Authentication using Hashed Fingerprint

Kawther A. Sallal,PhD
College of Applied Sciences
Sultanate of Oman

Salah M. Darwash,PhD
College of Applied Sciences
Sultanate of Oman

ABSTRACT

Due to the great increase in information technology systems where user authentication is needed, security in those systems relies on using PINs or passwords. During the last years, the scientific community is trying to improve biometric techniques to be accepted as an alternative to other user authentication schemes. Fingerprints are the oldest and most widely used form of biometric identification. local and global features are important features in fingerprint images used for classification and matching purposes. The main goal of this work is using the fingerprint technology to generate a number of hashes that can be used for identifying person identity and authentication purposes. local and global features has been used to obtain a robust recognition system where a robust algorithm is used to extract these features accurately. The orientation and flow of ridges is used as the key factors for processing to avoid eliminating true features. Then, the hashing concept has been applied on the calculated distance between each feature extracted inside the region of interest and the core point. Finally, the extracted hash values is compared with those stored in the database. It is shown by the experiments that the presented verification system improves the features extraction accuracy and the performance of the matching process.

Keywords

Biometrics, Fingerprints, Feature Extraction, singular point, Hash Function, and Authentication

1. INTRODUCTION

Most IT systems require verification or identification of users. Known as “authentication,” this identification is commonly done with passwords (“what you know”) or cards and badges (“what you have”). Biometric authentication – biometrics for short – is a third method based on “who you are.” It has definite advantages. For example, biometrics can eliminate problems of forgotten passwords or lost cards because “who you are” is always with the user. Because of these advantages, biometrics is currently becoming more popular for convenient and secure authentication [1][9].

Every authentication method has both strengths and weaknesses. Although biometric authentication is no exception to this, it does provide another choice. Its strength lies in the fact that it cannot be forgotten, misplaced or shared. Its weakness comes from not being 100% accurate and because some people may be unwilling to use it.

Fingerprint verification is a quick and convenient method of establishing an individual’s identity. Among all the biometric techniques, fingerprint is the oldest [2]. They have long been used for identification because of their immutability and individuality. Immutability refers to the permanent and unchanging character of the pattern on each finger. Individuality refers to the uniqueness of ridge details across individuals; the probability that two fingerprints are alike is about 1 in 1.9 x 10^{15}. A fingerprint is the pattern of ridges and valleys on the surface of the finger. The uniqueness of a fingerprint is determined by the topographic relief of its ridge structure and the presence of certain ridge anomalies termed as minutiae points or local features. Minutiae are local features of fingerprints and are restricted to two types: ridge ending and ridge bifurcation and illustrated in Figure (1). [2]

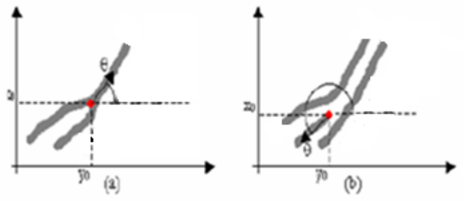


Figure (1) end point and bifurcation point

In fingerprint recognition, the problem is the existence of false minutiae which increase FAR and FRR in fingerprint matching. Therefore, the enhancement of the fingerprint image and the false minutiae elimination form an important part of the system. Global features of a fingerprint can be defined as the points of maximum curvature of the concave ridges in the fingerprint image. Fingerprint images of poor quality with cracks and scars, dry skin, or poor ridge and valley fail to correctly localize global features [3][4]. Therefore, the detection should necessarily consider a large neighborhood in the fingerprint. On the other hand, for an accurate localization of the global features, the approach should be sensitive to the local variations in a small neighborhood.

In this work, the overall fingerprint authentication system could be divided into image pre -processing, minutiae extraction, core point detection, hashes generation, and matching.

2. Fingerprint Based Authentication

There are two types of fingerprint-based authentication techniques: graph-based and minutia-based. In this work, we concentrate on the latter because minutia are widely believed to be the most discriminating and reliable features of a fingerprint. In addition, the amount of information needed to be stored in the template database for fingerprint matching is smaller and the processing time is shorter than that of graph-based algorithms. A fingerprint-based authentication system consists of two main steps: user enrollment and user authentication. In the first step, an acquisition system captures an image of the user’s fingerprint. A series of image processing procedures are then applied to the image to detect and extract the minutiae. Now, the extracted minutiae are stored in a database and the user is considered enrolled. During user authentication, the user supplies a fingerprint image which is again processed to detect and extract the minutiae. These minutiae are then compared against the reference minutiae stored in the template database. A reference score is calculated based upon the number of minutiae that match. The user is considered authenticated if the score exceeds a specified threshold.

3. Proposed System

3.1 Image processing

The quality of the ridge structures in a fingerprint image is very important; it carries the required information for minutia extraction. Ideally, in a good fingerprint image, the ridges and valleys should alternate and flow in constant direction. This regularity facilitates the detection of ridges and consequently, allows features to be extracted from the thinned ridges. In practice, a fingerprint image may not always be good due to elements of noise that corrupt the clarity of the ridge structures. This corruption may occur due to differences in skin conditions and impression such as scars, moisture, dirt and bad contact with a fingerprint scanner. Thus, image enhancement techniques are used to reduce noise and improve ridges against valleys using the Gabor filter method. Gabor filters have both frequency and orientation properties, which mean the filters can be effectively directed to specific frequency and direction values [5] [6] [7]. Then, Ridge extraction is implemented. It's the process that converts a grey level image to a binary image. This facilitates the extraction of minutiae because it enhances the contrast between the ridges and valleys in a fingerprint image. The final image enhancement step typically performed prior to minutia extraction is thinning.

Thinning is the operation that erodes the foreground pixels until they became one pixel wide. The standard thinning algorithm is used, which performs the thinning operation using two sub iterations. Each sub iteration starts by examining the neighborhood of each pixel in the binary image, and based on a set of pixel deletion rules, it checks if the pixel can be deleted or not. These sub iterations continue until no more pixels can be deleted. Applying a thinning algorithm to a fingerprint image keeps the connectivity of the ridge structures while forming a skeletonized version of the binary image [8].

Example of a thinned image can be shown in Fig.2. In contrast to Figure (2), it can be shown that employing a series of image enhancement stages prior to thinning is effective in facilitating the reliable extraction of minutiae.

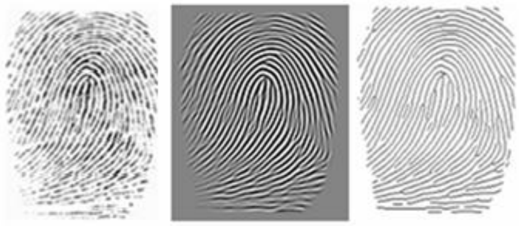


Figure (2) Thinning Results

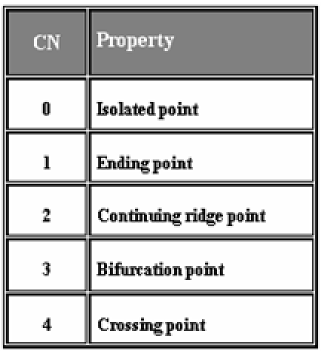
3.2 Minutia Extraction

Cross Number (CN) concept is the most common method of minutiae extraction [1]. This method uses the skeleton image where the ridge pattern is eight connected. The features are extracted by scanning the local neighborhood of each ridge pixel in the image using a 3x3 window. Then, the CN value is computed, which is defined as the half of the sum of the differences between pairs of adjacent pixels in the block's eight-neighborhood.

CN (P) (1)

Where *p0* to *p7* are the pixels belonging to an ordered sequence of pixels defining the 8-neighborhood of *p* and *val (p)* is the pixel value. Using the properties of the CN as shown in Table 1, the ridge pixel can then be classified as a ridge ending, bifurcation or non-minutiae point. For example, a ridge pixel with a CN of one refers to a ridge ending, and a CN of three refers to a bifurcation.

Table (1) CN properties



CN	Property
0	Isolated point
1	Ending point
2	Continuing ridge point
3	Bifurcation point
4	Crossing point

From the skeleton image, all ridge pixels referring to a CN of one and three have been detected successfully. Additionally, the results show that there are no candidate minutiae pixels that have been missed, and no pixels that have been falsely marked as features pixels. Hence, it can be shown that the CN technique is able to accurately detect all valid bifurcations and endings from the skeleton image. Result of minutiae extraction is illustrated in Figure (3).

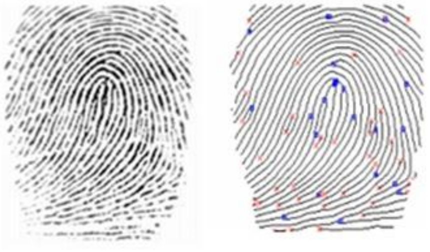


Figure (3) Minutiae Extraction

3.3 Singular Point Detection

Singular points are important features of fingerprints and are widely used for fingerprint classification and matching; hence, it is important to obtain a reliable estimation of the orientation field around these points. Singular points are the points in a fingerprint where the orientation field is discontinuous and unlike the normal ridge flow pattern, the ridge orientation varies significantly.

To meet the requirement of an accurate and reliable localization for the reference point, a reference point detection method based on the orientation field is used.

Figure (4) Singular Point Result

The basic steps are:

- Estimate the orientation field *O* using Gabor filter.
- Initialize *A*, a label image used to indicate the reference point.
- Locate the block that contains a big difference in orientation values.
- For each pixel *(i, j)* in *A*, compute the difference in orientation values with its neighbors.
- Find the maximum value in A and assign its coordinate to the core, i.e., the reference point.

Although this successfully detects the reference point in most of the cases, including arch and double loops, in double loop case the reference point is the point of more curvature region in fingerprint image. An example of reference point location in fingerprint images of arch and double loop type is shown in Figure (4).

3.4 Region Cropping

The situation of fingerprint is changing every time the person puts his finger on the device or even in the case of using the ink. Therefore, if the system wants to extract the same hashes or some of those every time the person logs in, it must determine a region of interest in fingerprint image.

In this method the estimated image's ridges frequency and the detected reference point are needed to determine a circle region because of the variety of fingerprint image resolution and called the region of interest. The circle is specified by the coordinates of its center (x_c, y_c) and its radius (r). The circle equation is:

$$(x - x_c)^2 + (y - y_c)^2 = r^2 \qquad (2)$$

Where (x, y) is the coordinate of a point on the circle. (x_c, y_c) is the coordinate of the center point and (r) is the radius.

For determining the region of interest in fingerprint image, the system needs to determine circle region, which its center is the reference point and radius is computed as follows:

$$R = C * F \qquad (3)$$

Where R is the radius, C is a constant, and F is the frequency

3.5 Generating the Hash Values

A hash function H is a transformation that takes an input m and returns a value h (called the hash value) [10]. In this work, the matching is performed using hashed minutia instead of the original template. These operations of finding minutiae and hashes can potentially be incorporated into the scanner itself, so that only the hashes will need to be transmitted and stored in the database. During verification, new hash values are produced and matched with those stored in the database.

Authentication is based on scores that can range between 0% and 100%. Therefore, the hash based system must adhere to the following additional properties:

- similar fingerprints should have similar hash values,
- different fingerprints should not have similar hashes,
- rotation and translation of the original template should not have a big impact on hash values,
- partial fingerprints should be matched if sufficient minutiae are present.

We assume that two fingerprints of the same finger can have different position, rotation and scale, coming from (possibly) different scanners and different positioning of the finger on the scanner. Therefore, the distance or the orientation is of fixed values. For each feature inside region of interest, the distance of this feature from the core point will be computed:

$$D = \sqrt{(xi - xc)^2 + (yi - yc)^2} \qquad (4)$$

Where (xi, yi) is the coordinate of feature and (xc, yc) is the coordinate of core point.

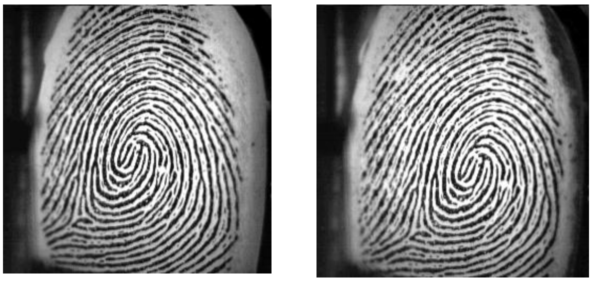
After determining the features' distances, the identification numbers is computed by using the MD5 hash function.

4. Experimental Results

The performance of the presented system is evaluated in this section. The fingerprint images used for experiments were obtained from the 2002 Fingerprint Verification Competition (FVC2002) database. Experiments were also conducted on inked images. The size of the image is 256 x 256 and 100 fingerprint images (4 samples for 25 individuals) with various image qualities were used for experiments. The extraction of features in fingerprint images is strongly related to the image quality.

The presented method achieved good performance in both robustness and efficiency. Figure (5) explains the extracted hash values of two samples taken for the same finger. There is a little difference in hash values explained with black color due to the situation of finger in the second sample. It is shown that depending on the distance or orientation give us an excellent results because it is not change with different situation of finger like rotation or translation.

By experiments, the matching rates of the proposed method for the three classes of image quality (V. Good, Good, Poor) are 98%, 89%, and 68% respectively. In poor images the matching rate is 68% because the local features can't be exactly extracted from fingerprint image because of the noise in different parts of image.



d41d8cd98f00b204e9800998ecf8427e	d41d8cd98f00b204e9800998ecf8427e
c983d95ed1995c4e5da3ce0317a7c0f1	c983d95ed1995c4e5da3ce0317a7c0f1
fbfe61003b8265132c50cff6d64384a9	fbfe61003b8265132c50cff6d64384a9
dc09afc901d7cabe915a0c7ba7f4881b	dc09afc901d7cabe915a0c7ba7f4881b
37d9e06c61cc1278cc86a358f659d53a	37d9e06c61cc1278cc86a358f659d53a
ea0065ade275f786b26994e69ccf25b1	ea0065ade275f786b26994e69ccf25b1
717e8661ee12fedd138523eb6d50211d	717e8661ee12fedd138523eb6d50211d
af4089f055b1718ba5ed1b59277a8013	**5cc94d1e512ada8cc3c4589fb25f149f**
e74ad76004d6a94154dc823832a3ead7	e74ad76004d6a94154dc823832a3ead7
092f316dc0a45567c36c3df936efffd1	**e207505a2ee333b679ec4b883f7d4799**
732c2df931e85f31af2862e3cef8454d	732c2df931e85f31af2862e3cef8454d
254edddaa37509ac787f0769c8464482	254edddaa37509ac787f0769c8464482
b1f38dd5fde7fbb4d73cb131704a3ff6	b1f38dd5fde7fbb4d73cb131704a3ff6
60ce15b3319dbaf92080060eeb41a352	60ce15b3319dbaf92080060eeb41a352
41d6e2138db31d0d3714eeaf9ec91405	41d6e2138db31d0d3714eeaf9ec91405
	fbb4d706c61c65ade2 b41a35e0317aaf

Figure (5) the hash values of two samples taken for the same fingers

5. CONCLUSIONS

In this work, practical and reliable method for user authentication is presented. Orientation and flow of ridges are the key factors for processing to avoid eliminating true features while processing.

Biometric technology is very difficult to detect and extract always the same or nearly the same features. The user can be authenticated by his/her biometric attributes and he/she will be either confirmed or refused. Hence some special treatment (to avoid the position change of some features) is necessary and this has been addressed in this work. The proposed method generates number of hash values for each user. It differs in context from other known methods of generation using biometrics. Using different features in fingerprint and generating more than one value give the proposed method a power performance in distinguishing the authenticated user from the impostor. The user can be identified if all or some of the new extracted hash values match with the enrolled values.

6. REFERENCES

[1] Jean-Christophe P., “Biometrics: Fingerprint Identification System”, M.Sc. Thesis**,** Institute for Computer Science Carleton University, Ottawa, Ontario, November 2011.

[2] Second Asian applied computing conference, “applied computing, Nepal, 2005, Springer.

[3] Mithun D.,Kangkhita K., Shamima Y., “ATM Transaction Security Using Fingerprint Recognition”, American Journal of Engineering Research, Volume-6, Issue-8, pp-41-45, 2017.

[4] Uludag U., Pankanti S., Prabhakar S., and Jain A., *“Biometric Cryptosystems: Issues and Challenges”*, Proceedings of the IEEE, vol.92, no. 6, June 2004.

[5] Prabhakar, S., Wang, J., Jain, A. K., Pankanti, S., and Bolle, R., "Minutiae verification and classification for fingerprint matching", In Proc. 15th International Conference Pattern Recognition (ICPR) (September 2000), vol. 1, pp. 25–29.

[6] Ross, A., Jain, A., and Reisman, J. A., "hybrid fingerprint matcher", Pattern Recognition 36, 7 (July 2003), 1661–1673.

[7] Fuliang W., “The Implementation of A Fingerprint Enhancement System Based on GPU via CUDA”, Master thesis of Science in Electrical Engineering, Blekinge Institute of Technology, Sweden, 2017.

[8] Louisa L., Seong L., and Ching Y., **“**Thinning Methodologies – A Comprehensive Survey**”**, IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 14, no. 9, p. 879, September 1992.

[9] Jason A., “The Basics of Information Security” 2nd edition, Elsevier, 2014.