International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Impact Factor (2012): 3.358

Secure E-Transactions through Bio Metrics System

Sakthivel .A[1], Jayakeerthi .M[2]

[1]Periyar University College of Arts & Science, Pennagaram, TamilNadu, India
[2]Nehru College of Arts & Science, Coimbatore, TamilNadu, India

Abstract: ***In the present day world, online shopping using WAP enabled mobile phone has widely come into use. Credit cards serve as the currency during e-business and e-Shopping. As technology has advanced in the negative side also hackers and spoofers steal misuse credit card numbers, even though the network has been made secure. So, in this paper, we have proposed a multi-biometric model (integrating voice, fingerprint and facial scanning) that can be embedded in a mobile phone, this making e-transactions more secure. The model is very cost effective as we have tried to use the hardware already present in the phone. This paper uses for image processing or facial recognition and finger print. We have also simulated a few graphs for voice recognition and facial verification using MATLAB 6.0.***

Keywords: biometrics, multi biometrics, face Recognition, Voice recognition

1. Introduction

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 & Tele conferencing Thus; these phones with wide roaming facility prove to be a really versatile device.

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.

3. Multi Biometrics

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.

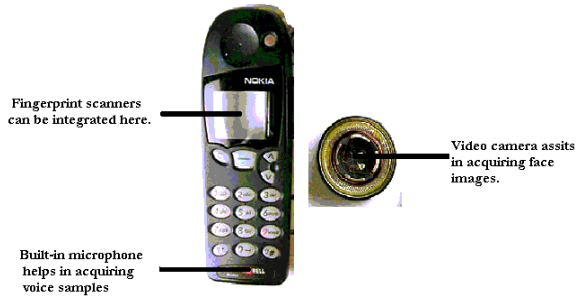
Here we present a multimodal system that can be embedded in a mobile phone, which integrates fingerprint, voice and facial scanning. It shuts down the problem of high False Rejection Rate of facial scanners, eliminates the fooling of fingerprint scanners and overshadows the disadvantage of voice recognition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

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 cards 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.

Also, a report in www.download.com stated that much anti-fraud 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.

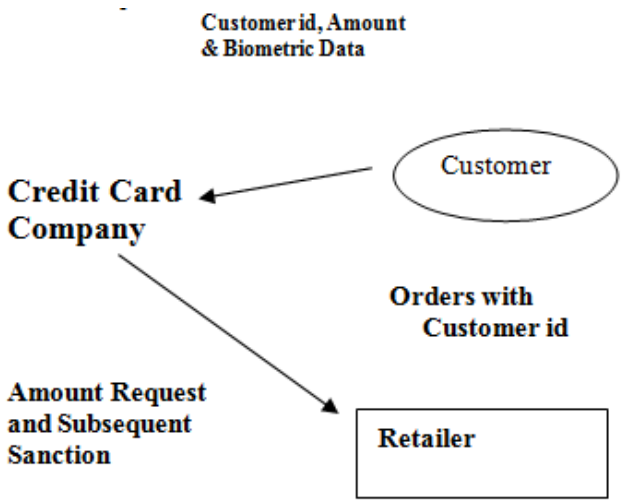
5. Future Mobile Phone



6. 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.



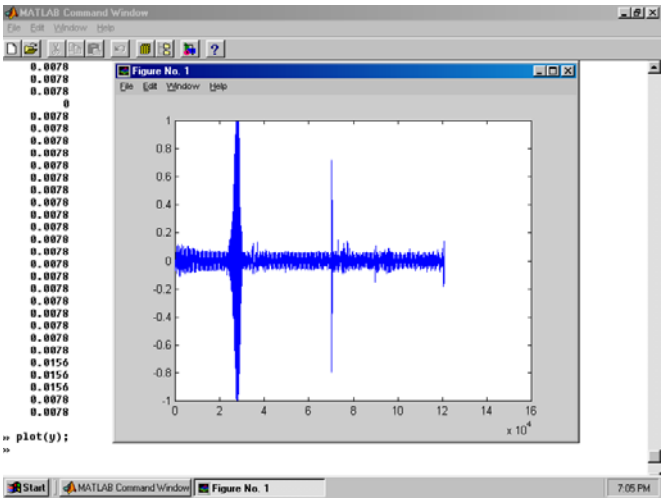
We in our IMAGE PROCCESSING LAB took two faces with small differences (you see a small dot in the forehead of second face) and programmed MATLAB to find the difference between the two.

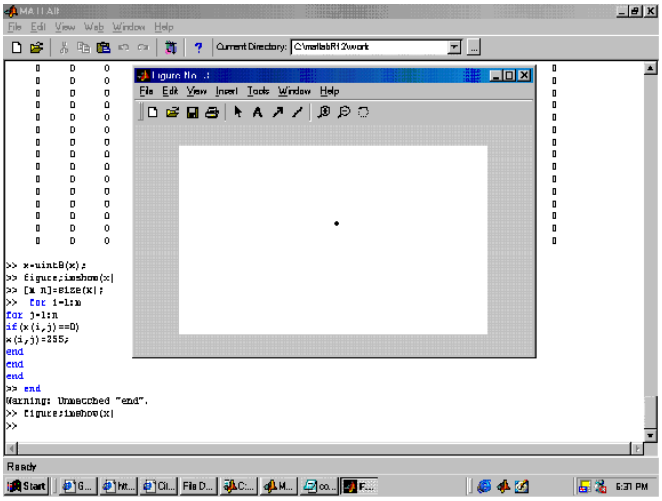
The output is place below:

Figure 1

Figure 2

Difference between two images can be founded by Matlabs





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

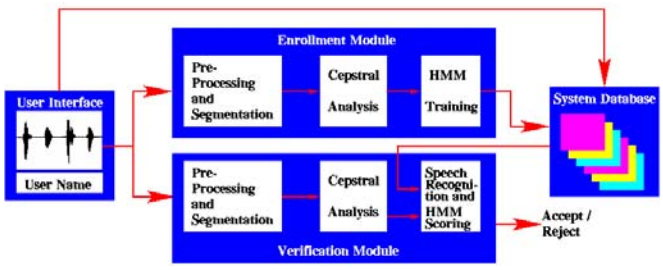
Now, there arises a problem. A man, without bread, make as a transaction successfully .A week later he makes another transaction with some hair grown on his chin and go for acquiring images of any part of the face like forehead, nose, ear etc.

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

7. 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.

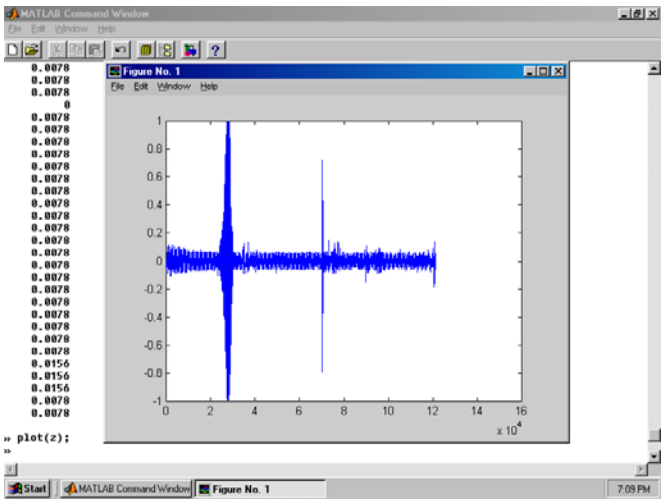


We recorded a person saying the letter 'a' directly into a sound recorder and plotted the graph1. This was simultaneously recorded in a tape recorder and Graph2 was plotted. The above graph shows some minute differences which prove that this system cannot be fooled by *imitation Verification Module.*

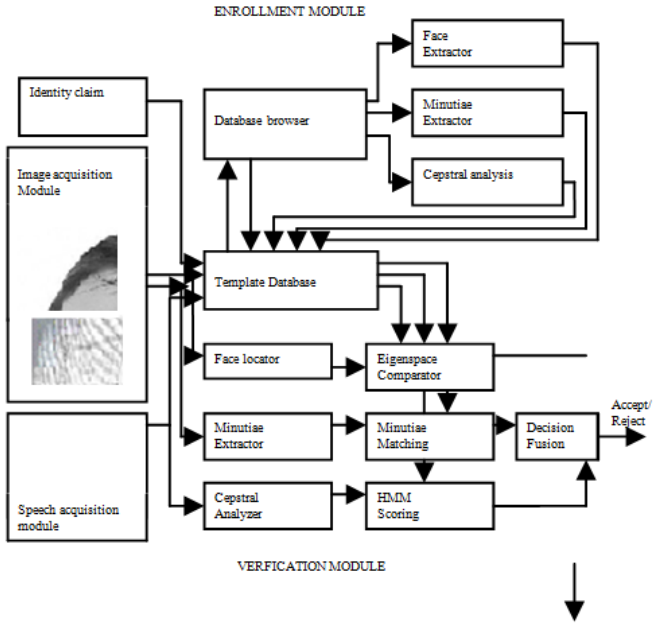
As every mobile phone have an in-built microphone and some have video camera, the need for an extra hardware for the speech and image acquisition is eliminated. A proposal for the display screen to act as a fingerprint acquisition is dealt later.

8. Finger Print 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%.

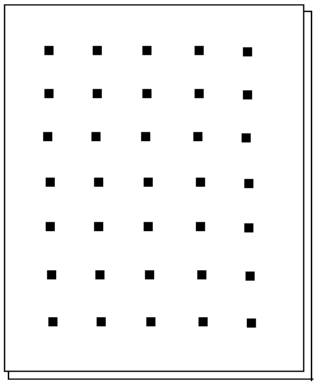


In today's world, fingerprint matching techniques can be placed into two categories: minutiae-based and correlation based. In minutiae based technique, the minutiae points are found and their relative placement are mapped on the finger whereas in correlation based technique, the fingerprint acquired 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.

The scanner here is a transparent layer above the screen. The scanner consists of arrays of capacitors of the size of 0.03µm. 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 other remains charged. Thus the finger print scanned and is sent further process.

9. Conclusion

Thus the Mobile multi biometrics can be embedded in Mobile phone. Phone is cost effective since no special Hardware in required and is highly secured. This is mobile Phone becomes a reality will provide more e-business and E-Transactions.



References

[1] Shuo Wang and Jing Liu, Department of Biomedical Engineering, School of Medicine, Tsinghua University, P. R.China " Biometrics on Mobile Phone " www.intechopen.com
[2] Informatica Economică vol. 13, no.1/2009 "Biometric Security for Cell Phones"
[3] Nimalan Solayappan and Shahram Latifi, Department of Electrical engineering, University of Nevada at Las Vegas, USA, "A Survey of Unimodal Biometric Methods"
[4] International Conference on Telecommunication Technology and Applications, Kounoudes et al., 2006, Voice Biometric Authentication for Enhancing Internet Service Security, pp. 1020-1025, with permission from IEEE.
[5] Bao, X.; Wang, J. & Hu, J. (2009). Method of Individual Identification based on Electroencephalogram Analysis. Proceedings of 2009 International Conference on New Trends in Information and Service Science, pp. 390-393, ISBN 978-0-7695-3687-3, Beijing, P.R.China, June 9-July 2, 2009.
[6] Snapshots of fingerprint security - Pro (retrieved from company release news [http://itunes.apple.com/us/app/fingerprint-security-pro/id312912865?mt=8)
[7] Reprinted from Proceedings of 2006 2nd International Conference on Telecommunication Technology and Applications, Kounoudes et al., 2006, Voice Biometric Authentication for Enhancing Internet Service Security, pp. 1020-1025, with permission from IEEE