Fuzzy Face Vault: How to Implement Fuzzy Vault with Weighted Features*

DaeHun Nyang[1] and KyungHee Lee[2]

[1] Graduate School of Information Technology and Telecommunications, Inha University, Incheon, 402-751, Korea
nyang@inha.ac.kr
[2] Department of Electrical Engineering, The University of Suwon, Suwon, 445-743, Korea
khlee@suwon.ac.kr

Abstract. Ari Juel et al from ISIT 2002 presented a fuzzy vault scheme, which is a framework to encrypt a cryptographic key with a fuzzy key[5]. Following their framework, many trials to implement mainly a fuzzy finger vault have been proposed that enables us to keep secretly a key with our finger print. Our work is to focus on instantiating the fuzzy information of the fuzzy vault scheme with human faces instead of fingers. Most of face authentication algorithms are dependent upon weighted features, which are incompatible with the original fuzzy vault scheme. To reflect the level of importance of individual features from feature set, we introduce another layer between captured feature set and points in the polynomial to be interpolated.

1 Introduction

Biometrics are very versatile tools, but information privacy of biometrics also must be fully guaranteed because once revealed, it cannot be canceled unlike the traditional cryptographic keys. Thus, researches on biometrics protection have been extensively performed both by biometrics society and by cryptographic society[2,3,4].

Ari Juel et al from ISIT 2002 presented a fuzzy vault scheme, which is a framework to encrypt a cryptographic key with a fuzzy key. Following their framework, many trials to implement mainly a fuzzy finger vault have been proposed that enables us to keep secretly a key with finger prints[6,7].

Our work is to focus on instantiating the fuzzy information of the fuzzy vault scheme with human faces instead of fingers. Face is usually open to public and thus, it is easier to capture a certain person's face image than her finger print. So it might be thought that using face images as a biometric key is more vulnerable

* This research was supported by the MIC(Ministry of Information and Communication), Korea, under the ITRC(Information Technology Research Center) support program supervised by the IITA(Institute of Information Technology Advancement)(IITA-2006-C1090-0603-0028).

C. Stephanidis (Ed.): Universal Access in HCI, Part I, HCII 2007, LNCS 4554, pp. 491–496, 2007.

compared with using hidden biometrics such like finger prints and iris patterns. However, considering unobtrusiveness of face recognition, protection of a key with features from face images are very convenient and thus, it is quite necessary to protect features from face images against the attack on database that stores large number of cryptographic keys encrypted with features from many person's face images. Assume the situation that features from many person's face images are not protected. Then, attacker can easily obtain large number of people's face features by cracking the database. However, if the features are protected using a scheme such as fuzzy vault, then the attacker does not obtain any good.

Because images capturing a human face are not always the same, it seems that human face is fit exactly into the framework of the fuzzy vault. The fuzzy vault scheme, however, depends on the error correction code such as Reed-Solomon code. So, only the number of correct features from freshly captured features determines whether the key can be correctly recovered or not. This is because one feature encrypts only one share of a key, where the share is a secretly-split share of a key using secret sharing scheme. Thus, the fuzzy vault framework cannot give an individual feature a weight, and this property of the fuzzy vault makes it hard to incorporate face features into the fuzzy vault framework. Because most face authentication scheme is based on classification algorithm such as the principal component analysis and the linear discriminant analysis, the feature set is composed of eigen vectors, among which some eigen vectors having large eigen values have more importance than others. Thus, direct incorporation of the existing face authentication schemes into the fuzzy vault does not reflect the degree of importance of individual features and consequently, it will substantially degrade the original classifier's classification capability. Our aim is to design a fuzzy face vault scheme that can reflect the importance of individual features, which results in more exact incarnation of face fuzzy vault. With our fuzzy face vault scheme, one can keep secretly a midterm key by encrypting it with one's face image.

2 Background: Fuzzy Vault

In [5], the fuzzy vault is created by making a generalized Reed-Solomon codeword representing a secret as a corresponding polynomial p. This codeword is computed over x- coordinates corresponding to elements in the feature set. To hide the codeword, chaff points are added, i.e., random noise in the form of random (x_i, y_i) pairs.

To unlock a vault, one must determine the codeword that encodes the secret. Recall that the feature set specifies the x-coordinates of "correct" points that lie on the polynomial that encodes the secret. Thus, if freshly captured feature set is close to the key feature set, then one can identify a large majority of these "correct" points. Any discrepancy between those feature sets will introduce a certain amount of error. Provided that there is sufficient overlap, however, this noise may be removed by means of a Reed-Solomon decoding algorithm. Consequently, the polynomial that encodes the secret can be successfully reconstructed

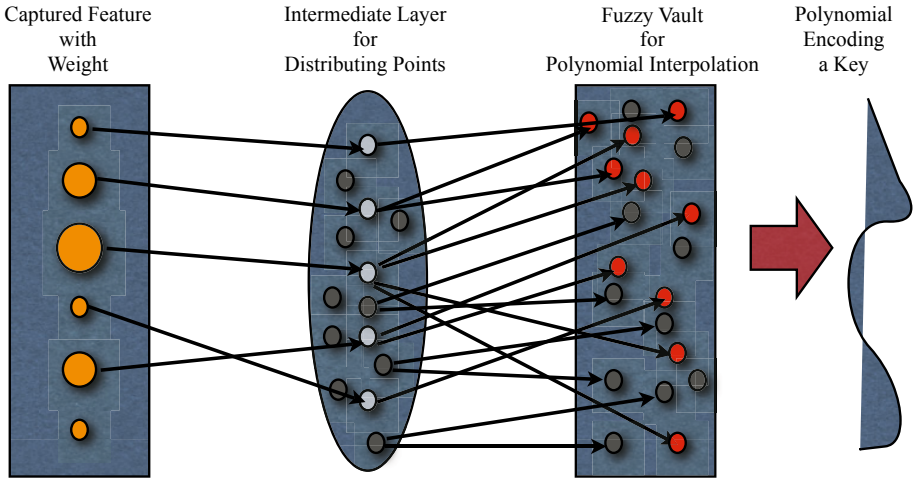

Fig. 1. Fuzzy Vault with Weighted Features

by one who has a "similar" feature set with that in the fuzzy vault construction. For more details, refer to [5].

3 Fuzzy Face Vault Scheme

As noticed in the previous section, the original fuzzy vault can neither be locked nor be unlocked by a weighted feature set. This is because irrespective of its importance of a certain feature it can hold only one share of a secret value. In this section, we show how to build a fuzzy vault scheme with weighted features.

To reflect the level of importance of individual features from feature set, we introduce another layer between captured feature set and points in the polynomial to be interpolated. In the original fuzzy vault, closest points to the captured feature set are directly chosen to reconstruct the polynomial that encodes the secret key. The intermediate layer of our scheme includes genuine weight values of the registered face image and counterfeit weight values as chaffs. In the intermediate layer, features with high weight values will give more information of points on the polynomial than ones with low eight values. This can be achieved by composing the fuzzy vault with points in the following way:

$$(h(f_1||0), f(h(f_1||0))), (h(f_1||1), f(h(f_1||1))), \ldots (h(f_1||m_1), f(h(f_1||m_1))),$$

$$(h(f_2||0), f(h(f_2||0))), (h(f_2||1), f(h(f_2||1))), \ldots (h(f_2||m_2), f(h(f_2||m_2))),$$

$$\ldots$$

$$(h(f_N||0), f(h(f_N||0))), (h(f_N||1), f(h(f_N||1))), \ldots (h(f_N||m_N), f(h(f_N||m_N))),$$

where f_i is a feature, m_i is an integral weight of a feature f_i, h() is oneway and collision free hash function such as SHA-1, f() is the polynomial that encodes

the secret key and finally || represents concatenation. That is, if more significant feature is found, then more points on the polynomial are obtained. This contrasts to the original fuzzy vault scheme, because this reveals only one point on the polynomial for one feature:

$$(f_1, f(f_1)), (f_2, f(f_2)), ...(f_N, f(f_N)).$$

Because given a face image from the same user, classifiers such as PCA and LDA usually give roughly-the-same dominant features, one has high probability that obtain many points on the curve and thus, one is prone to restore the stored secret key from the polynomial.

Followings is our fuzzy vault construction algorithm, where all parameters regarding security are the same as those in [5].

Public parameters: A field $\mathcal{F}$, a Reed-Solomon decoding algorithms RSdecode.
Input: Papameters k, t and r such that $k \leq t \leq r \leq q$. A secret $\kappa \in \mathcal{F}^k$. A feature set $F = \{f_i\}_{i=1}^{t}$, where $f_i \in \mathcal{F}$.
Output: A set R of numbers $\in \mathcal{F}$ and a set S of points $\{(x_i, y_i)\}_{i=1}^{r}$ such that $x_i, y_i \in \mathcal{F}$.
Algorithm LOCK

$X, R, S \leftarrow \emptyset$;
$p \leftarrow \kappa$;
`for` $i = t+1$ `to` r `do /* Chaffing */`
  $R \leftarrow R \bigcup r$, where $r \in \mathcal{F}$ and randomly chosen.
  $x_i \leftarrow r$;
  Choose randomly m, where $1 \leq m \leq \text{weight}_{\max}$;
  `for` $j = 1$ `to` m `do`
    $y_j \leftarrow \mathcal{F} - \{f(h(x_i||j)\}$;
    $S \leftarrow S \bigcup (x_i, y_j)$;
`for` $i = 1$ `to` t `do /* Inserting Genuine Features */`
  $R \leftarrow R \bigcup f_i$;
  $x_i \leftarrow f_i$;
  $m \leftarrow \text{weight}_{x_i}$;
  `for` $j = 1$ `to` m `do`
    $y_j \leftarrow \{f(h(x_i||j))\}$;
    $S \leftarrow S \bigcup (x_i, y_j)$;

Resulting two sets (R, S) are the fuzzy vault with weighted features. The set R does only have genuine features and a number of chaffs, where the chaffs are not points on the curve but single noisy numbers. The second set S has points on the curve f, but it also has chaffing points that disturbs an attacker. The set R plays a role of the intermediate layer, and thus, a genuine feature in the set maps into multiple points in the set S. Naturally, chaffing numbers in R do have also multiple points in the set S. By doing this, we achieved both the same level of security of original fuzzy vault and the applicable characteristic of weighted features.

To unlock our fuzzy vault, following unlock algorithm will be used.

Public parameters: A field $\mathcal{F}$, a Reed-Solomon decoding algorithms RSdecode.
Input: Papameters k, t and r such that $k \leq t \leq r \leq q$ and two sets (R, S).
Output: A value $\kappa' \in \mathcal{F}^k \bigcup' null'$.
Algorithm UNLOCK

$Q \leftarrow \emptyset$;
`for` $i = 1$ `to` t `do`
  $x_i \xleftarrow{(b_i, o)} R$;
  `for` $j = 1$ `to` m_{x_i} `do`
    $y_j \leftarrow f(h(x_i||j))$
    $Q \leftarrow Q \bigcup (x_i, y_j)$
$\kappa' \leftarrow$ RSdecode(k, Q);
`output` κ';

Here, the unlock algorithm finds firstly closest numbers from the set R, from which it can derive multiple points on the curve if the found number is significant. More important the feature it finds, more points on the secret curve will be revealed. Errors from mistakenly capturing odd numbers can be recovered with Reed-Solomon decoder if the number of errors is not so big.

4 Cost Evaluation

The cost to construct and maintain our fuzzy face vault is small in terms of computation, because only added operation is evaluation of one way hash function. However, in view of storage, our scheme requires several times bigger memory than the original fuzzy vault framework because intermediate layer is introduced and also more than one points from one feature are built. However, the size of memory is feasible in most applications because the fuzzy vault itself will be stored usually in the server. Even though it is to be stored in devices with limited memory such as smart cards, by reducing dimension of classifier without sacrificing much security, we can make it fit to those kind of devices.

5 Conclusion

In this paper, we presented a method to incorporate a biometric scheme with weighted features into the fuzzy vault scheme for cancelable biometrics. We specify a method to implement the framework using well-known face authentication schemes such as PCA and LDA. Here, the fuzzy face vault fortunately does not involve in such problems like pre-alignment in fuzzy finger vault, which is an obstacle to practical implementation of fuzzy finger vault systems.

In other biometrics schemes that are heavily depending upon weights of extracted features, our scheme can be a guide to construct fuzzy vault in efficient and secure manner.

References

1. Shamir, A.: How to Share a Secret, Commun. of the ACM 22, 612–613 (1979)
2. Davida, G.I., Frankel, Y., Matt, B.J.: On enabling secure applications through off-line biometric identification. In: IEEE Symposium on Privacy and Security (1998)
3. Davida, G.I., Frankel, Y., Matt, B.J.: On the relation of error correction and cryptography to an offline biometric based identification scheme. In: Workshop on Coding and Cryptography (1999)
4. Juels, A., Wattenberg, M.: A fuzzy commitment scheme. In: 6th ACM Conference on Computer and Communication Security, pp. 28–36 (1999)
5. Juel, A., Wattenberg, M.: A fuzzy vault scheme. In: IEEE International Symposium on Information Theory (2002)
6. Clancy, T.C., Kiyavash, N., Lin, D.J.: Secure Smartcard-Based Fingerprint Authentication. In: ACM SIGMM 2003 Multimedia, Biometrics Methods and Applications Workshop, pp. 45–52 (2003)
7. Uludag, U., Jain, A.: Fuzzy fingerprint vault. In: Workshop: Biometrics: Challenges Arising from Theory to Practice, pp. 13–16 (2004)