A Study of Biometric Approach Using Fingerprint Recognition

Ravi Subban and Dattatreya P. Mankame

Abstract—Fingerprint (FP) serves to identify that the person authenticating is who he/she claims to be. FP identification is popular biometric technique due to easiness in acquiring, availability of plenty sources (i.e., ten fingers) for collecting data and their established use. This paper summarizes the research work carried out in FP matching techniques, recognition methods and their performance analysis.

Index Terms—Biometric, fingerprint, unimodal.

I. INTRODUCTION TO FINGERPRINT BIOMETRIC

Biometric identification of a person is fast, easy-to-use, precise, trustworthy and economical over traditional knowledge-based and token-based methods. A biometric system contains mainly an image capturing module, a feature extraction module and a pattern matching module as shown in Fig. 1. An image capturing module acquires the raw biometric data of a person using a sensor. Utilizing suitable algorithm/s feature extraction module improves the quality of the captured image. Database module stores the biometric template information of enrolled Persons. Pattern matching module compares the extracted features with the stored templates, which in-turn generates match score [1].

Fingerprint biometric concept: FP biometric is the commonly used oldest and solely method internationally accepted as legal method to identify a person. FP is the impressions of the minute ridge (called as dermal) of the finger. FP ridges and valleys are unique and unalterable. FP biometric is used in numerous applications that include civilian and commercial applications like military, law enforcement, medicine, education, civil service, forensics, driver license registration, cellular phone access [2], [3], computer log-in and like [4]. Today live FP readers based on optical, thermal, silicon, ultrasonic approach are used instead of old method of ink to capture FP. FP identification is based on minutiae or location and direction of the ridge endings and bifurcations (splits) along a ridge path. The two commonly used FP 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. Experimental results show that the fingerprint based systems have very low FRR (False Rejection Rate) of 3 to 7% and 0.001 to 0.01% of FAR (False Acceptance Rate). The pre-requisite to match the FP is classification. The classification is treated as course level matching. The FP can be classified as whorl, right loop, arch, tented arch. In order to ensure the performance of FP identification, enhancement algorithms are needed to improve clarity of input fingerprint images.

The customary FP pattern types are shown in Fig. 2 to Fig. 9.

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. 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.

2) Radial Loops and Ulnar Loops: Ulnar loop pattern loops flow in the direction of the thumbs.

3) 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. 6.

4) Central Pocket loop Whorl has a pattern with minimum one recurving ridge shown in Fig. 7 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.

5) 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. 8.

6) Accidental Whorl is the only pattern which is connected with minimum two deltas. It unites two or more distinctive types of patterns excluding the plain arch as shown in Fig. 9 [5].
The remaining of the paper is structured as follows. Section II presents related work carried out in the FP biometric. Section III depicts performance analysis of biometric modalities.

II. RELATED WORK ON FINGERPRINT BIOMETRIC

The recent developments in biometrics recognition of a person lead to improvements in reliability and accuracy. The related work for Fingerprint Recognition (FR) technologies analyzed with different parameters such as matching techniques, recognition methods, retrieval concepts, security, weather conditions for image acquisition and the like are summarized in this section.

A. Matching Techniques and Recognition Methods

The FP matching performance is evaluated by means of FAR, FRR, EER (Equal Error Rate), GAR (Genuine Accept Rate, GAR=1-FRR).

Zhifan Gao et al. [6] Introduce a method for FR using neighbor local graphical structure to match the point in a pattern and global matching to overcome the problem of noisy data. EER of 3.5% to 5.6% is obtained on FVC2002 database.

Zin Mar Win et al. [7] use a correlation based FR system. The scheme uses Gabor filters for FP feature extraction. The test results of low FAR, FRR and 97% accuracy are reported.

Zhu Le-Qing [8] proposes a knuckle print recognition scheme based on SURF (Speeded-Up Robust Features) algorithm. The test results on PolyU FKP database show accuracy of 96.91% and average matching time 0.106 for identification.

Jucheng Yang et al. [9] propose a secured approach for FR based on set of assembled geometric moment and Zernike moment. The results on FVC2002 database show EER=2.27%, average enroll time=1.77s and average match time=0.19s.

Avinash Kumar Jha et al. [10] devise Neural Network based scheme for FR. The test result for same fingerprint show recognition quotient of 0.937 and less than 0.5 for different fingerprint.

S. Malathi et al. [11] develop a novel methodology for partial FP matching based on pores corresponding to their Local Binary Pattern (LBP) features. The NIST SD30 database result is tested and best match score is obtained.

G. Danese et al. [12] present a parallel architecture for a fast FP matching algorithm based on Band Limited Phase Only spatial Correlation (BLPOC). The experimental results on FVC2002 database show low FAR and FRR.

Yun Yang and JiaMi [13] design an ATM terminal based on FR. The scheme uses Gabor filter for image enhancement. The system ensures enhanced security for stability and reliability.

Fernando Cornelio Jimenez Gonzalez et al. [14] explain a method to overcome the problem of controlled pressure and humidity for image acquiring. The proposed method uses negative Laplace filter and non-stationary analysis of short time Fourier transform and algorithm to find match percentage in the verification process. The test results in varying conditions show the FRR=1.34%-4.88%, FA (False Acceptance) = 0%-1%, RR = 95.12% - 98.2%.

Chomtip Pornpanomchai et al. [15] propose the FR by Euclidean distance method. The test results show a precision of 95% for the ST-BIO Card Reader Model: BCR100T V3.0, and 85% for the VeriFinger Sample DB database. The average access time reported is 19.68 seconds per image.

Shimon Modi et al. [16] report performance evaluations of FR of different sizes and with different sensors, minutiae count, FNMR, FMR, image quality scores. The result shows Fingerprint images above or at level 5 are acceptable.

A. C. Ramachandra et al. [17] designs a scheme for FR using Inter Ridge Variation (FRIVR) algorithm. The experimental results on FVC2002 show the improvement in RR by 80-100%.

Liu Cuilin et al. [18] forwards a method using dynamic password and FR for high-security e-mail system. The method ensures improved safety for e-mails with lower efficiency.

Kaisheng Zhang et al. [19] propose an Automatic FR System(AFRS). The technique utilizes embedded hardware, open source LINUX operating system and related tools. Wenzhou Liu et al. [20] brings to notice a novel idea in which the fingerprint is stored into IC cart of the ID card via microcomputer system. It is then matched with the information of the holder whenever required. The scheme ensures reliable performance, easy to use and higher security.

Haiyun Xu et al. [21] depict a method for increasing matching speed by compressing spectral minutiae feature using Column PCA (Principal Component Analysis) and Line DFT (Line Discrete Fourier Transform) reduction techniques. The reduction rate of 94% and a speed of 125000 comparisons per second is reported and the experimental results on MCYT database show EER=0.29%, FAR=99.8% and on FVC2002-DB2 database show EER=3.72%, FAR=95.6%.

F. G. Hashad et al. [22] discusses a FP identification scheme using Mel Frequency Cepstral Coefficients (MFCCs). The test result proves the scheme is efficient in the presence of noise.

Rajesh Singla and Kalpana Saini [23] comprehend a technology to evaluate FP verification algorithms. The method proves to be suitable for commercial FR algorithms.

Ron F Stewart et al. [24] discuss FR technique in rugged outdoor conditions, i.e. in cold weather. It analyzes recognition performance and image quality of the data.

Fig. 2. Plain Arch. Fig. 3. Tented Arch. Fig. 4. Ulnar Loop. Fig. 5. Radial loop.

Fig. 6. Plain whorl. Fig. 7. Central pocket loop whorl Fig. 8. Double loop. Fig. 9. Accidental whorl.
captured over a period of two years.

Hourieh Fakourfar and Serge Belongie [25] devise a method to assess the effect of water-induced finger that degrade the performance of minutiae-based FR system. The test results show EER on dry finger 2.13% and wrinkled finger 3.15%. The True positive rate (TPR) 96.7% for dry finger and 72.4% for wrinkled finger is reported.

De-Song Wang et al. [26] propose FP based authentication method using mobiles. The method is better for computational complexity with Khan’s and Yoon-Yoo’s scheme.

Jing Luo et al. [27] describe a novel FR algorithm using Ellipsoidal basis function neural network (EBFNN). The test results on FVC2000/ FVC 2002/ FVC 2004 report the RR of 90.5% to 91.8%.

Mihai Hulea et al. [28] delineates a distributed FP identification and verification system which integrates FR and Global Positioning System methods.

S. Mill'stein et al. [29] reports very powerful algorithms for both full and partial fingerprints. The test result using Spacing Frequency Transform Algorithm (SFTA) based on the Fast Fourier Transform of the images and Line Scan Algorithm (LSA). The result reports 95% accuracy for partial FPs and 99% accuracy for full FPs.

Yong Nyuo Shin et al. [30] designs a prototype to provide authentication to medical staff. The prototype ensures reliable electronic medical record system.

Wang Yuan et al. [31] ascertain a FP minutiae matching scheme which involves vector matching with variable weight modification and local area matching process. The test result on FVC2002 database show lower FAR and same level of FRR, less recognition time and high reliability.

Faisal Farooq et al. [32] demonstrate a technique to convert FP into a binary string template using minutiae triplets. The test results show the EER=0% for verification, EER=1.59% for lost-token and EER=0% for cancel ability. The merits are registration points elimination and provide high security.

Gualberto Aguilar et al. [33] appraise FR concept using fusion of FFT (Fast Fourier Transform) and Gabor filters for enhancement of image. The test results show RR of 94.1%, FAR of 2.3% and FRR of 3.6%.

Aliaa A. A. Youssif et al. [34] exemplify an AFRS based on fusion of minutiae and correlation matching techniques. The test result on biometrics lab, Italy database report matching rate 98.5% to 100% in identical twins with different thresholds.

B. Y. Hiew et al. [35] comprehend a concept for FR using digital camera. The Gabor features obtained by the Gabor filters are compressed using PCA and then matching is performed with the help of cosine angle. It reports improved result in terms of segmentation, enhancement and core point detection.


Dingrui Wan and and Jie Zhou [37] use Decision level fusion scheme to combine density map matching with conventional minutiae based matching. The test results with THU and FVC2002 database show 98.8% RR as compared with singly minutiae based technique of 95.5%. The scheme overcomes the problems of spurious minutiae due to poor quality images.

T. Amornraksa and S. Tachaphetpi boon [38] formulate a method for FR based on the DCT features of a discrete image. The test results using k-nearest neighbour (k-NN) classifier show 100% RR and the low computational effort.

Jinwei Gu et al. [39] recommend a novel representation for FPs that includes both minutiae and model-based orientation field. The test results prove the proposed system is more accurate and robust and takes less than 0.30s for matching.

Naveena Marupudi et al. [40] depict multimodal biometrics using voice and FP. The novel method uses segmentation using morphological operations and minutiae marking using triple branch counting. The test results on FVC2002 and SDK 4.2 show 25% of FAR and FRR.

Ajita Rattani et al. [41] devise minutiae matching algorithm for multi biometrics, which reports RR of 91.82% with FAR=10.97% and FRR=5.38%.

Te-Jen Su et al. [42] reveal a FR system based on Cellular Neural Networks (CNN) algorithms. The results prove CNN is better than either continuity of line or degree of thinning.

Issam Dagher et al. [43] suggest a technique for FR using fuzzy ARTMAP neural network architecture. The test result on UOB (University Of Balamand) database report better identification accuracy.

Marius Tico et al. [44] adopt a method for FR using wavelet features. The test results with K-NN classifier show the RR of 98.1% to 100%. The method also provides security.

Chih-Jen Lee et al. [45] illustrate FR using local Gabor based method. The test result shows the proposed method have higher RR than global Gabor-based approach.

B. Security

Rajeswari Mukesh et al. [46] identify 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.

Ruyi Zheng et al. [47] appraise the problem of fast FP retrieval in a large database using clustering-based descriptors. The experimental results on NIST database using SVN classifiers and orientation image report the accuracy of 86.68% and fastest matching time 0.056s.

Emile J. C. Kelkboom et al. [48] analyse the cross matching performance of the auxiliary data AD of the Fuzzy Commitment Scheme (FCS). The result on MCYT database show that cross matching performance is not as good as system performance.

Lifeng Lai et al. [49] determine the performance of reusable biometric security systems, in which the same biometric information is reused in multiple locations is analysed.

Lifeng Lai et al. [50] evaluate the single-use biometric system under a privacy security trade off framework. The test results report adequate security.

Francis Minthang Bui et al. [51] explore various strategies related to key binding with QIM in a BE context are examined. The obtained results demonstrate that the QIM method facilitates tuning of the system performance.
P. Bera et al. [52] determine a complete security analysis framework. The proposed framework facilitates in debugging of network security implementation efficiently.

Maneesh Upmanyu et al. [53] formulate a provably secure and blind biometric authentication protocol, which addresses the concerns of user’s privacy, template protection and trust issues. Experimental results on four biometric datasets (face, iris, hand geometry, and FP) show that the authentication in the encrypted domain does not affect the accuracy. Tanya Ignatenko et al. [54] address the privacy leakage in biometric secrecy systems. Biometric part assures the authenticity of a user, while the cryptographic part provides strong secrecy and avoids privacy leakage.

Chun-I. Fan and Yi-Hui Lin [55] construct a three-factor authentication scheme which combines biometrics with passwords and smart cards to provide high-security.

Bon K. Sy [56] illustrates a practical secure data retrieval and authentication techniques for complex distributed systems. The test result report ERR=8%, FAR=13.7% and FRR=3.8%.

### III. DISCUSSION

The pursuits of knowledge on the diverse area of FP biometric systems envisage the importance of FP biometric system to provide strong authentication. The summary of our study shows that of the FR is having edge over other biometric traits. Table I depicts performance comparison of different biometric technologies based on parameters like EER, FAR and FRR. The enumerated result plays a pivotal role for establishing identity for the industry like law enforcement, forensic science community and with general public. This leads to the invention of next generation faster and higher quality acquisition devices.

<table>
<thead>
<tr>
<th>Biometric</th>
<th>EER (Equal Error Rate)</th>
<th>FAR (False Acceptance Rate)</th>
<th>FRR (False Rejection Rate)</th>
<th>Subjects</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Face</td>
<td>NA</td>
<td>1%</td>
<td>10%</td>
<td>57,437</td>
<td>varied light, indoor/outdoor</td>
</tr>
<tr>
<td>Finger print</td>
<td>2%</td>
<td>2%</td>
<td>2%</td>
<td>25,000</td>
<td>rotation and exaggerated skin distortion</td>
</tr>
<tr>
<td>Hand geometry</td>
<td>1%</td>
<td>2%</td>
<td>2%</td>
<td>129</td>
<td>with rings and improper placement</td>
</tr>
<tr>
<td>Iris</td>
<td>0.01%</td>
<td>0.94%</td>
<td>0.99%</td>
<td>1,224</td>
<td>indoor environment</td>
</tr>
<tr>
<td>Key strokes</td>
<td>1.8%</td>
<td>7%</td>
<td>0.1%</td>
<td>15</td>
<td>during 6 months period</td>
</tr>
<tr>
<td>voice</td>
<td>6%</td>
<td>2%</td>
<td>10%</td>
<td>30</td>
<td>text dependent and multilingual</td>
</tr>
</tbody>
</table>

### IV. CONCLUSION AND FUTURE ENHANCEMENT

This paper presented the related works and performance analysis for fingerprint biometric. The performance evaluation is done on surveyed works with different parameters and existing methods. Biometrics presents obvious advantages over password and token-based security. The survey study various issues related to uni-modal biometric systems is discussed. The security and privacy concerns that biometric authentication raises need to be addressed. It is surveyed 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


[18] P. Bera et al. [52] determine a complete security analysis frame work. The proposed framework facilitate in debugging of network security implementation efficiently.

[19] Maneesh Upmanyu et al. [53] formulate a provably secure and blind biometric authentication protocol, which addresses the concerns of user’s privacy, template protection and trust issues. Experimental results on four biometric datasets (face, iris, hand geometry, and FP) show that the authentication in the encrypted domain does not affect the accuracy. Tanya Ignatenko et al. [54] address the privacy leakage in biometric secrecy systems. Biometric part assures the authenticity of a user, while the cryptographic part provides strong secrecy and avoids privacy leakage.

[20] Chun-I. Fan and Yi-Hui Lin [55] construct a three-factor authentication scheme which combines biometrics with passwords and smart cards to provide high-security.

[21] Bon K. Sy [56] illustrates a practical secure data retrieval and authentication techniques for complex distributed systems. The test result report ERR=8%, FAR=13.7% and FRR=3.8%.


S. Ravi is now working as assistant professor in the Department of Computer Science, School of Engineering and Technology, Pondicherry University, Pondicherry from 2011 to till date. His research interests include Digital Image Processing, Face Detection and Face Recognition, Machine Vision and Pattern Recognition. He has published 49 research papers (23 - International Journals, 12 - IEEE International Conferences, 10 - International Conferences and 4 - National Conferences.), He is a member of the IEEE from 2006.

Dattatreya P. Mankame completed his M. Tech in Computer Science and Engineering from VTU, Belgua, Karnataka, India and currently pursuing Ph. D in Computer Science and Engineering at Pondicherry University. Pondicherry, India. He is presently working in the Information Science and Engineering department at K.L.E.Institute of Technology, Hubli, Karnataka, India since 2008. His research interests are Biometrics, Pattern Recognition. He is member of Computer Society of India (CSI) Bangalore Chapter.