Generation of Reliable PINs from Fingerprints

Conference Paper · July 2007

DOI: 10.1109/ICC.2007.202 · Source: IEEE Xplore

Han Fengling
RMIT University

Jiankun Hu
UNSW Australia

This full text paper was peer reviewed at the direction of IEEE Communications Society subject matter experts for publication in the ICC 2007 proceedings.

Generation of Reliable PINs from Fingerprints [1]

Fengling HAN, Jiankun HU, Leilei HE, Yi WANG

School of Computer Science and Information Technology,
Royal Melbourne Institute of Technology, Melbourne VIC 3001, Australia.

Abstract—**Generating reliable biometric passwords/PINs is a very challenging research topic in access security control. This paper provides a method for the generation of a reliable password/PIN from fingerprint images. A fictitious triangle whose sides are composed of lines connecting two minutiae points closest to the core of a fingerprint image is constructed. The maximal side, the minimal and medial angles, together with the minutiae type involved in the three sides of this triangle are used as the source of password/PIN generation. The noise-tolerant transform criteria convert a decimal value to one digit PIN is provided. Experiments based on public database are presented.**

I. Introduction

Sensitive information should only be accessed by legitimate users. With the overall level of fraud steadily rising, access security becomes more and more important. There are three main ways to authenticate an identity: 1) *Knowledge-based*: Something you know, like password or personal identification number (PIN); 2) *Token-based*: Something you have, like a smartcard; and 3) *Biometric-based*: something you are, a measurable trait. Knowledge-based techniques are currently the most frequently used method for user authentication. Most token-based authentication systems also use knowledge-based authentication to prevent impersonation through theft or loss of the token.

A PIN is a secret shared between a user and a system for access control. In operation, a user is required to provide a login name or token (such as a banking card) and a confidential PIN to gain access to the system. Upon receiving the User ID and PIN, the system will compare the received PIN with the template PIN under the claimed user ID. If they match, then the user is granted the access. If they do not match, the access request is denied. Despite their wide usage, password/PIN has a number of shortcomings. Simple or meaningful PINs are easier to remember, but are vulnerable to attack. PINs that are complex and arbitrary are more secure, but are difficult to remember. Since users can only remember a limited number of PINs, they tend to write them down or will use similar or even identical PINs for different purposes. To make thing worse, password/PIN based authentication scheme can not assure that the user is who s/he claims to be. A correct password/PIN does not verify the identity of a person, it only verifies that the person has the right information [1]. This is an inherently serious flaw for the conventional password/PIN technology.

As an alternative to password/PIN authentication technology, biometric authentication has now become more popular in civilian applications such as access control, financial security et al. [2]. Biometrics is the science of identifying individuals by a particular physiological or behavioral characteristic, such as voice, fingerprint, face, iris or signature et al. Fingerprints are arguably the most popular biometric currently in use [3]. Biometric techniques may ease many of problems in password/ PIN systems: they can confirm that a person is actually present and without requiring the user to remember anything.

A biometric system may be viewed as a pattern recognition system whose function is to classify a biometric signal into one of several identities (identification) or into one or two classes – genuine and imposter users (verification). The most difficult problem in providing a biometrics password/PIN is the unreliability of biometric features while PIN demands correctness in every digit [4].

Two prints of the same finger are rarely identical, even though they are likely to be close. Fingerprint triangle which gives immunity against noise and distortion was first proposed by Germain et al. [3]. Bhanu and Tan reported a fingerprint indexing approach with features of minutiae triangle [5] and [6]. This paper presents a scheme of generating reliable passwords/PINs from a fictitious triangle that is constructed by three lines connecting two minutiae points closest to the core. Compared with the minutiae triangle used in Refs. [3], [5] and [6], the parameters in this triangle are more stable. Therefore, a transform which tolerates a limited number of errors in the pasword/PIN could be achieved. This authentication scheme is very useful in mobile applications (embedded systems such as smart cards, mobile devices et al.) because it is simple, cheap and has a quite high level of security even the device is lost or stolen.

The rest of this paper is organized as follows. Section II provides related work on the fingerprint personal authentication. Section III proposes the scheme of generating reliable passwords/PINs from fingerprint images. Section IV is the conclusion.

[1] The work is financially supported by the ARC Linkage project **LP0455324.**

1-4244-0353-7/07/$25.00 ©2007 IEEE

II. Fingerprint Personal Authentication

This section introduces some background knowledge of fingerprint personal authentication.

A. Fingerprint personal authentication (FPA)

Fingerprint is the most widely used biometric authentication technology [3], [7]. A human fingerprint contains a rather smooth flow of ridges. The pattern of ridges on each person's fingers uniquely characterizes that individual and contains sufficient information to distinguish that people from any other [3]. Typically, FPA systems rely on ridge endings and ridge bifurcations, which are called minutiae as shown in Fig.1. The major strength is that these features of fingerprints are unique. A typical fingerprint image contains 40 minutiae. The Federal Bureau of Investigation (FBI) in the US claims that no two individuals can have more than eight common minutiae [8]. Another strength is that fingerprint devices can be made very small and rather cheap, therefore they can be suitable for many civilian applications especial in mobile applications.

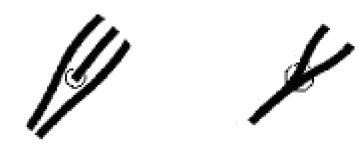
There are two general ways in which fingerprint based biometric systems are used: verification and identification. Identification answers the question "who is this person". It means that the system checks all the stored identities for a match. This is also called a one-to-many comparison. Verification answers the question "are you the person you claim to be". This is also called a one-to-one comparison. If the matching is performed on the smartcards, it will always be a question of verification. The algorithm of fingerprint personal verification system consists of two steps:

1) Registration (enrolment): a number of interested parameters are extracted from the fingerprint image.

2) Verification: the template is used in comparison with a query fingerprint image.

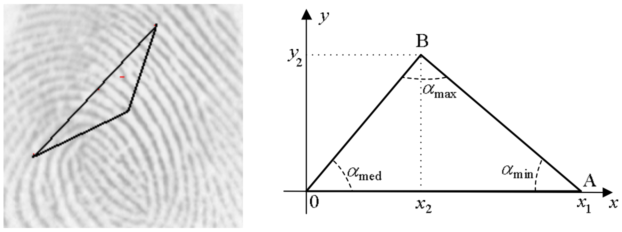
B. Minutiae triangles in fingerprint indexing

Fig.2a shows a minutiae triangle in a fingerprint image. Features of triangular used in fingerprint indexing have been presented in Refs. [3], [5] and [6]. In [3], the full index consists of the length of three sides, three angles measured with respect to the fiducial side and the ridge count between each pair. In [5] and [6], triangle's angles, handedness, type, direction, and maximum sides are used as features in fingerprint indexing and classification



(a) (b)

Figure 1. (a) Ridge ending; (b) Ridge bifurcation.



(a) (b)

Figure 2 Minutiae triangle in a fingerprint image. (a) FVC2000 Db1_a_8; (b). A minutiae triangle

Since the finger is not a rigid object and the process of projecting the three-dimensional shape of the finger onto the two-dimensional sensor surface is not precisely controlled, different impressions of a finger are related to each other by various transformation [5]. It is assumed that one vertex, *O*, of triangle is (0, 0), and it is not changed under distortion. Suppose the location of points A and B are $(x_1, 0)$ and (x_2, y_2), $x_1>0$, $y_2>0$, and $x_2 \in (-\infty, +\infty)$ in Fig.2b. Because of the uncertainty of minutiae locations, A and B move to $A'(x_1+\Delta x_1, 0)$ and $B'(x_2+\Delta x_2, y_2+ \Delta y_2)$, respectively, and α changes to $\alpha+\Delta\alpha$. In Ref. [5] and [6], the analysis of angle changes under distortions showed that angles are invariant under translation, rotation and scale. The maximal side, the minimal angle (α_{min}) and the medial angle (α_{med}) in a minutiae triangle are taken as components of the index to construct a model database for fingerprint identification [5].

III. Proposed Password/PIN Generation From Fingerprint Images

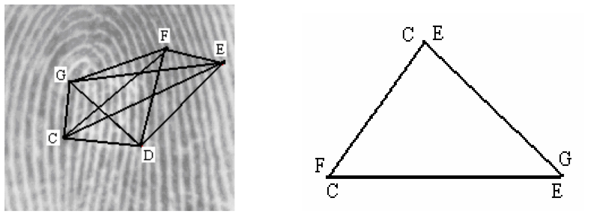
Due to the presence of spurious points and the missing of some minutiae, the minutiae are unique but unreliable. Experiments show that the minutiae closest to core in fingerprints image are relatively stable.

In this paper, a fictitious triangle constructed from three lines, each of them connecting two minutiae points closest to core in a fingerprint image is used in the generation of PIN. This section proposes a scheme of password/PIN generation from fingerprint images.

A. Construction of the triangle and parameters analysis

In this scheme, the fictitious triangles are constructed by the following rules:

1) Pick up five minutiae points closest to core, C, D, E, F and G in fingerprints images;



(a) (b)

Figure 3 (a) Five minutiae points and lines between any two points with DB1_a_11; (b) A triangle constructed with the three longest lines in (a).

2) Calculate the distances between any two points, as shown in Fig.3a;

3) Construct a triangle with the three longest lines as shown in Fig.3b.

Note that the selection of triangle in Fig.3b is different from that in Refs. [3], [5] and [6]. The fictitious triangles in our work are constructed using three longest lines, CE, GE and CF. This triangle concerns four minutiae points C, E, F, G. Extensive experiments have been conducted both on the minutiae triangle in the above mentioned references and the fictitious triangle proposed in this paper. It is observed that short sides appearing in random minutiae triangles are more sensitive to errors which are not present in the proposed triangles. Parameters in the fictitious triangles proposed here are more robust to noise than those in the minutiae triangle.

We can move the proposed fictitious triangle to the Cartesian coordinate system. Referenced to the triangle shown in Fig.2b, the length of the maximal side is x_1, the minimal angle, α_{min}, and the medial angle, α_{med}, can be expressed as:

$$\alpha_{min} = \frac{x_2(x_2 - x_1)}{x_1\sqrt{(x_1 - x_2)^2 + y_2^2}} \qquad (1)$$

$$\alpha_{med} = \frac{x_2}{\sqrt{x_2^2 + y_2^2}} \qquad (2)$$

x_1, α_{min} and α_{med} in this fictitious triangle together with the type of minutiae involved in the starting and ending points are selected for generating a reliable password/PIN.

In order to generate a PIN, the parameters in this triangle are studied further. We take FVC2000 database for experiments. The average values of x_1, α_{min} and α_{med} with 50 fingers each having 8 impressions are as shown in Fig.4.

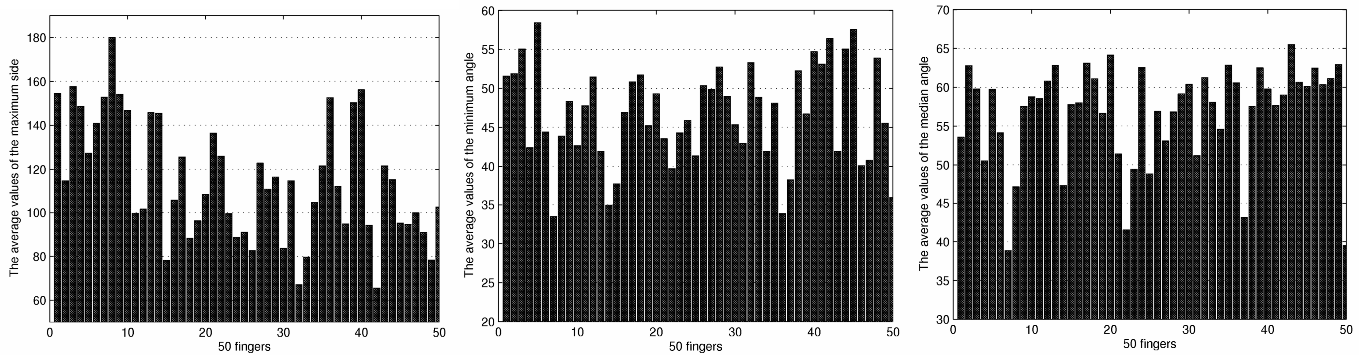
Due to the presence of deformations, the impressions of each finger can not always be exactly the same. The variations of x_1, α_{min} and α_{med} with 50 fingers with each having 8 impressions, are illustrated in Fig.5. The deviation of each quantity, $\bar{E}$, is calculated by:

$$\bar{E} = E_{\max} - E_{\min} \qquad (3)$$

From Fig.4, for 50 fingers with 8 different impressions each, the average values of x_1 varies from 65 to 181, α_{min} varies from 33.5° to 58.4°, and α_{med} from 38.9° to 65.5°. And from Fig.5, the difference between the maximum and the minimum values of the maximal side, x_1, of 50 fingerprints in database varies from 2.2 to 11.2; for the minimal angle, varies from 0.7° to 5.6°, and the medial angle, from 0.6° to 4.5°. Based on the distribution of these three values and their variation range, a transform to each quantity can be design. After the transformation, the quantity corresponding to each of three values with different impressions of same finger should always keep the same.

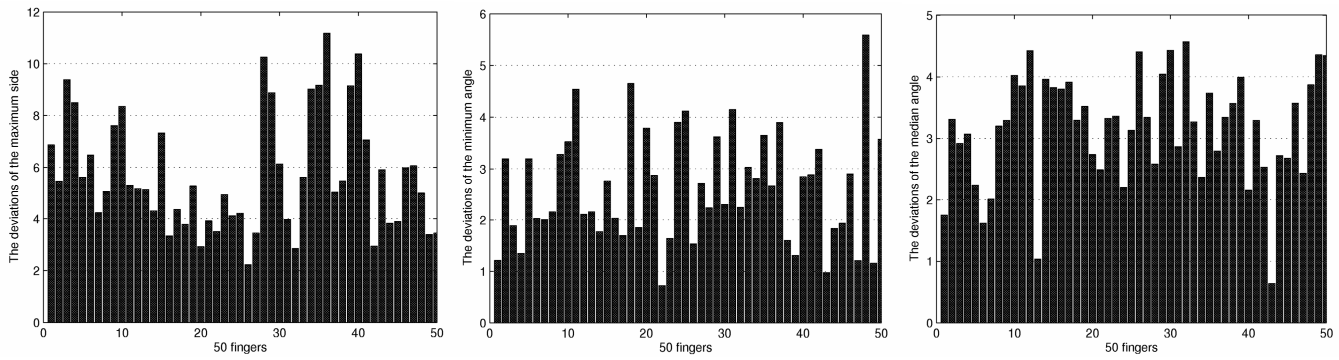
B. PIN generation from fingerprint image

In this research, a nine-digit PIN(k) (k=1, …, 9) composed of two parts is produced from each finger. The first part is a six-digit binary PIN(1),…, PIN(6) corresponds to the type of minutiae involved in the three sides of fictitious triangle. The second part PIN(7), PIN(8) AND PIN(9) is a three-digit decimal integer from the error-tolerate transform to x_1, α_{min} and α_{med}.



(a) (b) (c)

Figure 4 The average values of selected parameters in the fictitious triangle; (a) The maximal side; (b) The minimal angle; (c) The medial angle.



(a) (b) (c)

Figure 5 The variation of selected parameters in the fictitious triangle; (a) The maximal sides; (b) The minimal (data 1) and medial (data 2) angles.

Each side of triangle connects two minutiae points (reference to Fig.3). Each point is either a minutiae bifurcation or ending (described with 0 or 1, respectively). Therefore, we have 2^6=64 types of minutiae combinations involved in the three sides for the first part PIN. For example, for the fingerprint image in Fig.3a, the detected five minutiae's type is C-0(bifurcation), D-0, E-1(ending), F-0 and G-0. The triangle in Fig.3b is constructed with three longest lines CE, the minutiae types are 0 and 1, GE: 0 and 1, CF: 0 and 0. Therefore, the first part PIN generated by minutiae type is 010100.

The second part PIN is extracted from decimal values of x_1, α_{min} and α_{med}, consists of a three-digit decimal integer. Each of the three decimal values needs to be quantized to a bin when used in the generation of PIN. For the purpose of obtaining an accurate decimal number as one digit of PIN from each value whenever this query finger presents, a transform which has the ability to tolerant a limited number of errors to each quantity is designed as:

$$PIN(k) = T(E_i, j) \quad k = 7, 8, 9 \tag{4}$$

where E_i is the value being processed in each impression, and i= 1, …, 8 correspond to 8 impressions, j=0, 1 is the round off information (stored on card when enrollment). j can help to tell the information of round off when quantizing an analog value to its nearest bins. The round off rule for the decimal number is:

1) 0, the value is rounded to its integer digit;

2) 1, the figure in integer digit kept unchanged if the figure in tenth digit is less than 5, and the figure in integer digit increased by 1 if the figure in tenth digit is greater than 5.

To design the noise-tolerant transforms which can convert noisy nonuniform inputs into reliable reproducible is crucial in this research. Noise-tolerant means that if the input changes but remains close, the output can be reproduced exactly [9]. In this research, the transforms are based on the distribution of average values (in Fig.4) and the deviations of each quantity (in Fig.5). For the three quantities, the maximal side, the minimal and medial angles, they can be expressed in a general form as:

$$T(E_i) = \frac{E_i - k}{m} \tag{5}$$

For a transform to E_i, the parameter m and k in (5) is mainly determined by the distribution of E_i and their deviations $\bar{E}$. Two design rules are:

1) The transform (5) is noise-tolerant to all the E_i in database;

2) $T(E_i)$ is roughly uniform distributed between 0 and 9.

For example, when designing k and m with the maximal side x_1, first, we consider the distribution of the maximal side (Fig.4a), which is between 65 and 181. Then pick up the ten groups of data with the top maximum deviations (from Fig.5a). After training, we obtain: k=19.7 and m=14. In combination with the round off information, this transform can make $T(x_1)$ noise-tolerant with all x_1 in the test database.

The details of this transform based on the fingers with ten top maximum deviations are as shown in Table I.

Those x_1 have the maximum deviations are always the biggest in the database, therefore their noise-tolerant values in Table I are always big. After obtained the noise-tolerate value, according to the second rule, a simple processing is used to assign them between 0 and 9. For this group of data, they are all greater than 3, then the following transform will help to achieve the seventh digit (the first digit of the second part) PIN:

$$\text{PIN}(3) = \text{fix}[(T(x_1, j) - 3) \times \frac{10}{7}] \tag{6}$$

TABLE I Second part PIN generated from the maximal side with fingers in DB1-a (k=19.7, m=14).

Finger no.	$x_{1\max}$	$x_{1\min}$	$T(x_{1\max})$	$T(x_{1\min})$	Round off	Noise tolerant value
43	158.4	147.2	9.91	9.11	0	9
48	159.1	148.7	9.96	9.21	0	9
33	116.3	106.0	6.90	6.16	0	6
3	162.5	153.1	10.2	9.53	1	9
42	127.1	117.9	7.67	7.01	0	7
47	155.4	146.3	9.69	9.04	0	9
41	110.0	101.0	6.45	5.80	1	6
34	121.5	112.6	7.27	6.64	1	7
5	152.5	144.0	9.49	8.88	1	9
12	151.6	143.3	9.42	8.83	1	9

where fix[X] means round the elements of X to the nearest integers towards zero.

Designing the noise-tolerant transforms for the minimal angle, α_{min}, and the medial angle, α_{med}, is relatively easy because their distributions and deviations are much narrower than those with the maximal side. Based on Fig.4b, Fig.5b and Fig.4c, Fig.5c, the transform for α_{min} is k=5 and m=7, for α_{med} is k=0 and m=5. The eighth digit PIN generated based on the minimal angle is:

$$\mathrm{PIN}(4) = \mathrm{fix}[T(\alpha_{\min}, j)] \tag{7}$$

and the ninth digit PIN generated for the medial angle is:

$$\mathrm{PIN}(5) = \mathrm{fix}[(T(\alpha_{med}, j)]\cdot \tag{8}$$

where j=0, 1 is the round off information.

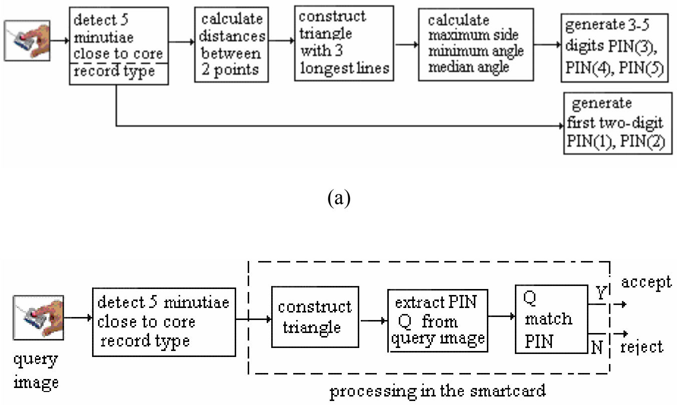
C. Performance evaluation

The performance evaluations have been performed on the randomly chosen 50 fingerprint with 400 (there are 8 impressions for each finger in the database) impressions on FVC2000 Db1_a. In the test, the first four impressions have been used to construct the template (nine-digit PIN). The types of minutiae involved in the fictitious triangle are recorded; they are used to generate the first part (six-digit binary) PIN. The transforms in (6) to (8), combined with the round off information are used to generate the second part (three-digit decimal integer) PIN. The rest four impressions of same finger are used in the verification test. In order to avoid the influences of pre-processing algorithm, the minutiae are located and extracted manually. Graph-based match can help to identify genuine minutiae pair between two impressions of the same finger in the automated fingerprint recognition.

During the enrollment process (as shown in Fig.6a), the first part PIN is generated by using the minutiae type associated with the three sides of fictitious triangle. The second part PIN is generated based on the transform and round off information for the maximal side x_1, minimal angle α_{min} and medial angle α_{med}. The average values of x_1, α_{min} and α_{med} are calculated based on the first four impressions. Considering the worst scenario of fingerprint distortion which did not presence at the enrollment process, here ±5% ~ ±9% deviation are added to the average values of x_1, α_{min} and α_{med}. If the deviation is ±5%, then the second part PIN are derived as: $(1\pm5\%)\bar{E}(x_1)$, $(1\pm5\%)\bar{E}(\alpha_{min})$, $(1\pm5\%)\ \bar{E}(\alpha_{med})$.

During the verification process (as shown in Fig.6b), the fingerprint scanner will detect 5 minutiae closest to the core. The type (bifurcation or ending) of these minutiae as well as their coordinates are extracted. Then the information is transferred to the smartcard. After that, the following processing are conducted on the smartcard:

i) Calculate the distances between any two points;
ii) Pick up three lines with the longest length;
iii) Construct a triangle with these three lines;
iv) Generate a query PIN Q.
v) Compare Q with that on the template. If matched, then the card holder can gain access to the system.


detect 5 minutiae close to core
record type
calculate distances between 2 points
construct triangle with 3 longest lines
calculate maximum side minimum angle median angle
generate 3-5 digits PIN(3), PIN(4), PIN(5)
generate first two-digit PIN(1), PIN(2)
query image
detect 5 minutiae close to core record type
construct triangle
extract PIN Q from query image
Q match PIN
Y
N
accept
reject
processing in the smartcard

(a)

(b)

Figure 6 Block diagram of authentication. (a) Enrolment; (b)Verification.

The Genuine Accept Rate (GAR) is used to evaluate the verification performance. During the enrollment, the templates (PINs) are derived from the first four impressions in the database. A deviation between ±5% to ±9% is added to the average value of x_1, α_{min} and α_{med}. Then a PIN for each finger is generated. During the verification, the input is any of the last four fingerprint impressions, a PIN are generated based on the query impressions. For the left 4 impressions of 50 fingers, the GAR with three values x_1, α_{min} and α_{med} are demonstrated independently as shown in Fig.7. As shown in Fig.7, if ±7% deviation is added to the three values x_1, α_{min} and α_{med}, for the 200 test impressions, 99% of GAR can be achieved, and if ±9% deviation is added, then 100% GAR can be achieved.

It is noted that the role of the first part PIN generated by minutiae type involved in the starting and ending point of three sides of the fictitious triangle are crucial. As we know, to keep the second part PIN stable, which are extracted from noise data, the transform must have a relative large noise-tolerant range. However, with the increase of deviations in the maximal side, the minimal angle and the medial angle, PIN(7), PIN(8) and PIN(9) are not quite distinctive. For example, we have three fingers, no.7, 36 and 39, share 924 for the second part PIN, while the minutiae type involved in the three sides of their corresponding triangle are 110111, 101010 and 001010, respectively. Therefore, PIN(1) to PIN(6) are always stable and distinctive. As a result, the nine-digit PIN can distinguish the three fingers.

Our application is smartcard based, therefore, even though there is the possibility that two PINs are same in a large database, it is not fatal in the real world applications.

Remark: The proposed scheme can be used in combination with other schemes. One particular combination is to construct a PIN consisting of a token as the first authentication layer and this biometric PIN as the second authentication layer. This will effectively reduce the false acceptance rate as the intrusive attempts have to pass the first hurdle. Given a relative small percentage of breaking token or PIN/password cases, the chance of breaking both token and biometric PIN is even lower.

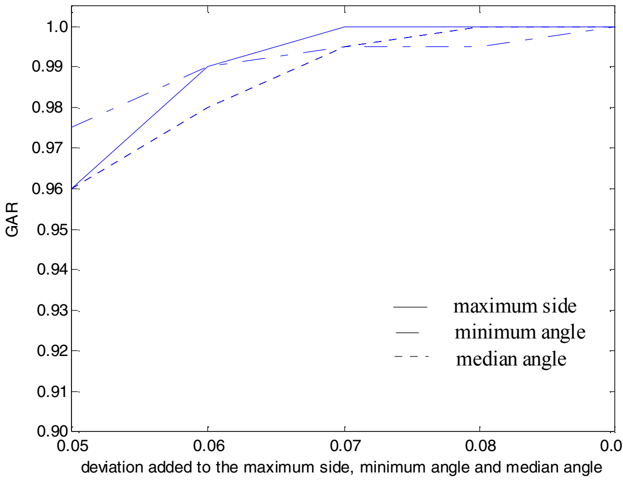


Figure 7 Evaluation of the PIN generation from fingerprint. Horizontal: deviation added to the average values of maximal side, minimal angle and medial angle; Vertical: Genuine Accept Rate.

IV. Conclusion

In this paper, the generation of PINs from fingerprint images has been studied. The foundation of this research is that the minutiae closest to the core of a fingerprint image is stable. Five minutiae closest to the core are detected. A fictitious triangle which is composed of three longest lines connecting two minutiae points is constructed. The type of minutiae involved in the starting and ending points of three sides of triangle are assigned to the first part (six-digit binary) PIN. The length of maximal side, the minimal and the medial angles of this triangle are converted to the second part (three-digit decimal integer) PIN with a noise-tolerant transform. Experiments based on the public database show that the PINs are stable.

In this proposed scheme, the information related to the PINs should be hashed when stored on the card. As templates protection is not the main topic of this research, we don't discuss much here.

This proposed scheme usually associated with the application of two-factor (smartcard and fingerprints) authentication. Storing the templates in the smartcard means that the comparison is made locally and not in a database or server, which will reduce the workload and cost of distriution of the key. The two parts nine-digit PIN extracted from fingerprint, together with the identification number of the smartcard will provide convienience to user and lead to high level of security.

References

[1] D. Gollman, Computer security, John Wiley & Sons, 1999.

[2] A. K. Jain, L. Hong and R. Bolle, "On-line fingerprint verification," *IEEE Trans. On Pattern Analysis and Machine Intelligence*, vol.19, no.4, pp.302-314, 1997.

[3] R. S. Germain, A. Califano, and S. Colville, Fingerprint matching using transformation parameter clustering, *IEEE Computational Science and Eng*., vol.4, pp.42-49, 1997.

[4] A. K. Jain, S. Pankanti, S. Prabhakar, L. Hong, and A. Ross, "Biometrics: A grand challenge," *Proc. Of international conference on pattern recognition*, vol.2, 935-942, August, 2004.

[5] B. Bhanu and X. Tan, "Fingerprint indexing based on novel features of minutiae triplets," *IEEE Trans. On Pattern Analysis and Machine Intelligence*, 25(5), pp.616-622, 2003.

[6] B. Bhanu and X. Tan, *Computational algorithms for fingerprint recognition*, Kluwer Academic Publishers, 2004.

[7] N. K. Ratha, K. Karu, S. Chen and A. K. Jain, "A real-time matching system for large fingerprint database," *IEEE Trans. On Pattern Analysis and Machine Intelligence*, 18(8), pp.799-813, 1996.

[8] P. Rerd, *Biometrics for network security*, Prentice Hall PTR.2004.

[9] Y. Dodis, L. Reyzin, and A. Smith, "Fuzzy extractors: How to generate strong keys from biometrics and other noisy data," *Adv. in Cryptology Eurocrypt* 2004, LNCS vol. 3027, Springer-Verlag, pp. 523--540, 2004.

[10] S. Giarmi and H. Magnusson, *Investigation of user acceptance for biometric verification/identification methods in mobile units*, Master thesis, Stockholm University/Royal Institute of Technology, Sweden. 2002.

[11] Human services card. http://www.privacy.org.au/Campaigns/ID_cards /HSCard.html