Current Issues and Challenges of Fingerprint Recognition

Amirah Hanani Binti Mohamad Jamil
Bachelor of Computer Science (Media Interactive)
Universiti Teknikal Malaysia Melaka, Hang Tuah Jaya,
Durian Tunggal, Melaka, Malaysia
amirahhananij@gmail.com

ABSTRACT

As we familiar with, fingerprint recognition technique is the dominant technology in the biometric market. A number of recognition techniques have been used to perform fingerprint matching. Straight forward matching between the fingerprint pattern to be identified and most of us already knew patterns would not serve well due to its high sensitivity to errors (such as various noises, damaged fingerprint areas, or the finger being placed in different areas of fingerprint scanner window and with different orientation angles, etc.).

Keywords: Fingerprint Matching, Pattern-Based Method; Minutiae-Based Method; Current Issues;

1. Introduction

In an increasingly digital world, reliable personal authentication has become an important human computer interface activity. Fingerprint recognition is a complex pattern recognition problem. It is difficult to design accurate algorithms capable of extracting salient features and matching them in a robust way, especially in poor quality fingerprint images and when low-cost acquisition devices with small area are adopted. There is a popular misconception that automatic fingerprint recognition is a fully solved problem since it was one of the first applications of machine pattern recognition. On the contrary, fingerprint recognition is still a challenging and important pattern recognition problem. The patterns, which are aggregate characteristics of ridges, and minutia points, which are unique features found within the patterns. There are several methods of pattern recognition [1]. This paper provides extra patterns and based on those pattern minutiae features are calculated and show matching between fingerprints. Minutiae-based systems generally rely on finding correspondences between the minutia points present in “first” and “copy of first” fingerprint images. These systems normally perform well with high quality fingerprint images and a sufficient fingerprint surface area. This effect is even more marked on intrinsically poor quality fingers, where only a subset of the minutiae can be extracted and used with sufficient reliability.

2. Research Method

Fingerprint Recognition Techniques: The architecture of fingerprint recognition system can be divided into four phases: Image acquisition, Image enhancement process, Feature extraction from the enhanced image and Pattern matching process (Figure 1).

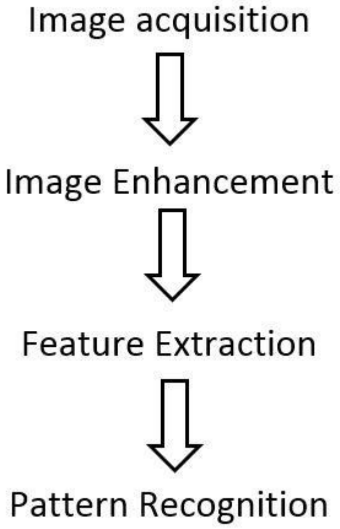

Figure 1, Steps to identify fingerprint image

A. Image acquisition

In this phase, image of Fingerprint is first acquired with the help of sensors. Captured images may be blurred or may contain noises, which Detroit the quality of an image and affect the performance of Fingerprint recognition system. The fingerprint image acquired may vary by location of finger placed, direction and stretching degree. [2]

B. Image Enhancement

After Image acquisition Image Enhancement will takes place. Sometimes image may be corrupted by various kind of noise such as creases, smudges and holes. Which is impossible to recover the true ridge/valley structures in the unrecoverable regions; any effort to improve the quality of the fingerprint image in these regions is pointless. Therefore, the reasonable enhancement algorithm is used to improve the clarity of ridges/valley structures of fingerprint images in recoverable regions and to mask out the unrecoverable regions, noise and missing minutiae etc. During process, noise can be removed with the help of filters utilized in processing/enhancement. The aim of this Image Enhancement phase is to provide the image of high quality. A high quality fingerprint image has the high contrast between the ridges and the valleys. A poor quality fingerprint image is low in contrast, noisy, broken, blur, missing minutiae. Techniques such as Grey-level smoothing, contrast stretching, histogram equalization, and Wiener filtering can be used as pre-processing steps before sophisticated fingerprint enhancement algorithm is applied [3] (Figure 2).

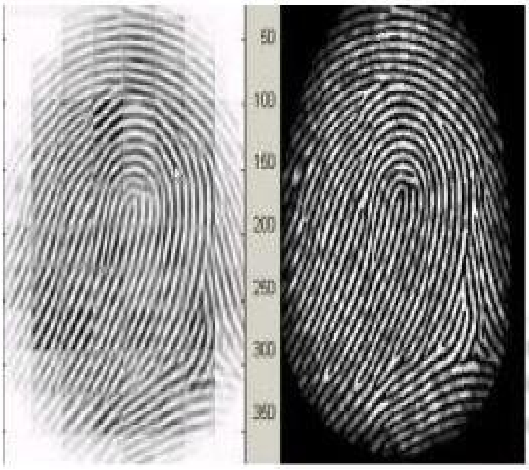

Figure 2, (a) Enhanced Image after Fast Fourier Transform (FFT), (b) Image before FFT

C. Feature Extraction:

Fingerprint pattern exhibits different types of fingerprint features [5]:

Level 1 (Global Level): When the ridges are parallel. They are classified as delta, loop and whorl which are representing in Figure 3.

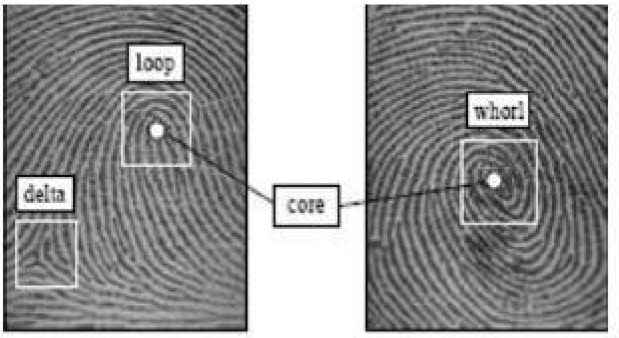

Figure 3, Delta, Loop, Whorl

i. Level 2 (Local Level): This is based on minutiae in which the ridges are not in order. They are classified as ridge ending, ridge bifurcation, lake, independent ridge, point or island, spur, crossover are shown in Figure 4.

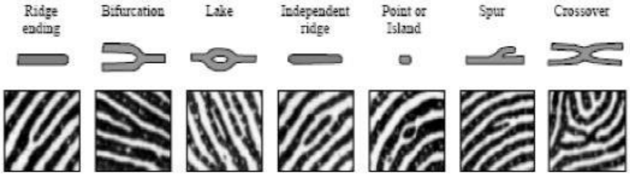

Figure 4, Ridge ending, Bifurcation, Lake, Independent ridge, Point or Island, Spur, Crossover

ii. Level 3 (Very Fine Level): Intra ridge details are detected. Sweat pores are showed at this level is shown in Figure 5.

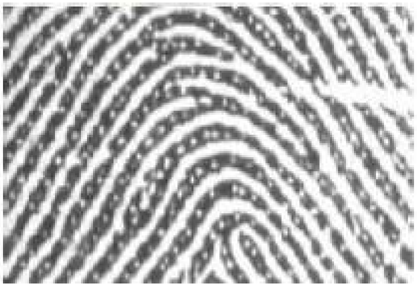

Figure 5, White pores are Sweat Pores.

D. Pattern Recognition

A pattern is an arrangement of descriptors. It is characterized by the order of the elements of which it is made, rather than by the intrinsic nature of these elements. Pattern recognition is divided into two parts: first one is Decision theoretic and second is Structural. The Decision theoretic deals with patterns described using quantitative descriptors, such as length, area, and texture. Structural category deals with patterns described by qualitative descriptors that are relational descriptors. Pattern recognition phase compare basic fingerprint patterns like a survey on Fingerprint Recognition Techniques 446 arch, whorl and loop between a candidate fingerprint and previously stored template. This requires that the images be aligned in the same orientation. In pattern recognition, the template has the type, size, and orientation of patterns within the fingerprint image [4, 3].

E. Fingerprint Matching

Fingerprint matching is the process used to determine whether two sets of fingerprint come from the same finger. One fingerprint is stored into the database and other is employee’s current

fingerprint. Minutiae point refers to the topical characteristic at the end point of the ridge part. The best way to compare fingerprints is to compare all visual information on the fingerprints. However, this is realistically impossible. Comparing all visual information requires too much data, and this is inappropriate to make a commercialized system. Actual commercialized systems do not store the fingerprint itself, but characteristics of the fingerprints, and codes related to the position of these points of characteristics. Since only characteristics are stored, they cannot be revived as fingerprint visuals, and therefore cannot be used as evidence in legal facilities
[2]

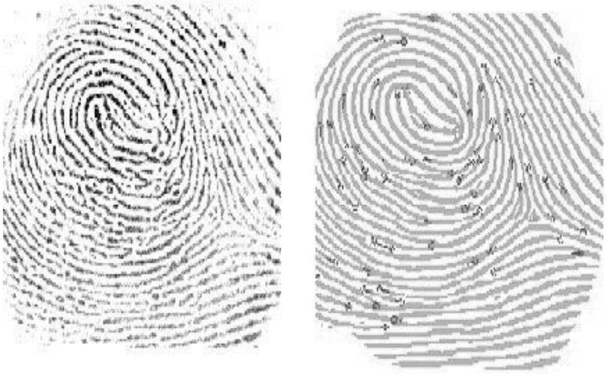

Figure 6, Fingerprint matching

The large number of approaches to fingerprint matching can be coarsely classified into three families.

1. **Correlation-based matching:**
   Two fingerprint images are superimposed and the correlation between corresponding pixels is computed for different alignments.
2. **Minutiae-based matching:**
   This is the one of the best technique. Minutiae are extracted from the two fingerprints and they can store as group of points in the two-dimensional manner. A minutia based matching consists of finding the alignment between the template and the input minutiae sets which results in maximum number of minutiae pairings.
3. **Pattern-based (or image-based) matching:**
   Pattern based matching compares two fingerprints. This requires that the images be aligned in the same orientation. In order to do this, the Pattern-based finds a middle point in the fingerprint image. In the image-based matching, the template contains the size, type and pattern orientation within the fingerprint image. The person fingerprint image is compared with the template to recognize the degree. Which focuses on implementation of minutiae based matching technique [3]. The full procedure is represented in Figure 6.

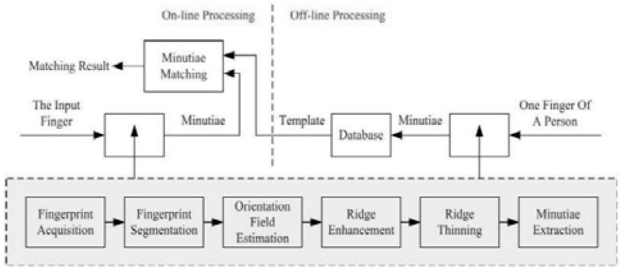

Figure 7. Implementation Procedure

Fingerprint Recognition System: Fingerprint identification is perhaps the oldest of all the biometric techniques. Fingerprints have a long history of use in police forensic science. Because of this, the authentication by fingerprint is the most convenient biometric element to identify a person. A large variety of solutions are already available and the technology is mature. Fingerprint technology can be used to authenticate a person versus a pin code when entered for an ATM/online debit transaction or a signature for a credit card transaction.

A verification system authenticates a person's identity by comparing the captured biometric characteristic with her own biometric template pre-stored in the system. An identification system recognizes an individual by searching the entire template database for a match.

3. Discussion

Lack of robustness against image quality degradation is one of the open issues in fingerprint verification [8, 9]. The performance is heavily affected by fingerprint image quality. It consists of several factors that determine the quality of a fingerprint image such as, skin conditions (e.g., dryness, wetness, dirtiness, temporary or permanent cuts and bruises), sensor conditions (e.g., dirtiness, noise, size), user cooperation, etc. Some of these factors cannot be avoided and some of them vary a long time. Poor quality images result in spurious and missed features that can degrade the performance of the overall system. Therefore, it is very important for a fingerprint recognition system to estimate the quality and validity of the captured fingerprint images. We can either reject the degraded images or adjust some of the steps of the recognition system based on the estimated quality. However, it has been found that simple fusion approaches are not always outperformed by more complex fusion approaches. Another recent issue in fingerprint recognition is the use of multiple sensors, either for sensor fusion [15] or for sensor interoperability [16, 10]. Fusion of sensors offers some important potentialities [15]:

a) The overall performance can be improved substantially.

b) Population coverage can be improved by reducing enrollment and verification failures

c) It may naturally resist spoofing attempts against biometric systems.

Regarding sensor interoperability, most biometric systems are designed under the assumption that the data to be compared is obtained uniquely and the same for every sensor, thus being restricted in their ability to match or compare biometric data originating from different sensors in practice. As a result, changing the sensor may affect the performance of the system. However, little effort has been invested in the development of algorithms to alleviate the problem of sensor interoperability. One of the example is the normalization of raw data and extracted features. As a future remark, interoperability scenarios should also be included in vendor and algorithm competitions. Due to the low cost and reduced size of new fingerprint sensors, several devices in daily use already include embedded fingerprint sensors (e.g., mobile telephones, PC peripherals, PDAs, etc.) However, using small-area sensors implies having less information available from a fingerprint and little overlap between different acquisitions of the same finger, which has great impact on the performance of the recognition system. Some fingerprint sensors are equipped with mechanical guides in order to constrain the finger position. Another alternative is to perform several acquisitions of a finger, gathering (partially) overlapping information during the enrollment, and reconstruct a full fingerprint image. In spite of the numerous advantages of biometric systems, they are also vulnerable to attacks [82]. Recent studies have shown the vulnerability of fingerprint systems to fake fingerprints [12, 21, 18, 20]. Surprisingly, fake biometric input to the sensor is shown to be quite successful. Aliveness detection could be a solution and it is receiving great attention [14, 23, 13]. It has also been shown that the matching score is a valuable piece of information for the attacker [24, 22, 19]. Using the feedback provided by this score, signals in the channels of the verification system can be modified iteratively and the system is compromised in a number of iterations. A solution could be given by concealing the matching score and just releasing an acceptance/rejection decision, but this may not be suitable in certain biometric systems [24]. With the advances in fingerprint sensing technology, new high resolution sensors are able to acquire ridge pores and even perspiration activities of the pores [17, 11]. These features can provide additional discriminative information to existing fingerprint recognition systems. In addition, acquiring perspiration activities of the pores can be used to detect spoofing attacks.

4. Conclusion

Despite all of the interest in fingerprint recognition systems, a number of serious concerns remain. The enrollment and matching performance can be poor, especially in real-world deployment situations, although combing multiple biometrics can improve performance a great deal. Usability and acceptance remains a problem, especially with certain populations (e.g., older people). In addition, the acceptance and success of a fingerprint recognition system is highly dependent on the context where it is being used, with the highest adoption and acceptance rates being found in situations where there is a direct and obvious benefit to the users (e.g., speeding border crossing). Also, the safe storage and privacy protection of biometric data is a serious worry for any large-scale deployment. All of these concerns should be considered by anyone considering adopting a fingerprint recognition system.

Bibliographies

[1] Ritu1 and Matish Garg2," A Review on Fingerprint-Based Identification System",Student, SBIET College, Pundri, Kaithal, India1Assistant Professor, SBIET College, Pundri, Kaithal, IJARCCE,Vol. 3, Issue 3, March 2014,India2

[2] 1Priyanka rani,2Pinki Sharma,"A Review Paper on Fingerprint Identification System ",IJARCST, Vol. 2, Issue 3 (July - Sept. 2014) Kaithal, Haryana, India

[3] Gurpreet Singh1 and Vinod Kumar2," Review On Fingerprint Recognition: Minutiae Extraction andMatching Technique",IJISR,Vol. 10 No. 1,pp. 64-70, Oct. 2014, Punjab, India

[4] Sangram Bana1 and Dr.Davinder Kaur2," Fingerprint Recognitionusing Image Segmentatio", IJAEST,Vol No. 5, IIT Roorkee, Roorkee

[5] Madhuri and RichaMishr," Fingerprint Recognition using Robust Local Features",IJARSSE,Volume 2, Issue 6, June 2012, INDIA.

[6] Introduction to Biometrics, http://ics1.mk.co.kr/file/cd104/biometrics1.pdf

[7] C.D'Souza, Leeda Jovita Rodrigues and Nausheeda B. "A survey On Fingerprint Recognition Techniques" Special Issue SACAIM 2016, pp. 441-447

[8] Simon-Zorita, D., Ortega-Garcia, J., Fierrez-Aguilar, J., Gonzalez-Rodriguez, J.: Image quality and position variability assessment in minutiae-based fingerprint verification. IEE Proceedings- Vis. Image Signal Process. 150(6), 402–408 (2003)

[9] Alonso-Fernandez, F., Fierrez, J., Ortega-Garcia, J., Gonzalez-Rodriguez, J., Fronthaler, H.,Kollreider, K., Bigun, J.: A comparative study of fingerprint image quality estimation methods. IEEE Trans. on Information Forensics and Security 2(4), 734–743 (2007)

[10] Alonso-Fernandez, F., Veldhuis, R., Bazen, A., Fierrez-Aguilar, J., Ortega-Garcia, J.: Sensor interoperability and fusion in fingerprint verification: A case study using minutiae- and ridge-based matchers. Proc. IEEE Intl. Conf. on Control, Automation, Robotics and Vision, ICARCV, Special Session on Biometrics (2006)

[11] Chen, Y., Jain, A.: Dots and incipient: Extended features for partial fingerprint matching. Proceedings of Biometric Symposium, Biometric Consortium
Conference (2007)

[12] Galbally-Herrero, J., Fierrez-Aguilar, J., Rodriguez-Gonzalez, J., Alonso-Fernandez, F., Ortega-Garcia, J., Tapiador, M.: On the vulnerability of fingerprint verification systems to fake fingerprint attacks. Proc. IEEE Intl. Carnahan Conf. on Security
Technology, ICCST (2006)

[13] Antonelli, A., Capelli, R., Maio, D., Maltoni, D.: Fake finger detection by skin distortion analysis. IEEE Trans. on Information Forensics and Security 1,
306–373 (2006)

[14] Derakhshani, R., Schuckers, S., Hornak, L., O'Gorman, L.: Determination of vitality from a non-invasive biomedical measurement for use in fingerprint scanners. Pattern Recognition 36, 383–396
(2003)

[15] Marcialis, G., Roli, F.: Fingerprint verification by fusion of optical and capacitive sensors. Pattern Recognition Letters 25, 1315–1322 (2004)

[16] Ross, A., Jain, A.: Biometric sensor interoperability: A case study in fingerprints. Proc. Workshop on Biometric Authentication, BIOAW LNCS-3087,
134–145 (2004)

[17] Jain, A., Chen, Y., Demirkus, M.: Pores and ridges: High resolution fingerprint matching using level 3 features. IEEE Trans. on Pattern Analysis and
Machine Intelligence 29(1), 15–27 (2007)

[18] Putte, T., Keuning, J.: Biometrical fingerprint recognition: dont get your fingers burned. Proc. IFIP TC8/WG8.8, Fourth Working Conf. Smart Card
Research and Adv. App. pp. 289–303 (2000)

[19] Martinez-Diaz, M., Fierrez-Aguilar, J.,
Alonso-Fernandez, F., Ortega-Garcia, J., Siguenza, J.: Hill-climbing and brute-force attacks on biometric systems: A case study in match-on-card fingerprint verification. Proc. IEEE Intl. Carnahan Conf. on
Security Technology, ICCST (2006)

[20] Matsumoto, T., Matsumoto, H., Yamada, K., Hoshino, S.: Impact of artificial gummy fingers on fingerprint systems. Proc. of SPIE, Optical Security and Counterfeit Deterrence Techniques IV 4677, 275–289
(2002)

[21] Ratha, N., Connell, J., Bolle, R.: An analysis of minutiae matching strength. Proc. International Conference on Audio- and Video-Based Biometric Person Authentication, AVBPA LNCS-2091,
223–228 (2001)

[22] Ratha, N., Connell, J., Bolle, R.: Enhancing security and privacy in biometrics-based authentication systems. IBM Systems Journal 40(3), 614–634 (2001)

[23] Schuckers, S., Parthasaradhi, S., Derakshani, R., Hornak, L.: Comparison of classification

methods for time-series detection of perspiration as a liveness test in fingerprint devices. Proc. International Conference on Biometric Authentication, ICBA, LNCS-3072, 256–263 (2004)

[24] Uludag, U., Jain, A.: Attacks on biometric systems: a case study in fingerprints. Proc. SPIEEI 2004, Security, Seganography and Watermarking of
Multimedia Contents VI pp. 622–633 (2004)

[25] Mrs. Hemlata Patel, Pallavi Asrodia “Fingerprint Matching Using Two Methods” Institute of
Technology Borawan, Khargone, India