International Journal of Advanced Smart Convergence Vol.6 No.2 65-71 (2017)
https://doi.org/10.7236/IJASC.2017.6.2.65

IJASC 17-2-8

A Study on Strong Minutiae Extraction for Secure and Rapid Fingerprint Authentication

Jin-Ho Han

Dept. Of Liberal Studies, Korean Bible University, Seoul, Korea
hjinob@bible.ac.kr

Abstract

Fingerprints are increasingly used for user authentication in small devices such as mobile phones. Therefore, it is important for Fingerprint authentication systems in personal devices to protect the user's fingerprint information while performing efficiently with a lightweight matching algorithm. In this paper, we propose a new method to extract strong minutiae with unique numbers from fingerprint images. Strong minutiae are at all times obtained from fingerprint images, and can be useful for secure and rapid fingerprint authentication. The binary information of strong minutiae of a fingerprint can be transformed securely and can create cancelable fingerprint templates. Also the bit-strings of strong minutiae decrease computing time necessary for the matching procedure between two fingerprints due to the simplicity of bitwise operations. First, we enroll several fingerprints images of a finger. From these images we select a reference fingerprint and put a number on each minutia. Following this procedure, we search for mated-minutiae between the reference fingerprint and other fingerprints one by one. Finally we derive unique numbers of strong minutiae of the finger. In the experiment with the FVC2004 fingerprint database, we show that using the proposed method, strong minutiae can be extracted successfully.

Keywords: *cancelable fingerprint templates, strong minutiae, bit-strings, rapid authentication.*

1. Introduction

There has been a recent increase in research on secure fingerprint authentication [1-3]. In a fingerprint authentication system, a user's fingerprint data are stored in fingerprint templates which will be used for verifying a match between two fingerprints. These fingerprint templates should be protected for the user's privacy. Fuzzy vault [4] can be used as a method for protecting fingerprint templates [5]. Generally, template protection techniques [6] have the following three properties:

i. Non-reversibility: it should be computationally infeasible to recover the original fingerprint data from the protected fingerprint template.

Manuscript Received: Apr. 14, 2017 / Revised: Apr. 21, 2017 / Accepted: May 1, 2017
Corresponding Author: hjinob@bible.ac.kr
Tel: +82-2-950-4301, Fax: +82-2-950-4301
Dept. of Liberal Studies, Korean Bible University, Seoul, Korea

ii. Accuracy: the accuracy of fingerprint recognition should be preserved after transformation

iii. Diversity: a fingerprint template cannot be matched from different applications.

Fingerprint templates are most commonly represented by minutiae information. The binary information of minutiae derived from a fingerprint image can be transformed easily and used for making secure fingerprint templates. Fingerprint information cannot be guessed from the transformed binary data, thereby guaranteeing the safety of the original fingerprint.

Strong features refer to high-quality features which can be distinguished easily from other features in biometric raw images. By carefully selecting strong features that are easier for a specific user to replicate, Randomized Biometric Templates (RBTs)[7] have also been proposed, creating a difficult environment for attackers to make guesses. Strong minutiae are specific minutiae which can always be obtained from fingerprint images.

When strong minutiae of a fingerprint are retrieved, the usages of these strong minutiae are as follows.

1) Strong minutiae of a fingerprint can be used as the biometric identification of the owner, because strong minutiae are always obtained from a user's fingerprint and can be distinguished from those of others.

2) The bit-strings of strong minutiae of a fingerprint can be transformed to be used as secure cancelable fingerprint template, which can be cancelled and replaced when compromised.

3) The bit-strings of strong minutiae decrease computing time for the matching between two fingerprints due to the simplicity of bitwise operations in the fingerprint authentication system.

The rest of this paper is organized as follows: section 2 contains a discussion of previous work related to secure fingerprint templates and the construction of bit-strings from minutiae as fingerprint templates. Section 3 describes the proposed method of selecting strong minutiae from fingerprint images. In section 4, through the experiment with the FVC2004 fingerprint database, we demonstrate how strong minutiae can be extracted by using the proposed method. Finally, conclusions are discussed in section 5.

2. Related Work

Many studies had been conducted to construct secure cancelable fingerprint templates. Ratha et al.[8,9] studied Cartesian, polar and functional transformation of minutiae features and proposed a one-way transformation. Ang et al.[10] previously proposed a key-based transformation method for cancelable fingerprint templates. The key was an angle of a line through a core point of an input fingerprint image. Lee et al.[11] generated a cancelable fingerprint template using translation and rotation invariant values around each minutia. Two changing functions were used to transform each minutia.

More recently, researchers have tried to construct bit-strings from minutiae as fingerprint templates, because bit-strings are easily transformed and are used to simplify a minutiae-based fingerprint matching algorithms.

Using minutiae location and direction information, Cappelli et al.[12] proposed a bit-oriented MCC(Minutia Cylinder-Code) method for minutiae matching. Lee et al.[13] described the process of generating bit-strings as fingerprint templates from the 3D array based on the (x,y)position and direction of the reference minutia. Here, it is explained that cancelable bit-strings are generated by changing the reference minutia into another minutia in turn. Wong et al.[14,15] introduced MLC(Multi-Line Code) which is a bit-string-based minutia descriptor used for cancellable fingerprint templates. Unfortunately, their proposed methods to extract bit-strings were not suitable for making fixed-length bit-strings. Fixed-length bit-strings enable rapid matching and bio-crypto-key generation.

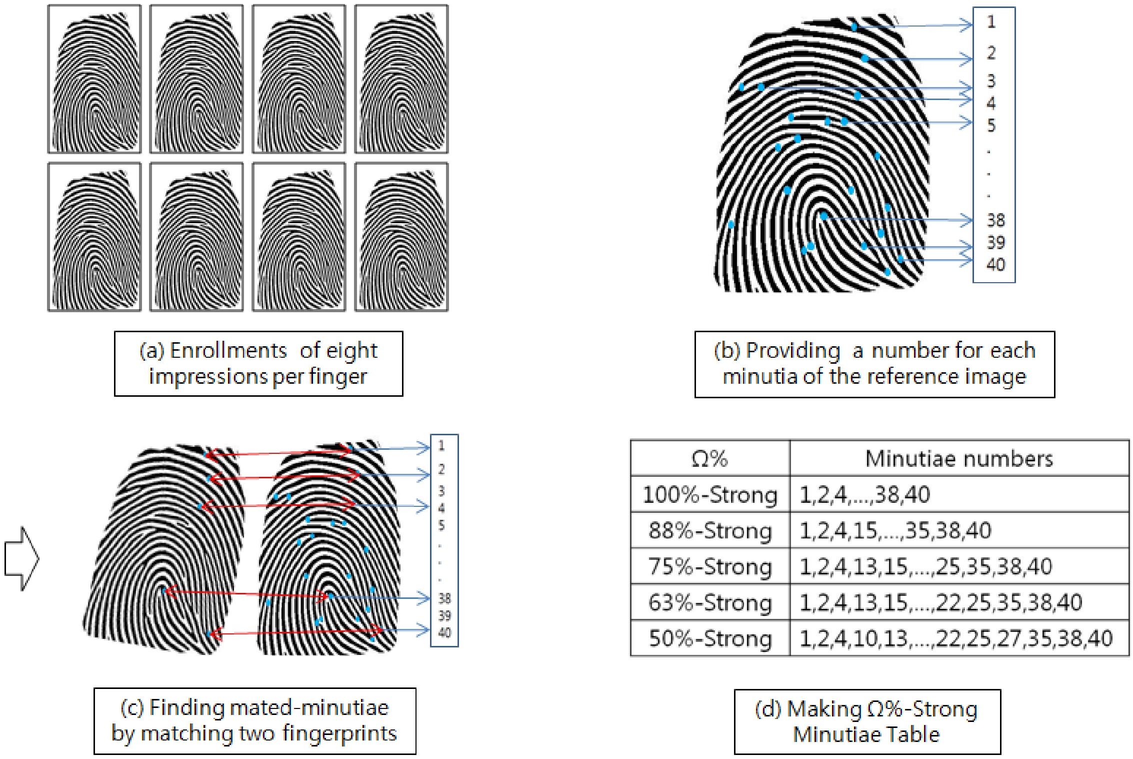
Afterwards Wong et al.[16] introduced a new method to extract fixed-length bit-strings from minutiae. They extracted variable-size bit-strings through MLC and changed these to fixed-length bit-strings using kernel principal components analysis (KPCA) and binarization techniques. Also, Jin et al.[17] proposed a generic framework to generate fixed-length bit-strings from fingerprint minutiae. The framework consists of four steps: 1) minutiae descriptor extraction, 2) kernel transformation for fixed-length vector generation, 3) binarization, and 4) matching.

In our proposed method, we adopt the mated-minutiae technique which pairs two minutiae with their information regarding (x,y)position and the direction angle to determine strong minutiae and put numbers on them. The main contributions of this paper are as follows.

1) We propose a method to extract strong minutiae, that is, to determine which numbers are those of strong minutiae.

2) We propose a method to identify each minutia with its unique number, by providing a number for each minutia of the reference fingerprint and keeping a record of this number.

3) We show particular circumstances where strong minutiae can be used as a biometric identification of a user.



(a) Enrollments of eight impressions per finger

(b) Providing a number for each minutia of the reference image

Ω%	Minutiae numbers
100%-Strong	1,2,4,...,38,40
88%-Strong	1,2,4,15,...,35,38,40
75%-Strong	1,2,4,13,15,...,25,35,38,40
63%-Strong	1,2,4,13,15,...,22,25,35,38,40
50%-Strong	1,2,4,10,13,...,22,25,27,35,38,40

(c) Finding mated-minutiae by matching two fingerprints

(d) Making Ω%-Strong Minutiae Table

Figure 1. Overall process of extracting strong minutiae

3. Proposed Method

The overall process of our proposed method for extracting strong minutiae from a fingerprint is shown in Figure 1. Our proposed method has four steps: 1) Fingerprint enrollment, 2) Providing a number for each minutia, 3) Finding mated-minutiae, and 4) Making a strong minutiae table.

3.1 Fingerprint enrollment Figures

Several impressions need to be enrolled per finger. All impressions have differences in terms of finger placement: different vertical position, high and low pressure against the sensor surface, varying degrees of skin distortion, rotation, moisture, which are all introduced in the FVC2004 fingerprint Database. Figure 1(a) shows fingerprint enrollments of eight impressions per finger.

3.2 Providing a number for each minutia

Among the enrolled impressions, we select a reference fingerprint which has the highest quality image and shows its minutiae well. We provide a number for each minutia of the reference fingerprint starting from one to the number representing the quantity of its minutiae. Now each minutia has its unique number. Figure 1(b) shows each minutia with unique numbers from one to forty.

Table 1. Selecting Strong Minutiae

```
INPUT: Reference fingerprint image $M_R$, Fingerprint images ($M_1,\ldots,M_n$),
       Number of images n, Threshold t, $k_i$=0 (i=1,…,N),
       N is the quantity of minutiae of $M_R$
OUTPUT: F number set of strong minutiae
for j = 1 to n do
{
    for i = 1 to N do
    {
        if compare($M_R$ and $M_j$)
        // whether $M_R$ and $M_j$ have i minutia concurrently or not
            then $k_i$++
        end if
    }
}
for i = 1 to N do
{
    if $k_i \geq t$
        F ← i   // number of strong minutia
    end if
}
return F
```

3.3 Finding mated-minutiae

In order to select a strong minutia of a fingerprint, we compared one of the enrolled impressions with the reference fingerprint one by one. With each comparison, we try to find mated-minutiae between them and add one point to the score of the minutia number of the reference fingerprint. Algorithm 1 shows how to select strong minutiae. If we have eight impressions per finger, we compared them seven times and all minutiae of the reference fingerprint have scores from one through eight. Figure 1(c) shows how to find mated-minutiae and determine each number of minutiae.

3.4 Making a strong minutiae table

After mated-minutiae in all impressions are identified, each minutia of the reference fingerprint has its score. With the scores of minutiae we make Ω%-strong minutiae table. Figure 1(d) shows an example of

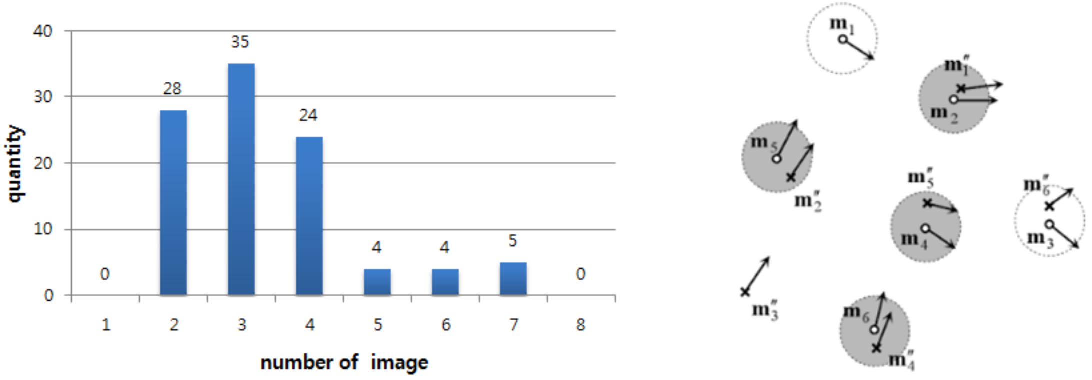
Ω%-strong minutiae table based on eight impressions of a finger. 100%-strong minutiae have eight point score and 88%-strong minutiae seven point score, 75%-strong minutiae six, 63%-strong minutiae five, and 50%-strong minutiae four.

Finally, we extract strong minutiae with varying levels of Ω%-strong.

3.5 Using strong minutiae as user's biometric identification

We consider an assumption that a user has enough time to make multiple trials for authenticating his own fingerprint and his original fingerprint image is stored in the authentication system. In this case, we may expect the input fingerprint samples are of high quality with good images and that their minutiae are extracted in abundance from the images. In the verification phase, it is determined whether the input fingerprint has some specific minutiae or not. If the specific minutiae are the strong minutiae of the original fingerprint image previously stored in the system, the strong minutiae can be used as the user's biometric identification for the purpose of authentication.

In terms of application an authentication system like this can be adopted in the fields of government administration, large companies, and hospitals.



(a) Quantity of each reference number in FVC2004DB1

(b) An example of finding mated-minutiae

Figure 2. Selecting reference fingerprint images and finding mated-minutiae

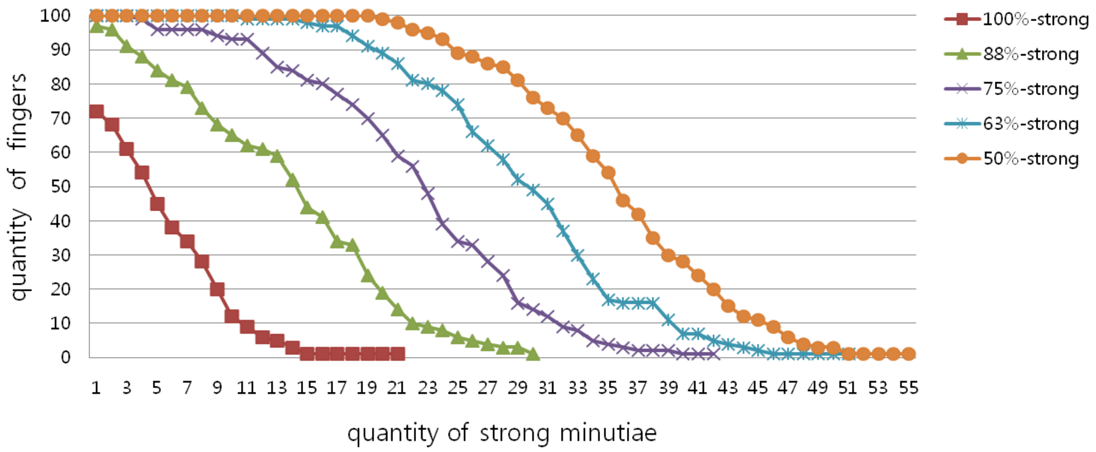


Figure 3. Quantity of strong minutiae in FVC2004 DB1

4. Experimental Results and Discussion

We used FVC2004 DB1 fingerprints which consisted of 100 fingers. Among 8 fingerprint images per finger, we selected a reference fingerprint image which was in good condition. Figure 2(a) shows the total of each number of reference images selected in FVC2004 DB1. Fingerprints numbered from 2 to 4 were selected 87 times from 100 fingers. Accordingly, images of number 2, 3 and 4 had higher quality than others.

Figure 2(b) shows an example of finding mated-minutiae [6]. The four gray circles denote successfully mated minutiae. When we determined whether two minutiae were mated or not, we used three elements which are x, y coordinates and the direction angle of the minutia. Using mate-minutiae technique between each image and the reference image we implemented Algorithm 1 to determine which numbers of minutiae of the reference image were strong.

Table 2. Quantity of strong minutiae in FVC2004 DB1

%-strong	quantity of impressions	maximum quantity	average quantity	quantity of fingers
100%-strong	8	21	4.6	72
88%-strong	7	30	13.1	97
75%-strong	6	42	21.7	100
63%-strong	5	51	28.9	100
50%-strong	4	55	35.0	100

After implementing Algorithm 1, we got each number of strong minutiae of the finger. For this experiment, we determine 100%-strong minutiae when all eight impressions have the same minutiae, 88%-strong minutiae when seven impressions have the same minutiae, 75%-strong minutiae with six impressions, 63%-strong minutiae with five, and 50%-strong minutiae with four.

Figure 3 illustrates the relationship between the quantity of fingers and the quantity of strong minutiae according to their Ω%-strong in FVC2004 DB1. Table 1 shows the maximum and average quantity of strong minutiae of all Ω%-strong. 100%-strong minutiae were found in 72 out of 100 fingers and had 4.6 strong minutiae as average quantity. 88%-strong minutiae were found in 97 out of 100 and had 13.1 strong minutiae as average quantity. 75%-strong minutiae were found in all 100 fingers and had 21.7 strong minutiae as average quantity. These results are meaningful considering that these FVC2004 DB1 fingerprints had been made for the contest of fingerprint authentication system all over the world. Therefore, through this experience we demonstrated how strong minutiae can be extracted using our proposed method.

5. Conclusion

In this paper we proposed a new method to extract strong minutiae and showed how to provide a unique number to each minutia. Also, we introduced particular circumstances where the unique number of each minutia of a fingerprint could be used as the biometric identification of the user. As shown in our experimental results, we expect 100%-strong minutiae to be obtained with a proper process to enroll fingerprints. We believe our study on extracting strong minutiae will be helpful to construct bit-strings from a fingerprint, which will be of significant use making cancelable fingerprint templates and rapid lightweight authentication algorithm for small devices such as mobile phones. Our next research will concern the construction of fixed-length bit-strings from strong minutiae of a fingerprint.

References

[1] N. Ratha, J. Connell, R. Bolle, and S.Chikkerur, “Cancelable biometrics: A case study in fingerprints,” in *Proc. of Intl. Conf. on Pattern Recognition*, pp. 370-373, 2006.

[2] N. Ratha, S. Chikkerur, J. Connell, and R. Bolle, “Generating cancelable fingerprint templates,” *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol 29. no.4, pp. 561-172, 2007.

[3] A. Jain, K. Nandakumar, and A. Nagar,“Fingerprint Template Protection: From Theory to Practice,” *Security and Privacy in Biometrics.* Springer London, pp. 187-214, 2012.

[4] A. Juels and M. Sudan, “A fuzzy vault scheme,” in *Proc. of IEEE Intl. Symp. on Information Theory*, 2002.

[5] D. Moon, et al., “Fingerprint Template Protection using Fuzzy Vault,” *LNCS 4707*, pp. 1141-1151, 2007.

[6] D. Maltoni, D. Maio, A. K. Jain, and S. Prabhakar, *Handbook of Fingeprint Recognition*, Springer-Verlag, London, 2009.

[7] L. Ballard, S. Kamara, F. Monrose, and M. Reiter, “Towards Practical Biometric Key Generation with Randomized Biometric Templates”, *CCS’08*, October 27-31, 2008, Alexandria, Virginia, USA, 2008.

[8] N. Ratha, J. Connell, and R. Bolle, and S. Chikkerur, “Cancelable biometrics: A case study in fingerprints”, In *Intl. Conf. on Pattern Recognition*, pp. 370-373, 2006.

[9] N. Ratha, S. Chikkerur, J. Connell, and R. Bolle, “Generating cancelable fingerprint templates”, *IEEE Transactions on Pattern Analysis and Machine Intelligence*, Vol 29. No.4, pp. 561-172, 2007.

[10] Ang R, Safavi-Naini R, McAven L. “Cancelable key-based fingerprint templates”, In: *Information security and privacy:10th Australasian conference(ACISP2005)*, 2005. p.242–52.

[11] Lee C, Choi J, Toh K, Lee S, Kim J. “Alignment-free cancelable fingerprint templates based on local minutiae information.”, *IEEE Transactionson Systems, Man and Cybernetics*, Part B 2007;37(4):980–92.

[12] R. Cappelli, M. Ferrara, and D. Maltoni, “Minutia cylinder-code: A new representation and matching technique for fingerprint recognition,” *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 32, no. 12, pp. 2128–2141, Dec. 2010.

[13] C. Lee, J. Kim, "Cancelable fingerprint templates using minutiae-based bit-strings", *Journal of Network and Computer Applications*, vol. 33, pp. 236-246, 2010

[14] W. J. Wong, M.L.D., Y. H. Kho, "A low complexity multi-line code for cancelable fingerprint template", in *Proc. of 2nd International Conference on Convergence Technology 2012, Korea Convergence Society*, Qingdao. pp. 61-65, 2012.

[15] W. J. Wong, A. B. J. Teoh, M. L. D. Wong, Y. H. Kho, "Enhanced multi-line code for minutiae-based fingerprint template protection", *Pattern Recognit. Lett*. vol. 34, Issue 11, pp. 1221–1229, Aug. 2013.

[16] W. J. Wong, A. B. J. Teoh, Y. H.Kho, M. L. D. Wong, "Kernel PCA enabled bit-string representation for minutiae-based cancellable fingerprint template", *Pattern Recongnition*, vol. 51, pp.197-208, Mar. 2016.

[17] Z. Jin, M. H. Lim, A. B. J. Teoh, Bo. M. Goi, Y. H. Tay, "Generating Fixed-Length Representation From Minutiae Using Kernel Methods for Fingerprint Authentication", *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. 46, Issue 10, Oct. 2016.