Multi Purpose Code Generation Using Fingerprint Images

Bashar Ne'ma and Hamza Ali
Software Engineering Department, Isra Private University, Jordan

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.*

Keywords: *Fingerprint matching, image enhancement, reference point, code generation, embedded system.*

Received December 31, 2007; accepted May 22, 2008

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 [3, 13]. 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.

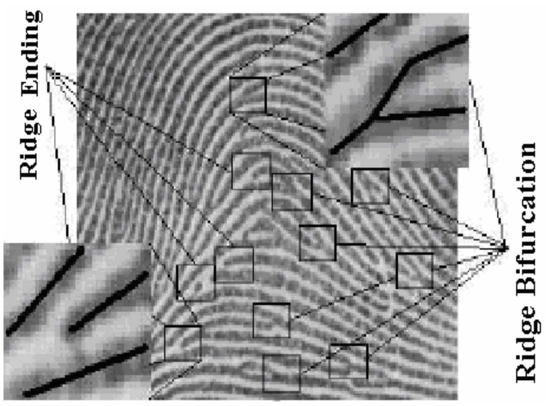


Figure 1. Examples of ridge and bifurcation.

The problem of assessing fingerprint image quality and identification has been addressed by many papers in biometric literature. Nill & Bouzas [18] proposed an objective image quality based on the digital image power of normally acquires scenes. Their system is designed to assess the quality of digital images and can be applied to fingerprints as well. Bolle [2] used ratio of directional area to other non-directional area as a quality measure. Shen *et al*. [23] applied Gabor filter to image sub-blocks in order to identify blocks with clear repetition of ridge and valley pattern as good quality blocks. Both previous approaches only use the local orientation information but neglect information on global uniformity and continuity.

The configurations of ridges and valleys within a local neighborhood vary with the quality of input fingerprint images, therefore a well defined sinusoidal shaped wave of ridges and valleys may not always be observed. Global features are needed for a more precise region mask classification. They both use subjective method to test the performance of their proposed quality analysis algorithms.

Ratha and Bolle [21] proposed a method for image quality estimation from wavelet compressed fingerprint image, where the fingerprint image is WSQ compressed. Still However, evaluating their quality measure is still a subjective matter.

Hong *et al.* [9] modeled the ridge and valley pattern as sine wave, and computed the amplitude, frequency as well as the variance of the sine wave in order to decide the quality of the fingerprint. They classified regions of fingerprint as recoverable or unrecoverable. If the percentages of recoverable blocks are smaller than a specified threshold, the input fingerprint is rejected as poor quality.

Lim and Yau [14] have proposed algorithms for estimating quality and validity of fingerprint images in spatial domain. They verify the repetition of ridge and valley patterns by the ratio of the eaten values obtained from covariance matrix for the image block's grey-level gradient. They use the quality of the feature extracted from the fingerprint images by the automatic fingerprints identification system as the benchmark in order to test the performance of their proposed image quality analysis procedure. Their system is aimed to flag poor quality or invalid fingerprint images.

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 [12, 26]. This work proposes a method to generate secure and strong multi-purpose code for fingerprint images.

After this introduction, section 2 describes the proposed system briefly together with the algorithm used. Section 3 outlines the developed programs for image preparation that 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 below in algorithm 1. This 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 (3 bytes), 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.

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 (Smoothing (Edge Detection (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.

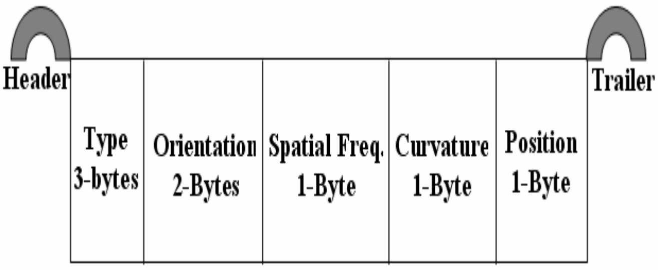


Figure 2. Structure of fingerprint code-block pattern.

The obtained code block pattern is then hashed using the widely known one way hash function (MD5 algorithm) [11-14] in order to achieve the final secure code. Algorithm 1 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 [15, 16, 17]. 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.

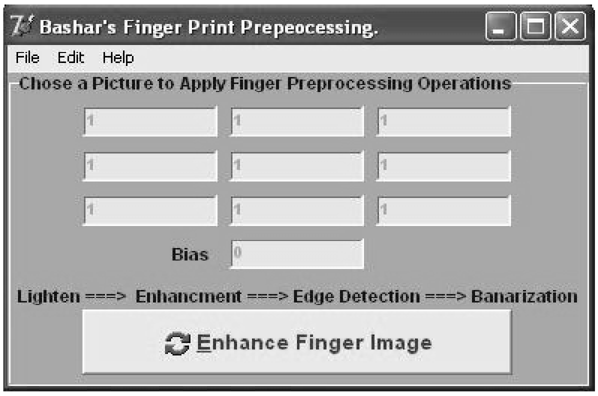
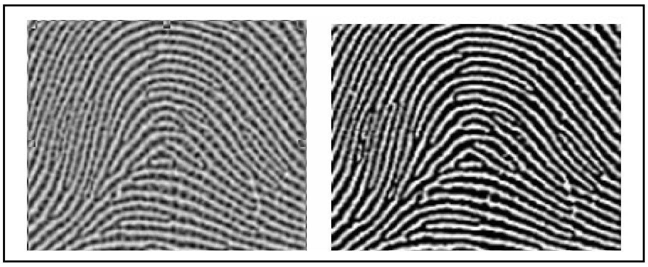


Figure 3. Proposed enhancement process.

3.1.1. 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 [6, 7].



(a) Before pre-processing. (b) After pre-processing.

Figure 4. Fingerprint image.

3.1.2. Post-Processing Enhancement

The operation that converts a grayscale image into a binary image is known as binarization [20]. 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.

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

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) [1, 8] 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 [13, 15, 17].

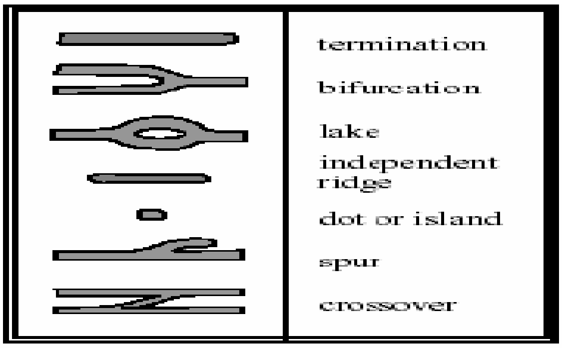


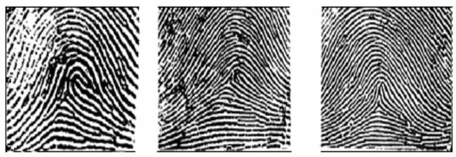
Figure 6. Minutia points characteristics.

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 [12]:

- 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.
- 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.
- 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.
- Curvature: refers to the rate of change of ridge orientation. This is measured in pixels and only one byte is allocated for this parameter.

- 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 [3, 12]. 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) [3].



(a) Loop.

(b) Arch.

(c) Whorl.

Figure 7. Basic ridge pattern groupings.

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 1.2×10^{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. Results Evaluation

Most reported approaches in the literature for singularity detection operate on the fingerprints image orientation, where the core point is the most commonly used reference point. A core point is defined as the point at which maximum direction change is detected in the orientation field of a fingerprint image or the point at which the directional field becomes discontinuous. The method implemented in the proposed work is based on the computation of the orientation field described before, and the application of a filter to detect the maximum direction change of the ridge flow. This approach can even locate an imaginary reference point in an arch type fingerprint image [3].

Experiment indicates that computation of the orientation field performs much better than a purely minutiae-based matching scheme. Currently, core information is being used to align the image and then trace vectors to the bifurcations; the vectors magnitudes are use as characteristics from the image along with the extracted minutiae also. The following areas of improvement are also being studied:

- New matching methods for comparing the ridge feature maps of two images of the same fingerprint.
- Constructing the ridge feature maps, using adaptive methods for optimal selection of the Gabor filters.
- State of the art applications of the fingerprints matching algorithm

6.1. Comparison of Binarization Based Methods

The proposed binarization-based method is compared with some other similar techniques. Maio [15] reports the average error percentage obtained with four different schemes marked B, C, D and E, which were based on binarization and thinning. We used fingerprints from the same sample set of Maio in order to compare those four schemes to our binarization scheme, named F. The sample set is composed of 5 fingerprints taken from real persons and 3 from auto created fingerprints. Figure 8 illustrates the comparison for the average error percentage obtained for the five different approaches. These results are reported in terms of undetected (dropped), non-existent (false), and type exchanged (exchanged) minutiae.

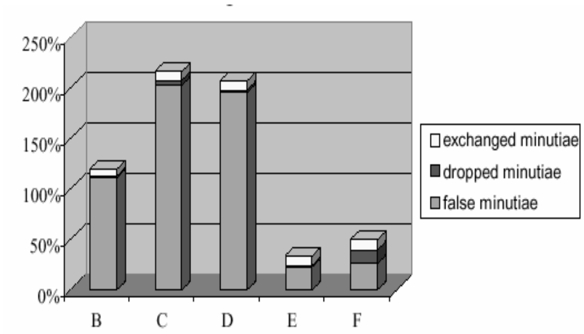


Figure 8. Comparison of 5 binarization based schemes.

6.2. Comparison of Direct Gray-Scale Methods

The enhancement results conducted on grayscale images by three different methods are compared. These three methods are (1) direct grayscale miniature detection, referred to as *G*, (2) modified Gabor-based filtering, referred to as *H* and (3) the suggested filtering method, referred to as *I*. Moreover, the comparison is extended to include the obtained results for the proposed binarization based approach, referred to as *F*. Figure 9 shows the comparison for the average error percentage obtained with methods *G, H, I* and *F*, for the same sample set as in section 6.1.

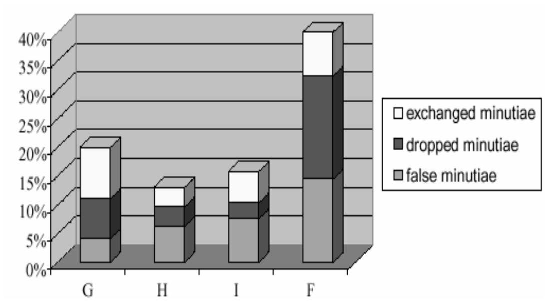


Figure 9. Comparison of 4 gray-scale approaches.

Moreover, some enhanced fingerprint images reported in reference [28] and obtained with the Gabor-based algorithm are compared those obtained by the proposed technique in this paper. The results are shown in Figure 10 and they clearly show the achieved improvement.

Figure 10. Enhancement results original gabor modified gabor and the proposed filter.

7. 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:

- New matching methods for comparing the ridge feature maps of two images of the same fingerprint.
- Constructing the ridge feature maps, using adaptive methods for optimal selection of the Gabor filters.
- State of the art applications of the fingerprint matching algorithm.

References

[1] Baruch O., "Line Thinning by Line Following," *Computer Journal of Pattern Recognition Letters*, vol. 8, no. 4, pp. 271-276, 1998.

[2] Bolle A., "System and Methods for Determining the Quality of Fingerprint Images," *Technical Report US596356*, 1999.

[3] Cappelli R., Maio D., and Malton D., "Fingerprint Classification by Directional Image Partitioning," *Computer Journal of IEEE Transactions on Pattern Analysis Machine Intelligent*, vol. 21, no. 5, pp. 402-421, 1999.

[4] Cappelli R., Maio D., and Maltoni D., "Fingerprint Classification by Directional Image Partitioning," *Computer Journal of IEEE Transactions on Pattern Analysis Machine Intelligent*, vol. 21, no. 5, pp. 402-421, 1999.

[5] E-Print Archive*, http: //e Print. iacr .org/2005 /425.pdf*, 2005.

[6] Freeman T. and Adelson E., "The Design and Use of Steerable Filters," *Computer Journal of IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 13, no. 9, pp. 891-906, 1991.

[7] Gonzalez C. and Woods E., *Digital Image Processing*, USA, Addison Wesley, 1993.

[8] Hollingum J., "Automated Fingerprint Analysis Offers Fast Verification," *Computer Journal of Sensor Review*, vol. 12, no. 3, pp. 12-15, 1992.

[9] Hong L. and Jain A., "Fingerprint Enhancement," *in Proceedings of the First IEEE WACV Sarasota*, Florida, pp. 202-207,1996.

[10] Hong L., Wan Y., and Jain A., "Fingerprint Image Enhancement: Algorithm and Performance Evaluation," *Computer Journal of IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 20, no. 8, pp. 777-789, 1998.

[11] Jain K., Hong L., and Bolle R., "On Line Fingerprint Verification," *Computer Journal of IEEE Transactions on Pattern Analysis Machine Intelligent*, vol. 19, no. 4, pp. 302-314, 1997.

[12] Jain K., Prabhakar L., Hong H., and Pankanti S., "Filter Bank Based Fingerprint Matching," *Computer Journal of IEEE Transactions on Image Processing,* vol. 9, no. 5, pp. 846-859, 2000.

[13] Jain K., Ross A., and Prabhakar S., "Fingerprint Matching Using Minutia and Texture Features," *in Proceedings of the International Conference on Image Processing (ICIP)*, Greece, pp. 282-285, 2001.

[14] Lim E., Jiang X., and Yau W., "Fingerprint Quality and Validity Analysis," *in Proceedings of IEEE ICIP*, USA, pp. 469-472, 2002.

[15] Mario D. and Maltoni D., "Direct Gray Scale Minutia Detection in Fingerprint," *Computer Journal of IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 19, no. 1, pp. 27-40, 1997.

[16] Mario D. and Maltoni D., "Direct Gray Scale Minutiae Detection in Fingerprints," *Computer Journal of IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 19, no. 1, pp. 27-40, 1997.

[17] Moayer B. and Fu K., "A Tree System Approach for Fingerprint Pattern Recognition," *Computer Journal of IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 8, no. 3, pp. 376-388, 1986.

[18] Nill N. and Bouzas H., "Objective Image Quality Measure Derived from Digital Image Power Spectra," *Computer Journal of Optical Engineering*, vol. 31, no. 4, pp. 813-825, 1992.

[19] O'Gorman L. and Nicherson J., "An Approach to Fingerprint Filter Design," *Computer Journal of Pattern Recognition*, vol. 22, no. 1, pp. 29-38. 1989.

[20] Perona P., "Steerable-Scalable Kernels for Edge Detection and Junction Analysis," *Computer Journal of Image and Vision Computing*, vol. 10, no. 10, pp. 663-672, 1992.

[21] Ratha K. and Bolle R., "Fingerprint Image Quality Estimation," *IBM Computer Science Research Report RC21622*, 1999.

[22] Rump Session CRYPTO, *http: //eprin t.iacr.org /2004/199.pdf*, 2004.

[23] Shen L., Kot A., and Koo M., "Quality Measures of Fingerprint Images," *in Proceedings of 3rd International Conference AVBPA,* pp. 182-271, 2001.

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

[25] The MD5 Message Digest Algorithm, ftp: //ftp .rf c-editor .org/in-notes /rfc1321.txt, 1992.

[26] Valstimil K., "Tunnels in Hash Functions: MD5 Collisions within a Minute," *IACR E Print Archive Report 2006/105*, 2006.

Bashar Ne'ma is an assistant professor at the Faculty of Science and Information Technology at Isra Private University, Jordan. He got his BSc in 1999 from Al-Manssor University College, Iraq and MSc and PhD in 1999 and 2004 respectively, from University of Technology, Iraq, in computer science.

Hamza Ali is an associate professor at the Faculty of Science and Information Technology at Isra Private University, Jordan. He got his BSc in 1968 from Basrah University, MSc and PhD in 1973 and 1977, respectively, from The University of London, UK.