Sept. 2006, Vol.21, No.5, pp.861–870 J. Comput. Sci. & Technol.

Fingerprint-Based Identity Authentication and Digital Media Protection in Network Environment

Jie Tian[1] (田 捷), Liang Li[1,2] (李 亮), and Xin Yang[1] (杨 鑫)

[1] *Center for Biometrics and Security Research, Key Laboratory of Complex Systems and Intelligence Science Institute of Automation, Chinese Academy of Sciences, Beijing 100080, P.R. China*

[2] *Graduate University of the Chinese Academy of Sciences, Beijing 100039, P.R. China*

E-mail: tian@ieee.org; liliang@fingerpass.net.cn; yx@fingerpass.net.cn

Received June 2, 2006; revised August 22, 2006.

Abstract Current information security techniques based on cryptography are facing a challenge of lacking the exact connection between cryptographic key and legitimate users. Biometrics, which refers to distinctive physiological and behavioral characteristics of human beings, is a more reliable indicator of identity than traditional authentication system such as passwords-based or tokens-based. However, researches on the seamless integration biometric technologies, e.g., fingerprint recognition, with cryptosystem have not been conducted until recent years. In this paper, we provide an overview of recent advancements in fingerprint recognition algorithm with a special focus on the enhancement of low-quality fingerprints and the matching of the distorted fingerprint images, and discuss two representative methods of key release and key generation scheme based on fingerprints. We also propose two solutions for the application in identity authentication without trustworthy third-party in the network environment, and application in digital media protection, aiming to assure the secrecy of fingerprint template and fingerprint-based user authentication.

Keywords biometrics, fingerprint recognition, cryptosystem, techniques and algorithms, information security

1 Introduction

In this age of networking, communication and mobility, biometric technologies are being used more and more widely as an effective means for the protection of data abuse and identity theft. Biometric technologies vary in complexity, capabilities, and performance and can be used to verify or establish a person's identity. Leading biometric technologies include fingerprint recognition, facial recognition, hand geometry, iris recognition, retina recognition, signature recognition and speaker recognition. Fingerprint recognition is one of the best known and most widely used biometric technologies. Automated Fingerprint Identification System (AFIS) has been commercially available since the early 1970s, and currently covers 44% of the biometrics market in 2006[1].

Significant improvements in fingerprint recognition technology have been achieved, though there are still many challenging tasks in terms of algorithms and applications. In the algorithm category, two of them are matching of non-linear distorted fingerprints and enhancement of low quality fingerprints. According to Fingerprint Verification Competition 2004 (FVC2004)[2], they are particularly insisted on: distortion, dry and wet fingerprints. Distortions in fingerprint images are caused by two main reasons, namely a 3D-2D warping process and a different non-orthogonal pressure in the acquisition. Low quality fingerprints are due to the changes of skin condition, climate, and on-site environment. How to cope with non-linear distortion and low quality fingerprints in the matching process is still a difficult task.

In the application category, one of the challenging tasks is the seamless combination of fingerprint biometric and information security infrastructure such as Public Key Infrastructure (PKI). In cyber-logical world, PKI can ensure that trusted relationships established and maintained with confidentiality, integrity, non-reputation and authentication based on cryptography. However, both PKI and other information security techniques fret about the problem of lacking the exact connection between cryptographic key and legitimate users. Because symmetric/asymmetric keys are long and random, and difficult to memorize, they are often stored somewhere (e.g., a smart card or a USB token) and accessed by using some alternative authentication, e.g., password. Thus, the identity in cyber-logical world is just verified by password. These limitations of traditional passwords can be ameliorated by the incorporation of fingerprint authentication techniques. The combination of fingerprint biometric and information security infrastructure is promising, but for current state-of-the-art technology, how to bridge the gap between fuzziness of fingerprint biometric and exactitude of cryptography and how to reach the point at which basic performance can be acceptably deployed still requires extensive and deep research.

This paper reviews the recent advancements in fingerprint recognition algorithm and in fingerprint-based

Regular Paper

Supported by the National Science Fund for Distinguished Young Scholars of China under Grants No. 60225008, the National Natural Science Foundation of China under Grants No. 60332010 and No. 60575007, the Young Scientists' Fund of National Natural Science Foundation of China under Grant No.60303022, the Natural Science Foundation of Beijing under Grant No.4052026, and the 242 National Information Security Plan.

cryptography, and then proposes two fingerprint cryptosystems for networked identity authentication without trustworthy third-party and for digital media protection respectively. In Section 2, we describe and compare the algorithms of enhancement of low quality fingerprints, and enumerate different methods for fingerprints matching and present the advancement in dealing with the distorted fingerprints. We also introduce the performance evaluation of these fingerprint recognition algorithms. In Section 3, we summarize various methods that combine fingerprint features with cryptographic keys. In Section 4, two implementation schemes of networked identity authentication and fingerprint-based digital media protection are proposed. A brief discussion and conclusion are presented in Section 5.

2 Fingerprint Recognition Algorithm

AFIS is based on the comparison between feature templates (one is from enrolled fingerprint and the other is from test fingerprint), then it makes a decision whether these two templates come from the same fingerprint or not. Fig.1 shows a typical structure of the recognition system. Fingerprint matching algorithms can be broadly classified as being minutiae-based and correlation-based[4]. The minutiae-based techniques attempt to align two minutiae sets to determine the total number of matched minutiae pairs. The correlation-based techniques, on the other hand, compare the global patterns of ridges and furrows to see if the ridge structures in the two fingerprint images align. Approximately 80% of vendors base their algorithms on the extraction of minutiae points. Other techniques are based on extracting global ridge patterns. The performance of both the minutiae-based methods and the correlation-based ones are affected by non-linear distortion and low quality fingerprint images.

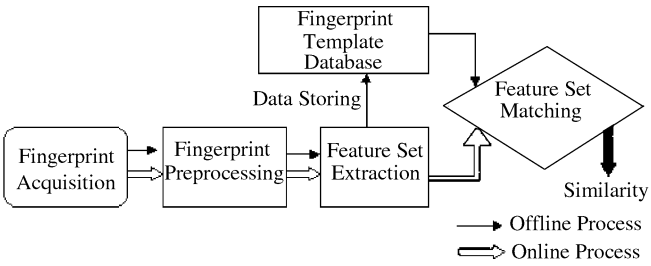


Fig.1. Typical structure of AFIS.

2.1 Enhancement of Low-Quality Fingerprints

The quality of fingerprint image degrades due to the changes of skin condition, climate, and on-site environment during the image acquisition process. Fig.2 shows four examples of low quality fingerprints. Generally, the adaptability of the AFIS relies on the enhancement of poor quality fingerprint images available or not. Such enhancement is so important that it seriously affects the performance of the recognition system. It is one of the most crucial and difficult tasks for fingerprint recognition.

Fig.2. Four examples of low quality fingerprints. (a) Too dry. (b) Too wet. (c) With many Scars. (d) Molted.

Image quality analysis is a critical component of a fingerprint live scan workstation. AFIS rejects a certain percentage of submitted fingerprint images because they fail to meet the criteria of the image quality. Failure to extract minutiae points is usually attributed to poor ridge flow, poor contrast and brightness in the image. Shen *et al.*[5] proposed a Gabor-feature based method to determine the quality of the fingerprint images.

Many standard and special image enhancement techniques have been developed for poor quality images. Shi *et al.*[6] proposed a new feature Eccentric Moment to locate the blurry boundary using the new block feature of clarified image for segmentation. Zhou *et al.*[7] proposed a model-based algorithm which is more accurate and robust to dispose the degraded fingerprints. They compute the coarse orientation field by traditional methods, and approximate the real orientation with smooth curves.

In order to enhance the poor quality prints efficiently, we must incorporate a robust ridge filter in respect of the quality of input fingerprint images. Lin *et al.*[8] assume that the parallel ridges and valleys exhibit some ideal sinusoidal-shaped plane waves associated with some noises, which cannot treat the poor quality images. Yang *et al.*[9] specify parameters deliberately through some principles instead of experience, preserving fingerprint image structure and achieving image enhancement consistency. This algorithm solves the problem of poor enhancement led by false estimation of local ridge direction. Zhu *et al.*[10] follow Lin's algorithm, but use a circle support filter and tuned the filter's frequency and size differently. This scheme rapidly enhances the fingerprint image and effectively overcomes the blocky effect. Mohammad *et al.*[11] propose a method using decimation-free directional filter bank (DFB) structure to improve the poor quality fingerprints.

These methods perform local estimation and contextual filtering in a dispersed manner, which often result in not only blocky artifacts but also poor estimation in local image characteristics. Another type of mechanisms based on nonlinear diffusion is proposed to solve the problem. Xie *et al.*[12] adapt an image structure tensor merging both the coherence enhancement diffusion[13] for processing flow-like pattern and

the forward and backward enhancement diffusion[14] for sharpening ridges. These algorithms utilize the global features of the ridge flow direction to restore the disconnection caused by the poor quality of images and obtain good performance.

Compared with the uncertainty of local ridge information, the global features can be preserved accurately in the attained fingerprint images. Therefore, many Fourier-domain based ridge filters are presented for the low-quality fingerprint images. Willis *et al.*[15] propose a Fourier domain based method that boosts up a low quality fingerprint image by multiplying the frequency spectrum by its magnitude. Zhu *et al.*[16] combine the two methods mentioned above by multiplying each filter vector with well designed weights to form a new filter vector. In addition, it applies a top-down iteration technique which can improve the robustness of the method.

2.2 Distorted Fingerprints Matching

How to cope with non-linear distortion of fingerprint impressions in the matching process is a challenging task. Distortions of fingerprints seriously affect the accuracy of almost all matching algorithm no matter the minutiae-based or the correlation-based. There are two main reasons contributed to the fingerprint distortion[30]. First, the acquisition of a fingerprint is a 3D-2D warping process[17,18]. The fingerprint captured with different contact centers usually results in different warping mode. Second, distortion will be introduced by the non-orthogonal pressure exert on the sensor. Fig.3 indicates two examples of large distortion between fingerprints.

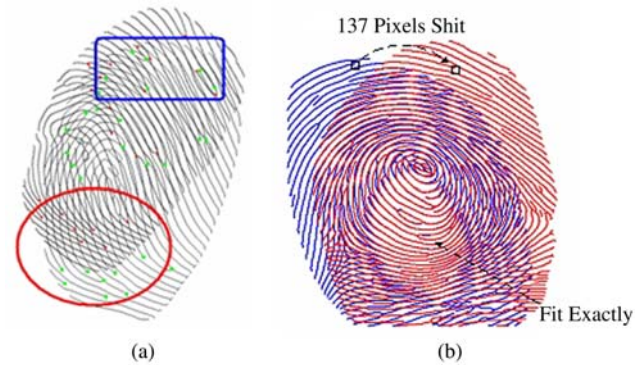


Fig.3. Two examples of large distortion. (a) In the rectangle region, the corresponding minutiae are approximately overlapped. While in the ellipse region, the maximal vertical difference of corresponding minutiae is above 100 pixels. (b) In the center region, the corresponding minutiae are approximately overlapped. While in the upper region, the maximal horizontal difference of corresponding minutiae is 137 pixels.

In order to improve the matching performance, some algorithms have been developed to deal with the non-linear distortion in fingerprints. Ratha *et al.*[19] propose a method to measure the forces and torques on the scanner directly, which prevents capturing with the aid of special hardware when excessive force is applied to the scanner. Dorai *et al.*[20] propose a method to detect and estimate the distortions occurred in fingerprint videos. But those two mentioned methods do not work with the collected fingerprint images. Maio and Maltoni *et al.*[21] propose a plastic distortion model to cope with the nonlinear deformations characterizing fingerprint images taken from on-line acquisition sensors. This model helps to understand the distortion process. However, it is hard to automatically and reliably estimate the parameters due to the insufficient and uncertain information. Lee *et al.*[22] addressed a minutiae-based fingerprints matching algorithm using distance normalization and local alignment to deal with the non-linear distortion. However rich information of the ridge/valley structure is not used and the matching performance is moderate. To improve the matching accuracy, Senior *et al.*[23] propose a method to convert a distorted fingerprint image into an equally ridge spaced fingerprint before matching. However, the assumptions of equal ridge spacing is less likely to be true for fingerprints — particularly in the place where ridges break down, e.g., around minutiae or near the edge of the fingerprint. Watson *et al.*[24] propose a method to improve the performance of fingerprint correlation matching by distortion tolerant filters. The improvement is achieved by multiple training fingerprints and a distortion-tolerant MACE filter. However, the algorithm is difficult to realize on line. Vajna *et al.*[25] also propose a method based on triangular matching to cope with the strong deformation of fingerprint images, which graphically demonstrate that the large cumulative effects can be a result of the small local distortions. Bazen *et al.*[26] employ a thin-plate spline model to describe the non-linear distortions between the two sets of possible matching minutiae pairs. By normalizing the input fingerprint with respect to the template, this method is able to perform a very tight minutiae matching. Ross *et al.*[27] use the average deformation computed from fingerprint impressions originated from the same finger based on thin plate spline model to cope with the non-linear distortions. Chen *et al.*[18] introduced a novel fingerprint verification algorithm based on the determination and inspection of the *registration pattern* (*RP*) between two fingerprints. The algorithm first coarsely aligns two fingerprints. Then determines the *possible RP* by optimally registered each part of the two fingerprints. Next, inspects the *possible RP* with a *genuine RP space*. If the *RP* makes a genuine one, a further fine matching is conducted. Different from the above mentioned methods, Chen *et al.*[28] propose an algorithm based on fuzzy theory to deal with the non-linear distortion in fingerprint images. The local topological structure matching was introduced to improve the robustness of global alignment. And a similarity computing method based on fuzzy theory, namely normalized fuzzy similarity measure, is conducted to compute the similarity be-

tween the templates and input fingerprints. Experimental results indicate that the algorithm works well with the non-linear distortions. For deformed fingerprints, the algorithm gives considerably higher matching scores compared with conventional matching methods. He *et al.*[29] make some modifications based on global comprehensive similarity which is more suitable for limited memory AFIS.

2.3 Performance Evaluation

In the last decade, with the rapid development of fingerprint recognition system, it is urgent to establish a common benchmark in this field. Participators could evaluate their algorithms on this common benchmark, compare the performance and provide an overview of the state-of-the-art in fingerprint recognition. There are two internationally authorized and accredited evaluation, namely Fingerprint Verification Competition (FVC) and Fingerprint Vendor Technology Evaluation (FpVTE[31]).

FVC is organized by the Biometric System Lab of University of Bologna, the Pattern Recognition and Image Processing Laboratory of Michigan State University and San Jose State University. It was held three times in 2000, 2002 and 2004. FVC 2006[3] will be hold in October 31, 2006, and the result of this competition will be published in January, 2007. The aim of FVC is to track latest advancements in fingerprint verification for both academia and industry, and to benchmark the state-of-the-art technology in fingerprint recognition. FVC has established a common benchmark allowing developers to compare their algorithms unambiguously, and has provided an overview of the most recent advancements in fingerprint recognition.

The Fingerprint Vendor Technology Evaluation (FpVTE) 2003 is an independently administered technology evaluation for fingerprint matching, identification, and verification systems. FpVTE 2003 has been conducted by the National Institute of Standards & Technology (NIST) on behalf of the Justice Management Division (JMD) of the U.S. Department of Justice. FpVTE has been designed to assess the capability of fingerprint systems to meet requirements for both large-scale and small-scale in real world applications. FpVTE 2003 consists of multiple tests performed with the combinations of fingers (e.g., single fingers, two index fingers, four to ten fingers) and different types and qualities of operational fingerprints (e.g., flat livescan images from visa applicants, multi-finger slap livescan images from present-day booking or background check systems, or rolled and flat inked fingerprints from legacy criminal databases).

It is necessary to analyze several performance metrics to determine the strengths and weaknesses of each algorithm. Two frequently adopted metrics are false match rate (FMR) and false nonmatch rate (FNMR). A false match occurs when a system incorrectly matches an invalid identity, and FMR is the probability of invalid individuals being wrongly accepted. A false nonmatch occurs when a system rejects a valid identity, and FNMR is the probability of valid individuals being wrongly rejected. For an AFIS, FMR reflects the security level and FNMR the convenience level. Clearly, the FMR must be very low to provide any confidence in the technology, and the FNMR must be sufficiently low so that users will not abandon the technique due to inconvenience. The FMR and FNMR are inversely related, and if systems were perfect, both error rates would be zero. However, because fingerprint recognition algorithms cannot identify individuals with 100% accuracy, a trade-off exists between the two rates.

Equal error rate (EER), an additional metric derived from FMR and FNMR, is often used to describe the accuracy of recognition algorithms. EER refers to the point at which FMR equals FNMR. EER can be used to give a threshold independent performance measure. The lower the EER, the better the system's performance, because the total error rate which is the sum of the FAR and the FRR at the point of the EER decreases. Setting a system's threshold at its EER will result in the probability that a person is falsely matched equaling the probability that a person is falsely not matched. However, this statistic tends to oversimplify the balance between FMR and FNMR, because in most real-world applications the need for security is not identical to the need for convenience.

FMR, FNMR and EER are three key indicators in both FVC and FpVTE to evaluate the performance of a fingerprint recognition algorithm. In addition to these metrics, FVC and FpVTE also adopt other performance metrics such as rate of rejecting to enroll (REJENROLL), rate of rejecting to match (REJNGRA and REJNIRA), ZeroFMR and ZeroFNMR from accuracy aspect, and average match time and enroll time, maximum memory allocated for enrollment and for match, average and maximum template size from efficiency aspect.

3 Fingerprint Keys

Biometrics and cryptography are considered as two potentially complementary security technologies and it is intuitive to link a biometric template with a cryptographic key. The security of a cryptographic system relies on the security of its cryptographic key in terms of Kerckhoffs Principle which was first stated by Auguste Kerckhoffs in 1883. In modern cryptographic system, the keys are secure enough to ensure confidentiality, integrity, non-reputation of data for practical applications, whereas they cannot establish the exact connection with authorized users. The basic expectation of biometric-based key is that the biometric component performs user authentication, while the other components of cryptographic system can still work effectively. Biometric signal or template itself, on the other hand, must be kept

secretly for the sake of security and privacy. They may be used in other applications once the biometric templates are stolen from one application, thus making different applications vulnerable to the attack and compromising the security of systems. Furthermore, biometric template leakage is an important privacy issue because biometrics cannot be changed and reissued which are different from secret keys.

By the means of integration biometrics into cryptographic keys, a biometric-based key method can be classified into key release scheme and key generation scheme, see Fig.4. There have been a number of research efforts addressing the issues based on fingerprint[32−35], iris[36], face[37], voice[38], signature[39], keystroke[40], and feature extraction techniques[41]. In the following, we will briefly introduce two representative methods of key release and key generation scheme, respectively. Both methods aim to solve the problem of fingerprint authentication within a cryptographic framework and the problem of fingerprint template protection.

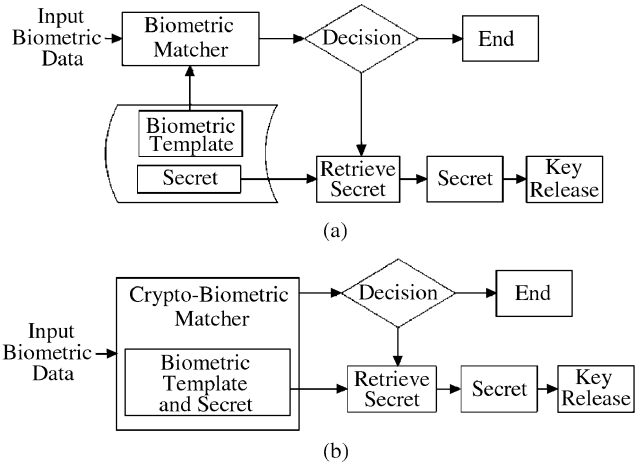


Fig.4. Two modes of combining biometrics with cryptography[35]. (a) Key release. (b) Key generation.

3.1 Key Release Scheme

The straightforward idea of fingerprint key release scheme is to combine a fingerprint template with a cryptographic key via a specific transformation or link algorithm. If an input fingerprint sample matches with the enrolled template successfully, the cryptographic key is released, otherwise, the key would not be released by the system. Thus, in such a scheme, the key release process is "wrapped" by fingerprint authentication, and user authentication and key release are completely decoupled. This method can alternate password authentication and almost make no change on current cryptographic system, but the template is not secure.

Soutar *et al.*[32] propose a practical key release scheme using correlation-based fingerprint matching algorithm and has commercialized this method into a product — Bioscrypt. Based on Fourier transformation theory, this algorithm first creates a correlation filter function $H(u)$ with several fingerprint images of a finger. $H(u)$ is designed to provide a tradeoff between discrimination capability and distortion tolerance. The algorithm then computes an output array $c_0(x)$, which is obtained by the correlation of the training fingerprint images with $H(u)$. In order to maximize the security of the templates, the complex conjugate of the phase component of $H(u)$, $e^{-i\varphi(H(u))}$ is multiplied with a randomly generated phase-only array $R(u)$ of the same size, resulting in $H_{stored}(u)$ and the discard of the magnitude of $H(u)$. In order to tolerate the variation in fingerprint samples, a given or randomly generated N-bit cryptographic key k_0 is linked with c_0 by using error correcting codes. This results in a lookup table LT. S bits of $H_{stored}(u)$ are encrypted by cryptographic key k_0 and hashed by some standard hashing function, e.g., SHA-1, forming an identification code id_0. Finally, $H_{stored}(u)$, LT and id_0 were stored into database as the template of the enrolled user. It is clear that this template is secure because neither fingerprint image nor cryptographic key can be retrieved from the template.

Verification process is symmetric with enrollment process with respect to the liking and the retrieving of the digital key. The user inputs one or more fingerprint images to combine with $H_{stored}(u)$ in template of this user retrieved from database. The correlation output $c_1(x)$ is then produced and used to retrieve a cryptographic key k_1 by using lookup table LT. Validate k_1 by creating a new identification code, id_1, and comparing it with id_0. If $id_0 = id_1$, k_1 is validated and released into the system, otherwise, no key is released into the system. Bioscrypt appears a promising idea that locks a cryptographic key in fingerprint template securely. Unfortunately, the FMR and FNMR are not reported in published literature.

3.2 Key Generation Scheme

Uludag *et al.*[35] propose a fingerprint key generation implementation called the fuzzy vault which is firstly introduced by Juels *et al.*[34] This construct aims to secure critical data (e.g., secret encryption key) with the fingerprint data in a way where only the authorized user can access the secret by providing the valid fingerprint. Here we describe this scheme briefly in two stages: encoding stage and decoding stage.

Encoding Stage. Assume that S is any secret data needed to be protected (e.g., a cryptographic key), and it is a 56-bit random stream in current implementation. The fuzzy vault first puts some structure (Cyclic Redundancy Check is adopted in proposed scheme) into secret S to identify the correct secret S. So 72-bit SC data is produced by concatenating 16-bit CRC data form the secret data S. SC is used to represent a polynomial with 8 coefficients, with degree $D = 7$. Hence, $p(x) = c_7x^7 + c_6x^6 + \cdots + c_1x + c_0$. SC is divided into non-overlapping 9-bit segments and each segment is declared as a specific coefficient, c_i, $i = 0, 1, 2, \ldots, 7$.

Assume that there are N unique template minutiae, $x_1, x_2, \ldots, x_N$, the author finds a set of ordered pairs $G = \{(x_1, p(x_1)), (x_2, p(x_2)), \ldots, (x_N, p(x_N))\}$. A second set of ordered pairs, called the chaff set C, is then generated from M random x-coordinates $c_1, c_2, \ldots, c_N$ (distinct from $x_1, x_2, \ldots, x_N$) such that $C = \{(c_1, d_1), (c_2, d_2), \ldots, (c_N, d_N)\}$ and $d_i \neq p(c_i)$, $\forall i$. The union of these two sets $G \cup C$ is randomized to produce vault set *VS*.

Decoding Stage. A user inputs his fingerprint and a number of minutiae points are extracted. Given N query minutiae (Q) $x_1^*, x_2^*, \ldots, x_N^*$, the points to be used in polynomial reconstruction are found by comparing x_i^*, $i = 1, 2, \ldots, N$, with the abscissa values of the vault V, namely ν_l, $l = 1, 2, \ldots, (M + N)$: if any x_i^*, $i = 1, 2, \ldots, N$ is equal to ν_l, $l = 1, 2, \ldots, (M + N)$, the corresponding vault point (ν_l, w_l) is added to the list of points to be used. Assume that this list has K points, where $K \leqslant N$. Now, for decoding a degree D polynomial, $(D+1)$ unique projections are necessary. All possible combinations of $(D+1)$ points among the list with size K are considered, resulting in $\binom{K}{D+1}$ combinations. For each of these combinations, the Lagrange interpolation polynomial is constructed. For a specific combination set given as $L = \{(v_1, w_1), (v_2, w_2), \ldots, (v_N, w_N)\}$, the corresponding polynomial is reconstructed. The coefficients of the reconstructed polynomial are mapped back to the decoded secret SC^*. If the CRC remainder on SC^* is not zero, there are errors. If the remainder is zero, with a very high probability, there are no errors. For the latter case, SC^* is segmented into two parts: the first 56 bits denote S^* while the remaining 16 bits the CRC data. Finally, the system outputs S^*. If the minutiae list of input fingerprint overlaps with the minutiae list of template in at least $(D+1)$ points, for some combinations, the correct secret will be decoded, namely, $S^* = S$ will be obtained. This denotes the desired outcome when the query and template fingerprints are from the same finger. This work is reported to derive a 56-bit fingerprint key with 14% false rejection rate.

4 Two Implementations of Fingerprint Cryptosystem

In this section, we propose two fingerprint coding schemes used for networked identity authentication and digital media protection respectively. First, both two schemes extract the global ridge pattern of fingerprints by using Fourier-Mellin Transformation (FMT), which is rotation and translation invariant. Second, to better incorporate with cryptography, we discretize the extracted feature and code them into binary bit stream by using two different ways. Finally, the two coding schemes are implemented for two applications, i.e., networked identity authentication without trustworthy third-party, and digital media protection.

4.1 Background of FMT Theory

Fourier-Mellin Transformation is an invariant transform in rotation, translation and scale. FMT is a powerful tool in applications such as image recognition and image registration applications. Fourier Transformation itself can provide the invariant results for translation in Cartesian coordinates and rotation by changing the Cartesian coordinate system to Polar coordinate system; Mellin Transformation carries out the invariance in scale necessary to obtain the resulting spectrum.

If an image $f_2(x, y)$ is a translated, rotated and scaled replica of $f_1(x, y)$ with translation (x_0, y_0), rotation θ_0 and uniform scale factor σ, then

$$f_2(x, y) = f_1(\sigma(x\cos\theta_0 + y\sin\theta_0) - x_0, \sigma(-x\sin\theta_0 + y\cos\theta_0) - y_0). \quad (1)$$

According to the Fourier Transform property, transforms of f_1 and f_2 are related by

$$F_2(u, v) = \exp(-j2\pi(ux_0 + vy_0)) \times \sigma^{-2}(F_1(\sigma^{-1}(u\cos\theta_0 + v\sin\theta_0), \sigma^{-1}(-u\sin\theta_0 + v\cos\theta_0)). \quad (2)$$

With magnitudes F_1 and F_2, rotation can be deduced by representing the rotation with polar coordinates, i.e., in polar representation

$$F_{2p}(\theta, r) = \sigma^{-2}F_{1p}(\theta - \theta_0, r/\sigma). \quad (3)$$

Scaling can be further deduced to a translation by using logarithmic for the radial axis, thus

$$F_{2pl}(\theta, \sigma) = \sigma^{-2}F_{1pl}(\theta - \theta_0, \log(r) - \log(\sigma)). \quad (4)$$

From (4), we can find that scale σ and rotation angle θ_0 can be deduced by using the second Fourier transformation (ignoring σ^{-2}). Let M_1 and M_2 be the magnitudes of FT of F_{1pl} and F_{2pl}, their Fourier magnitudes spectra in polar representation are related by

$$M_1(\xi, \eta) = M_2(\xi, \eta). \quad (5)$$

The above equation implies that invariant features of a pair of images are exploited by FMT and can be used for image recognition. By using phase correlation technique, scale, angle information and translational movement can be retrieved, and can be used for image registration.

In addition to that, the linear property of FMT feature provides a convenient way to fuse multiple fingerprint templates into one reference template T_{ref}, which can be formulated as follows:

$$T_{ref} = \frac{1}{n}\sum_{i=1}^{n} T_i \quad (6)$$

where n is the number enrolled fingerprints of one finger.

Producing T_{ref} from multiple enrolled fingerprint images could relax variability that occurs during the acquisition stage.

4.2 Identity Authentication in Network Environment

There are three general ways to identify yourself to a computer system, based on what you know, what you have, or who you are. "what you know" approaches such as passwords and PINs are low-reliability techniques because they can be lost, stolen, or guessed. "What you have" technologies such as RFID cards and e-tokens also can be stolen. In network environment, a "dual factor" authentication scheme that pairs a what-you-have technique (e-token) with a what-you-know technique (password) is usually implemented to improve the security.

Current identity authentication in network environment primarily focuses on Public Key Infrastructure (PKI) or Identity Based Encryption (IBE). However, these techniques authenticate user's identity relying on one or many trustworthy third-party(s) that require(s) database running online, therefore the whole system is vulnerable and in low efficiency[45]. In this section, we propose a networked identity authentication scheme that combines what-you-have (USB token) with who-you-are (fingerprint biometric). This is designed for user verification in secure communication of network environment without trustworthy third-party. This scheme comprises of fingerprint feature coding, dual-factor matching and fingerprint certificate technique.

BioHash[42] is used here to discretize the fingerprint feature, which is based on iterated inner products between tokenized pseudo-random number and magnitude spectrum of FMT. The discretization process is described as follows.

1) Magnitude spectrum of FMT: $\Gamma \in \mathbb{R}^M$, with M, the magnitude spectrum dimension.

2) Use token to generate a basis set of pseudo random number, $\{r_i \in \mathbb{R}^M | i = 1, 2, \ldots, m\}$.

3) Apply the Gram-Schmidt process to transform the basis set into an orthonormal set of matrices $\{r_{\perp i} \in \mathbb{R}^M | i = 1, 2, \ldots, m\}$.

4) Compute $\{\langle \Gamma | r_{\perp i} \rangle \in \mathbb{R} | i = 1, 2, \ldots, m\}$ where $\langle \cdot | \cdot \rangle$ is inner product operation.

5) Binarize m bits the inner product into $\{b_i \in 2^m | i = 1, 2, \ldots, m\}$ in terms of a pre-specified threshold τ.

Fingerprint certificate records personal information and fingerprint cipher template of legitimate user, which contains the digital signature of the authority as well. These certificates can be downloaded and accessed by the other users. The cipher template of live-scan fingerprints can match with the one stored in certificate on the occasion of identity authentication. Therefore the combination of cipher template matching technique and fingerprint certificate technique implement identity authentication without trustworthy third-party participating online, and the fingerprint feature is protected reliably at the same time.

The role of the whole system can be abstracted as the authority TA, user A and user B. TA is the centre of the whole system which produces and preserves the master key, computes the private key for user and deliver the USB token. In the initialization stage of system, TA sets up a secure communication region and computes the master key and public parameters on hyper-singular elliptic curve. The mathematical theory is based on bilinear Diffie-Hellman problem. In registration stage, users show his legitimate documents to the authority for the application of registration. Then TA sets the harden key of USB token and stores the cipher template of live-scan fingerprint into the token. The public parameters and cryptography functions are stored in the token as well. USB token has the function of plagiary- and temper-resistant, cryptography computation and fingerprint verification. The authority delivers the token to users face to face and produces the fingerprint certificates. On the occasion of secret communication between user A and user B, the message receiver must authenticate the identity of message sender. Assume that A sends message M to B, A computes the communication key K with a bilinear map and the ID of B and then encrypts M and fingerprint cipher template with K. A sends the encrypted message and cipher template to B together with the hash of the plain text. After the cipher text is received, B matches the received cipher template with fingerprint certificate of A. That is the first round of authentication. Then B computes communication key with private key of B and the ID of A. That is the second round of authentication.

4.3 Digital Media Protection

So far the most efficient method of digital media protection is the encryption with cryptographic key. Thus here we are more concerned about the protection of cryptographic keys of this problem. In traditional cryptography, if the encryption and decryption keys are not identical, the decryption operation will fail and produce useless random data. Because biometric signals or their representations of the same person vary dramatically on site, the issue dealing with the variability of the biometric data within the cryptographic framework is a very challenging problem. A solution to this problem is feature discretization technique and error correcting technique. Magnitude spectrum of FMT is still adopted as a feature to represent a fingerprint.

An overview of the process of Encoding and Decoding is stated below, with reference to Figs.5 and 6.

Encoding:

Step 1. Image preprocessing and Fourier-Mellin transformation.

Locate the reference point of fingerprints and extract the region of interest with size 128×128 by using reference point detection method described in [43], then compute the magnitude image by Fourier-Mellin transformation. Finally the reference template T_{ref} is produced by averaging the magnitudes of spectrum of enrolled fingerprints.

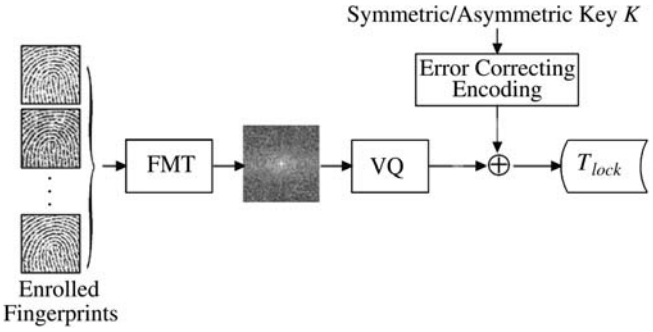


Fig.5. Overview of encoding process.

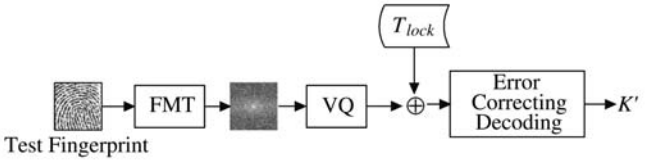


Fig.6. Overview of decoding process.

Step 2. Vector quantization.

Extract a 32×32 centre block of T_{ref} and discretize it into binary bit stream T_{bin} by a predefined partition array. The partition array is trained before vector quantization using k-means clustering.

Step 3. Encoding K with error correcting technique.

Encode the symmetric/asymmetric key K, which encrypts the digital media, by using a two-layer error correction method[38]. The outer layer uses Hadamard code to correct errors at bit level, and the inner layer uses a Reed-Solomon code to correct errors at block level. Whether the two-layer error correcting method can work is based on the experimental proof that bit difference of different fingerprints is about 50%, while that of same fingerprints is about 20%.

Step 4. Locking K with T_{bin}.

Lock encoded K with T_{bin} by XOR operation to produce T_{lock} and then discard K. T_{lock} has perfect secrecy because neither K nor T_{bin} can be derived from T_{lock}.

Step 5. Storing hash value of K and T_{lock}.

Obtain the hash value $H(K)$ of key K with standard hashing function SHA-1, and store it in USB key or other physical token, together with T_{lock}.

Decoding:

Steps 1 and 2 are the same as respective step in encoding process, resulting in T_{bin} of input test fingerprint.

Step 3. Unlocking K and error correction decoding.

Unlock K by XORing T_{lock} with T_{bin} of input test fingerprint and obtain a sample key K'. K' is then decoded with a symmetric order as encoding process.

Step 4. Comparing $H(K)$ and $H(K')$.

If $H(K')$ is identical to $H(K)$, the correct key K' is released to system, otherwise, return error to system. The cryptographic key K can be recovered provided that test fingerprint is sufficiently similar with enrolled fingerprint and bit differences between two binary streams can be corrected by the error correcting method.

4.4 Experiments

In this subsection, the proposed methodologies are evaluated on a fingerprint image database. Here we focus on the performance of discriminating capability and information protection of fingerprint coding scheme. The performance of whole applications is not reported in this paper. The fingerprint image database we used consists of 800 fingerprint images from 100 different fingertips, with 8 samples from each fingertip. These images were captured by SymWave SW6888 swipe-type sensor. This sensor is cost-effective and easy to be integrated in USB tokens or mobile devices. A 128×128 square region centered in the reference point was cropped after core point detection via the method proposed in [43].

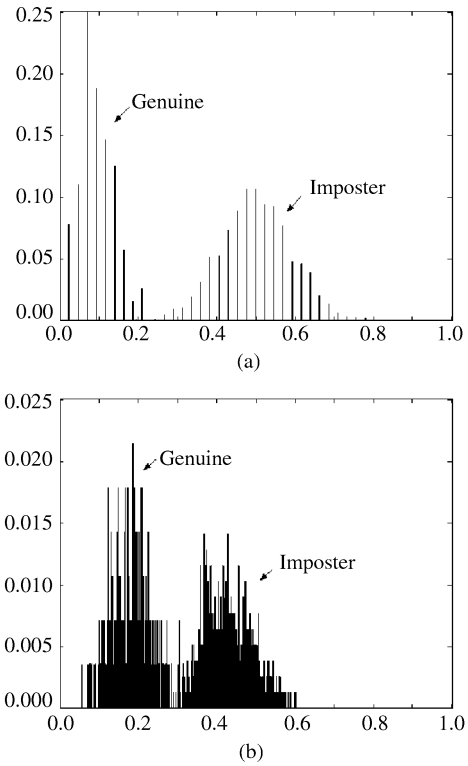


Fig.7. Hamming distance distribution of genuine and imposter population. (a) For *Hash*. (b) For *VQ*.

In the following we denote two coding schemes described in Subsections 4.3 and 4.4 by *Hash* codes and *VQ* codes, respectively. Fig.7 illustrates the genuine and imposter population distribution for *Hash* and *VQ*, respectively. The genuine distribution shows the results when two images of the same fingertip are compared, but when two images come from different fingerprints, the imposter distribution is the outcome. Fig.7(a) shows no overlapping for Hash codes in between two populations. It implies that *Hash* coding scheme have stronger discriminating capability because it incorporates with another authenticating factor-serialized random number sequence. Fig.7(b) shows that *VQ* codes from the

same fingertip disagree in about 15%∼25% of the bits, whereas the disagreement of VQ codes from different fingertip is usually 40%∼60%.

The characteristics of *FAR*, *FRR* and *EER* are illustrated in Fig.8. Note that *Hash* codes obtained $EER = 0\%$ when FMT features are discretized into 128-bit sequence. The *EER* of VQ codes is 2.5%. We used two-layer error correcting method in [36] to correct the error bits of cryptographic keys caused by variations of VQ codes. VQ codes after error correcting obtained $FAR = 0\%$, and the corresponding *FRR* is 9.8%, which is smaller than the *FRR* of previous systems[33,35].

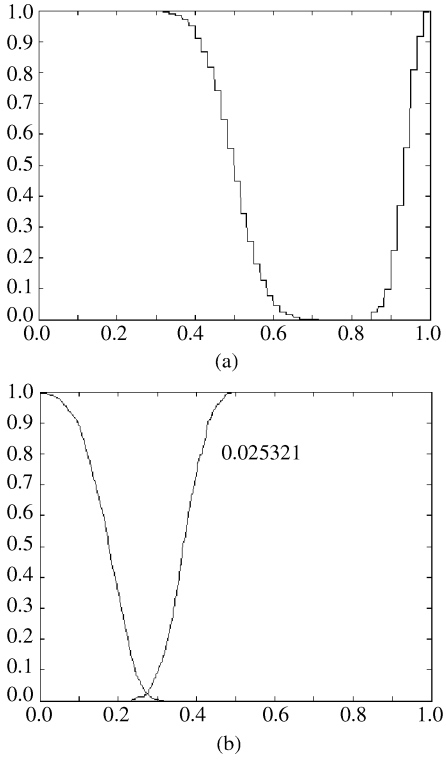


Fig.8. FAR vs. FRR. (a) For *Hash*. (b) For *VQ*.

5 Conclusions

With the advancements of networking, communication and mobility, the security of traditional cryptosystem are facing more threats from insides or outsides of the system. Current information security techniques are facing the problem of lacking the exact connection between cryptographic key and legitimate users. Biometric technologies provide a more reliable method of secure identity authentication and can be used in security system to protect against data abuse and identity theft. Some researchers have studied the interaction between cryptography and biometrics such as fingerprint, face, iris, keystroke, etc. However, a number of challenging research problems in biometric technology, e.g., robust matching algorithm, effective image enhancement, need to be addressed to improve the performance of biometric system[44]. On the other hand, the matching of biometric identifiers within a cryptographic framework is a very tough problem because a natural gap exists between the variability of biometrics and exactitude of cryptography.

This paper overviews recent advancements of fingerprint recognition algorithms with a special focus on the enhancement of low-quality fingerprints and the matching of the distorted fingerprint images. Both issues are significant and arduous tasks in fingerprint recognition because they seriously affect the overall performance of the whole recognition system. Then we discuss two representative methods of key release and key generation scheme based on fingerprint. Two solutions for application in identity authentication without trustworthy third-party in network environment and application in digital media protection are proposed as well, aiming to assure the secrecy of fingerprint template and fingerprint-based user authentication.

The combination of fingerprint biometric and cryptography is a promising idea for user authentication in network environment. But when fingerprint-based cryptosystem come into practical use, it is important to bear in mind that effective security cannot be achieved by relying on technology alone. Technology and users must work together as part of an overall security process. That is the way to integrate the visual identity in cyberlogical world with physical identity in real world.

References

[1] Biometrics Market and Industry Report 2006–2010. International Biometric Group, http://www.biometricsgroup.com.

[2] Biometric Systems Lab, Pattern Recognition and Image Processing Laboratory, Biometric Test Center. http://bias.csr.unibo.it/fvc2004/.

[3] Biometric Systems Lab, Pattern Recognition and Image Processing Laboratory, Biometric Test Center. http://bias.csr.unibo.it/fvc2006/.

[4] O'Gorman L. Fingerprint verification. Biometrics: Personal Identification in a Networked Society. Jain A K, Bolle R *et al.* (eds.), Kluwer Academic Publishers, 1999, pp.43–64.

[5] Shen L L, Kot A, Koo W M. Quality measures of fingerprint images. In *Proc. 1st Audio- and Vedio-Based Person Authentication*, Halmstad, Sweden, 2001, pp.266–271.

[6] Shi Z C, Wang Y C, Qi J, Xu K. A new segmentation algorithm for low quality fingerprint image. In *Proc. 3rd Int. Conf. Image and Graphics*, Hong Kong, China, Dec. 18–20, 2004, pp.314–317.

[7] Gu J W, Zhow J. Model-based orientation field estimation for fingerprint recognition. In *Proc. IEEE Conference on Image Processing*, Barcelona, Spain, 2003, pp.899–903.

[8] Lin H, Wan Y, Jain A K. Fingerprint image enhancement: Algorithm and performance evaluation. *IEEE Trans. Pattern Anal. Machine Intell.*, 1998, 20(8): 777–789.

[9] Yang J W, Liu L F, Jiang T Z, Fan Y. A modified Gabor filter design method for fingerprint image enhancement. *Pattern Recognition*, 2003, 24: 1805–1817.

[10] Zhu E, Yin J P, Zhang G M. Fingerprint enhancement using circular Gabor filter. In *Proc. 1st Int. Conf. Image Analysis and Recognition*, Porto, Portugal, 2004, pp.750–758.

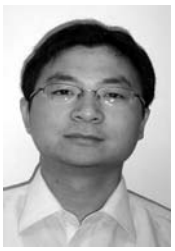
[11] Mohammad A U K, Mohammad K K, Mohammad A K. Fingerprint image enhancement using decimation-free directional filter bank. *Info. Tech. Journal*, 2005, 4(1): 16–20.

[12] Xie M H, Wang Z M. Fingerprint enhancement based on edge-direct diffusion. In *Proc. 3rd International Conference on Image and Graphics*, Hong Kong, China, 2004, pp.274–277.

[13] Weickert J. A review of nonlinear diffusion filtering in scale-space theory in computer vision. *Lecture Notes in Computer Science 1252*, Springer-Verlag, 1997, pp.3–28.

[14] Gilboa G, Zeevi Y Y, Sochen N A. Forward and backward diffusion processes for adaptive image enhancement denoising. *IEEE Trans. Image Processing*, 2002, 11(7): 689–703.
[15] Willis A J, Myers L. A cost-effective fingerprint recognition system for use with low-quality prints and damaged fingertips. *Pattern Recognition*, 2001, 34(2): 255–270.
[16] Zhu G C, Zhang C. A top-down fingerprint image enhancement method based on Fourier analysis. In *Proc. 5th Chinese Conf. Biometric Recognition*, Guangzhou, China, 2004, p.439.
[17] Bazen A M, Gerez S H. Elastic minutiae matching by means of thin-plate spline models. In *Proc. Int. Conf. Pattern Recognition*, Quebec, Canada, Aug. 11–15, 2002, pp.985–988.
[18] Chen H, Tian J, Yang X. Fingerprint matching with registration pattern inspection. In *Proc. 2nd Auido- and Vedio-Based Person Authentication*, Guildford, UK, 2003, pp.327–334.
[19] Ratha N K, Bolle R M. Effect of controlled acquisition on fingerprint matching. In *Proc. 14th Int. Conf. Pattern Recognition*, Brisbane, Australia, Aug. 17–20, 1998, pp.1659–1661.
[20] Dorai C, Ratha N, Bolle R. Detecting dynamic behavior in compressed fingerprint videos: Distortion. In *Proc. IEEE Conf. Computer Vision and Pattern Recognition*, Hilton Head Island, USA, 2000, pp.2320–2326.
[21] Cappelli R, Maio D, Maltoni D. Modelling plastic distortion in fingerprint images. In *Proc. Int. Conf. Advances in Pattern Recognition*, Rio de Janeiro, Brazil, March 11–14, 2001, pp.369–376.
[22] Lee D, Choi K, Kim J. A robust fingerprint matching algorithm using local alignment, In *Proc. Int. Conf. Pattern Recognition*, Quebec, Canada, Aug. 11–15, 2002, pp.803–806.
[23] Senior A, Bolle R. Improved fingerprint matching by distortion removal. *IEICE Trans. Inf. and Syst., Special Issue on Biometrics*, 2001, E84-D(7): 825-831.
[24] Watson C, Grother P, Cassasent D. Distortion-tolerant filter for elastic-distorted fingerprint matching. In *Proc. SPIE Optical Pattern Recognition*, Orlando, USA, April 26, 2000, pp.166–174.
[25] Vajna Z M K. A fingerprint verification system based on triangular matching and dynamic time warping, *IEEE Trans. Pattern Anal. Machine Intell.*, 2000, 22(11): 1266–1276.
[26] Bazen A M, Gerez S H. Fingerprint matching by thin-plate spline modelling of elastic deformations. *Pattern Recognition*, 2003, 36(8): 1859–1867.
[27] Ross A, Dass S, Jain A K. A deformable model for fingerprint matching. *Pattern Recognition*, 2005, 38(1): 95–103.
[28] Chen X J, Tian J, Yang X. A new algorithm for distorted fingerprints matching based on normalized fuzzy similarity measure. *IEEE Trans. Image Processing*, 2006, 15(3): 767–776.
[29] He Y L, Tian J. Fingerprint matching based on global comprehensive similarity. *IEEE Trans. Pattern Anal. Machine Intell.*, 2006, 28(6): 850–862.
[30] Chen X J, Tian J, Yang X. An algorithm for distorted fingerprint matching based on local triangle features set. *IEEE Trans. Info., Forensics and Security*, 2006, 1(2): 169–177.
[31] FpVTE 2003. http://fpvte.nist.gov/.
[32] Soutar C, Roberge D, Stoianov A *et al.* Biometric Encryption. ICSA Guide to Cryptography, McGrow-Hill, 1999.
[33] Clancy T C, Kiyavash N, Lin D J. Secure smart card-based fingerprint authentication. In *Proc. 2003 ACM SIGMM Workshop on Biometrics Methods and Application*, Berkley, CA, 2003, pp.45–52.
[34] Juels A, Sudan M. A fuzzy vault scheme. In *Proc. IEEE International Information Theory Symp.*, Lausanne, Switzerland, 2002, p.480.
[35] Uludag U, Pankanti S, Jain A K. Fuzzy vault for fingerprints. In *Proc. 5th Audio- and Video-Based Biometric Person Authentication*, New York, USA, 2005, pp.310–319.
[36] Hao F, Anderson R, Daugman J. Combining crypto with biometrics effectively. *IEEE Trans. Computers*, 2006, 55(9): 1081–1088.
[37] Goh A, Ngo D C L. Computation of cryptographic keys from face biometrics. *Lecture Notes in Computer Science 2828*, Lioy A, MazzocchiIto D (eds.), Springer-Verlage, 2003, pp.1–13.
[38] Monrose F, Reiter M K, Li Q, Wetzel S. Cryptographic key generation from voice. In *Proc. 2001 IEEE Symposium on Security and Privacy*, Oakland, CA, 2001, pp.202–213.
[39] Hao F, Chan C W. Private key generation from on-line handwritten signatures. *Information Management & Computer Security*, 2002, 10(2): 159–164.
[40] Monrose F, Reiter M K, Wetzel R. Password hardening based on keystroke dynamics. In *Proc. 6th ACM Conf. Computer and Communications Security*, Singapore, 1999, pp.73–82.
[41] Dodis Y, Reyzin L, Smith A. Fuzzy extractors: How to generate strong keys from biometrics and other noisy data. *Lecture Notes in Computer Science 3027*, Cachin C, Camenisch J (eds.), Springer-Verlag, 2004, pp.523–540.
[42] Jin A T B, Ling D N C, Goh A. BioHashing: Two factor authentication featuring fingerprint data and tokenised random number. *Pattern Recognition*, 2004, 37: 2245–2255.
[43] Liu M H, Jiang X D, Kot A C. Fingerprint reference-point detection. *EURASIP J. Applied Signal Processing,* 2005, 4: 498–509.
[44] Jain A K, Ross A, Pankanti S. Biometrics: A tool for information security. *IEEE Trans. Information Forensics and Security*, 2006, 1(2): 125–143.
[45] Li L, Tian J, Yang X. A novel identity authentication technique without trustworthy third-party based on fingerprint verification. *Lecture Notes in Computer Science 3917*, Chen H C, Wang F Y, Yang C C *et al.* (eds.), Springer-Verlag, 2006, pp.175–176.

Jie Tian received the Ph.D. degree (with honor) in artificial intelligence from the Institute of Automation, Chinese Academy of Sciences (CAS) in 1992. From 1994 to 1996, he was a postdoctoral fellow at the Medical Image Processing Group, University of Pennsylvania. Since 1997, he has been a professor in the Institute of Automation, CAS. His research interests are the medical image process and analysis, pattern recognition, etc. He has published more than 50 papers in academic journals and international conferences. He received National Science & Technology Advance Award in 2003 and 2004 respectively. He is the reviewer of "Mathematical Reviews" and a senior member of IEEE Computer Society.



Liang Li received his B.S. degree from Northwestern Polytechnical University, in 2002. Now he is a Ph.D. candidate in CAS. His research interests include pattern recognition, machine learning, and image processing and their applications in biometrics.

Xin Yang received the B.S., M.S., and Ph.D. degrees in intelligent instrument from Tianjin University, China in 1994, 1997, and 2000 respectively. From 2001 to 2003, she was a postdoctoral fellow at the Biometric Research Group, Key Laboratory of Complex Systems and Intelligence Science, Institute of Automation, CAS. Since 2003, she has been an associate professor. Her research interests are bioinformatics, pattern recognition, etc.