A Survey on Fingerprint Matching Techniques

Dilip Tamboli
P.G. Scholar, Electronics & Telecomm Engg
SSGI Bhilai,
Chhattisgarh, India

Mr. Sandeep B Patil
Associate Professor, Electronics & Telecomm Engg
SSGI Bhilai,
Chhattisgarh, India

***Abstract*- Fingerprint matching is the process used to determine whether two sets of fingerprint ridge detail come from the same finger. Fingerprints are the oldest and most widely used form of biometric identification. Everyone is known to have unique, immutable fingerprints. However fingerprint images get degraded and corrupted due to variations in skin and impression conditions. Thus image enhancement techniques are employed prior to minutaie extraction and matching algorithm.**
Fingerprints, because of their uniqueness and other related characteristics are the most widely used & highly accepted biometrics.
So in this paper a review of different fingerprint matching techniques has been.

Keywords: Fingerprint, minutaie, unique, immutable, identification, extraction.

I. INTRODUCTION

Biometrics –

Biometrics is the science of verifying the identity of an individual through physiological measurements or behavioral traits. Since biometric identifiers are associated permanently with the user they are more reliable than token or knowledge based authentication methods. Biometrics offers several advantages over traditional security measures. These include

Non-repudiation: With token and password based approaches, the perpetrator can always deny committing the crime pleading that his/her password or ID was stolen or compromised even when confronted with an electronic audit trail. There is no way in which his claim can be verified effectively

Accuracy and Security: Password based systems are prone to dictionary and brute force attacks. Furthermore, such systems are as vulnerable as their weakest password. On the other hand, biometric authentication requires the physical presence of the user and therefore cannot be circumvented through a dictionary or brute force style attack.

Screening: In screening applications, we are interested in preventing the users from assuming multiple identities (e.g. a terrorist using multiple passports to enter a foreign country). This requires that we ensure a person has not already enrolled under another assumed identity before adding his new record into the database. Such screening is not possible using traditional authentication mechanisms and biometrics provides the only available solution. The various biometric modalities can be broadly categorized as

Physical biometrics: This involves some form of physical measurement and includes modalities such as face, fingerprints, iris-scans, hand geometry etc.

Behavioral biometrics: These are usually temporal in nature and involve measuring the *way* in which a user performs certain tasks. This includes modalities such as speech, signature, gait, keystroke dynamics etc.

Chemical biometrics: This is still a nascent field and involves measuring chemical cues such as odor and the chemical composition of human perspiration.

Many classifications are given to patterns that can arise in the ridges and some examples are given in the figure 1.1 to the right.

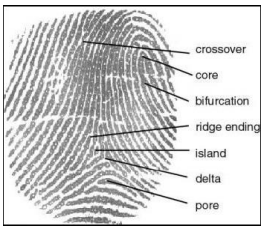

Figure 1.1 Minutiae features

Fingerprint is one of the important and most widely used biometric system in the modern automated world where machines are replacing the human in almost every aspect of life.

These points are also known as the minutiae of the fingerprint. The most commonly used minutiae in current fingerprint recognition technologies are ridge endings and bifurcations because they can be easily detected by only looking at points that surround them

Minutiae based fingerprint authentication systems are widely used by both human experts and machines. These systems usually rely on “local discontinuities in the ridge flow pattern” called minutiae. According to the empirical study, two individuals will not have more than seven common minutiae. The set of minutiae are restricted into two types Ridge endings and Ridge bifurcations. Ridge endings are the points where the ridge curve terminates, and ridge bifurcations are the points where a ridge splits from a single path to two paths at a Y-junction. The positions and angular orientations of these points within a fingerprint uniquely characterize the fingerprint. In an increasingly digital world, reliable personal authentication has become an important human computer interface activity. National security, e-commerce, and access to computer networks are some examples where establishing a person’s identity is vital.

A fingerprint is the feature pattern of one finger as shown in figure 1.2. It is an impression of the friction ridges and furrows on all parts of a finger. These ridges and furrows present good similarities in each small local window, like parallelism and average width.

Figure 1.2 Fingerprint image from a sensor

However, shown by intensive research on fingerprint recognition, fingerprints are not distinguished by their ridges and furrows, but by features called Minutia, which are some abnormal points on the ridges as shown in figure 1.3. Among the variety of minutia types reported in literatures, two are mostly significant and in heavy usage:

- Ridge ending - the abrupt end of a ridge
- Ridge bifurcation - a single ridge that divides into two ridges

Figure 1.3(a) two important minutia features (b) Other minutiae features

A fingerprint is the representation of the epidermis of a finger. At a macroscopic analysis a fingerprint is composed of a set of ridge lines which often flow parallel and sometimes produce local macro singularities called **whorl, loop & delta**. Which is shown in figure 1.4

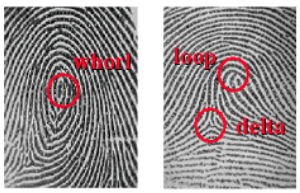

Figure 1.4 Whorl, loop and delta

II. Related Work

A. *BIOMETRIC SECURITY: FROM 1950-2012*

The term “Biometrics” is derived from the Greek words “bio” (life) and “metrics” (to measure) (Rood and Hornak, 2008). Automated biometric systems have only become available over the last few decades, due to the significant advances in the field of computer and image processing. Although biometric technology seems to belong in the twenty first century, the history of biometrics goes back thousands of years. The ancient Egyptians and the Chinese played a large role in biometrics history. Today, the focus is on using biometric face recognition, iris recognition, retina recognition and identifying 34 characteristics to stop terrorism and improve security measures. This section provides a brief history on biometric security and fingerprint recognition geometry was implemented successfully at the Olympic Games and the system implemented was able to handle the enrollment of over 65,000 people. Drs. Leonard Flom and Aran Safir, in 1985, found out that no two irises are alike and their findings were awarded a patent during 1986. In the year 1988, the first semi-automated facial recognition system was deployed by Lakewood Division of Los Angeles Country Sheriff's Department for identifying suspects (Angela, 2009). This was followed by several land marked contributiona by Sirovich and Kirby (1989), Turk and Pentland (1991), Philipis et al. (2000) in the field of face recognition. The next stage in fingerprint automation occurred at the end of 1994 with the Integrated Automated Fingerprint Identification System (IAFIS) competition

III. Fingerprint Matching Techniques

Fingerprint matching refers to finding the similarity between two given fingerprint images. The choice of the matching algorithm depends on which fingerprint representation is being used. Typically, a matching algorithm first attempts to recover the translation, rotation and deformation parameters between the given image pair and then determines the similarity between the two images. Fingerprint matching is considered a challenging problem due to the noise in the fingerprint images, large intra-class variation and small interclass variations between different impressions of the same finger. As each authentication application has different performance requirement, there is a need to continually improve the matching performance of the current systems. This section reviews some of the reported matching algorithms. The available matching algorithms can be broadly classified into three categories depending on the type of features used. They are

- Correlation based matching
- Minutia based matching
- Ridge feature based matching

A. *Correlation Based Matching*

In order to match two fingerprints using the correlation based technique, the fingerprints are aligned and the correlation is computed for each corresponding pixels, however, as the displacement and rotation are unknown it is necessary to apply the correlation for all possible alignments. The singularity information may be useful in order to find an approximated alignment. The main drawback of this method is its computational complexity and less tolerance to non-linear distortion and contrast variation. This method has several disadvantages.

i It fails if the images are highly distorted. The distortion is more pronounced in global fingerprint patterns; thus considering the local regions can minimize distortion to some extent. Bazen et al. (2000) and Nandakumar and Jain (2004) present some approaches to localized correlation-based matching.

ii Increased complexity: The computational complexity of this method is high. This problem can be solved by using Fourier domain method (Coetzee and Botha, 1993) and Fourier-Mellin transformation (Sujan and Mulqueen, 2002).

B. *Minutia Based Methods*

This is the most popular and is widely used in commercial applications, because of its good performance and low computation time, especially for good quality images. This method tries to align the minutiae of the input image (query template) and stored templates (reference template) and find the number of matched minutiae. After alignment, two minutiae are considered in matching if the spatial distance

and direction difference between them are smaller than a given tolerance. A correct aligning of fingerprint is very important in order to maximize the number of matched minutiae.

C. Ridge Feature Based Matching

A matching using the ridge feature in form of finger code consists of computing the difference of two finger code vectors (query and reference). However, before applying the finger code, it is important to align the fingerprint images, which is really a big problem, as in the case of other methods. In some cases the singularity may be used for that purpose. A finger code also may be used as a complementary to minutia based method in order to improve the overall matching accuracy. The original approach of this method used circular finger codes, considering as center the core point

IV. CONCLUSIONS

Fingerprint matching system is widely used in forensic applications like criminal investigation, terrorist identification and other security issues. Eventually fingerprint matching will be used to secure the safety and reliability of a variety of business in the industrial sector, including the personal devices and financial industry. The comparison is made with three different state-of-the-art fingerprint matchers. The additional automatically extracted features will include to improve the matching performance without an increase in manual labor.

REFRENCES

[1] Heeseung Choi, Kyoungtaek Choi, and Jaihie Kim, June 2011, Fingerprint Matching Incorporating Ridge Features With Minutia, IEEE Transactions On Information Forensics And Security, 6(2), 338-345.

[2] Jianjiang Feng, 2008, Combining minutiae descriptors for fingerprint matching, IEEE Transactions on Information Forensics and Security Pattern Recognition, 41 (9), 342 – 352.

[3] Anil K. Jain, Jianjiang Feng, Abhishek Nagar and Karthik Nandakumar, 2008,On Matching Latent Fingerprints, IEEE Transactions On Pattern Analysis And Machine Intelligence, 5(2), 1-8.

[4] Prabhakar, S, Jain, A.K, Jianguo Wang, Pankanti S, Bolle, 2011, Minutia Verification and Classification for Fingerprint Matching, International Conference on Pattern Recognition, 1(5), 25-29.

[5] Anil K. Jain, Salil Prabhakar, Lin Hong, and Sharat Pankanti, "Filter bank-based fingerprint matching," *IEEE Transactions on Image Processing*, vol. 9, no. 5, pp. 846–859, May 2000.

[6] Anush Sankaran, Tejas I. Dhamecha, Mayank Vatsa and Richa Singh, 2011, On Matching Latent to Latent Fingerprints in Proc, Int. Joint Conf.Biometrics, 1-6.

[7] Hrechak, AK and McHugh, JA. Automated fingerprint recognition using structural matching, Pattern Recognition, vol.23, no.8, 1990, pp.893-904. UK.

[8] Jain, A., Lin, H. and Bolle, R., On-line fingerprint verification, IEEE Transactions on Pattern Analysis & Machine Intelligence, vol.19, no.4, April 1997, pp.302-14. Publisher: IEEE Comput. Soc, USA.

[9] Jiang, X., Yau, W., Fingerprint minutiae matching based on the local and global structures, Proceedings 15th International Conference on Pattern Recognition. ICPR- 2000. IEEE Comput. Soc. Part, vol.2, 2000, pp.1038-41 vol.2. Los Alamitos, CA, USA.

[10] Zhiguo Yang, Yashuo Li, Yilong Yin, Xuzhou Li, 2012, a Template Selection Method Based on Quality for Fingerprint Matching, 9th International Conference on Fuzzy Systems and Knowledge Discovery (FSKD), IJECCT, 7(10), 1382-1385.

[11] Bal, A. M. El-Saba, and M. S. Alam, 2005, Improved fingerprint identification with supervised filtering, enhancement, Appl. Opt. **44**(5), 647–654.

[12] V. K. Vijaya Kumar, A. Mahalanobis, and R. D. Juday,2005, Correlation Pattern Recognition,Cambridge,University, 8(2), 295–356

[13] Choonwoo Ryu, Hakil Kim and Anil K. Jain, 2006, Template Adaptation based Fingerprint Verification to appear in Proc. of ICPR, 1-4.

[14] Maltoni, D. Maio, A. K. Jain, and S. Prabhakar, 2009, Handbook of Fingerprint Recognition, Springer, 4(5), 167–233.

[15] Jinwei GU, Jie Zhou and Chunyu Yang, July 2006, Fingerprint Recognition by Combining Global Structure and Local Cues, IEEE Transactions On Image Processing, 15(7), 1952-1964