# AUTOMATIC SECURE FINGERPRINT VERIFICATION SYSTEM BASED ON FUZZY VAULT SCHEME

*Shenglin Yang and Ingrid Verbauwhede*

Department of EE, UCLA, Los Angeles, CA 90095

**ABSTRACT**

In this paper, we construct an automatic secure fingerprint verification system based on the fuzzy vault scheme to address a major security hole currently existing in most biometric authentication systems. The construction of the fuzzy vault during the enrollment phase is automated by aligning the most reliable reference points between different templates, based on which the converted features are used to form the lock set. The size of the fuzzy vault, the degree of the underlying polynomial, as well as the number of templates needed for reaching the reliable reference point are investigated. This results in a high unlocking complexity for attackers with an acceptable unlocking accuracy for the legal users.

## 1. INTRODUCTION

An authentication system based on biometric information offers greater security and convenience than the traditional methods of personal verification. Along with the rapid growth of this emerging technology, the system performance, such as accuracy and speed, is continuously improved. The biometric verification is based on the comparison of the features extracted from an input and a template fingerprint images. The storage of the reference template is a key factor in the total system security. Thus it is essential to protect the template from possible attacks. One approach is to encrypt the template using a secret key before storing it. When the input signal comes, the matcher decrypts the template and then performs the comparison. However, this defeats the purpose of most biometric devices: one tries to be independent of pin codes or secrets entered by the user. Some dedicated attacks still can extract the secure key, and in turn, the template by tracking the revealed information from the physical implementation. An example is Side Channel Attacks (SCA) [1]. A clean 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 hash 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 fingerprint biometrics, the exactness for different captures is not available, and the match algorithms are normally based on the similarity. To address this problem, we adopt the idea of the fuzzy vault scheme [3] to conduct the biometric authentication. This paper is organized as following: section 2 briefly reviews some related work about secure authentication methods. Section 3 presents the basic idea and the implementation of the fuzzy vault scheme. Section 4 discusses the strategies for the feature extraction as well as the alignment of the input fingerprint images to make the system automatic and adaptive. Section 5 shows some experimental results and analysis. Finally section 6 draws a conclusion.

## 2. RELATED WORK

Fingerprint authentication is a very attractive technique to replace traditional passwords or pin codes. The main challenge for embedded versions is to provide a secure storage of the reference template. Embedded devices are vulnerable to eavesdropping and attacks. Thus alternative protection mechanisms need to be investigated. Recently, a novel cryptographic technique called the fuzzy commitment scheme has been proposed for biometric authentication [4]. The scheme integrates well-known error-control coding methods 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 added will result in a failure of the matching. To overcome this problem, [3] proposed a new version, 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 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 aligned in a black box. Our work will address the alignment problem in a systematic way to make the authentication system automatic and adaptive. Instead of any formats of the biometric template, we randomly generate a bit stream as the secret and only a one-time comparison is needed for each attempt of the verification algorithm.

## 3. FUZZY VAULT SCHEME

In a fuzzy fault scheme, similar to a secret key strategy, a set of elements $A$ is compiled with a secret and published in an encrypted form. At the same time, a large number of impostor elements are added to conceal the genuine information. In order to extract the secret, one must have another 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 security systems, where the exactness of the lock and unlock keys is usually unavailable.

We adopt fingerprint to perform the user authentication. In order to address the security problem posed by the leakage of the stored biometric information, instead of templates, we store a machine-generated bit stream as the secret. The way we present the secret is to hide it as coefficients for a polynomial, $p(x)$. Then the polynomial is used as the underlying frame to construct the fuzzy vault. Fingerprint verification is usually based on the pattern matching of the feature sets extracted from the fingerprint images. Here we describe the feature of a fingerprint image as $\alpha_i$, $i=1,2,...,n$, where $n$ is the total number of 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 $\beta_j$ and $\eta_j$, $j=1,2,...,r$, where $\eta_j \neq p(\beta_j)$ and $r$ is the size of the impostor set. It is noticed that the distance between any $\beta$ and any $\alpha$ must be greater than a minimum distance $d_{\min}$ to guarantee that the system is tolerant to variation less than $d_{\min}/2$ in distance. The selection of the minimum distance depends on the characteristic of the feature point as well as the performance requirement.

There exits a one-to-one projection from set $X=\{\alpha_i, \beta_j\}$ to set $Y=\{p(\alpha_i), \eta_j\}$. During the unlocking procedure, a user's fingerprint is captured and processed to get the feature set $\alpha'$. For each $\alpha'_k$, we search through all elements in the fuzzy vault to reach the closest element $\chi_k \in \mathrm{X}$ and its corresponding $\gamma_k \in \mathrm{Y}$. Thus, the set $(\chi_k, \gamma_k)$, $k=1,2,...,m$, 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. We assume that both the numbers of the lock set and the unlock set are larger than the degree of the polynomial $p(x)$, $d$. 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 is big enough to satisfy the polynomial reconstruction condition, the verification process is successful. Ideally, from security point of view, the unlock set is a uniformly distributed random set. To successfully attack the fuzzy vault without any knowledge about the lock set, one has to first separate the genuine pairs from the impostor pairs by brute force trials. Since the number of the impostor pairs is far larger than the number of the genuine pairs, the separation operation is quite difficult.

Now the verification is equivalent to the problem below: Given $m$ pairs of points $(\chi_i, \gamma_i)$, $i=1,2,...,m$, such that there exists a polynomial $p(x)$ of degree at most $d$ such that for all but $k$ values of $(\chi_i, \gamma_i)$, $\gamma_i = p(\chi_i)$. According to the Berlekamp-Welch error correcting codes theory, if $2k+d<m$, 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 $\deg(W)\le k$. After the $2k+d+1$ unknowns are calculated, $p(x)=N/W$ is the result polynomial [10].

## 4. FEATURE SELECTION

In order to construct the lock set, the features extracted from the fingerprint images need to satisfy these two conditions: (1) distinguishing from each other so that no more than one feature results in a same pair in the lock set; (2) the difference between the features obtained from several scans of fingerprint for a same finger is acceptably small. In the following sections, we will discuss the selection of the features as well as the automatic feature alignment.

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]. The size of the image obtained from the fingerprint sensor is $256\times256$ pixels. Therefore the coordinates for minutiae are $(x, y)\in F\times F$, where $F$ is a finite field $GF(2^{16})$. We found that the effect of shifting and rotation on the position of the minutiae features is not ignorable and will result in difficulty of matching between two fingerprints. In other words, this feature is not invariant to the position and angle of the input fingerprints. To solve this problem, we first try to find another set of features, which is robust against the rotation. Instead of putting the minutiae in the Cartesian coordinate system, we observe them in the Polar coordinate system. If the origin for the Polar coordinate system is correctly selected, the proposed feature will be independent of the rotation of the input images. In order to find the reference point to be the origin, we adopt the methodology proposed in [11]. A simplified rotation and translation invariant feature is constructed as:

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

Figure 1 indicates the details of the local feature, where $r$ is the distance between two minutiae, $\theta$ is the position angle, and $\varphi$ is the direction difference between a minutia and the origin. 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:

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

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

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. $T(W)$ 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 $T(W)=55$. By thoroughly searching $sl(i,j)$, minutiae pairs $(M_A(i), M_B(j))$ can be ordered

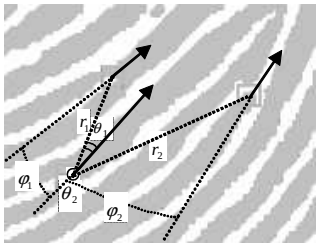


**Fig. 1. Concept of the proposed feature**

according to the associated similarity level. Intuitively, the pair with largest similarity level can be taken as the reference pair. To find a more 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. However, there are cases that from three fingerprint templates, the reliable pair cannot be successfully reached. This failure can be detected automatically 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 really reliable. In this case, more templates are needed to perform the selection. Figure 2 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%.

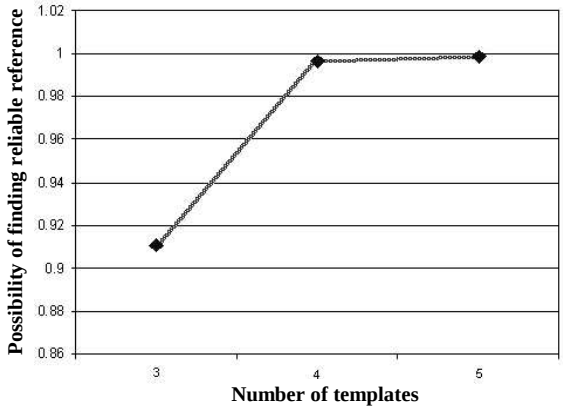


**Fig. 2. Relationship between the possibility of finding reliable reference and the number of templates**

After finding the most reliable reference point, we align the rest of the minutiae in one template fingerprint and also store the local structure of the reference minutia. Then the next step is to figure out the corresponding point in the input fingerprint based on the stored local structure and then convert the rest of the minutiae in a polar system. The polar coordinates of the input fingerprint minutiae are the unlock set used in our fingerprint fuzzy vault. The whole system works in the finite field $GF(2^{16})$. Since both r and $\theta$ in the coordinates $(r,\theta)$ are represented by 8 bits, the concatenation of these two values, $(r<<8)+\theta$, is an element of $GF(2^{16})$.

## 5. EXPERIMENTAL RESULT AND ANALYSIS

The selection of the fuzzy vault parameters is very important for the verification performance. First, the degree of the underlying polynomial, $d$, indicates the length of the machine generated secret. Considering that the Berlekamp-Welch error correcting codes theory condition inequation $2k+d<m$, for a successful decoding, the polynomial degree must satisfy: $d<m-2k$, where $m$ is the total number of the input minutiae points. Intuitively, the maximum acceptable number for "mistaken" points in the unlock set should vary along with the total unlock set size $m$. For fingerprints with larger number of minutiae, the maximum value of $k$ increases accordingly to maintain the same error tolerance capability. Meanwhile, the degree of the underlying polynomial can be made larger to increase the system security level. By introducing this self-adaptive scheme, the fuzzy vault will be suitable for fingerprints with a different number of feature points. Let $d=m/l$, $l=1,2,...,9$, Figure 3 shows the relationship between the unlocking complexities of the fuzzy vault and the degree of the polynomial, where $m=40$ for a typical case. From the figure, we can find that higher degree polynomial provides higher unlocking complexity, in turn, higher level of security. However, in case of a fixed number of minutiae, for a higher degree polynomial, the maximum acceptable number of "mistaken" points becomes smaller, which will increase the False Reject Rate (FRR) for the verification system.

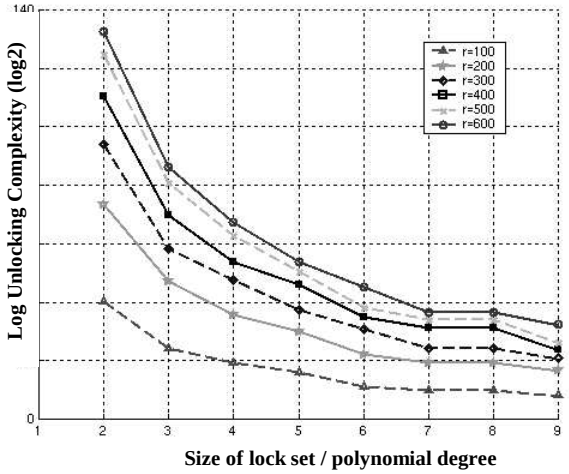


**Fig. 3. The unlock complexity varies according to the degree of polynomial for different number of impostor points "r".**

The number of the impostor points needs to be taken into consideration during the fuzzy vault construction. If the number of impostor points is set too small, according the unlocking algorithm, the input features are more likely to be closer to one of the lock set points even if they still have quite large distance, which will result in higher False Accept Rate (FAR). Figure 4 shows how the verification accuracy varies along with polynomial degrees for difference size of the impostor set.

From Figure 3 and Figure 4, we can see that an appropriate polynomial degree and impostor set size are needed to achieve the desirable trade off between system security and matching accuracy. To make the effect more clear, we introduce a new

metric to describe the performance of the designed system called Complexity-Accuracy Factor:

$$F = (ACC - TH_{ACC}) \times (UC - TH_{UC}),$$

where $ACC$ is the matching accuracy of the system, $TH_{ACC}$ is the minimum desirable matching accuracy, $UC$ is the fuzzy vault unlocking complexity, and $TH_{UC}$ is the minimum acceptable unlocking complexity required by the design criteria. This Complexity-Accuracy Factor provides developer a guideline to choose parameters for the fuzzy vault to satisfy the requirements of the design. Combining the previous results, Figure 5 shows how the polynomial degree and the impostor set size influence the Complexity-Accuracy Factor of the system, where we set $TH_{ACC} = 0.70$ and $TH_{UC} = 35$.

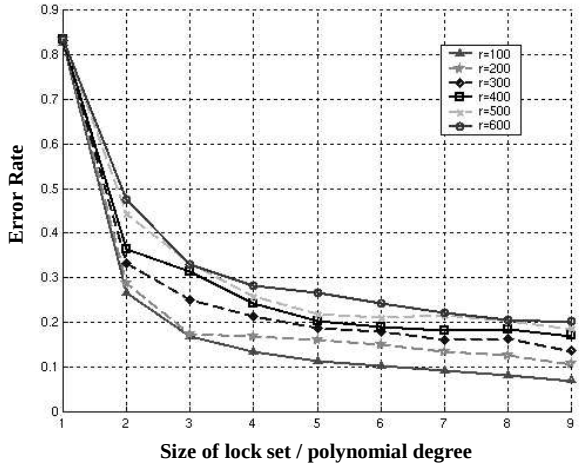


**Fig. 4. The verification accuracy varies according to the degree of polynomial for different number of impostor points.**

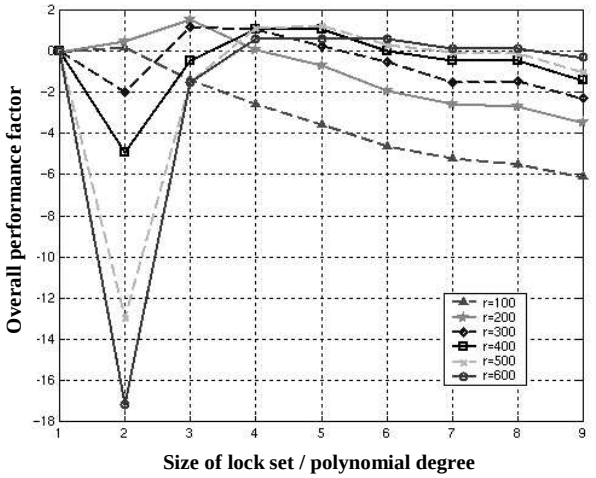


**Fig. 5. The influence of the polynomial degree and the chaff set size on the system performance**

## 6. CONCLUSION

Our database consists of 10 fingerprints per finger from 10 different fingers, forming a total 100 fingerprint images. Employing the automatic fuzzy vault construction methodology and the error-correct coding based unlocking algorithm with the following parameters: impostor set size $r = 200$, underlying 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, but relatively higher compare to most traditional fingerprint verification algorithms [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 codes theory, $k < (m-d)/2$, is more strict than other existing minutiae-based fingerprint verification algorithms. The big advantage is that a fuzzy vault scheme does not require storing sensitive information.

## 7. ACKNOWLEDGEMENT

The authors would like to acknowledge the funding of NSF account no CCR-0310527 and UC MICRO.

## 8. 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, A.K. and McHugh, J.A., "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.