



International Journal of Emerging Technologies in Computational and Applied Sciences (IJETCAS)

www.iasir.net

Biometric Fingerprint identification system for curtailing the masqueraded accesses: A framework approach

¹Syed Mohsin Saif*, ²Mudasir Manzoor Kirmani, ³Ziema Mushtaq

^{1,2}Research Scholar, Dept. of CS & IT,

School of Computer Science and Information Technology,
Maulana Azad National Urdu University, (Central University)
Hyderabad, India, 500 032, Hyderabad, INDIA.

³Department of Computer Science, University of Kashmir,
Hazratbal, Srinagar, Jammu and Kashmir 190006 INDIA.

Abstract: Recognition, identification and verification are the main building blocks of any biometric security system. Security is considered at par to any other services rendered to run any organization public or private, small or big. It is the organizational data and other patterns which make organizations to withstand their fame, serviceability, reputation etc. there is no doubt that biometric systems have gained popularity by providing well versed security fabrication to ensure perfect and efficient processing required at different algorithmic stages.

Biometric system is essentially a pattern recognition system which recognizes a person by determining the authenticity of a specific physiological (e.g., fingerprints, face, retina, iris, palm geometry) or behavioral (e.g., gait, signature, voice) characteristic possessed by that person. Among all the presently employed biometric techniques, fingerprint identification systems have received the most attention due to the long history, reliable nature, universality, uniqueness and acceptability biometric characteristic as it is unique and persistence. Fingerprint is the pattern of ridges and valleys on the surface of fingertip. However, recognizing fingerprints in poor quality images is still a very complex job, so the fingerprint image must be preprocessed before matching. A framework to deal with the fingerprints with acquired deformity like noise so as to have minimum false acceptance ration.

Keywords: Biometrics, fingerprint, noise, recognition and identification

I. Introduction

As security is continuing to be the main and most prominent and challenging domain to be taken care of, after every single moment in time new techniques and strategies are being made by, malicious users, criminal, amateur hackers and professional hackers. For any organization whether public or private, small or big information matters at par to other subsidiary installations. To ensure security at all the levels like personal security, system security, application security and message security biometrics has proved out to be more powerful and efficient in comparison to traditional token and knowledge based systems.

A wide variety of systems requires reliable personal recognition schemes to either confirm or determine the identity of an individual requesting their services. The purpose of such schemes is to ensure that the rendered services are accessed only by a legitimate user and no one else. To achieve this motive biometrics is believed to be the unique and universal approach for automatic individual identification [1]. Biometrics has played a vital and evolutionary role to counter these challenges to ensure the varsity of the system in smooth and secure way. Since the dawn of the biometrics, threats like modification, fabrication, interception and interruption of the valuable assets showed positive declination. Biometric technologies are becoming the foundation of the extensive array of highly secure identification and personal verification solutions. Physiological characteristics include fingerprint, face recognition, hand geometry, iris, palm, vascular pattern etc. Behavioral characteristics are the traits that are learned or acquired like dynamic signature verification, speaker verification, gait, key stroke dynamics etc. [2].

II. Biometric Modalities

A biometric modality refers to a system built to recognize a particular biometric trait [3]. Face, fingerprint, hand geometry, palm print, iris, voice, signature, gait, and keystroke dynamics are examples of biometric traits [4]. In the context of a given system and application, the presentation of a user's biometric feature involves both biological and behavioral aspects. Many of the issues associated with biometric systems are not modality-specific, although of course the choice of modality has implications for system design and, potentially, system performance

- a. **Face Recognition:** a digital video camera image is used to analyze facial characteristics such as the distance between eyes, mouth or nose. These measurements are stored in a database and used to

compare with a subject standing before a camera [5]. Facial-scan technology is based on the standard biometric sequence of image acquisition, image processing, distinctive characteristic location, template creation, and matching [6]. An optimal image is captured through a high resolution camera, with moderate lighting and users directly facing a camera [6].

- b. **Fingerprints:** the patterns of ridges and valleys on the “friction ridge” surfaces of fingers have been used in forensic applications for over a century. Friction ridges are formed in utero during fetal development, and even identical twins do not have the same fingerprints. A fingerprint usually appears as a series of dark lines that represent the high, peaking portion of the friction ridge skin, while the valleys between these ridges appears as white and are the low, shallow portion of the friction ridge skin.
- c. **Iris:** a circular colored membrane surrounding the eye’s pupil. The outer side of iris is surrounded by the sclera (white of the eye), is complex as well as distinctive enough to be useful for personal recognition. The visual texture of the iris initiates its prominence since fetal development and continues till 2 years to make it stable [7]. It is almost impossible to tamper the texture of the iris surgically and even the artificial iris can be traced out efficiently.
- d. **Hand Geometry:** refers to the shape of the human hand, size of the palm, and the lengths and widths of the fingers.
- e. **Vein Geometry:** a person's veins are completely unique. A person's veins differ between their left and right sides. To use a vein recognition system, we simply place our finger, wrist, palm or the back of our hand on or near the scanner. A digital picture is taken using near-infrared light. The hemoglobin in the blood absorbs the light, and hence veins appear black in the picture
- f. **Retinal Scan:** is based on the blood vessel pattern in the retina of the eye. The principle behind the technology is that the blood vessels at the retina provide a unique pattern, which may be used as a tamper-proof personal identifier [8]. Since infrared energy is absorbed faster by blood vessels in the retina than by surrounding tissue, it is used to illuminate the eye retina.
- g. **Palm Print:** combine some of the features of fingerprints and hand geometry. Human palms contain ridges and valleys, like fingerprints, but are much larger, necessitating larger image capture or scanning hardware.
- h. **Voice:** directly combines biological and behavioral characteristics. The sound an individual makes when speaking is based on physical aspects of the body (mouth, nose, lips, vocal cords, and so on) and can be affected by age, emotional state, native language, and medical conditions.
- i. **Signature:** person signs his or her name typically changes over time. It can also be strongly influenced by context, including physical conditions and the emotional state of the signer.
- j. **Gait:** the manner in which a person walks, has potential for human recognition at a distance and potentially, over an extended period of time.

III. Fingerprint Identification

Fingerprints are the patterns formed on the epidermis of the fingertip. A fingerprint usually appears as a series of dark lines that represent the high, peaking portion of the friction ridge skin, while the valleys between these ridges appears as white space. and are the low, shallow portion of the friction ridge skin.. Fingerprints are made up of series of ridges and valleys (also called as furrows) on the surface of the fingertip and have core around which pattern like swirls, loops or arches are curved to ensure that each print is unique [9]. Fingerprint is composed of ridges and valleys. The interleaved pattern of ridges and valleys are the most evident structural characteristic of a fingerprint. The ridges are the single curved segment and valleys are the region between two ridges. The most commonly used fingerprint features are minutiae. Minutiae are the discontinuities in local ridge structure. They are used by forensic experts to match two fingerprints. There are about 150 different types of minutiae [10]. Among these minutiae types “ridge ending” and “ridge bifurcation” are the most commonly used as all the other types of minutiae are combinations of ridge endings and ridge bifurcations. A ridge ending is defined as the ridge point where a ridge ends abruptly [9]. A ridge bifurcation is defined as the ridge point where a ridge forks or diverges into branch ridges [9].

A popular way to categorize biometric recognition/verification system can be grouped into horizontal and vertical categorization. In horizontal categorization the applications which share some similarities in features they require from the fingerprint recognition system. In vertical categorization the applicable application are designed some the bases of particular industrial perspective [11]. Horizontal: Physical access control, Logical access control, Transaction authentication, Device access control, Time and attendance, Civil identification, Forensic identification, Vertical categorization: Health care, Financial, Gaming and hospitality (casinos, hotels, etc), Education, Retail, High technology and telecommunications, Federal, state, municipal, or other governments, Military, Law enforcement, Surveillance. Frequently, ridges and valleys go in parallel but sometimes they bifurcate or terminate. Bifurcation is present when the ridge suddenly split into two ridges and termination exist when the ridge abruptly stop. In fact, bifurcation and termination represent some of important

minutiae points. Minutiae mean small details that can determine important local features in the fingerprint. The most common minutiae types are the following and shown in figure 1 and 2 respectively [11].

- Termination
- Bifurcation
- Lake
- Independent ridge
- Point or island
- Spur
- Crossover



Figure 1

Minutia	Meaning
	Termination
	Bifurcation
	Lake
	Independent ridge
	Point or island
	Spur
	Crossover

Figure 2

As far as the application of biometric fingerprint recognition in forensics is concerned, it can be used to perform Corpse Identification, Criminal investigation and even can render its practices to get Missing children's back to their parents. Biometric Fingerprint identification is believed to be one of the most popular and publicized security techniques. Because of their uniqueness and consistency over time, fingerprints have been used for identification for over a century, more recently becoming automated (i.e. a biometric) due to advancements in computing capabilities. Due to this popularity and ease of use fingerprint identification is one of most widely accepted biometric technique to filter the access and aid the recognition system to maintain the efficiency in serving security domains of both public and corporate world. Fingerprint authentication has revolutionized the e-commerce, because it ensures the trusted authentication of the dealing business parties. All the 75% e-commerce users, who were worried about the security and privacy of transmitting their credit card data via internet [12, 13] have breathed calmly because fingerprint authentication has facilitated the trusted e-commerce technology [14]. Fingerprint systems have good response time when compared with AIFS to match the candidate fingerprint [14].

IV. Fingerprint Matching

The two main categories of fingerprint matching techniques are minutiae-based matching and pattern matching. Pattern matching simply compares two images to see how similar they are [16]. Pattern matching is usually used in fingerprint systems to detect duplicates. The most widely used recognition technique, minutiae-based matching relies on behavior of the ridges like termination, bifurcation, dots or even smooth flow, which forms minutiae of the fingerprint, are fundamental constructors for any biometric fingerprint authentication system. In addition to these there are other distinct, but rudimentary morphological ridge behaviors like dots (very small ridges); islands (ridges slightly longer than dots); ponds or lakes (space between two temporary divergent ridges); spurs (a notch protruding from a ridge); bridge (small ridge joining two longer adjacent ridges); crossover (two ridges that cross across each other) as shown in Figure 2 [15].

V. Proposed Framework

The original image is subjected to undergo pre-processing, minutiae extraction and post-processing stages to obtain, the best possible minutiae with less or no spurious minutiae. The obtained reference template is then stored in the database for identification purpose. The Algorithm for performing these operations is shown below in Figure 3.

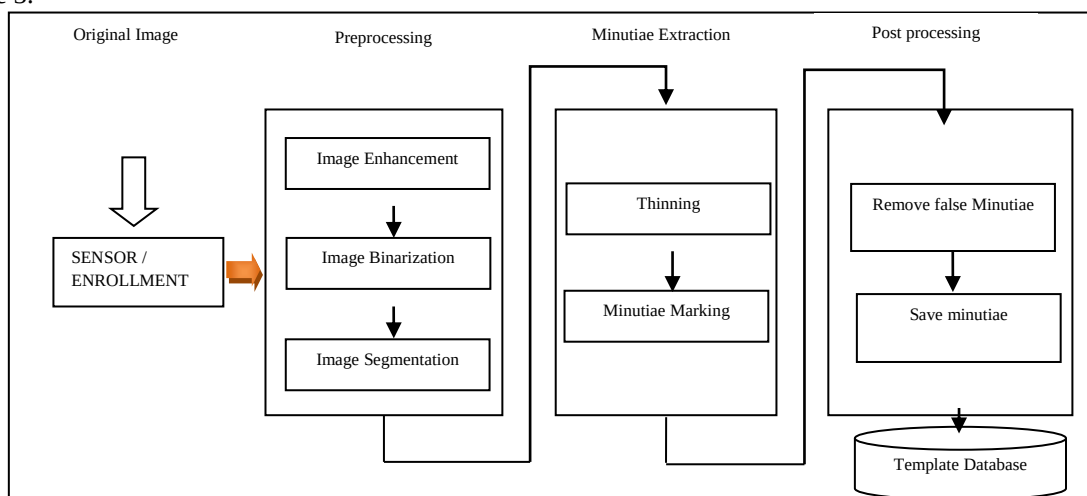


Figure 3: Modular Diagram for Enrollment of an Ideal Image

In real time, the image acquired is not of good quality to perform accurate identification, as the images are prone to noise. The fingerprint images obtained from the sensors are treated with noise reduction filtering and edge detection in addition to enhancement operations performed on original image to obtain the best possible minutiae. The algorithm for study to eliminate the noise effects from the corrupted image is represented diagrammatically in Figure 4 below;

The filtered image obtained is further subjected to undergo various edge detection techniques to obtain the accurate and perfect minutiae.

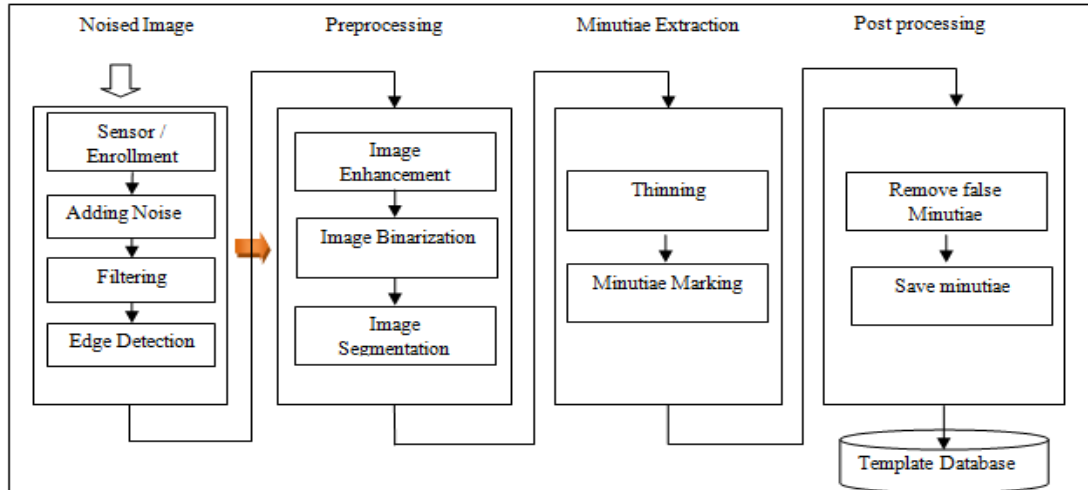


Figure 4: Modular Diagram for Enrollment of a Noisy Image

The important phase of my study to analyze the effectiveness of the proposed system is achieved by performing minutiae matching; the flow of the algorithm performed to do the operation is shown below in Figure 5.

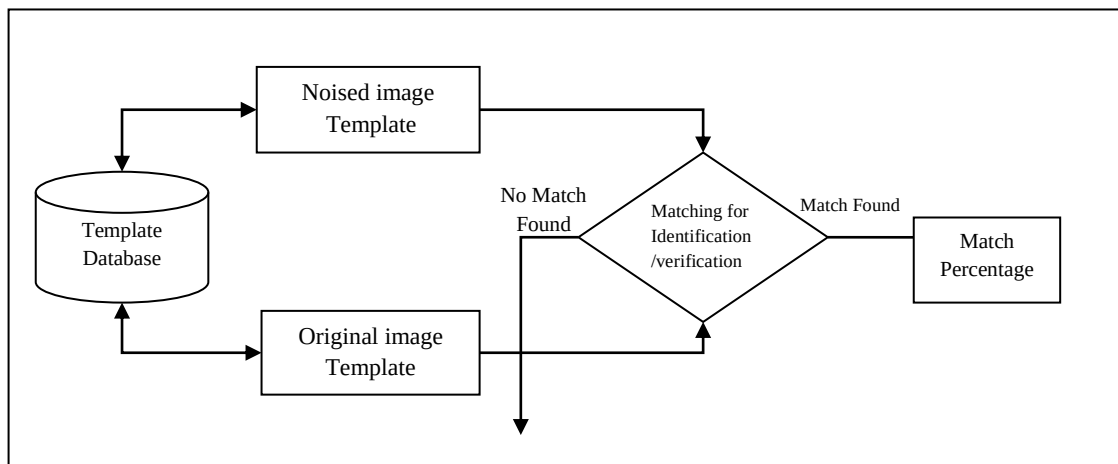


Figure 5: Modular Diagram for Verification / Identification of Fingerprint

VI. Results And Conclusion

The proposed system is implemented using MATLAB 7.8(R2009a) and the fingerprint sample images were obtained from online biometric database (CASIA Fingerprint Image Database for testing version 1.0", <http://biometrics.idealtest.org>)[17]. To evaluate the proposed framework fingerprint images were treated with all the stages of the algorithm as specified in the finger 3 and 4. After the preprocessing and post processing of the fingerprint, the obtained minutiae were subjected for matching process to find the accuracy of the algorithmic framework. It was found that the framework showed better matching percentage. The false and spurious minutiae were efficiently eliminated. The other conditions which usually are being faced by the biometric fingerprint system is the condition of sensors and other environmental parameters. These situations were simulated using in build MATLAB function to find the counter measures to reduce false acceptance ratio. Biometrics have played a grave role in setting and establishing most versatile modalities to ensure both recognition and identification of any individual who so ever claims for accessibility into the restricted corridors of sensitive databases. The performance of a fingerprint feature extraction and matching algorithms heavily depends upon the quality of the input fingerprint image. The behavior of the deformity on the fingerprint can either have additive, multiplicative or random effects on the overall image matrix. An efficient framework to

deal and negotiate the impacts of these deformities on the biometric system is proposed. Minimum false acceptance ratio can be achieved. Simultaneously better public acceptance can be obtained. The proposed framework is not end to miles but in deed needs to consider multimodal biometric system so that the dynamic biometric security system can be established.

VII. References

- [1]. Salil P *et al.*, "Biometric Recognition: sensor characteristics and image Quality", *IEEE Instrumentation & Measurement Magazine*, June 2011.
- [2]. "Biometrics History", *National Science and Technology council(NSTC) , Committee on technology, Committee on Home land and national security*, Campell J, "Speaker recognition: A tutorial", *Proceedings of IEEE*, vol.85 (9), 1437-1462, 1997.
- [3]. Nalwa V, "Automatic on-line signature verification", *Proceedings of IEEE*, vol.85 (2), 213-239, 1997.
- [4]. Manoj G, "Biometric Technologies Overview", *SANS Reading Room*, <http://rr.sans.org/authentic/biometric2.php>.
- [5]. Samir N, "Biometrics: Identity Verification in a Networked World, New York", *Wiley and Sons, Inc*, 65-75, (2002).
- [6]. Salil P *et al.*, "Biometric Recognition: sensor characteristics and image Quality", *IEEE Instrumentation & Measurement Magazine*, June 2011.
- [7]. Julian A, "Biometrics: Advanced Identity Verification, London:", *Springer-Verlag*, 2002.
- [8]. Subcommittee on Biometrics., www.biometrics.gov , 2006
- [9]. Ishpreet Singh Virk and Raman Maini, "Fingerprint Image Enhancement and Minutiae Matching in Fingerprint Verification", *Journal of Computing Technologies*, vol. 1, June 2012.
- [10]. L. Hong, Y. Wan and A. Jain, "Fingerprint Image Enhancement: Algorithm and Performance Evaluation", *IEEE Pattern Analysis and Machine Intelligence*, vol. 20, No. 8, pp. 777-787, 1998.
- [11]. David M *et al.*, "Handbook of Fingerprint Recognition", *second edition, Springer*, 2009.
- [12]. Fingerprint Recognition, *BioEnable Technologies Pvt. Ltd., E-204, 3rd floor, Railway Station Complex, CBD Belapur, Navi Mumbai, MH, India*, 2005
- [13]. Fingerprint Recognition, *BioEnable Technologies Pvt. Ltd., E-204, 3rd floor, Railway Station Complex, CBD Belapur, Navi Mumbai, MH, India*, 2005
- [14]. John R, "Electronic Commerce", *Charles River Media, 4th edition*, 2003.
- [15]. John R, "Net Privacy: A Guide to Developing and Implementing an Ironclad eBusiness Privacy Plan", *McGraw-Hill*, 2001.
- [16]. Atul S. Chaudhari *et al.* "Implementation of Minutiae Based Fingerprint Identification System using Crossing Number Concept", *Journal of Computer Trends and Technology (IJCTT) – volume 8 number 4– Feb 2014*
- [17]. CASIA Fingerprint Image Database for testing version 1.0", <http://biometrics.idealtest.org>.