International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2018 IJSRCSEIT | Volume 3 | Issue 4 | ISSN : 2456-3307

Fingerprint Based Authentication Using Image Processing Techniques

C. Thirumoorthi
Assistant Professor , Department of Information and Computer Technology, Hindusthan College of Arts and Science, Coimbatore, Tamil Nadu, India

ABSTRACT

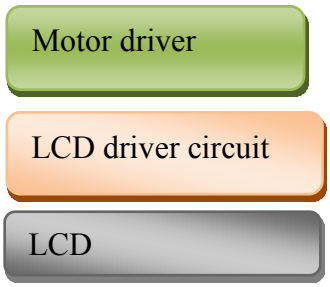
Fingerprint Based ATM (Automatic Teller Machine) is a desktop application where fingerprint of the user is used as a authentication. The finger print minutiae features based image processing are different for each human being so the user can be identified uniquely. Instead of using ATM card Fingerprint based ATM is safer and secure. There is no worry of losing ATM card and no need to carry ATM card in your wallet. You just have to use your fingerprint in order to do any banking transaction. The user has to login using his fingerprint and he has to enter the pin code in order to do further transaction. The user can withdraw money from his account. User can transfer money to various accounts by mentioning account number. In order to withdraw money user has to enter the amount he want to withdraw and has to mention from which account he want to withdraw (i.e. saving account, current account) .The user must have appropriate balance in his ATM account to do transaction. User can view the balance available in his respective account.

Keywords : ATM, Image Processing, Finger Print, Transaction And Authentication.

I. INTRODUCTION

Fingerprinting or finger-scanning technologies are the oldest of the biometric sciences and utilize distinctive features of the fingerprint to identify or verify the identity of individuals [1]. All fingerprints have unique characteristics and patterns. A normal fingerprint pattern is made up of lines and spaces. These lines are called ridges while the spaces between the ridges are called valleys. It is through the pattern of these ridges and valleys that a unique fingerprint is matched for verification and authorization.

Figure1: Authentication for ATM



These unique fingerprint traits are termed “minutiae” and comparisons are made based on these traits . On average, a typical live scan produces 40 “minutiae” [2].

There are five stages involved in finger-scan verification and identification. Fingerprint (FP) image acquisition, image processing, and location of distinctive characteristics, template creation and template matching. A scanner takes a mathematical snapshot of a user's unique biological traits. This snapshot is saved in a fingerprint database as a minutiae file. The first challenge facing a finger-

scanning system is to acquire high-quality image of a fingerprint[3][4]. The standard for forensic-quality fingerprinting is images of 500 dots per inch (DPI) [5].

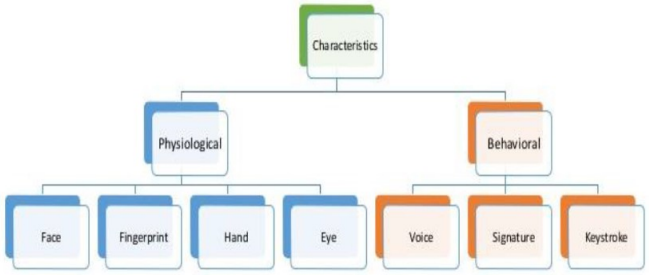


Figure 2 : Methods of Identification System

II. FINGERPRINT AUTHENTICATION

The fingerprint authentication problem can be grouped into two sub-domains. One is fingerprint verification and the other is fingerprint identification (Figure 1.3). In addition [6], different from the manual approach for fingerprint authentication by experts, the fingerprint authentication here is referred as FAA (Fingerprint Authentication in ATM), which is program based [7].

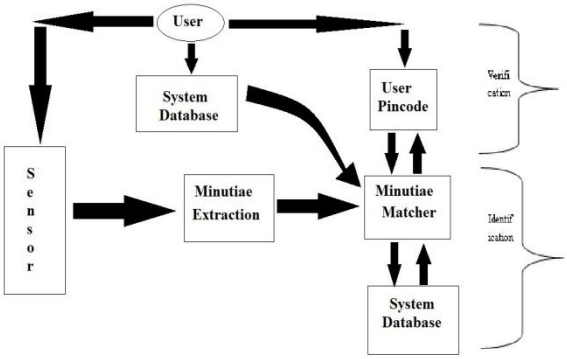


Figure 3 : Verification vs. Identification

Fingerprint verification is to verify the authenticity of one person by his fingerprint. The user provides his fingerprint together with his identity information like his PIN-CODE [8]. The fingerprint verification system retrieves the fingerprint template according to the PIN-CODE and matches the template with the real time acquired fingerprint from the user. Usually it is the underlying design principle of AFAS (Automatic Fingerprint Authentication System). Fingerprint identification is to specify one person's identity by his fingerprint(s). Without knowledge of the person's identity, the fingerprint identification system tries to match his fingerprint(s) with those in the whole fingerprint database[9]. It is especially useful for criminal investigation cases. And it is the design principle of AFIS (Automatic Fingerprint Identification System). However, all fingerprint recognition problems, either verification or identification, are ultimately based on a well-defined representation of a fingerprint[10].

A. ADVANTAGES AND DISADVANTAGES

ADVANTAGES

1. It is the most economical biometric PC user authentication technique.
2. It is one of the most developed biometrics.
3. Easy to use.
4. Small storage space required for the biometric template, reducing the size of the database memory required.
5. It is standardized.
6. Replace traditional methods (PINs)

DISADVANTAGES

1. Misidentification
2. False Acceptance
3. False Rejection
4. Limitations for individual
5. Dry, wet or dirty hands.
6. For some people it is very intrusive, because it is still related to criminal identification

III. IMAGE PROCESSING

Image processing is the process of converting the finger image into a usable format. This results in a series of thick black ridges (the raised part of the fingerprint) contrasted to white valleys. At this stage, image features are detected and enhanced for verification against the stored minutia file [11]. Image enhancement is used to reduce any distortion of the fingerprint caused by dirt, cuts, scars, sweat

and dry skin. The next stage in the fingerprint process is to locate distinctive characteristics. There is a good deal of information on the average fingerprint and this information tends to remain stable throughout one's life [12].

Most fingerprints have a core, a central point around which swirls, loops, or arches are curved. These ridges and valleys are characterized by irregularities known as minutiae, the distinctive feature upon which finger-scanning technologies are based. A typical finger-scan may produce between 15 and 20 minutiae [13].

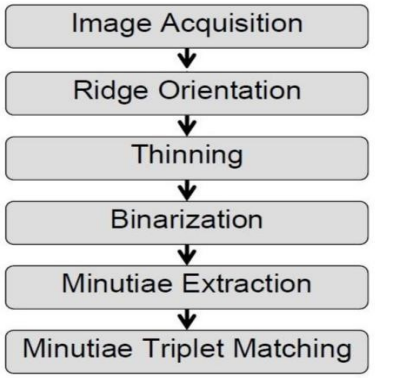


Figure 4 : Steps of fingerprint recognition

A template is then created. This is accomplished by mapping minutiae and filtering out distortions and false minutiae. The tricky part is comparing an enrolment template to a verification template. Positions of a minutia point may change by a few pixels, some minutiae will differ from the enrolment template. Many finger-scan systems use a smaller portion of the scanned image for matching purposes [14].

A. DEVICE DESCRIPTION:

Sensor: A Sensor is a Device, Modules or Subsystem whose purpose is to detect physical property and records or otherwise respond to it. Send information to other electronic, frequently a computer processor[15].

Pre-processor: It is a program that processes its **input data to produce output** that is used as input to another program [16].

Feature Extraction: Its starts from an **initial set** of measured **data** and builds derived values intended to be informative [17].

Template Generator: It's a **tool** used for **developing websites, email and document** template without manually formatting, writing computer **programming language** code.

Enrolment: It is the process of **entering and verifying data** to register in the particular site [18].

Database: It is an **collection of data**. A relation database more restrictively is a collection of schemas, tables, queries

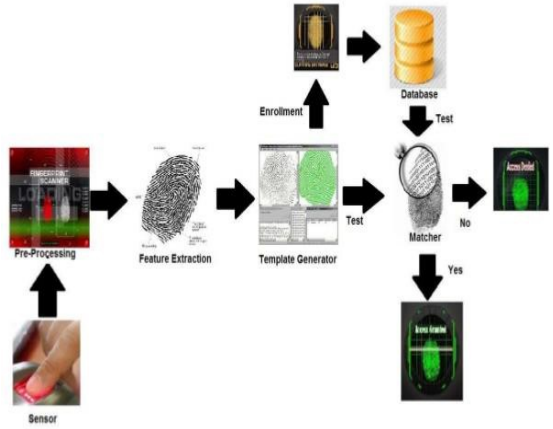


Figure 5 : Procedure of Image processing

B. APPROACHES FOR FINGERPRINT RECOGNITION:

Two representation forms for fingerprints separate the two approaches for fingerprint recognition.

1. **Minutia - based:** The first approach, which is minutia-based, represents the fingerprint by its local features, like terminations and bifurcations. This approach has been intensively studied, also is the backbone of the current available fingerprint recognition products. We also concentrate on this approach in our project [19].

2. **Image-based:** The second approach, which uses image-based methods, tries to do matching based on the global features of a whole fingerprint

image. It is an advanced and newly emerging method for fingerprint recognition. And it is useful to solve some intractable problems of the first approach. But our project does not aim at this method, so further study in this direction is not expanded in our work [20][21].

C. METHODOLOGY

An embedded system is a combination of software and hardware to perform a dedicated task. Some of the main devices used in embedded products are microprocessors and microcontrollers. Fingerprint based ATM cashbox accessing system using PIC microcontroller is implemented. Microcontroller forms the controlling module and it is the heart of the device. Initially we store the fingerprint of bank manager and that will be verified with the fingerprint that we are giving when the time of authentication.

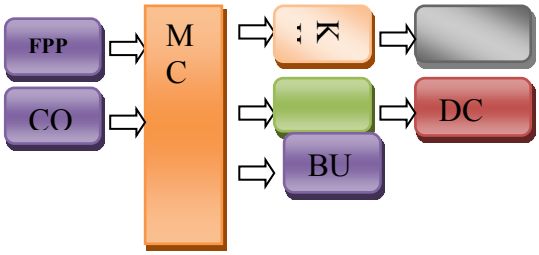


Figure 6 : Block diagram of fingerprint based ATM

If both the fingerprints are matched then ATM cashbox will open, otherwise buzzer will give alarm. Fingerprint based ATM cashbox accessing system using PIC microcontroller is implemented. Microcontroller forms the controlling module and it is the heart of the device. Initially we store the fingerprint of bank manager and that will be verified with the fingerprint that we are giving when the time of authentication. If both the fingerprints are matched then ATM cashbox will open, otherwise buzzer will give alarm.

BLOCK DIAGRAM OF METHOLOGY

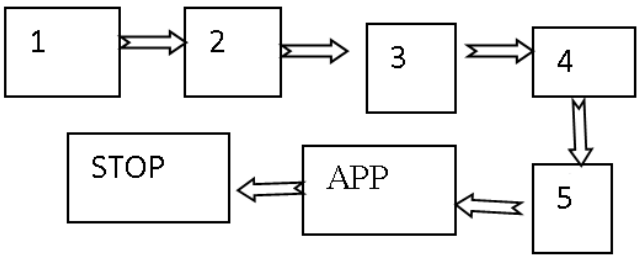


Figure 7 : Block Diagram of Mythology

1. FEASIBLE STUDY

The essence of this project is taken from various books and journals based on various integrity and security check systems. Various PDF were downloaded via Internet and references.

Subject related to the interface study has been done by understanding the .Net, Matlab and SQL server environment and studying the language use to code the logic from the references.

2 .TARGET

Target of our project is to providing an addition of sophisticated level of security and integrity to the user performing transactions through traditional ATM Systems.

3. STEP-BY-STEP DESIGNING

In this project following steps are taken for the designing of the system:

a. A biometric sensor performs scanning of the fingerprint of intended user.

b. Minutiae algorithm performs matching of that image with the images stored in database.

c. Generating matlab data with the help of

MATLAB.

d. Creating database for the storage of data.

e. Developing interface as a connecting medium of the user & machine.

f. Fetching required information needed for proper security check from user side.

4 .TESTING

The following steps are performed during testing the whole system:

a. Performing unit testing.

b. Creating test cases for integrity testing and whole system testing.

IV. RESULT

The result is being measured by comparing the security components of the ATM system or by matching the PIN-Code and the fingerprint pattern matching which decide the end result of the system.

The fingerprint based ATM authentication system is designed such that the door access can be controlled using fingerprint authentication. The status of the door access is displayed on the LCD. The schematic depicts the interfacing of each component with microcontroller and input output modules. The schematic depicts the interfacing of each component with microcontroller and input output modules. The manager can access the vault based on the fingerprint authentication. His fingerprint is previously stored in fingerprint module. When the manager tries to access it for the next time to store the money in ATM his fingerprint will be checked for verification. If the fingerprint matches with the initially stored data, then cashbox is opened. Otherwise the system denies the operation by producing a buzzer on the alarm. The system consists of finger print module, DC motor, LCD display. These are interfaced to the PIC microcontroller.

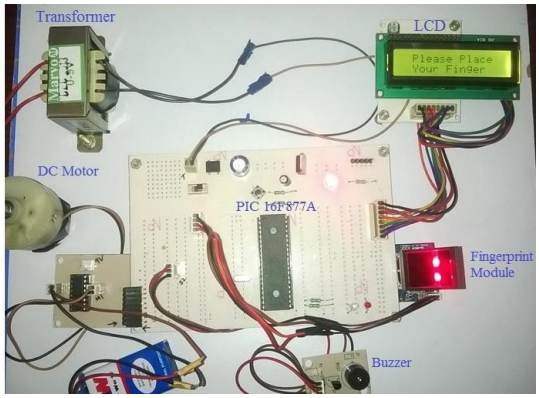


Figure 8 Experimental setup of fingerprint based ATM

When a user registers his fingerprint to the finger print module, this is fed as input to the microcontroller. The micro controller is programmed in such a way that the input from the user is checked compared with user database and displays the relevant information on the LCD display. When a authorized person is recognized using finger print module the door is accessed using DC motor.

V. CONCLUSION

Finger-scan technology is being used throughout the world and provides an able solution. In the present days it is being used for computer network access and entry devices for building door locks. Fingerprint readers are being used by banks for ATM authorization and are becoming more common at grocery stores where they are utilized to automatically recognize a registered customer and bill their credit card or debit account. Finger-scanning technology is being

used in a novel way at some places where cafeteria purchases are supported by a federal subsidized meal program. The system can be extended using a GSM module. The GSM module sends alert messages to the respective authorities when unauthorized person`s finger print is detected.

VI. REFERENCES

[1]. Fukuoka M, Yano S, Giaccone G, Tamura T, Nakagawa K, Douillard JY, Nishiwaki Y, Vansteenkiste J, Kudoh S, Rischin D and Eek R. Multi-institutional randomized phase II trial of gefitinib for previously treated patients with advanced non–small-cell lung cancer. Journal of Clinical Oncology, 2003; 21(12): 2237-2246.

[2]. Pretreatment Evaluation of Non–Small-cell Lung Cancer, American Journal of Respiratory and Critical Care Medicine, Vol. 156, No. 1 (1997), pp. 320-332.

[3]. Halpern MT, Gillespie BW and Warner KE. Patterns of absolute risk of lung cancer mortality in former smokers. Journal of the National Cancer Institute, 1993; 85(6): 457-464.

[4]. Mohammed AA, Hussein JA., Hybrid transform coding scheme for medical image application. In IEEE ISSPIT 10', 2010; 237-240.

[5]. Zhang SQ, Zhang SF, Wang XN, Wang Y. The Image Compression Method Based on Adaptive Segment and Adaptive Quantified. In IEEE 3rd ICICIC'08, 2008; 353-353.

[6]. Xie Y, Jing X, Sun S, Hong L. A fast and low complicated image compression algorithm for predictor of JPEG-LS. In IEEE IC-NIDC, 2009; 353-356.

[7]. Roy AB, Dey D, Mohanty B and Banerjee D. Comparison of FFT, DCT, DWT, WHT Compression Techniques on Electro cardiogram & Photo plethysmography Signals, AnamitraBardhan Roy -Special Issue of International Journal of Computer Applications (0975 – 8887) International Conference on Computing, Communication and Sensor Network (CCSN) 2012.

[8]. Mridul Kumar Mathur, GunjanMathur, Image Compression using DFT through Fast Fourier Transform Technique, International Journal of Emerging Trends & Technology in Computer Science (IJETTCS), volume 1, Issue 2, July – August 2012.

[9]. Walaa M. Abd-Elhafiez, WajebGharibi, Color Image Compression Algorithm Based on DCT Blocks, International Journal of Computer Science Issues, IJCSI, vol. 9, Issue 4, July 2012, pp. 323-328.

[10]. Singh H, Sharma S., Hybrid Image Compression Using DWT, DCT & Huffman Encoding Techniques. International Journal of Emerging Technology and Advanced Engineering, 2012; 2(10): 300-306.

[11]. Anoop Mathew and Bensiker Raja Singh D, ―Image Compression using Lifting based DWT‖, International Journal of computers, Information Technology and Engineering, Jan-June 2009.

[12]. Elharar.E, Adrian Stern, OferHadar,"A Hybrid Compression Method for Integral Images Using Discrete Wavelet Transform and Discrete Cosine Transform", Member, IEEE, and BahramJavidi, Fellow, IEEE.

[13]. Sriram. B, Thiyagarajans. S, ―Hybrid Transformation technique for image compression,Journal of theoretical and applied information technology, 31st July 2012 Vol. 41 No.2.

[14]. Harjeet pal singh, Sakhi Sharma, Hybrid Image Compression Using DWT, DCT & Huffman Encoding Techniques International Journal of Emerging Technology and Advanced Engineering, (ISSN 2250-2459, Volume 2, Issue 10, October 2012.

[15]. Dr.T.Karthikeyan, C.Thirumoorthi, "A Survey on Embedded Zero Tree Wavelet", International Journal of Computer Science (IJCS), ISSN: 2348-6600, Vol.2, Issue 2, No: 3, Ref-ID: IJCS-061, Page No: 353-357, October- 2014.

[16]. Dr.T. Karthikeyan, C.Thirumoorthi ,"Easy Optimization of Image Transformation using sFFT Algorithm with HALIDE Language", in International IEEE Conference on "Contemporary Computing and Informatics (IC3I 2014)" published in IEEE xplore, Pages : 1188 - 1190 (2014), ISSN: 978-1-4799-6629-5/14, November 2014.

[17]. Dr.T. Karthikeyan, C.Thirumoorthi, "Embedded zero tree Wavelet (EZW) Algorithm based Image Transformation for Easy Optimization with

HALIDE Language", International Journal of Applied Engineering Research (IJAER), ISSN 0973-4562 ,Vol. 10, No.55, pp. 1551-1554, June 2015.

[18]. Dr.T. Karthikeyan, C.Thirumoorthi, "Medical image compression technique with transform method for lung cancer CT scan image: A Review", in International Journal of control Theory and Applications (IJCT) (ISSN 0974-5572), International science press, Serials publications, volume 9, issue 26, pp 193-200, August 2016.

[19]. Dr.T. Karthikeyan, C.Thirumoorthi, "A novel approach on discrete cosine transform based image compression technique for lung cancer", Biosciences Biotechnology Research Asia (BBRA), Vol. 13, issue 3, page no: 1679-1688, September 2016.

[20]. Dr.T. Karthikeyan, C.Thirumoorthi, "A hybrid medical image compression techniques for lung cancer", Indian Journal of Science and Technology (IJST) (ISSN (Print):0974-6846 ISSN (Online):0974-5645), Volume 9, Issue 39, pp 1-6, October 2016.

[21]. Dr.T. Karthikeyan, C.Thirumoorthi, "A study on discrete wavelet transform compression algorithm for medical images", in Biomedical Research, Allied Academies Journals (ISSN 0970-938X (print) 0976-1683 (Electronic)), volume 28 , issue 4 , page no 1574-1580, February 2017.