International Journal of Emerging Trends & Technology in Computer Science (IJETTCS)
Web Site: www.ijettcs.org Email: editor@ijettcs.org, editorijettcs@gmail.com
Volume 2, Issue 2, March – April 2013 ISSN 2278-6856

Biometrics in Secure e-Transaction

Ms. Swati S Bobde[1], Prof. D. N. Satange[2]

[1]Post Graduate Student, Dept of Computer Science,
Arts, Commerce & Science College, Amravati

[2]Asstt. Professor, Dept of Computer Science,
Arts Commerce & Science College, Amravati

Abstract- ***In the present day word, 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 steal, misuse credit card numbers, even though the network has been made secure. So, in this seminar report, 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 reorganization and finger print. We have also simulated a few graphs for voice recognition and facial verification using MATLAB. The paper topic Biometrics in Secure E-Transactions CSE Seminars very clearly explains the indispensable role of biometrics for secure-transactions. The topic says that as technology has advanced there has been a negative side also hackers as spoofers steal/ misuse credit card numbers, even though the network has been made secure. The paperr abstract gives some insight into Multibiometrics. It says that 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.***

Keywords-Biometrics, Multibiometrics, Face Recognition, Voice Recognition, Iris Recognition, Finger Print Identification

1.INTRODUCTION

In an era of Information Technology, mobile phones are more and more widely used Worldwide, not only for basic communications, but also as a tool to deal with personal Affairs and process information acquired anywhere at any time. It is reported that there are more than 4 billion cell phone users over the world and this number still continues to grow as predicted that by 2015 more than 86% of the world population will own at least one cell phone. 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. Biometrics in Secure E-Transactions clearly explains the indispensable role of biometrics for secure-transactions. This paper discusses that as technology has advanced there has been a negative side also hackers as spoofer's steal / misuse credit card numbers, even though the network has been made secure. This paper, proposes a multi-biometric model **(integrating voice, fingerprint and facial scanning)** that can be embedded in a mobile phone this making e-transactions more secure.

2. BIOMETRICS

The term "biometrics" is derived from the Greek words "bio" (life) and "metrics" (to measure). Automated biometric systems have only become available over the last few decades, due to significant advances in the field of computer processing. Many of these new automated techniques, however, are based on ideas that were originally conceived hundreds, even thousands of years ago. Biometrics(or biometric authentication) refers to the identification of humans by their characteristics or traits. Biometrics 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. 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. 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.

Traditional security practices often involve the use of two authentication methods: possession based and knowledge based. Knowledge based authentication requires that the users remember a user name and password or PIN numbers or answers to security questions. Possession based can use radio frequency IDs, Smart Cards, Interactive Tokens etc. Possession based authentication has the same usability issue as the knowledge based authentication, if the object used for authentication is forgotten at home, in the hotel room, in the car etc the authentication

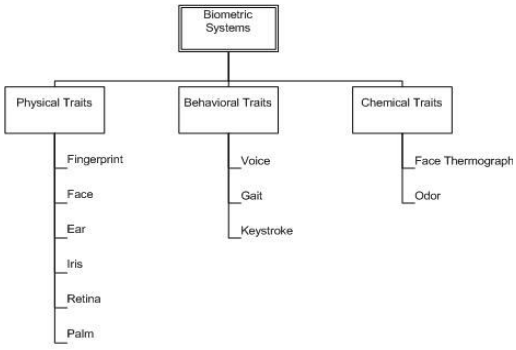

Figure 1. Biometric Systems Classes[1]

It is unlikely that several unimodal systems will suffer from identical limitations. Multi-
biometric systems can integrate these unimodal systems sequentially, simultaneously, a combination thereof, or in series, which refer to sequential, parallel, hierarchical and serial integration modes, respectively Multi-biometric 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 pass-code) cannot be performed. Biometric security systems are using:

- Physical human identifiers like fingerprint,
face, iris, retina, DNA, hand geometry and vein geometry
- Behavioral identifiers like speech, signature, and keystroke timing
- Chemical identifiers like odor and body heat.

Biometric systems are used for two purposes. One is to verify that the user is genuine by comparing the acquired biometric trait with the one stored for that user. The other purpose the biometrics are used is to identify a user in which case the acquired biometric trait is compared with a collection of the same traits from multiple users.[3]

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. Multi-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 iris and finger scanning systems by worn-out or cut fingerprints. While unimodal biometric systems are limited by the integrity of their identifier, sequential, parallel, hierarchical and serial integration modes, respectively. Broadly, the information fusion is divided into three parts, pre-mapping fusion, midst-mapping fusion, and post-mapping fusion/late fusion. In pre-mapping fusion information can be combined at sensor level or feature level.

Sensor-level fusion can be mainly organized in three classes:

(1) Single sensor-multiple instances,
(2) intra-class multiple sensors, and
(3) Inter-class multiple sensors.

Feature-level fusion can be mainly organized in two categories:

(1) intra-class and
(2) Inter-class.

Intra-class is again classified into four subcategories:

(a) Same sensor-same features,
(b) Same sensor-different features,
(c) Different sensors-same features, and
(d) Different sensors-different features[1]

4. NEED FOR BIOMETRICS IN MOBILE PHONES

Now a days, 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 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. Biometric systems can be integrated with cell phones in two ways: As a biometric collecting device or as a stand-alone system to protect unauthorized use of the cell phone. In the first case cell phones are collecting

the biometric and then they are passing it via internet or via voice communication to a remote location where it is processed and matched. This proves useful for remote transactions when the identity of the caller has to be proven. As an example, the user calls his bank to make a transaction, he is going to introduce himself as Swati Bobade and in order to verify his identity he is asked to recite a passphrase. The voice recording is then processed and compared with the sample that was collected when the user enrolled in the system. Face, fingerprint, signature or key stroke are other biometric traits that today's cell phones have the capabilities to collect and transfer them to a remote location. The other implementation of biometric systems on cell phones is that the entire biometric system resides on the cell phone and it serves the purpose of preventing unauthorized access to cell phone's functions and data. Biometric systems can replace the annoying PIN security and with a swipe of a finger the phone can be unlocked and used. Today's implementations of biometric systems on cell phones include fingerprint recognition, voice recognition, face recognition, signature recognition and keystroke recognition.

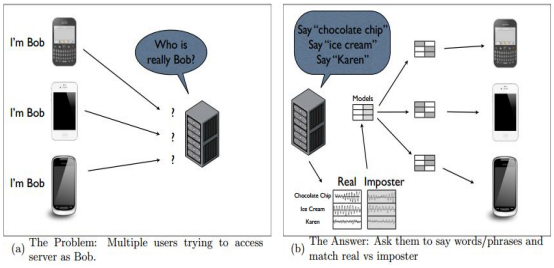

Figure 2. Feasible scenarios of biometrics on mobile phone[1]

Incorporated with advanced sensing platforms which could detect physiological and behavioral signals of various kinds, many types of biometric methods could be implemented on cell phones. This offers a wide range of possible applications such as personal privacy protection, mobile bank transaction service security, and telemedicine monitoring. The use of sensor data collected by mobile phones for biometric identification and authentication is an emerging frontier and has been increasingly explored in the recent decade. A typical architecture of this technology can be seen in Fig. 4.

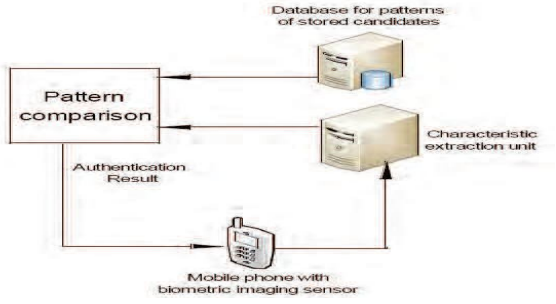

Figure 3 Mobile biometric authentication system (Xie & Liu, 2010) [5]

5. FUTURE MOBILE PHONE

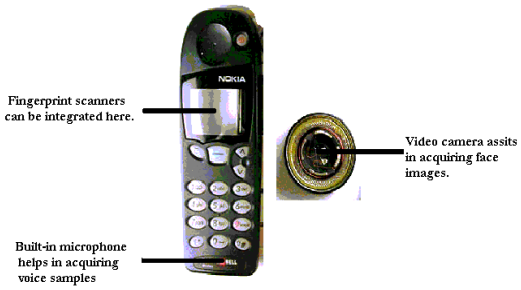

Figure 4.future mobile phone [1]

example of recent advances which successfully implemented biometrics on mobile phones

6. FINGER PRINT INDENTIFICATION ON MOBILE PHONE

Fingerprint biometric has been adopted widely for access control in places requiring high level of security such as laboratories and military bases. By attaching a fingerprint scanner to the mobile phone, this biometric could also be utilized for phone related security in a similar manner.fig.5.

7. 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:[1]

Figure.5. Snapshots of fingerprint security - Pro (retrieved from company release news)[6]

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:[1]

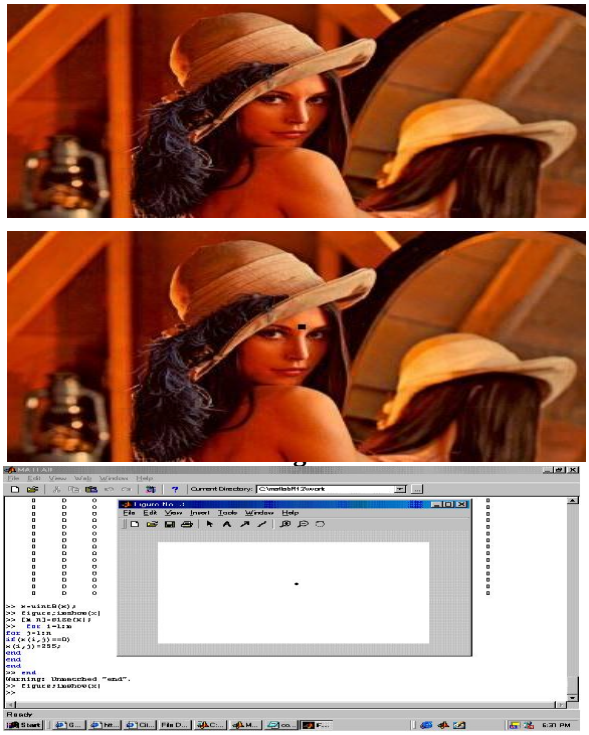

Figure 8. Difference between two image can be found by MATLAB [1]

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.

8. 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 spectral 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.. A voice signal conveys a person's physiological characteristics such as the vocal chords, glottis, and vocal tract dimensions. Automatic speaker recognition (ASR) is a biometric method that encompasses verification and identification through voice signal processing. The speech features encompass high-level and low level parts. While the high-level features are related to dialect, speaker style and emotion state that are not always adopted due to difficulty of extraction, the low-level features are related to spectrum, which are easy to be extracted and are always applied to ASR.

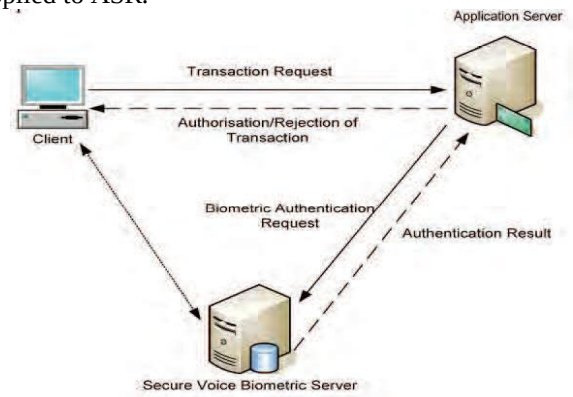

Figure 9. Voice biometric authentication for e-commerce transactions via mobile phone. [7]

9. IRIS RECOGNITION

With the integration of digital cameras that could acquire images at increasingly high resolution and the increase of cell phone computing power, mobile phones have evolved into networked personal image capture devices, which can perform image processing tasks on the phone itself and use the result as an additional means of user input and a source of context data (Rohs, 2005). This image acquisition and processing capability of mobile phones could be ideally utilized for mobile iris biometric.

Recently, iris recognition technology has been utilized for the security of mobile phones. As a biometric of high reliability and accuracy, iris recognition provides high level of security for cellular phone based services for example bank transaction service via mobile phone.

One major challenge of the implementation of iris biometric on mobile phone is the iris image quality, since bad image quality will affect the entire iris recognition process. Previously, the high quality of iris images was

achieved through special hardware design. For example, the Iris Recognition Technology for Mobile Terminals software once used existing cameras and target handheld devices with dedicated infrared cameras (Kang, 2010). To provide more convenient mobile iris recognition, an iris recognition system in cellular phone only by using built-in mega-pixel camera and software without additional hardware component was developed (Cho et al., 2005). Considering the relatively small CPU processing power of cellular phone, in this system, a new pupil and iris localization algorithm apt for cellular phone platform was proposed based on detecting dark pupil and corneal specular reflection by changing brightness & contrast value. Results show that this algorithm can be used for real-time iris localization for iris recognition in cellular phone. In2006, OKI Electric Industry Co., Ltd. announced its new Iris Recognition Technology for Mobile Terminals using a standard camera that is embedded in a mobile phone based on the original algorithm OKI developed, a snapshot of which can be seen in Fig. 10.

Figure 10. Iris recognition technology for mobile terminals. [8]

10. CHALLENGES TO MOBILE PHONE

In order to ensure the accuracy and efficiency of biometrics recognition on mobile phones, computing power and storage capacity of mobile phones are still needed to be significantly enhanced. Currently, the implementation of biometrics on mobile phones usually requires the simplification of algorithm used in conventional biometrics in order to be adapted for the relatively small CPU processing power of a cellular phone. This adaption will inevitably reduce the accuracy and security level, which highly limits the performance of mobile phone enabled biometric techniques. In addition, the essential hardware i.e. biometric sensors embedded on mobile phones are also required to provide better performance, e.g. higher resolution of image acquired with digital cameras on mobile phones, at lower cost while maintaining their miniaturization feature.[2]

11. OUTLOOK OF FUTURE DEVELOPMENT IN MOBILE PHONES

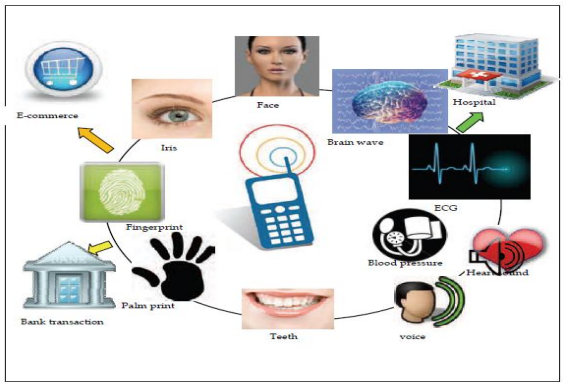

Figure11. An outline of future development in biometrics on mobile phone[1]

Numerous types of biometrics hold the potentials of being implemented onmobile phones. According to the different types of signals needed to be collected for feature extraction, applicable biometric methods can be classified into the imaging type, mechanical type and electrical type. The imaging type includes, but is not limited to the recognition of face, teeth and palm print in addition to fingerprint and iris, utilizing images captured by the camera embedded in the mobile phone. The mechanical type involves voice, heart sound using microphones and blood pressure by specific and miniaturized sensors attached to the mobile phone. Not only ECG can be used in mobile biometrics, the electroencephalography (EEG) identification also has applicability in this new area. The mobile phone based biometrics is also developing towards a multimodal functionality, which combines several biometric recognition methods to provide more reliable and flexible identification and authentication. Promising applications include personal privacy security, e-commerce, mobile bank transactions, e-health technology, etc. A grand outlook of future development in mobile phone based biometrics is outlined in the diagram below:

12. CONCLUSION

In this Paper, we study how the mobile phone can be used in biometrics. This versatile technique has so far proven to be a unique and promising participant in the areas of biometrics. Not only can mobile phone deliver successful solutions in the traditional biometric arenas of human identification and authentication, it has also been instrumental in securing the resource-constrained body sensor networks for health care applications in an efficient and practical manner. At the same time, there remain many challenges to be addressed and a lot more new technologies to be explored and developed. Before successful consumer-ready products are available, a great deal of research and development is still needed to improve all aspects of the mobile phone based biometric system. With a modicum of expectation, it is hoped that this chapter will play a part in further stimulating the research momentum on the mobile phone based biometrics. The paper concludes that the mobile multi-biometrics can be embedded in mobile phone. Phone is cost effective since no special hardware is required and is

highly secure. Thus, this mobile phone if it becomes a reality will provide more secure e-Business and E-Transactions.[2]

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

[8] (OKI introduces Japan's first iris recognition for camera-equipped mobile phones and PDAs, In: OKI Press Releases, 27.11.2006, Available from http://www.oki.com/en/press/2006/z06114e.html)