytics, safety, or entertainment reasons.


Further opportunities for 5G technology to enhance self-driving car technology exist. These opportunities are yet to be explored by regular examination of the safety performance of autonomous vehicles.

Technology and network evolution bring incredible and useful advancements to society. 5G's promises to bring safer and smarter self-driving cars would be one of the most remarkable developments of our time.

References:

www.wikipedia.org





AGE INVARIANT FACE RECOGNITION

USING 3D AGING MODEL

-Sajini Stalin

A major challenge in automatic face recognition is to achieve temporal invariance. In other words, the goal is to come up with a representation and matching scheme that is robust to changes due to facial aging. Facial aging is a complex process that affects both the 3D shape of the face and its texture (e.g., wrinkles). These shape and texture changes degrade the performance of automatic face recognition systems. This aging process also appears in different manifestations in different age groups. While facial aging is mostly represented by facial growth in younger age groups, it is mostly represented by relatively large texture changes and minor shape changes (e.g., due to change of weight or stiffness of skin) in older age groups. Therefore, an age correction scheme needs to be able to compensate for both types of aging processes.

Some of the face recognition applications where age compensation is required include identifying. 1) missing children, 2) screening, and 3) multiple enrollment detection problems. These three scenarios have two common characteristics: 1) significant age difference between probe and gallery images (images obtained at enrollment and

"Facial recognition software is already quite accurate in measuring unchanging and unique ratios between facial features that identify you as you. It's like a fingerprint."

- Jan Chipchase

verification stages and 2) inability to obtain a user's face image to update the template (gallery). However, facial aging has not received substantial attention compared to other facial variations due to pose, lighting, and expression. Most of the current work on face recognition is focused on compensating for the variations that degrade face recognition performance.

3D aging modelling technique is something that can be used to compensate for the age variations to improve the face recognition performance. The aging modelling technique adapts view-invariant 3D face models to the given 2D face aging database. The proposed approach is evaluated on three different databases (i.g., FG-NET, MORPH, and BROWNS) using FaceVACS, a state-of-the-art commercial face recognition engine.





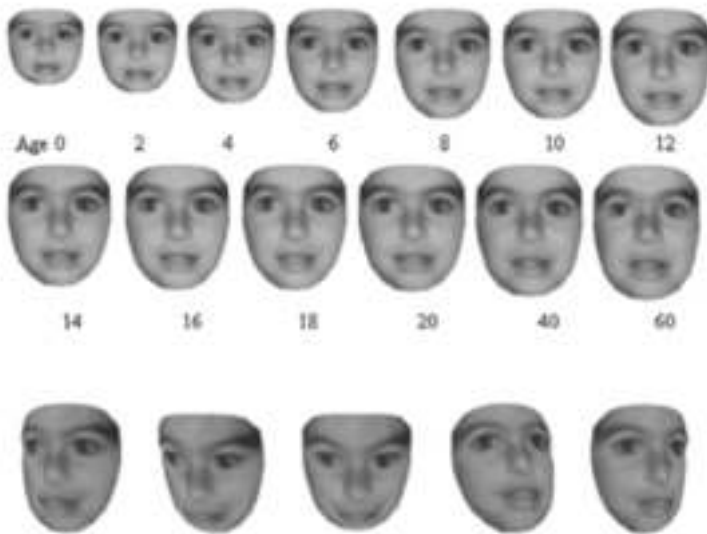
Studies on face verification across age progression have shown that: 1) Simulation of shape and texture variations caused by aging is a challenging task as factors like lifestyle and environment also contribute to facial changes in addition to biological factors, 2) the aging effects can be best understood using 3D scans of human head, and 3) the available databases to study facial aging are not only small but also contain uncontrolled external and internal variations. It is due to these reasons that the effect of aging in facial recognition has not been as extensively investigated as other factors that lead to intraclass variations in facial appearance.

The performance of these models is evaluated in terms of the improvement in the identification accuracy. Usually, the larger the number of subjects and the larger the database variations in terms of age, pose, lighting, and expression is, the smaller the recognition performance improvement due to aging model.

The proposed method for aging modelling has the following features:

- **3D aging modelling:** We use a pose correction stage and model the aging pattern more realistically in the 3D domain. Considering that the aging is a 3D process, 3D modelling is better suited to capture the aging patterns. We have shown how to build a 3D aging model given a 2D face aging database. The proposed method is our only viable alternative to building a 3D aging model directly as no 3D aging database is currently available.
- **Separate modelling of shape and texture changes:** We have compared three different modelling methods, namely, shape modelling only separate shape and texture modelling and combined shape and texture modelling (e.g., applying second level PCA to remove the correlation between shape and texture after concatenating the two types of feature vectors). We have shown that the separate modelling is better than combined modelling method, given the FG-NET database as the training data.
- **Evaluation using a state-of-the-art commercial face matcher, FaceVACS:** All of the previous studies on facial aging have used PCA-based matchers. We have used a state-of-the-art face matcher, FaceVACS from Cognitec, to evaluate our aging model. The proposed method can thus be useful in practical applications requiring age correction process. Even though we have evaluated the proposed method only on one particular face matcher, it can be used directly in conjunction with any other 2D face matcher.





- Diverse Databases: We have used FG-NET for aging modelling and evaluated the aging model on three different databases, FG-NET (in leave-one-person-out fashion), MORPH, and BROWNS. We have observed substantial performance improvements on all the three databases. This demonstrates the effectiveness of the proposed aging modelling method.

The proposed aging model construction takes about 44 seconds. The aging model is constructed offline; therefore, its computation time is not a major concern. In the recognition stage, the entire process, including feature points detection, aging simulation, enrollment, and matching takes about 12 seconds per probe image. Note that the gallery images are preprocessed offline. All computation times are measured on a Pentium 4, 3.2GHz, 3GByte RAM machine. Thus the proposed model is capable of handling both growth (developmental) and adult face aging effects unlike the presently used models.

References:
www.ieee.org
www.medium.com





INTERNET OF BODIES

Future of Bionic Embedded Systems

-Pranav Prakash

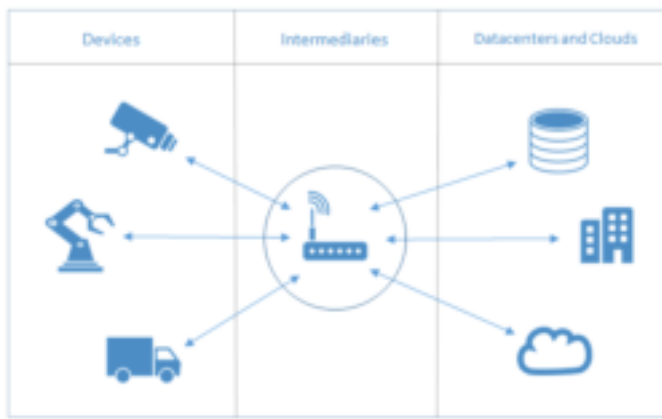
“If you think that the internet has changed your life, think again. The Internet of Things is about to change it all over again!” —
Brendan O’Brien

The imminent development in the widely useful Internet of Things (IoT) domain, is the unavoidable future of technology right now. In simple terms, IoB is IoT entering the human body. Instead of devices connected to the internet as in IoT, it's human bodies that are now connected to a network and thus will become the new data discovery platform with the potential to be remotely controlled and monitored.

Internet of Bodies is referred to as the future of tech, but this future isn't that far away. At present, IoB is already among us in the forms of wearable devices and has found its presence in the health care domain. Pacemakers for heart patients are the most common example.

Another is the 'smart pill', a drug with sensors embedded in it, able to send data right from our stomachs to a remote device connected to the internet for medical supervision. A brain implant that could substitute parts of the brain is dubbed as a relief for the cure-less Parkinson's or Alzheimer's. This can also be helpful for the treatment of spinal injuries where the devices will replace biological neurons, enabling locomotion of paralysed limbs. In short, drastic improvements in the medical field can be brought about by this emerging technology which undoubtedly holds a lot of potential.





Basic IoT Architecture

IoB can generally be classified into three generations. The first generation is the body external type which includes wearable devices like Apple Watches and Smart Bands by Fitbit and others.

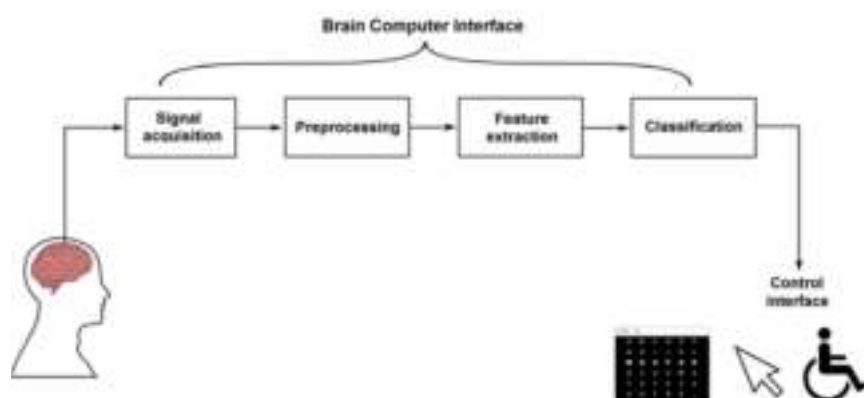
We have already been introduced to the idea of continuous monitoring of our bodies with “health accessories” that have come into vogue recently. Next is the body internal type which has the previously mentioned advancements like pacemakers and implants coming under it. The third generation will see the body embedded type which includes sensors buried inside your skin, an example would be the much elusive Brain Computer Interface (BCI) where the human brain merges with an external device and allowing for a real-time connection with remote computers that receive live data updates, for the purposes of controlling and monitoring.

A radio frequency identification (RFID) microchip, which is the size of a grain, implanted under the skin can make identification possible with just a wave of hand, eliminating the need for biometric identification methods or having to carry an identity card or even remembering a password. Your presence anywhere in the premises could be detected.

IoB is in fact only an extension of IoT and the difference between the two is merely skin deep. It is estimated that about 20 billion IoT devices will be connected to the internet by the year 2020.

In the context of IoB, these connected entities will be human beings that are alive and breathing.

We are already aware of the threats that the IoT domain is expected to face. The significant vulnerabilities, if exploited, can result in very serious implications. We are under constant surveillance today, as evidenced by the recent nuisances involving Amazon’s Alexa and Google Home. If that was a question of losing control of our surrounding environment, imagine losing autonomy over our own bodies.



References:
www.sciencedirect.com
www.medium.com



DEALING WITH SPAM AS A MACHINE LEARNING PROGRAMMER

Explore, Plot and Visualize Your Data

-Nikil S Kumar

*"A breakthrough in Machine Learning would be worth ten Microsofts."
-Bill Gates*

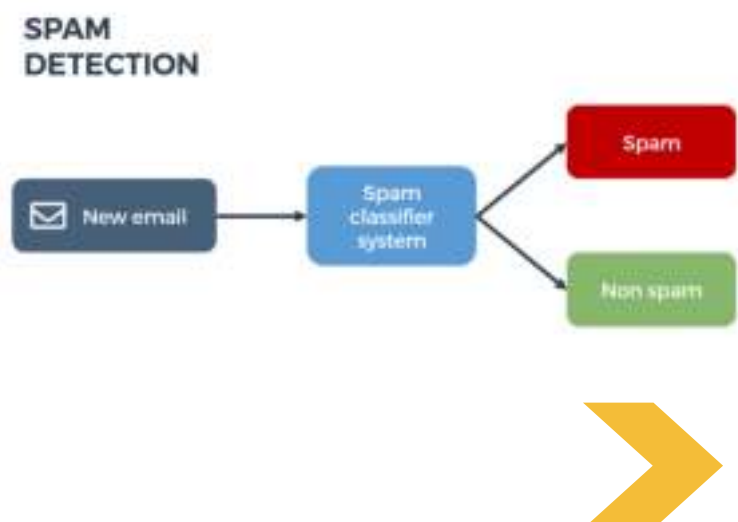
Spams are universally despised mails, whether it's at an industrial level or personal level. As we see our mail fill up with useless mails while we miss out on the important mails, our frustrations know no bounds. Spammers are a nuisance in both professional and local fields as they are looking for gullible internet users.

Spam companies are now grouping together and are the cause of huge amounts of loss in industries. The industrial network is very important network that guarantees the normal functioning of the company and dealing with spam causes huge waste of productive time.

The question remains, how to deal with them? Machine learning is the ability to automatically learn and improve from experience without being explicitly programmed. As a machine learning programmer there are various tools at your disposal to deal with the nuisance of spam.

. A few methods to list are using a Gaussian Mixture Model (GMM), or using Naives Bayesian classifiers, or many other methods. While there are many tools only a few give a satisfying acceptable result. GMM model is one such model. Spam identification using Gaussian Mixture Model (SIGMM) is a model where the precision of the model increases as size of the training set increases.

It is able to label large amounts of unlabeled data with very few labeled data. The GMM model in Spam identification outperforms other models in the same domain.



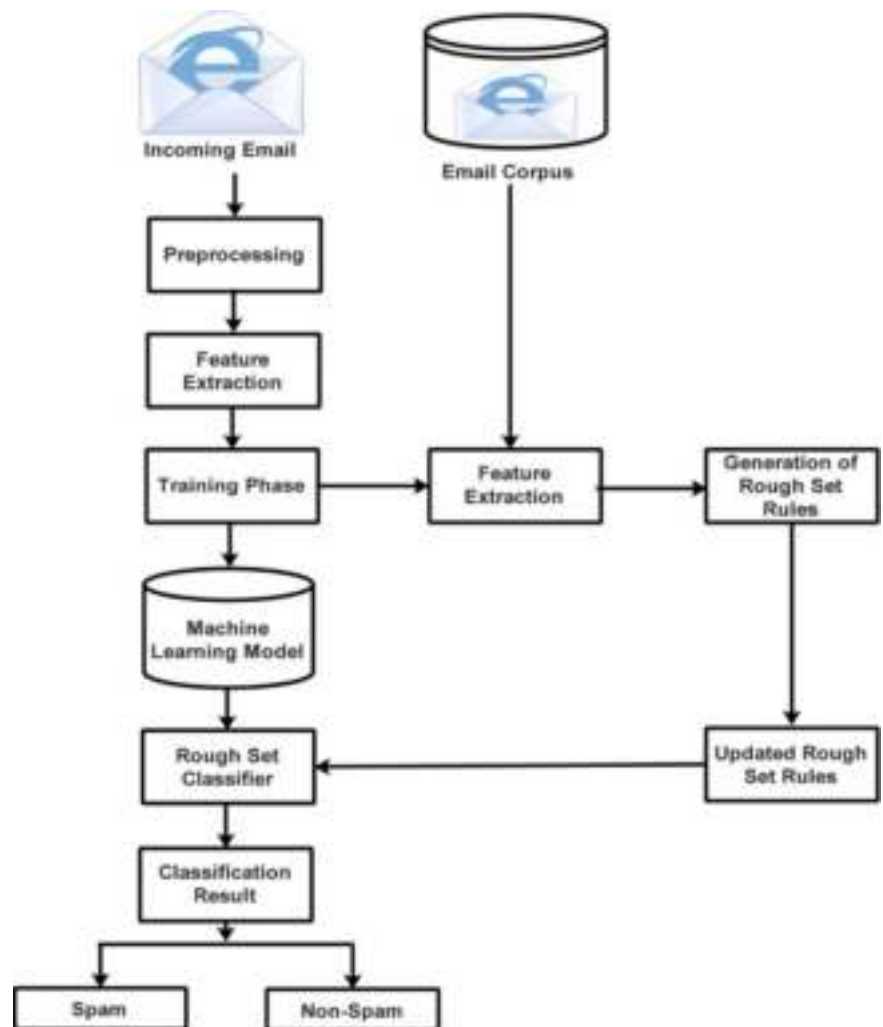
The Machine Learning Process



So why dedicate your time to understanding the GMM model? GMM model is used for clustering of information that can be used for analysis in large amounts of data.

Hence the scope lies in the Big Data Analytics. GMM models are popular in astronomy and oceanography for its ability to produce satisfactory result while processing large amounts of data. It produces better result if the data is centered on the mean. So as a machine learning programmer using the GMM model to identify spams would save the internet users from the bane of spams. It may save even billion of rupees if the filter is as effective and detailed.

It can also be applied as filters for more generic class as for Actors, Engineers and other classes. The scope of this field remains unseen, and new bounds are yet to be discovered. Hence the programmers have a huge direction to work towards as the horizons keep expanding.



References:

www.springer.com



IMAGE FORGERY

-Sibin Varghese

We are living in an age, where anything can be manipulated or altered with the help of modern technology. With the increasing applications of digital imaging, different types of software tools are introduced for processing images and photographs. They are used to make forged images to make it look real or objects can be added or deleted.

Today's digital technology has begun to remove trust in our knowledge. Forged photographs are appearing as real photographs. As the availability of multimedia data in digital form has increased, it has come to a tremendous growth of tools to manipulate digital multimedia contents. Image forgery means manipulation of the digital image to conceal some meaningful or useful information from it.

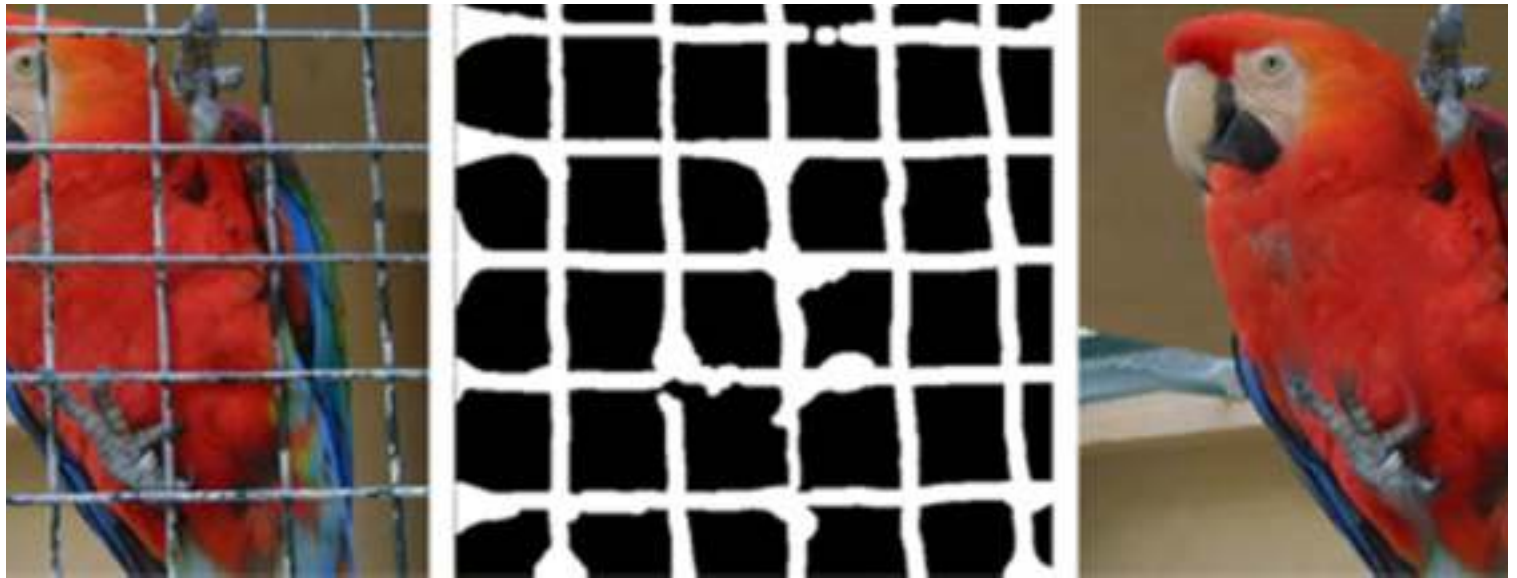
Sometimes it is difficult to identify the edited region from the original image. The detection of a forged image is driven by the need of authenticity and to maintain integrity of the image.

TYPES OF DIGITAL IMAGE FORGERY

A. Copy-Move Forgery

In copy-move forgery (or cloning), some part of the picture of any size and shape is copied and pasted to another area in the same picture to shroud some important data as demonstrated.





b. Image Forgery using Splicing

Image splicing uses cut-and-paste systems from one or more images to create another fake image. When splicing is performed precisely, the borders between the spliced regions can visually be imperceptible.

c. Image Resampling

To make an astounding forged image, some selected regions have to undergo geometric transformations like rotation, scaling, stretching, skewing, flipping and so forth. This step plays an important role in the resampling process and introduces non-negligible statistical changes.

DIGITAL IMAGE

FORGERY DETECTION METHODS

Digital Image forgery detection methods are classified into two:

- Active approach
- Passive approach

In Active approach, some information will be embedded in an image in the form of digital watermark. In the case of passive approach, there will be no information embedded in the image while passive approach is also well suited for real time applications.

Reference:
www.ieee.org

