International Journal of Fuzzy Logic and Intelligent Systems, vol. 11, no. 4, December 2011, pp. 286-292
http://dx.doi.org/10.5391/IJFIS.2011.11.4.286

RN-ECC Based Fuzzy Vault for Protecting Fingerprint Templates

Dae-Jong Lee[1], Yong-Nyuo Shin[2] , Seon-Hong Park and Myung-Geun Chun[1]*

[1] College of Electrical & Computer Engineering, Chungbuk National University, Cheong-Ju, 361-763, Korea
[2] Department of Computer Engineering, Hanyangcyber University, Seoul 133-791, Korea

Abstract

Biometrics systems are used in a wide range of areas, including the area of crime prevention, due to their unique characteristics. However, serious problems can occur if biometric information is disclosed to an unauthorized user. To address these issues, this paper proposes a real valued fuzzy vault method, which adopts a real number error correction code to implement a fuzzy vault scheme for protecting fingerprint temples. The proposed method provides the benefit of allowing the private key value to be changed at any time, unlike biometric template such as a fingerprint, which is not easily renewable even if its security has been breached. The validity of the proposed method is verified for fingerprint verification.

Keywords: Fuzzy vault, RN-ECC, Fingerprint recognition, Biometrics, Information security

1. Introduction

Biometric technology can prevent various illegal acts related to identification through its positive function of authenticating individuals. However, biometric technology can also be used to trace personal profiles, related transactions, or changes in the database without the consent of the person in question, and accumulate diverse personal information with regard to a particular individual. ISO 24745 presents three major requirements for biometric technology – irreversibility, unlinkability, and renewability[1].

Recently, techniques to protect biometric templates have been actively studied. Generally, these techniques are based on feature transformation or biometric cryptosystem. Feature transformation methods can be divided into the BioHashing and robust hashing method, depending on the use of the method that allows inverse transformation. On the other hand, there are two methods of biometric cryptosystem – the key generation method that generates the encryption key directly from the biometric information, and the key binding method that binds the encryption key with the biometric information and extracts the key later, if necessary, using the biometric information[2].

The feature transformation method is based on the function that is defined by the user-specified key value or password. In particular, if inverse transformation is possible, there is an additional requirement for the key value to be protected. However, the safety of the system can be improved, since the attacker must have the biometric information as well as the key value in order to attack the biometric system. These days, the BioHashing method based on random rectangular coordinates is most widely being studied [2]. The input feature vector generates a particular value through the inner product with rectangular coordinates that are generated randomly in advance and saved in a token, and the value is made binary using the specified threshold value to have the intended BioHashing value. The experiment result shows that this method provides the benefit of a low "false accept rate." However, it also has several shortcomings and limitations as described below [3].

The first problem is that the original biometric template can be obtained if the user-defined key value used for the inverse transform function is disclosed. The second problem is that the degree of similarity between templates before transformation must be maintained in order to prevent deterioration of the recognition rate, because matching occurs at the transformed domain. Therefore, the recognition rate can be changed significantly depending on the selection of the transform function. The final problem occurs when the large-scale random matrix is used to increase the recognition rate. In this case, the benefit of using the biometric algorithm can be lost, as the assessment function of the matrix itself becomes greater than the assessment function by the biometric information, and there is a risk of increasing the false accept rate.

Manuscript received Nov. 12, 2011; revised Nov. 29, 2011; accepted Dec. 2;
+Corresponding author
This research was supported by Basic Science Research Program through the National Research Foundation of Korea(KRF) funded by the Ministry of Education, Science and Technology (2011-0026223)

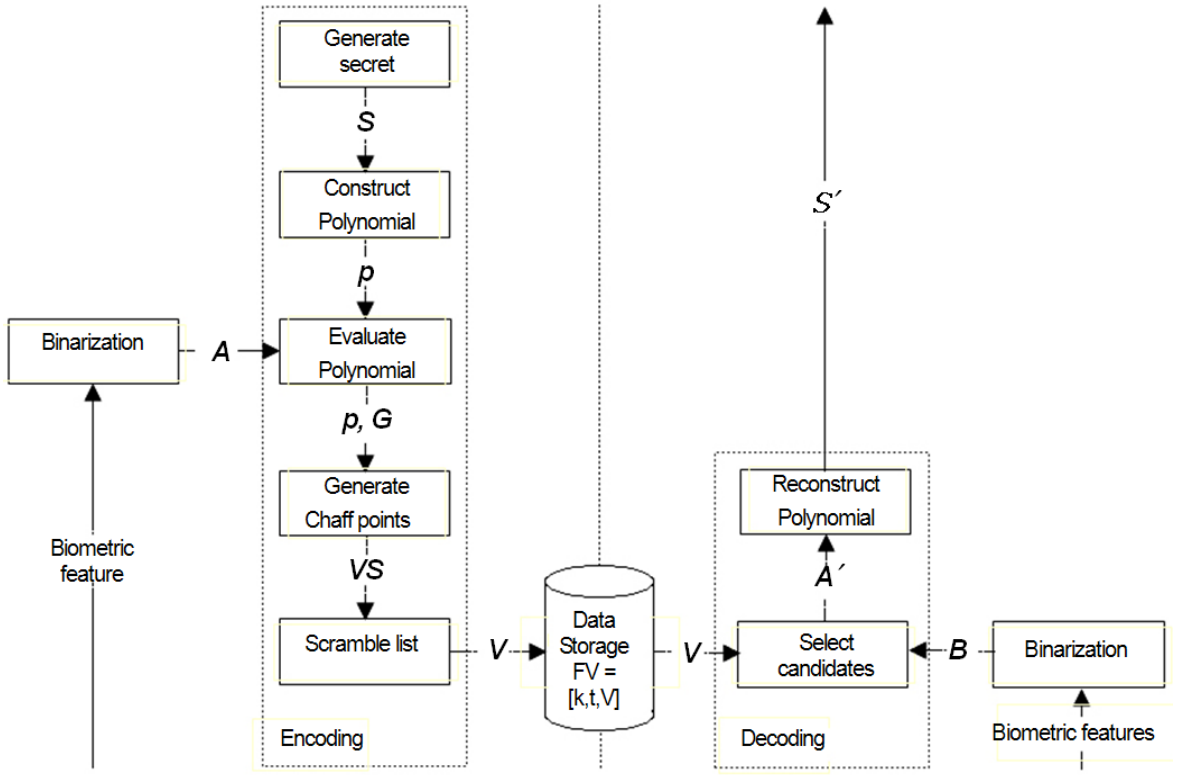


Fig. 1 Biometrics by fuzzy vault scheme[5]

This paper proposes a fingerprint template protection technique to ensure the privacy and security of the biometric information based on a real number fuzzy vault, using real-number error correction code. The error correction code or CRC (Cyclic Redundancy Check) has been used to cope with fluctuations of the biometric information, when binding the key with the polynomial coefficient and extracting the key using the biometric information, based on the finite field polynomial. However, implementation becomes complex in this case, and the real-number matching device cannot be used that was developed to match the biometric information. To overcome these shortcomings, the RN (Real Number)-ECC (Error Correcting Code) was adopted, which as the approximation characteristics of a real-number polynomial.

This paper is composed as follows. In chapter 2, the biometric template protection technique using the fuzzy vault will be reviewed. Chapter 3 describes a proposed real number based fingerprint fuzzy vault method. Chapter 4 analyzes the experiment results. In Chapter 5, conclusions will be given.

2. Biometric information protection technique using the fuzzy vault

The fuzzy vault process consists of encoding and decoding proposed by Jules and Sudan to protect the important information [4]. Encoding is performed as follows. Alice tries to hide a confidential information S using the set A. The polynomial function $P(x)$ is constructed with the secret S. Then, elements in the set A are assigned to the variable x of the polynomial function, and thus points on the polynomial $P(x)$ are generated. To hide polynomial $P(x)$ from the attacker, lots of chaff points that are irrelevant to $P(x)$ are inserted to generate V (Vault), and then encoding is completed.

On the other hand, a genuine user Bob tries to obtain S in the vault using the set B. If there are many matches between B elements and A elements, B will identify most points on the polynomial $P(x)$ from V. However, the points identified using the set B may include points that are irrelevant to the polynomial expression. These erroneous points will be corrected using the error correcting code, and Bob can obtain S accurately.

For an attacker, B and A almost does not match, thus the attacker cannot access S due to many chaff points. The fuzzy vault algorithm can narrow the gap between ambiguity of the key and the accuracy required by the encryption structure, because the error correcting code is used even when the set B doesn't accurately match the set A. In addition, set A and secret S are simultaneously protected by chaff points that are irrelevant to the polynomial function.

One of the characteristics of biometric information is that biometric information extracted during the registration process for the same person can be different when it is obtained for authentication. For fingerprint recognition, the value can differ

depending on the degree of alignment with the sensor. Therefore, the fuzzy vault, which introduces the concept of "fuzzy" among the concepts described above, can be well combined with the biometric system.

Figure 1 shows the diagram that combines the traditional fuzzy vault scheme and the biometric system. The encoding process to make the fuzzy vault can be described as follows. The user generates S randomly, which is composed of *K*-bit, and will be used as an identifier of the user. S is split into $(\{s_1, s_2, ..., s_{K/l}\})$ that is composed of l-bits evenly, and these bits compose the coefficient of the polynomial $P(x)$ that has the (K/l) coefficient, because all arithmetic operations of the general fuzzy vault system (coefficients having the l -bit value) are based on the finite field $GF(2^l)$. In conclusion, the polynomial $P(x)$ can be expressed by $d = ((K/l)-1)$, $P(x) = s_1 + s_2 x + \cdots + s_{(K/l)} x^{(K/l)-1}$. For the fuzzy vault, two sets (T, N) need to be generated.

The first set is for the genuine user $T = \{(a_1, P(a_1)), (a_2, P(a_2)), ..., (a_A, P(a_A))\}$, which is created by calculating the polynomial $P(x)$ using the quantized biometric feature value $A = \{a_1, a_2, ..., a_A\}$. All components of the user vault set T will be used to recover the polynomial function, while unlocking the vault. Therefore, the generated point should be at least $(d+1)$. Here, the set T is deemed to be composed of A points.

The second set is N, which is composed of several chaff points. These points play an important role in hiding the vault set T. $N = \{(v_1, w_1), (v_2, w_2), ..., (v_Q, w_Q)\}$ where v_1 is the corresponding x value as the input of the polynomial function, and w_1 is the corresponding polynomial function value. The x value used here should not be overlapped with the values belonging to T. That is, it is generated randomly within the scope of the field, while $(v_i \neq a_j, i = 1,2,..., q,\ j = 1,2,..., A)$, and satisfies the condition that it is not located at the polynomial $P(x)(w_i \neq P(v_i), i = 1,2,..., q)$. The final vault V is created by mixing the set T and N that are composed in this way. Then, all registration processes are completed, and the vault that is created will be stored on the smart card or USB memory to protect privacy.

To open a vault, two inputs (vault V and B) are required. The vault (V) is obtained from the storage media, whereas the test B can be obtained by acquiring biometric features from an individual. However, this process usually causes a serious problem when applied to an actual biometric system. First, the feature values of the biometric system, such as the fingerprint can vary due to external variables whenever the biometric information is obtained. Therefore, it is quite rare for sets A and B to match exactly as shown in the above process. So, error detection and correcting code to detect or modify the error with the extracted S' is required.

Error correction code has been studied actively since Shannon introduced the concept that "information can be transmitted or saved without loss, using error correction code" in his 1948 paper. Among these studies, the Reed-Solomon code [10] is most widely used in the fuzzy vault study area. The Reed-Solomon (RS) code is the error correcting code developed by Irving Reed and Gus Solomon in 1960, and belongs to the category of multiple BCH(Bose-Chaudhuri-Hoquenghem) code. This error correction code is widely used to improve the reliability of various digital communication systems and data storage systems.

Thus far, most fuzzy vault studies used the RS code. However, all variables and input values should be expressed in the value of Galois Field $GF(q)$ in order to apply this code. As a result, the feature value having the real-number value extracted from the fingerprint or face cannot be directly used. Furthermore, generalized inverse, which has been widely used in the linear algebra when calculating inverse of the polynomial function, cannot be used. In terms of security, this limitation means that the similar identifier, which can issue the real-number S for high security, cannot be issued, because S is given by the binary bit array only, and length at this time is limited by the size of the Galois Field in use. In addition, there is another shortcoming that the matching value for the finally extracted S' and S cannot use various similarity values defined in the real field. Therefore, this study proposes a real fuzzy vault based on real-number operation. For this, RN-ECC (Real Number Error Correcting Code) is required. RN-ECC has been widely studied since it was introduced by Marshall [11] and has been widely used[12].

3. Real fingerprint fuzzy vault technique based on RN-ECC

This paper proposes a real fuzzy vault method using the real-number ECC for the fingerprint recognition. Thus far, ECC or CRC (Cyclic Redundancy Check) have been used to overcome the changes of biometric information, when binding the key to the coefficient of the polynomial and extracting it again using the biometric information, based on the finite field polynomial. However, as described before, these approaches have the shortcomings of making implementation complex, and the real-number matching method cannot be used when matching with the ECC. Therefore, a RN-ECC was adopted to overcome these shortcomings. The RN ECC can be briefly described as follows [11].

Let us denote $\{x_i\}$ composing of the real-number data K as a row vector $x = [x_0, x_1, \cdots, x_{K-1}]$. Then, a N length code vector $y = [y_0, y_1, \cdots, y_{N-1}]$, $K < N$,can be expressed as follows.

$$y = xG \tag{1}$$

where G is a $K \times N$ generator matrix with the rank of K.

The block code can be expressed by the (N,K) code. Channel error will be marked as e. The matrix G^{-1} is the right inverse of G's $K \times N$, which satisfies the following relation and enables x to be restored accurately, if there is no channel noise.

$$GG^{-1} = I_K \tag{2}$$

$(N-K)\times N$ parity check matrix H, of which the rank is $N-K$, can be defined using the conjugate transpose * as follows.

$$GH^{*} = 0 \tag{3}$$

The code vector to estimate r can be described as follows.

$$r = y + e \tag{4}$$

Then, the syndrome s of the received vector r can be calculated as follows.

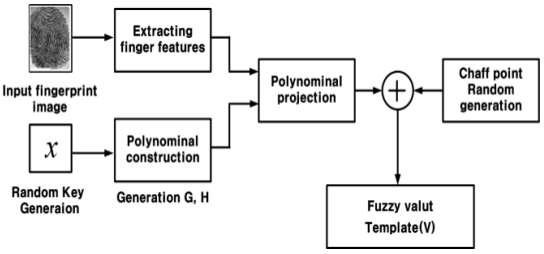
$$s = rH^{*} = (y+e)H^{*} = eH^{*} \tag{5}$$

where e is an unknown error pattern at N dimension, and $e = r - y$. Therefore, if the error value e is very small, the syndrome s comes to have a very small value. If both the transmitted code vector y and the received vector r are identical, the syndrome s becomes 0. If the syndrome s is close to 0, the row vector $\hat{x}$ to obtain can be finally estimated as follows.

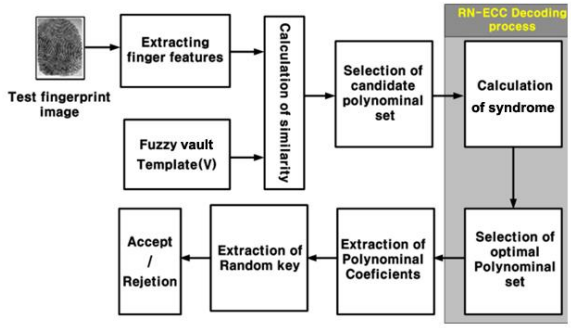
$$\hat{x} = rG^{T}(GG^{T})^{-1} \tag{6}$$

Figure 2 shows a proposed real valued fingerprint fuzzy vault technique based on the RN-ECC. First, a random key x is generated and assigned to an individual during the registration process. Then, a generator matrix G and the parity check matrix H are generated (explained in Eq. (1) and (3), respectively), using various basis functions, and the code vector y is generated that is described in Eq. (1). The code vector u is to use as the polynomial coefficient values to generate the value of $p(x)$. At the next step, the generated polynomial function and the feature value of the registered fingerprint are used to find the function values of $p(x)$. Finally, some chaff points are generated to protect the features of the fingerprint.

For the verification, features of the fingerprint are extracted from a captured image, and the candidate polynomial with high similarity is selected by comparing the extracted feature value and ones from the fuzzy vault. The selected candidate polynomial set contains the polynomial function corresponding to the fingerprint used at registration process, as well as generated by the chaff points. The proposed RN-ECC decoding process is performed for selecting the sets corresponding to the genuine fingerprint among these candidate polynomial sets.



(a) Registration process



(b) Verification process

Fig. 2 Proposed real valued fingerprint fuzzy vault method based on RN-ECC

To decode the RN-ECC, extraction process of the polynomial coefficient values for the selected candidate polynomial sets is required. From this, a polynomial coefficient value $\hat{r}$ is estimated and its syndrome value s is also calculated from Eq. (5). Afterwards, the coefficient value $\hat{r}$ is selected if this has the minimum syndrome s value. Then, the private key value, $\hat{x}$ is restored from the Eq. (6) that uses the estimated coefficient $\hat{r}$ and the generator matrix G, which was generated during the registration process. The final verification is performed by comparing the value $\hat{x}$ with x.

The advantage of the proposed method is that the private key value can be easily renewable unlike a fingerprint template. Moreover, it is difficult to extract the registered fingerprint template even though the fuzzy vault is disclosed in the case that the registered fingerprint template is not available, because the fuzzy vault contains also a lot of chaff points.

4. Experiment result and analysis

To evaluate the performance of the proposed method, 6 fingerprint images for one finger were collected from 60 persons. The chain code contour technique was used to extract the features of the obtained fingerprint [13-15]. The features extracted from the fingerprint can be expressed by location, angle, and type according to the chain code, and so they can be expressed as $m_i = (x_i, y_{i,}, \theta_{i,}, t_i)$ having the coordinate of x, y as well as angle θ. To apply the proposed method, the representative fingerprint features of each individual and the

chaff points were required. That is, 12 distinct feature values were extracted from each person using 6 fingerprint images based on the similarity analysis.

After selecting the representative features (x, y, θ), a second order polynomial $p(x, y, \theta)$ is generated for the selected representative features was constructed as follows.

$$p(x,y,\theta) = a_0 + a_1 x + a_2 y + a_3 \theta + a_4 xy + a_5 x\theta + a_6 y\theta + a_7 x^2 + a_8 y^2 + a_9 \theta^2 \quad (7)$$

To calculate the polynomial coefficient a_i described in Eq. (7), the random key S, generated matrix G, and parity check matrix H, which will be used to restore the coefficient value during the verification process, are required. In this work, we select the random key as $S = [11,22,33,44,55,44,33,22]$, and construct matrix G and parity check matrix H using the DCT (Discrete cosine transform) matrix and DFT (Discrete Fourier transform) matrix[11][12]. Now, lots of chaff points are required to protect the fingerprint template. Here, even though the FRR (False Reject Rate) increases as much as the number of chaff points, it can act favorably from the perspective of protecting the fingerprint features.

To analyze performance according to the number of chaff points, an experiment was conducted by varying the number from 100 to 1000. Figure 3 shows the representative features and chaff points when the number of chaff point is 200.

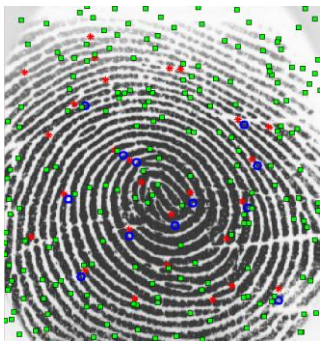


Fig. 3. Fingerprint image including chaff points

Figure 4 shows the polynomial values for 200 chaff points as well as for 12 genuine feature values. As shown in Figure 4, the polynomial corresponding to the genuine feature (data number 1 ~ 12) matches the polynomial. However, the polynomial corresponding to the chaff points contains the different values from the polynomial value calculated by the predefined polynomial function in the fuzzy vault.

The proposed method recognizes the fingerprint as described below. First, candidate feature values and their polynomial values are extracted from the fuzzy vault by comparing the live features of the fingerprint with the stored values in the fuzzy vault which also contains chaff points. To calculate the polynomial coefficient in Eq. (7), at least 10 genuine features are required.

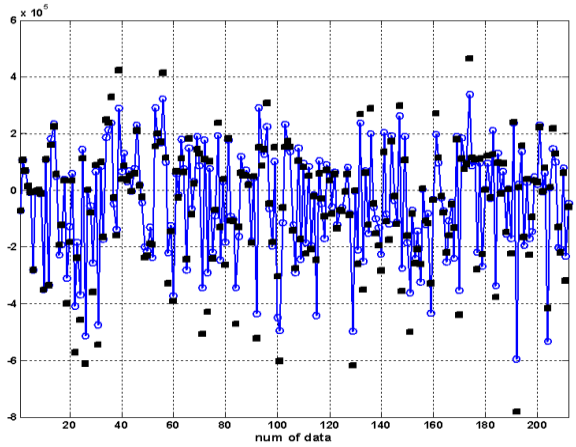


Fig. 4 Polynomial values including chaff points

In this work, the number of selected candidate feature values n was increased from 12 to 18 in order to assess performance. To restore the polynomial coefficient value among n selected candidate feature values, 10 feature values should be selected to compute the coefficient by matrix inverse given by Eq. (7). For the selecting process, we adopts the exhaustive search , that is, complete search for all combinations. For example, if n = 18, the syndrome value is calculated for the candidate feature set $C(18,10) = 43{,}758$. After then, the coefficients having the lowest syndrome value is restored, and finally the key value is extracted using the restore coefficient value. Here, more processing time is required for increasing n, however it has a positive impact from the security perspective since one can increase the number of chaff points.

Table 1 shows the recognition rates of the selected values. FAR in Table 1 refers to the false accept rate, whereas FRR refers to the false reject rate. The number of fingerprints subject to FRR was 180 (60 persons x 3 fingerprints), whereas the number of fingerprints used subject to FAR was 3,540 (59 persons x 6 fingerprints). As shown in Table 1, FAR was 0% regardless of the number n, and FRR decreases as the number n increases. The number n was set to 15 in this study with consideration of processing tim,e and performance of the proposed method was analyzed in various ways.

Table 1. Verification rate according to n

n	Number of combination	FAR(%)	FRR(%)
12	66	0	15
13	286	0	12.78
14	1001	0	10.28
15	3003	0	7.78
16	8008	0	5.28
17	19448	0	4.17
18	43758	0	3.61

Table 2 shows the comparison between the proposed method and chain code algorithm. The proposed method shows 0% FAR regardless of the number of chaff points. FRR increases as the number of chaff points increases. That is, FRR was 3.9% when the number of chaff points was 100, whereas FRR was 20% when the number of chaff points was 1,000. The higher number of chaff points, the stronger security is. That is, approximately $C(112,10) = 5.6594 \times 10^{13}$ times are required to find the genuine features when there are 100 chaff points. For the chain code based fingerprint recognition method, the FAR increases and the FRR decreases, as the threshold value increases.

When the number of chaff points is set to 200, providing a higher level of security in order to compare two methods, the FAR was 0% and the FRR was 7.78%. For the chain code based fingerprint recognition method, the FAR was 1.94% and the FRR was 3.84%. From the perspective of the FRR, the chain code based fingerprint recognition method shows 3.94% lower than the proposed method. However, the proposed method shows better result in terms of the FAR.

Moreover, the chain code based fingerprint recognition method provides no alternative method once the fingerprint information has been disclosed. On the other hand, the proposed method offers outstanding performance in terms of security, because the fingerprint template can be protected by the fuzzy vault scheme, and the polynomial set included in the fuzzy vault template can be changed by changing the key value.

The DCT matrix was applied to the performance shown in Tables 1 and 2 to create the generated matrix G and parity check matrix H. In addition to these basis matrices, this paper evaluated the performance of the proposed method for the generally used DFT matrix. Table 3 shows the recognition performance, depending on the type of the used basis function. As shown in Table 3, there is no meaningful difference in performance between the method using the DCT matrix and the DFT matrix. From this, it is verified that the proposed method is robust to choose basis function.

5. Conclusion

This paper proposed a new fuzzy vault method which uses the real-number error correcting code for hiding and restoring the feature values of the fingerprint. The error correcting code or CRC has been used to overcome fluctuations in the biometric information, when binding the key with the polynomial coefficient and extracting the key using the biometric information, based on the finite Galois field polynomial. However, as indicated previously, implementation becomes complex, and the real-number matching device that was developed to match the biometric template cannot be used. To overcome these shortcomings, the RN- ECC was adopted. The proposed method produced a better result than previous methods in terms of recognition performance and security. The secure binding with identity reference will be further studied [16].

Table 2. Verification rate according to the number of chaff points

Proposed method			Chain code based fingerprint recognition method		
Number of chaff points	FAR(%)	FRR(%)	Threshold value	FAR(%)	FRR(%)
100	0	3.9	10	1.94	8.88
200	0	7.78	20	1.94	3.84
300	0	9.73	30	2.5	1.43
400	0	10.83	40	2.77	0.51
500	0	11.61	50	2.78	0.16
600	0	13.61			
700	0	16.39			
800	0	17.22			
900	0	17.5			
1000	0	20			

Table 3. Verification rate according to the type of basis Function

Number of chaff points	DCT		DFT	
	FAR(%)	FRR(%)	FAR(%)	FRR(%)
100	0	3.9	0	3.89
200	0	7.78	0	7.78
300	0	9.73	0	9.72
400	0	10.83	0	10.83
500	0	11.61	0	11.67
600	0	13.61	0	13.61
700	0	16.39	0	16.39
800	0	17.22	0	17.22
900	0	17.50	0	17.50
1000	0	20.00	0	20.00

References

[1] Y. Shin, M. Kwon, Y. lee, J. Park, and M. Chun, “Biometric and Identity Reference Protection,” Journal of Korean Institute of Intelligent Systems, Vol, 19, No. 2, pp. 160-167, 2009.

[2] A. Teoh, Y. Kuan, S. LEE Cancellable Biometrics and Annotations on BioHash, Pattern Recognition 41, 2008

[3] A. Kong and K. Cheung, D. Zhang, An Analysis of BioHashing and its invariants, Pattern Recognition 39,

2005
[4] Juels A and Sudan M, "A fuzzy vault scheme," Proceeding of IEEE Int. Symposium on Information Theory, 2002.
[5] N. Karthik, A. Jain, "Fingerprint-based fuzzy vault: implementation and performance," IEEE Trans on Information Forensics and Securities, Vol. 2, 2007.
[6] P. Li and J. Tian, An alignment-free fingerprint cryptosysten based on fuzzy vault scheme, Journal of Network and Computer Applications, 2010.
[7] Y. Wang and K. N. Plataniotis, "Fuzzy vault for face based cryptographic key generation," in Proc. Biometrics Symposium 2007,
[8] F. Thomas, Z. Xuebing, B. Christoph, Fuzzy Vault for 3D face recognition systems, Int. Conf. on Intelligent information hiding and multimedia signal processing, 2008
[9] L. Yiun Joo, P. Kang Ryong, L. Sung Joo, B. Kwanghyuk, K. Jaihie, A new method for generating an invariant ISIS private key based on the fuzzy vault system, IEEE Trans. on System, Man, Cybernetics, Vol. 38, 2008.
[10] K. Moon, Error Correcting Code: Mathematical Methods and Algorithm, Wiley-Interscience, 2005
[11] T. Marshall, Coding of real-number sequences for error correction: a digital signal processing problem, IEEE Journal of Selected Areas in Communication, Vol. SAC-2, 1984.
[12] A. Kumar and A. Makur, Improved coding-theoretic and subspace-based decoding algorithms for a wider class of DCT and DST codes, IEEE Trans. on Signal Processing, Vol. 58, 2010.
[13] Govindaraju V., Z. Shi and J. Schneider, "Feature Extraction Using a Chain-coded Contour Representation," Int. Conf. on Audio and Video Based Biometric Person Authentication, Surrey, UK, 2003.
[14] Chikkerur S., Govindaraju V. and Alexander N. Cartwright, "K-plet and Coupled BFS: A Graph-Based Fingerprint Representation and Matching Algorithm," Lecture Notes in Computer Science, Vol. 3832, pp. 309-315, 2006.
[15] Asker M. Bazen and Sabih H. Gerez., "Fingerprint matching by thin-plate spline modeling of elastic deformations," Pattern Recognition, Vol. 36, pp. 1859-1867, 2003.
[16] Mi Kyeong You, Man-Jun Kwon, Sang Ho Lee and Myung Geun Chun, "Secure Binding of Identity Reference and Biometric Reference" Journal of Korean Institute of Intelligent Systems, Vol, 20, No. 5, pp. 610-616, 2010.

Dae-Jong LEE
Postdoc of the Chungbuk National University
Research Area: signal processing, biometrics
E-mail : bigbell@chunbuk.ac.kr

Yong-Nyuo Shin
Professor of the Hanyangcyber University
Research Area: telebiometric, mobile programming
E-mail : ynshin@hycu.ac.kr

Seon-Hong Park
Graduated student Chungbuk National University
Research Area: biometrics, robot control
E-mail : parkseonhong@chungbuk.ac.kr

Myung-Geun Chun
Professor of the Chungbuk National University
Research Area: biometrics, information processing
E-mail : mgchun@chunbuk.ac.kr