DESIGNING A NOVEL APPROACH FOR FINGERPRINT BIOMETRIC DETECTION: BASED ON MINUTIAE EXTRACTION

Hossein Jadidoleslamy

Information Technology Engineering Group, Department of Information Technology, Communications and Security, University of Malek Ashtar, Tehran, Iran
tanha.hossein@gmail.com

ABSTRACT

People authentication based on fingerprint is one of the most important people authentication techniques which it used biology specifications. The main purpose of this paper is discussing on minutiae-based extraction methods for fingerprints comparison and presenting a new pattern matching algorithm in this area; of course, this algorithm also has been presented based on comparing fingerprint features (especially minutiae points).

KEYWORDS

Biometric, Fingerprint, Minutiae, Automated Fingerprint Identification System (AFIS), Extraction, Matching

1. INTRODUCTION

Fingerprint is unique for any people and it can be used as peoples' signature to authenticate them [1, 2]. The most famous softwares of this category is using on criminology. Nowadays, it is increasing request for automatic comparison of fingerprints. Some of this system's applications are as following:

- Access control to the physical places;
- Access control to the computer, network and other resources;
- Access control to the customers' banking accounts;

In other side, while comparing fingerprint images, it is possible to occur following errors:

- Different scratch;
- Destroyed and incomplete fingerprint;
- Inappropriate image (inappropriate deployment location of finger on the scanner glass or being displaced the finger rather than special situation or being rotated the finger with special angle lead to incomplete and italic image of finger on scan process);

An advanced solution for solving this problem is extracting the features of fingerprint image (such as start, end and intersection points of fingerprint lines) and then, doing comparison between different sets of fingerprint features. However, the presented solution requires to an advanced and reliable algorithm to process fingerprint image; this algorithm should be had following capabilities:

- Removing scratch [3, 24];
- Features extraction [8, 9, 12, 19];
- Displaced or rotated fingerprint comparison [24, 25];
- Being fast to be applicable in environments, along with many users;
The volume and size of extracted features (for storing into the information-base on microchip);

Although there are many algorithms to verify fingerprint [4, 5], it is not easy to acquiring a comprehensive solution to obviating all requirements. This paper has been organized into 7 sections, including: section2 will discuss about fingerprint based systems; section3 represented some discussions about fingerprint and its various properties; section4 posed pattern extraction methods; section5 presented the proposed pattern matching algorithm and different kinds of fingerprint scanners; section6 expressed the conclusion; and finally, section7 presented some posed and new research topics on this domain.

2. FINGERPRINT-BASED SYSTEMS

The most important challenge of governments in current century is counter-measuring with biggest century spoofing; i.e. identity forgery or impersonation and it is only possible by using of biometric parameters. At the current time, biometric plays an important role on following areas:

- Peoples' verification;
- Access control;
- Computer security;
- Banking;
- Access times;
- Unknown peoples' specification;

As Figure1 shows, fingerprint biometric systems have functionalities such as image receipt, image process, features extraction [19] and pattern matching [20, 21]. These softwares are calling AFIS (Automated Fingerprint Identification System) [3, 4]. The necessity of producing an AFIS software is technical and scientific fingerprint verification [3, 5, 6]. In next sections, the paper will be discussed about fingerprint verification based on pattern, features verification, features extraction and how to comparing fingerprints. Following figure is showing how an AFIS system operates [3, 13].

3. FINGERPRINT DIFFERENT DIMENSIONS

3.1. Fingerprint Feature Extraction
Fingerprint feature extraction is the most important process in AFIS systems [3, 10]. By attention to the used algorithm capability, this process is verifying different features of a fingerprint (such as minutiae points, core, delta and pattern) and it is storing them into a data structure (called template).

This data structure can be according to the NIST specified standards or a special structure of used algorithm [11]. But a good algorithm has capability to converting its template to the NIST standards and vice-versa. Also, it is possible to discussing about presenting new templates for storing the template; it is necessity to attention to the following hints for creating this template, such as:

- Being small the size and volume of the template; since, it leads to increasing of comparison speed and it provides possibility of storing templates in smart cards, too;
- Removing unnecessary features of the template; so that it requires to less memory and leads to comparison speed increment;

As a result, more features leads to increasing the comparison accuracy and then, more precise result and also, it leads to volume and size increment and comparison speed reduction; therefore, by attention to the case of algorithm applicability should select best option (it is necessary to have be existed balance and fairness between templates volume, size, search speed, comparison accuracy and speed). For example, in criminal authentication systems, accuracy of verification [6, 7] has more important rather than volume, size and speed parameters.

### 3.2. Fingerprint Template

The first difference between fingerprints is created design and template of fingerprint lines (it called “pattern” and it be categorized as “classification”). Following figure (Figure 2) is showing three different patterns. These patterns are dividing into 4 major categories, including:

- Whorl;
- Left Loop (LL);
- Right Loop (RL);
- Arch;

![Figure 2. Different Types of Fingerprint Patterns](image)

**3.2.1. Whorl Pattern**

In the Whorl pattern, fingerprint lines create concentricity circles image.
3.2.2. Left Loop Pattern

In the Left Loop pattern, it is possible to see a rotation or curvature on the left direction of image.

3.2.3. Right Loop Pattern

The Right Loop pattern has the similar rotation or curvature on the right direction of image.

3.2.4. Arch Pattern

In the Arch pattern, there are some arches in the form of Hill in the middle of image.

It is clear completely which it is not required to comparing 2 different patterns' fingerprints while comparing fingerprints; since the probability of matching 2 fingerprints with various and different patterns is zero. Of course, the most automated systems do not use the matching of these features for comparison [22, 23]. Because it is possible to acquiring a correct pattern of fingerprint from a vertical and complete input image (no rotation); but usually the incoming image do not has these features (it may be had rotation, curvature or it may be incomplete); so it will not be had the required features; this leads to increase the probability of incorrect detection or recognition [17, 18]; then, it leads to error or fault. The main application of this feature on the identity verification systems is classifying fingerprint cards [4, 7].

3.3. Fingerprint Features

Fingerprint features are points which they are observable and distinguishable from collision fingerprint lines or curve forms. These points create the base of fingerprint verification process. In Figure 3, there are three different kinds of fingerprint features [24, 25].

![Figure 3. Different Features of a Fingerprint Pattern](image)

These features have been divided into 4 major classifications, including: Minutiae, Core, Double Core and Delta.

Minutiae are start, end, collision and 2-branched points of fingerprint lines which they create the base of fingerprints comparison and they have been specified by green color in above figures.

The core is the center of rotation in RL (Right Loop) and LL (Left Loop) patterns which they have been determined by red umbrella in the above figures.

Double core is the center of circle in Whorl pattern.
Deltas are rectangle form points which they have been created from lines collision and they usually be seen in the right or left direction of loops, which they have been shown by red color tripetalous sign in above figures.

All of these features are stored into a data structure which it is created by fingerprint algorithm programmers (it called "template") and while comparing fingerprints, the templates be compared to each other.

There are some standards to storing fingerprint features which they have been created by NIST [11]. Size and volume of template is an important factor which it is affected on speed of comparison and microchips' storage capacity. Any one of these features should be had a special data structure. For example, following data structures are proposed for fingerprints' features and their templates.

3.3.1. Date Structure to Storing Minutiae Points

typedef enum MinutiaType_{
    mtUnknown = 0,
    mtEnd = 1,
    mtBifurcation = 2,
    mtOther = 3
} MinutiaType;

typedef struct Minutia_
{
    short X;
    short Y;
    MinutiaType Type;
    byte Angle;
    byte Quality;
    byte Curvature;
    byte G;
    vector < MinutiaNeighbor > MinutiaNeighborSet;
} Minutia;

X, Y: A minutia coordinates in fingerprint image;  
Minutiae type: It determines type of minutiae (2-branched, line-end, island or etc);  
Angle: Minutiae angle into the image;  
Quality: Minutiae quality (it depends to the image quality);  
Curvature: Nearest slot to the minutiae (rather than fingerprint lines);  
G: Minutiae value or weight (amount of neighbor's minutiae, its type, situation and quality);  
Minutiae neighbor set: The set of points of neighbor's minutiae;

3.3.2. Data Structure to Storing Minutiae Points of Neighbors

typedef struct MinutiaNeighbor_
{
    int Index;
    byte RidgeCount;
} MinutiaNeighbor;

Index: The number of neighbor's minutiae;  
Ridge count: The distance between neighbor minutiae and the candidate minutiae;

3.3.3. Data Structure to Storing Core Points

typedef struct Core_
{
    short X;
    short Y;
    byte Angle;

3.3.4. Data Structure to Storing Delta Points

typedef struct Delta_
{
    short X;
    short Y;
    byte Angle1;
    byte Angle2;
    byte Angle3;
} Delta;

X, Y: Delta coordinates into the fingerprint image;
Angle (X): Triple-angles of delta into the fingerprint image;

3.3.5. Data Structure to Storing Double Core Points

typedef struct DoubleCore_
{
    short X;
    short Y;
} DoubleCore;

X, Y: The double core coordinates into the fingerprint image;

3.3.6. Data Structure to Storing Template

typedef struct FingerprintRecord_
{
    short Index;
    short Class;
    vector <Minutia> MinutiaSet;
    vector <Core> CoreSet;
    vector <Delta> DeltaSet;
    vector <DoubleCore> DoubleCoreSet;
} FingerprintRecord;

Index: The fingerprint index;
Class: The fingerprint pattern;
MinutiaeSet: Set of minutiae points;
CoreSet: Set of core points;
DeltaSet: Set of delta points;
DoubleCoreSet: Set of double core points;

4. MINUTIAE EXTRACTION TECHNIQUES

This process is including of direct detection of minutiae, binary image creation and image optimization steps; at the next sections, these steps have presented in comprehensive.

4.1. Minutiae Direct Detection

Automatic detection of minutiae is very important processes, especially in fingerprint along with low quality; while that signal disorder and contrast shortage leads to forming pixel similar to a
minutiae or being hide real minutiae. In this method, a new technique has been proposed based on following lines lump; it extracts minutiae from the gray-scale image, directly \cite{9, 10, 15}.

According to the Figure4, this method at the first step finds and specifies the fingerprint lines path by using of an especial algorithm; for this purpose, a gray-scale image be used: into this image, the fingerprint lines prominence being shown by a spectrum of gray pixels which the most prominence will be shown by most severity of dark color (the most prominence will show the line path). The fingerprint lines will be specified by finding these maximums and tracking them. As Figure4 is showing, a pseudo-code of above algorithm can be as follows.

According to the Figure5, in the second step, minutiae points should extract from the acquired lines; it is possible to have be existed a minutiae whereas lines has been ended or they cut off each other. So, for this purpose, all of acquired lines of the image should be scanned in once; it is possible to use of an algorithm which it creates a second image (including of detected lines) from the primary image and it signs lines by scanning or traversing them; when all lines be signed, i.e. the whole image has been scanned. As Figure5 shows, a pseudo-code for minutiae detection algorithm can be as follows.
Figure 5. The Second Step of Minutiae Direct Detection Algorithm and Its Pseudo-code

4.2. Binary Image Creation

Figure 6 is showing how can create a binary image; this method is a common algorithm in AFIS systems which it converts the fingerprint primary image to the gray-scale format and then, by using of an especial process, it will be converted to a binary image [3, 17, 26]. The goal of this conversion is being specified fingerprint lines in attention to the color severity difference in prominence or hill points of lines and slots. When being determined these lines, it is possible to find minutiae points of lines, intersection points and start or end of lines.
In different algorithms, the main difference is in primary image process [26]; after primary process, extracting minutiae points is almost same and it uses of similar techniques. By attention to the Figure 7, the minutiae are classified into 2 main types, including:

1. Bifurcation: in this case, minutiae are determined from intersection location of 2 lines (connection or intersection point);

2. End: in this case, minutiae are the end points or start points of lines;

Figure 7. Different Types of Minutiae Point Extraction

4.3. Image Optimization

This method can be used as a pre-process for all minutiae-extraction algorithms [8, 9, 14, 26]. In this method the primary image of fingerprint be processed and a part of image be filtered which it is ambiguous or it has not appropriate quality and it increases the probability of detecting false minutiae (be filtered). Also, an image part which it can be reconstructed, it be improved navigation. For example, some of fingerprint lines which they are clear, but in part of image has been removed from the created image; due to scratch or incomplete contact of finger with scanner [25], they have to be reconstructed. After doing this process, the minutiae extraction will be did from an appropriate, more reliable and better quality image which it will be significant on result of comparison and fingerprints' verification [15, 16, 26], directly.

5. The Proposed Pattern Matching Algorithm

5.1. Fingerprints' Comparison

Fingerprints’ comparison is started by comparing templates, that it is based on finding similarity between minutiae points of 2 fingerprints' templates. Neighbor minutiae are told to points which they are placed near to the candidate minutiae and they are selected by 2 methods, including:

1. Selection with angle P/2;

2. Selection with angle P/4;
As above figure shows (Figure 8), to selecting neighbor minutiae, it is necessary to move in contrast to the trigonometric from angle of candidate minutiae and in any sector, the first observed minutiae be selecting as neighbor. In this method, it most select 4 neighbor minutiae by using of angle P/2 and it most select 8 neighbor minutiae by using of angle P/4. In above figure, the candidate minutiae have been specified by blue color and the selection angle was being P/4; as a result, 8 neighbor minutiae have been specified by yellow color. It is clear which by selecting angle P/4, the comparison accuracy and template's volume and size be increased and as a result, it leads to reducing the comparison speed.

By selecting angle greater than P/2, the number of neighbor minutiae will be reduced to 2 or 3 minutiae at most which it is not appropriate to checking the value of a minutiae (matching accuracy). Also, by selecting angle less than P/4, the number of neighbor minutiae will be more than 8 numbers which it leads to increasing template volume and size and reducing comparison speed. By attention to the done researches, the angle P/4 and almost 8 neighbor minutiae is appropriate to determining minutiae value and comparison speed. So that in the above figure has been shown, the candidate minutiae and its neighbors are specifying a template. Matching of 2 fingerprints is considering minutiae points to finding similar templates. One of most main parameters to finding similarity between 2 minutia templates is the distance between 2 minutiae points which it called ridge count. Of course, this parameter does not measure based on any one of usual length measurement units, but its calculation unit is counting the number of lump between 2 minutiae points. So that above figure is showing the distance between candidate minutiae and its second neighbor is 6 slots. Usually, it is possible to detect 20 to 40 minutiae of any fingerprint image; fingerprints comparison at least requires 5 to 7 minutiae; one single minutiae does not have any value; i.e. an alone minutiae is not important, but a set of minutiae points can presented a pattern for comparison. To comparing fingerprints with less than 5 minutiae (like 3 or 4 minutiae), it is possible to finding much similar under-patterns (triangular or quadrilateral figures) in heterogeneous and non-similar fingerprints. To obviate this error, it should be existed at least 5 minutiae for comparison. The following figure (Figure 9) has been shown the similarity patterns of 2 compared fingerprints.
Comparison process of 2 fingerprints requires to a very complex algorithm, which it should be had capabilities such as comparing displaced, moved, rotated, defective and incomplete fingerprints [24]. Also, it must be had entitled high speed.

5.2. Fingerprint Images Enrollment

AFIS software systems use fingerprint images reception sensors to registering fingerprint images. These sensors are famous as fingerprint scanner, and they classified into 2 major categories, including:

5.2.1. Capacitance scanner;

5.2.2. Optical scanner;

Capacitance scanners deploy into devices in internal and they usually being used on mobile phones and notebook computers. Optical fingerprint scanners play important role in AFIS softwares; receiving a good image along with high quality is depending to extracting features with high quality. Optical scanners at least should create an image with 500 dpi resolution (this image usually is in 256 bit gray-scale format).

Optical scanners divide into different kinds by attention to the capability of simultaneous reception of some fingerprint, including:

- Single fingerprint: in this kind, which it is the most common and most cheep existent scanners, only an image of a finger be scanned in each time.

- Double fingerprint: this kind of scanner is similar to single scanner apparently, but in this scanner the location of fingerprint image is greater (almost double); so, it can take image of 2 fingers each time, simultaneously (Figure10).
• Live scanner: this kind of scanner is professional and it can take image of 4 fingers, simultaneously (Figure 11).

Another classification of optical scanners is based on capability of creating roll and flat images. The flat image of fingerprint which it be received by contacting finger with surface of scanner glass (that it be called as flat); all optical scanners can create this kind of image. In this kind of image, only finger surface which it contacts to scanner glass surface, it be used to creating image and due to circularity of fingers surfaces, there is not possibility of full contact between finger and scanner glass surface; so, a part of the finger be scanned.
The method of receiving roll images is difference; in this method, the finger being located on the scanner glass surface from left-end part which slots of fingerprint be started and it rotates to the right-direction, slowly; this rotation be continued to right-end part of fingerprint. The fingerprint scanner creates a full image of fingerprint by starting scan during rotation step. The roll image is almost double flat image and also the number of extracted minutiae is almost double. Roll images usually be used in criminal and authentication systems. Usually live scanners and some of single fingerprint models have this capability. Possibility of reception this kind of image leads to significant price difference with different kinds of flat.

By attending to the Figure12, AFIS systems can process analog images [3]; analog images be registered by ink on fingerprint cards in traditional authentication systems. To processing analog, these cards are scanned by common scanners with 500 dpi resolution and created images be processed by AFIS software. The scanned images of analog cards can not be qualified as optical scanners images; but their process is necessary and require to transferring recorded and archived information of related organizations to the AFIS system.

![Figure 12. Analog Image Processing by AFIS](image)

5.3. Functionality of Different Kinds of Scanners

5.3.1. Capacitance Scanners Functionality

According to the Figure13, capacitance scanners create an image of fingerprint by measuring existent difference between produced electrical signals by slots and lump of fingerprint lines. These kinds of scanners using a type of conductive sensor which it created by an array of sensors. Dimensions of these sensors are usually 20*15 mm.
5.3.2. Optical Scanners Functionality

According to the Figure 14, optical Scanners use of CCD (charge-coupled device) or CMOS (complementary metal-oxide-semiconductor) sensors. They are both doing operations such as light absorption and its conversion to the electrical signals. These sensors are consist of thousands pixel in a linear or matrix array which they created an image of scanned fingerprint by light radiation to the scanner glass surface and recording reflex of the light intensity into the array.
6. CONCLUSION

Image processing softwares are fully depending to the input images; so, the best minutiae extraction algorithms will show weak results while they receiving flawed and ambiguous input data. By attention to the done considerations, it proposes which minutiae extraction algorithms execute image optimization process before the main process. This process leads to removing false minutiae and verifying correction minutiae. By implementing this algorithm in an optimal method, the process of a fingerprint image will be done at a moment; also, in attending this process does before than features extraction, it will not has effect on comparison time (it only has very partial effect on whole time).

The discussed algorithms have capability to compare 25000 to 50000 fingerprints per second; some of reasons of this difference are as follows:

- Implementation method of comparison algorithm,
- Pattern volume and size,
- Number of minutiae per each template,
- Image rotation,

One of methods to reducing the comparison time in large scale (comparison of hundreds millions templates) is using of data clustering algorithm to dividing templates into small groups and doing parallel comparison on these set of clusters. As a result, by this method by increasing the number of clusters and reducing the number of templates in each cluster, the comparison time will be reduced and broke into a part of a second. The main property of the presented pattern into this paper is having completeness, integrity and low size. Then, it leads to the structure of fingerprint record template (which it can be used for different goals such as comparison speed and comparison accuracy). Also, the presented algorithm has attention to the image optimization which it leads to reducing the error of false minutiae detection; besides, it can be used as a pre-process for each pattern extraction algorithm. The presented algorithm has less speed than minutiae direct detection algorithms and binary image creation algorithms; but it has more accuracy which it affects directly on the result of comparison algorithm.

It is hoping which this paper can play a significant role to improving the fingerprint matching algorithms of biometric authentication industry by presented proposals.

7. FUTURE WORKS

This paper was an introduction to fingerprint identification based on minutiae point matching. Some of most important research topics in fingerprint biometric detection are as following:

- Automatically computing the local ridge frequency, that is used in Gabor filters [12, 13] and minutiae templates;
- Improving the minutiae templates;
- Using fingerprint classification to speed up the algorithm;
- Allowing non linear transformation in the matching Process [21, 23];
- An investigation into a filter whose primary aim is to specifically enhance the minutia points;
- Further study into the statistical theory of fingerprint minutiae;
REFERENCES


Author Biography

H. Jadidoleslamy is a PhD student in Information Technology (IT)-Information Security at the University of Malek Ashtar in Tehran, Iran. He received his Bachelor Degree in Information Technology (IT) engineering from the University of Sistan and Balouchestan (USB), Zahedan, Iran, in September 2009. He also has been received his Master of Science degree from the University of Guilan, Rasht, Iran, in March 2011. His research interests is including Computer Networks (especially Wireless Sensor Network), Information Security (by focusing on Intrusion Detection System), and E-Commerce. He may be reached at tanha.hossein@gmail.com or jadidoleslamy@gmail.com.