Research Inventy: International Journal of Engineering And Science
Vol.6, Issue 4 (April 2016), PP -128-133
Issn (e): 2278-4721, Issn (p):2319-6483, www.researchinventy.com

High End Security Approach for Banking Transaction and Image Quality Assessment through Iris and Face Recognition

T Maheshwar [1], M Mahesh [2], Mukramuddin [3]
[1,2,3]*ECE Department, Sree Dattha Institute of Engineering & Science*

Abstract: *To ensure the actual presence of a real legitimate trait in contrast to a fake self-manufactured synthetic or reconstructed sample is a significant problem in biometric authentication, which requires the development of new and efficient protection measures. In this paper, we present a novel software-based fake detection method that can be used in multiple biometric systems to detect different types of fraudulent access attempts. The objective of the proposed system is to enhance the security of biometric recognition frameworks, by adding liveness assessment in a fast, user-friendly, and non-intrusive manner, through the use of image quality assessment. The proposed approach presents a very low degree of complexity, which makes it suitable for real-time applications, using 25 general image quality features extracted from one image (i.e., the same acquired for authentication purposes) to distinguish between legitimate and impostor samples.*
Keywords: *Biometric application (Finger print, Iris), GSM Modem, EEPROM., matlab*

I. Introduction

Fake biometrics means by using the real images iris images captured from a printed paper and Fingerprint captured from dummy finger) of human identification characteristics create the fake identities like fingerprint, iris on printed paper. Fake user first capture the original identities of the genuine user and then they make the fake sample for authentication but biometric system have more method to detect the fake users and that's why the biometric system is more secure, Because each person have their unique characteristics identification. Biometrics system is more secure than other security methods like password, PIN, or card and key. A Biometrics system measures the human characteristics so users do not need to remember passwords or PINs which can be forgotten or to carry cards or keys which can be stolen. Biometric system is of different type that are face recognition system, fingerprint recognition system, iris recognition system.

II. The Hardware System

Micro controller: This section forms the control unit of the whole project. This section basically consists of a Microcontroller with its associated circuitry like Crystal with capacitors, Reset circuitry, Pull up resistors (if needed) and so on. The Microcontroller forms the heart of the project because it controls the devices being interfaced and communicates with the devices according to the program being written.

ARM7TDMI: ARM is the abbreviation of Advanced RISC Machines, it is the name of a class of processors, and is the name of a kind technology too. The RISC instruction set, and related decode mechanism are much simpler than those of Complex Instruction Set Computer (CISC) designs.

Liquid-crystal display (**LCD**) is a flat panel display, electronic visual display that uses the light modulation properties of liquid crystals. Liquid crystals do not emit light directly. LCDs are available to display arbitrary images or fixed images which can be displayed or hidden, such as preset words, digits, and 7-segment displays as in a digital clock. They use the same basic technology, except that arbitrary images are made up of a large number of small pixels, while other displays have larger elements.

GSM Modem: GSM/GPRS RS232 Modem from rhydo LABZ is built with sim com Make SIM900 Quad-band GSM/GPRS engine, works on frequencies 850 MHz, 900 MHz, 1800 MHz and 1900 MHz It is very compact in size and easy to use as plug in GSM Modem.

III. Design of Proposed Hardware System

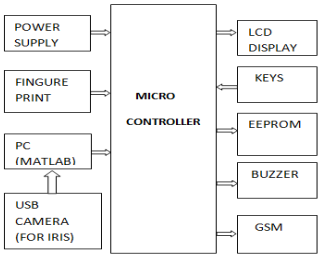

Fig.1. Block diagram

The design of entire system consisted of two part which are hardware and software. The hardware is designed by the rules of embedded system, and the steps of software consisted of three parts. The more details are shown as follows. Nowadays, using the ATM (Automatic Teller Machine) which provides customers with the convenient banknote trading is very common. However, the financial crime case rises repeatedly in recent years; a lot of criminals tamper with the ATM terminal and steal user's credit card and password by illegal means. Once user's bank card is lost and the password is stolen, the criminal will draw all cash in the shortest time, which will bring enormous financial losses to customer. How to carry on the valid identity to the customer becomes the focus in current financial circle. Traditional ATM systems authenticate generally by using the credit card and the password, the method has some defects. Using credit card and password cannot verify the client's identity exactly. In recent years, the algorithm that the fingerprint recognition continuously updated, which has offered new verification means for us, the original password authentication method combined with the biometric identification technology verify the clients' identity better and achieve the purpose that use of ATM machines improve the safety effectively.

The embedded ATM client authentication system is based on fingerprint recognition and Iris recognition which is designed after analyzed existed ATM system. The LPC2148 chip is used as the core of this embedded system which is associated with the technologies of fingerprint recognition and current high speed network communication, Iris recognition. The primary functions are shown as follows:

Fingerprint recognition: The masters' fingerprint information was used as the standards of identification. It must certify the feature of the human fingerprint before using ATM system.

Iris recognition: Iris recognition is an automated method of biometric identification that uses mathematical pattern-recognition techniques on video images of one or both of the irises of an individual's eyes, whose complex random patterns are unique, stable, and can be seen from some distance.

Remote authentication: System can compare current client's fingerprint and iris information with remote fingerprint and iris data server.

Telephone alarming: Once an exception happens, such as log in as the fake identity, the system will start the phone alarm to inform client and bank staff as soon as possible.

Message alarming: the message can be send to the relevant staff's mobile phone without any noise, in order to carry on emergency processing.

Police network connection: The system can call the police via the police network. Two discriminate analysis methods: Besides the fingerprint recognition, the mode of password Recognition can be also used for the system.

IV. Board Hardware Resources Features

Finger print

The design of algorithm based on fingerprint recognition is so vital for the whole system. We would approach two steps to process the images of fingerprint.

1) The detail of fingerprint recognition process

The first step was the acquisition of fingerprint image by above device mentioned in the algorithm, and the results could be sent to the following process. Secondly, pre-processing the images acquired. After obtain the fingerprint image, it must be pre-processing. Generally, pre-processing of ones is filtering, histogram computing, image enhancement and image binarization. Lastly, the characteristic value was extracted, and the results of the above measures would be compared with the information of owner's fingerprint in the database so as to verify whether the character is matched, and then the system returned the results matched or not.

2) The design of fingerprint image enhancement

Fingerprint recognition module is an extremely important part of the system, the high-quality images was the major factors of influencing the performance in the system. There is a lot of noise in fingerprint image; the image enhancement was the precondition for recognition of fingerprint characteristics. The algorithm of fingerprint recognition based on the algorithm of Gabor and direction filter was used. Fingerprint enhancement algorithm based on Gabor filter could be better to remove noise, strengthen the definition between the ridge and valley, it could significantly improve the image enhancement processing capacity, but this algorithm was slow in dealing with the high capacity requirements. Fingerprint enhancement algorithm based on direction filter has faster processing capabilities, but it was not good to handing the large noise areas. So combination of these two algorithms could obtain better effects. The algorithm based on direction filter was used in the clear area, and based on Gabor filter was used in the recoverable region.

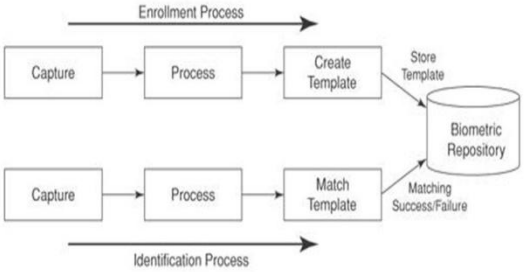

Fig2. Finger print recognition process

Iris recognition

Iris recognition is a method of identifying people based on unique patterns within the ring-shaped region surrounding the pupil of the eye. The iris usually has a brown, blue, gray, or greenish color, with complex patterns that are visible upon close inspection. Because it makes use of a biological characteristic, iris recognition is considered a form of biometric verification. In iris recognition, the identification process is carried out by gathering one or more detailed images of the eye with a sophisticated, high-resolution digital camera at visible or infrared (IR) wavelengths, and then using a specialized computer program called a matching engine to compare the subject's iris pattern with images stored in a database.

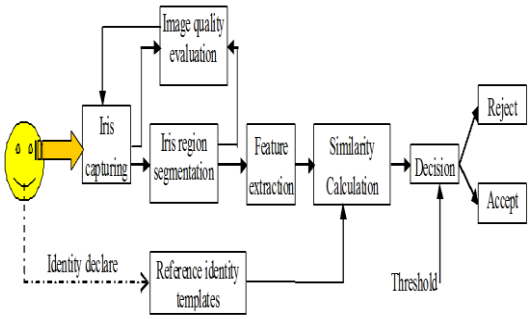

Fig 3. Iris recognition process

FACE RECOGNITION:

Face tracking has become an increasingly important research topic in the computer vision, mainly due to its large amount of real-world situations where such methods can be applied. Although the definition of the problem to be solved is very easy to understand, it is very difficult to come up with a robust solution due to variations in illumination, pose, appearance, etc. Initially, this project gives a brief introduction to the current state-of-the-art of both face detection and face tracking techniques. Finally, face tracking algorithm is implemented, this giving a robust solution for a specific context.

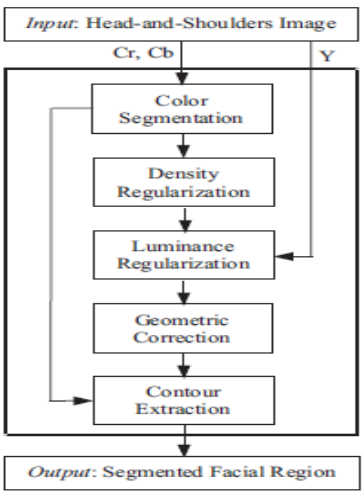

Fig. 5. Outline of face segmentation algorithm.

Keys: The Password can be entered using the keypad provided on the ATM.

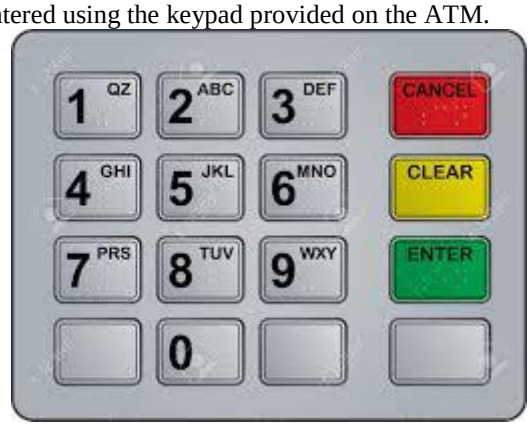

Fig 4.Keys for ATM

Buzzer:

The "Piezoelectric sound components" introduced herein operate on an innovative principle utilizing natural oscillation of piezoelectric ceramics. These buzzers are offered in lightweight compact sizes from the smallest diameter of 12mm to large Piezo electric sounders. Today, piezoelectric sound components are used in many ways such as home appliances, OA equipment, audio equipment telephones, etc. And they are applied widely, for example, in alarms, speakers, telephone ringers, receivers, transmitters, beep sounds, etc.

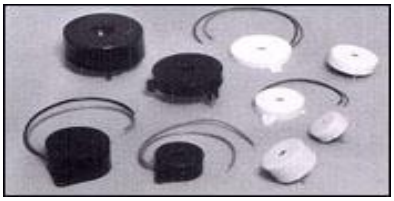

Fig5. Types of Buzzers

Basically, the sound source of a piezoelectric sound component is a piezoelectric diaphragm. A piezoelectric diaphragm consists of a piezoelectric ceramic plate which has electrodes on both sides and a metal plate (brass or stainless steel, etc.). A piezoelectric ceramic plate is attached to a metal plate with adhesives. Fig. 2 shows the oscillating system of a piezoelectric diaphragm. Applying D.C. voltage between electrodes of a piezoelectric diaphragm causes mechanical distortion due to the piezoelectric effect. For a misshaped piezoelectric element, the distortion of the piezoelectric element expands in a radial direction

EEPROM

EEPROM (also written **E^{2}PROM** and pronounced "e-e-prom", "double-e prom", "e-squared", or simply "e-prom") stands for **E**lectrically **E**rasable **P**rogrammable **R**ead-**O**nly **M**emory and is a type of non-volatile memory used in computers and other electronic devices to store small amounts of data that must be saved when power is removed, e.g., calibration tables or device configuration. Unlike bytes in most other kinds of non-volatile memory, individual bytes in a traditional EEPROM can be independently read, erased, and re-written. When larger amounts of static data are to be stored (such as in USB flash drives) a specific type of EEPROM such as flash memory is more economical than traditional EEPROM devices. EEPROMs are organized as arrays of floating-gate transistors. An EPROM usually must be removed from the device for erasing and programming, whereas EEPROMs can be programmed and erased in-circuit, by applying special programming signals. Originally, EEPROMs were limited to single byte operations which made them slower, but modern EEPROMs allow multi-byte page operations. It also has a limited life - that is, the number of times it could be reprogrammed was limited to tens or hundreds of thousands of times. That limitation has been extended to a million write operations in modern EEPROMs. In an EEPROM that is frequently reprogrammed while the computer is in use, the life of the EEPROM can be an important design consideration. It is for this reason that EEPROMs were used for configuration information, rather than random access memory.

GSM Module

GSM (Global System for Mobile communication) is a digital mobile telephone system that is widely used in many parts of the world. The mobile communications has become one of the driving forces of the digital revolution. Every day, millions of people are making phone calls by pressing a few buttons. Little is

known about how one person's voice reaches the other person's phone that is thousands of miles away. Even less is known about the security measures and protection behind the system. The complexity of the cell phone is increasing as people begin sending text messages and digital pictures to their friends and family. The cell phone is slowly turning into a handheld computer. All the features and advancements in cell phone technology require a backbone to support it. The system has to provide security and the capability for growth to accommodate future enhancements. General System for Mobile Communications, GSM, is one of the many solutions out there. GSM has been dubbed the "Wireless Revolution" and it doesn't take much to realize why GSM provides a secure and confidential method of communication.

GSM (Global System for Mobile communication) is a digital mobile telephone system that is widely used in many parts of the world. GSM uses a variation of Time Division Multiple Access (TDMA) and is the most widely used of the three digital wireless telephone technologies (TDMA, GSM, and CDMA). GSM digitizes and compresses data, then sends it down a channel with two other streams of user data, each in its own time slot. GSM operates in the 900MHz, 1800MHz, or 1900 MHz frequency bands. GSM has been the backbone of the phenomenal success in mobile telecoms over the last decade. Now, at the dawn of the era of true broadband services, GSM continues to evolve to meet new demands. One of GSM's great strengths is its international roaming capability, giving consumers a seamless service. This has been a vital driver in growth, with around 300 million. In the Americas, today's 7 million subscribers are set to grow rapidly, with market potential of 500 million in population, due to the introduction of GSM 800, which allows operators using the 800 MHz band to have access to GSM technology too.

GSM together with other technologies is part of an evolution of wireless mobile telecommunication that includes High-Speed Circuit-Switched Data (HCSD), General Packet Radio System (GPRS), Enhanced Data GSM Environment (EDGE), and Universal Mobile Telecommunications Service (UMTS). GSM security issues such as theft of service, privacy, and legal interception continue to raise significant interest in the GSM community. The purpose of this portal is to raise awareness of these issues with GSM security. The mobile communications has become one of the driving forces of the digital revolution. Every day, millions of people are making phone calls by pressing a few buttons. Little is known about how one person's voice reaches the other person's phone that is thousands of miles away. Even less is known about the security measures and protection behind the system. The complexity of the cell phone is increasing as people begin sending text messages and digital pictures to their friends and family. The cell phone is slowly turning into a handheld computer. All the features and advancements in cell phone technology require a backbone to support it. The system has to provide security and the capability for growth to accommodate future enhancements. General System for Mobile Communications, GSM, is one of the many solutions out there. GSM has been dubbed the "Wireless Revolution" and it doesn't take much to realize why GSM provides a secure and confidential method of communication.

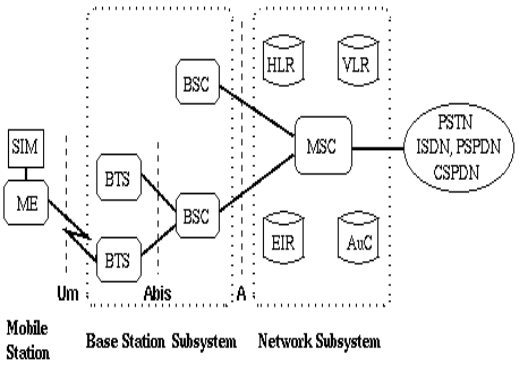

Fig.6. General Architecture of a GSM network

V. Conclusion

In this paper the access to the ATM is provided in more secure manner. Any fraudulent access by the fake user is eliminated with the help of biometric techniques like Finger print Authentication, Iris recognition and Face recognition. Also if the login is detected as fake identity the bank staff and police are informed immediately via message using GSM.

References

[1]. S. Prabhakar, S. Pankanti, and A. K. Jain, "Biometric recognition:Security and privacy concerns,"IEEE Security Privacy, vol. 1, no. 2,pp. 33–42, Mar./Apr. 2003.

[2]. T. Matsumoto, "Artificial irises: Importance of vulnerability analysis,"in Proc. AWB, 2004.

[3]. J. Galbally, C. McCool, J. Fierrez, S. Marcel, and J. Ortega-Garcia, "Onthe vulnerability of face verification systems to hill-climbing attacks,"Pattern Recognit., vol. 43, no. 3, pp. 1027–1038, 2010.

[4]. A. K. Jain, K. Nandakumar, and A. Nagar, "Biometric template security,"EURASIP J. Adv. Signal Process., vol. 2008, pp. 113–129, Jan. 2008.

[5]. J. Galbally, F. Alonso-Fernandez, J. Fierrez, and J. Ortega-Garcia,"A high performance fingerprint liveness detection method based onquality related features,"Future Generat. Comput. Syst., vol. 28, no. 1,pp. 311–321, 2012.

[6]. K. A. Nixon, V. Aimale, and R. K. Rowe, "Spoof detection schemes,"Handbook of Biometrics. New York, NY, USA: Springer-Verlag, 2008,pp. 403–423.

[7]. ISO/IEC 19792:2009, Information Technology—Security Techniques—Security Evaluation of Biometrics, ISO/IEC Standard 19792, 2009.

[8]. Biometric Evaluation Methodology. v1.0, Common Criteria, 2002.

[9]. K. Bowyer, T. Boult, A. Kumar, and P. Flynn,Proceedings of the IEEE Int. Joint Conf. on Biometrics. Piscataway, NJ, USA: IEEE Press, 2011.

[10]. G. L. Marcialis, A. Lewicke, B. Tan, P. Coli, D. Grimberg, A. Congiu,et al., "First international fingerprint liveness detection competition—LivDet 2009," in Proc. IAPR ICIAP, Springer LNCS-5716. 2009,pp. 12–23.

[11]. M. M. Chakka, A. Anjos, S. Marcel, R. Tronci, B. Muntoni, G. Fadda,et al., "Competition on countermeasures to 2D facial spoofing attacks,"in Proc. IEEE IJCB, Oct. 2011, pp. 1–6.