Security Enhancement of Biometrics, Cryptography and Data Hiding by Their Combinations

Jing Dong and Tieniu Tan

National Laboratory of Pattern Recognition, Institute of Automation,
Chinese Academy of Sciences, P.O.Box 2728, 10190,Beijing,China

Keywords: Security enhancement, Biometrics, Data Hiding, Cryptography

Abstract

The security of multimedia information in general and the security of visual information in particular have increasingly become an issue of great concern in our networked society. Biometrics, cryptography and data hiding provide effective and often complementary solutions to information security from different perspectives. In this paper, we present a brief overview on the state-of-the-art of research on the security enhancement of biometrics, cryptography and data hiding by their combinations, with focus on the problems of cryptographic key management and biometric template protection. This paper is intended to provide a reference point for newcomers and to promote more activities in these important security issues.

1 Introduction

The increasing popularity of biometrics [10], cryptography [34] and data hiding [24] is driven by the common demand on information security. Numerous efforts have been made in developing effective methods in these areas in order to achieve an enhanced level of information security. There are two paramount issues in information security enhancement. One is to protect the user possession and control the access to information by authenticating an individual's identity. The other is to ensure the privacy and integrity of information and to secure information communication. Biometrics, cryptography and data hiding provide solutions to the above two issues from different perspectives.

Cryptography is the science of writing in secret code and is an ancient art. The goal of cryptography extends beyond merely making data unreadable. It also extends into user authentication. Secret-key cryptography and public-key cryptography are the two major cryptographic architectures. The security of a cryptographic system is dependent on the secrecy of the cryptographic key. Therefore, the key issue in cryptography is key management.

Biometric authentication, or simply biometrics refers to establishing automatic personal recognition based on the physical and behavioral characteristics of an individual (e.g. face, voice, fingerprint, gait, hand geometry, iris, gene, etc.). Biometrics offers greater security and convenience than traditional identity authentication systems (based on passwords and cryptographic keys) since biometrics characteristics are inherently associated with a particular individual, making them insusceptible to being stolen, forgotten, lost or attached. A critical problem in a biometric system itself is to ensure the security of the unique biometric data, because once the biometric templates are compromised, the whole authentication system is compromised. Therefore, how to protect the biometric templates in the database and to secure transmission of the biometric templates through the open network is a vital security issue in biometrics.

Data hiding is aiming at private information protection, securing information transmission (e.g. steganography) and digital rights authentication (e.g. watermarking). Besides using some encryption algorithms to encode the biometric data for protection, one of the major reasons to take advantages of data hiding for biometric template protection is because data hiding complements cryptography in secret information communication and integrity authentication. Watermarking can help to detect the tempered biometric data while steganography can help to secure transmission of biometric data.

Given the security limitations (potential loopholes) of biometrics, cryptography, data hiding and their complementarity, a natural and intuitive solution to the enhancement of their security is to develop methods which take advantages of their respective strength and complementarity. For example, as mentioned above, biometrics can be used to protect the key in cryptography, while cryptography and data hiding can be used to protect biometric templates. Noticeable efforts have been made along this line over the past decade [7][27][4][31][36]. In this paper, we attempt to present an overview of the state-of-the-art of research in this increasingly important topic by putting biometrics, cryptography and data hiding in the same context of security enhancement. Given the practical importance of cryptographic keys and biometric templates, our focus will be on methods which seek combinations of biometrics, cryptography and data hiding to enhance the security of these keys and templates. This paper is intended to provide a reference point for newcomers and to promote more activities in this important area.

The rest of this paper is organized as follows. In Section 2, we will investigate the key management problem of combining

biometrics to cryptographic systems (bio-cryptosystems). In Section 3, we will review current work on biometric templates protection with the assistance of cryptography and data hiding. Finally, in Section 4, we will discuss possible directions for further research.

2 Security Enhancement of Cryptography by Combination with Biometrics

A combination of biometrics and cryptography has the potential to provide a higher assurance of the legal information holder. A crucial issue in cryptographic systems is the problem of key management. Hence, how to make use of biometrics in cryptographic systems (or bio-cryptosystems) is often related to the issue of how to combine biometrics with cryptographic "keys". There are several ways to combine biometrics with a cryptosystem, namely biometrics key release, biometrics key generation and biometrics key binding. In a key release mode, biometrics plays a predetermined role in a cryptosystem. The key would be released to users only if biometric matching is successful. A key generation mode requires the key of a cryptosystem being derived directly from a biometric template, hence the unique biometrics provides an unique key for the security system based on some transform or feature extraction. In the key binding mode, the system binds a cryptographic key with the user's biometrics at the time of enrollment. The key would be retrieved only upon a successful authentication. The key generation/binding modes seem to be more secure than the key release mode because in key release mode, the user authentication and key release are two separate parts. However, whatever mode a biometric cryptosystem takes, one major difference between biometrics and cryptographic key management should be addressed. The conventional cryptography systems do not need any complex pattern recognition strategy as in biometric systems. They almost always depend on an accurate key matching process. That is, it requires that keys are exactly correct and does not tolerate a single bit error. However, as biometric characteristics are known to be variable and noisy and each new biometric sample is always different, only an approximate match under a threshold between the input biometric data to a corresponding stored template would lead the authentication successful. Therefore, how to build a bridge between the fuzziness of biometric matching and the exactness of key based cryptography systems seems to be a great challenge for bio-cryptosystems. During the past several years, a number of researchers have made efforts on this issue and have attempted to design secure bio-cryptosystmes. In the following, we discuss these efforts.

2.1 Bio-cryptosystems

Many biometric patterns, including online signatures, fingerprints, iris, voice, face and palmprint have been used to generate or bind the keys to cryptographic systems. The original concept of biometric-based keys is due to *Tomko et al.* [29]. Fingerprint was considered a key that would encrypt a set of randomly generated numbers which in turn could generate a private or a public key in a cryptographic system. The method used Fourier transform and could be implemented via optical or digital processing. The earlier work in *Bodo* [3] suggested a cryptographic key being extracted directly from a biometric template where a randomly chosen key can be connected with the biometric. The key in this scheme is not cancelable. If it is compromised, this particular biometric is lost forever. In the paper by *Janbandhu and Siyal* [11], it is suggested to generate a biometric signature directly from a biometric template using some standard cryptographic algorithms. Unlike *Bodo*, their cryptographic key can be changed. However, the biometric template must have all the bits exactly correct, which is unrealistic for all the biometrics except DNA pattern. *Davida et al.* [5] proposed a scheme that a biometric template itself, or a hashed value derived from it, is used as a cryptographic key. It was also suggested to use some error correction codes to compensate for bit variations.

Soutar et al. [27] proposed a new, more advanced approach of biometric-key binding algorithm using an optical correlation-based fingerprint matching system. Their algorithm binds a cryptographic key with the user's fingerprint images at the time of enrollment and uses Fourier processing to compensate for fingerprint image displacement. A filter is designed to obtain a tradeoff between distortion tolerance and discrimination of these images. A key with 128 bits, is linked to the output data via a lookup table and an error correcting code. Similar work was done on palmprint cryptosystem in [35]. A 1024-bit binary string is extracted from the palmprint images using differential operations and then translated to a 128 bits encrypting key using a hash function with error correcting code. *Hao and Chen* [9] worked on handwritten signatures and defined 43 signature features extracted from dynamic information like velocity, pressure, altitude, and azimuth. They used feature coding to quantize each feature into bits which were concatenated to form a binary string. Their experiments reported a 28% false rejection rate and 1.2% false acceptance rate.

Goh and Ngo [8] introduced a new technique called bio-hashing and applied it to face images. A set of random orthogonal vectors (which are kept secret) are generated and an inner product between each vector and the biometric feature set is computed and binarized to produce a 80-bits key with a 0.93% false rejection rate for the system.This work also begins a parameters based bio-cryptosystem. *Monrose et al.* [20] introduced a technique called biometrically hardened passwords. It deals with keystroke dynamics or voice recognition. A password provided by the user is pre-pended by a key extracted from a biometric component, thus making the password hardened with the biometrics.

Juels and Wattenberg proposed a "fuzzy commitment scheme" in [13]. A biometric template is supposed to be in the form

of an ordered bit string, which is XOR-ed with a same length codeword of an error correcting code. This codeword then generates a cryptographic key. *Martini and Beinlich* [19] proposed a virtual PIN scheme, which is practically identical to the fuzzy commitment scheme [13]. Gabor filters were used for feature extraction. The authors suggested using LDPC (low density parity check) codes for error correction. The ability of these codes to handle very large block sizes may be beneficial for future development. Similar approach was used by *Tuyls et al.* [30]. In their work, The authors extracted reliable components from the template and applied BCH error correcting code.

Recent literature introduced a "secure sketches" scheme [6] as a link between biometrics and cryptography. The "secure sketch" scheme is a way to extract strong keys from noisy data such as biometrics. It could help to handle biometric data matching as an error correction issue. The scheme with quantization is applied to face biometrics and good results are obtained in [17]with the average key size of 73 bits.

2.2 Fuzzy Vault

In addition to the above schemes, *Juels and sudan* [12] introduced a novel cryptographic construction called "fuzzy vault". In this scheme, secret message (e.g. biometric key) is embedded in a polynomial as its coefficients after being transmitted as an unordered string, and the values computed by the polynomial could be added with some chaff points which do not lie on the polynomial to form a vault. Only the subsequently similar biometric representation could be matched and the secret message could be derived from the vault during the authentication progress. The ability of fuzzy vault to deal with variations in the biometric data along with the ability to work with unordered sets, makes it a good solution for bio-cryptosystems. The "fuzzy vault" scheme became an important milestone in the development of bio-cryptosystems and gathered increasing attention among the researchers. Therefore, in this section, we focus on this promising scheme.

Clancy et al. [4] propose a fingerprint vault. At the enrollment, five fingerprints of a user are acquired. The fingerprint minutiae position is extracted from each fingerprint. Correspondence between the minutiae from the five fingerprints is established based on a bounded nearest-neighbor algorithm. Then the vault is created using polynomial encoding and error correction, combined with the chaff points. Satisfying results are obtained in their experiments. The limitation of this work is that it assumes the fingerprints are pre-aligned and it is also not clear about their database used in their experiments. *Uludag et al.* [31] explore an extension approach on fingerprint with the framework of fuzzy vault without resorting to simulating the error-correction step. The correspondence of the minutiae across images was manually established as well. The limitation of their approach includes high time complexity during decoding. *Yang et al.* [28] proposed a modified fuzzy vault scheme, where minutiae are aligned relative to the reference minutiae pair. For a small database of fingerprints, the authors obtained a false reject rate at 17%. *Nagar and Chaudhury* [23] proposed another modified fuzzy vault scheme which is used within asymmetric cryptosystem. Almost zero error rate is reported for a small database of fingerprints.

In addition to fingerprints, *Kholmatov et al.* [14] apply fuzzy vault on online signatures. They extract minutiae points (trajectory crossings, endings and points of high curvature) from online signatures, and used these points during the locking and unlocking phases of the vault. Then a 128-bit long key is divided into non-overlapping chunks to obtain the coefficients of an 8th degree polynomial. Although their performance was evaluated using online signature samples only supplied by 10 subjects enrolled to the system and their method is a relatively straightforward extension of *Uludag et al.* [31], this is the first real application of the fuzzy vault scheme using online signatures.

In recent work, *Lee et al.*[16] proposed a method of applying iris data to fuzzy vault. They introduce a pattern clustering method and they used the iris feature extraction algorithm based on ICA (Independent Component Analysis) in order to produce unordered sets for fuzzy vault. Also, the experimental results showed an encouraging potential on real application with an average of 85% genuine accept rate while almost 0% false accept rate.

The "fuzzy vault" scheme is one of the popular cryptographic solution to solve the key management problem of cryptographic systems at the same time to protect templates stored in biometric systems. The "vault" seems to be a secure storage for biometric data because it contains the useful biometric template data mixed up with the meaningless chaff points. Therefore, the information of biometric template would not be leaked out unless the identification completed correctly. Besides fuzzy vault schemes, the above work addressed the problem to make the cryptographic key management securer and more convenient using biometrics. As we all know, for any authentication based security systems, the security of templates data is crucial. The potential loss of biometric data would also be an important security problem of the bio-cryptosystems. Hence, how to ensure the security of biometric templates, or, how to secure the transmission of biometric information in the network environment becomes very important and urgent. In the next section, we will discuss current work on biometric template protection by taking advantage of combining cryptography and data hiding.

3 Security Enhancement of Biometrics by Combination with Cryptography and Data Hiding

3.1 Protecting Biometric Templates with Cryptography

With the convenience of information exchange across the Internet, the storage of sensitive data on open networks calls for many security concerns. Several methods have been suggested in the literature to protect biometric templates from revealing important private information. A straightforward method of protecting the biometric templates is to encrypt the biometric data before storage or transmission. Besides using cryptography directly, other cryptographic approached are also used for reference. The hard-to-invert function is commonly used in cryptographic scheme, for it is computationally impossible to find the original data from a transformed one. There are some cases in the robust hash functions that small changes in a biometric sample would yield the same hash value. In stead of storing the original biometric data x in the database, only its value generated by a hash function $H(x)$ is stored. Hence, if the biometric data is compromised or attacked, we can change for another new representation, which also provide the same authentication information. Furthermore, we could apply different hash functions on different applications. We just need to adopt another new transformation for the system if the biometric template is compromised. The concept of cancelable biometrics was first introduced by *Ratha et al.* [25] (see also in [26]). They proposed the use of distortion functions to generate biometric data that can be canceled if necessary. They used a non-invertible transformation function that distorts the input biometric signal (e.g., face image) prior to feature extraction, or alternately, modifies the extracted feature set (e.g., minutiae points) itself. When a stored template is compromised, then the current transformation function is replaced with a new function thereby canceling the current (compromised) template and generating a new one.The security of these schemes depends on the difficulty to invert the transformation to get the original biometric data.

Linnartz and Tuyls [18] proposed the use of shielding functions to protect the biometric templates from a hostile administrator of the biometric system. The authors accomplish this method by using delta-contracting and epsilon-revealing functions to preprocess the biometric data acquired from an individual. These functions make it computationally prohibitive for an administrator to estimate the original data of the user.

3.2 Protecting Biometric Templates using Data Hiding

Cryptography and data hiding (e.g. steganography and watermarking) have been seen as a pair of complementary techniques. Cryptography focuses on methods to make encrypted information meaningless to unauthorized parties, whereas data hiding is based on concealing the privacy information itself. Steganography-based techniques can be used for transferring critical biometric information (such as the template) from a client to a server. On the other hand, digital watermarking can be used to embed proprietary information (such as company logo or signature) in the host template data to protect the intellectual property rights of that data. The watermark, which resides in the biometric data itself and is not related to lock-unlock operations, provides another line of defense against illegal utilization of the biometric data. Of course the security of these schemes relies on the security of their watermarking algorithms. The ”digital signature” is a successful example of combining biometrics to watermarking, with its purpose to protect the legal rights of documents possession. As for biometric template protection, we also discuss current work on combining biometric with data hiding in the rest of this section.

Pankanti and Yeung [28] proposed a fragile watermarking method for fingerprint image tampering detection. A watermark image is embedded in the fingerprint image, by utilizing a verification key. Their method can localize any region of the image that has been tampered. To increase the security of the watermark, the original watermark image is first transformed into another mixed image, then the mixed image is used as a new watermark image. This image does not have a meaningful appearance, contrary to original watermark image which can contain specific logo or text. The authors show that their watermarking technique does not lead to a significant performance loss in fingerprint verification.

In a series of work [33] [2] [32], *Jain and Uludag* introduced several methods for combining data hiding with biometrics. In [33], their watermarking methods preserve the quantized gradient orientations at and around watermark embedding locations (so all of the fingerprint features extracted using gradient information are preserved) and singular points in the fingerprint image. In [2], they presented a fingerprint image watermarking method that can embed facial information into host fingerprint images. The watermark data, which consists of the eigen-face coefficients of a user's face, can be used in authenticating the host fingerprint image. Their experimental results also claimed their scheme does not introduce any significant degradation for fingerprint recognition performance. In their subsequent work, *Jain et al.* introduced two applications of an amplitude modulation-based watermarking method [32] in which they hide a user's biometric data in a variety of images. The first application is related to increasing the security of biometric data exchange based on steganography. The biometric data (fingerprint minutiae) that need to be transmitted (possibly via a non-secure communication channel) is hidden in a host (also called cover and carrier) image, whose only function is to carry the data. The host image is not related to the hidden data in any way. The second application is based on a previous study in [2]. They embedded facial information in fingerprint images rather than other images. In this application, the

data is hidden in such a way that the features that are used in fingerprint matching are not significantly changed during encoding/decoding. As a consequence, the verification accuracy based on decoded watermarked images is very similar to that of original images. This scheme provided a double authentication for biometric templates.

Zebbiche et al. [15] proposed another method using watermarking to protect fingerprint data. They introduced an application of wavelet-based watermarking method to hide the fingerprint minutiae data in fingerprint images. The application provided a high security to both hidden data (i.e. fingerprint minutiae) and the host image (i.e. fingerprint). The original unmarked fingerprint image is not required to extract the minutiae data. The method is essentially introduced to increase the security of fingerprint minutiae transmission and can also be used to protect the original fingerprint image.

Vatsa et al. [22] presented a novel biometric watermarking algorithm for improving the recognition accuracy and protecting the face and fingerprint images from tampering. Multi-resolution DWT (discrete wavelet transform) is used for embedding the face image in a fingerprint image. They also proposed using a SVM (supporting vector machine) based learning algorithm to select the best quality pixels from two extracted face images to generate a high quality image for recognition. Their face recognition accuracy is reported above 80% and was improved to 97% with the aid of SVM. In the subsequent work [21], they proposed a combined DWT and LSB (Least Significant Bit) based biometric watermarking algorithm that securely embeds a face template in a fingerprint image. The proposed algorithm is against geometric and frequency attacks and protects the integrity of both the face template and the fingerprint image. Experimental results were performed on a database of 750 face and 750 fingerprint images. Also, a multi-modal biometric approach is used as a metric to evaluate the combined performance of both face and fingerprint recognition.

Farid et al. [1] extended the digital watermarking technique – Phasemark, originally developed solely for image authentication, to biometrics (particularly the fingerprints) to assist in forensic analysis. Using a signature extracted from the Fourier phase of the original image, they hide an encoded signature back into the original image forming a watermarked image. Then, the detection process computes the Fourier transform of the watermarked images, extracts the embedded signature and then correlates it with a calculated signature. Various correlation metrics determine the identity degree of biometric authentication. In their work, they demonstrated two different scenarios of applications, where the original image may be present or absent. However, the detection performances are not good enough for real application.

4 Discussions and Conclusions

Biometrics, cryptography and data hiding provide effective and often complementary solutions to information security from different perspectives. Each of them, however, suffers from security loopholes on its own. Growing efforts are being made to eliminate such loopholes and to further enhance information security by taking advantage of the respective strength and complementarity of biometrics, cryptography and data hiding. In this paper, we have presented a brief overview on the state-of-the-art of research on the security enhancement of biometrics and cryptography by their combinations.

Although significant progress has been made in security enhancement of biometrics and cryptography over the past decade, much remains to be done. The most promising solution to security enhancement of biometrics and cryptography is perhaps the so-called fuzzy vault scheme where the safety of cryptographic keys and biometric templates is bounded in a two-in-one fashion. Hence, the fuzzy vault scheme deserves further study. More efforts should be made on building the bridge between the fuzziness of biometric matching and the exactness of cryptographic key validation. Also, multi-modality bio-cryptosystems should also be on the agenda for future research since each single biometric modality has its weakness. Furthermore, a larger and common database should be built for performance evaluation of bio-cryptosystems.

Various cryptographic techniques have been applied to protect the safety and integrity of biometric data, especially biometric templates used in biometric authentication. Data hiding (and watermarking in particular) has also been adopted to protect biometric data and biometric templates. Regardless of using biometric template as the watermark, or using biometric image as the host image, data hiding can provide an additional layer of security for biometric template protection in terms of tempering detection and secure transmission. However, since the process of data hiding will change the characteristics of biometric data to some extent, one may consider some passive image forensics methods for detecting possible tempering of the biometric data. In addition, security enhancement methods should also be explored which make simultaneous use of biometrics, cryptography and data hiding.

Acknowledgment

This work is funded by research grants from National Key Technology R&D Program 2006BAH02A13.

References

[1] F. Ahmed and I.S. Moskovitch. Composite signature. based watermarking for fingerprint authentication. *Proc. ACM Multimedia and security Workshop*, 2005.

[2] A.K.Jain, U.Uludag, and R.K.Hsu. Hiding a face in a fingerprint image. *Proc. of Intl Conf. on Pattern Recognition*, 3:756–759, 2002.

[3] A. Bodo. Method for producing a digital signature with aid of a biometric feature. *German patent DE 42 43 908 A1*, June 30, 1994.

[4] T. C. Clancy, N. Kiyavash, and D. J. Lin. Secure smartcard-based fingerprint authentication. *Proc.ACMSIGMM 2003*, 4263:45–52, 2003.

[5] G.I. Davida, Y. Frankel, and B.J. Matt. On enabling secure applications through off-line biometric identification. *In Proc. of Symp on Security and Privacy*, page 148C157.

[6] Y. Dodis, L. Reyzin, and A. Smith. Fuzzy extractors: How to generate strong keys from biometrics and other noisy data. *In Eurocrypt, ser. LNCS*, 3027:523C540, 2004.

[7] F.Hao, R.Adnderson, and J.Daugman. Combining crypto with biometrics effectively. *IEEE Trans.on Computers,*, 55(9), 2005.

[8] A. Goh and D.C.L. Ngo. Computation of cryptographic keys from face biometrics. *Intl Federation for Information Processing*, 2828:1C13, 2003.

[9] F. Hao and C.W. Chan. Private key generation from on-line handwritten signatures. *Information Management and Computer Security*, 10(2):159–164, 2002.

[10] A. K. Jain, R. Bolle, and S. Pankanti. Biometrics: Personal identification in networked society. *Norwell, MA: Kluwer*, 1999.

[11] P.K. Janbandhu and M.Y. Siyal. Novel biometric digital signature for internet based applications. *Information Management and Computer Security*, 9(5):205C212, 2001.

[12] A. Juels and M.Sudan. A fuzzy vault scheme. *Proc.of Intl. Symposium on Inofrmation Theory*, page 408, 2002.

[13] A. Juels and M. Wattenbeg. A fuzzy commitment scheme. *In 6th ACM Conference on Computer and Communications Security*, pages 28–36, 1999.

[14] A. Kholmatov and B. Yanikoglu. Biometric cryptosystem using online signatures. *21st Intl. Symposium on Computer and Information Sciences*, 4263, 2006.

[15] K.Zebbiche and L. Ghouti *et al*. Protecting fingerprint data using watermarking. *First NASA/ESA Conf. on Adaptive Hardware and Systems (AHS'06)*, pages 451–456, 2006.

[16] Y. J. Lee, K.Bae, and et al. Biometric key binding: Fuzzy vault based on iris images. *LCNS*, 4642:800–808, 2007.

[17] Q. Li, Y. Sutcu, and N. Memon. Secure sketch for biometric templates. *Advances in Cryptology C ASIACRYPT 2006,Lecture Notes in Computer Science*, 4284:99– 113, 2006.

[18] J.P. Linnartz and P. Tuyls. New shielding functions to enhance privacy and prevent misuse of biometric templates. *In Proc. Audio- and Video-based Person Authentication*, page 393C402, 2003.

[19] U. Martini and S. Beinlich. Virtual pin: Biometric encryption using coding theory. *Proc. of the 1st Conference on Biometrics and Electronic Signatures of the GI Working Group*, page 91C99, 2003.

[20] F. Monrose, M.K. Reiter, and R. Wetzel. Password hardening based on keystroke dynamics. *Intl. Journal on Information Security, Springer*, 1(2):69C83, 2002.

[21] M.Vatsa and R.Singh *et al.* Robust biometric image watermarking for fingerprint and face tmeplate protection. *IEICE Electronics Expressp*, 3(2), 2006.

[22] M.Vatsa, R.Singh, and A.Noore. Improving biometric recognition accuracy and robustness using dwt and svm watermarking. *IEICE Electronics Expressp*, 2(12), 2005.

[23] A. Nagar and S. Chaudhury. Biometrics based asymmetric cryptosystem design using modified fuzzy vault scheme. *ICPR06*, pages 537–540.

[24] F. P. Petitcolas, R.J.Anderson, and M.G.Kuhn. Information hidingła survey. *Proc.of IEEE,*, 87(7), 1999.

[25] N. Ratha, J. Connell, and R. Bolle. Enhancing security and privacy in biometrics-based authentication systems. *IBM Systems Journal*, 40(3):614C634, 2001.

[26] N. Ratha and J. Connell *et al.* Cancelable biometrics: A case study in fingerprints. *Intl. Conf. on Pattern Recognition*, page 370C373, 2006.

[27] C. Soutar and D. Roberge *et al*. Biometric encryption. *ICSA Guide to Cryptography, McGrow-Hill*, 1999.

[28] S.Yang and I. Verbauwhede. Secure fuzzy vault based fingerprint verification system. *13th Asilomar Conference on Signals, Systems, and Computers*, 1:577C581, 2004.

[29] G.J. Tomko, C. Soutar, and G.J. Schmidt. Fingerprint controlled public key cryptographicsystem. *U.S. Patent 5541994*, July 30, 1996.

[30] P. Tuyls and A. H. M. Akkermans *et al*. Practical biometric authentication with template protection. *5th International Conference, AVBPA*, 3546(3):436 – 446, 2005.

[31] U. Uludag and S. Pankanti *et al.* Biometric cryptosystems: Issues and challenges. *Proceedings of the IEEE*, 92(6):948C960, 2004.

[32] U.Uludag. Hiding biomtric data. *IEEE Trans. on PAMI*, 25(11):1494–1498, 2003.

[33] U.Uludag, B.Gunsel, and M.Ballan. A spatial method for watermarking of fingerprint images. *Proc. 1st Intl.Workshop on Pattern Recognition in Information Systems*, pages 26–33, 2001.

[34] W.Stallings. Cryptography and network security: Principles and practice. In *Prentice Hall*, 2003.

[35] K. Wang X. Wu, D. Zhang. A palmprint cryptosystem. *Proc. Intl. Conf. of Biometrics*, pages 1035–1042, 2007.

[36] Y.Sutcu, Q.Li, and n.Memon. Protecting biometric templates with sketch: Theory and practice. *IEEE Trans.on Information Forensics and Security*, 2(3), 2007.