Schemes of Utilizing Partial Fingerprints for User Verification

Qinghai Gao

Department of Criminal Justice & Security Systems, Farmingdale State College

2350 Broadhollow Road, Farmingdale, NY 11735

Email: GaoQJ@farmingdale.edu

Abstract: Fingerprint verification is widely used in access control. However, it is a challenging problem using partial fingerprint for such purpose. In this paper we propose methods using partial fingerprint to verify user. From minutiae-sparse partial fingerprints, we first construct a supertemplate by combining the minutiae points from these partial fingerprints. Then the subtemplates constructed through randomized selection will be matched against the supertemplate. These methods have two advantages: (1) it protects the privacy of a user's fingerprint data; (2) it increases the number of available biometrics for a user. Our preliminary experiments show promising results.

Keywords: Verification, partial fingerprint, minutiae, supertemplate, subtemplate, privacy

Introduction

Currently, a majority of fingerprint verification systems utilize minutiae points (ridge ending and ridge bifurcation) as the distinguishing characteristics. Deformation factors, such as translation, rotation, and skin wetness and elasticity, can significantly change these minutiae and result in false non-match. Verification with low quality partial fingerprints is even more challenging due to the limited number of minutiae points and their significant variations from one partial fingerprint image to another.

Psychologically, biometric applications raise privacy concerns [1-6]. In biometric systems biometric data have to be saved in a centralized database or distributed on smart cards. Potential users of biometrics are unwilling to give out their biometric data because they concern whether their biometric data will be protected sufficiently and how their biometric data will be used. The typical answer to this concern is that biometric data has to be secured with cryptographic algorithm. Another problem closely related to the privacy issue of biometrics is that human being has limited number of biometrics. Therefore, it is a desirable to generate multiple independent biometric templates from biometric image (s). The partial fingerprint based verification methods we are proposing in this paper mainly focus on achieving this goal.

The rest of the paper is organized as follows. Section 2 reviews previous work done by others on matching partial fingerprints. Section 3 briefly states our contribution. Section 4 introduces the methods of generating partial fingerprint images and the matching algorithm. In section 5 we give our preliminary testing results. Section 6 summarizes and concludes the paper.

Literature review

Generally it is easier to obtain partial fingerprints than full fingerprints. Partial fingerprint based verification has attracted the attention of many biometrics researchers. Wang [7] listed the following four scenarios that can produce partial fingerprints: latent prints in crime scene; fingerprint image from compact 2D sensor; damaged fingerprint image; disregarding the noisy region of fingerprint images. In addition, incorporative user may also purposely submit partial fingerprint to an automatic fingerprint identification system to avoid being identified.

The two major types of features being used in fingerprint matching are local features and global features. Global features, such as core and delta, are characterized by the attributes that capture the global spatial relationships of a fingerprint. Local features, such as the relative locations and orientations of minutiae points (ridge ending and bifurcation) in a local area are comparatively invariant with respect to certain global distortions such as rotation and translation.

Due to the nature of partial fingerprints, partial fingerprint matching largely depends on local features because the global singular structures (cores and deltas) may not even exist in them. Moreover, localized features have the ability to tolerate some distortions. A number of researchers have studied the problem of matching a partial fingerprint to full template fingerprints.

Jea and Govindaraju [8] proposed a minutia-based approach to matching incomplete or partial fingerprints with full fingerprint templates. They generate a five-element secondary feature vector. For each minutia and its two nearest-neighbors, they construct a 5-element vector containing the two Euclidean distances from the central minutia to its neighbors, the angle formed by the corresponding line segments, and the two orientation differences between the central minutia and each neighbor. This approach can tolerate certain amount of global distortion because the vectors are constructed with local features. Since this approach largely depends on the existence of adequate number of minutiae, it is unlike to perform well on partial fingerprint with very few or no minutiae.

Kryszczuk et al. [9] [10] proposed to utilize pore locations to match fingerprint fragments with the following with the assumption that the level-3 features, such as sweat pores, will compensate for the decreased level-2 features (Minutiae points).They showed that the smaller the partial fingerprint, the greater the benefits of using pores. In their proposal, fingerprints are aligned by correlating the partial fingerprint with the candidate portion on the full fingerprint.

Chen and Jain [11] developed methods for partial fingerprint recognition with the following two level-3 features: dots, which are an isolated ridge units between normal ridges, and incipients, which are thin and often fragmented ridges appearing between normal ridges. Unlike sweat pores, which naturally follow the ridge structure and appears only on ridges, dots and incipients appear in valleys. However, not all fingerprints have these two types of features.

Kisel et al. [12] proposed minutiae based fingerprint matching method. It uses translation and rotation invariant local structures consisting of central minutia point and its neighboring minutiae points. The number of neighboring minutiae points for the central minutiae point is determined by a distance-based threshold. This approach does not require any fingerprint alignment.

Choi et al. [13] proposed approach to constructing an entire fingerprint template from a number of partial fingerprint images by using recursive mosaicking. However, it is often difficult to collect adequate number of partial fingerprint to construct a reliable full fingerprint. Moreover, construction procedures often introduce spurious features.

Ryu et al. [14] proposed methods to handle missing, spurious, and altered minutiae due to fingerprint distortion. They generated fingerprint super-templates containing highly probable true minutiae points, in which the credibility and the type of each minutia are updated with Successive Bayesian Estimation as more fingerprint images become available.

In spite of all these efforts, partial fingerprint identification is still a challenging problem.

Our Contribution

In this paper, we explore new authentication scheme using partial fingerprints. This scheme has two advantages: (1) it increases the number of available biometrics for a user; (2) it protects the privacy of a user's biometric data due to the randomized minutiae selection process. And a user does not need to know which parts of his fingers are being used for a particular authentication system.

Method

In this paper we propose an approach to constructing subtemplates from minutiae-sparse multiple partial fingerprints.

Identification with partial fingerprint is still an ongoing research problem because partial fingerprints often contain small number of minutiae points. One question we ask is whether multiple partial fingerprints can make positive identification. To answer this question we propose an approach to synthesizing a template by combining multiple partial fingerprints and then constructing subtemplates from the synthesized template. One or more of the subtemplates will be stored as the enrollment template(s). During verification a user's newly generated full fingerprint template will be matched against the enrolled subtemplate.

Currently, many fingerprint identification systems require it users to provide all his fingerprints upon enrollment. That is to say, a user needs to provide 10 rolled fingerprints. Some users may be reluctant to do that. Here we propose a fingerprint verification system that only requires a user to register a few randomly selected partial fingerprints, based on the observation that four non-matching partial fingerprints (Top, Bottom, Left, and Right) can be easily acquired from one human finger, as illustrated in Fig. 1. Therefore, every user can potentially have 40 partial fingerprints.

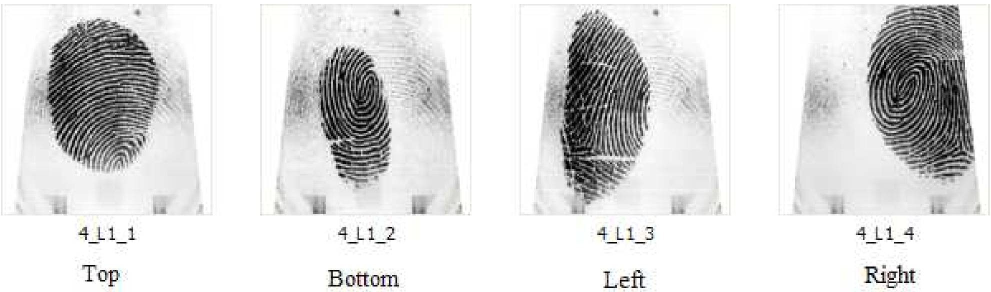

Fig. 1 Illustration of four partial images from finger 4_L1 (CASIAv5 [15])

To protect user's privacy, we recommend using the following procedure to acquire partial fingerprints: use a user-specific random number (key) to determine the number (4~8) and positions of the partial fingerprints to be taken. All ten fingers of a user will be inserted sequentially into the scanner. However, only the selected parts of the fingers will be imaged. The user does not have to know where the selected partial fingerprints are from.

Assume only four out of the 40 partial fingerprints are utilize for authentication, there will be more 91,000 different choices for each user. What are the four partial fingerprints for a particular system is determined by the secret key, known only to the system. Not only is this scheme a good solution to the biometric number limitation problem, but also it protects the privacy of biometric data.

To test our proposals we utilize NIST fingerprint software [16] to match fingerprint minutiae templates. More details can be obtained from [17]. All the matching results in this paper are obtained with this algorithm.

Results

Partial fingerprints often contain limited number of minutiae points and they rarely match with each other unless there are sufficient overlapping. Fig. 2 shows five partial fingerprints. From Fig. 2 it can be seen that Fingerprint 97_R2_2 has a counterclockwise rotation of 135 degree relative to Fingerprint 97_R2_0 and they have some overlapping with each other. Their mutual matching scores are given in Table 1.

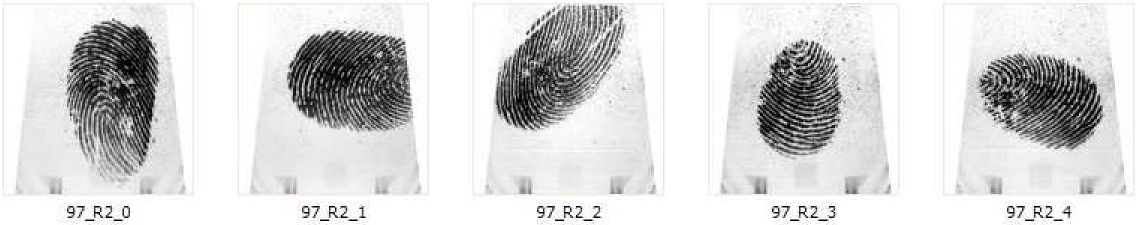

Fig. 2 Five partial fingerprints from finger 97_R2 (CASIAv5 [15])

Table 1 Matching results for the five partial fingerprints of finger 97_R2

Fingerprint#	97_R2_0	97_R2_1	97_R2_2	97_R2_3	97_R2_4
97_R2_0	358	0	45	14	9
97_R2_1	0	109	3	21	4
97_R2_2	45	3	317	9	6
97_R2_3	14	21	9	169	10
97_R2_4	9	4	6	9	190

As can be seen from Table 1, except the score between 97_R2_0 and 97_R2_2, all the other non-self matching scores are less than 40 - the threshold of NIST fingerprint software [16]. Therefore, they do not match.

To construct subtemplates from the five partial fingerprints, we combine their minutiae templates to form a synthetic supertemplate containing 171 minutiae points, and then randomly select various numbers of minutiae points from the supertemplate. Matching is carried out between the subtemplates and the supertemplate. The experiments are repeated 40 times. The results are given in Table 2.

As can be seen from Table 2, on average a user can be authenticated with a fingerprint containing as low as 25 minutiae (Average score: 44.110). However, we believe that a fingerprint should have more than 25 minutiae points to reduce the possibility of being falsely rejected.

Assume we decide to use subtemplate containing 40 minutiae points for user verification. With the supertemplate containing 171 minutiae, we can construct four mutual exclusive subtemplates. Since the five partial fingerprints are obtained from one finger.

Table 2 Average matching scores between subtemplates and the supertemplate

#Minutiae	Average score	Standard deviation
15	15.09	5.66
20	28.19	7.82
25	*44.11*	13.07
30	62.43	15.09
35	89.33	22.52
40	119.21	25.61
45	146.33	28.2
50	182.9	29.18
55	216.9	30.79
60	256.3	32.96
65	307.3	41.72
70	357.45	41.81

We obtained the curve in Fig. 3 by plotting the average scores against the numbers of minutiae points given in Table 2. The equation indicates that the match scores exponentially increase with the number of minutiae points in subtemplates.

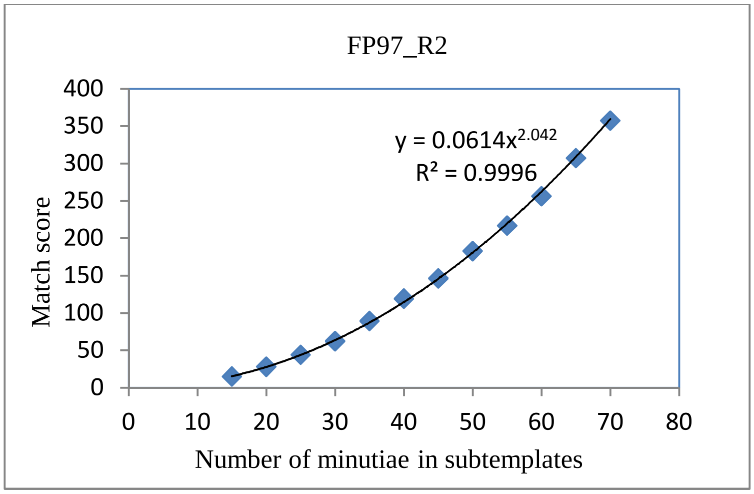

Fig. 3 Effects of number of minutiae on average match score for FP97_R2

To check the validity of the equation in Fig. 3, we calculate the number of minutiae based on the matching score between the original partial fingerprints and the supertemplate. The results are given in Table 3. From Table 3 we can see that the average error rate is about 5%. Therefore, the equation in Fig. 3 closely represents the relationship between matching score and the number of minutiae points in a subtemplate.

Table 3 Calculated numbers of minutiae points for the 5 partial fingerprints

Fingerprint	Match score	Real #Minutiae (RM)	Calculated #minutiae (CM)	|RM-CM|	Error (%)
97_R_0	152	45	45.9	0.9	0.02
97_R_1	64	26	30.1	4.1	0.16
97_R_2	111	36	39.4	3.4	0.09
97_R_3	67	30	30.74	0.74	0.02
97_R_4	84	34	34.3	0	0.00
97_R2*	2097	171	166	4	0.02

*97_R2 contains all the minutiae from the other five partial fingerprints

Another question to ask is whether the subtemplates constructed by random selection could increase False Acceptance Rate (FAR). To answer the question we match the supertemplate 97_R2 against the CASIA DBv5. The results are plotted in Fig. 4.

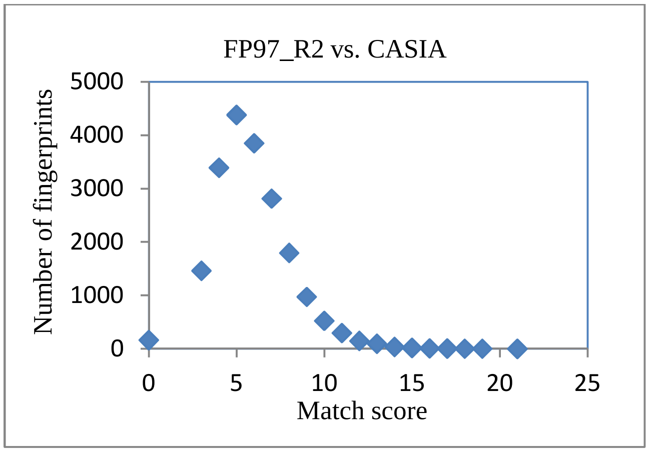

Fig. 4 Results of matching FP97_R2 against CASIA DBv5

From Fig. 4 we can see that all of the match scores are less than 25. Given the threshold value 40, there is no match between the supertemplate and the templates in the database. Given the fact that a subtemplate will not have a higher matching score than its supertemplate, we can conclude that using subtemplates does not increase FAR.

Conclusion

In this paper we proposed schemes for user verification using partial fingerprint minutiae subtemplates. We first construct a supertemplate by combining the minutiae points from multiple partial fingerprints. Then the subtemplates constructed through subset selection from the supertemplate will be matched against the supertemplate. Our experimental results showed that on average a subtemplate with 25 or more minutiae points is sufficient for user verification without increasing FAR. Multiple mutual exclusive subtemplates can be generated from the supertemplate constructed from multiple partial fingerprints from one finger – a solution to the number limitation problem of biometrics.

Not only do the proposed subtemplate matching schemes increase the number of available fingerprints for a user. More importantly, they offer a new solution to protect the privacy of a user's fingerprint data with randomized selection of minutiae subsets and secret key based partial fingerprint selection.

Acknowledgement

Portions of the research in this paper use the CASIA-FingerprintV5 collected by the Chinese Academy of Sciences' Institute of Automation (CASIA).

References

[1] M. Wadman (1999). Biometrics group counters privacy fears. *Nature*, 398(6727): 451.
[2] B. Schneier (1999). Inside risks: The use and abuse of biometrics. *Communications of the ACM*, 42:136.
[3] J. Grijpink (2005). Two barriers to realizing the benefits of biometrics: a chain perspective on biometrics and identity fraud as biometrics' real challenge. *Computer Law & Security Report*, 21(2): 138-145.
[4] M. Bronstein & A. Bronstrein (2002). Biometrics was no match for hair-raising tricks. *Nature*, 420(6917): 739.
[5] I. Buhan & P. Hartel (2005). The state of the art in abuse of biometrics (Internal Report).
[6] W. Abernathy & L. Tien. Biometrics: who's watching you. *Electronic Frontier Foundation.* Available at: http://www.eff.org/Privacy/Surveillance/biometrics/
[7] Y. Wang & J. Hu (2011). Global ridge orientation modeling for partial fingerprint identification. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 11(1): 72-87.
[8] T. Jea & V. Govindaraju (2005). A minutia-based partial fingerprint recognition system. *Pattern Recognition*, 38(10): 1672-1684.
[9] K. Kryszczuk, A. Drygajlo, & P. Morier (2004). Extraction of level 2 and level 3 features for fragmentary fingerprints. *Proceedings of the Second COST Action 275 Workshop*, pp. 83–88.
[10] K. Kryszczuk, P. Morier, & A. Drygajlo (2004). Study of the distinctiveness of level 2 and level 3 features in fragmentary fingerprint comparison. *BioAW2004, Lecture Notes in Computer Science*, 3087: 124-1033.
[11] Y. Chen & A. Jain (2007). Dots and incipients: extended features for partial fingerprint matching, *Proc. Biometric Symposium, Biometric Consortium Conference*, Baltimore.
[12] A. Kisel, A. Kochetkov, & J. Kranauskas (2008). Fingerprint minutiae matching without global alignment using local structures. *Informatica*, 105(1): 31-44.
[13] K. Choi, H. Choi, S. Lee, & J. Kim (2007). Fingerprint image mosaicking by recursive ridge mapping. *IEEE Transactions on Systems, Man, and Cybernetics-Part B*, 37(5): 1191-1203.
[14] W. Ryu, Y. Han, & H. Kim (2005). Super-template generation using successive bayesian estimation for fingerprint enrollment. *Audio- and Video-based Biometric Person Authentication*, 3546: 261-277.
[15] CASIA-Fingerprint V5. Download from: http://biometrics.idealtest.org/
[16] Available at: http://fingerprint.nist.gov/
[17] C. Wilson, C. Watson, M. Garris, & A. Hicklin (2003). Studies of fingerprint matching using the NIST verification test bed (VTB). Available at: ftp://sequoyah.nist.gov/pub/nist_internal_reports/ir_7020.pdf