Security-Enhanced Fuzzy Fingerprint Vault Based on Minutiae's Local Ridge Information*

Peng Li, Xin Yang, Kai Cao, Peng Shi, and Jie Tian

Institute of Automation, Chinese Academy of Sciences, Beijing 100190 China
tian@ieee.org, jie.tian@ia.ac.cn
http://www.fingerpass.net

Abstract. Fuzzy vault is a practical and promising fingerprint template protection technology. However, this scheme has some security issues, in which cross-matching between different vaults may be the most serious one. In this paper, we develop an improvement version of fuzzy vault integrating minutiae's local ridge orientation information. The improved fuzzy fingerprint vault, a two factor authentication scheme to some extent, can effectively prevent cross-matching between different fingerprint vaults. Experimental results show that, if and only if the fingerprint and the password of users are simultaneity obtained by the attacker, the fuzzy vault can be cracked. Results under three scenarios indicate that, although the authentication performance of Scena.1 decreases a little in term of GAR, the security of Scena.2 and Scena.3, hence the security of the whole scheme, is enhanced greatly.

Keywords: Fuzzy vault, Cross-matching, Minutiae descriptor, Hermit's interpolation polynomial, SHA-1.

1 Introduction

Traditional biometric systems expose some disadvantages, for example, template security issue due to raw data storage and irrevocability issue because of the inherence property of biometric (e.g., fingerprint, iris, face). We can hardly find solutions for these disadvantages solely by means of biometric theory itself. Therefore, the technology combining biometrics and cryptography, called biometric encryption, biometric template protection or biometric cryptosystem, has attracted remarkable attention, because it may provide potential solutions for the above problems. A good survey for this field can be found in [1].

Over past years, many technologies which integrate biometrics with cryptography were proposed. Souter et al. [2] performs Fourier Transform upon fingerprint

* This paper is supported by the Project of National Natural Science Foundation of China under Grant No. 60875018 and 60621001, National High Technology Research and Development Program of China under Grant No. 2008AA01Z411, Chinese Academy of Sciences Hundred Talents Program, Beijing Natural Science Foundation under Grant No. 4091004.

M. Tistarelli and M.S. Nixon (Eds.): ICB 2009, LNCS 5558, pp. 930–939, 2009.

images and then combines the phase information with a random-selected key to make a Lookup Table. If the decryption step succeeds, the correct key is released from the Lookup Table, otherwise a reject signal is given. This is the first practical algorithm in this field but no performance results have been reported. Biohashing [3] is a two-factor authentication method, which uses WFMT(Wavelet Fourier Mellin Transform) feature of fingerprints and performs iterative inner product upon WFMT and a group of random number vectors. The 0-EER can be achieved providing the key (random number vector) is not stolen. However, if the key is stolen, the EER may be much higher than the plain biometric system [4]. Juels and Sudan [5] proposed the fuzzy vault scheme to try to bridge the gap between the fuzziness of biometrics and the exactitude of cryptography. Lee et al. [6] proposed a cancelable fingerprint template technology, using the local minutiae information. This method provided some promising results using transformed fingerprint templates.

Among all the technologies above, fuzzy vault(FV) is the most practical one in the term of security and authentication performance. Juels and Sudan [5] first proposed the fuzzy vault scheme. Clancy et al.[7] proposed the implementation of fuzzy vault for fingerprint, using the cartesian coordinates of minutiae. Holding the assumption that the query and template fingerprints were prealigned, they reported FRR≈20-30%(FAR≈0). Uludag et al.[8][9] and Nandakumar et al.[10] proposed more robust and effective implementation of fuzzy fingerprint vault. They also developed an automatic alignment method in the encryption domain, using ridge curvature maximum values(i.e., so-called helper data). The performance they reported is FRR≈10%(FAR≈0%), making significant improvement compared to Clancy's implementation. Although fuzzy fingerprint vault becomes more and more effective, there remains some security and privacy issues involved with it. As pointed out in [11], fuzzy fingerprint vault leaks some information about the original fingerprint minutiae template. Chang et al.[12] exploited the chaff points' statistical property to distinguish real minutiae from the chaff. Kholmatov and Yanikoglu [13] realized the correlation against fuzzy fingerprint vault, obtaining 59% success rate for two correlated fingerprint databases. Nandakumar et al.[11] tried to solve this problem using password as an additional authentication layer. However, if the password is obtained by the attacker, he/she can perform cross-matching just as [13] shows. In addition, Li et al.[14] pointed that Reed-Solomon correction code is not appropriate for fuzzy vault. After analyzing CRC, we think that it is not suitable for fuzzy vault either, so SHA-1 is used to replace CRC in our security-enhanced scheme to check the key's correction. Minutiae descriptor has been used for enhancing the security of fuzzy fingerprint vault [16], but it can not prevent cross matching described in [13].

In this paper, we propose a security-enhanced fuzzy fingerprint vault integrating the local minutiae information into the original scheme. From each minutia, we derive the corresponding invariant value based on the descriptor proposed in [15]. Afterwards the original minutiae are transformed into deformation domain using the invariant values. The procedures of encoding and decoding for fuzzy fingerprint vault are performed in the deformation domain.

2 Methods Enhancing FV's Security

The security of fuzzy fingerprint vault is mainly enhanced by transforming all the original minutiae into deformation domain. Like [6], the transforming method extracts from each minutia a translation and rotation invariant value, which is obtained by using a user-specific random vector and the orientation information of the neighboring regions around each minutia. And then we compute the transformation amount for each minutia by using the designed changing function. However, we compute the local ridge orientation vector using minutiae decriptor[15], rather than equal angel sample in all the concentric circles[6]. And the changing function is generated using Hermit's Interpolation Polynomial, in place of piece-wise linear interpolation[6]. The transformation accuracy is improved through resorting to minutiae descriptor and Hermit's Interpolation Polynomial. The encoding and decoding phases of fuzzy vault are carried out in the transformed domain. Respectively, the encoding and decoding procedures of security-enhanced fuzzy fingerprint vault are shown in Fig. 1 and Fig. 2.

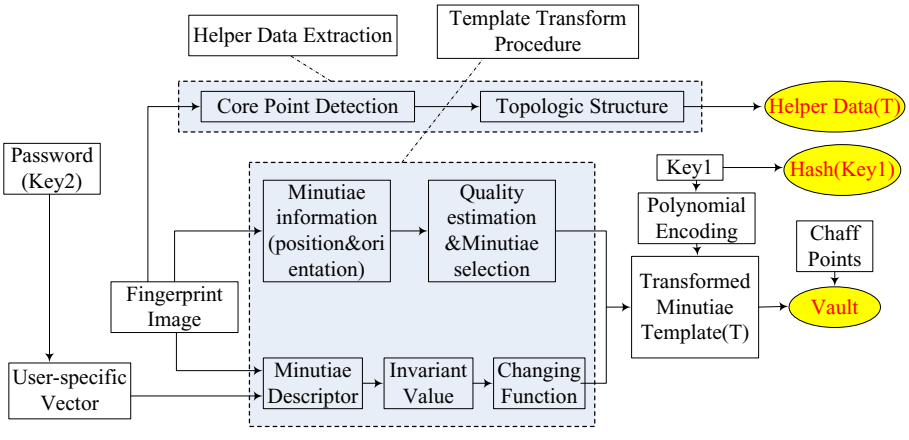


Fig. 1. Encoding procedure of security-enhanced fuzzy fingerprint vault

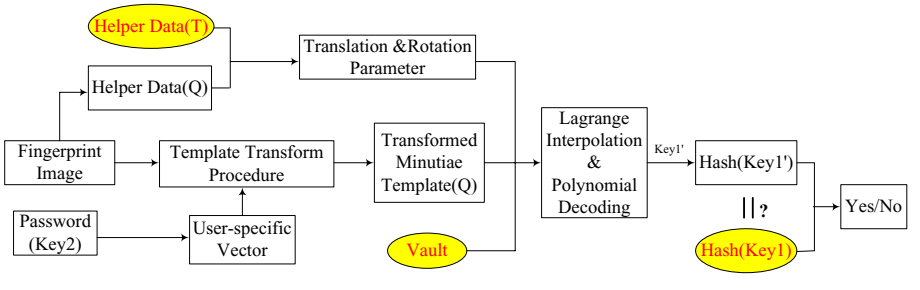


Fig. 2. Decoding procedure of security-enhanced fuzzy fingerprint vault

2.1 Invariant Value Extraction

We compute each minutia's invariant value using a similar method described in [6]. However, in [6], the authors conduct equal angle sample in all the concentric circles, which may miss some ridge information in outer layer circles because the arcs connecting two adjacent sample points may cross two or more adjacent ridges. So we adopt ridge orientation-based minutiae descriptor[15] to compute the invariant value. Fig. 3 shows the difference between sample structure in [6] and minutiae descriptor sample structure. We adopt the same parameter setting as [15]. The minutiae descriptor consists four concentric circles and the radius are 27, 45, 63 and 81 pixels. Respectively, they contain 10, 16, 22 and 28 points, uniformly sampled in the corresponding circle. In all 76 sample points are obtained. Fig. 3 shows that minutiae descriptor can acquire more information than equal angle sample method. One difference is that we extract the minutiae descriptor in thinned ridge image. For the sample point `sp_i`(denoting its position with `co_i` and its 8-neighborhood with `nh_i`), we compute its orientation `O_i` as follows:

```
If sp_i locates in any thinned ridge
  Then co_i is recorded;
Else If sp_i locates in no thinned ridge AND a ridge point is
within nh_i
  Then the nearest ridge point rp_i is recorded;
Else If sp_i locates in no thinned ridge AND no ridge point is
within nh_i
  Then sp_i is labeled as a background point;
If a ridge point is recorded
  Then O_i is computed by the ridge orientation;
Else If the background point
  Then O_i is the same as the corresponding minutia's orientation;
```

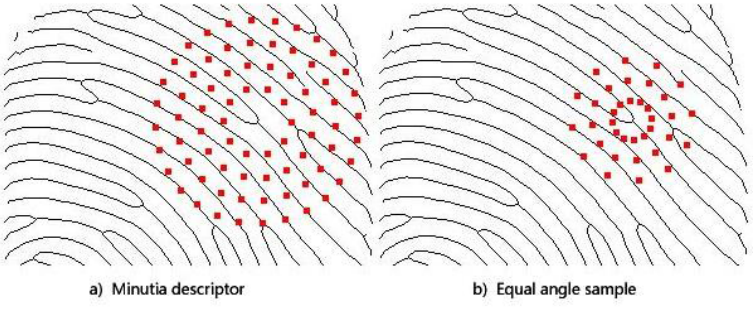


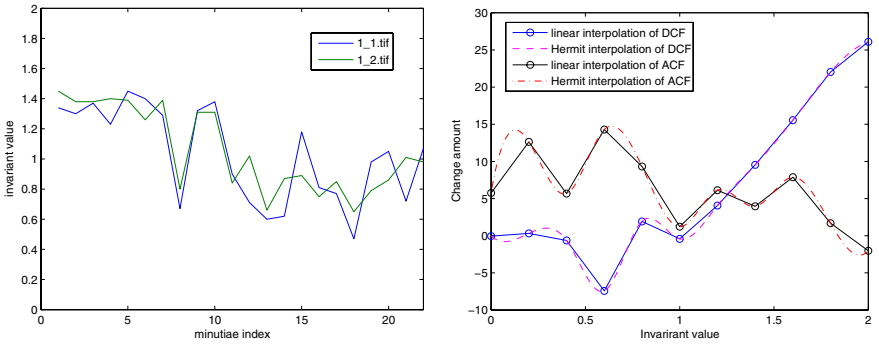
Fig. 3. Minutia descriptor vs. Equal angle sample

Denote the i-th minutia's orientation θ_i and the j-th sample point's orientation θ_{ij}. Thus we can obtain a 76-dimension translation and rotation invariant vector, depicted in (1):

$$T_i = [d(\theta_{i,1} - \theta_i), d(\theta_{i,2} - \theta_i), ..., d(\theta_{i,76} - \theta_i)]$$
$$d(\theta_1, \theta_2) = \begin{cases} \theta_1 - \theta_2, & \text{if } -\frac{\pi}{2} < (\theta_1 - \theta_2) < \frac{\pi}{2} \\ \theta_1 - \theta_2 + \pi, & \text{if } -\pi < (\theta_1 - \theta_2) < -\frac{\pi}{2} \\ \theta_1 - \theta_2 - \pi, & \text{if } \frac{\pi}{2} < (\theta_1 - \theta_2) < \pi \end{cases} \quad (1)$$

The subsequent procedure of generating an invariant value is the same as [6]. First, generate an user-specific random vector R_{pwd} with the same length as T_i, i.e., 76. Then two 76-dimen vectors are normalized to obtain t_i and r_{pwd}. Finally, the i-th invariant value corresponding to i-th minutia is computed using inner product, as shown in (2).

$$m_i = t_i \circ r_{pwd} \quad (2)$$



(a) (b)

Fig. 4. (a) "Invariant" values of corresponding minutiae in "1_1.tif" and "1_2.tif" in FVC2002 DB2 set A. The X axis is the minutiae index (22 in all) and the Y axis is the invariant value; (b) Hermit's Interpolation Polynomial is smoother than piece-wise linear interpolation.

In theory, m_i is translation and rotation invariant, but it changes a little sample to sample due to the presence of noise and feature extraction error. We compute all the corresponding minutiae's invariant values of image "1_1.tif" and "1_2.tif" in FVC2002 DB2 set A. Our minutiae extraction algorithm finds 22 couples of corresponding minutiae. Fig. 4(a) shows the difference of the invariant values computed in "1_1.tif" and "1_2.tif", using the same password(i.e., random generator). From Fig. 4(a), we can see that 18 couples of corresponding minutiae have "invariant" values with absolute error less than 0.2, and 12 couples have the ones with absolute difference less than 0.1. The tiny difference can be compensated in the following minutiae matching procedure, using bounding box matching method as used in [10].

2.2 Changing Function Design

Compared to [6], the biggest improvement that our design method makes lies in the interpolation method. We employ Hermit's Interpolation Polynomial, a smoother interpolation curve, to replace the piece-wise linear interpolation used in [6].

The transformation (translation and rotation) amount of each minutia is determined by the output of the changing function, whose input is the invariant value corresponding to the minutia. In theory, if the same "invariant" values are obtained from differently impressed fingerprint images, the transformation amount will be accordant. So the geometric relation between original fingerprint templates is preserved after transformation. That is why the encoding and decoding procedures of fuzzy fingerprint vault can be conducted in the transformed domain. Designing a group of changing functions which can derive coherent output from the invariant value is a challenging problem. Our change function is designed as follows:

1) Create two random number sequences X and Y, whose ranges are respectively limited in $[-\beta, -\alpha] \cup [\alpha, \beta]$ and $[-\eta, -\gamma] \cup [\gamma, \eta]$, using the user's password as seed;

2) Sum the outputs of X and Y as the control points of two changing function, respectively. The control points of distance change function(DCF) and angle change function(ACF) are generated as following equation (3):

$$\begin{aligned} L_{pwd}(nT) &= x_0 + x_T + ... + x_{(n-1)T} + x_{nT} = \sum_{i=0}^{n} x_{iT} \\ \Theta_{pwd}(nT) &= y_0 + y_T + ... + y_{(n-1)T} + y_{nT} = \sum_{i=0}^{n} y_{iT} \end{aligned} \tag{3}$$

3) Perform Hermit's Interpolation Polynomial to obtain the values of $L_{pwd}(p)$ and $\Theta_{pwd}(p)$ between $(k-1)T$ and kT. Hermit's Interpolation Polynomial is smoother than linear interpolation used in [6]. Fig. 4(b) can show this point (typically, $\alpha = 5, \beta = 10, \eta = 5, \gamma = 10$). The contrastive minutiae maps before and after transformation of a fingerprint from FVC2002 DB2 are shown in Fig.5(b) and Fig.5(c). Fig.5(d) lays transformed minutiae map upon original minutiae map and shows that there are few couples of minutiae identified as corresponding.

2.3 Encoding

In the security-enhanced fuzzy fingerprint vault, besides the key concealed in the Vault, we also need a password, which is used to generating invariant value and the changing function, as elaborated in the two subsections above. So our scheme is somewhat two-factor authentication scheme: password+fingerprint. If and only if correct fingerprint and password(Key2) are presented, Key1 will be released, otherwise a reject signal is given. We will confirm this point in the subsequent experiments. The encoding procedure is as shown in Fig.1.

During vault encoding phase, we first extract all the minutiae and use minutiae quality estimation method, as employed in[10], to select 20-40 top-ranking and well-separated minutiae. At the same time, the invariant value corresponding to each minutia is computed using the Key1(password) and the ridge orientation based minutiae descriptor, hence the change function. Afterwards the selected minutiae are changed into the transformation domain by using the user-specific

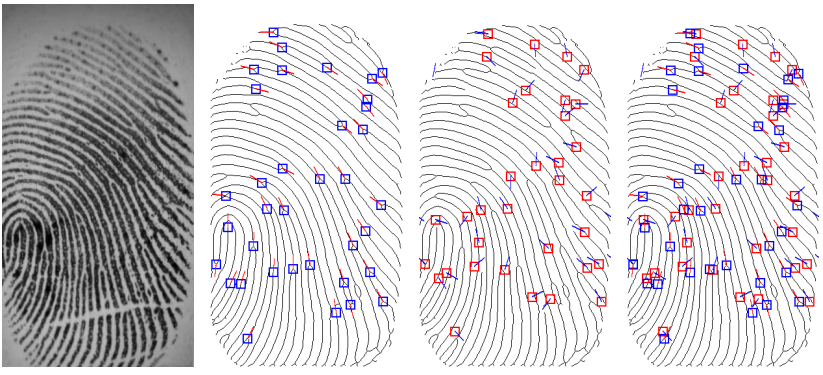


Fig. 5. (a) A fingerprint from FVC2002 DB2; (b) Minutiae map before transformation; (c) Minutiae map after transformation; (d) Transformed minutiae map overlays original minutiae map

changing function. Then we generate in the Galois Field $GF(2^{16})$ a polynomial f, whose coefficient is determined by the Key2 with length 16*n(n-1 is the polynomial degree). The transformed minutiae's location and orientation $x_i (i = 1, 2, ..., r)$ are encoded and projected in the polynomial f to obtain $f(x_i)$, and then $\{(x_i, f(x_i), i = 1, 2, ..., r\}$ are stored into the vault. A group of chaff points $\{(y_j, z_j)(j = 1, 2, ..., s)\}$, which don't lie in f, are added into the vault. Now the vault consisting $r+s$ elements has been created. In addition, topological structure based helper data extraction method [17] is used in our scheme and the helper data are also stored in encoding procedure to be used for automatic alignment in encrypted domain. Based on Li et al.[14]'s analysis, we replace the CRC-16 with SHA-1 check, that is to say, we compute *SHA-1(Key2)* and store it for key check in the decoding phase.

2.4 Decoding

In decoding phase(see Fig.2), a query fingerprint image is presented with the user's password. The same template transformation method is performed by using the query's invariant values to obtain Template(Q). Meanwhile, the query's helper data(Q) are also extracted and compared with helper data(T) to acquire the translation and rotation parameter, according to which Template(Q) is aligned to obtain Template(Q'). Afterwards a bounding-box minutiae matcher, as used in [10], is adopted to search the corresponding minutiae in the vault. Thus an unlocking set, in which each element consists $n(n-1$ denotes the polynomial degree) candidate points, is decoded to get the candidate $Key2'$. Then SHA-1($Key2'$) is computed and compared with SHA-1($Key2$). If these two hash values equal, it proves that $Key2' = Key2$ and the user's key is restored correctly, otherwise a failure will be reported.

3 Experiments

In order to validate the authentication performance and security of our improved fuzzy vault scheme, experiments are conducted under three scenarios: normal scenario(Scena.1), password-stolen scenario(Scena.2) and fingerprint-stolen scenario(Scena.3). The 1st and 2nd samples of each finger in FVC2002 DB2 Set A are selected for experiments because they have less transformation than other samples. The control point range parameters are set empirically and typically as: $\alpha = 5, \beta = 10, \gamma = 5, \eta = 10$, which makes a trade-off between authentication performance and security.

For Scena.1, assuming the attacker has no knowledge of the user's password, fingerprint minutiae templates from the same finger are transformed using the same password. For genuine test, the first sample is used for template and the second for query, which yields 100 trials in all. For imposter test, the first samples of the first 10 fingers are used for template respectively, the first sample of fingers, whose index is larger than the template finger, is used for query. This branch experiment yields 945 trials in all. The terms GAR(Genuine Accept Rate) and FAR(False Accept Rate) are used to indicate the performance. Table 1 gives the GAR and FAR corresponding to original fuzzy vault and our proposed scheme. Results show that the GARs of security-enhanced FV scheme have tiny decrease than original scheme, while FARs of two schemes approximately equals. In spite of this point, please note that the most valuable point of our proposed scheme lies in that it can eliminate the possibility of cross-matching between two vaults from the same finger. However it could satisfy the need of typical cryptography protocol, for example typical 128-bit AES key(n=8).

Table 1. Performance comparison of proposed security-enhanced FV scheme and the original FV scheme in Scena.1

	Degree	**7**	**8**	**9**	**10**	**11**
Proposed scheme	**GAR(%)**	89	88	86	84	82
	FAR(%)	0.07	0.03	0.04	0.03	0.02
Original scheme	**GAR(%)**	92	92	90	89	87
	FAR(%)	0.3	0.06	0.02	0.01	0

For Scena.2, given the user's password is stolen by the attacker, i.e., using the same password and fingerprints from different fingers to crack our scheme. We conduct 198 trials in all in this branch experiments, and the term CSR (Cracking Success Rate, the ratio of successful cracking times to total cracking times) is used to evaluate the security. Table 2 shows the security in this scenario. It can be seen that if the user's password is lost, the possibility of our proposed scheme being cracked is small. For Scena.3, assuming the user's original fingerprint information is stolen by the attacker and the user reissues a new vault using another transformation version of his/her fingerprint, i.e., using the original fingerprint minutiae information and a random selected key to crack the new issued vault. In

all 200 trials are conducted on selected fingerprint samples in this branch experiments, and the same term CSR is used to evaluate the result, which is shown in Table 3 with regard to different polynomial degrees. The result shows that if the user's fingerprint is stolen by the attacker and is used to attack the new issued vault, the success possibility is low enough to prevent this case. Combination of Scena.2 and Scena.3's results shows that, if and only if the correct password and the query fingerprints from the same finger as the template fingerprint are present simultaneously, the vault could be decoded successfully.

Table 2. CSR of proposed security-enhanced FV scheme in Scena.2

Degree	**7**	**8**	**9**	**10**	**11**
CSR(%)	0.5	0.5	1.0	0	0.5

Table 3. CSR of proposed security-enhanced FV scheme in Scena.3

Degree	**7**	**8**	**9**	**10**	**11**
CSR(%)	2.0	1.5	1.5	1.0	0.5

4 Security Analysis

In this section, we employ the min-entropy method, adopted in [16], to analyze the security of our proposed scheme. Assuming both minutiae location and orientation are uniformly distributed, the min-entropy of minutiae template M^T given the vault V can be computed as

$$H_\infty(M^T|V) = -log_2\left(\frac{\binom{r}{n+1}}{\binom{r+s}{n+1}}\right), \tag{4}$$

where, r, s and n denote number of minutiae, number of chaff points and polynomial's degree respectively and they are typically 20, 200, 8, respectively, so the typical security of our proposed scheme is approximately 34 bits in normal scenario. In password-stolen scenario and fingerprint-stolen scenario, the CSR is so small that the security under the two scenarios could not be affected. So we can conclude that the security measures of Scena.2 and Scena.3 both are approximately 34 bits. Because of the possibility of cross-matching's existence, previous schemes[7][8][9][10] usually can not achieve their claimed security. We eliminate the possibility of cross-matching to assure the security measure that our proposed scheme can achieve.

5 Conclusion

This paper employs the minutiae's local ridge information to improve the security of fuzzy fingerprint vault by eliminating the possibility of cross-matching between different vaults. Experimental results show that the authentication performance leads a tiny decrease. However, it can still satisfy the typical security need.

References

1. Jain, A.K., Nandakumar, K., Nagar, A.: Biometric Template Security. EURASIP Journal on Advances in Signal Processing 2008, Article ID 579416, 17 pages (2008)
2. Soutar, C., Roberge, D., Stoianov, A., Gilroy, R., Kumar, B.V.K.V.: Biometric Encryption, ICSA Guide to Cryptography. McGraw-Hill, New York (1999), http://www.bioscrypt.com/assets/Biometric_Encryption.pdf
3. Jin, A.T.B., Ling, D.N.C., Goh, A.: Biohashing: Two Factor Authentication Featuring Fingerprint Data and Tokenised Random Number. Pattern Recognition 37, 2245–2255 (2004)
4. Lumini, A., Nanni, L.: An Improved BioHashing for Human Authentication. Pattern Recognition 40, 1057–1065 (2007)
5. Juels, A., Sudan, M.: A Fuzzy Vault Scheme. In: Lapidoth, A., Teletar, E. (eds.) Proceeding of IEEE Int. Symp. Information Theory, p. 408 (2002)
6. Lee, C., Choi, J.Y., Toh, K.A., Lee, S.: Alignment-Free Cancelable Fingerprint Templates Based on Local Minutiae Information. IEEE Transactions on Systems, Man, and Cybernetics, Part B 37(4), 980–992 (2007)
7. Clancy, T.C., Kiyavash, N., Lin, D.J.: Secure Smartcard-based Fingerprint Authentication. In: Proceeding of ACMSIGMM 2003 Multimedia, Biometrics Methods and Applications Workshop, pp. 45–52 (2003)
8. Uludag, U., Pankanti, S., Jain, A.K.: Fuzzy Vault for Fingerprints. In: Proceedings of Fifth International Conference on AVBPA, Rye Town, USA, pp. 310–319 (2005)
9. Uludag, U., Jain, A.: Securing Fingerprint Template: Fuzzy Vault with Helper Data. In: Proceedings of the 2006 Conference on Computer Vision and Pattern Recognition Workshop (2006)
10. Nandakumar, K., Jain, A.K., Pankanti, S.: Fingerprint-Based Fuzzy Vault: Implementation and Performance. IEEE Transactions on Information Forensics and Security 2(4), 744–757 (2007)
11. Nandakumar, K., Nagar, A., Jain, A.K.: Hardening Fingerprint Fuzzy Vault Using Password. In: Lee, S.-W., Li, S.Z. (eds.) ICB 2007. LNCS, vol. 4642, pp. 927–937. Springer, Heidelberg (2007)
12. Chang, E.C., Shen, R., Teo, F.W.: Finding the Original Point Set Hidden among Chaff. In: Proceedings of the 2006 ACM Symposium on Information, computer and communications security, pp. 182–188. ACM Press, New York (2006)
13. Kholmatov, A., Yanikoglu, B.: Realization of Correlation Attack Against the Fuzzy Vault Scheme. In: Proceedings of 2008 SPIE / Biometrics, Security, Forensics, Steganography, and Watermarking of Multimedia Contents, vol. 7, pp. 68190O–68190O-7 (2008)
14. Li, Q., Liu, Z., Niu, X.: Analysis and Problems on Fuzzy Vault Scheme. In: Proceedings of 2006 International Conference on Intelligent Information Hiding and Multimedia Signal Processing, pp. 244–250 (2006)
15. Tico, M., Kuosmanen, P.: Fingerprint Matching Using An Orientation-based Minutia Descriptor. IEEE Transactions on Pattern Analysis and Machine Intelligence 25(8), 1009–1014 (2003)
16. Nagar, A., Nandakumar, K., Jain, A.K.: Securing Fingerprint Template: Fuzzy Vault with Minutiae Descriptor. In: International Conference of Pattern Recognition (to appear) (2008)
17. Li, J., Tian, J., Yang, X., Shi, P., Li, P.: Topological Structrue based Fuzzy Vault Alignment Method. In: International Conference of Pattern Recognition (to appear) (2008)