International Journal of Electrical, Electronics and Computer Engineering **3**(2): 61-66(2014)

ISSN No. (Online): 2277-2626

Fingerprint Recognition System: A Review

Ms. Ankita Kute* and Mr. Vivek Kumar**

**M. Tech. Scholar, Department of Computer Science and Engineering, LNCTS, Bhopal, (MP) India*

***Assistant Prof., Department of Computer Science and Engineering, LNCTS, Bhopal, (MP) India*

(Corresponding author: Ms. Ankita Kute)

(Received 05 July, 2014 Accepted 28 August, 2014)

ABSTRACT: The biometrics system is mainly focuses on fingerprint recognition and how this system would be implemented. If it is implemented in our laboratory, this system would authenticate or contradict the uniqueness of each individual endeavoring to gain access to the laboratory region with a given sum of precision. The main problem in using such particular scanner comes from the security functions Microsoft integrates. The signal caring of all the information from the fingerprint scan is encrypted, and the major challenge will come from deciphering these signals. An additional key challenge of this will understand the methods used to analyze the information from the scan. There are several different methods has been implemented by different researchers for the fingerprint recognition system. In this paper the literature of the different approaches are discussed.

Keywords: Fingerprint, biometric system, scan, Face recognition, IRIS Technology.

I. INTRODUCTION

Biometrics is the skill and tools of measuring and analyzing biological data. In information technology, biometrics pass on to technologies that concludes and scrutinizes the human bodies character, such as, fingerprints, DNA eye, retinas and irises, voice patterns, facial patterns and hand dimensions, for authentication reason. Fingerprints are mainly widely used their high adequacy, immutability and uniqueness.

A. Why choose biometric?

Biometric authentication uses features of your personal physiology, like as your retinal image or fingerprint, to identify you as you. This skill has been adapted to personal computers to permit users to log in to their accounts using biometric recognition, most frequently fingerprints. Setting up your computer to use biometric verification can be safest than a password, because it is much harder for a hacker to crack than a password is. Luckily, you can effortlessly set up biometric verification in just a few minutes. An association of rest part of the paper is done in such a ways: next section presents the literature of work done and in last concluded the paper.

B. Types of Biometric

Finger print: A fingerprint is an impression of the friction ridges of all or any part of the finger [1, 2, 3]. Fingerprint matching technique can be placed into two classes. One of them is minutiae-based and the other one is a correlation-based. Minutiae based methods find the minutiae points primarily and them map their relation placement on the finger. The correlation based methods require the specific location of a registration point and are affected by image transformation and rotation.

Face recognition: A facial recognition system is an application of computer for robotically identifying or verifying a person from a digital image or a video frame from a video resource [4].

IRIS Technology: This recognition system uses the iris of eye which is colored area that surrounds the pupil iris patterns are exclusive and are obtained through video based image acquisition system. Each iris organization is featuring a multifaceted outline. This can be a combination of explicit features called as corona, crypts, filaments, freckles, pits, furrows, striations and rings [5].

Hand Geometry Technology: It is related to the fact that nearly each person's hand is shaped in a different way and the shape of a person's hand does not transform after certain age. Such techniques comprise the assessment of length, width, thickness and surface area of the hand [6-7].

Retina Geometry Technology: It is based on the blood vessel pattern in the retina of the eye as the blood vessels at the back of the eye have a inimitable prototype, from eye to eye and person to person. Retina is not unswervingly observable and so a coherent infrared light source is necessary to illuminate the retina. A retina scan has an error rate of 1in 10,000,000, Compared to fingerprint identification error being sometimes as high as 1 in 500 [9, 14].

Signature Verification Technique: The signature dynamics identification is based on the dynamics the signature rather than an immediate comparison of the signature itself subsequently. The dynamic is measured as a means of the pressure, routes, acceleration and the length of the strokes, dynamics integer of strokes and their duration [15, 16].

Speaker Recognition technique: Voice is also physiological peculiarity because every person has dissimilar pitch, but voice identification is mainly based on the study of the way a person speaks, commonly classified as behavioral [17, 14].

C. Biometric is used for two authentications method

Verification: It involves confirming or denying a person's claimed identity. A basic identity (e.g. ID number) is accepted and a biometric template of the subject taken is matched using a 1:1 matching algorithm to confirm the person's identity Shown in Fig. 1.

Identification: This involves establishing a person's identity based only on biometric measurements. The comparator equivalent the obtained biometric with the ones stored in the database bank using a 1: N matching algorithm for recognition.

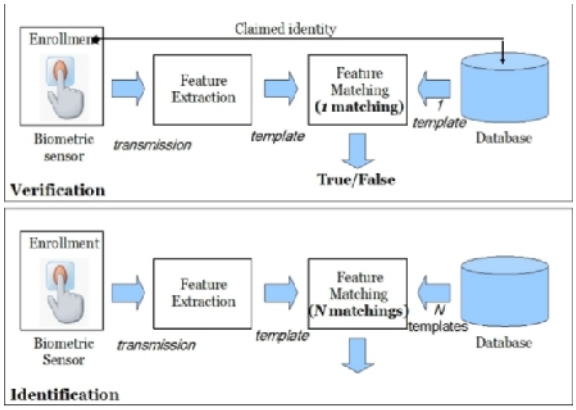

Fig.1. Identification and verification.

There are a number of advantages of biometric technology:

- Biometric identification can provide tremendously precise, secured access to message fingerprints, retinal and iris scans generates enormously unique data sets when done properly.
- Current methods like password authentication have
- Robotic biometric recognition can be done very hastily and unvaryingly, with a minimum of training.
- Your uniqueness can be confirmed without resort to documents that may be stolen, lost or altered.

What is fingerprint?

Fingerprints are the minute ridges, whorls and valley patterns on the tip of each finger. They achieved from stress on a baby's tiny producing fingers in the womb. No two people have been gotten to have the same fingerprints – they are totally unique. There's a one in 64 billion possibilities that your fingerprint will match up accurately with someone else's. Fingerprinting is one form of biometrics, a science that uses people's physical quality to recognize them.

Fingerprints are idle for this reason because they're inexpensive to assemble and scrutinize, and they not at all change even as people age.

Loop **arch** **whorl**

Fig. 2. Loop, arch and whorl.

Each of the ridges of fingerprints form outline known as loops, whorls or arches:-

Arches: - slope upward and then down, like very narrow mountains Shown in Figure 2.

Loops: - starts on one side of the finger, curvature around or upward, and outlet the other side.

Whorls: form a circular or spiral model.

Table 1: Comparisons with various techniques.

Biometric identifier	**Universality**	**Distinctiveness**	**Permanence**	**Collectability**
DNA	H	H	H	L
Ear	M	M	H	M
Face	H	L	M	H
Fingerprint	M	H	H	M
IRIS	H	H	H	M
Signature	L	L	L	H

II. FINGERPRINT TECHNOLOGY

The traditional method uses the ink to get fingerprint onto a piece of paper .this piece of paper is then scanned using a traditional scanner. Now in modern approach, live fingerprint readers are used. Such technologies are based on optical, thermal, silicon or ultrasonic principles [1-3] it is oldest of all the biometric technique Optical fingerprint reader comprise of the source of light the light sensor and a special reflection surface that change the reflection according to pressure. Some of the readers are fitted out with processing and memory chips as well.

Optical fingerprint reader: The size of optical finger is around 10*10**15. It is difficult to minimize them much more as the reader has to comprise the source on light reflection surface and sensor.

Optical silicon fingerprint: An Optical silicon fingerprint sensor is related to the capacitance of fingerprint.

Ultrasound fingerprint: It is newest and least common. They use ultrasound to monitor the fingerprint surface, the user place the finger on piece of glass and the ultrasonic sensor moves and reads whole fingerprint. The common framework of fingerprint identification system (FIS) [8] fingerprints matching is last step in automatic fingerprint identification system (AFIS) fingerprint matching technique can be classified into three types:

- Correlation based matching,
- Minutiae based matching,
- Feature based matching [9].

The minutiae based matching is the most accepted and widely used method, being the basis of the human based fingerprint comparison. In [10] a fingerprint minutia matching method was proposed. Comparing the fingerprint minutiae by using both the local and global arrangement of minutiae. The local organization of a minutia explains the rotation and transformation invariant feature of the minutia in its neighborhood. It is used to find the corresponding of two minutiae sets increase the reliability of the global comparing. The global structure of minutiae reliably determines the uniqueness of fingerprint. Therefore the local and global structure of minutiae together provide a solid basis for reliable and robust minutiae matching this matching scheme is suitable for online processing for one to one matching but not on embedded devices and yet requires high resolution images.

In [11], a fingerprint minutiae matching algorithm was proposed, which is hasty, precise and appropriate for the real time fingerprint recognition system. This method is very proficient for minutiae based.

III. EVALUATION

The time is used to biometric authentication with provide the degree of security is concerned. In this paper we have already discussed the various types of biometric authentication techniques in this part we will discuss different techniques and find degree of security.

There are various parameters with help of biometric authentication techniques. These factors are described below [12, 13, and 14].

A. Factors of Evaluation

False accept Rate (FAR) and false match rate (MAR): The probability that the system incorrectly declares successful match between the input pattern and non-matching pattern in the database. It measures the percent of unacceptable matches. These systems are significant since they are significant since they are commonly used to prohibit action by disallowed.

False Reject Rate (FRR) or false non-match Rate (FNMR): The probability that the system mistakenly declares of Match amid between the input pattern and the matching templates in the database. It computes the percent of valid inputs being rejected.

Relative operating characteristic (ROC): Normally, the matching algorithm presents a decision using some parameters (e.g. a threshold)

In biometric system the FAR and FRR can usually be traded off adjacent to each other by changing those parameters. The ROC plot is attained by graphing the values of FAR and FRR, changing the variables absolutely.

Equal error Rate (EER): The rates at which both allow and refuse errors are equal. ROC or DET plotting is used since how FAR and FRR can be changed, is publicized clearly. When rapid comparison of two systems is compulsory, the ERR is regularly used, acquired from the ROC plot by taking the point where FAR and FRR have the identical value. Lower the EER, the more precise the system is considered to be.

Failure to enroll Rate (FTE or FER): The percentage of data input is considered invalid and fails to input into system. Failure to enroll happens when the data obtained by the sensor are considered invalid or of poor quality.

Failure to Capture Rate (FTC): Within automatic system, the probability that the system fails to detect a biometric characteristic when presented correctly is generally treated as FTC.

Template Capacity: It is defined as the greatest number of groups of data which can be input the method.

Result of evaluation: The evolution of various techniques using the above parameter is presented in a tabular format.

Table 2: Evaluation of biometric techniques.

Biometric	EER	FAR	FRR	Subject
face	NA	1%	10%	37437
Hand print	1%	2%	2%	129
iris	.01%	.94%	.99%	1224
fingerprint	2%	2%	2%	25000
Keystrokes	1.8%	7%	.1%	15
voice	6%	2%	10%	30

IV. RELATED WORK

Bharkad and Kokare [18] they proposed discrete wavelet packet transform (DWPT) based feature extraction method is illustrated for fingerprint matching. The wavelet packet transform is useful on miniature area of fingerprint image. The performance of wavelet packet disintegration is evaluated on the standard database available at the Website of Bologna University. The idleness of discrete wavelet packet transform is reduced without conciliating the meticulousness. The discrete wavelet packet transform with reduced idleness gives the improved performance over the discrete wavelet transform (DWT), Gabor filter and minutiae based method. Alkhathami, Han and Schyndel [19] proposed an approach for embedding two watermarks into fingerprint images using the Discrete Cosine Transform (DCT) algorithm. The key role of the proposed algorithm is to add more authentication factors based on the watermark messages and to defend the ownership of the fingerprint image while the information used for identification or verification of a fingerprint image mostly lies in its minutiae, the initiated watermarking algorithm does not affect fingerprint features. Initial watermark is created based on a unique identification number that can identify the user. The hash function (SHA2) is applied to generate the hash value of the user identification number to encode the watermark prototype. Subsequently, it is embedded into the fingerprint image while evading the minutiae positions. Secondly the watermark is a gray image that is inserted into first watermarked image. The removal stage does not require the original fingerprint image. They measure the influence of the watermarks on the fingerprint features based on the comparison amongst the total number of extracted minutiae points before and after the embedding process. The existing schema shows a high PSNR value**.** Conti, Vitello and Sorbello and Vitabile [20] the author proposed an advanced method for personal recognition based on fractional fingerprint is proposed. The system is based on fingerprint local analysis and micro-features, endpoints and bifurcations, drawing out. The proposed approach starts from minutiae taking out from a fractional fingerprint image and ends with the final matching score amongst fingerprint pairs. The calculation of likelihood ratios in fingerprint identification is computed by trying each probable overlapping of the fractional image with whole image. The primary experimental results conducted on the PolyU (Hong Kong Polytechnic University) free database show an encouraging performance in terms of identification accuracy. Alkhathami, Han and Schyndel [21] proposed a new digital watermarking technique for fingerprint images using the Dual-Tree Complex Wavelet Transform (DTCWT). The watermark is embedded into the real and imaginary parts of the DTCWT wavelet coefficients. The work is focuses on the study of watermarking method for fingerprint images that are composed from different angles without mortifying minutiae points. They examined the effect of the watermark on the fingerprint features after the watermark embedding progression. VeriFinger V5.0 is used to resolve the matching score among the template and the watermarked images. The user's characteristics are linked with the fingerprint features to add an extra authentication factors to the authentication process. SHA2 hash function is used to encode the user identification digit by generating the hash value and translate it into a binary image to build the watermark data. The original fingerprint image is not essential to extract watermark data. The method has been tested using the CASIA fingerprint image database with 500 fingerprint images from 100 persons**.** Wen, Qi, Li, Zhang, Gong and Cao [22] proposed a novel robust and efficient minutia-based fingerprint corresponding algorithm. There are two main contributions. Initially, apply a set of global level minutia reliant features, i.e., the behaviors that determine the reliabilities of the extracted minutiae and the area of overlapping regions among the query and template images of fingerprints. The accomplishment of these easy-to-get minutia reliant features presents coherence to the well-accepted fingerprint template standards. In addition, the logical amalgamation of them results in the robustness to deprived quality fingerprint images. subsequently implement a hierarchical recognition strategy, which applies a method of global matching that improves the local matching resolution towards a authentic result over the whole images. Additionally, the much improved accuracy, our algorithm also endorses the efficiency, because matches with other state-of-the-art matching approaches; it does not formulate the use of any time-consuming operations or any multifaceted feature structures. The experimental results exhibit the proposed method exhibits an exceptional accuracy that exceeds the performance of well-known minutia based matchers. Sayeemuddin, Pithadia and Vandra [23] proposed a extremely simple algorithm that uses Laplacian of Gaussian (LoG) filter, edge filter (LoG based) and morphological operations. This algorithm does not necessitate block wise calculation of mean and variance. The algorithm also takes benefit of the fact that most fingerprint images are vertical or within 45 degrees to the vertical. An algorithm is applied on FVC2004-DBl, DB2, DB3 and FVC2000-DB3 public database. The algorithm shows that it gives good output even for low quality images.

V. PROPOSED FINGERPRINT MATCHING SYSTEM

Fingerprint matching system consist of 5 step,

- Thinning of the fingerprint image.
- Core point detection.
- Minutiae extraction
- Feature vector construction.
- Distance based matching.

Thinning algorithm: The most current thinning algorithm used in fingerprint pre-processing operation need the step of binarization before thinning as in [2,4,7,17-21]

Binarization causes the following problem:

- A considerable amount of information may be lost during the bi-narization method.
- Bi-narization is time consuming and may introduction a large number of spurious minutiae.
- In the absence of a priori enhancement step, most of the Binarization technique does not provide satisfactory results when applied to low quality image.

The impact of using the proposed thinning algorithm over that involving a bi-narization step was found to increase the overall recognition rate by a ratio of 7% to 9%, when tested on the FVC 2000 dataset.

VI. CONCLUSION

The Fingerprint identification systems for the human being verification are incredibly fast and truthful for more consistent and sheltered system. This paper presents the some technologies related to fingerprint identification system and discusses the literature of the work done to implement the system. Among the discussed method the performance of the some method is extremely good and some provides less effective. Some of the method is fail to match the two images with different direction may fail to match. So in future we have to develop such method which can match the images with different orientation and also improve the quality of images.

REFERENCES

[1]. A. Ross, S. Dass, and A.K. Jain, "A deformable model for fingerprint matching", *Journal of pattern Recognition, Elsevier,* Vol. **38**, no1.

[2]. T. Matsumoto, H. Hoshinok. Yamada and Hasino, "Impact of artificial gummy fingers on fingerprint systemt", In *Proc. of SPIE*, volume 4677.

[3]. Abijyev, R.H. Altunkaya, k."neural network based biometric personal identification", frontiers in the convergence of and bioscience and information Techonologies, jeju, oct.2007.

[4]. M.A Dabbah, W.L. Woo, and S.S Dlay, "secure Authentication for Face Recognition,". *In proc.of IEEE symposium on Computational intelligence in image and signal processing,* Apr. 2007.USA.

[5]. Sanjay R.Ganorkar, Ashok A .Ghatol,"Irise Recognition; An Emerging Biometric Techonology", in *Proc. of the 6th WSEAS international conference on signal Processing, Robotics and Automation, Greece, feb.2007.*

[6]. E. Kukula, S. Elliott" Implementation of Hand Geomrtey at purdue University's Recreational center: An Analysis of User Perpective and system performance", in *Proc. Of Annul International carnahan conference on Security Techonology, UK, Oct 2001.*

[7]. A. Kumar, D.C Wong, H.C. shen, and A.K jain, "personal Verification Using palmprint and hand geometry Biometric", In Proc. Of 4th international Conference on Audio-and video based biometric person Authentication, Guildford, UK, jun. 2003.

[8]. Ji L, Yi Z. fingerprint orientation field estimation using ridge projection. Pattern Recogn. 2008; **41**: 1491-503.

[9]. Liu f, Zhao Q, Zhang D.A novel hierarchical fingerprint matching approach. *Pattern Recogn* 2011; 44:1604-13.

[10]. Jiang X, YAU WY. Fingerprint minutiae based on the local and global structure in *Proc in conf on pattern recognition* (15),vol. **2**; 200.p.1042-5

[11]. Jie Y, Fang Y, Renjie Z., Qifa S. fingerprint minutae matching algoritham for real time sysrem. *Pattern Recogn* 2006; **39**:143-6.

[12]. A.K. Jain, S. Pankanti, S. Prabhakar, L. Hong, A.ross, and J.L. Wayman, "biometric: a grand challenge" *In Proc. of International Conference on pattern Recognition, Cambridge*, U.K., Aug. 2004, pp.935-942.

[13]. J. Phillips, Martin, C. Wilson, and M. Przybocki, "An introduction to evaluating biometric system", *IEEE computer society*, volume **33**, No.2000, pp. 56-63.

[14]. J.L Wayman, A.K. Jain, D. Maltoni, and D. Maio, Eds, "Biometric system: technology, design and performance evaluation", New York: Spring Verlag, 2005.

[15]. Samir K. Bandopadhaya, Swarned Mukherjee, Debeashis Ganguly, Poulumi Das "Statistical Approach for offline hand written Signature verification", *Journal of computer science publication*, volume **4** , ISSUES 3, May .2008, pp.181-185.

[16]. J.L. Wayman, "Fundamentals of BIOMETRIC Authentication Techonologies", International Journal of image and graphics, world scientific publication, volume**1**, No.1, Jan 2001, pp93-113.

[17]. Kar, B. Kartik, B. Dutta, P.K. "Speech and face biometric person Authentication", in *Pro of IEE International conference on industrial Technology, India*, Dec.2006, pp391-396.

[18]. Sangita Bharkad, Manesh Kokare, "Fingerprint Matching using Discreet Wavelet Packet Transform", 2013 *3rd IEEE International Advance Computing Conference (IACC).*

[19]. Mohammed Alkhathami, Fengling Han and Ron Van Schyndel, "Fingerprint Image Protection Using Two Watermarks Without Corrupting Minutiae", 2013 *IEEE 8th Conference on Industrial Electronics and Applications (ICIEA).*

[20]. V. Conti, G. Vitello and F. Sorbello, S. Vitabile, "An Advanced Technique for User Identification using Partial Fingerprint", 2013 *Seventh International Conference on Complex, Intelligent, and Software Intensive Systems*.

[21]. Mohammed Alkhathami, Fengling Han and Ron Van Schyndel, "Fingerprint Image Watermarking Approach Using DTCWT without Corrupting Minutiae", 2013 *6th International Congress on Image and Signal Processing (CISP 2013).*

[22]. Wen Wen, Zhi Qi, Zhi Li, Junhao Zhang, Yu Gong and Peng Cao, "A Robust and Efficient Minutia-based Fingerprint Matching Algorithm", 2013 *Second IAPR Asian Conference on Pattern Recognition*.

[23]. Shaikh Mohammed Sayeemuddin, Paml V. Pithadia, Dhannesh Vandra, "A Simple and Novel Fingerprint Image Segmentation Algorithm", 2014 *International Conference on Issues and Challenges in Intelligent Computing Techniques (ICICT).*