Alignment-Free Fuzzy Vault Scheme for Fingerprints

Gurgen Khachatryan
American University of Armenia
Yerevan, Armenia
gurgenkh@aua.am

Aram Jivanyan
American University of Armenia
Yerevan, Armenia
ajivanyan@aua.am

Hovik Khasikyan
American University of Armenia
Yerevan, Armenia
hkhasikyan@aua.am

ABSTRACT

In this paper we develop a new construction of alignment-free fuzzy vault cryptosystem for fingerprints. The fuzzy vault scheme aims to secure user's critical data (secret encryption key) with the fingerprint data in a way that only the legitimate user is able to access the key by providing his fingerprint. The existing fuzzy vault constructions usually need a pre-alignment of registered fingerprint. Recently one approach for alignment-free fuzzy vault scheme has been introduced which requires a fingerprint core detection. However, the main drawback of the method is that not all fingerprints have a core point. We expose a novel construction which is based on local texture feature detections near the minutiae points. In this paper a general construction of the new scheme is described and one specific implementation is investigated.

Keywords

Fuzzy Vault, biometric cryptosystem, fingerprint alignment.

1. INTRODUCTION

Fuzzy vault scheme [1] is one of the most famous techniques to construct biometric cryptosystems, which aims to encode the user's secret key with human biometric data and ensure noise-tolerant decoding. In general fuzzy vault setting Alice places his secret K in a vault and locks it using unordered set A. Unordered set means that the relative positions of set element do not change the characteristics of the set. The vault can be unlocked with another set B which overlaps with A to a great extent. The procedure for constructing fuzzy vault is as follows: First Alice selects a polynomial P of variable x that encodes her secret K, more clearly the coefficients of P are fixed according to the secret. She then computes the polynomial projections P(A) for the elements of A. In the next step some randomly generated chaff points are added to the vault that does not lie on the polynomial P. The final set R is composed of the P (A) and chaff points. Using error-correcting coding (e.g. Reed-Solomon codes) it is assumed that the vault can be opened with another set B, which differs from A but has enough common elements. The security of this scheme is based on the infeasibility of the polynomial reconstruction problem. Fuzzy vault scheme is implemented for human biometric, where fuzziness can come from the variability of biometric data.

2. FUZZY VAULT SCHEME FOR FINGERPRINTS

Now we describe the fuzzy vault scheme with more details by providing the construction of fuzzy vault for fingerprints exposed in [2]. The implementation operates on the fingerprint minutia features. In general each minutia is represented as a (x,y,θ) triplet, denoting its row coordinate, column coordinate and angle of the associated ridge as is shown in the Figure 1.

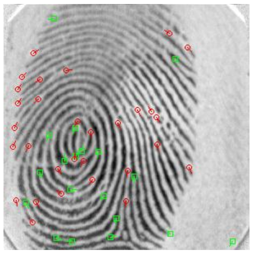

Figure 1.

The x and y coordinates of the minutia are used for locking and unlocking the vault. The template and query fingerprints are aligned at first step for compensating the translation and rotation errors. Then 16-bit CRC code for the secret key K is generated. Assuming that K is 128 bit-length, 144-bit length data S is composed of the K and 16-bit CRC code. S is represented as a polynomial

$$(u) = s_8 u^8 + s_7 u^7 + \cdots + s_1 u^1 + s_0$$

with 9 coefficients in GF(2^16). Simply S is divided into non-overlapping 16-bit segments and each segment is declared as a specific coefficient. From now all the operations take place in the GF(2^16). The x and y coordinates (8 bits each) of each minutia are concatenated as [x |y] to compose the locking/unlocking data unit u. Assuming that N minutiae are used , we get the locking / unlocking template feature set as follows.

$$U = \{u_1, u_2, \dots, u_N\}$$

Then two sets composed of point pairs need to be generated. The first set G called genuine set is composed by evaluating the polynomial P on the template minutia features set U:

$$G = \{[u_1, P(u_1)], [u_2, P(u_2)], .., [u_N, P(u_N)]\}$$

The second set C called the chaff set is composed in the following way. At first M elements c_1, c_2, ... , c_M are randomly chosen from the field GF (2^16) and then another M elements d_1, d_2, ... , d_M are chosen with the constraint that the pairs (c_i, d_i) do not fall onto the polynomial P(u). Chaff set C is

$$C = \{[c_1, d_1], [c_2, d_2], \dots, [c_M, d_M]\}.$$

Union of the two set G and C is randomized to compose the fuzzy vault of secret S. Thus, we obtain the following fuzzy vault

$$FV = \{[v_1, w_1], [v_2, w_2], \dots, [v_{M+N}, w_{M+N}]\}$$

This scheme of Uludag and Jain is one of the most famous fingerprint based fuzzy vaults scheme which motivated to more research work on this direction. There has been found also serious drawbacks of this system [12]. The main disadvantages of this scheme are the fact that the accuracy of alignment in encrypted domain cannot be ensured and the information leakage may be caused because of the alignment. An alignment-free fuzzy vault scheme was proposed in [13] where the authors proposed to use polar coordinates of minutia points with respect to the fingerprint core point. However, the fingerprint core point detection is a challenging task itself. Except this fact, the next serious drawback of such an approach is the fact that not all fingerprints have core points.

3. ALIGNMENT-FREE FUZZY VAULT FOR FINGEPRINTS

The locking/unlocking approach used in the scheme described above can be treated as a point pattern matching method. However, the fingerprint can also be viewed as a system of oriented texture. The oriented texture descriptors provide a good representation for visual content in the image. Jain et. al. [3] describes a global texture descriptor scheme called "finger code" that utilizes both global and local ridge descriptions. Chickur et al [5] presents a novel fingerprint representation method, which uses localized texture features. Unlike the described scheme, where point matching is used, we use local texture matching approach in order to obtain position and rotation invariance. Alignment-free fuzzy vault scheme.

3.1. General Method

The fuzzy vault scheme we want to introduce is similar to the scheme described above except the locking/ unlocking units specification.

In our method the biometric information is based on the specific local texture features around minutia points. The fingerprint to be enrolled is preprocessed using an enhancement scheme [4] to make the features robust to variable conditions under acquisitions. Then minutiae extraction is performed to identify the location and orientation of all the points of interest within the fingerprint. We then extract a 32x32 square neighborhood S, left above corner coincides with the minutia and the above side is going on the minutia's associated ridge orientation. Note that during each enrollment the fingerprint can have different orientations, but each minutia's associated ridge's orientation relative to the fingerprint remains unchanged, which ensures that the extracted 32x32 features will be the same at different enrollments. Of course, some noise still will be added to the textures. The noise is minimized during the enhancement phase. Then a special function LTD (Local Texture Descriptor) is computed on each texture. The LTD function takes as an input the 32x32 texture which can be treated as a binary matrix, and computes on the input data a 16 bit texture code. The computed code can be figured already as a vault locking/ unlocking unit. In [5] Chikkerur et. al gave a fingerprint representation using localized texture features, where they used Gabor functions to represent the texture images. They represented 32x32 regions around the fingerprint image using basis Gabor functions that span two scales and four orientations resulting in 272 expansion coefficients. The image can, therefore, be approximately represented as

$$I(x, y) = \sum_{n=1}^{136} a_n\, G_n(x, y)$$

The identification process is held with Gabor coefficients. However, there is no security estimation for the proposed scheme. Although fingerprint representation using Gabor coefficients is under our construction, here we provide another simple approach for texture code evaluation.

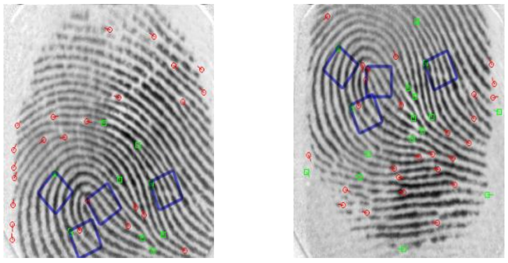
a. b.

Figure 2.

3.2. Implementation

Experiments have been conducted on the FVC2002 DB1 and DB2 databases. Both databases are obtained from 110 fingers with 8 impressions each. The experiments have shown the following results. Our texture code generation is based on the method described in [6] where simple scheme is described for constructing fault-tolerant passwords from biometric data. The password generation function LTD is an injective function

$$\mathrm{LTD} \quad : \; \{0,1\}^{32\,\mathrm{x}\,32} \rightarrow \{0,1\}^{16}$$

which can be treated as a concatenation of smaller texture descriptors functions

$$\mathrm{LTD} = \mathrm{LTD}_1 || \mathrm{LTD}_2 || \ldots || \mathrm{LTD}_{16}$$

$$\mathrm{LTD}_i \quad : \; \{0,1\}^{n\,\mathrm{x}\,m} \rightarrow \{0,1\}$$

The 32x32 region is divided into 16 small subregions of size n x m. Note that [n, m] pair can take values from the set {[8,8], [4,16],[16,4]}. Then the mean of Hamming weight of sub regions R_i is computed for over all database.The derived mean value M for 8 x 8 sub regions R_i is 27. The LTD_i function works as follows.

$$\mathrm{LTD}_i = \begin{cases} \mathrm{HW}(R_i) > M \; : \; 1 \\ \mathrm{HW}(R_i) \leq M \; : \; 0 \end{cases}$$

Different authentication methods and approaches can be used for vault unlocking. Let’s assume that the fuzzy vault F is stored in the database which hides the necessary secret key. The query fingerprint is scanned and all minutia’s descriptor codes are obtained by the method described above. For authentication we must search the obtained codes in the fuzzy vault F. Taking into account the possible noise effects, some noise-tolerant method should be considered in order to minimize the authentication errors.

Figure 3.

One naïve approach for LTD code derivation is to use the hamming distance comparator method, where some threshold is allowed. If the distance of query fingerprint minutia’s code differs from one of vault’s codes less than the given threshold, then match is registered. And the matched vault code is considered as a candidate code for lock decoding. For estimating the performance of the proposed system, a publicly available fingerprint database FVC2002-DB2 is used. This database stores fingerprints of 100 different fingers and for each finger 8 different enrollments are registered.

The following experiments have been carried out to calculate the FRR of the proposed fuzzy vault scheme. A fuzzy vault is constructed for each fingerprint by using its first registration image. Each fuzzy vault contains in average 15 genuine codes obtained from the minutiae related textures. Yet another two hundred chaff points are added to vault to make it secure. Then for each fingerprint’s vault 7 authentication attempts are performed by using the available registrations of the given fingerprint. We use the method of calculating the Hamming distance between query fingerprint’s minutia’s codes and the fuzzy vault units.

HD	FRR		FRR	HD
1	100%		76%	5
2	95%		65%	6
3	88%		59%	7
4	82%		54%	8

Table 1: FRR

A specific Hamming distance threshold is specified which determines the coincidence procedure. Two different codes are considered equivalent if their hamming distance does not exceed the given threshold. By changing the threshold value of the hamming distance, different FRR values are obtained. Of course, the FRR decreases as the threshold increases. Some results are shown in Table 1.

To calculate the FAR of the proposed system a fuzzy vault is constructed for each fingerprint of existing 100 users by using the first registrations of each fingerprint. Then for each constructed vault an authentication attempt is made by trying all 8 registration images of the remained 99 fingerprints. The authentication method is the one used for calculating the FRR of the system. Varying the hamming threshold different values are obtained for FAR. Several results are shown in Table 2 where N stands for the count of necessary vault unlocking units.

HD	FAR		FAR	HD
1	0		0.009%	5
2	0		0.01%	6
3	0		0.05%	7
4	˜0%		0.1%	8

Table 2: FAR

The biometric variability exposed at different registrations of the same fingerprint can have rotational or distortion characteristics. A random noise also may be added to the biometrics, but as usual some rotations of image appears during different enrollments. The texture descriptor codes obtained by the method described above have a positional character which means that simple rotations of the image can result in a new code whose hamming distance greatly varies from the original one. The resulted codes would have long common substrings starting at different positions. Another common case of noisy enrollment is the case when some part of the captured image has pure quality while the rest part of the captured image is of high quality. This also means that the resulted codes would have long enough common substrings. The motivation of using another authentication method is arising from these considerations. The method of using the longest common substring finding algorithm can be considered except the hamming distance comparison. Yet another advanced method will be the algorithm of finding the longest common fuzzy substring where it will be allowed the common substring to differ in some positions. This is left for further research.

4. CONCLUSION

In this paper we have introduced a novel construction of alignment-free fuzzy vault scheme which does not require high cost operations of fingerprint alignments. We have exposed one simple password generation method from the localized texture features. However, more accurate methods must be investigated which are able to output effectively discriminative, informative and at the same time privacy-protective short binary representation of the fingerprint textures. The passcode generation method greatly affects the system performance parameters. The investigation of security aspects of the proposed scheme is another subject of further research work.

5. ACKNOWLEDGEMENT

This research has been carried out within the project "Application of Security to Biometrics and Communications" sponsored by the Volkswagen Foundation.

REFERENCES

[1] A. Stoianov, T. Kevenaar, and M. van der Veen, "Security issues of biometric encryption," in Proc. of the Toronto Int. Conf. Science and Technology for Humanity (TIC-STH), 2009, pp. 34–39.

[2] U. Uludag and A.K. Jain, "Fuzzy Fingerprint Vault", Proc. Workshop: Biometrics: Challenges Arising from Theory to Practice, pp. 13-16, 2004.

[3] A. Jain, S. Prabhakar, L. Hong, and S. Pankanti. Filterbank-based fingerprint matching. In Transactions on Image Processing, volume 9, pages 846–859, May 2000.

[4] S. Chikkerur, C. Wu, and V. Govindaraju. A systematic approach for feature extraction in fingerprint images. In International Conference on Biometric Authentication, 2004.

[5] S. Chikkerur, S. Pankanti, A. Jea, N. Ratha, R. Bolle. "Fingerprint Representation Using Localized Texture Features. "

[6] V. Balakirsky, A.J. Han Vinck "A Simple Scheme for Constructing Fault–Tolerant Passwords from Biometric Data"

[7] A. Juels and M. Wattenberg, "A Fuzzy Commitment Scheme", In G. Tsudik, Ed., Sixth ACM Conf. Computer and Comm. Security, pp. 28-36, 1999.

[8] U. Uludag, S. Pankanti, S. Prabhakar and A. K. Jain, "Biometric Cryptosystems: Issues and Challenges", Proc. IEEE, vol. 92, no. 6, pp. 948-960, 2004.

[9] K. Nandakumar, A. Nagar, A. Jain "Hardening Fingerprint Fuzzy Vault using Password"

[10] P. Tuyls and J. Goseling, "Capacity and examples of templateprotecting biometric authentication systems," in Proc. ECCV Workshop BioAW (LNCS), vol. 3087, pp. 158 – 170, 2004.

[11] R. Ang, R. Safavi-Naini, and L. McAven, "Cancelable key-based fingerprint templates," in Proc. of the Australasian Conf. on Information Security and Privacy ACISP'05 (LNCS 3574), 2005, pp. 242–252.

[12] P. Mihailescu, "The fuzzy vault for fingerprints is vulnerable to brute force attack," CoRR, vol. abs/0708.2974, 2007.

[13] P. Lia, 1, X. Yanga, 1, K. Caoa, X. Taoa, R. Wanga, J. Tian "An alignment-free fingerprint cryptosystem based on fuzzy vault scheme"