Secure Fuzzy Vault Based Fingerprint Verification System

Shenglin Yang
UCLA Dept of EE
Los Angeles, CA 90095
+1-310-267-4940
shengliny@ee.ucla.edu

Ingrid M. Verbauwhede
UCLA Dept of EE & K.U.Leuven
Los Angeles, CA 90095
+1-310-794-5209
ingrid@ee.ucla.edu

***Abstract*--This paper describes a secure fingerprint verification system based on the fuzzy vault scheme, where the sensitive biometric template is not stored, but a transformed version. We propose an adaptive alignment technique to reach the most reliable reference point, and a methodology to construct a set of rotation and shifting invariant features, acting as the lock set for the fuzzy vault. We investigate the parameters of the fuzzy vault and the number of the templates needed to obtain a reliable reference point, such that a high unlock complexity for attackers with an acceptable unlock rate for the legal users is achieved.**

I. INTRODUCTION

The authentication system based on biometric information offers greater security and convenience than the traditional methods of personal recognition. Along with the rapid growing of this emerging technology, the system performance, such as accuracy and speed, is continuously improved. One of the most significant disadvantages of all the biometric recognition systems is that the biometric key cannot be easily recalled. Therefore storing the biometric template securely is becoming extremely important. One possible approach is to encrypt the template using a secret key before storing it. As soon as the input signal comes, the matcher decrypts the template and performs the comparison. However, some dedicated attacks can still extract the secure key, and in turn, the template by tracking the revealed information from the physical implementation, such as variations in time, power consumption and electromagnetic radiation. These types of attacks are called Side Channel Attacks (SCA), among which the differential power analysis (DPA) is the most powerful one. It relies on statistical analysis and error correction to extract information from the power consumption that is correlated to secret data [1]. One solution to this problem is to store a noninvertible transformed version, for instance a hash, of the template on the embedded device, and the comparison is performed in the transformed space. One main property of a cryptographic random hash function is that the output hush value will not give any information about even part of the input [2]. Therefore, the similarity in the input will not reflect in the output hash value. However, for most biometrics, the exactness for different captures is usually not available, and the match algorithms are normally based on the similarity. To address this problem, we adopt the idea of fuzzy vault scheme [3] to conduct the fingerprint authentication.

This paper is organized as following: section II briefly reviews some related work about the secure authentication methods as well as the fingerprint matching techniques. Section III presents the basic idea and the implementation of the fuzzy vault scheme. Section IV discusses the strategy used to align the input fingerprint images to make the system automatic and adaptive. Section V shows some experimental results. And finally Section VI draws a conclusion.

II. RELATED WORK

There have been many research efforts aiming at the fingerprint user identification. Recently, a novel cryptographic construction called fuzzy commitment scheme has been proposed and employed in the field of biometric authentication.

A. Fingerprint Fuzzy Vault

The fuzzy commitment scheme is first proposed in [4] to integrate well-known error-control coding and cryptographic techniques to construct a novel type of cryptographic system. Instead of an exact, unique decryption key, a reasonable close witness can be accepted to decrypt the commitment. This characteristic makes it possible for protecting the biometric data using traditional cryptographic techniques. However, since the fuzzy vault used in this scheme does not have the property of order invariance, any elements missing or adding will result in the failure of matching. To overcome this problem, [3] proposed a new architecture, which possesses the advantage of order-invariance. At the same time, the authors suggested that one of the important applications of the fuzzy commitment is to secure biometric systems. Following this direction, [5] employed the fuzzy vault scheme on a secure smartcard system, where the fingerprint authentication is used to protect the private key. In the biometric cryptosystem, the secret information is hidden as coefficients in a polynomial, which acts as the frame of the fuzzy commitment. The fingerprint vault construction is based on the assumption that the fingerprint features are extracted and well aligned in a black box. Our work will address the alignment problem in a systematic way to make the authentication system automatic and adaptive.

This work is sponsored by the NSF, account no CCR-0310527 and UC MICRO.

0-7803-8622-1/04/$20.00 ©2004 IEEE

B. Fingerprint Matching Algorithm

For modern embedded fingerprint recognition systems, the matching algorithm is usually based on the minutiae feature. The reason is, on the one hand, the minutiae of the fingerprint are widely believed the most discriminating and reliable feature, and on the other hand, the template size of the minutiae is much smaller and the processing speed is higher than that of graph-based matching. These characteristics are very important for saving memory and energy on the embedded devices. Reference [6] uses the local structure of the minutiae to describe the characteristics of the minutiae set. This approach has higher processing speed, and is robust to rotation and partial prints. However, the local structure usually has less distinct features because it only represents parts of the whole minutiae set. Alignment-based matching algorithms take use of the shape of the ridge connected to the minutiae [7]. This might improve the system accuracy, but results in a larger template size. Some other researches combine the local and global structures [8]. The local structure is used to find the correspondence of two minutiae sets and increase the reliability of the global matching, while the global structure reliably determines the uniqueness of a fingerprint. In our work, the local-global information integration is employed to perform the fingerprint minutiae alignment before the features are ported into the fuzzy vault.

To address the problem of SCA, [9] divides the fingerprint match engine into two parts. Only the relatively small secure part containing the sensitive biometric information is executed on a specialized DPA-proof logic block, which does not reveal the power consumption variations during operations. In spite of the careful division, the secure part still consumes large numbers of area and energy due to the special design of the DPA-proof logic as well as the frequent data exchange between the embedded processor and the DPA-proof block. In this work we replace the biometric template stored in the DPA-proof block with a randomly generated bit stream and only a one-time comparison is needed for each attempt of the verification algorithm.

III. Fuzzy Vault Scheme

A. The basic idea of fuzzy vault

Fuzzy vault scheme is a simple and novel cryptographic construction. Suppose we have a secret, which we want to share with some specific persons, but do not want to post it indiscriminately on some untrusted places, such as a public website. One approach is to compile a set of elements A with the secret and publish it in an encrypted form. To extract the secret information, one needs to have an unlock set B, which is close to A, to unlock the vault. This vault is a form of error-tolerant cryptographic algorithm and proved very useful in many circumstances, such as fuzzy human factor based authentication systems, where exactness of the unlock key is usually unavailable. Several examples are presented in [3] including the biometric applications, which we plan to investigate in this paper.

Follow the idea in [5], the fuzzy encrypt key consists of a set of elements $lock_i$, $i = 1,2,\dots,n$, where n is the size of lock set. The fuzzy vault contains all pairs ($lock_i, p(lock_i)$), where $p(x)$ is a known polynomial. Besides these "true" pairs which represent the characteristics of the lock set, large number of impostor pairs ($impostor_j$, $p'(impostor_j)$), where $j = 1,2,\dots,r$ and $p'(x) \neq p(x)$, are also added to the fuzzy vault. $p'(x)$ is a random function. For a legal user, a set of elements $unlock_i$, which is reasonably close to $lock_i$, is available. Also we assume that the numbers of lock set and unlock set are larger than the degree of the polynomial, d. Therefore, the user can unlock this fuzzy vault by trying to reconstruct the polynomial using the unlock set. If the overlap between the lock set and the unlock set satisfies the polynomial reconstruction condition, the verification process successes. From an attacker's point of view, ideally, the unlock set is a uniformly distributed random set. To successfully attack the fuzzy vault without any knowledge about the lock set, the attacker has to first separate the "true" pairs from the "impostor" pairs by brute force trials. Since the number of the impostor pairs is far larger than that of the true pairs, the separation operation is formidably difficult.

B. Fingerprint Fuzzy Vault

As we mentioned before the security requirement of the biometric template storage is very strict since the biometric data are usually irreplaceable and the lost of these precious information might lead to serious security problems. To address this issue, instead of storing the biometric template, we store a machine-generated bit stream as the secret. The way we present the secret is to hide it as the coefficients for a polynomial, $p(x)$, which is used as the frame to construct the fuzzy vault.

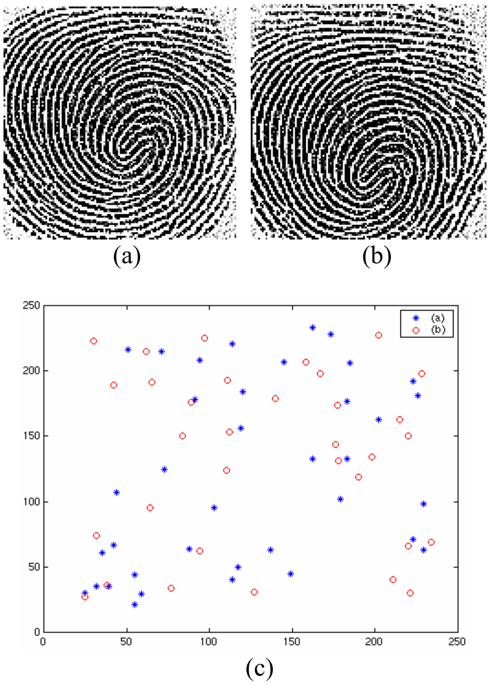
Fingerprint verification is usually based on the pattern matching of the feature extracted from the fingerprint images. Here we describe the minutiae feature of a fingerprint image as α_i, $i = 1,2,\dots,n$, where n is the total number of the feature points. Thus the pairs ($\alpha_i, p(\alpha_i)$) form the lock set of the fingerprint fuzzy vault. For the impostor pairs, we randomly choose β_j and η_j, $j = 1,2,\dots,r$, where $\eta_j \neq p(\beta_j)$. Note that the distance between any β and any α must be greater than a minimum distance $d_{\min}$. The value of $d_{\min}$ depends on the characteristic of the feature points as well as the performance requirement. We will discuss this in section V. There exits a one-to-one projection between the set $X = \{\alpha_i, \beta_j\}$ to the set $Y = \{p(\alpha_i), \eta_j\}$. During the unlocking procedure, the user's fingerprint is captured and processed to get the minutiae feature set $\{\alpha_i'\}$. Since two biometric readings are rarely exactly the same, even though they are likely to be close, $\{\alpha_i'\}$ and $\{\alpha_i\}$ are usually not identical. To perform the unlocking, for each α_i', we search in the whole fuzzy vault to reach the closest element $\chi_k \in \mathrm{X}$ and it's corresponding $\gamma_k \in \mathrm{Y}$. Thus, the set (χ_k, γ_k), $k = 1,2,\dots,m$, is the unlock set generated as the key to the fuzzy vault, where m is the number of features extracted from the user's input fingerprint.

Now the verification is equivalent to the problem below: Given m pairs of points $(\chi_i, \gamma_i) \in F \times F$, there exists a polynomial p of degree at most d such that for all but k values of (χ_i, γ_i), $\gamma_i = p(\chi_i)$, where $2k + d < m$. According to the Berlekamp-Welch error correcting code theory, this problem can be solved by finding the solution for a linear constraint system $N(\chi_i) = \gamma_i * W(\chi_i)$, $i = 1,2,...,m$, where $\deg(W) \le k$ and $\deg(K) \le d$. After all the unknowns are calculated out, $p = N / W$ is the result polynomial [10].

In order to act as the lock set, the features extracted from the fingerprint images need to satisfy two conditions: (1) distinguishable from each other so that no more than one feature results in a same pair in the lock set; (2) the difference between several scans of print from a same finger is acceptable small. In the following sections, we will discuss the selection of the feature as well as the automatic feature alignment, which will be proven very important for automatic authentication systems.

IV. Feature Selection

Fingerprint minutiae are defined as the endings of one ridge and the crossings of two ridges. The most straightforward way to construct the lock set is to use the (x, y) coordinates of each minutia [5]. However, Fig. 1 shows that the effect of the fingerprint shifting and rotation on the position of the minutiae features is not ignorable and will result in difficulty of matching. Therefore, this feature depends on the position and angle of the input fingerprints. In order to address this problem, we propose a new feature $\{r, \theta\}$, where r is the distance between one minutia and a specific reference point, and θ is the associated direction as shown in Fig. 2. Both r and θ are represented by 8 bits, and the concatenation of these two values, $(r << 8) + \theta$, is an element of the finite field $GF(2^{16})$. If the specific reference point is correctly chosen, the proposed feature will be independent of the shifting and rotation of the input images. Fig. 3 shows four aligned sets of minutiae from a same finger.


(a)

(b)

(c)

Fig. 1. The effect of shifting and rotation on the feature position. (a) and (b) are two prints from a same finger; (c) is the positions of the features.

In order to find the reference point, we adopt the methodology proposed in [11]. A simplified rotation and translation invariant local feature is constructed as:

$$M = (d_1, d_2, \theta_1, \theta_2, \varphi_1, \varphi_2)$$

Fig. 2 indicates the details of this local feature. Assume $M_A(i)$ and $M_B(j)$ are the local feature vectors of the i^{th} minutia of the fingerprint A and the j^{th} minutia of the fingerprint B, respectively, the similarity level of these two minutiae can be defined as:

$$sl(i,j) = \begin{cases} 1 - \dfrac{|M_A(i) - M_B(j)|_W}{A}, if |M_A(i) - M_B(j)|_W < A(W) \\ 0, otherwise \end{cases}$$

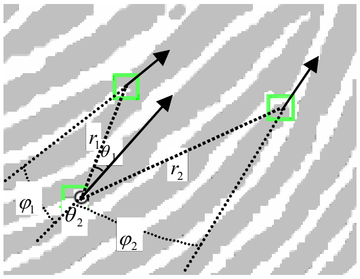


Fig. 2. Concept of the proposed feature

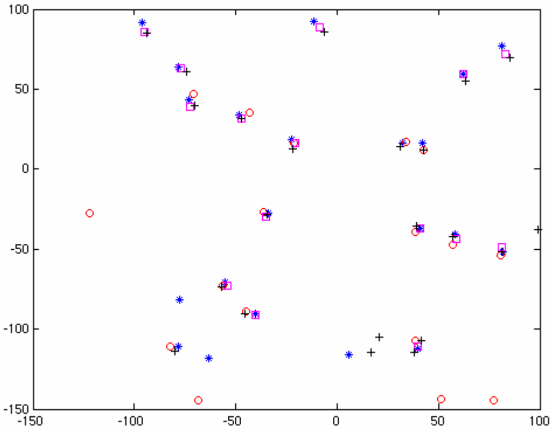


Fig. 3. Overlap of four minutiae feature sets aligned based on the well-selected reference point.

$$i = 1,2...p \quad j = 1,2...q$$

where p and q are the total numbers of minutiae in fingerprint A and B, respectively. $|M_A(i) - M_B(j)|_W$ is the weighed distance between two local feature vectors. $A(W)$ is a fixed threshold, which is related to the weight vector W. In this paper, we set $W = (1,1,8,8,8,8)$ and $A(W) = 55$. By thoroughly searching $sl(i,j)$, minutiae pairs $(M_A(i), M_B(j))$ can be ordered according to the associated similarity level. Intuitively, the pair with largest similarity value can be taken as the reference pair. To find the reliable reference pair, we use three fingerprints (A , B , C) from one finger as the templates and the similarity metric we use is $sl_{AB}(i,j) + sl_{BC}(j,k)$. The largest value indicates the most reliable minutia in three of these prints. Fig. 4 presents the distribution of the similarity levels for all possible combinations of the minutiae in three fingerprints.

After finding out the most reliable reference point, we align the rest of the minutiae in polar system and also store the local structure of the reference minutia. Then the next step is to figure out the refer point in the input fingerprint based on the stored local structure and convert the rest of the minutiae in a polar system. The polar coordinates of the input fingerprint minutiae is what we use as the unlock set in our fingerprint fuzzy vault.

V. Result

We get ten prints for each finger, among which three are randomly chosen to be the templates for reaching the reliable reference minutia. However, there are cases that from three templates, the reliable pair cannot be successfully achieved. In an automatic system, this failure needs to be detected by introducing a threshold to limit the minimum similarity for being the reference feature point. If the sum-up similarity level $sl_{AB}(i,j) + sl_{BC}(j,k)$ is less than the threshold, it shows that the reference point is not reliable. In this case, more templates are needed to perform the selection. Fig. 5 shows the number of templates needed experimentally. From the result we find that four templates during enrollment phase can guarantee to achieve the reliable reference point with a possibility higher than 99%.

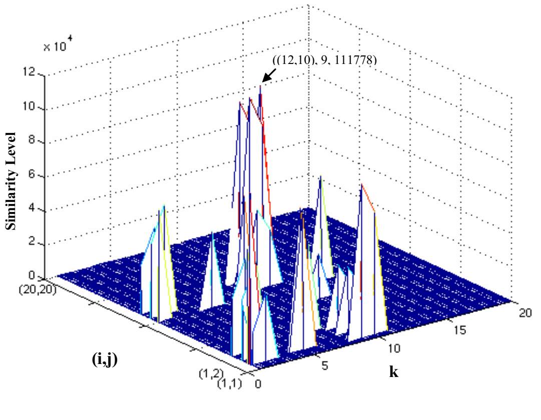


Fig. 4. Distribution of the similarity for three fingerprints.

The selection of the fuzzy vault parameters is very important for the verification performance. First we investigate the effect of the degree of the polynomial, d. According to the Berlekamp-Welch error correcting code theory, the condition inequation is $2k + d < m$. In other words, to successfully decode the fuzzy vault, the number of the impostor points must satisfy: $k < (m - d)/2$, where m is the total number of the input minutiae points. Intuitively, the maximum acceptable impostor point number should depend on the total unlock set size m. For fingerprints with larger number of minutiae, the degree of the underlying polynomial needs to be larger, so that the maximum value of k increases accordingly. By introducing this self-adaptive scheme, the fuzzy vault will suit for fingerprints with different size of feature sets. Fig. 6 shows the relationship between the unlocking complexities of the fuzzy vault and the degree of the polynomial, where $m = 30$ for a typical case. From this figure, we can find that higher degree polynomial provides higher complexity, in turn, higher level of security. However, from another point of view, for higher degree polynomial, the maximum acceptable impostor point size becomes smaller, which will increase the False Reject Rate (FRR) for the verification system. Therefore a suitable polynomial degree is needed to achieve the desirable tread-off between the security and the matching accuracy. Experiments show that for $m / d = 3$, the successful unlocking rate is about 83%, which is acceptable in most of the realistic implementations. In this paper, we choose $d = \lfloor M/3 \rfloor$.

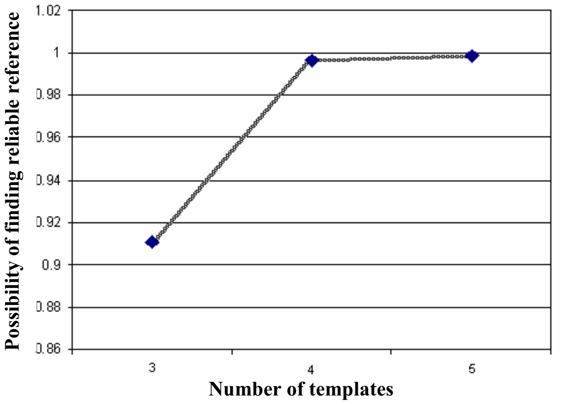


Fig. 5. Relationship between the possibility of finding reliable reference and the number of templates

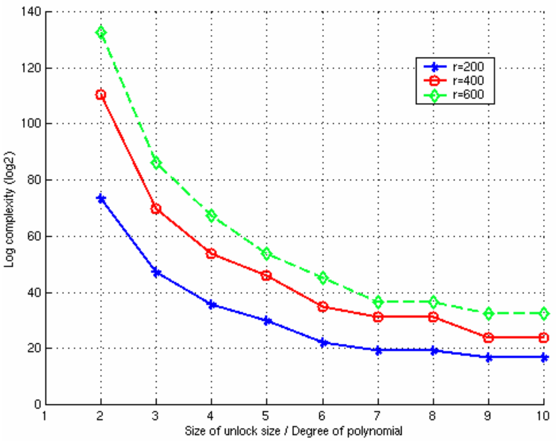


Fig. 6. The unlock complexity varies according to the degree of polynomial for different size of impostor point.

The experiments also show that the minimum distance between any impostor points and any lock set points is another important parameter, which affects the performance. When we randomly generate the impostor points, we need to make sure the minimum distance is satisfied. The minimum distance needs to be at least twice as large as the acceptable distance of a minutia position between different scans. Fig. 7 shows the relationship between the minimum distance and the matching accuracy.

Besides the minimum distance, the number of the impostor points also needs to be taken into consideration during the fuzzy vault constructing. If the number of the impostor points is set too small, according to the unlocking algorithm, the input features are more likely to be closer to the lock set points, which will result in higher False Accept Rate (FAR). Similarly, if the size of impostor points is too big, a feature point is more likely to be classified as an impostor point. This will lead to higher False Reject Rate (FRR).

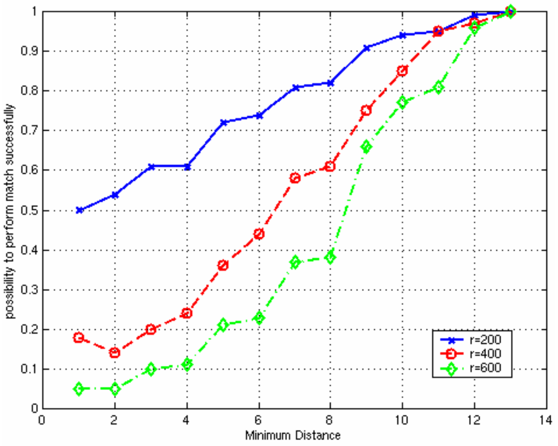


Fig. 7. The relationship between the possibility of successful matching and the minimum distance of impostor point for different impostor size.

VI. Conclusion

We construct our database by 10 prints per finger from 10 different fingers, forming a total 100 fingerprint images. Employing the automatic fuzzy vault construction and unlocking algorithms with the following parameters: impostor points size $r = 200$, polynomial degree $d = \lfloor M/3 \rfloor$, and minimum distance $d_{\min} = 13$, the successful unlocking rate is about 83%. The error rate is acceptable, while relatively higher compared to the traditional fingerprint verification algorithm [2]. This degradation can be explained by the characteristic of the underlying error-correct coding scheme we adopted for the fuzzy vault unlocking since the condition for the Berlekamp-Welch error correcting code theory is more strict compared to the existing minutiae-based fingerprint verification algorithm.

References

[1] Kocher, P., Jaffe, J., and Jun, B., Differential power analysis, Proceeding of Advances in Cryptology – Crypto'99. 19th Annual International Cryptology Conference. 1999, pp.388-97. Berlin, Germany.

[2] Anderson, R.J., Security Engineering, A Guide to Building Dependable Distributed Systems, John Wiley & Sons, 2001.

[3] Juels, A. and Sudan, M., A fuzzy vault scheme, Proceedings 2002 IEEE International Symposium on Information Theory, 2002, pp.408. Piscataway, NJ.

[4] Juels, A. and Wattenberg, M., A fuzzy commitment scheme. 6th ACM Conference on Computer and Communications Security, 1999, pp.28-36, New York, NY.

[5] Clancy, T.C., Kiyavash, N., and Lin, D.J., Secure smartcard-based fingerprint authentication, ACM Workshop on Biometrics: Methods and Applications, Nov. 2003, pp. 45-52, Berkeley, CA.

[6] Hrechak, AK and McHugh, JA. Automated fingerprint recognition using structural matching, Pattern Recognition, vol.23, no.8, 1990, pp.893-904. UK.

[7] Jain, A., Lin, H., and Bolle, R., On-line fingerprint verification, IEEE Transactions on Pattern Analysis and Machine Intelligence, vol.19, no.4, April 1997, pp.302-14.

[8] Jiang, X. and Yau, W., Fingerprint minutiae matching based on the local and global structures, Proceedings 15th International Conference on Pattern Recognition. 2000, pp.1038-41 vol.2. Los Alamitos, CA.

[9] Yang, S. and Verbauwhede, I., A secure fingerprint matching technique, ACM Workshop on Biometrics: Methods and Applications, Nov. 2003. pp. 89-94, Berkeley, CA.

[10] Gemmell, P. and Sudan, M., Highly resilient correctors for polynomials, Information Processing Letters, vol.43, no.4, Sept. 1992, pp.169-74, Netherlands.

[11] Yang, S., Sakiyama, K. and Verbauwhede, I., A Secure and Efficient Fingerprint Verification System for Embedded Systems, 37th Asilomar Conference on Signal, Systems, and Computers, Nov. 2003, pp. 2058-2062, Pacific Grove, CA.