Generate a Secured Multi-Purpose Code from Fingerprint Images

Dr. Bashar M. Nema [*] Nuha Sami Muhsin[*]*

Abstract

Extracting minutia and other features from fingerprint images is one of the most important steps in automatic fingerprint identification and classification. This paper proposes a method for the generation of long and secure code that may be used for multi-purpose applications, such as ATM, coded door locks and other security measures. The method consists of two phases; the first phase is carried out using fingerprint image enhancement and thinning. The second phase consists of extracting minutia, ridge ending, bifurcation and all other features in order to produce initial pattern. Finally, the multi-purposes secure code is generated by applying the one-way MD5 hash function on that pattern. The achieved results are discussed for security improvement. The proposed technique also shows considerable improvement in the minutia detection process in terms of both efficiency and speed.

***Key-Words:* - Fingerprint matching, Image, reference point, code generation, embedded system.**

[*] **Al-Mustansiriya University**

[*] ***Baghdad University**

1 . Introduction

Fingerprints today are considered as the most widely used biometric features for personal identification. Most automatic systems for fingerprint comparison are based on minutia matching [1, 2]. The objectives of biometric recognition are user convenience (e.g., money withdrawal without ATM card or PIN), better security (e.g., difficult to forge access) and higher efficiency (e.g. lower overhead for computer password maintenance).

Minutia characteristics are local discontinuities in the fingerprint pattern which represent terminations and bifurcations. A ridge termination is defined as the point where a ridge ends abruptly. A ridge bifurcation is defined as the point where a ridge forks or diverges into branch ridges as in Figure 1.

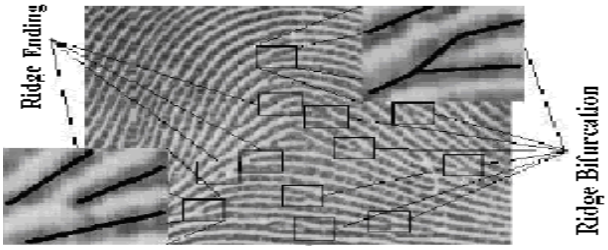

Figure 1. Examples of ridge and bifurcation

Most of the minutia detection methods which have been proposed in the literature are based on image binarization, while some others extract the minutia directly from Gray scale images [3]. This work proposes a method to generate secure and strong multi-purpose code for fingerprint images.

After introduction, section 2 describes proposed system briefly together with the algorithm used. Section 3 outlines the developed programs for image preparation includes both enhancement and thinning. Section 4 presents the feature extraction process for code generation.

Section 5 discuses hashing and security of the obtained results and finally section 6 concludes the work.

2 The Proposed System

The fingerprints image for any person can be utilized to generate unique code. The fingerprint image passes through a sequence of operations that includes lightening, smoothing, edge detection and binarization, then proceeds to thinning process and then an initial code is generated, prior to final secure code achievement. This section summarizes these processes in few steps are shown in algorithm 1.

Algorithm (1): The Proposed System:

Step-1: Obtain the fingerprint image for which a secure code is needed.
Step-2: Use image processing concept, enhance the fingerprint image according to the following sequence

Lightening è Smoothing è Edge Detection è Binarization

*{**Note**: A computer program is written in Delphi language to perform the above sequence of processes. The resulting interface screen is shown in figure 3 }*

Step-3: Perform thinning process on the binarized output image of step 2.
Step-4: Extract the features of fingerprint image after step 3 and construct an initial code block.
Step-5: Apply hashing **MD5** algorithm on the obtained initial code block of step 4 in order to find the secure code.

The above algorithm summarizes the proposed system steps to produce the secure code. The whole process consists of three types of actions; image preparation, feature extraction and hashing. These actions are outlined in the following sections in more details.

The code block pattern is built of five sub-blocks, embedded in between a header and a trailer. These sub-

blocks are reflections of the five chosen characteristic parameters of the minutia in a fingerprint image, which will be defined later in section 5.

Suitable lengths (in bytes) are chosen by authors for each parameter as follows: [type (3bytes),orientation (2 bytes), spatial frequency (1 byte), curvature (1 byte) and position (1 byte)]. Figure 2 shows a schematic diagram for this code block pattern together with the chosen length for each sub-block.

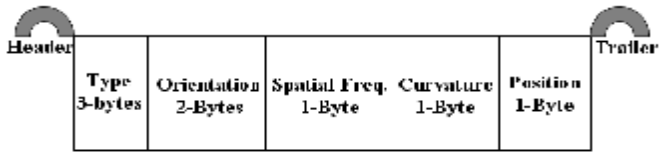

Figure 2. Structure of Fingerprint code-block pattern

The obtained code block pattern is then hashed using the widely known one way hash function (MD5 algorithm) [5 - 8] in order to achieve the final secure code. The following algorithm summarizes the proposed system steps to produce the secure code.

3 .Image Preparations

Two major treatments are involved in fingerprint preparation; image enhancement and thinning.

3.1 Image Enhancement:

In order to normalize the starting image some binarization-based approaches are applied. The binarization and thinning processes must be preceded by smoothing operation, based on convolution with a mask [9 - 11]. The image enhancement phase consists of lightening, smoothing, edge detection and binarization processes. One filtering program written in Delphi language is developed combining all these operations. The main interaction screen for this program is shown in Figure 3. Lightening and

smoothing combined together as one stage is called pre-processing enhancement while edge detection and binerization combined together is called post-processing enhancement.

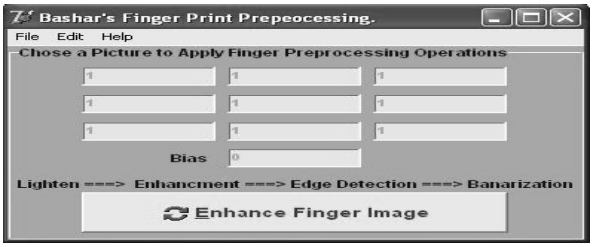

Figure 3. Proposed Enhancement Process

a. Pre-processing Enhancement

This stage consists of lightening and smoothing processes. Sobel and lightening filters are implemented used in order to get an enhanced fingerprint image. Since contrast is expanded for most of the image pixels, the transformation improves the delectability of many image features. A pixel-wise adaptive Wiener method for noise reduction is also applied and the results are shown in figure 4 [12, 13].

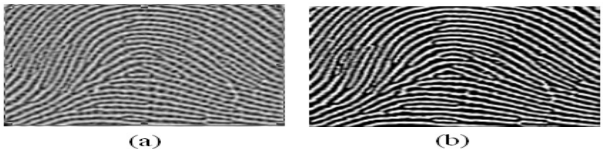

Figure 4. Fingerprint image (a) before pre-processing (b) after pre-processing

b. Post-processing Enhancement

The operation that converts a grayscale image into a binary image is known as binarization [14]. We carried out the binarization process using adaptive threshold. Each pixel is

assigned a new value (1 or 0) according to the mean intensity in the local neighborhood, using equation 1. 13 * 13 pixels frames are used throughout the experimental work.

$$I_{new}(n1, n2) = 1 \quad \text{if} \quad I_{old} >= \text{Local mean.} = 0 \quad \text{otherwise} \qquad .....(1)$$

Where I_{new} and I_{old} are the new and old frame intensity.

3.2 Image Thinning

After these image enhancement operations, Optimized Parallel Thinning Algorithm (OPTA) [15, 19] is applied and the resulting program interface is shown in figure 5 prior to feature extraction stage.

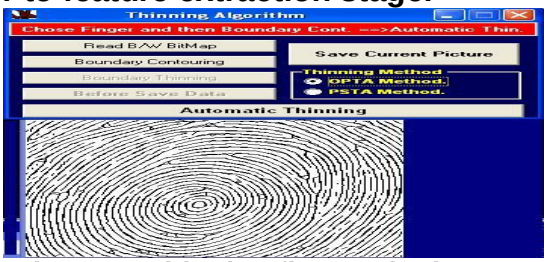

Figure 5. Thinning fingerprint image.

4. Feature Extraction

The thinned fingerprint image is scanned for the extraction of the minutia features. The results are saved in a secured database for identification purposes. The minutia point's characteristics considered in this paper include termination, bifurcation, lake, independent ridge, dot or island, spur and crossover as summarized in figure 6. [1, 16, 17]

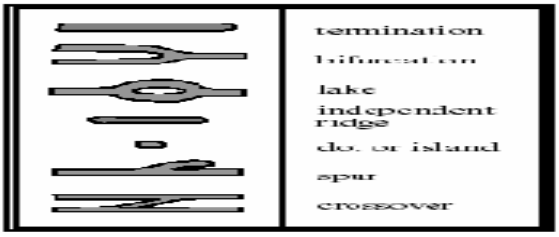

Figure 6. Minutia Points Characteristics.

Five parameters for these minutia points are considered for the proposed idea of features extraction program used. These parameters are type, orientation, spatial frequency, curvature and position. They are referred to as follows: [18]

1. **Type: Specifies the type of minutia points. This may be Ridge Termination (RGT), Ridge Bifurcation (RGB), Lake (LAK), Dot (DOT), Short Ridge (SHT), Spur (SPR) or Crossover (CVR). Three bytes allocated for this parameter.**
2. **Orientation: Each minutia point faces a particular direction. It is either clockwise (CW) or counter clock wise (CC). Two bytes are allocated for this parameter.**
3. **Spatial Frequency: Refers to how far apart the ridges are in the neighborhood of the minutia point. This is measured in pixels and only one byte is allocated for this parameter.**
4. **Curvature: Refers to the rate of change of ridge orientation. This is measured in pixels and only one byte is allocated for this parameter.**
5. **Position: Refers to its x, y location. It is measured either in absolute sense or relative to fixed points such as the Core or Delta points. One byte is allocated for this parameter.**

There are number of basic ridge pattern groupings which have been defined. Three of the most common are loop, arch and whorl. The LOOP is the most common type of fingerprint pattern. Statistically, it accounts for about 65% of all classification of fingerprint features [2, 18]. There are many types of loops as shown in figure 7-a. The ARCH pattern is a more open curve than the Loop. There are two types of arch patterns, the Plain Arch and the Tented Arch as shown in figure 5-b.

The WHORL patterns occur in about 30% of all fingerprints and are defined by at least one ridge that makes a complete circle as shown in figure 7-c. [2]

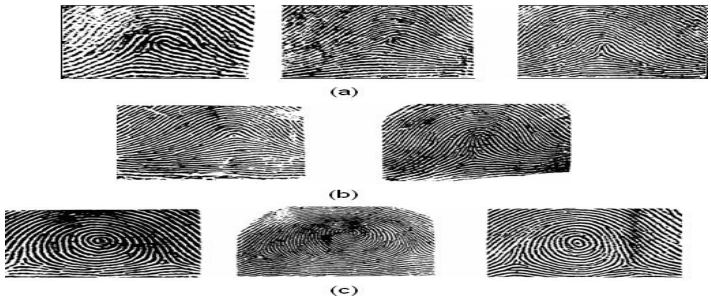

Figure 7. Basic Ridge Pattern Groupings, (a) loop, (b) Arch, (c) Whorl.

Depending on these features, we generate a string of 14 bytes length as an initial code that is saved in a database .Then this entry or code is passed to the one-way hash MD5 algorithm to generate the secure Multi-Purpose Code.

5. Hashing and Security of the Code

The Structure of Fingerprint extracting pattern is illustrated in figure 5. More details description about the contents of each field of this pattern is given below:

- **Header: header of the initial pattern. (3-bytes in length).**
- **Type: 3-Bytes which may contain RGT, RGB, SPR, DOT, LAK, SHT or CVR symbols, i.e. it is one of seven choices.**
- **Orientation: 2-Bytes which may be contain CW or CC.**
- **Spatial Frequency: 1-Byte which may contain values ranges from 1 to 255.**
- **Curvature: 1-Byte which may contains values ranging from 5 to 60 in steps of 5.**

- **Position: 1-Byte which may contain values ranges from 0 to 255 in steps of 1.**
- **Trailer: Trailer of the initial code. (3-bytes in length).**

After the system gets the previously described features, a one way hash function, MD5 is applied to generate a code, giving strong one way secure pattern. The strength of this code can be illustrated as follows:

- **The length of the code (14-bytes).**
- **The personal fingerprint features can not be retrieved or generated back from secure code because MD5 is a one way hash function.**
- **Analysis of the generated features code may prove to be complex because the samples rate of putting features deals with $1.2x10^{13}$ test items.**
- **Saving of generated secure code in the identification data base is normalized, i.e. all generated codes have same code length. This code is unique for the person, whose fingerprint image is in the question.**

6. Conclusions

A novel fingerprint representation technique that uses minutia extraction and core detection has been demonstrated. Experiments indicate that the computation of the orientation field performs much better than a purely minutia based matching scheme. Currently, core information is being used to align the image and then trace vectors to the bifurcations. The magnitudes of the vectors are used also as characteristics for the fingerprint image along with the extracted minutia. The resulting secure code is unique for each fingerprint and therefore, it might be used as a mean to generate private keys personalized to the signatories. Moreover, the generated secure code may be beneficial for other related application areas, such as:
(1) New matching methods for comparing the ridge feature maps of two images of the same fingerprint.

(2) Constructing the ridge feature maps, using adaptive methods for optimal selection of the Gabor filters.
(3) State of the art applications of the fingerprint matching algorithm.

References:

[1] A. K. Jain, A. Ross and S. Prabhakar, **Fingerprint Matching Using Minutia And Texture Features**, *Proceedings of the International Conference on Image Processing (ICIP)*, Thessaloniki, Greece, Vol. 3, 2001, pp 282-285.
[2] R. Cappelli, D. Maio and D. Malton, **Fingerprint Classification By Directional Image Partitioning,** *IEEE Trans. Pattern Anal. Mach. Intell*. Vol. 21, No. 5, 1999, pp 402-421.
[3] A. K. Jain, L. Hong and R. Bolle, **On-line Fingerprint Verification,** *IEEE Trans. Pattern Anal. Mach. Intell*. Vol. 19, No. 4, 1997, pp 302-314.
[4] K. Valstimil, **Tunnels in Hash Functions: MD5 Collisions within a Minute,** *IACR ePrint archive Report 2006/105*, 18 March, 2006.
[5] R. Ronald, **The MD5 Message Digest lgorithm**,*ftp://ftp.rfc-editor.org/in-notes/rfc1321.txt*, 1992.
[6] X. Wang et. al., **Collisions for Hash Functions MD4, MD5 and RIPEMD, *Rump session, CRYPTO*,** *http://eprint.iacr.org/2004/199.pdf*, 2004.
[7] J. Liang and X. Lai, **Improved Collision Attach on Hash Function MD5, Cryptology** *ePrint Archivehttp://ePrint.iacr.org/2005/425.pdf*, Nov. 2005.
[8] L. Hong, Y. Wan and A. Jain, **Fingerprint Image Enhancement: Algorithm and Performance Evaluation**, *IEEE Transaction on Pattern Analysis and Machine Intelligence*, Vol. 20, No. 8, 1998, pp 777-789.
[9] L. Hong, A. Jain et. al., **Fingerprint Enhancemen**t, *Proceeding of the First IEEE WACV, Sarasota*, Vol. 20, No. 8, FL, 1996. pp 202-207.

[10] D. Sherlack et.al., **Fingerprint Enhancement by Directional Fourier Filtering,** *IEEE Proceedings on Visual Imaging Signal processing,* 1994, pp 87-94.

[11] L. O'Gorman. and J. Nicherson, **An Approach to Fingerprint Filter Design, *Pattern Recognition*,** Vol. 22, No. 1, 1989, pp 29-38.
[12] W. T. Freeman and E. Adelson, **The Design and use of Steerable Filters,** *IEEE Transactions on Pattern Analysis and Machine Intelligence*, Vol. 13, No. 9, 1991, pp 891-906.
[13] R. C. Gonzalez and R. E. **Woods, *Digital Image Processing***, New York, USA, Addison-Wesley, 1993.
[14] P. Perona, **Steerable-Scalable Kernels for Edge Detection and Junction Analysis**, *Image and Vision Computing*, Vol. 10, No. 10, 1992, pp 663-672,
[15] J. Hollingum, **Automated Fingerprint Analysis Offers Fast Verification**, *Sensor review*, Vol. 12, No. 3, 1992, pp 12-15.
[16] D. Mario and D. Maltoni, **Direct Gray-scale Minutia Detection in Fingerprint,** *IEEE Tans. Pattern Analysis and Machine Intelligence*, Vol. 19, No. 1, 1997, pp 27-40.
[17] B. Moayer And K. Fu, **A tree system Approach for Fingerprint Pattern Recognition,** *IEEE Transaction on Pattern Analysis and Machine Intelligence*, Vol. 8, No. 3, 1986, pp 376-388.
[18] A. Jain, K. Prabhakar, L. Hong and S. Pankanti, **Filter bank based fingerprint matching,** *IEEE Trans. Image Process,* Vol. 9, No. 5, 2000, pp 846-859.
[19] O. Baruch, **Line Thinning by Line Following, *Pattern Recognition Letters*,** Vol. 8, No. 4, 1998, pp 271-276.

توليد الرمز الآمن متعدد الأغراض باستخدام بصمة الأبهام

د. بشار مكي نعمة* نها سامي محسن**

المستخلص

عملية استخلاص الصفات ذات الأهمية العالية من بصمة الأبهام تعد واحدة من الخطوات المهمة للتمهيد لعملية التعرف او التصنيف لبصمة الأبهام. يعمل البحث المقترح على وضع طريقة مبتكرة لغرض تكوين او توليد نموذج سري يملك خصائص العشوائية العالية وكذلك العدد الكبير من الأحرف التي من الممكن استخدامها لاحقا في الكثير من التطبيقات مثل تطبيقات الدخول على الماسنجر او البريد الألكتروني ..الخ.تتكون الطريقة المقترحة من مرحلتين، الأولى تتلخص بتحسين وتمثيل بصمة الأبهام بواسطة استخدام ادوات معالجة الصور، اما المرحلة الثانية فنستخلص بها مجموعة من الخصائص الوحيدة من البصمة التي تعد اساسا للتعريف بالشخص البشري. واخيرا بالعتماد على تلك الخصائص المستخلصة يكوّن الرمز السري باستخدام ال MD5 .توصل البحث الى مجموعة من الحقائق والنتائج ذات الأهمية العالية.

*الجامعة المستنصرية
** جامعة بغداد