Comparative Study on Finger Print Matching Algorithms

[1]*ANKAMMA RAO PAMULAPATI*, [2]*R. JEYA*
[1]M.Tech, SRM University, Email: ank_pamulapati@yahoo.com.
[2] Asst. Prof, Department of Computer science and Engineering, M.Tech,
SRM University, Email: jeya.r@ktr.srmuniv.ac.in

ABSTRACT- Fingerprints are the most popular and studied biometric characteristics. Their stability and uniqueness make fingerprint identification system extremely reliable and useful for security applications. This paper addresses the issue of selecting an optimal algorithm for fingerprint to design a system that matches the needed specifications in performance and correctness. Two approaches have been discussed in this document based on minutiae located in a fingerprint and based on the contents of the frequency and ridge of the ridge of a fingerprint.

Keywords—Biometrics, Fingerprints, Minutiae Extraction

1.INTRODUCTION

Conventional security systems utilized either knowledge based methods (passwords or PIN), and token-based methods (passport, driver license, ID card) and were prone to scam because PIN numbers could be forgotten or hacked and the tokens could be lost, duplicated or stolen. To address the requirement for robust, reliable, and foolproof personal identification, authentication systems will essentially need a biometric component.

The word “biometrics " comes from the Greek language and is derived from the words bio (life) and metric (to measure). Biometric systems utilize the physical characteristics of a person (such as fingerprints, iris or veins) or behavioral characteristics (such as voice, handwriting or typing rhythm) to decide their identity or to confirm that they are who they claim to be. Biometric technology most widely utilized is the fingerprint system. Indeed, the fingerprint can be utilized to change the PIN or password in most aspects of security. Fingerprints can be utilized instead of PIN in smart card applications, passwords on workstations, etc. Much researches on fingerprint technology are underway worldwide. There are two types of fingerprint systems: fingerprint verification and identification. The verification system is mapped one-to- one, and is based on the comparison of two groups of minutiae, correspondingly corresponding to two fingers to compare. It is essentially the identity verification since you must enter some information about yourself; the information is verified using your fingerprint.

The fingerprint identification system, on the other hand, is a one-to -many matching. A database of extracted fingerprint features is utilized to recognize and verify the input fingerprint.

Enrollment and authentication are the two main processes involved in a biometric security system. Upon enrollment, biometric measurements are captured from a subject and related information from the raw measurements is gleaned by the feature extractor, and this information is stored on the database. During authentication, biometric information is detected and compared with the database using pattern recognition techniques which involve a feature extractor and a biometric matcher working in cascade. A typical automated biometric-based identification system consists of six main components shown in Figure 1.

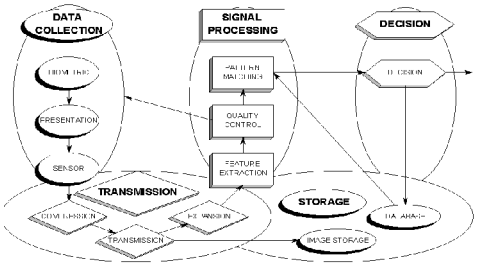

Fig. 1 A generic biometrics-based system

The data gaining component obtains biometric data in digital format using a sensor. The second and third components of the system are optional, depending on the storage requirements of the system. The fourth component uses a feature extraction algorithm to generate a feature vector whose components are digital characterization of the underlying biometrics. The fifth component of the system is the matcher that compares the feature vectors to produce a score that indicates the degree of similarity between the pair of biometric data under consideration. The sixth component of the system is a decision maker that can be programmed to accommodate the system specifications. System performance and accuracy is mainly determined by two parameters - FAR and FRR. A real person could be wrongly recognized as an impostor. This scenario is referred to as “false rejection” and the corresponding error rate is called the false rejection rate (FRR), an impostor could also be wrongly recognized as authentic. This scenario is referred to as "false accept” and the corresponding error rate is called the false acceptance rate (FAR). FAR and FRR are widely used measurements in today’s commercial environment.

2. CLASSES OF FINGERPRINT

Galton-Henry classification system accounts for more than 120 fingerprint classes. The five most common classes are:

• Arch: ridges enter from one side, rise to form a small bump, then go down and to the opposite side. No loops or delta points are present.

• Tented Arch: similar to the arch except that at least one ridge has high curvature, thus one core and one delta points.

• Left loop: one or more ridges enter from one side, curve back, and go out the same side they entered. Core and delta are present.

• Right loop: same as the left loop, but different direction.

• Whorl: contains at least one ridge that makes a complete 360 degree path around the center of the fingerprint. Two loops (same as one whole) and two deltas can be found.

• Fingerprints in databases are non-uniformly distributed in these classes. The natures proportion was presented in the slides (see the table) last time.

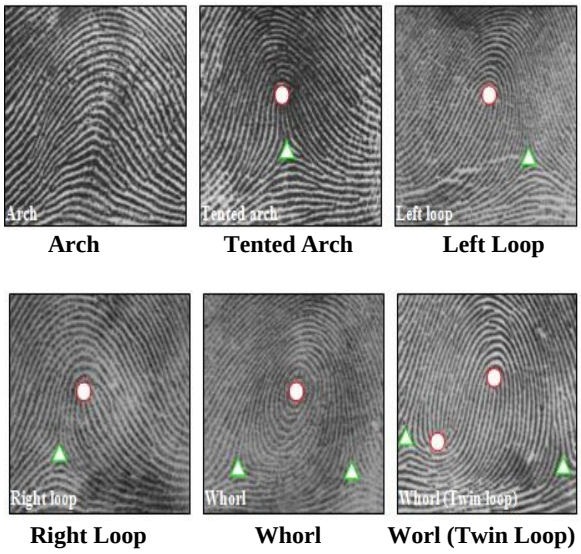

Fig. 2 Classes of fingerprint

Techniques fingerprint classification have been a subject of research for over 30 years. Many classification methods have been developed. Though, most of them utilize the same set of features: ridge line flow, image orientation, singular points, and Gabor filter responses. Orientation image contains all the information necessary to classify fingerprints into five broad classes listed above.

3. Fingerprint Recognition

Archaeologists discovered fingerprints pressed into clay tablet contracts dating back to 1792–1750 b.c. in Babylon as shown in figure (3). In ancient China, it was common practice to use inked fingerprints on all official documents, such as contracts and loans. The oldest known document showing fingerprints dates from the third century b.c. Chinese historians have found finger and palm prints pressed into clay and wood writing surfaces and surmise that they were used to authenticate official seals and legal documents.

Figure 3. Babylon fingerprints

As soon as fingerprints were discovered to be a reliable means of identification, criminals began to devise ways to alter them so they could avoid being identified. Two important facts of fingerprint that have risen from researches and practices are: a person's fingerprint will not naturally change structure after about one year after birth and the fingerprints of individuals are unique.

Fingerprint recognition is one of the most well-known and popular personal identification and security, because of their uniqueness and easy to use. Fingerprint recognition or fingerprint authentication refers to the automated method of verifying a match between two human fingerprints. fingerprint recognition system is the most matured and accepted biometric system. Fingerprints are one of many forms of biometrics used to identify individuals and verify their identity. Latent fingerprints are not visible, but techniques can bring them out. Dusting surfaces such as drinking glasses, the faucets on bathroom sinks, telephones, and the like with a fine carbon powder can make a fingerprint more visible.

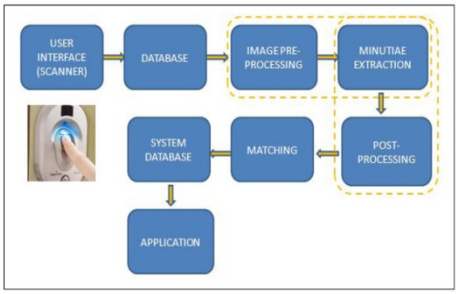

Fig.4: General process of finger print recognition

The fingerprint recognition problem can be grouped into three sub-domains: fingerprint enrollment, verification and fingerprint identification. In addition, different from the manual approach for fingerprint recognition by experts, the fingerprint recognition here is referred as AFRS (Automatic Fingerprint Recognition System), which is program-based.

Verification is typically used for positive recognition, where the aim is to prevent multiple people from using the same identity. Fingerprint verification is to verify the authenticity of one person by his fingerprint. There is one-to one comparison in this case. In the identification mode, the system recognizes an individual by searching the templates of all the users in the database for a match. Therefore, the system conducts a one to-many comparison to establish an individual's identity.

The following are Fingerprint Recognition Techniques:

A. Minutiae Extraction Technique

Most finger scanning technologies are based on Minutiae. Minutia-based techniques represent the fingerprint by its local characteristics, such as layoffs and bifurcations. This approach has been widely studied, is also the backbone of the products currently available fingerprint recognition. This is the most popular and widely used technique, being based on the comparison of the fingerprints made by fingerprint examiners. Minutiae extracted from the two fingerprints, and stored as a series of points in the two-dimensional plane. Minutiae-based matching essentially consists of finding the alignment between the template and the input minutiae sets those results in the maximum number of minutiae pairings.

B. Pattern Matching or Ridge feature based Techniques features extraction and template generation are based on a series of ridges as opposed to discrete points that constitute the basis of technical pattern matching. The advantage of pattern matching techniques on minutiae extraction is that the minutiae points can be affected by wear and disadvantages are that they are sensitive to the proper placement of

the finger and require for large storage templates.

Pattern based algorithms compare the basic fingerprint patterns (arch, whorl and loop) between a previously stored template and a candidate fingerprint. This needs that the images are aligned in the same orientation. To do this, the algorithm finds a central point in the fingerprint image and focuses on it. In a pattern-based algorithm, the template contains the type, size and orientation patterns in the fingerprint image alignment. The image of the candidate fingerprint is graphically compared with the template to determine the degree to which they correspond.

C. Correlation Based Technique

Two fingerprint images are superimposed and the correlation between corresponding pixels is computed for different alignments (e.g. various displacements and rotations). The cross-correlation is a well-known measure of image similarity and the maximization in (1); it allows us to find the optimal registration. The direct application of (1) rarely leads to acceptable results, mainly due to the following problems:
i) Non-linear distortion makes impressions of the same finger significantly different in terms of global structure; the use of local or block-wise correlation techniques can help to deal with this problem.
ii) Skin condition and finger pressure cause image brightness, contrast, and ridge thickness to vary significantly across different impressions. The use of more sophisticated correlation measures may compensate for these problems.
iii) A direct application of (1) is computationally very expensive. Local correlation and correlation in the Fourier domain can improve efficiency.

4. Design Based On Minutiae Extraction

Most automatic systems for fingerprint comparison are based on minutiae matching Minutiae are local discontinuities in the fingerprint pattern. A total of 150 different minutiae types have been identified. In practice only ridge ending and ridge bifurcation minutiae types are used in fingerprint recognition. Examples of minutiae are shown in figure 5.

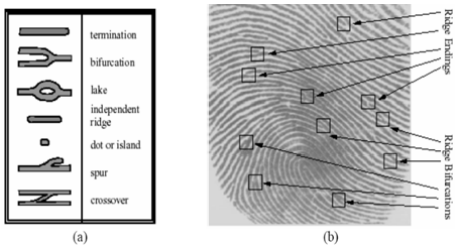

Fig. 5. (a) Different minutiae types, (b) Ridge ending & Bifurcation

The building blocks of a fingerprint recognition system are as follows (as shown in fig. 6):

A. Image Acquisition

A number of methods are used to acquire fingerprints. Among them, the inked impression method remains the most popular one. Inkless fingerprint scanners are also present eliminating the intermediate digitization process.

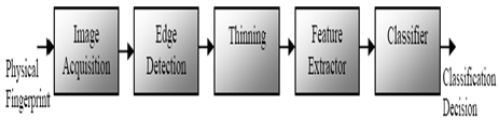

Fig. 6. Fingerprint Recognition System

B. Edge Detection

An edge is the boundary between two regions having the properties of relatively distinct gray level. The idea underlying most edge-detection techniques is the computation of a local derivative operator as "Roberts", "Prewitt 'or 'Sobel' operators.

C. Thinning

An important approach to representing the structural shape of a plane region is to reduce it to a graph. This reduction may be accomplished by obtaining the skeleton of the region via thinning (also called skeletonizing) algorithm.

The thinning algorithm while deleting unwanted edge points should not:
• Remove end points.
• Break connectedness.
•Cause excessive erosion of the region.

D. Feature Extraction

A multilayer perception (MLP) of three layers is trained to detect the minutiae in the thinned fingerprint image of size 300x300. The first layer of the network has nine neurons associated with the components of the input vector. The hidden layer has five neurons and the output layer has one neuron. The network is trained to output a "1" when the input window in centered on a minutiae and a "0" when it is not.

The networking will be trained using:
• The back propagation algorithm with momentum and learning rate of 0.3.
• The Al-Alaoui back propagation algorithm.
E. Classifier
After scanning the entire fingerprint image, the resulting output is a binary image revealing the location of minutiae. In order to prevent any falsely reported output and select "significant" minutiae, two more rules are added to enhance the robustness of the algorithm:
1) At those potential minutiae detected points, we reexamine them by increasing the window size by 5x5 and scanning the output image.
2) If two or more minutiae are too close together (few pixels away) we ignore all of them.

5. Design Based On Gabor Filter

Most methods for identifying fingerprint minutiae using the characteristics of fingerprints. For small scale fingerprint recognition system, it would not be effective to go through all stages of preprocessing (edge detection, smoothing, slimming ... etc), instead of Gabor filters are used directly to extract the characteristics from the fingerprint gray level as shown in FIG 5. No preprocessing step is needed before extracting features.

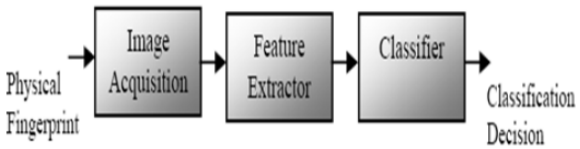

Fig. 6. Building blocks for the Gabor approach

A. Image Acquisition
The procedure is the same explained in the 1st approach.

B. Feature Extractor
Gabor filter based features have been successfully and widely applied to face recognition, pattern recognition and fingerprint enhancement.

C. Classifier
The classifier is based on the k-nearest neighborhood algorithm KNN. "Training" of the KNN consists simply of collecting k images per individual as the training set. The remaining images consists the testing set.

The classifier finds the *k* points in the training set that are the closest to *x* (relative to the Euclidean distance) and assigns *x* the label shared by the majority of these k nearest neighbors. Note that *k* is a parameter of the classifier; it is typically set to an odd value in order to prevent ties.

D. Suggested Enhancement
In order to enhance the performance of the 2nd approach below is a list of proposed ideas:
• Instead of using only the magnitude Gabor filter features, try to use also the phase of the filter.
• Try to other classifiers such as back propagation and ALBP. Indicate the number of layers used as well as the number of neurons. The Gabor filter assumes a sinusoidal plane wave.

6. CONCLUSION

The issue of selecting an optimal algorithm for fingerprint matching in order to design a system that matches the expectations of performance and precision is of great concern to designers. In order to attain a desired accuracy and performance of the system, two methods have been widely used, first is minutiae and second one is Gabor filter based. Minutiae are local discontinuities in the fingerprints pattern. For small scale fingerprint recognition system, it would not be effective to undergo all stages of pre-processing (edge detection, smoothing, thinning etc. also as technical minutiae-based) instead Gabor filters are used to extract features directly from the gray level fingerprint. The Gabor filter method is widely accepted approach to the comparison of fingerprints.

7. REFERENCES

[1] Bolle R, Connell J, et al. Guide to Biometrics, Springer, 2003.

[2] Jain LC, Intelligent Biometric Techniques in Fingerprint and Face Recognition, CRC Press, 1999.

[3] Maltoni D, Jain A K, Maio D, Prabhakar S, Handbook of Fingerprint Recognition, Springer, 2004.

[4] Vacca JR, Biometric Technologies and Verification Systems, Butterworth-Heinenmann, 2007.

[5] Munir, M. U., Javed, M. Y., "Fingerprint Matching using Gabor Filters," 2005.

[6] NTSC Subcommittee on Biometrics, "Fingerprint Recognition", 2000.

[7] http://www.isc365.com/ Biometrics_Security_Vs_Convenience.aspx

[8] http://www.csse.uwa.edu.au/ ~pk/Research/MatlabFns

[9] http://biometrics.cse.msu.edu/ fingerprint.html.

[10] http://basis.csr.unibo.it/fvc2002/.

[11] Megha Kulshrestha, Pooja and V. K. Banga "Selection of an Optimal Algorithm for Fingerprint Matching"

Authors:

1) ANKAMMA RAO PAMULAPATI
Student, M.Tech CSE Dept.,
SRM University, Chennai, India.
Email: ank_pamulapati@yahoo.com.

2) R. JEYA
Asst. Prof, CSE Dept., M.Tech,
SRM University, Chennai, India.
Email: jeya.r@ktr.srmuniv.ac.in.