Asian Journal of Computer Science and Technology
ISSN: 2249-0701 Vol.8 No.S1, 2019, pp. 4-6

A Review on Biometrics Authentication System Using Fingerprint

P. Sureshbabu[1] and M. Sakthivadivu[2]
[1]Associate Professor & Head, [2]Assistant Professor
[1&2]Department of Computer Science, Bharathidasan College of Arts & Science, Tamil Nadu, India
E-Mail: ptsuresh77@gmail.com, kaushalsakthi@gmail.com

Abstract **- Technology based on Biometric identification and verification is one leading research area. It deals with the concept analyzing the human body characteristics through Biometric devices for various authentications process. There are many Biometric authentication systems are available for verification process. This paper discusses the role of Fingerprint authentication. FP recognition is highly used biometric technique, because of abundance sources (i.e. ten fingers) availability for collecting data. Discussion on Fingerprint matching techniques, recognition methods and their performance analysis are made in the paper.**
Keywords: **Authentication, Biometric, Fingerprint (FP), Patterns.**

I. INTRODUCTION TO BIOMETRIC

"Biometrics" is a word which derived from Greek words *bio* and *metrics* which gives the meaning "life" and "measure" respectively. Automatic biometric method is available over the last few decades, because of major break troughs in the field of computer processing. A biometric system contains mostly depends an image capturing concept, a feature extraction module and a pattern matching module as revealed in Fig.1. Image capturing systems get the unprocessed biometric data of a person using a sensor.
Making use of appropriate algorithm's quality of the captured image improved. Database stores the biometric pattern information of Humans. Pattern matching concept evaluates the extracted features with the stored data, which in-turn produce match attain level [1].

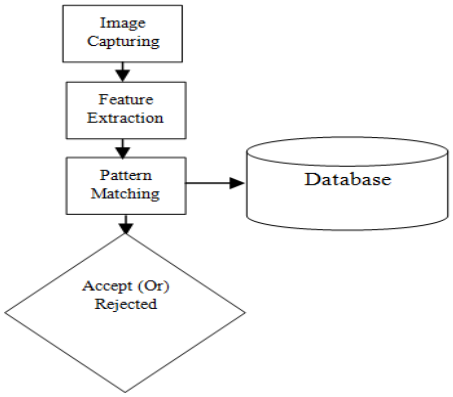

Fig.1 Biometric Method

A. Biometric History over the Period of Time

Biometrics has provided a sizeable solution to business community who are facing issues like undocumented access, ID swapping, manual symbol checks, credential replacements and more. There has been much advancement in biometrics environment, which makes reliable security and costs cutting in safety measures. Biometrics has good authentication operation that has numerous advantages over customary way and now they are offered at lesser costs.

B. Benefits of Biometrics

The benefits of a Biometric Authentication are numerous. Various benefits are

1. Accurate Identification
2. Accountability
3. Easy and Safe for Use
4. Time Saving
5. User Friendly Systems
6. Security

C. Fingerprint Biometric Concept

Fingerprint Biometric is the frequently used traditional method which is internationally accepted as lawful technique to recognize a person. Fingerprint is the impressions of the tiny ridge (dermal) of the finger. Fingerprint ridges and valleys are unique and unalterable. Fingerprint biometric is used in numerous applications that comprise of various applications like military, law enforcement, medicine, education, civil service, forensics, driver license registration, Mobile Phone access [2], [3], System log-in process and like [4]. Nowadays live Fingerprint readers based on optical, ultrasonic methods and etc are used in place of traditional method of ink to capture Fingerprint. It is a identification system based on minutiae or location and direction of the ridge endings and bifurcations (splits) along a ridge path. The two commonly used Fingerprint matching techniques are minutiae-based matching and pattern matching.

Pattern matching just compares two image for checking similarity. Minutiae matching relies on minutiae points i.e. location and direction of each point. The pre-requisite to match the Fingerprint is classification. The classification is treated as course level matching. The Fingerprint can be classified as whorl, right loop, arch, tented arch. In order to ensure the performance of Fingerprint identification, enhancement algorithms are needed to improve clarity of input fingerprint images. The usual Fingerprint patterns are shown in Fig. 2 and Fig. 3.

TABLE I BIOMETRIC HISTORY OVER THE PERIOD OF TIME -

1858 – First systematic capture of hand images for identification purposes was recorded
1936 – Concept of using the iris pattern for identification was proposed
1960 – Face recognition becomes semi-automated
1965 – Automated signature recognition research begins
1974 – First commercial hand geometry systems become available
1992 – Biometric Consortium is established within US Government
2010 – U.S. national security apparatus utilizes biometrics for terrorist identification
2013 – Apple includes fingerprint scanners into consumer target Smartphone's

Source – National Science and Technology Council (Nstc) Report

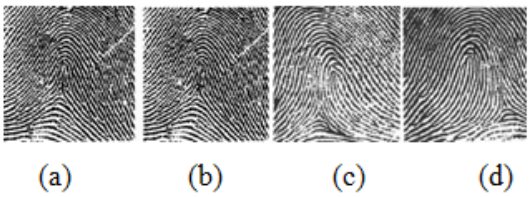

Fig. 2 (a) Plain Arch (b) Tented Arch (c) Ulnar loop (d) Radial loop

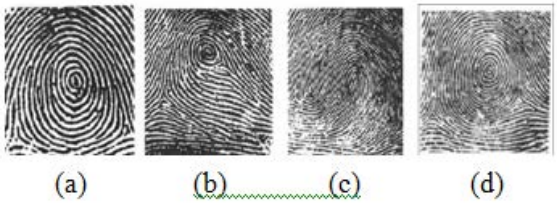

Fig. 3 (a) Plain whorl. (b) Central pocket loop whorl (c) Double loop (d) Accidental whorl

1. Plain Arch and Tented Arch

Plain Arch is a pattern that has ridges at one side, make a rise at the centre, and flow or tend to flow towards the opposite side as shown in Fig 2(a) and 2(b). Tented Arch has resemblance to plain arch but, ridges create an angle or a steep thrust. It possesses some basic characteristics of the loop as shown in Fig. 3. Radial Loops and Ulnar Loops: Ulnar loop pattern loops shown in Fig. 2(c) flow in the direction of little finger, while in Radial loop pattern shown in Fig. 2(d) loops flow in the direction of the thumbs.

2. Plain Whorl

Consists of pattern with two deltas and minimum one ridge will make a complete circuit of spiral, oval or any form of circle. The imaginary line drawn between two deltas will touch or cross, at least one recurving ridge within the inner pattern area as shown in Fig. 3(a). Central Pocket loop Whorl has a pattern with minimum one recurving ridge shown in Fig. 3(b) or an obstruction at right angles to the line of flow. The imaginary line drawn between two deltas will not cut or touch the inner recurving ridge in the inner pattern. Double Loop Whorl is distinguished with two separate loop formations. It is composed of two separate and distinct sets of shoulders and two deltas as shown in Fig 3(c). Accidental Whorl is the only pattern which is connected with minimum two deltas. It unites two or more distinctive type of patterns excluding the plain arch as shown in Fig. 3(d). The rest of the paper is organized as follows. Related work of Fingerprint is presented in Section II. Section III depicts Fingerprint biometric authentication system. Conclusion of this paper is discussed in Section IV.

II. FINGERPRINT BIOMETRIC RELATED WORKS

The latest improvements in biometrics identification of a person lead to reliability and accuracy in the authentication system. Fingerprint Recognition technologies examined with various parameters such as matching techniques, recognition methods, retrieval concepts, security, and weather conditions for image acquisition.

A. Matching Techniques and Recognition Methods

The Fingerprint matching performance is analyzed with FAR, FRR, EER (Equal Error Rate), GAR (Genuine Accept Rate). Zin Mar Win *et al.* [5] use a correlation based Fingerprint method. The method uses Gabor filters for Fingerprint feature extraction. The test results of low FAR, FRR and 97% accuracy are reported. Haiyun Xu *et al.* [6] design a system for improving matching speed by compressing spectral minutiae feature using Column PCA (Principal Component Analysis) and Line DFT (Line Discrete Fourier Transform) reduction techniques. De-Song Wang *et al.* [7] presented a Fingerprint based authentication system with Smartphone's. This scheme is better for computational complexity with Khan's and Yoon-Yoo's scheme.

B. Security Systems

Rajeswari Mukesh *et al.* [8] proposed visual threshold cryptographic method to keep compressed FP template information securely at the server to avoid hacking. Lossy compression technique DCT is used for compressing. The results prove FAR and FRR of 0.2% and better efficiency, reduces falsification and maintenance cost. Lifeng Lai *et al.* [9] designed a reusable biometric security systems, in which the same biometric information is reused in multiple locations is analyzed. Bon K. Sy [10] designed practical secure data retrieval and authentication techniques for complex distributed systems.

III. RECOGNITION OF FINGERPRINT BIOMETRIC SYSTEM

Usually inked Fingerprint impressions recorded on a fingerprint card are scanned and processed by an automated fingerprint identification system (AFIS). Though, the ink process is being swapped with live-scan technology that depends on a moving light source and the principle of frustrated total internal reflection [11].

Images impression got by the live-scan reader can be directly feed into an AFIS for subsequent processing. Various advantages of new technology over the AFIS are elimination of ink, finding the quality of image before recording, many copies of the single image can be obtained, and the instant creation of an electronic fingerprint image file.

Fingerprints Identification processed in two stage process. The first stage, classification, performs a coarse classification of fingerprints into one of five classes. The second stage performs matching of details present in each fingerprint image. This two stage process is required so that efficient queries against databases of up to 50 million sets of fingerprints can be performed. Filtering based on fingerprint pattern classification from one or more fingers accomplishes this. Fingerprints can easily be classified into one of five classes or types: arch, tented arch, left loop, right loop, and whorl. There are at least four major approaches to automatic Fingerprint classification. These are structural, syntactic, statistical and the artificial neural network (ANN) approach.

The second stage performs a search against the candidate fingerprints from the first stage using minutia. A minutiae is the point where a ridge either terminates or bifurcates into two or more ridges and is defined in terms of x and y coordinates, and ridge orientation angle. A fingerprint consists of ridges which are the raised portions of the skin and the valleys between the ridges. Diagrammatic representation of Biometrics Authentication System shown in the fig. 4.

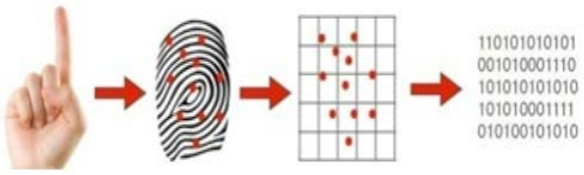

Fig. 4 Biometrics Authentication System

Due to the storage requirements of these uncompressed image files, they are generally not retained on-line. To reduce file size, the JPEG algorithm has been used to compress the fingerprint images. However, due to the 8x8 pixel tiling used in JPEG's DCT, blocking effects begin to appear as compression ratios exceed 8:1. A different approach, based on wavelet technology, was developed and adopted for use by the FBI. Rather than using an 8x8 pixel tile size, the wavelet scalar quantization (WSQ) algorithm globally compresses the image. This enables a compression ratio of 15:1 with minimal visual degradation in reconstructed images.

To date, fingerprints have been primarily used by law enforcement applications and for background clearances. With the availability of inexpensive live scanners, fingerprints are beginning to be applied to verification applications.

IV. CONCLUSION

This paper discussed the related works and performance of biometric fingerprint authentication. The review is made on a variety of issues related to biometric authentication systems are discussed. The want of safety and privacy concerns of biometric authentication has to be addressed. It is reviewed that automatic fingerprint recognition is the best candidate biometric technology for explosives security from an analysis of the requirements: security, usability, ruggedness, size, form factor, privacy and operational temperature range.

REFERENCES

[1] Y. J. Wang and K. N. Plataniotis, - "An analysis of random projection for changeable and privacy-preserving biometric verification", *IEEE Transactions on Systems, MAN and Cybernetics*, Vol. 40, No.5, pp. 1280-1293, Oct. 2010.

[2] R. Ribalda, G. G. de Rivera, Á. de Castro, and J. Garrido, - "A mobile biometric system on-token system for signing digital transactions, IEEE Security & Privacy", Vol.8, No. 2, pp. 13-19, March-April 2010

[3] M. Bishop and C. Irvine, - "New pathways in identity management", Vol. 8, No. 6, pp. 64-67, November /December 2010.

[4] S. Kumar and E. Walia, - "Analysis of various biometric techniques", *International Journal of Computer Science and Information Technologies*, Vol. 2, No. 4, pp. 1595-1597, January 2011.

[5] Z. M. Win and M. M. Sein, - "Fingerprint recognition system for low quality images", *In Proc, the SICE Annual Conference*, Waseda University, Tokyo, Japan, pp. 13-18, Sep 2011.

[6] H. Y. Xu, R. N. J. Veldhuis, T. A. M. Kevenaar, and T. A. H. M. Akkermans, - "A fast minutiae-based fingerprint recognition system", *IEEE Systems Journal*, Vol. 3, No. 4, Dec. 2009

[7] J. Luo, S. Z. Lin, J. Y. Ni, and M. Lei, - "An improved fingerprint recognition algorithm using EBFNN", Second *International Conference on Genetic and Evolutionary Computing*, pp. 504-507, IEEE, 2008.

[8] R. Mukesh and V. J. Subashini, - "Fingerprint based authentication system using threshold visual cryptographic technique", *IEEE-International Conference on Advances in Engineering, Science and Management*, Mar 30-31, pp. 16-19, 2012

[9] L. F. Lai, S. W. Ho, and H. V. Poor, "Privacy–security trade-offs in biometric security systems" - part II: multiple use case, *IEEE Transactions on Information Forensics and Security*, Vol. 6, No. 1, March 2011.

[10] B.K.Sy, Secure computation for biometric data security—application to speaker verification, *IEEE Systems Journal*, Vol. 3, No.4, December 2009.

[11] L.Gerhardt, D.Crockett, J.Attili, and A.Presler – "Fingerprint imagery using frustrated total internal reflection". *In Proc. of the 1986 International Carnahan Conference on Security Technology*, pages 251-255, 1986.