Fingerprint Recognition System : Design & Analysis

Dibyendu Nath[1] **Saurav Ray[2]** **Sumit Kumar Ghosh[3]**
Dept. of Computer Science & Engineering,
Heritage Institute of Technology,
Kolkata, India.
{[1]dev.nath.cs, [2]saurav.ray.hitk, [3]sumit.hitk.ghosh}@gmail.com

***Abstract*— Fingerprint Recognition is one of the research hotspots in Biometrics. It refers to the automated method of verifying a match between two human fingerprints. It is essentially a challenging pattern recognition problem where two competing error rates: the False Accept Rate (FAR) and the False Reject Rate (FRR) need to be minimized. Advancement of computing capabilities led to the development of Automated Fingerprint Authentication Systems (AFIS) and this led to extensive research especially in the last two decades. In this paper, we attempt to give a comprehensive scoping of the fingerprint recognition problem and address its major design and implementation issues as well as give an insight into its future prospects.**

***Keywords*- Fingerprint Recognition, Biometrics, Identification, Verification, Security, Authentication**

I. INTRODUCTION

In order to access the Internet or any other important resource safely, high-security authentication systems are essential. However studies [10] show that users usually choose weak passwords, frequently re-use passwords across multiple sites and often forget them. According to the *2002 NTA Monitor Password Survey*, heavy web users have an average of 21 pass-words, 81% of users choose a common password and 30% write their passwords down or store them in a file. Automated identity authentication using fingerprint recognition [4, 3] is an effective solution in such cases.

Historically speaking, fingerprints have been long associated with criminology, specifically forensics. Development of cheaper and robust automated fingerprint authentication systems coupled with the inherent ease of fingerprint acquisition, has led to its widespread commercial and civilian applications. One of the world's largest fingerprint recognition systems is the *Integrated Automated Fingerprint Identification System* (IAFIS), maintained by the FBI in the US since 1999.

A. Fingerprint as a Biometric

"Two like fingerprints would be found only once every 10^{48} years" — Scientific American, 1911.

Individuality of fingerprints is based on empirical observations. However Golfarelli *et al* [6] formulated the optimum Bayesian decision criterion for a biometric verification system and obtained a theoretical equal error rate (EER) of 1.31 x 10^{-5} for a hand-geometry-based verification system and of 2 x 10^{-3} for a face-based verification system. Similarly Pankanti *et al* [5] also showed that there is limited probability of correspondence of two fingerprints.

B. Classification & Indexing of Fingerprints

Fingerprint authentication includes two subdomains: one is fingerprint verification (*Am I who I claim I am?*) and the other is fingerprint identification (*Who am I?*), the latter being more difficult requiring extensive indexing and classification of fingerprints for efficient retrieval.

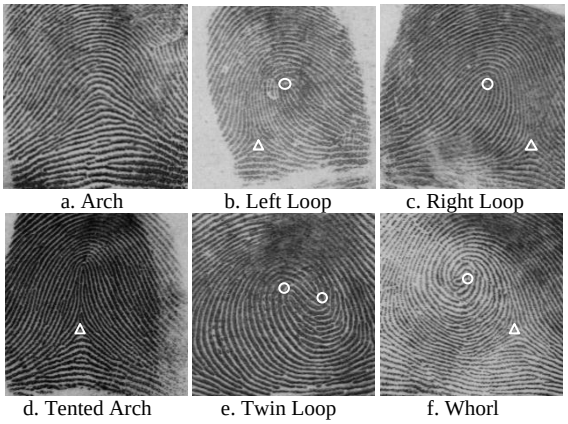


Fig. 1: Fingerprint classification involving 6 classes - critical points in a fingerprint called core & delta marked as circles & triangles

Nearly all fingerprint classification schemes used today are derived from the famous "*Henry System*" [1] – a detailed fingerprint indexing method for aiding manual fingerprint comparison. For instance, the FBI uses one variant which recognizes eight different types of patterns: radial loop, ulnar loop, double loop, central pocket loop, plain arch, tented arch, plain whorl, and accidental.

Whorls are usually circular or spiral in shape. Arches have a mound-like contour, while tented arches have a spike-like or steeple-like appearance in the center. Loops have concentric hairpin or staple-shaped ridges and are described as "radial" or "ulnar" to denote their slopes; ulnar loops slope toward the little finger side of the hand, radial loops toward the thumb.

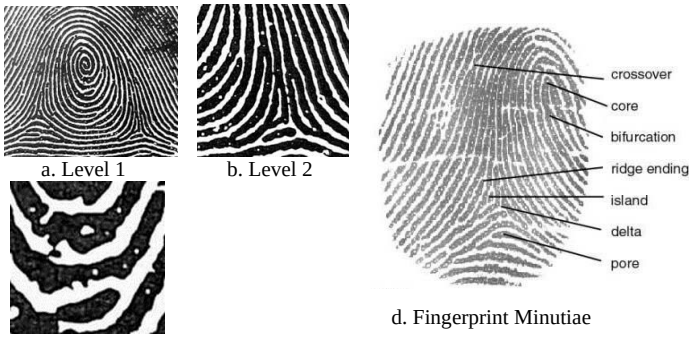
Fingerprint classification & indexing is a difficult pattern recognition problem due to small inter-class variability compared to large intra-class variations in fingerprint patterns. Germain *et al* [15] describe a popular efficient

technique for indexing into large fingerprint databases using minutiae triplets in their indexing procedure. More efficient classification schemes have also been proposed like [7] by Jain, *et al*.

II. Fingerprint Features

A fingerprint is an impression of the epidermal ridges of a human fingertip. A hierarchy of three levels of features, namely, Level 1 (pattern), Level 2 (minutiae points) and Level 3 (pores and ridge shape) are used for recognition purposes. Most AFISs employ Level 1 & Level 2 features.

Level 1 features refer to the overall pattern shape of the unknown fingerprint—a whorl, loop or some other pattern. This level of detail cannot be used to individualize, but it can help narrow down the search. Level 2 features refers to specific friction ridge paths — overall flow of the friction ridges and major ridge path deviations (ridge characteristics called minutiae) like ridge endings, lakes, islands, bifurcations, scars, incipient ridges, and flexion creases.



a. Level 1 b. Level 2 c. Level 3 d. Fingerprint Minutiae

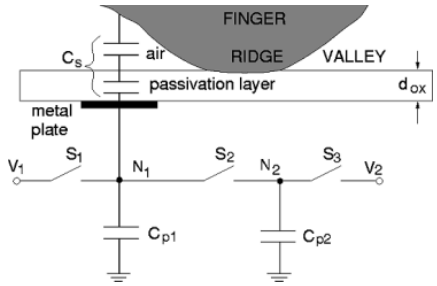
Fig. 2: Fingerprint Features

Level 3 detail [14] refers to the intrinsic detail present in a developed fingerprint — pores, ridge units, edge detail, scars etc. High resolution sensors (~1000dpi) are required for extraction of Level 3 features. But as [8] shows, EER values are reduced (relatively ~20%) using them along with Level 1 & 2 features. Moreover Level 3 features offer greater success in partial fingerprint recognition as shown in [9].

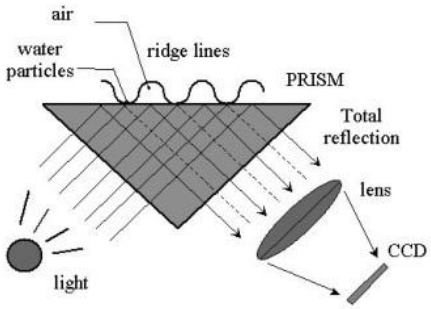
III. Fingerprint Sensing

Fingerprint sensing techniques can be of two types – *off-line scanning* and *live-scanning*. In off-line sensing fingerprints are obtained on paper by *"ink technique"* which are then scanned using paper scanners to produce the digital image. Most AFISs use live-scanning where the prints are directly obtained using an electronic fingerprint scanner. Almost all the existing sensors belong to one of the three families: *optical*, *solid-state*, and *ultrasound*.

Optical sensors, based on the frustrated total internal reflection (FTIR) technique are commonly used to capture live-scan fingerprints in forensic and government applications. They are the most common fingerprint sensors. An important breakthrough in sensor technology was the development of optical sensors based on fiber-optics as described in the US patent [21], leading to sensor miniaturization and enhanced portability.



a.Capacitive Solid-State Sensor [20]



b. Optical Sensor using FTIR

Fig. 3: Fingerprint Sensors

Solid-state touch and sweep sensors — silicon-based devices that measure the differences in physical properties such as capacitance or conductance of the friction ridges and valleys dominate in commercial applications. Tartagni and Guerrieri [22] describe a feedback capacitive sensing scheme using a 200x200 element sensor array implement in standard 2-metal CMOS technology. Jeong-Woo Lee *et al* [20] discusses another such solid-state sensor, based on capacitive differences, capable of producing 600dpi fingerprints. Many commercially available sweep sensors like Fujitsu MBF320 are based on such low-power solid-state devices.

Fig. 4: Latent Fingerprint

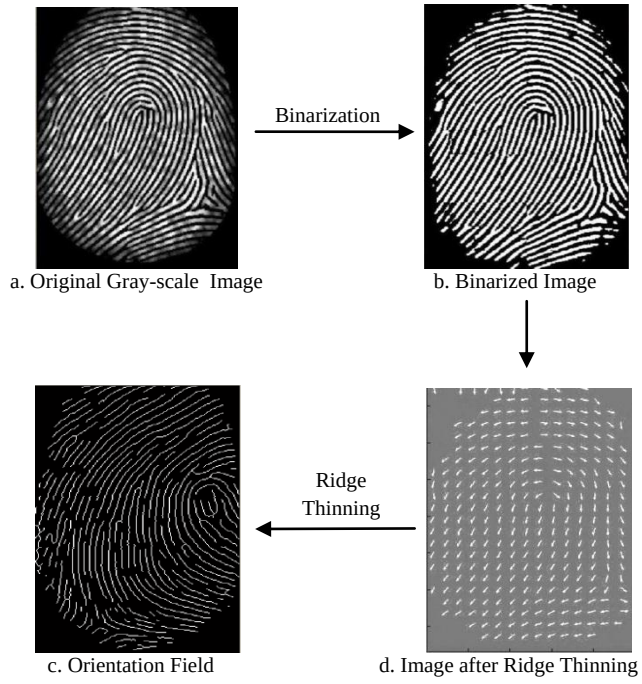
A special case of off-line sensing is the acquisition of *a latent fingerprint* from a crime scene [19]. Used extensively in forensics, latent prints are accidental impressions left by friction ridge skin on a surface, due to natural secretions of the eccrine glands present on skin. While tremendous progress has been made in plain fingerprint matching, latent fingerprint matching continues to be a difficult problem. Poor quality of ridge impressions, small finger area, and large non-linear distortion are the main difficulties in latent fingerprint matching, compared to plain fingerprint matching.

IV. Feature Extraction Techniques

For the purpose of automation, a suitable representation i.e. feature extraction of fingerprints is essential. This representation should have the following properties –

- Retention of discriminating power of each fingerprint at several levels of resolution
- Easy computability
- Amenable to automated matching algorithms
- Stable and invariant to noise and distortions
- Efficient and compact representation

Several feature extraction methods have been proposed and implemented successfully over the years. Roughly speaking there are four categories of methods based on fingerprint feature extraction by image processing [11].The first category of methods extract minutiae directly from the gray-level image [1, 23, 25, 34] without using binarization and thinning processes while the second category extracts features from binary image profile patterns [15, 25, 26]. The third category of methods uses machine learning [25, 28, 29] for extracting minutiae and the last category extracts minutiae from binary skeletons [2, 30].



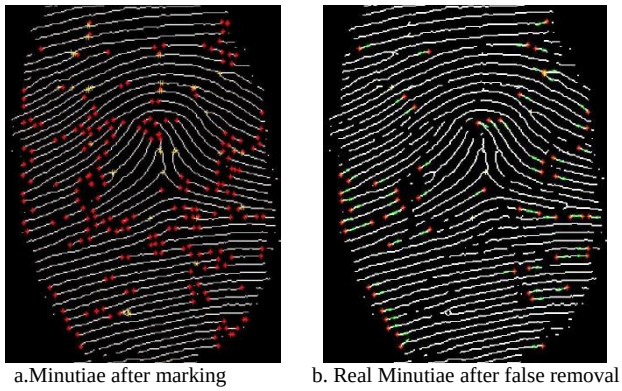
a. Original Gray-scale Image b. Binarized Image

c. Orientation Field d. Image after Ridge Thinning

Fig. 4: Minutiae Extraction from Fingerprint Image

Binarization is the process by which an enhanced gray-level image is transformed into a binary image for subsequent feature detection. Good binarization algorithms should minimize information loss and also provide efficient computational complexity. A binarization approach based on the peak detection in the cross section gray-level profiles orthogonal to the local ridge orientation has been proposed by Ratha, et al [31]. Liang et al [27] proposed an Euclidean distance transform method to obtain a near-linear time binarization of fingerprint images.

Fingerprint ridge thinning is basically elimination of redundant pixels till each ridge is just one pixel thick. An innovative iterative thinning technique has been proposed by Ahmed and Ward [32] while a multi-scale thinning approach has been proposed by You, *et al* [33].



a.Minutiae after marking b. Real Minutiae after false removal

Fig. 5: Minutiae Extraction

After initial fingerprint feature extraction some post-processing is required for removing false or spurious minutiae detected in highly corrupted regions or introduced by previous processing steps (e.g., thinning). Chen and Kuo [24] proposed a three-step false minutiae filtering method, which dropped minutiae with short ridges, minutiae in noise regions, and minutiae in ridge breaks using ridge direction information. Another method for removing all the spurious pixels generated at the thinning stage in order to facilitate subsequent minutiae filtering has been proposed by Zhao and Tang [30].

V. Fingerprint Matching Techniques

Matching fingerprint images is an extremely difficult problem, mainly due to the large variability in different impressions of the same finger (i.e., large *intra-class* variations). Fingerprint matching algorithms are roughly classified into 3 major categories –

C. Correlation-based Matching :

Two fingerprint images are superimposed and the correlation between corresponding pixels is computed for different alignments (e.g. various displacements and rotations). Fourier transform [12] as well as Fourier-Mellin Transform [13] can be used to speed up the correlation computation.

D. Feature-based (or Minutiae- based) Matching :

Typical fingerprint recognition methods employ feature-based matching, where minutiae (i.e., ridge ending and ridge bifurcation) are extracted from the registered fingerprint image and the input fingerprint image, and the number of

corresponding minutiae pairings between the two images is used to recognize a valid fingerprint image. Alternatively, Jain *et al.* [2] used a string matching technique while Isenor and Zaky [17] propose a graph-based fingerprint matching algorithm. Fan *et al.* [18] describes a fingerprint verification algorithm based on a bipartite graph construction between model and query fingerprint feature clusters.

The minutiae matching problem has been generally addressed as a point pattern matching problem which has been extensively studied yielding families of approaches known as relaxation methods, algebraic and operational research solutions, tree-pruning approaches, energy-minimization methods, Hough transform, etc.

E. Pattern-based (or Image-based) Matching

Pattern based algorithms compare the basic fingerprint patterns (e.g., local orientation and frequency, ridge shape, texture information) between a previously stored template and a candidate fingerprint. The images need to be aligned in the same position, about a central point on each image. The candidate fingerprint image is then graphically compared with the template to determine the degree of match.

The image-based techniques include both optical as well as computer-based image correlation techniques. Recently, several transform-based techniques have also been explored. For instance, a phase-based fingerprint image matching technique using 2D discrete Fourier transforms has been proposed by Ito, *et al* [35] while Hamamoto [16] describes a Gabor filter based fingerprint matching technique.

VII. Major Implementation & Design Issues

A fingerprint recognition system can make two types of errors: a *false match*, when a match occurs between images from two different fingers, and a *false non-match*, when images from the same finger are not a match. Thus the chief objective behind the design of a good fingerprint matching system is to reduce both these errors. However both the error rates cannot be reduced simultaneously as they are inversely dependent on each other.

Another important design issue is the security of the fingerprint recognition system itself along with the fingerprint template database. The unauthorized use or disclosure of fingerprint template information from such databases can be a serious security and privacy threat.

Although fingerprint recognition has been extensively studied, there are still many *open research problems* in this domain, for instance :

- Efficient Automated Fingerprint Classification
- Fully Automated Latent Fingerprint Recognition
- Altered or Fake Fingerprint Detection
- Efficient Compression of Fingerprint Templates
- Automated Artificial Fingerprint Generation

Latent fingerprint matching poses another whole new set of problems altogether. Compared to good quality full fingerprints acquired using live-scan or inking methods during enrollment, latent fingerprints are often smudgy and blurred, capture only a small finger area, and have large nonlinear distortion. Hence they require enhanced extraction and matching techniques to make latent fingerprint recognition free of manual matching and fully automated.

VIII. Conclusions

Fingerprint Authentication has been studied for well over a century. However, its use has truly become widespread and mainstream only in the last few decades due to development of automated fingerprint recognition systems. The ever-increasing demand for reducing the error and failure rates of automated fingerprint recognition systems and the need for enhancing their security have opened many interesting and unique research opportunities that encompass multiple domains such as image processing, computer vision, statistical modeling, cryptography, and sensor development. Our preliminary analysis shows that fingerprints have been proven to be an excellent if not the best biometric and its potential has not yet been fully realized.

But still, issues such as fingerprint authentication at a distance, real-time identification in large-scale applications with billions of fingerprint records, developing secure and revocable fingerprint templates that preserve accuracy, and scientifically establishing the uniqueness of fingerprints will likely remain as grand challenges in the near future.

References

[1] E. Henry, *Classification and Uses of Finger Prints*, Routledge, London, 1900.

[2] A. K. Jain, L. Hong, and R. M. Bolle, "On-line fingerprint verification", IEEE Trans. on Pattern Analysis and Machine Intelligence, 19(4):302–313, April 1997.

[3] D. Maltoni, D. Maio, A. K. Jain & S. Prabhakar, *Handbook of Fingerprint Recognition*, Springer, 2003.

[4] P. Komarinski, *Automated Fingerprint Identification Systems*, Elsevier Academic Press, 2004

[5] S. Pankanti, S. Prabhakar, and A. K. Jain, "On the Individuality of Fingerprints", IEEE Transactions on PAMI, Vol. 24, No. 8, pp. 1010-1025, 2002.

[6] Golfarelli M., Maio D., and Maltoni D., "On the Error-Reject Tradeoff in Biometric Verification Systems" IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 19, no.7, pp. 786-796,1997.

[7] A. K. Jain, S. Prabhakar and S. Pankanti, "Matching and Classification: A Case Study in Fingerprint Domain", Proc. INSA-A (Indian National Science Academy), Vol. 67, A, No. 2, pp. 223-241, March 2001.

[8] Anil Jain, Yi Chen, and Meltem Demirkus, "Pores and ridges: fingerprint matching using level 3 features," 18th International Conference on Pattern Recognition, pp. 477 – 480, 2006.

[9] K. Kryszczuk, A. Drygajlo, and P. Morier, "Extraction of level 2 and level 3 features for fragmentary fingerprints," Proc. of the 2nd COST275 Workshop, Vigo, Spain, pp. 83-88, 2004.

[10] D. Florencio and C. Herley, "A large-scale study of web password habits," Proceedings of the 16th International conference on the World Wide Web, 2007.

[11] R. C. Gonzalez and R. E. Woods., *Digital Image Processing*, Prentice Hall, Upper Saddle River, NJ, 2002.
[12] Coetzee L. and Botha E.C., "Fingerprint recognition in low quality images," Pattern Recognition, vol. 26, no. 10, pp. 1441-1460, 1993.
[13] Sujan V.A. and Mulqueen M.P., "Fingerprint identification using space invariant transforms," Pattern Recognition Letters, vol. 23," no. 5, pp. 609-619, 2002.
[14] Q. Zhao, A. K. Jain, "On the utility of extended fingerprint features: a study on pores," IEEE Computer Society Workshop on Biometrics, CVPR2010, San Francisco, U.S., June 18, 2010.
[15] R. S. Germain, A. Califano, and S. Colville, "Fingerprint matching using transformation parameter clustering", IEEE Computational Science and Engineering, pages 42–49, Oct-Dec 1997.
[16] Y. Hamamoto, "A Gabor filter-based method for identification", Intelligent Biometric Techniques In Fingerprint And Face Recognition, pages 137–151. CRC Press, Boca Raton, 1999.
[17] D. K. Isenor and S. G. Zaky, "Fingerprint identification using graph matching," Pattern Recognition, 19(2):113–122, 1986.
[18] K.-C. Fan, C.-W. Liu, and Y.-K. Wang, "A fuzzy bipartite weighted graph matching approach to fingerprint verification," In Proc. of the IEEE International Conf. on Systems, Man and Cybernetics, pages 729–733, Oct 1998.
[19] Colins M.W., "Realizing the Full Value of Latent Prints", California Identification Digest, 1992.
[20] J.-W. Lee, D.-J. Min, J. Kim, and W. Kim, "A 600-dpi capacitive fingerprint sensor chip and image-synthesis technique," IEEE Journal of Solid-State Circuits, Vol. 34, No. 4, April 1999
[21] Ichiro Fujieda, Yuzo Ono, Seijin Sugama, "Fingerprint image input device having an image sensor with openings", United States Patent 5446290, August 29, 1995.
[22] M. Tartagni and R. Guerrieri, "A fingerprint sensor based on feedback capacitive sensing scheme," IEEE Journal of Solid-State Circuits, Vol. 33 Issue: 1, pages 133 - 142, Jan 1998
[23] L. Jinxiang, H. Zhongyang, and C. Kap Luk, "Direct minutiae extraction from gray-level fingerprint image by relationship examination," In International Conference on Image Processing (ICIP), volume 2, pages 427–430 vol.2, 2000.
[24] Z. Chen and C. H. Kuo. "A topology-based matching algorithm for fingerprint authentication." In IEEE International Carnahan Conference on Security Technology, pages 84–87, 1991.
[25] B. Bir and T. Xuejun. "Fingerprint indexing based on novel features of minutiae triplets". Pattern Analysis and Machine Intelligence, IEEE Transactions on, 25(5):616–622, 2003.
[26] C. Wu, Z. Shi, and V. Govindaraju, "Fingerprint image enhancement method using directional median filter," In Biometric Technology for Human Identification, SPIE, vol. 5404, pages 66–75, 2004.
[27] A. B. Xuefeng Liang and T. Asano, "A near-linear time algorithm for binarization of fingerprint images using distance transform," In Combinatorial Image Analysis, pages 197–208, 2004.
[28] S. Prabhakar, A. K. Jain & S. Pankanti, "Learning fingerprint minutiae location and type, Pattern Recognition," 36(8):1847–1857, 2003.
[29] V. K. Sagar, D. B. L. Ngo, and K. C. K. Foo, "Fuzzy feature selection for fingerprint identification", In Security Technology, 1995. Proceedings, IEEE 29th Annual 1995 International Carnahan Conference on, pages 85–90, 1995.
[30] F. Zhao and X. Tang, "Preprocessing and post-processing for skeleton-based fingerprint minutiae extraction," Pattern Recognition, 40(4):1270–1281, 2007.
[31] N. K. Ratha, S. Chen, and A. K. Jain, "Adaptive flow orientation-based feature extraction in fingerprint images," Pattern Recognition, 28(11): 1657–1672, 1995.
[32] M. Ahmed and R. Ward, A rotation invariant rule-based thinning algorithm for character recognition, Pattern Analysis and Machine Intelligence, IEEE Transactions on, 24(12):1672–1678, 2002.
[33] X. You, B. Fang, V. Y. Y. Tang, and J. Huang "Multiscale approach for thinning ridges of fingerprint." In Second Iberian Conf. on Pattern Recognition and Image Analysis, vol. LNCS 3523, pp 505–512, 2005.
[34] D. Maio and D. Maltoni, "Neural network based minutiae filtering in fingerprints," Fourteenth International Conf. Pattern Recognition, volume 2, pages 1654–1658, 1998.
[35] K. Ito, T. Aoki, H. Nakajima, K. Kobayashi and T. Higuchi, "A fingerprint recognition algorithm using phase-based image matching for low-quality fingerprints", Proc. IEEE International Conference on Image Processing, 2005.