15

Chaos-Based Biometrics Template Protection and Secure Authentication

Xiaomin Wang, Taihua Xu and Wenfang Zhang
School of Information Science and Technology, Southwest Jiaotong University
China

1. Introduction

With the increasing development of global economy and information technology, more and more fields require reliable identity authentication. And with information age characterized by digitalization and recessiveness of identity, a key problem to be solved is how to identify a person's identity accurately and ensure information security. In this regard, a variety of inherent human biometrics were gradually understood and studied, thus the development of biometric identification technology is considerable. The gradual yet profound application of biometric identification system today has improved security and creates much convenience to identity authentication. However, there are still some inherent problems that need to be solved. For instance, masquerade attack, difficulties to republish when the template is lost and a series of other potential threats. The existences of these threats have created a bottleneck, constraining further development of the biometric identification technology.

In this chapter, we will firstly give a review mainly on the theories and techniques of biometrics template protection, and then present a novel chaos-based biometrics template protection with secure authentication scheme. The proposed scheme is lightened by fuzzy extractor, yet includes two-layer error-correcting (one is BCH error-correcting code, the other is chaotic spread spectrum encryption) to achieve a good authentication performance of GAR=99.5% and FAR=0%. In addition, the functional features of proposed authentication scheme are: (1) do not need user to remember secret information such as password, or store them into physical media such as token or smart card; (2) no biometric template and any other secret information stored in server end; (3) the user's biometric template is cancellable; (4) user's registering information can be updated freely and easily. (5) with the help of user's inaccurate biometric template, secret information (user maybe knows or unknowns) can be accurately recovered. These interesting features push forward the proposed scheme having potential application in biometric-based authentication/identification systems.

1.1 Biometric and biometric identification systems

Traditional identity authentication methods are based on what is physically possessed such as ID cards and what can be mentally stored in the memory such as passwords and keys. The shortfalls of both are for instance ID cards can easily be lost or forged while passwords and keys can either be easily guessed or forgotten respectively. Short passwords are often easy for memory but easily guessed by others. On the other hand, long passwords (commonly known as keys) although cannot be easily guessed are prone to memory

problem. Key storage is therefore an issue and it is recommended that general long keys are stored in key cards and at the same time use short passwords to protect the Key Cards (Wang et al., 2006, Wang et al., 2007). Eventually, short passwords are still essential to identity authentication security.

Biometric (Tian, 2005) features inherited in person include two major categories which are person's physical characteristics and behavioural characteristics. Physiological characteristics are fingerprints, face, iris, palm prints, and voice to name but a few. Behavioural characteristics include gait, signature, keystrokes etc. These characteristics have attracted a large number of scholars who conducted extensive and thorough research on them. In order to perform the identification, an automatic technology is adopted to measure these features, and have them compared with data from a database template. This infers that identification and biometric identification technology is the solution to the certification.

Before the popularization and application of computers, biometrics was carried out manually mainly by artificial experts (e.g. American FBI for instance have large fingerprint experts). The development of productivity and popularity of information technology today have made biometrics to be automated using computers. The Automatic Fingerprint Identification System (AFIS) for example is one of the automated systems ever established. A typical AFIS includes an off-line register and an on-line identification process, as shown in Fig.1 (Li et al, 2009). The off-line register includes signal acquisition, feature extraction, template storage and other necessary steps. The on-line identification includes a signal acquisition, feature extraction, registration, template matching etc. Biometric identification system has two modes for identity authentication: authentication (1:1) and identification (1: N). Authentication mode test are "you the person you claimed", and identification mode test verifies "your identity information in the database and who you are". The two methods have large gap in aspects of their algorithm processing time complexity.

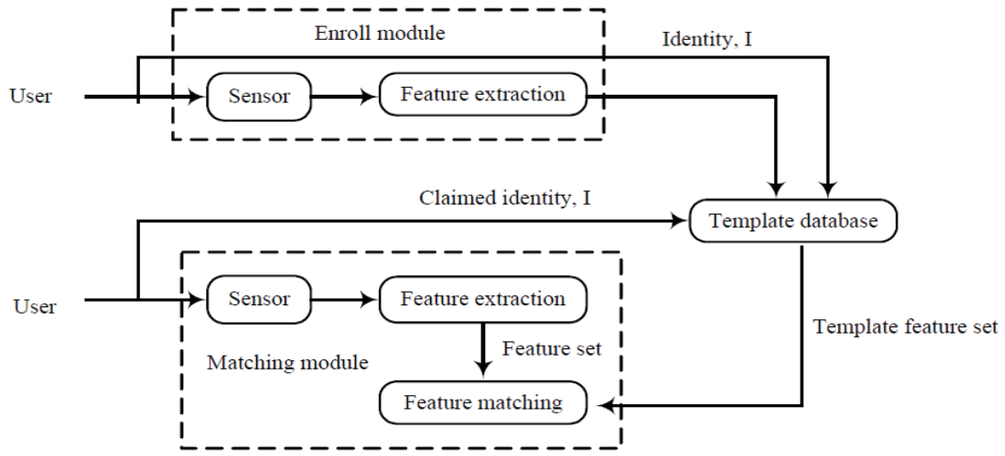


Fig. 1. Enroll model and matching module of biometric system (Li et al, 2009).

1.2 The defects of traditional biometric identification system

Traditional biometric identification system has increased in terms of recognition accuracy and speed. Yet, most traditional fingerprint identification systems adopt minutiae as their recognition features and the information of location where the direction of minutiae are stored for comparison in the form of pure data. The traditional system stores original

coordinates of minutiae and their value of direction, unfortunately, without any encryption. With the development of hardware attack and crack technology the whole biometrics identification system will be completely exposed to the scope of hacker attacks, threatening the security and privacy of user identity. Unlike passwords and keys that can be reset after their loss, the loss of biometric is permanent.

Cappelli et al. (2007) shows in a novel approach that the original fingerprint can be reconstructed automatically from standard minutiae-based templates. This may unlikely fool a human expert but is definitely possible to successfully attack even state-of-the-art automatic recognition systems, provided that one is able to present reconstructed images to the system. Thus there is the higher need for template security of biometric identification systems. Besides outside threats to template security, biometrics identification system is also facing a variety of other types of attacks.

In particular, Ratha et al. (2001a) did specific analysis on the sources of vulnerable attacks on the biometric identification system, and put them into 8 categories, as shown in Fig.2.

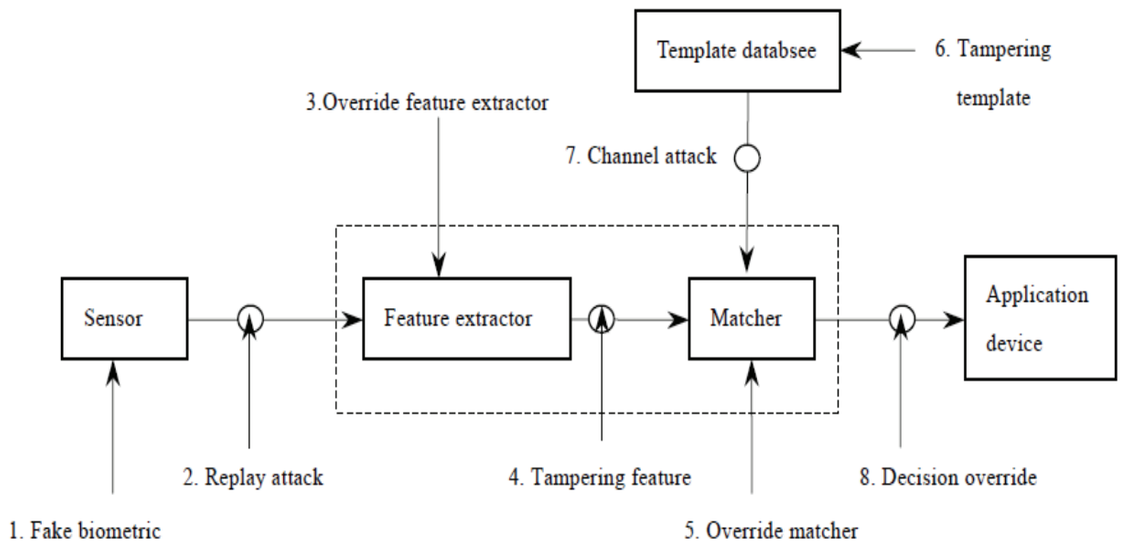


Fig. 2. Possible attack points in a generic biometrics-based system (Ratha et al, 2001a).

The eight basic sources of attack are described as below:

1. Fake biometric at the sensor: In this mode of attack, a possible reproduction of the biometric being used will be presented to the system. Examples include a fake finger, a copy of a signature, a face mask.
2. Resubmission of old digitally stored biometrics signal: In this mode of attack, an old recorded signal is replayed into the system bypassing the sensor.
3. Override feature extract: The feature extractor could be attacked with a Trojan horse so that it would produce feature sets chosen by the hacker.
4. Tampering with the feature representation: After the features have been extracted from the input signal they are replaced with a different synthesized feature set (assuming the representation is known).
5. Override matcher: The matcher is attacked to always directly produce an artificial high or low match score.

6. Tampering with stored templates: The stored template attacker tries to modify one or more templates in the database which could result in authorization for a fraudulent individual, or at least denial of service for the person associated with the corrupted template.
7. Channel attack between stored templates and the matcher: The templates from the stored database are sent to the matcher through a channel which could be attacked to change the contents of the templates before they reach the matcher.
8. Overriding Yes/No response: If the final result can be overridden with the choice of result from the hacker, the final outcome is very dangerous. Even if the actual pattern recognition system had excellent performance characteristics, it has been rendered useless by the simple exercise of overriding the result.

Due to the existence of the above threats to biometric system, it can be said that biometrics have degenerated gradually from "inherent features of you" to "features of what you have" to a certain extent. On the contrary passwords and keys can overcome this danger through encryption. Biometric cannot be protected directly through encryption, for instance, the hash function, as the great Hash intra-variance of it. However, it provides a feasible way for protecting the safety of biometric templates that combined biometric science and cryptography. There is the biggest obstacle to above combination that the contradiction between accuracy required by cryptography and inherent ambiguity of biometrics even if more and more researchers realized the advancement of the combination. How to overcome that contradiction in the condition of guarantying authentication performance of the system is the content of study on various biometric templates protection algorithm.

2. Review of biometric template protection technologies

This section focuses on classical biometric template protection theory and algorithms in the academic field. In a general viewpoint, we divided the biometric template protection into four groups: (1) **Biohashing** (Jin et al, 2004a, 2004b, 2004c, 2005, 2006, 2007, 2008; Lumini & Nanni, 2006, 2007; Jain et al, 1999; Nanni & Lumini, 2006, 2008a, 2008b; Connie et al, 2004; Ling et al, 2004, 2006; Maio & Nanni, 2005); (2) **Template encryption** (Soutar et al,1999; Davida et al, 1998; Juels & Sudan, 2002); (3) **Geometric transform of template technology** (Ratha et al, 2006, 2007; Ang et al, 2005; Clancy et al, 2003; Lee C et al, 2007; Lee Y et al, 2007; Tulyakov et al, 2005, 2007; Hao et al, 2006; Jain et al, 2006; Juels & Wattenberg, 1999; Juels & Sudan, 2002; Davida et al, 1998; Wang & Plataniotis, 2008; Uludag et al, 2005; Nandakumar et al, 2007; Kholmatov & Yanikoglu, 2008; Chang, 2006; Dodis et al, 2004, 2006; Mihailescu, 2007; Scheirer & Boult, 2007; Nyang & Lee, 2007; Jin et al, 2007; Buhan et al, 2007; Boyen, 2004; Boyen et al, 2005; Li, Q et al, 2006; Sutcu, 2007; Tong et al, 2007; Arakala et al, 2007; Zhang et al, 2008); and (4) **Template hiding transmission** (Khan et al, 2007, 2010).

2.1 Biohashing

The cancellable biometrics issue was addressed by Connie et al. (2004) which adopted a technique known as BioHashing. Jin et al. (2004c) proposed a novel approach of two-factor authenticator, based on iterated inner products between tokenised pseudo-random number and the user specific fingerprint feature, which generated from the integrated wavelet and Fourier–Mellin transform (WFMT), and hence produced a set of user specific compact code that named as BioHashing. WFMT features were chosen in this algorithms because in WFMT framework, wavelet transform preserves the local edges and noise reduction in the

low-frequency domain (high energy compacted) after the image decomposition, and hence makes the fingerprint images less sensitive to shape distortion. In addition to that, the reduced dimension of the images also helps to improve the computation efficiency.

The fingerprint feature vector is acquired after fingerprint image passed through wavelet transform, FFT transform, log-polar transform and high-pass filtering. As log-polar transform, the vector is invariable to translation, rotation and scale. Pseudo-random number can be calculated based on a seed that stores in USB token or smart card microprocessor through a random number generator. And a data T can be produced by iterating inner product between the pseudo-random number and the wavelet FMT fingerprint feature. Then the biohashing code is obtained by quantizing T with T=0 if $T \leq \tau$, otherwise T=1, where τ is a preset threshold. The BioHashing progression can be illustrated as in Fig. 3.

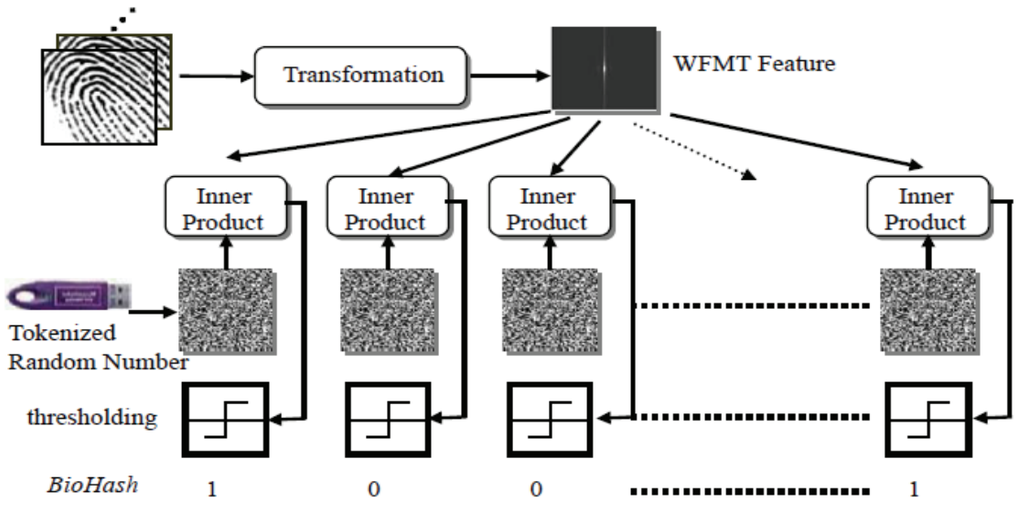


Fig. 3. Demonstration of BioHashing process (Jin et al, 2004c).

However, if the user token was stolen, the performance of BioHashing would be lower than that using only the biometric data (Lumini & Nanni, 2007; Nanni & Lumini, 2006, 2008). It can be concluded that the main factor is pseudo-random number, instead of fingerprint itself.

Lumini & Nanni (2007) proposed an improved BioHashing approach which is more robust than the original method. They consider that the case of loss of random number can be solved by extending the length of hashing key. Then they put forward four improvement measures to extend the length of key, i.e.

- **NORMALIZATION:** Processing with orthogonalization of generated vector.
- **τ VARIATION:** Instead of using a fixed value for τ, use several values for τ and obtain varying τ between $\tau_{\max}$ and $\tau_{\min}$, with p steps of

$$\tau_{step} = (\tau_{\max} - \tau_{\min}) / \mathrm{p} \tag{1}$$

- **SPACES AUGMENTATION:** Augment the length of key to k times of origin by space augmentation to be K spaces.
- **FEATURES PERMUTATION:** Using q permutations of biometric vector and obtained by round-shifting the coefficients of a fixed amount thus obtaining q bit vectors.

The result of improved BioHashing procedure, if all the above solutions are exploited, is a set of $k \cdot p \cdot q$ BioHash codes, which are compared by the Hamming distance. The verification task is performed by training a classifier for each BioHash code and finally by combining these classifiers by a fusion rule (we suggest the SUM rule).Thus it enormously increased length of hashing key, the problem of original algorithm is solved.

Biohashing algorithm was originally proposed for the fingerprint, but the algorithm requires highly differentiated fixed-length features which are very difficult to extract in the fingerprint. FingerCode (Jain et al, 1999) has a fixed length, but a low discriminabiltity, can not assure the certificated performance under the circumstance of loss of random number (Lumini & Nanni, 2007). The Biohashing algorithms of other biometrics, such as face, palmprint, have been proposed and carried out relevant research (Jin et al, 2004a, 2004b, 2006; Nanni & Lumini, 2006, 2008a; Connie et al, 2004; Jin & Ling, 2005; Ling et al, 2004, 2006). Some of the new technology applied also to Biohashing algorithms, such as probabilistic neural network (PNN) (Lumini & Nanni, 2006), Gray coding (Jin et al, 2007, 2008).It also applied to Biohashing algorithms that the technology of multimodal fusion and multi-feature fusion, to settle the problem of high EER in the term of loss of random number (Maio & Nanni, 2005; Lumini & Nanni, 2006; Nanni & Lumini, 2008).

2.2 Biometric template encryption

Bioscrypt algorithm was proposed by Soutar et al. (1999), which is one of the earliest algorithms about biometric encryption. The basic idea is based on image processing and Fourier transform. The algorithm has two steps: enrollment (as shown in Fig. 4(a)) and verification (as shown in Fig. 4(b)).

Enrollment phase: In the stage E-1 called Image Processing, combine a series of input fingerprint images with a random (phase) array to create two output arrays that are $H_{stored}(u)$ and $c_0(x)$; In the stage E-2 called Key linking, link a cryptographic key k_0, to the pattern, $c_0(x)$, via the link algorithm; In the stage E-3 called Identification code creation, create an identification code id_0, derived from the key k_0.

Verification phase: In the stage V-1 called Image Processing, combine $H_{stored}(u)$ from the bioscrypt, with a new series of input fingerprint images to create an output pattern, $c_1(x)$; In the stage V-2 called Key Retrieval, extract a key k_1 from $c_1(x)$ using the retrieval algorithm; In the stage V-3 called Key Validation, validate k_1 by creating a new identification code id_1, and comparing it with id_0.

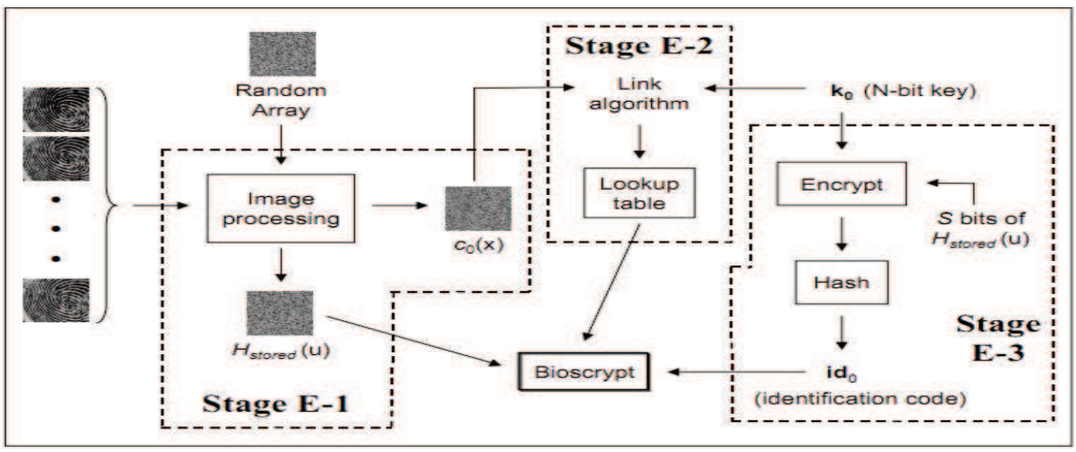
Also, there are criticisms to the algorithm from literature (Davida et al, 1998; Juels & Sudan, 2002) that the algorithm carried no rigorous security guarantees. It does not count the entropy loss of algorithm in enrollment phase and not present definitely the rejection rate and false acceptance rate. In addition, the authors assume that the corresponding fingerprint image is pre-registration in the course of the experiment, in fact, it is difficult to achieve.

2.3 Geometric transform of template technology

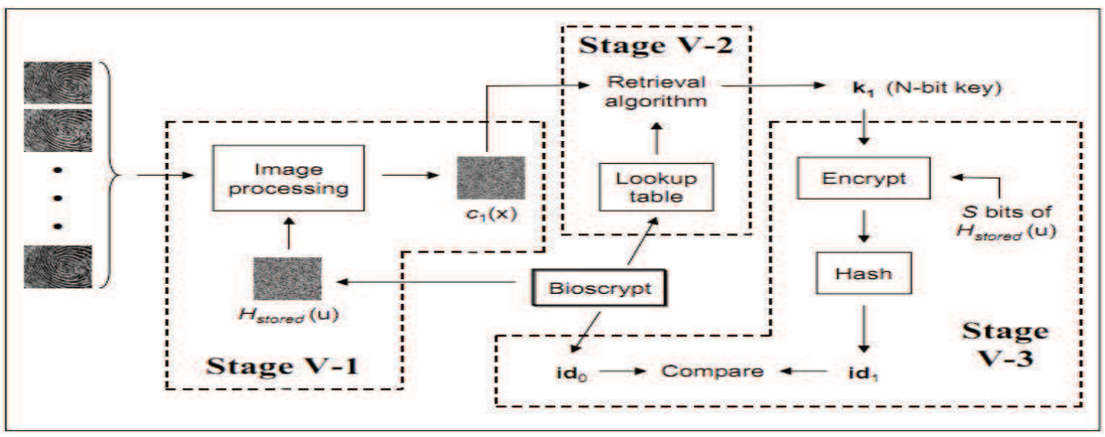
2.3.1 Geometric features transform

Ang et al. (2005) consider a key-dependent geometric transform that is applied to the features extracted from a fingerprint, to generate a key-dependent cancellable template for the fingerprint. The method reduce the EER according to the experiment with FVC2002 database, while the drawback of the method is that it has to detect singularity, and singularity itself is difficult to detect precisely, so the associated error will be introduced,

what's more, some types of fingerprints does not have singularity(such as arch). In addition, there is some inaptitude when folded templates are treated with common matching, such as there may be a coincidence that the minutiae to be overwritten while folded.



(a)



(b)

Fig. 4. (a). Enrollment phase of Bioscrypt algorithm (Soutar et al, 1999). (b). Verification phase of Bioscrypt algorithm (Soutar et al, 1999).

Ratha et al. (2006, 2007) presented a method of template transform. The method transforms the set of fingerprint minutiae from original space to another space using a one-way function. However, the performance of transformed template is lower than original template using the method. The reason is that there is deviation of transformed minutiae position from expectation, and additional registration to transformation function can avoid the descend mentioned above, but the registration is difficult to control. Lee C et al. (2007) presented a method without additional registration to transformation function, whereas, the method still does not reduce the risk of that system is attacked as loss of key.

Actually, Tulyakov et al. proposed a method named Symmetric Hash Functions for Fingerprint Minutiae (Tulyakov et al, 2007; Jain et al, 2006). They presented a method of hashing fingerprint minutia information and performing fingerprint identification in

hashing space. Due to the disorder of templates minutiae, input of hash function was not dependent on sequence (i.e. symmetric). Specifically, given n minutia points $\{c_1, c_2, \ldots, c_n\}$, they constructed following m symmetric hash functions and employed one or some of them:

$$\begin{aligned} &h_1(c_1, c_2, \cdots, c_n) = c_1 + c_2 + \cdots + c_n \\ &h_2(c_1, c_2, \cdots, c_n) = c_1^2 + c_2^2 + \cdots + c_n^2 \\ &\cdots \\ &h_m(c_1, c_2, \cdots, c_n) = c_1^m + c_2^m + \cdots + c_n^m \end{aligned} \tag{2}$$

where c_i (i =1, 2, … , n) are complex numbers, represent the information of minutiae structure.

They spread the concept of two factor authentication using key binding method. In order to enhance the security, they establish random relationship between a class of hash function and pair of minutiae structure by a particular user's key, so different user has different relationship between hash function and pair of minutiae structure.

2.3.2 Fuzzy commitment scheme

Juels & Wattenberg (1999) proposed a fuzzy commitment scheme. The early theoretical research combined well-known techniques from the areas of error-correcting codes and cryptography to achieve a typical key binding scheme. Actually, this scheme derived from bit commitment scheme of cryptography, and follows the concept of commitment and witness and uses them for the inherently fuzzy biometric data. Fuzzy commitment scheme F has two sections: commitment and decommitment. In terms of commitment, F shall be constructed so as to commit an error-correcting codeword c using a witness x, where both c and x are n-bit strings. In biometric scenarios, x typically represents a biometric template, such as a fingerprint. The codeword c represents a secret key protected under this template. Deviation $\delta = x - c$, so commit: $\{\mathbf{hash}(c), \delta\}$, where $\mathrm{hash}(\bullet)$ is hash function. While consider the decommitment, user input a biometric vector x', a secret c' can unlocked from commitment according the formula: $c' = x' - \delta = x' - x + c$. If x is very closed to x' in a certain distance (i.e. Hamming distance), c' can be considered to be identical to c, as well as verification of **hash** (c') and hash(c) , and thus achieve the authentication.

Based on the fuzzy commitment scheme, Hao et al. (2006) designed and implemented an iris encryption scheme. Compared to the fingerprint, iris is more suitable for the search of encryption because IrisCode is more canonical in coding. IrisCode has a fixed length of 2048-bit, together with some encryption algorithm to generate immediately, and the encryption and decryption is very easy to operate.

2.3.3 Fuzzy vault scheme

Juels & Sudan (2002) presented the fuzzy vault scheme on the foundation of fuzzy commitment scheme. The most valued characteristic of the algorithm is linking the fuzziness of biometric with accuracy of cryptography perfectly.

The detailed implementation of the algorithm can be described as follows:

a. "Lock" vault: Alice aims to lock a secret K under an unordered set A. She selects a polynomial p in a single variable x such that p encodes K in some way and computes the p (A), projection of A lying on the polynomial p, thus form a finite point set (A, p

(A)). She then creates a number of random chaff points, with point set (A, p (A)) constitute the Vault

b. "Unlock" vault: Suppose now that Bob wishes to unlock *K* by means of an unordered set B. If B overlaps substantially with A, then B identifies many points in R that lie on polynomial p. Using error correction, he is able to reconstruct p exactly and thereby *K*. If B does not overlap substantially with A, then it is infeasible for Bob to learn *K*, because of the presence of many chaff points.

Based on the work of Juels et al, Clancy et al. (2003) advanced the conception of fingerprint vault. Firstly, use user's five fingerprints to register, extract position of minutiae as input, manage correspondence problem between fingerprint features by nearest neighbor algorithm. In considering the size of fingerprint pressing region, author add *N* chaff points to the minutiae set, where the distance of chaff points to the minutiae and the distance between chaff points themselves aren't smaller than *d*, thus form the encrypted fingerprint vault. Being different from Juels et al, Clancy et al. describes the order of fingerprint polynomial in detail. Considering the decryption, using the nearest neighbor algorithm for extracted minutiae feature from matching fingerprint, search out the corresponding points in fingerprint vault, then take the points as input of RS correction code algorithm to compute the correct form of encrypted polynomials. The work contributes to describe the implementation method of fuzzy vault in the field of fingerprint in detail, achieve 69-bit security on the basis of 20% to 30% of the rejection. While like reference (Davida et al, 1998), the drawback is the corresponding pre-registration fingerprint image which the authors assume.

Uludag et al. (2005) presented a more practical scheme named Fuzzy Vault for Fingerprint on the basis of Fuzzy Vault and Fingerprint Vault. Nandakumar et al. (2007) notice that since the fuzzy vault stores only a transformed version of the template, aligning the query fingerprint with the template is a challenging task. So they propose the idea that add a password to the periphery of fuzzy vault system, and it is deformed minutiae parameter that are stored in new template but original data, where the deformed parameter is correlated to the user set-up password. Encryption mechanism is independent on the security of fuzzy vault, so system is under double protection and attacker can take the legality user data only by breaching two systems in the one time. Compared to ordinary fuzzy vault system, enhanced system has a higher rejection rate, but the cost is enhanced algorithm time complexity.

Gradually fuzzy vault is extended to other biometric (Nyang & Lee, 2007; Wang & Plataniotis, 2008; Lee, Y, 2007). Nyang & Lee (2007) show how can fuzzy vault be introduced to the weighted principal component analysis (PCA) of face, and introduce a so-called intermediate layer so that more points heavy weighted feature construct, at the same time, hash the feature and corresponding construction data using the SHA-1 function, whereas there is no concrete experimental validation. The PCA features of face are mapped into binary data with two random orthonormal matrixes (R_1, R_2), the result is some binary features in the 16-bit length and used for the encoding and decoding of fuzzy vault (Wang & Plataniotis, 2008). Lee, Y (2007) proposes a new method of applying iris data to the fuzzy vault. The author obtains 16 27-bit length iris features by the methods of independent component analysis (ICA)-based feature extraction and K-means cluster pattern. Experiment on the database BERC iris, which have 99×10=990 iris images, constituted by author. Zero FAR and about 0.775% FRR are obtained.

Fuzzy Vault has become one of the most potential methods on biometric template protection technology. With the gradually abroad research and application of it, some researchers attend the corresponding attacks strategy (Scheirer & Boult, 2007; Kholmatov & Yanikoglu, 2008; Mihailescu, 2007; Chang, 2006). Scheirer & Boult (2007) review briefly some of the known attacks against biometric fuzzy vault (BFV) and biometric encryption (BE) techniques, including attack via record multiplicity, surreptitious key-inversion attack, and novel blended substitution attacks. And apply each of these attacks on the Fuzzy Vault and biometric encryption system. Kholmatov & Yanikoglu (2008) implemented attack via record multiplicity using 200×2+400 fingerprints and can correlate 59% of vaults approving the claim of fuzzy vault's vulnerability against attack by comparison between two vaults from same finger, which show that the fuzzy vault is threatened by attack via record multiplicity on the ratio more than 50%, the ratio will increase when there are three or more correlated vaults. Mihailescu (2007) proved that the system is vulnerable to the brute force attack and also gave several suggestions which can improve the fingerprint vault to a cryptographically secure algorithm by mathematic analysis. Chang (2006) thought that genuine minutiae can be distinguished from chaff points by statistical characteristics of all points, actually chaff points tend to concentrate, they proved that the genuine minutiae can be found in much less searching time than force attack in the means of mathematic analysis and experimental validation. All of these attack are based on the fact that the vault contain genuine minutiae data, in other words, there is definitely entropy loss. So, these attacks will have no entry point if those genuine minutiae are not stored in vault by some certain transformation.

2.3.4 Fuzzy extractor

Dodis et al. (2004) proposed a concept of secure sketch and fuzzy extractor, aimed to achieve reliable and secure authentication to user, they attempt to convert random biometric signal into stable key which can be used in encryption. Some certain information of secure sketch can be extracted from biometric signal by the operation that can tolerate error in a certain degree. The published information can reconstruct original template perfectly while signal similar with original template is input. Meanwhile, the linchpin of the method is that the original template cannot be reconstructed by the republished information. Fuzzy extractor extracts approximate uniformly distributed random signal **R** from the input biometric signal, so **R** can be applied as a Key to all of the encryption.

In order to construct concrete algorithm for various biometric signal, Dodis et al. make use of three measure spaces, such as hamming distance, set distance, and edit distance. In the space of hamming distance, Dodis et al. view fuzzy commitment (Jin et al, 2007) as optimal secure sketch, and reform it into approximate optimal fuzzy extractor using general construction method. In the space of set distance, they view fuzzy vault as approximate optimal secure sketch, and reform it into approximate optimal fuzzy extractor using same construction method. In the space of edit distance, they define the transformation from edit space to set space in order to transform optimal fuzzy extractor of set space into edit space. Also, authors prove that the optimal secure sketch and fuzzy extractor can be constructed if entropy loss satisfies some certain condition.

Literatures (Dodis et al, 2006; Buhan et al, 2007; Boyen, 2004; Boyen et al, 2005; Li, Q et al, 2006; Sutcu, 2007) contribute to the study of key generation method. Literatures (Tong et al, 2007; Arakala et al, 2007) extract robust key respectively from feature of fingercode and

feature of minutiae structure, and progress attempt of practical algorithm. Although the result isn't ideal, they contribute exploratively to the research of the issue. Literature (Zhang et al, 2008) actualizes iris-based fuzzy extractor, analyzes the influence on the performance of identification of difference between iris feature codes, and designs two layer cascade error-correcting scheme in which iterative codes and Reed-Solomon codes are applied.

2.4 Hidden transmission of biometric template

Khan et al. (2007) presented a chaotic secure content-based hidden transmission scheme of biometric data. Encryption and data hiding techniques are used to improve the security and secrecy of the transmitted templates. Secret keys are generated by the biometric image and used as the parameter value and initial condition of chaotic map, and each transaction session has different secret keys to protect from the attacks. Two chaotic maps are incorporated for the encryption to improve the system's resistance against attacks. Encryption is applied on the biometric templates before hiding into the cover/host images to make them secure, and then templates are hidden into the cover image. Experimental results show that the security, performance, and accuracy of the presented scheme are encouraging comparable with other methods found in the current literature. In 2010, Khan et al. proposed another means of hidden biometric template transmission named chaos and NDFT-based spread spectrum technique to conceal fingerprint-biometrics templates into audio signals. Fingerprint templates are encrypted by chaotic encryption, encoded by the BCH codes, modulated by chaotic parameter modulation (CPM), and then hid into the chaotically selected random sampling points of the host speech signal by non-uniform discrete Fourier transform (NDFT). The template extraction process is completely blind and does not require original speech signal, thus the extraction depends on the secret key. Experimental and simulation results show that the scheme is robust against common signal processing attacks, and accomplishes perceptual transparency by exploiting the masking effects of human auditory system (HAS).

3. The biometric template protection with secure authentication scheme based on fuzzy extractor and chaotic spread spectrum encryption

In this section, a biometric template protection scheme based on fuzzy extractor for biometric authentication is proposed. Instead of only using one layer error-correcting code (ECC) or two cascaded ECCs in published literatures, a ECC followed by chaotic spread spectrum encryption is utilized in our scheme. The scheme is evaluated using 160 4095-bit fingerprint codes from 20 different fingers, with 8 samples for each finger. Simulation experiments show that both security and privacy of biometric template can be effectively protected.

3.1 Chaotic spread spectrum encryption using coupled n-NDFs

Since the intra-class variance among the samples from same finger may achieve to 25%-30%, the chaotic spread spectrum encryption technique, instead of ECC, is used here to improve the error-correcting ability, with attendant encryption function. In the following subsection, n-dimensional nonlinear digital filter (n-NDF) is preferred to serve as the underlying chaotic system to produce secure spread spectrum code.

3.1.1 Chaotic spread spectrum code base on *n*-dimensional NDF

Nonlinear digital filters (NDFs) have received attention in chaotic secure communication, hash function and pseudorandom bit generator. The reason is that the *n*-NDF outputs *n*-dimensional uniform distributed chaotic signal when it satisfies Kelber conditions (Wang & Zhang, 2007). Fig.5. depicts the block diagram of an *n*th-order NDF, whose state equation is given by

$$\begin{cases} \mathrm{z}_1(t+1) = h \circ \mathrm{mod}(\sum_{i=1}^{n} c_i \, \mathrm{z}_i(t) + \phi) \\ \mathrm{z}_q(t+1) = \mathrm{z}_{q-1}(t) \qquad , q = 2,3,\cdots,n \\ y(t) = \mathrm{z}_1(t+1) \end{cases} \tag{3}$$

where $\phi \in (-1,1)$ denotes input signal, y(t) the output signal, $\mathrm{z} = \{z_1, z_2, \cdots, z_n\}^T \in (-1,1)^n$ the initial states of filter, $\mathbf{c} = \{c_1, c_2, \cdots c_n\}$ the filter coefficients, $h(.)$ the piecewise linear map defined by

$$h(x,p) = \begin{cases} (2x+1-p)/(1+p) & x \in (-1,p] \\ (-2x+1+p)/(1-p) & x \in (p,1) \end{cases}, \text{ and } \; mod(v) = v - 2 \cdot \left\lfloor \frac{v+1}{2} \right\rfloor .$$

For describing convenience, the discretization form of *n*-NDF above is denoted as $y(i+1) = \mathrm{F}(\phi, \mathbf{z}, \mathbf{c}, i)$. It has been proven that *n*-NDF is an ergodic chaotic system with *n*-D uniform distribution provided that the system is not decomposable and the coefficients $c_n \in Z, |c_n| > 1, c_i \neq 0, i \in \{1,2,...,n-1\}$.

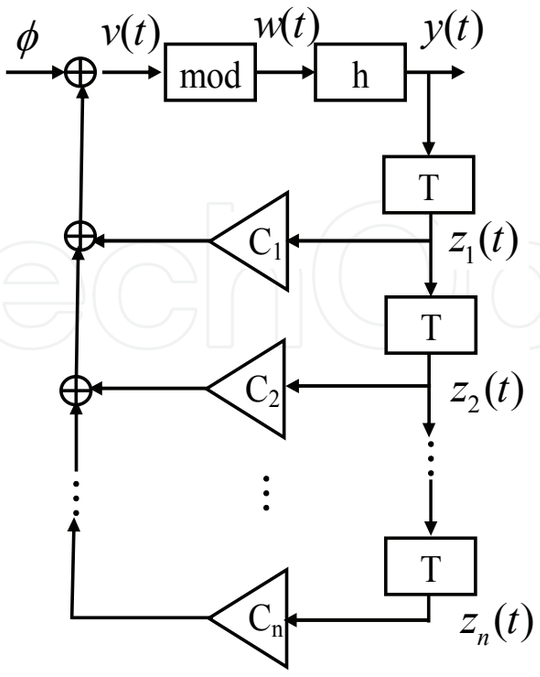


Fig. 5. Block diagram of the *n*th-order NDF.

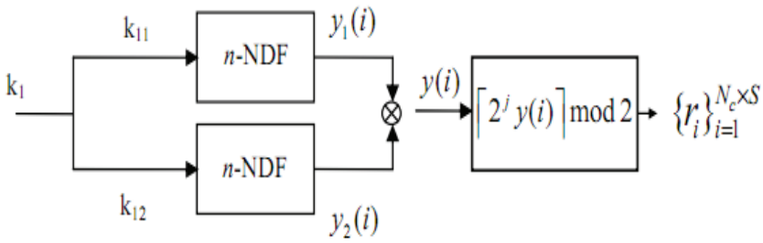


Fig. 6. Generating chaotic spread spectrum sequence by coupling two *n*-NDFs.

In the following, we couple two independent *n*-NDFs, as depicted in Fig. 6, to generate chaotic spread spectrum sequence. The two independent *n*-NDFs are expressed as

$$\begin{cases} \mathrm{y}_1(i+1) = \mathrm{F}_1(\phi_1, \mathbf{z}_1, \mathbf{c}_1, i) \\ \mathrm{y}_2(i+1) = \mathrm{F}_2(\phi_2, \mathbf{z}_2, \mathbf{c}_2, i) \end{cases}, \ \mathrm{y}_1, \mathrm{y}_2 \in (-1,1) \tag{4}$$

Then couple two outputs of Eq.(4) as $\mathrm{y}(i) = mod(\mathrm{y}_1(i) + \mathrm{y}_2(i))$ (The symbol " $\otimes$ " in Fig.6.), and quantize y(i) uniformly to get the binary spread spectrum sequence $r_i = \lceil 2y(i) \rceil \bmod 2$.

3.1.2 Chaotic spread spectrum encryption

Figure 7 shows that the process of chaotic spread spectrum encryption is with the encryped operation XOR, at the same time with code spectrum spread. Specifically, under the control of key k_1, chaotic spread spectrum sequence $\{r_i\}_{i=1}^{N_c \times S}$ can be obtained, then XOR it with each error correction encoded binary code $c_j (j = 1, \cdots N_c)$, the result $w_i = r_i \oplus c_{\lceil i/s \rceil}$ is the spreading encryption information corresponding to $C = \{c_j\}_{j=1}^{N_c}$.

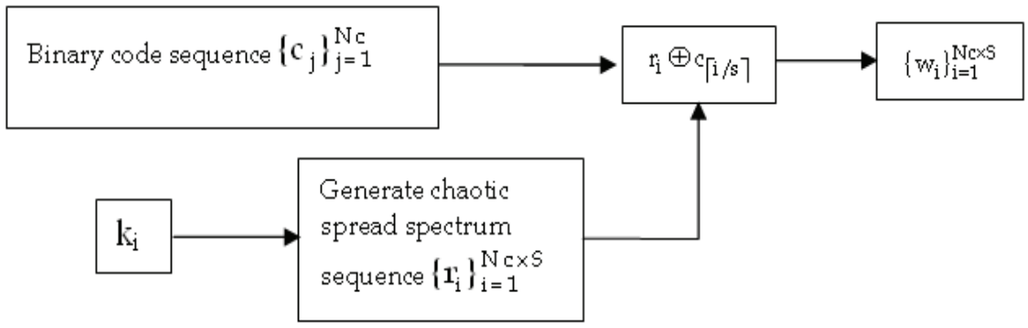


Fig. 7. The process of chaotic spread spectrum operation.

Based on the chaotic spread spectrum sequence r_i, the process of chaotic spread spectrum encryption is defined as

$$\begin{aligned} w &= \{w_i\}_{i=1}^{N_w} \\ &= \{r_i \oplus c_{\lceil i/s \rceil}\}_{i=1}^{N_C \times S} \\ &= \{c_j \oplus r_{(j-1)\times S+1}, c_j \oplus r_{(j-1)\times S+2}, \cdots, c_j \oplus r_{(j-1)\times S+S}\}_{j=1}^{N_c} \end{aligned} \tag{5}$$

where symbol " $\oplus$ " denotes bit-XOR operation, **S** is spread factor, **Nc** the bit-length of original message, r_i the spread spectrum sequence, and w the spreaded sequence with bit-length $N_w = S \times N_c$. With the increasing **S**, the error correction capability can also be improved. The critical work is to decide a suitable **S** by experiments to discriminate the intra-class samples and inter-class samples.

Regarding the de-spread spectrum, it is the inverse process of Fig.7. Assume the spread information is $w^* = \{w_j^*\}_{j=1}^{N_w}$, corresponding to the original message w, the de-spread process is composed of correlation and decision phases defined by Eq.(6) and Eq.(7), respectively. The c_j^* in Eq.(7) is the recovered binary code sequence corresponding to c_j.

$$\begin{aligned} d &= \{d_j\}_{j=1}^{N_c} \\ &= \{\sum_{i=1}^{S} w_{(j-1)\times S+i}^* \oplus r_{(j-1)\times S+i}\}_{j=1}^{N_c} \end{aligned} \tag{6}$$

$$c_j^* = \begin{cases} 0 & d_j < S/2 \\ 1 & d_j \geq S/2 \end{cases} \tag{7}$$

3.2 The proposed biometric template protection scheme

The way of centralized storage of biometric data in the database have security guarantees by using the chaotic *n*-NDF, where the hash value $H(R)$ of random secret information **R** instead of biometric w_0 itself stored in the database, can play the same protection effect as a password on authentication system. Given that the one-way hash function $H(.)$ is safe and collision free, the proposed scheme is a safe fingerprint identification system.

The proposed scheme includes two stages: registration and authentication. In the stage of registration, *l*-bit random number R was selected first, and then carry out BCH encoding operation on it and R′ is obtained. Next, perfrom chaotic spread spectrum on R′ to get sequence R′′. At the same time w_0' is reached from the user's fingerprint code w_0 after BCH decoding operation on the w_0, then publish pub=R′′ $\oplus$ w_0'. The stage of authentication is the recovery process of R. Suppose w_1 is the fingerprint code what is to be authenticated, similarily the w_1' is the data obtained from the BCH decoding on the w_1, as $pub \oplus w_1'$= (R′′ $\oplus$ w_0') $\oplus$ w_1'=R′′ $\oplus$ (w_0' $\oplus$ w_1'), while $w_0' \oplus w_1'$can be viewd as noise which disturbes R′′. The registration and identification process can be seen as that R passes an additive noise channel of digital communication system. Similar fingerprint feature code have less different bits equivalently less noise, while the different fingerprint feature code have more different bits, resulting in greater noise. When the R'' is disturbed by noise P, through the appropriate error-correcting code that R can be recovered when similar fingerprint feature is authenticated while different fingerprint feature can not. Assume R be recovered as R_1, the authentication is valid or not depending on whether the hash value of R_1 equals the pre-stored hash value H (R) or not.

Utilizing the ECC, chaotic spread spectrum and fuzzy extractor, the proposed scheme consists of registration process and authentication process, which is illustrated in Fig.8. and described as follows.

Registration process

User's fingerprint data is collected firstly in the registration phase, and carry out features extraction and coding, calculate R and *pub* from the BCH decoding of fingerprint template w_0', where R is the secret random number and *pub* is public data. H(*R*) is calculated by the one-way hash function. R, H(*R*) and *pub* are stored in server database, thus complete the registration.

1. Randomly select a secret R and perform BCH encoding: R′ ← BCH(*R*);
2. Perform chaotic spread spectrum operation on R′: R″ ← Chaotic_SS(*R*′);
3. To decrease the distance of intra-class samples, perform BCH decoding on the user's biometric template w_0: w_0' ← De_BCH(w_0);
4. Perform bit-XOR operation on R″ and w_0' to get public information: *pub* ← R″ ⊕ w_0';
5. Store *pub* and Hash value of R on server for user authentication: server ← {*pub*, H(*R*)}, where H(.) is a cryptographic hash function.

Authentication process

In the authentication phase the user's fingerprint information is collected and the fingerprint feature is denoted as w_1. The authentication process is as follows.

1. extract the user's fingerprint template w_1 and execute BCH decoding on it: w_1' ← De_BCH(w_1);
2. retrieve the *pub* information from server, and bit–XOR it with w_1′: R_1'' ← w_1' ⊕ *pub*;
3. perform chaotic de-spread spectrum operation on R_1'': R_1' ← Chaotic_DS(R_1'');
4. perform BCH decoding on R_1': R_1 ← De_BCH(R_1');
5. match the hash value of R_1 and the hash value of R stored in server, if H(R_1)==H(R), the user is authenticated, otherwise, the user is rejected.

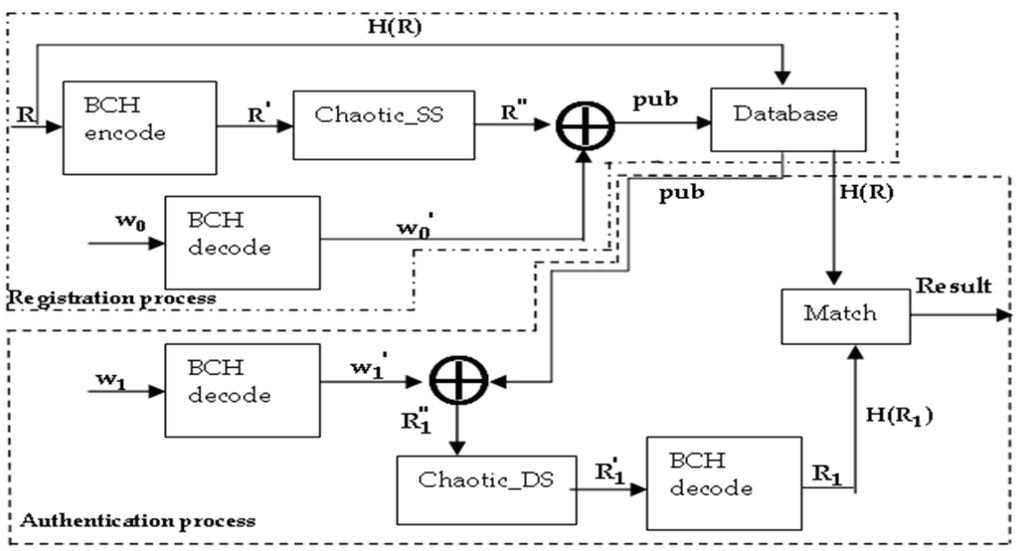


Fig. 8. Block diagram of the proposed scheme.

Note that two minor things in registration and authentication phases have to be processed. One is how to initialize the initial states and coefficients of coupled *n*-NDFs in chaotic spread/de-spread spectrum process. This can optionally split H(R) into 32-bit strings for

each state and coefficient. If the length of H(R) is not enough long, we can hashing R one more times until the total hash length meets requirement. The other is bit-XOR operations in $pub \leftarrow R'' \oplus w_0'$ and $R_1'' \leftarrow w_1' \oplus pub$, where two operands are required to be identical bit length, otherwise bit-expansion is necessary. That is, if the bit length of w_0' is smaller than that of R'', repeatedly concatenate w_0' so that its length is enough long. Otherwise, trim w_0' so that its length equals to that of R''. As for $R_1'' \leftarrow w_1' \oplus pub$, the way of processing is similar.

3.3 Security analysis

In this subsection, we will briefly illustrate the privacy protection and cancellable ability of proposed scheme.

Privacy protection: Early biometric-based authentication systems directly store user's biometric templates in server, this way may cause template disclosing by database manager or hacker, even the templates are stored in smart card. In the proposed scheme, only H(R) and *pub* are stored in server. Since $H(\cdot)$ is one-way cryptographic hash function, it's computationally infeasible to recover R. Moreover, R is randomly selected by authenticated user, the attacker can not derive R and biometric template from H(R) and *pub*. Therefore, the proposed scheme has strong privacy protection.

Template cancellation: The template cancellation of proposed scheme is different from traditional template cancellations, but in fact it can achieve to the purpose of "template cancellation". In this scheme, on the one hand, users select different random secret R for different application systems, and thus different systems stored different information H(R) and *pub*. This way adversary can not obtain any secret information R or biometric template of a user, though they collect all the stored information of the same user from multiple authentication systems. On the other hand, when user's register information requires update, user only need reselect random secret information R_{new} and calculate $H(R_{new})$ and pub_{new}. After re-registering, the old information $H(R_{old})$ and pub_{old} are not valid any more. Moreover, it is not conductive to derive the user's biometric template from the newly registered information $H(R_{new})$ and pub_{new}, even when attacker got the $H(R_{old})$ and pub_{old}. Therefore, the multiple re-registering information from the same user does not decrease the security. From system function point of view, the proposed scheme inherently owns revocable-biometric ability.

3.4 Experimental results

The proposed method is evaluated using the fingerprint database of FVC 2004 [FVC 2004], where there are 8 impressions for each of the 100 distinct fingers with image size of 328x364 at a resolution of 500dpi.

We select 8 impressions for each of the 20 distinct fingers. Among these fingerprint images, 60 images for 20 fingers (each finger has 3 images) are used to parameter tuning before testing, while the rest fingerprint images are used to evaluate the scheme. Fig.9 shows 3 images of one finger of 20 fingers. The evaluation criteria used here are fault accept rate (FAR) and fault reject rate (FRR).

Firstly, we use 60 images for parameter optimizing. There are two parameters (i.e. *n*, *k*) in BCH error-correcting code, and one parameter (i.e. spread factor S) in chaotic spread spectrum. The optimization target is balancing the FRR for intra-class samples, the FAR for

inter-class samples and computational load. Based on such optimization principle, one of the tuning parameter set are valued as n=63, k=10 and spread factor S=40.

Fig. 9. Three images of one finger of 20 fingers for parameter tuning.

In the rest 100 samples, we select 2 samples from the rest 5 samples of each finger, that one sample is used to registration while the other is used to authentication. We perform such intra-class experiments for $20 \times C_5^2 = 200$ times. The experiment result is listed in table 1. The data of table 1 shows that the FRR=0.5% and GAR=99.5% in the scheme. When we improve the error-correcting capability by increasing the spread factor or BCH parameters, the FRR will decrease as expected at the cost of time complexity and storing volume.

parameters	Right accept number	False refuse number	FRR
N=63, k=10, spread factor=40	199	1	0.5%

Table 1. FRR experiment result for intra-class samples

In addition, we randomly select 2 inter-class samples from the rest 100 samples to evaluate the FAR. Fig.10 shows one experimented group of that. Such experiments are performed for $C_{100}^2 - 20 \times C_5^2 = 4750$ times with the same parameters as table 1, and the statistical result is summarized in table 2.

Fig. 10. One experimented group for the FAR evaluation.

parameters	Right refuse number	False accept number	FAR
N=63, k=10, spread factor=40	4750	0	0

Table 2. FAR experiment result for inter-class samples

The inter-class experiments show that no fingerprint sample has been accepted by fault, i.e. the FAR=0. It should not be surprise for such result, because the difference of two inter-class samples is so large that exceeds the error-correcting capability of BCH and spread spectrum under the selected parameters.
From the experimental FRR and FAR index of the proposed scheme, it can be seen that the scheme has high right accept rate for the intra-class fingerprints while keep ideal fault accept rate for the inter-class fingerprints. Of course, the above experiments are not enough to test the scheme and come to final conclusion. More samples, more kinds of biometrics and great number of experiments are necessary to evaluate the biometric system.

4. Conclusion

In this chapter, we have presented a biometric template protection scheme based on fuzzy extractor for biometric authentication. Instead of only using one layer error-correcting code (ECC) or two cascaded ECCs in published literatures, an ECC followed by chaotic spread spectrum encryption is utilized in this scheme. We performed a series of experiments to evaluate the performance of the system and the experimental results show that the proposed system is robust against noises and attacks. Moreover, the proposed system can be easily realized in the real biometric applications.

5. References

Ang, R. Rei, S. & Luke, M. (2005). Cancellable key-based fingerprint templates, In: *Information Security and Privacy,* Boyd, C. & Nieto, J, pp. 242−252, Springer Berlin, ISBN 978-3-540-26547-4, Heidelberg, Germany

Arakala, A. Jeffers, J. & Horadam, K. (2008). Fuzzy extractors for minutiae-based fingerprint authentication. In: *Proceedings of the ICB 2007,* Lee SW, Li SZ, pp.760−769, Springer Berlin, ISBN 978-3-540-74548-8, Heidelberg, Germany

Boyen, X. (2004). Reusable cryptographic fuzzy extractors, *Proceedings of The Conference on Computer and Communications Security,* ISBN 1-58113-961-6, Washington DC, USA, Octorber 2004

Boyen, X. Dodis, Y. Katz, J. Ostrovsky, R. & Smith, A. (2005). Secure remote authentication using biometric data. In: *Advances in Cryptology â€“ EUROCRYPT 2005,* Cramer, R, pp. 147−163, Springer Berlin, ISBN 978-3-540-25910-7 , Heidelberg, Germany

Buhan, I. Doumen, J. Hartel, P. & Veldhuis, R. (2007). Fuzzy extractors for continuous distributions, *Proceedings of The Conference on Computer and Communications Security,* ISBN 1-59593-574-6, Singapore , March 2007

Cappelli, R. Lumini, A. Daio, D. & Maltoni D. (2007). Fingerprint image reconstruction from standard templates. *IEEE Trans on Pattern Analysis and Machine Intelligence*, Vol.29, No.9, (September 2007), pp.1489−1503, ISSN 0162-8828

Chang, E. Shen, R. & Teo, F. (2006). Finding the original point set hidden among chaff, *Proceedings of Conference on Computer and Communications Security,* ISBN 1-59593-272-0, Taipei, China, March 2006

Clancy, T. Kiyavash, N. & Lin, D. (2003). Secure smartcard-based fingerprint authentication, *Proceedings of the ACMSIGMM 2003 Multimedia, Biometrics Methods and Applications Workshop. Association for Computing Machinery*, (November 2003), pp. 45−52, ISSN 1-58113-779-6

Connie, T. Jin, A. Goh, A. & Ling, D. (2004). PalmHashing: A novel approach for dual-factor *authentication. Pattern Analysis & Applications,* Vol.7, No.3, (August 2004), pp. 255−268, ISSN 1433-7541

Davida, G. Frankel, Y. & Matt, B. (1998). On enabling secure applications through off-line biometric identification, *Proceedings of the IEEE Symposium on Security and Privacy*, ISBN 0-8186-8386-4, Oakland, May 1998

Dodis, Y. Reyzin, L. & Smith, A. (2004). Fuzzy extractors: How to generate strong keys from biometrics and other noisy data. In: *Advances in Cryptology - EUROCRYPT 2004,* Cachin, C. & Camenisch, J, pp.523−540, Springer Berlin, ISBN 978-3-540-21935-4, Heidelberg, Germany

Dodis, Y. Katz, J. Reyzin, L, Smith A. (2006). Robust fuzzy extractors and authenticated key agreement from close secrets. *Advances in Cryptology-Crypto*, Vol.4117, (2006), pp.232−250, ISSN 0302-9743

FVC2004 http://bias.csr.unibo.it/fvc2004

Hao, F. Anderson, R. & Daugman, J. (2006). Combining crypto with biometrics effectively. I*EEE Trans on Computers*, Vol.55, No.9, (September 2006), pp. 1081−1088, ISSN 0018-9340

Jain, A. Prabhakar, S. Hong, L. & Pankanti, S. (1999). FingerCode: A filterbank for fingerprint representation and matching. *Proceedings of IEEE Computer Society Conference on Computer Vision and Pattern Recognition*, ISBN 0-7695-0149-4, Fort Collins, CO, June 1999

Jain, A. Ross, A. & Pankanti, S. (2006). Biometrics: A tool for information security. *IEEE Trans on Information Forensics and Security*, Vol.1, No.2, (June 2006), pp. 125−143, ISSN 1556-6013

Jin, A. Ling, D. & Goh, A. (2004). An integrated dual factor authenticator based on the face data and tokenised random number, In: *Biometric Authentication*, Zhang, D. & Jain, A. pp. 117−123, Springer Berlin, ISBN 978-3-540-22146-3, Heidelberg, Germany

Jin, A. Ling, D. & Goh, A. (2004). Personalised cryptographic key generation based on FaceHashing. *Computers & Security*, Vol.23, No.7, (October 2004), pp. 606−614, ISSN 01674048

Jin, A. Ling, D. & Goh, A. (2004). Biohashing: Two factor authentication featuring fingerprint data and tokenised random number. *Pattern Recognition*, Vol.37, No.11, (November 2004), pp.2245−2255, ISSN 0031-3203

Jin, A. & Ling, D. (2005). Cancellable biometerics featuring with tokenised random number. *Pattern Recognition Letters*, Vol.26, No.10, (July 2005), pp.1454−1460, ISSN 01678655

Jin, A. Goh, A. & Ling, D. (2006). Random multispace quantization as an analytic mechanism for biohashing of biometric and random identity inputs. *IEEE Trans on Pattern Analysis and Machine Intelligence*, Vol.28, No.12, (December 2006), pp.1892−1901, ISSN 0162-8828

Jin, A. Toh, K. & Yip, W. (2007). 2^N Discretisation of biophasor in cancellable biometrics. In: *Advances in Biomet*rics, Lee, S. & Li, S, pp. 435−444, Springer Berlin, ISBN 978-3-540-74548-8, Heidelberg, Germany

Jin, A. Yip, W. & Lee, S. (2008). Cancellable biometrics and annotations on BioHash. P*attern Recognition*, Vol.41, No.6, (June 2008), pp. 2034−2044, ISSN 00313203

Juels, A. & Wattenberg, M. (1999). A fuzzy commitment scheme, *Proceedings of the 6th ACM conference on Computer and communications security,* ISBN 1-58113-148-8, Singapore, November 1999

Juels, A. & Sudan, M. (2002). A fuzzy vault scheme, *Proceedings of the 2002 IEEE International Symposium on Information Theory,* (2002), pp.408

Khan, MK. Zhang, JS. & Tian, L. (2007). Chaotic secure content-based hidden transmission of biometrics templates. *Chaos, Solitons, and Fractals,* Vol.32, No.5, (June 2007), pp. 1749–1759, ISSN 09600779

Khan, MK. Xie, L. & Zhang, JS. (2010). Chaos and NDFT-based concealing of fingerprint biometric data into audio signals for trustworthy person authentication. *Digital Signal Processing: A Review Journal,* Vol.20, No.1, (January 2010), pp. 179–190, ISSN 10512004

Khan, MK. Zhang, JS. Wang, XM. (2008). Chaotic Hash-based Fingerprint Biometric Remote User Authentication Scheme on Mobile Devices, *Chaos, Solitons and Fractals*, vol.35, No.3, (2008), pp.519-524, ISSN 09600779

Kholmatov, A. & Yanikoglu, B. (2008). Realization of correlation attack against the fuzzy vault scheme, *Proceedings of SPIE - The International Society for Optical Engineering,* ISBN 9780819469915, San Jose, CA, United states, January 2008

Lee, C. Choi, J. Toh, K. Lee, S. & Kim, J. (2007). Alignment-Free cancelable fingerprint templates based on local minutiae information. *IEEE Trans on Systems, Man, and Cybernetics, Part B: Cybernetics*, Vol.37, No.4, (August 2007), pp. 980−992, ISSN 1083-4419

Lee, Y. Bae, K. Lee, S. Park, K. & Kim, J. (2007). Biometric key binding: Fuzzy vault based on iris images. In: *International Conference on Advances in Biometrics, Proceedings of the ICB 2007,* Lee, S. & Li, S, pp. 800−808, Springer Berlin, ISBN 978-3-540-74548-8, Heidelberg, Germany

Li, Q. Sutcu, Y. & Memon, N. (2006). Secure sketch for biometric templates. In: *Advances in Cryptology - ASIACRYPT 2006,* Lai, XJ. & Chen, KF, pp. 99−113, Springer Berlin, ISBN 978-3-540-49475-1, Heidelberg, Germany

Li, P. Tian, J. Yang, X. Shi, P. & Zhang, YY. (2009).Biometric Template Protection. *Journal of Software*, Vol.20, No.6,2009,(June 2009), pp.1553−1573

Ling, D. Jin, A. & Goh, A. (2004). Eigenspace-Based face hashing. In: *Biometric Authentication*, Zhang, D. & Jain, A. pp. 195−199, Springer Berlin, ISBN 978-3-540-22146-3, Heidelberg, Germany

Ling, D. Jin, A. & Goh, A. (2006). Biometric Hash: High-Confidence face recognition. *IEEE Trans on Circuits And Systems for Video Technology*, Vol.16, No.6, (June 2006), pp. 771−775, ISSN 1051-8215

Lumini, A. & Nanni, L. (2006). An advanced multi-modal method for human authentication featuring biometrics data and tokenised random numbers. *Neurocomputing*, Vol.69, No.13-15, (August 2006), pp. 1706−1710, ISSN 09252312

Lumini, A. & Nanni, L. (2007). An improved BioHashing for human authentication. *Pattern Recognition*, Vol.40, No.3, (March 2007), pp.1057−1065, ISSN 0031-3203

Maio, D. & Nanni, L. (2005). Multihashing, human authentication featuring biometrics data and tokenized random number: A case study FVC2004. *Neurocomputing*, Vol.69, No.1-3, (December 2005), pp. 242−249, ISSN 09252312

Mihailescu, P. (2007). The fuzzy vault for fingerprints is vulnerable to brute force attack,In: *Computer Vision and Pattern Recognition,* 22.08.2007, Available from:
http://arxiv.org/abs/0708.2974v1

Nandakumar, K. Jain, A. & Pankanti, S. (2007). Fingerprint-Based fuzzy vault: Implementation and performance. *IEEE Trans on Information Forensics and Security*, Vol.2, No.4, (November 2007), pp. 744−757, ISSN 1556-6013

Nanni, L. & Lumini, A. (2006). Empirical tests on BioHashing. *Neurocomputing*, Vol.69, No.16-18, (Octorber 2006), pp.2390−2395, ISSN 09252312

Nanni, L. & Lumini, A. (2008). Random subspace for an improved BioHashing for face authentication. *Pattern Recognition Letters*, Vol.29, No.3, (February 2008), pp. 295−300, ISSN 01678655

Nyang, D. & Lee, K. (2007). Fuzzy Face Vault. How to implement fuzzy vault with weighted features. In: *Proceedings of the Universal Access in HCI,(HCII 2007)*, Stephanidis, C, pp.491-496, Springer Berlin, ISBN 978-3-540-73278-5, Heidelberg, Germany

Ratha, N. Connell, J. & Bolle RM. (2001).An analysis of minutiae matching strength, In: *Audio and Video-Based Biometric Person Authentication,* Bigun, J. & Smeraldi, F, pp. 223−228, Springer Berlin, ISBN 978-3-540-42216-7, Heidelberg, Germany

Ratha, N. Connell, J. Bolle, R. & Chikkerur, S. (2006). Cancelable biometrics: A case study in fingerprints, *Proceedinds of the 18th Int'l Conf. on Pattern Recognition (ICPR 2006)*, ISBN 1051-4651, HongKong, September 2006

Ratha, N. Chikkerur, S. Connell, J. & Bolle, R. (2007). Generating cancelable fingerprint templates. *IEEE Trans on Pattern Analysis and Machine Intelligence*, Vol.29, No.4, (April 2007), pp.561−572, ISSN 0162-8828

Scheirer, W. & Boult, T. (2007). Cracking fuzzy vaults and biometric encryption, *Proceedings of Biometrics Symposium,* ISBN 978-1-4244-1549-6, Colorado, USA, September 2007

Soutar, C. Roberge, D. Stoianov, A. Gilroy, R. & Vijaya, K. (1999). Biometric encryption,In: *ICSA Guide to Cryptography*, McGraw-Hill, Available from
http://www.bioscrypt.com/assets/Biometric_Encryption.pdf

Sutcu, Y. Li, Q. & Memon, N. (2007). Protecting biometric templates with sketch: Theory and practice. *IEEE Trans on Information Forensics and Security*, Vol.2, No.3, (August 2007), pp.503−512, ISSN 1556-6013

Tian, J. & Yang X. (2005).*Biometric Recognition Theory and Application*, Publishing House of Electronics Industry, ISBN 9787302184195 ,Beijing,China

Tong, V. Sibert, H. Lecoeur, J. & Girault, M. (2007). Biometric fuzzy extractors made practical: A proposal based on FingerCodes. In: *Proceedings of the ICB 2007,* Lee SW, Li SZ, pp. 604−613, Springer Berlin, ISBN 978-3-540-74548-8, Heidelberg, Germany

Tulyakov, S. Farooq, F. Govindaraju, V. (2005). Symmetric hash functions for fingerprint minutiae. In: *Pattern Recognition and Image Analysis*, Singh, S. Singh, M. Apte, C. & Perner, P, pp.30-38, Springer Berlin, ISBN 978-3-540-28833-6, Heidelberg, Germany

Tulyakov, S. Farooq, F. Mansukhani, P. & Govindaraju, V. (2007). Symmetric hash functions for secure fingerprint biometric systems. *Pattern Recognition Letters*, Vol.28, No.16, (December 2007), pp. 2427−2436, ISSN 01678655

Uludag, U. Pankanti, S. & Jain, A. (2005). Fuzzy Vault for Fingerprints. In: *Audio- and Video-Based Biometric Person Authentication,* Kanade T, Jai AK, Ratha NK, pp. 310−319, Springer Berlin, ISBN 978-3-540-27887-0, Heidelberg, Germany

Wang, XM. & Zhang, JS. (2007). Secure and Efficient Pseudorandom Bit Generator for Chaotic Stream Ciphers. *Chinese Physics Letters*, Vol.24, No.5, (feburary 2007), pp.1166−1169, ISSN 0256-307X

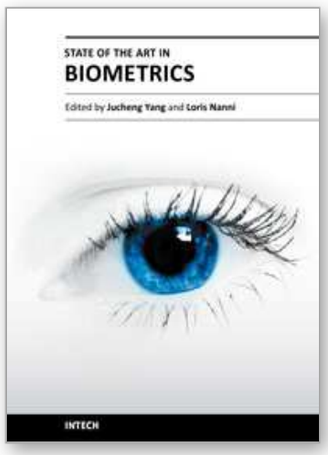
Wang, XM. Zhang, JS. Zhang, WF. & Khan, MK. (2006). Security Improvement on the Timestamp-based Password Authentication Scheme Using Smart Cards, *Proceedings of IEEE International Conference on Engineering of Intelligent Systems*, Islamabad, April 2006.

Wang, XM. Zhang, WF. Zhang, JS. Khan, MK. (2007). Cryptanalysis and Improvement on Two Efficient Remote User Authentication Schemes Using Smart Cards, *Computer Standards & Interfaces*, vol.29, No.5, (July 2007), pp.507-512, ISSN 0920-5489.

Wang, XM. Zhang, WF. (2008). An efficient and secure biometric remote user authentication scheme using smart cards, *IEEE Pacific-Asia Workshop on Computational Intelligence and Industrial Application*, Wuhan China, December 2008.

Wang, Y. & Plataniotis, K. (2008). Fuzzy vault for face based cryptographic key generation, *Proceedings of the Biometrics Symposium,* ISBN 978-1-4244-1549-6, Baltimore, January 2008

Zhang, F. Feng, D. & Sun, Z. (2008). An iris authentication scheme based on fuzzy extractor. *Journal of Computer Research and Development*, Vol.45, No.6, (December 2007), pp.1036−1042, ISSN 100021239



State of the art in Biometrics

Edited by Dr. Jucheng Yang

ISBN 978-953-307-489-4
Hard cover, 314 pages
Publisher InTech
Published online 27, July, 2011
Published in print edition July, 2011

Biometric recognition is one of the most widely studied problems in computer science. The use of biometrics techniques, such as face, fingerprints, iris and ears is a solution for obtaining a secure personal identification. However, the â€œoldâ€ biometrics identification techniques are out of date. This goal of this book is to provide the reader with the most up to date research performed in biometric recognition and descript some novel methods of biometrics, emphasis on the state of the art skills. The book consists of 15 chapters, each focusing on a most up to date issue. The chapters are divided into five sections- fingerprint recognition, face recognition, iris recognition, other biometrics and biometrics security. The book was reviewed by editors Dr. Jucheng Yang and Dr. Loris Nanni. We deeply appreciate the efforts of our guest editors: Dr. Girija Chetty, Dr. Norman Poh, Dr. Jianjiang Feng, Dr. Dongsun Park and Dr. Sook Yoon, as well as a number of anonymous reviewers

INTECH
open science | open minds

InTech Europe
University Campus STeP Ri
Slavka Krautzeka 83/A
51000 Rijeka, Croatia
Phone: +385 (51) 770 447
Fax: +385 (51) 686 166
www.intechopen.com

InTech China
Unit 405, Office Block, Hotel Equatorial Shanghai
No.65, Yan An Road (West), Shanghai, 200040, China
中国上海市延安西路65号上海国际贵都大饭店办公楼405单元
Phone: +86-21-62489820
Fax: +86-21-62489821

IntechOpen