Components of Fingerprint Biometric System

Ms. Meghna B. Patel
Asst. Professor,
MCA, UVPCE
Ganpat University, Kherva.

Mr. Ronak B. Patel Inchrge
Principal,
Shri C. J. Patel College of
Computer Studies, Visnagar.

Dr. Ashok R. Patel
Prof. & Head,
Department of Computer
Science,
HNGU, Patan.

Abstract

The term "biometrics" is derived from the Greek words "bio" (life) and "metrics" (to measure). Automated biometric systems have only become available over the last few decades, due to significant advances in the field of computer processing. Many of these new automated techniques, however, are based on ideas that were originally conceived hundreds, even thousands of years ago. In the field of authentication today, there are currently three methods to authenticate oneself to another person or a system.

(1) Knowledge-Based ('what you know')

(2) Object-Based ('what you have')

(3) ID-Based/Biometric-Based ('who you are')

Biometric authentication is automated method of identifying a person or verifying the identity of a person based on a physiological or behavioral characteristic. A biometric authentication can possible through Fingerprint recognition, Face recognition, Iris, Hand Geometry, Voice recognition, Dynamic Signature, Keystroke, Retina, Gait, Facial Thermograph etc. Due to the variety of different biometrics available, the generic architecture for a fingerprint biometric System can be split into the following logical structural components:

(1) Biometric Capture Device
(2) Biometric Template Store
(3) Result Generator

Keywords *- Biometric Authentication, Biometric Capture Device, Biometric Template Store, Result Generator*

1. Introduction

There are different biometrics like fingerprint, face, Voice etc available and different system architectures can be also built for different biometrics, A generic architecture for Fingerprint biometric system is shown in following Figure 1. It can be divided into following parts.

(1) Biometric Capture Device
(2) Biometric Template Store
(3) Result Generator

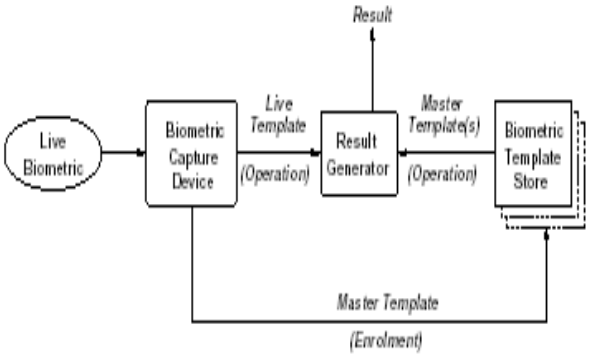

Figure 1. Logical components of a generic biometric system

2. Biometric Capture Devices

The following sections describe the function of each component of a fingerprint capture device.

2.1. Scanning
2.2. Pre-Processing and Feature Extraction
2.3. Template Creation

2.1. Scanning

For fingerprints there are numbers of alternative data capture devices. The main objective of a fingerprint scanner, regardless of the method it uses, is to provide the system with an image of the fingerprint that is as accurate as possible. For most applications, the image is produced at a resolution of 500 dpi using an 8-bit grey-scale. The different kinds of fingerprint scanners are as below.

(1) Optical
(2) Capacitance
(3)Thermal
(4)Pressure
(5) Ultrasound

2.2. Pre-Processing and Feature Extraction

The fingerprint pattern, when analyzed at different scales, exhibits different types of features.

At the global level, the ridge line flow delineates a pattern similar to one of those shown in Figure 2. Singular points, called loop and delta (denoted as squares and triangles, respectively in Figure 2), are a sort of control points around which the ridge lines are "wrapped". Singular points and coarse ridge line shape are very important for fingerprint classification, but their distinctiveness is not sufficient for accurate matching. External fingerprint shape, orientation image, and frequency image also belong to the set of features that can be detected at the global level.

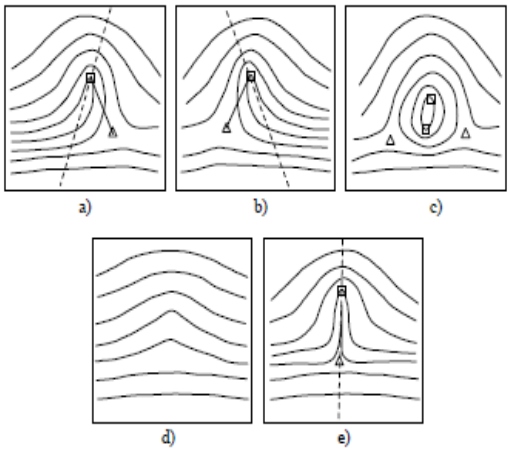

Figure 2. Fingerprint patterns as they appear at a coarse level: a) left loop; b) right loop; c) whorl; d) arch; and e) tented arch; squares denote loop-type singular points, and triangles deltatype singular points.

At the local level, a total of 150 different local ridge characteristics, called minute details, have been identified. These local ridge characteristics are not evenly distributed. Most of them depend heavily on the impression conditions and quality of fingerprints and are rarely observed in fingerprints. The two most prominent ridge characteristics, called minutiae (see Figure 3), are: ridge termination and ridge bifurcation. A ridge ending is defined as the ridge point where a ridge ends abruptly. A ridge bifurcation is defined as the ridge point where a ridge forks or diverges into branch ridges. Minutiae in fingerprints are generally stable and robust to fingerprint impression conditions. Although a minutiae-based representation is characterized by a high saliency, a reliable automatic minutiae extraction can be problematic in low-quality fingerprints (hence the suitability of this kind of representation is not optimal).

At the very-fine level, intra-ridge details can be detected. These are essentially the finger sweat pores (see Figure 3) whose position and shape are considered highly distinctive. However, extracting pores is feasible only in high-resolution fingerprint images (e.g., 1000 dpi) of good quality and therefore this kind of representation is not practical for most applications.

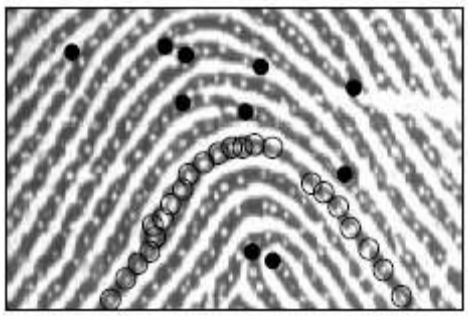

Figure 3. Minutiae (black-filled circles) in a portion of fingerprint image; sweat pores (empty circles) on a single ridge line.

After a fingerprint image has been captured using the scanner, it is rarely of sufficient quality to begin feature extraction. Due to variability in the capture process caused by humidity, dirt, oil, lighting or other similar factors (depending on the scanner used), the image needs to be enhanced to provide an accurate image. After it has been enhanced the appropriate minutiae points can be extracted. The following steps (in no particular order) are the basic steps that may be utilized before a template can be created.

2.2.1. Image binarisation
2.2.2. Ridge thinning
2.2.3. Ridge orientation estimation
2.2.4. Ridge smoothing
2.2.5. General image enhancement

2.2.6. Singularity detection
2.2.7. Minutiae point extraction
2.2.8. Spurious minutiae removal

The reason that the two tasks, pre-processing and feature extraction, have been combined in this section is that the exact division of the steps involved in these processes is not clear. As each commercial producer utilizes their own proprietary algorithms, the order and composition (of the above) that each uses cannot be determined.

2.2.1 Image Binarisation

This is the process of converting the input image into a binary image. Typically the input image (from the scanner) is an 8-bit grey-scale image. From this, each pixel is tested, with those below a particular level being converted to white, and those above converted to black.

2.2.2. Ridge Thinning

Ridge thinning is often applied to make minutiae point extraction simpler. This is because the actual point of the ridge ending or bifurcation can be determined to the pixel if each ridge has been thinned to a single pixel in width. Thinning algorithms are quite common in image processing.

2.2.3. Ridge Orientation Estimation

Ridge orientation estimation is the process of determining the orientation of the ridge at any pixel (that is part of a ridge). This is usually achieved by partitioning the image into sections, and estimating the orientation of any and all ridges that pass though each section. The result of this step is the creation of an orientation map. This is a grid of N by M sections, with an associate orientation for each section. It should be noted that the orientations of the orientation map go both ways, as all ridges flow in two directions (i.e. a section with an orientation of 37 degrees would be equivalent to storing 217 degrees).

2.2.4. Ridge Smoothing

In order to prevent spurious minutiae points from being extracted, ridge smoothing can be employed. This is a heuristically based method of detecting and somehow fixing areas that have generated abnormal ridge structure due to dirt, scarring, other external factors or errors in capture. While again, no commercial information is available on how this is achieved; the following are ridge smoothing criteria.

- If a branch in [an orientation map] is roughly orthogonal to the local ridge direction and its length is less than a specified threshold then it will be removed.
- If a break in a ridge is short enough and no other ridges pass through it, then it will be connected.

2.2.5. General Image Enhancement

This section represents all the additional general image enhancement algorithms that can be utilized to improve the quality of the captured image at some stage in this process. For example, [Hong et al. 1997] utilizes an algorithm that uses normalization, region masking and Gabor filtering to improve some areas of a noisy image, while ignoring unrecoverable, or extremely noisy sections.

2.2.6. Macro-Singularity Detection

The detection of the macro-singularities (cores and deltas) of a fingerprint is often utilized in this process, to determine the overall shape of the fingerprint, or provide reference points for the location of minutiae points.

2.2.7. Minutiae Point Extraction

Extracting the minutiae points is generally achieved through the tracing of a thinned ridge line searching for intersections with other lines and end points. Intersections and end points are often determined by testing the surrounding eight pixels of the current pixel. If there is only one ridge pixel then the current pixel is a ridge ending. If there are more than two, then the pixel is at a ridge intersection (or bifurcation). A demonstration of this can be seen in Figure 4.

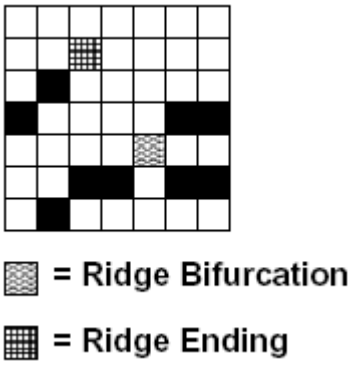

Figure 4. Detection of minutiae points through the number of surrounding ridge pixels

It should be noted that the above method is not standard, but specific to the method used in [Jain et al. 1996]. Other minutiae extraction algorithms may place the minutiae point one pixel away from the ridge ending, one pixel in (on the ridge line) from the ridge ending, or some other value altogether. The same concept applies to bifurcations as well. This means that given the exact same image in two different systems, the templates will most likely be different, based on minutiae extraction alone, let alone all the other variations.

2.2.8. Spurious Minutiae Removal

Often, even with all the prior image and ridge enhancements, spurious minutiae points are generated due to excess noise that could not be filtered out. When

this occurs it is still possible to remove some of them, although this process is again based on heuristics. For example, the following are spurious minutiae removal criteria

- If several minutiae form a cluster in a small region, then remove all of them except for the one nearest to the cluster centre.
- If two minutiae are located close enough, facing each other, but no ridge lines lie between them, then remove both of them.

2.3. Template Creation

Once all the minutiae points that the system considers to be valid have been identified, the template for the captured image can be created. Again depending on the implementation, the data stored will vary, sometimes quite significantly. The following is a list of the most common information associated with each minutiae point that can be stored in a template (see also Figure 5):

Location: This is usually the x and y coordinates of the minutiae point. The location of the origin for the coordinate axes is system dependent. Possible positions are at a particular corner of the image or some location unique to the current image, typically the central core point (if present).

Direction: This is typically the direction vector of the ridge at the minutiae point, as determined by the associated orientation map. Depending on the system being used, the direction associated with a minutiae point can be different (as orientation maps are bi-directional). For example, at a ridge ending, it is possible to associate the direction that the ridge was heading when it stopped, or the direction back along the ridge (see Figure 5). The direction associated with ridge bifurcations has even more possibilities, due to the combination of at least three lines at a point.

Type: The type of minutiae point is also stored in some systems. This allows the result generator to discriminate ridge endings from bifurcations. In addition, some systems store the location (and hence the associated type) of the core and delta points, to provide reference points, or added detail on the type and shape of the fingerprint.

Curvature: For ridge endings and bifurcations, the ridge is usually not straight at the location of the minutiae point. Therefore some systems also store the curvature of the ridge at that point. This adds more detail to the template, which is designed to improve matching accuracy.

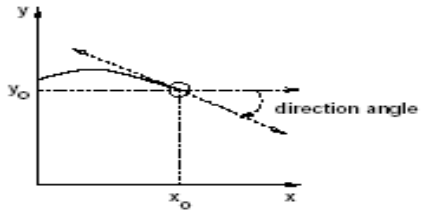

Figure 5. Depiction of a ridge ending, with associated x,y coordinate values and direction

Also, templates can vary in size, with some implementations using a fixed size template from as small as 50 bytes. By using a fixed size template, the minutiae extraction process must also evaluate each minutiae point in an attempt to store the most important points. However, many vendors do not utilize this methodology due to the variation of captured fingerprints, even in successive captures.

Alternatively, templates can be variable in size. This allows all the detected minutiae points to be included in the template. This illustrates the issue of ensuring a good quality fingerprint during enrolment. If a noisy or otherwise corrupted image is used, there will be numerous spurious minutiae points generated, some of which may not be detected and subsequently removed. With variable size templates, all remaining spurious minutiae points will be added to the template (along with the valid minutiae points). Thus, the valid user will have a lower chance of generating the required confidence during authentication.

3. Biometric Template Store

Implementation of the template store is another area that is typically system dependent. In order to increase search speed for identification (one-to-many searches) many producers implement their own databases, and even hardware. Some implementations index the template databases by their overall shape. However, with almost a third of fingerprints being whorls, (according to [International Biometric Group]), this may provide very little increase in searching performance.

4. Result Generator

The result generator is what performs the matching process. Here the live template is compared with the master template (for authentication). Reliably 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). The main factors responsible for the intra-class variations are: displacement, rotation, partial overlap, non-linear distortion, variable pressure, changing skin condition, noise, and feature extraction errors. Therefore, fingerprints from the same finger

may sometimes look quite different whereas fingerprints from different fingers may appear quite similar (see Figure 6).

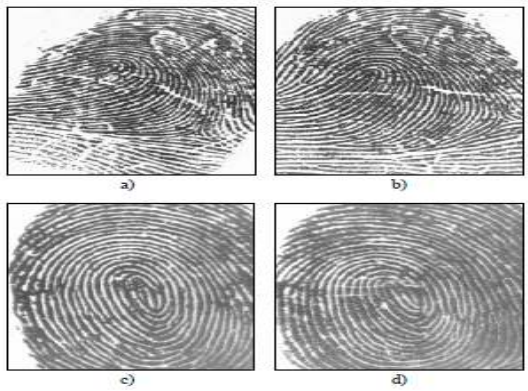

Figure 6. Difficulty in fingerprint matching. Fingerprint images in a) and b) look different to an untrained eye but they are impressions of the same finger. Fingerprint images in c) and d) look similar to an untrained eye but they are from different fingers.

Human fingerprint examiners, in order to claim that two fingerprints are from the same finger, evaluate several factors:

Global pattern configuration agreement, which means that two fingerprints must be of the same type.

Qualitative concordance, which requires that the corresponding minute details must be identical.

Quantitative factor, which specifies that at least a certain number (a minimum of 12) of corresponding minute details must be found.

Corresponding minute details, which must be identically inter-related. In practice, complex protocols have been defined for fingerprint matching and a detailed flowchart is available to guide fingerprint examiners in manually performing fingerprint matching.

Automatic fingerprint matching does not necessarily follow the same guidelines. In fact, although automatic minutiae-based fingerprint matching is inspired by the manual procedure, a large number of approaches have been designed over the last 40 years, and many of them have been explicitly designed to be implemented on a computer. A (three-class) categorization of fingerprint matching approaches is:

correlation-based matching: two fingerprint images are superimposed and the correlation (at the intensity level) between corresponding pixels is computed for different alignments (e.g., various displacements and rotations)

minutiae-based matching: minutiae are extracted from the two fingerprints and stored as sets of points in the two-dimensional plane. Minutiae matching essentially consists of finding the alignment between the template and the input minutiae sets that results in the maximum number of minutiae pairings;

ridge feature-based matching: minutiae extraction is difficult in very low-quality fingerprint images, whereas other features of the fingerprint ridge pattern (e.g., local orientation and frequency, ridge shape, texture information) may be extracted more reliably than minutiae, even though their distinctiveness is generally lower. The approaches belonging to this family compare fingerprints in term of features extracted from the ridge pattern.

Given a complex operating environment, it is critical to identify a set of valid assumptions upon which the fingerprint matcher design could be based. Often there is a choice between whether it is more effective to exert more constraints by incorporating better engineering design or to build a more sophisticated similarity function for the given representation. For instance, in a fingerprint matcher, one could constrain the elastic distortion altogether and design the matcher based on a rigid transformation assumption or allow arbitrary distortions and accommodate the variations in the input images using a clever matcher. In light of the operational environments mentioned above, the design of the matching algorithm needs to establish and characterize a realistic model of the variations among the representations of mated pairs.

5. Conclusion

This paper presents the generic architecture of Fingerprint Biometric System which shows how Fingerprint Recognition works. Also present the three main parts of architecture. And below those parts it shows the different components which are used in recognize the person using Fingerprint Authentication.

6. References

[1] www.biometric.org
[2] www.cubs.buffalo.edu
[3] Paul Reid, “Biometric for Network Security”
[4] Anil K. Jain, Patrick Flynn, Arun A. Ross, “Handbook of Biometric”
[5] Davide Maltoni,Dario Maio,Anil K. Jain, Salil Prabhakar, “Handbook of Fingerprint Recognition”
[6] Dr Dhaval R Kathiriya, Dr. N.N Jani, “Biometric Authentication System and Smart card technologies”