SDJ INTERNATIONAL COLLEGE

Bachelor of Computer Applications (BCA)
Programme

Seminar Report

BCA Sem VI
AY 2021-22

Topic Title: BIOMETRICS IN E-SECURE TRANSACTION

by

Exam No.	Name of Student
2019024844	RAJPUT VIVEK SURENDRA

Seminar Guide by :
KRISHNA KHANDWAL

SDJ INTERNATIONAL COLLEGE

CERTIFICATE

This is to certify that Mr./Ms. RAJPUT VIVEK SURENDRA examination number 2019024844 has satisfactorily completed his/her Seminar work entitled Biometrics In E-Secure Transactions as partial fulfillment of requirements for BCA Sem VI, during the academic year 2018-19.

Date: 23/02/2022

Place: Surat

(Aditi Bhatt)
Coordinator
SDJ International College,
Surat

Acknowledgement

The success and final outcome of this seminar required a lot of guidance and assistance from many people and I am extremely fortunate to have got this all along the completion of my seminar work. Whatever I have done is only due to such guidance and assistance and I would not forget to thank them.

I owe our profound gratitude to our Director Mr. Deepak Vaidya, Coordinator Mrs. Aditi Bhatt, Head of Department Mr. Vaibhav Desai and Seminar guide Prof. Nidhi Desai and Prof. Chirag Prajapati, and all other Assistant professors of SDJ International College, who took keen interest on my Seminar work and guided me all along, till the completion of my seminar work by providing all the necessary information for presenting a good Concept. I am extremely grateful to them for providing such a nice support and guidance though they had busy schedule managing the college affairs.

I am thankful and fortunate enough to get support and guidance from all Teaching staffs of Bachelor of Computer Application Department which helped me in successfully completing my seminar work. Also, I would like to extend my sincere regards to all the non-teaching staff of Bachelor of Computer Application Department for their timely support.

<Signature>

<Name of the Student>
<Exam No>

INDEX

Heading Line Arial 16 Bold
Sub heading Arial 12 Bold
Content Arial 11
Content Width Alignment Justify

Example:

Introduction (Heading)

Seminar Topic (Sub heading)

(Content) On the Insert tab, the galleries include items that are designed to coordinate with the overall look of your document. You can use these galleries to insert tables, headers, footers, lists, cover pages, and other document building blocks. When you create pictures, charts, or diagrams, they also coordinate with your current document look.

Header: College Logo (Left Side) & Name of Seminar (Right Side)
Footer: Page number (Middle)

1. <u>INTRODUCTION:</u>

Mobile phones have ceased to be exclusive status of the high class and, today has become an indispensable electronic gadget in the life of many. The main reason for their higher market penetrations in recent days is their incredible array of functions at an affordable cost. Apart from setting remainders and sending e-mails, they are also used in

- e-business
- SMS messaging
- Chatting
- Telemedicine and teleconferencing

Thus, these phones with wide roaming facility prove to be a really versatile device.

An increasing number of people are overwhelmed by the efficiency and convenience of internet for making web-based transactions globally, as it is the technology of the 21" century. Intemet is an amazing tool and it has changed the lifestyle of the people considerably.

It is the ease of use, efficiency, and time factor, which have contributed to the growth and popularity of e-commerce. According to the Anderson survey, 3% of the companies are now virtual and by 2010, 40% of the companies will be virtual.

This will make e-Commerce all pervasive in a few years time and people may even not venture out to buy anything except on the internet. But lately security issues on ecommerce transactions have raised a few questions which need to be taken care of.

The consistency on internet privacy protection plays a major role to boost the growth of e-commerce. E-commerce industry is slowly addressing security issues on their internal networks.

2. BIOMETRICS:

A biometric system is a recognition system, which makes a personal identification by determining the authenticity of a specific physiological or behavioral characteristic possessed by the user. This method of identification is preferred over traditional methods involving passwords and PIN numbers for various reasons:

- The person to be identified is required to be physically present at the point of identification.
- Identification based on biometric techniques eliminates the need to remember a password or carry an identity.

Depending on the context on which a biometric system works, it can be Either classified as an identification system or a verification (authentication) system identification involves in establishing a person's identify whereas in verification involves confirming or denying a person's claiming identity.

The evolution of cyber threats is increasingly threatening traditional access methods based on user IDs and passwords to authenticate digital identity, pushing companies to adopt new technologies and systems that are safer for users

2017 saw over half a billion stolen accounts in the world and almost 17.8 million violated domains. Faced with the numerous violations of sensitive personal data, consumers now recognize the inadequacy of traditional passwords, often vulnerable (however we must say the fact that even in 2017 the most used password was confirmed 123456), and see more and more in the adoption advanced technological systems the opportunity **to improve their computer security**.

Biometric recognition is an **information system that allows the identification of a person based on some of its main physiological and behavioral characteristics**.It is based on hardware systems for data acquisition that integrate the **software components** that allow, through mathematical algorithms, to perform data analysis and reconstruct the identity of a person and recognize it.

Biometrics are body measurements and calculations related to human characteristics. Biometric authentication (or realistic authentication) is used in computer science as a form of identification and access control. It is also used to identify individuals in groups that are under surveillance.

Biometric identifiers are the distinctive, measurable characteristics used to label and describe individuals. Biometric identifiers are often categorized as physiological characteristics, which are related to the shape of the body.

Examples include, but are not limited to mouse movement,[1] fingerprint, palm veins, face recognition, DNA, palm print, hand geometry, iris recognition, retina and odor/scent. Behavioral characteristics are related to the pattern of behavior of a person, including but not limited to typing rhythm, gait, signature, behavioral profiling, and voice.

Some researchers have coined the term 'behaviometrics' to describe the latter class of biometrics.[2]

More traditional means of access control include token-based identification systems, such as a driver's license or passport, and knowledge-based identification systems, such as a password or personal identification number. Since biometric identifiers are unique to individuals, they are more reliable in verifying identity than token and knowledge-based methods; however, the collection of biometric identifiers raises privacy concerns about the ultimate use of this information.

3. MULTIBIOMETRICS:

A multi-biometrics system is obtained by the integration of multiple individual biometrics models. A numbers of models integrating hand geometry, keystroke dynamics, face and iris recognition system have flooded the markets in recent years.

Here we present a multimodal system that can be embedded in a mobile phone, which integrates fingerprint, voice and facial scanning. It shuts down the problem of high False Rejection Rate of facial scanners, eliminates the fooling of fingerprint scanners and overshadows the disadvantage of voice recognition models.

Biometric systems which permit the fusion of two or more types of biometric systems are known as Multimodal biometric systems.

The sources of information from different characters are acquired, pre- processed, features extracted and compared with the stored templates in the database.

Finally based on matching, decision about recognition is made. The fusing of information of biometric characters can take place in any of the levels.

Various fusion techniques are available for multimodal biometrics such as sensor level, feature level, score level, rank level and decision level fusion.

This paper presents a fusion modal for multimodal biometric system using face and voice biometric traits. Proposed fusion modal involves feature level, match score level, rank level & decision level fusion.

Log Gabor & LBP features are used for facial feature extraction and voice features are extracted using MFCC & LPC features.Matching module will be carried out by comparing the test fused feature vectors with all training data using Euclidian distance measure.

KNN Classifier is used for decision making. In future it is planned to evaluate performance of various fusion techniques based on EER, FAR & FRR.

Multimodal biometric systems use multiple sensors or biometrics to overcome the limitations of unimodal biometric systems. For instance iris recognition systems can be compromised by aging irises and electronic fingerprint recognition can be worsened by worn-out or cut fingerprints. While unimodal biometric systems are limited by the integrity of their identifier, it is unlikely that several unimodal systems will suffer from identical limitations. Multimodal biometric systems can obtain sets of information from the same marker (i.e., multiple images of an iris, or scans of the same finger) or information from different biometrics (requiring fingerprint scans and, using voice recognition, a spoken passcode).

Multimodal biometric systems can fuse these unimodal systems sequentially, simultaneously, a combination thereof, or in series, which refer to sequential, parallel, hierarchical and serial integration modes, respectively. Fusion of the biometrics information can occur at different stages of a recognition system. In case of feature level fusion, the data itself or the features extracted from multiple biometrics are fused. Matching-score level fusion consolidates the scores generated by multiple classifiers pertaining to different modalities. Finally, in case of decision level fusion the final results of multiple classifiers are combined via techniques such as majority voting. Feature level fusion is believed to be more effective than the other levels of fusion because the feature set contains richer information about the input biometric data than the matching score or the output decision of a classifier. Therefore, fusion at the feature level is expected to provide better recognition results.

Spoof attacks consist in submitting fake biometric traits to biometric systems, and are a major threat that can curtail their security. Multi-modal biometric systems are commonly believed to be intrinsically more robust to spoof attacks, but recent studies[15] have shown that they can be evaded by spoofing even a single biometric trait.

4. NEED FOR BIOMETRICS IN MOBILE PHONES:

Nowadays, shopping through the internet has become very popular and surely, a WAP enabled mobile phone provides the facilities to consumers to shop online. Credit cards continue to be an efficient tool for online money transactions.

But, on the other hand, credit card's number can be stolen on its way to its destination and can be misused by hackers. Thus, e-Business through a mobile phone becomes insecure.

Software, like those provided by ArticSoft and ISC, created a back door entry and were largely involved in data spoofing. In addition to this, many user and companies were prone to the attack of many viruses and Trojan horses.

With so much of problems faced, the service provide turned their attention towards biometrics to prevent data spoofing and to provide secure e-Transactions

Mobile biometric authentication is primarily used for mobile banking and e-commerce. For example, customers can authenticate transactions that originate from their mobile banking or retail applications using facial recognition or voice biometrics..

Fintech companies that integrate with customer bank accounts also leverage mobile biometrics to authenticate transactions. These can be at a physical point of sale (e.g., performing facial recognition when using Apple Pay or Samsung Pay in a brick-and-mortar location) or to authenticate electronic transfer of funds through a mobile fintech app (e.g. amazon.Pay or PayTm).

Multimodal biometrics applies the use of two or more biometric modalities for multi-factor authentication. The implementation of multimodal biometrics should strike the right balance between matching performance and convenience; that is, multimodal biometrics will ideally reduce the likelihood of a false positive without adding complexity to the user experience.

Constantly using passwords on a smartphone can be a pain, not to mention a high security risk. Luckily, popular mobile browsers like Chrome and Firefox Lite are now supporting biometrics for authentication to make logging in to social media, email, and online shopping accounts easier and more secure. Here’s what you need to know about the Web Authentication API.

Authenticate your profile on your mobile device

Chrome OS, Windows, MacOS, Linux, and Android are all adding features to help users safely log in using biometric identification via USB, Bluetooth, and NFC devices connected to smartphones and tablets. With such convenience, users can verify their accounts on the go.

Preventing cyberattacks with browser-based biometrics.

Passwords are notoriously bad at protecting users’ accounts and the information they store. Facial scans, fingerprints, and voice recognition would make it exponentially harder for hackers to commit identity theft. That means you’re also less likely to be duped by an email from a hacker pretending to be your boss asking for the company credit card’s details.

Enjoy more secure online transactions

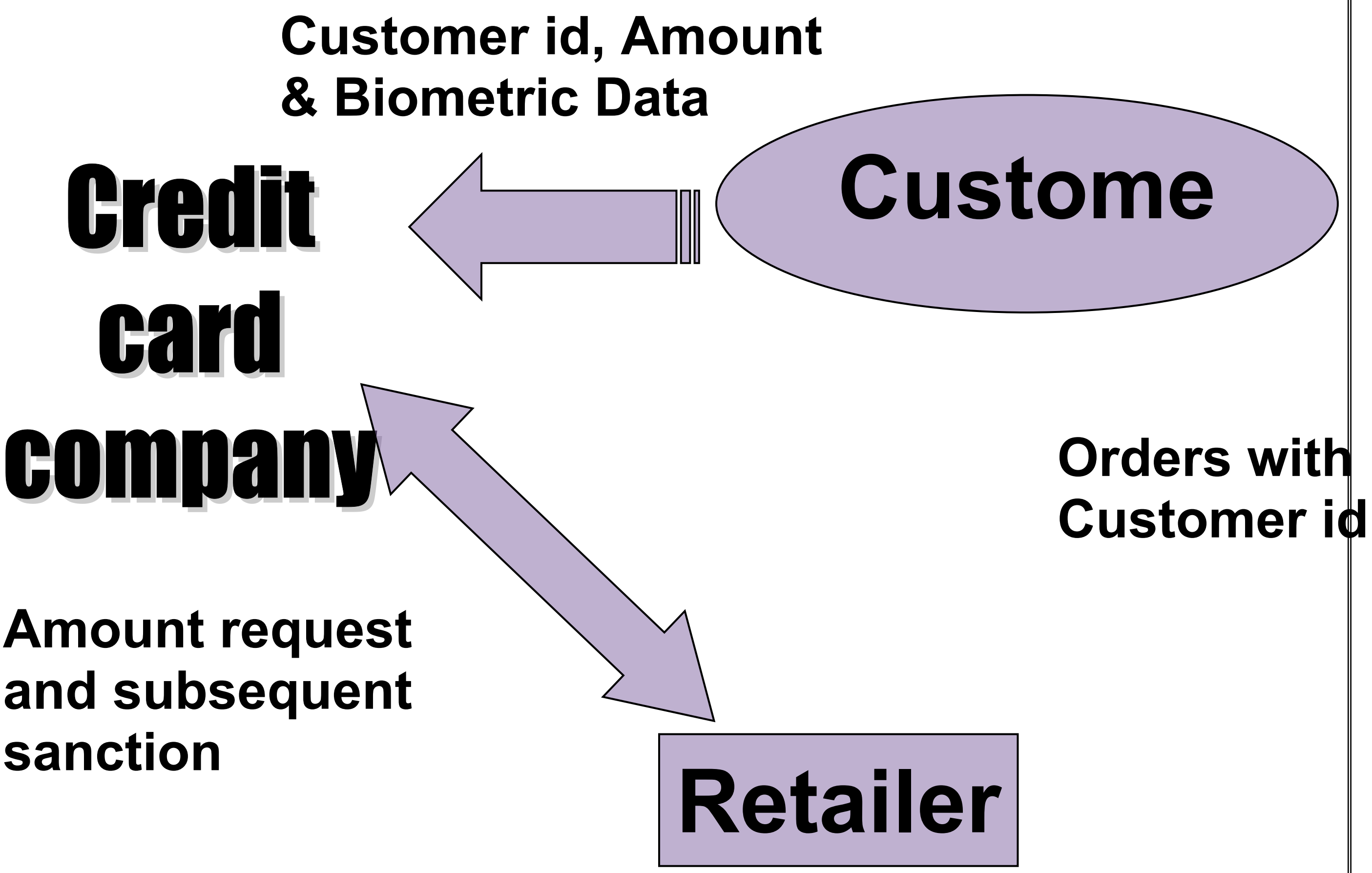
Biometric verification will also retire the need for logging in your information when shopping online, streaming video, using cloud applications, and other internet-based transactions. Windows 10 has already adopted features that offer limited account management with fingerprints and facial scans. Samsung phones now have Samsung Pay, which turns them into digital wallets that are protected by fingerprint or iris scans.

5. FACE RECOGNITION:

Facial recognition is considered to be one of the most tedious among all scans. Further, difficulty in acquisition of face and cost of equipments make it more complex.

However, some WAP enabled phones like CX 400K and LG-SD1000 manufactured by LG electronics, have built in camera that can acquire images and can be transmitted over internet. This it is sent to the credit card company to verify the face received matches with the face in their database. If it matches, the goods are sent, else the order is rejected.

protocol



Customer id, Amount & Biometric Data

Credit card company

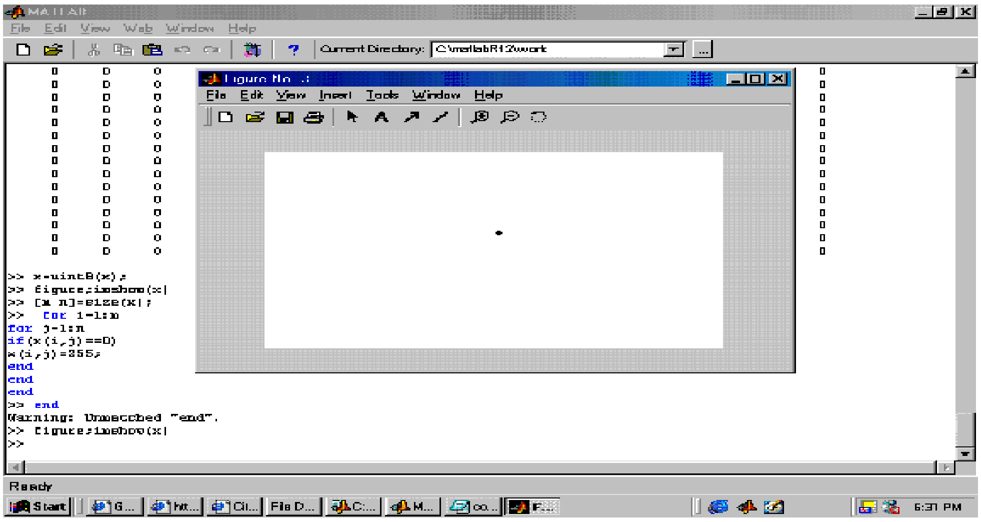
Custome

Orders with Customer id

Amount request and subsequent sanction

Retailer

We in our IMAGE PROCCESSING LAB took two faces with small differences (you see a small dot in the forehead of second face) and programmed MATLAB to find the difference between the two. The output is place below:



```
     0     0     0
     0     0     0
     0     0     0
     0     0     0
     0     0     0
     0     0     0
     0     0     0
     0     0     0
     0     0     0
     0     0     0
     0     0     0
     0     0     0
     0     0     0
     0     0     0
     0     0     0

>> x=uint8(x);
>> figure;imshow(x)
>> [m n]=size(x);
>>   for i=1:m
for j=1:n
if(x(i,j)==0)
x(i,j)=255;
end
end
end
>> end
Warning: Unmatched "end".
>> figure;imshow(x)
>>
```

MATLAB
File Edit View Web Window Help
Current Directory: C:\matlabR12\work
Figure No. 1
File Edit View Insert Tools Window Help
Ready
Start
6:31 PM

Difference between two images can be found by MATLAB.

The above simulations shows that even two persons having almost similar face with minute difference can also be differentiated.

Now, there arises a problem. A man, without bread, make as a transaction successfully .A week later he makes another transaction with some hair grown on his chin and go for acquiring images of any part of the face like forehead, nose, ear etc.

Hence, this type of facial scanning system can be used as a part of the multi-biometric system we have presented above.

•Facial geometry uses geometrical characteristics of the face. May use several cameras to get better accuracy (2D, 3D...) •Skin pattern recognition: (Visual SkinPrint)
•Facial thermo gram: uses an infrared camera to map the face temperatures
•Smile: recognition of the wrinkle changes when smiling

Facial Geometry: Many different methods based on geometrical characteristics of the face have been developed such as "local feature analysis", "Eigen face or Principal Component Analysis",

Skin Pattern Recognition: Visual Skin Print relies on standard hardware -most web-cams and higher resolution mass-market video cameras, connected to a PC, will work. Visual Skin Print™ is based on a simple yet powerful idea: using the details of the skin for authentication

Facial Thermo Gram: Facial thermo gram requires an (expensive) infrared camera to detect the facial heat patterns that are unique to every human being. Technology Recognition Systems worked on that subject in 1996-1999. Now disappeared. Face Recognition in Hyper spectral Images" is an article describing a variant using several wavelengths.

Smile Recognition: The Stony Brook university system relies on probing the characteristic pattern of muscles beneath the skin of the face.

Guan takes two snaps of a person in quick succession, asking subjects to smile for the camera. He then uses a computer to analyze how the skin around the subject's mouth moves between the two images. The software does this by tracking changes in the position of tiny wrinkles in the skin, each just a fraction of a millimeter wide.

A facial recognition system is a technology capable of matching a human face from a digital image or a video frame against a database of faces, typically employed to authenticate users through ID verification services, works by pinpointing and measuring facial features from a given image.

Development began on similar systems in the 1960s, beginning as a form of computer application. Since their inception, facial recognition systems have seen wider uses in recent times on smartphones and in other forms of technology, such as robotics. Because computerized facial recognition involves the measurement of a human's physiological characteristics, facial recognition systems are categorized as biometrics.

Although the accuracy of facial recognition systems as a biometric technology is lower than iris recognition and fingerprint recognition, it is widely adopted due to its contactless process.[1] Facial recognition systems have been deployed in advanced human–computer interaction, video surveillance and automatic indexing of images.

Automated facial recognition was pioneered in the 1960s. Woody Bledsoe, Helen Chan Wolf, and Charles Bisson worked on using the computer to recognize human faces. Their early facial recognition project was dubbed "man-machine" because the coordinates of the facial features in a photograph had to be established by a human before they could be used by the computer for recognition.

On a graphics tablet a human had to pinpoint the coordinates of facial features such as the pupil centers, the inside and outside corner of eyes, and the widows peak in the hairline. The coordinates were used to calculate 20 distances, including the width of the mouth and of the eyes. A human could process about 40 pictures an hour in this manner and so build a database of the computed distances.

A computer would then automatically compare the distances for each photograph, calculate the difference between the distances and return the closed records as a possible match.

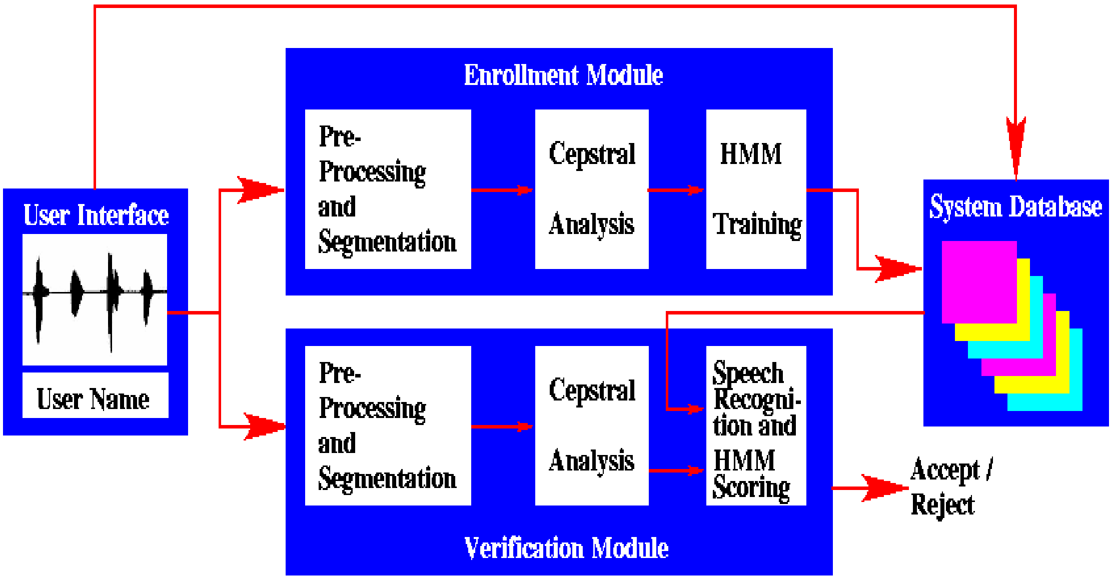
6. VOICE RECOGNITION:

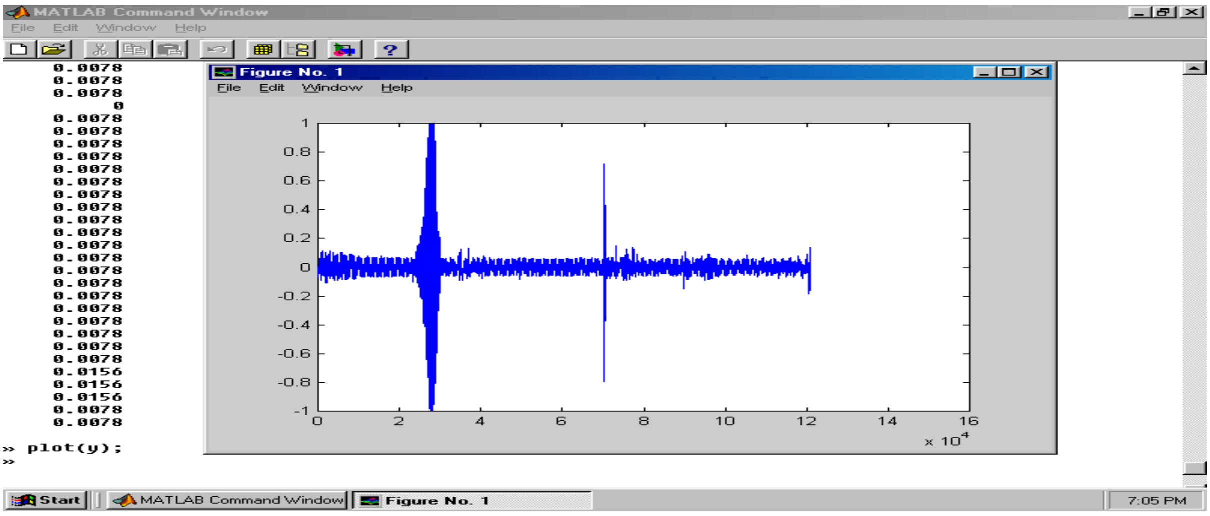
The speaker-specific characteristics of speech are due to difference in physiological and behavioral aspects of the speech production system in humans. The main physiological aspect of the human speech production system is the vocal tract shape.

The vocal tract modifies the spectral content of an acoustic wave as it passes through it, thereby producing speech. Therefore, it is common in speaker verification systems to make use of features derived only from the vocal tract.

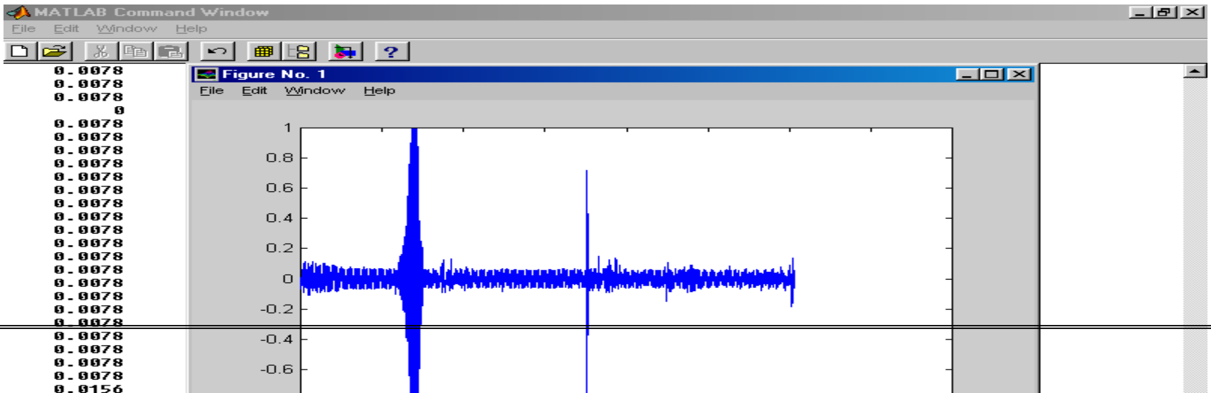
The microphone in the mobile phone captures the speech. Then, using cepstral analysis, an utterance may be represented as a sequence of feature vectors.

Utterances, spoken by the same person but at difference times, result in similar yet a different sequence of features vectors. So, the irrespective of the mood of the consumer, his transaction is accepted or rejected. The following algorithm may be used in voice verification.





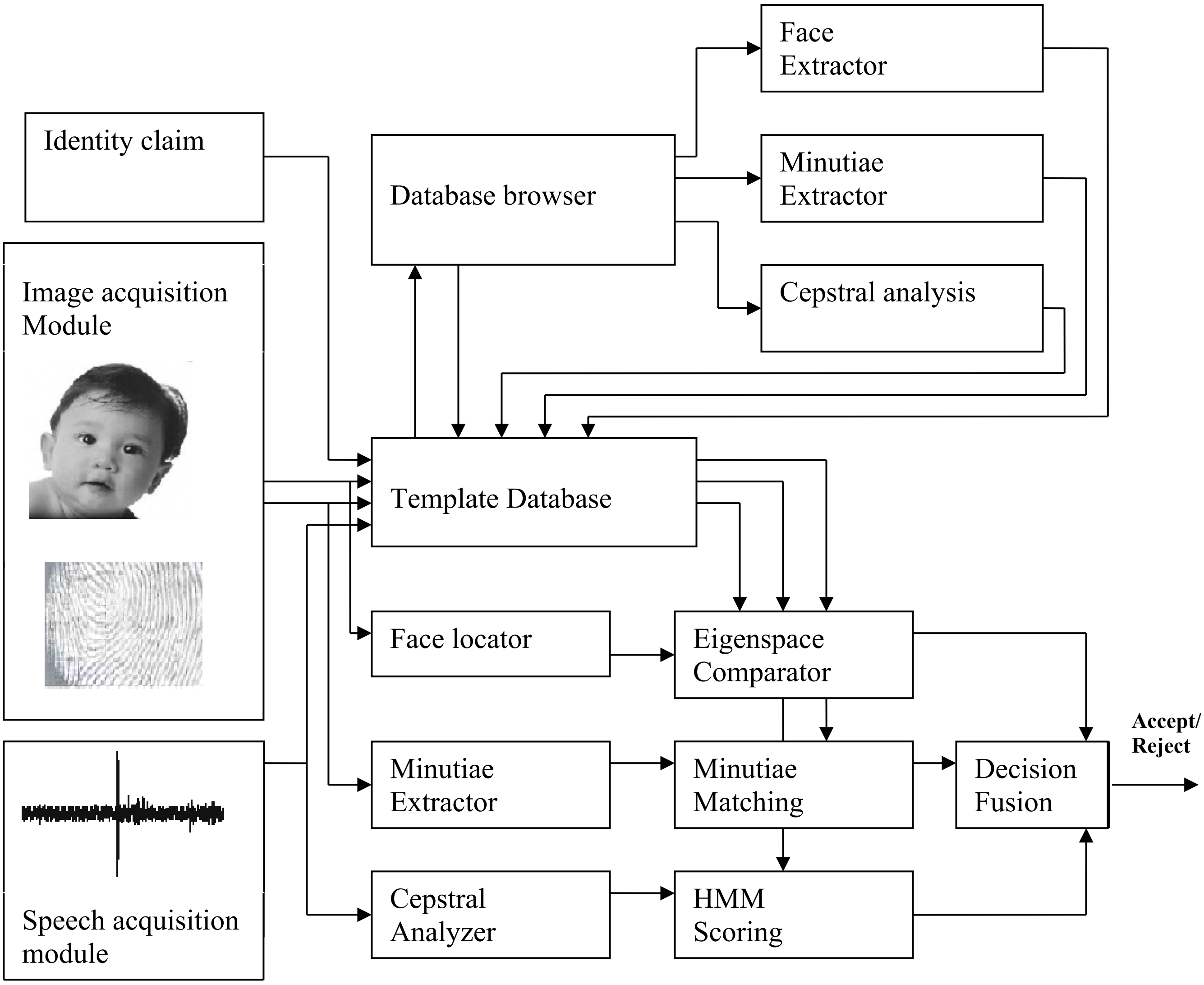
```
    0.0078
    0.0078
    0.0078
         0
    0.0078
    0.0078
    0.0078
    0.0078
    0.0078
    0.0078
    0.0078
    0.0078
    0.0078
    0.0078
    0.0078
    0.0078
    0.0078
    0.0078
    0.0078
    0.0078
    0.0078
    0.0078
    0.0078
    0.0078
    0.0156
    0.0156
    0.0156
    0.0078
    0.0078

» plot(y);
»
```



```
    0.0078
    0.0078
    0.0078
         0
    0.0078
    0.0078
    0.0078
    0.0078
    0.0078
    0.0078
    0.0078
    0.0078
    0.0078
    0.0078
    0.0078
    0.0078
    0.0078
    0.0078
    0.0078
    0.0078
    0.0078
    0.0078
    0.0078
    0.0078
    0.0156
```

Graph2 was plotted. The above graph shows some minute differences which prove that this system cannot be fooled by *imitation.*

ENROLLMENT MODULE



VERFICATION MODULE

As every mobile phone have an in-built microphone and some have video camera, the need for an extra hardware for the speech and image acquisition is eliminated. A proposal for the display screen to act as a fingerprint acquisition is dealt later.

Voice or speaker recognition is the ability of a machine or program to receive and interpret dictation or to understand and carry out spoken commands.

Voice recognition has gained prominence and use with the rise of AI and intelligent assistants, such as Amazon's Alexa, Apple's Siri and Microsoft's Cortana.

Voice recognition systems enable consumers to interact with technology simply by speaking to it, enabling hands-free requests, reminders and other simple tasks.

Voice recognition software on computers requires that analog audio be converted into digital signals, known as analog-to-digital conversion.

For a computer to decipher a signal, it must have a digital database, or vocabulary, of words or syllables, as well as a speedy means for comparing this data to signals.

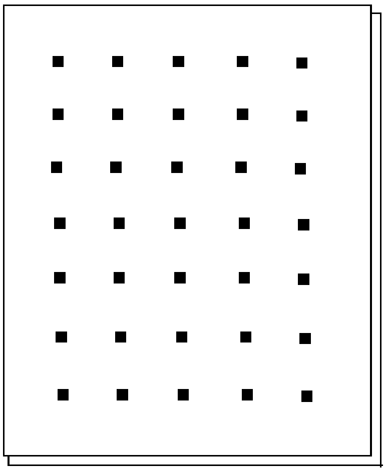
The speech patterns are stored on the hard drive and loaded into memory when the program is run. A comparator checks these stored patterns against the output of the A/D converter -- an action called pattern recognition.

7. FINGERPRINT ACQUISITION:

Finger based scanning is one of the oldest methods used for verification. Fingerprints, unique and immunable for all are made of series of ridges and furrows on the surface of the finger. These ridges and furrows determine the uniqueness of the fingerprints. Apart from these, minute points (i.e. local ridge characteristics that occur at either a ridge bifurcation or a ridge ending also play role in fool-proofing this biometric technique.

To reduce the search time and the computational complexity, fingerprint classification is undertaken and thus fingerprints are classified as whorl, right loop, left loop, arch, and arch. Recently researchers and scientists achieved a great feat by improving the fingerprint classification to 94%.

In today’s world, fingerprint matching techniques can be placed into two categories: minutiae-based and correlation based. In minutiae based technique, the minutiae points are found and their relative placement are mapped on the finger whereas in correlation based technique, the fingerprint acquired from the person is checked for certain points previously stored in the database. If both matches, the person is given authentication, else he is denied permission.



Transaction scanner embedded above display screen

The scanner here is a transparent layer above the screen. The scanner consists of arrays of capacitors of the size of 0.03□m. capacitors with such a small size can be manufactured with MEMS technology. When the consumer places his thumb on the scanner, the points at which his fingerprint touches the screen get discharged whereas others remain charged. Thus the fingerprint is scanned and is then sent for further process.

The oldest form of the fingerprint acquisition is the inked method in which an ink is applied over the finger and impression of the finger is taken over a real physical substrate, then a highly trained operator oversees the capture.

Security of data is a vital issue in modern computational devices, where mobile devices make it more sensitive. To ensure the safety of data as well as software systems fingerprint is one of the most authentic features.

Mobile devices use light architecture, which imposes a challenge to fingerprint verification techniques. Acquisition of fingerprints in small scanner also implies the difficulties of partial matching algorithms.

TIR technique of fingerprint scanning presented in this paper which can be implemented in integrated sensors. In our proposed method, system's robustness also augmented as the authentication is mainly focused on personal use.

Minutiae-based fingerprint matching algorithm is improvised which reduced the process interval and enabled the user defined sensitivity level of the system.

Fourier domain filtering techniques have made the system more reliable as well as it improved pre-processing efficiency reducing the uncertainty of feature loss and ridge discontinuity.

8.CONCLUSION:

Thus, this mobile multi-biometrics can be embedded in mobile phone. Phone is cost effective since no special hardware in required and is highly secured. Thus, this mobile phone becomes a reality will provide more e-Business and E-Transactions.

In this research, an attempt has been made for a technology solution based on the uniqueness of iris image as a biometric, for customer identification and authentication to secure e-commerce transactions. This is a very effective and robust method for preventing credit card fiaud when making e-commerce transactions.

Research leading to this application using iris image as a biometric is very premature at this time. Standards are yet to be established to capture high quality iris images.

The PCA technique is a good method for processing and extraction of key features of ins image and not difficult to implement compared to other feature extraction techniques like discrete wavelet transform etc.

Complex algorithms for encryption and decryption may be researched. The growth of e-commerce is purely dependent on customem hust for secure transactions. Global security laws and technology solutions will contribute towards this goal.

9.REFERENCES:

1)"Biometrics" by Samir Nanavathi, Dreamtech Wiley Publications.
2)"Biometrics made easy for you" by John walker.
3)"Science and Technology" a supplementary of "The HINDU"
4) J.G. Daugman, "High Confidence Visual Recognition of Persons by a Test of Statistical Independence", IEEE Tans. Pattern Analysis and Mchine Intelligence, vo1.15, pp.1148-1161, November 1993.

5) Berggren, L, “Iridology: A critical review”, Acfa Ophfhafnmlogica 63(1): 1-8, 1985. [SICockbum, D.M, “A study of the validity of iris diagnosis”, Australian Journal ofOptomery64: 154-157, 1981.