International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 4 Issue 02, February-2015

A Study of Iris Template Protection Techniques for a Secure Iris Recognition System

Rajeev Gupta
MMICT&BM(MCA)
Maharishi Markandeshwar University
Mullana (Ambala), INDIA

Ashok Kumar
Department of Computer Engg., MMEC
Maharishi Markandeshwar University
Mullana (Ambala), INDIA

***Abstract*- Iris Template protection is a crucial requirement when designing a biometric based authentication system. It refers to techniques used to make the stored iris template inaccessible to unauthorized users. From an iris template, information about the user can be revealed and identity theft can occur. Iris Template protection can be performed by using template distortion techniques, biometric cryptosystems, watermarking and data hiding techniques.**

Keywords—Iris template; Cryptosystem; Watermarking; Hybrid Techniques

I. INTRODUCTION

A secure iris recognition system for personal authentication is the major demand of society in order to conflict the epidemic growth in identity theft. It is urgently needed to meet the increased security requirements in a variety of applications to secure information in databases. Iris template security is one of the most crucial issues in designing a secure iris recognition system for personal authentication. The major factors which effects an iris recognition system are may be *Internal* or *External* factors. The internal factors consists *intrinsic failures* occur due to inbuilt limitations in the sensing, feature extraction, or matching technologies as well as the limited discrimination of the specific biometric feature; and external factors consists *extrinsic failures* may occurs due to resourceful hackers can covertly acquire the biometric characteristics of a genuine user, improper administration in biometric system, insecure hardware, software, and the communication channels between the various modules. This paper summarizes the various iris template protection techniques for a secure iris recognition system. Part II focuses on major threats in iris recognition system; Part-III presents the major attacks on iris recognition system as well as attacks on Iris Template Database; Part IV focuses on various iris template protection techniques for a secure iris recognition system with their advantages and limitations and Part-V presents the summary and conclusion.

II. MAJOR THREATS IN IRIS RECOGNITION SYSTEM

An Iris Recognition System is vulnerable to various types of threats as discussed below [21][30].

- *Circumvention:* An impostor may gain access to the system protected by biometrics and peruse sensitive data. He/ she can violate the privacy of the enrolled user and can also modify sensitive data.
- *Repudiation:* A legitimate user may access the facilities offered by an application.
- *Covert acquisition:* An intruder may stealthily obtain the raw biometric data of a user to access the system.
- *Conspiracy:* An individual with wide super-user privileges (such as an administrator) may deliberately modify system parameters to permit incursions by an intruder.
- *Coercion:* An impostor may force a legitimate user to grant him access to the system.
- *Denial of Service (DoS):* An attacker may overwhelm the system resources to the point where legitimate users desiring access will be refused service.

III. MAJOR ATTACKS ON IRIS RECOGNITION SYSTEM AND IRIS TEMPLATE DATABASE

The major attacks on iris recognition system are categorized into four different levels [5]: Interface Level, Communication Channels Level, Module Level and Database Level attacks. *Interface level attacks* are mainly replaying a fake or intercepted biometric to gain access to the system. *Communication channels level attacks* take advantage of physical and crypto-graphical vulnerabilities in the data transfer between modules in order to intercept or alter the data. *Module level attacks* exploit software loopholes to access the system, either by modifying the output regardless of the input (Trojan Horse Attack) or by exploiting exceptions not handled by the algorithm. It is also always possible to attack a biometric system by overriding the output of the decision module. *Database level attacks* are concerned to biometric template stored in the database. Here, unauthorized user can also allow the use of intercepted biometrics into other biometric systems using the same trait, also referred to as function creep [28].

A template represents a set of prominent features that summarizes the biometric data of a person. Due to its compact nature, it is commonly assumed that the template cannot be used to extract complete information about the original biometric signal. Furthermore, since the templates are typically stored in an encrypted form, it is substantially

difficult to decrypt and determine the contents of the

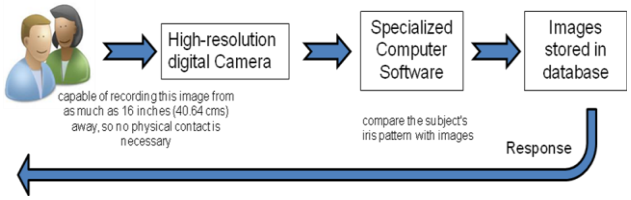

Fig. 1 Identification Process of Iris Recognition Technology[23]

stored template. Database level Attacks on the iris template can lead to the following three susceptibilities:

- A template can be replaced by an impostor's template to gain unauthorized access,
- A physical spoof can be created from the iris template [1][6] to gain unauthorized access to the system
- The stolen template can be replayed to the matcher to gain unauthorized access.

There are two major ways of attacking the template database:

- *Fake*, in which attackers first reconstruct the biometric sample according to an intercepted feature template [2], and then import it to cheat the biometric system and get a legal login or an intention export;
- *Replacement*, in which attackers directly use an imposter identity data to replace a genuine one in a database and get a legal identity.

IV. Iris Template Protection Techniques

Several techniques have been suggested in the literature to protect iris templates from revealing important information. An ideal iris template protection scheme should possess the following four properties [30].

- *Diversity:* The secure iris template must not allow cross-matching across databases, thereby ensuring the user's privacy.
- *Revocability:* It should be straightforward to revoke a compromised iris template and reissue a new one based on the same existing data.
- *Security:* It must be computationally hard to obtain the original iris template from the secure iris template. This property prevents an adversary from creating a physical spoof of the biometric trait from a stolen iris template.
- *Performance:* The iris template protection scheme should not degrade the recognition performance (FAR and FRR) of the iris recognition system.

The iris template protection techniques discussed in the paper can be broadly classified into five categories: Feature Transformation, Biometric Cryptosystem, Watermarking, Hybrid and Haptic Biometric Techniques (see Fig. 2).

A. *Feature Transformation Techniques:*

In F*eature Transformation Approach*, a transformation function is used on the iris template and only the transformed iris template is stored. Depending on the characteristics of the transformation function, F or according to the nature of the transform, the feature transformation approach can be further categorized into two categories:

⇨ Invertible Feature Transformation

⇨ Non-invertible Feature Transformation

1) *Invertible Feature Transformation:*

Invertible Feature Transformation is also known as *Salting* or *Biohashing.* It is a popular iris template protection approach in which the biometric features are transformed

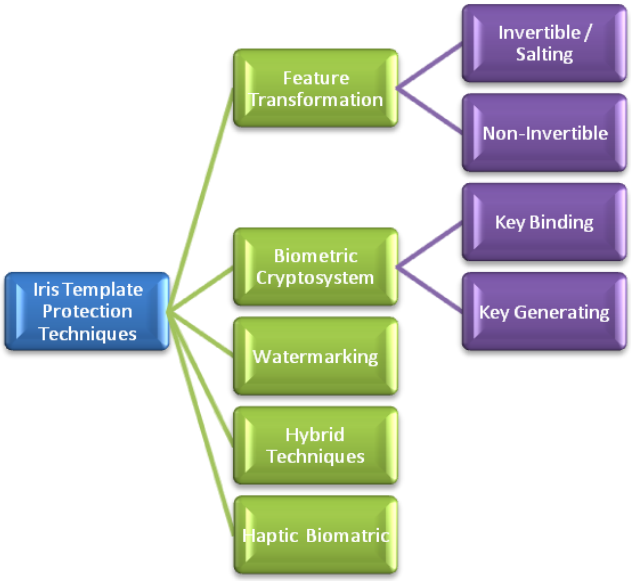

Fig. 2 Categorization of Iris Template Protection Techniques

using a function defined by a user-specific key or password. Since the transformation is invertible to a large extent, the key needs to be securely stored or remembered by the user and presented during authentication. This need for additional information in the form of a key increase the entropy of the biometric template and hence makes it difficult for the adversary to guess the template. Invertible feature transformations rely on the secrecy of the user specific key in securing the iris template since the transform is invertible.

Advantages:

- Introduction of key results in low false accept rates.
- Multiple templates for the same user biometric can be generated by using different keys.
- It is easy to revoke the compromised template and replace it with a new one generated by using a different user-specific key.

Limitations:

- The template is no longer secure, because the transformation is usually invertible due to user-specific key is compromised.
- Since matching takes place in the transformed domain, the salting mechanism needs to be designed in such a way that the recognition performance does not degrade.

An example of invertible feature transformation approach is generating a pseudo random password and integrating it into the template creation [8] and iris template security and revocability. But this approach cannot be successfully appended on Daugman's binary Iris Code based authentication systems.

Another example of this approach is introducing an iris shuffling algorithm [24][25] that uses a binary n-bit key to shuffle the iris code after dividing it in n segments. Their results show that the algorithm not only achieves revocability, but also increases seperability between the hamming distance distributions of genuine and imposter users.

2) Non-Invertible Feature Transformation:

Non-Invertible Feature Transformation is another popular iris template protection approach, in which, iris template is secured by applying a non-invertible transformation function to it. Non-invertible transform refers to a one-way function, *F*, that is "easy to compute" but "hard to invert" in the cartesian, polar and transformation domain. The main characteristic of this approach is that even if the key and/or the transformed template are known, it is computationally hard for an adversary to recover the original iris template.

Advantages:

- It is hard to recover the original biometric template even when the key is compromised, so, this scheme provides better security than the salting approach.
- Diversity and revocability can be achieved by using application-specific and user-specific transformation functions, respectively.

Limitations:

- The main drawback of this approach is the trade-off between discriminability and noninvertibility of the transformation function.

An example of non-invertible feature transformation approach is Ratha et al. [21] [22] introduced the concept of cancelable biometrics. They proposed one-way transformations in the cartesian, polar and transformation domain. In [19] they suggest two different ways of creating cancelable iris templates by applying non-invertible one-way transformation. The first method involves shifting and combining rows of the unwrapped iris image or binary iris template, and the second method uses a key to add a random noise pattern or a synthetic iris pattern again to the original unwrapped iris or the binary template to generate the cancelable template.

B. Biometric Cryptosystems:

Biometric cryptography is the science of combining traditional cryptographic methods with biometrics either for securing the cryptographic keys or also for securing biometric templates. In other words, Biometric cryptosystems refer to algorithms that combine biometrics with cryptography. However, they can also be used as an iris template protection mechanism. In a biometric cryptosystem, some public information about the biometric template is stored. This public information is usually referred to as *helper data* and hence, biometric cryptosystems are also known as *helper data-based methods* [7].

Biometric cryptosystems have three main challenges [29]:

- To accommodate Intra-user variability/Intra-class Stability
- To successfully distinguish between different users
- Neither Template nor Cryptographic key could independently be extracted from stored information

Depending on how the helper data is obtained, Biometric cryptosystems can be further categorized as:

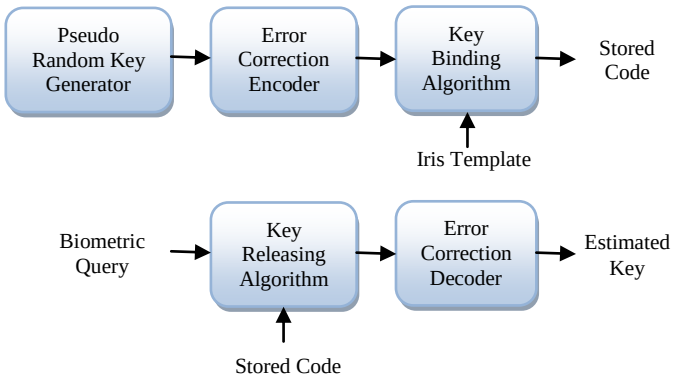

Fig. 3 Generic Key Binding Biometric Cryptosystem

⇨ *Key Binding Biometric Cryptosystems*

⇨ *Key Generating Biometric Cryptosystems*

1) Key Binding Biometric Cryptosystem:

In a *Key binding biometric cryptosystem*, the biometric template is secured by monolithically binding it with a key within a cryptographic framework. In other words, Key-binding biometric cryptosystems transfer a key (generated by a pseudo random number generator and encoded by an error correction encoder.) into the stored identity code (See Fig. 2). The key-binding algorithm integrates both the codeword and biometric template into the stored identity code. When a biometric query differs from the template within certain error tolerance, the associated codeword with similar amount of error can be recovered which can be decoded to obtain the exact codeword and hence, recover the embedded key.

Advantages:

- This approach is tolerant to intra-user variations in biometric data and this tolerance is determined by the error correcting capability of the associated codeword.

Limitations:

- Matching has to be done using error correction schemes and this precludes the use of sophisticated matchers developed specifically for matching the original biometric template.
- This can possibly lead to a reduction in the matching accuracy.
- In general, biometric cryptosystems are not designed to provide diversity and revocability.

One of the widely used key-binding biometric cryptosystem is the "fuzzy commitment" scheme [4] suggested by Juels and Wattenberg, in which the user selects a secret message C from a set of codewords of some error-correcting code at the enrollment time.

Another widely used Key binding biometric cryptosystem is "Fuzzy sketches" were studied in [18] to apply them to protect iris templates. A coding/decoding scheme was suggested that achieved near classical performance rates.

Some other Key binding Biometric Cryptosystem to protect iris template is "fuzzy vault [10][11]",

2) Key Generating Biometric Cryptosystem:

Key-generating biometric cryptosystems transfer a key (combined with the biometric query to generate the stored code) into the stored identity code (See Fig. 4). Direct cryptographic key generation from biometrics is an attractive proposition but it is a difficult problem because of the intra-user variability. Key generating biometric cryptosystems usually suffer from low discriminability which can be assessed in terms of *key stability* and *key entropy*. Key stability refers to the extent to which the key generated from the biometric data is repeatable. Key entropy relates to the number of possible keys that can be generated. Note that if a scheme generates the same key irrespective of the input template, it has high key stability but zero entropy leading to high false accept rate. On the other hand, if the scheme generates different keys for different templates of the same user, the scheme has high entropy but no stability and this leads to high false reject rate. While it is possible to derive a key directly from biometric features, it is difficult to simultaneously achieve high key entropy and high key stability.

Advantages:

Direct key generation from biometrics is an appealing template protection approach which can also be very useful in cryptographic applications.

Limitations:

It is difficult to generate key with high stability and entropy.

An example of Key generating biometric cryptosystem is Dodis et al. [27] introduced the concepts of *secure sketch* and *fuzzy extractor* in the context of key generation from biometrics. The secure sketch can be considered as helper data that leaks only limited information about the template, but facilitates exact reconstruction of the template when presented with a query that is close to the template. The fuzzy extractor is a cryptographic primitive that generates a cryptographic key from the biometric features.

Another approach proposed by Davida et al. [15] [16] for template protection based on the iris biometric.

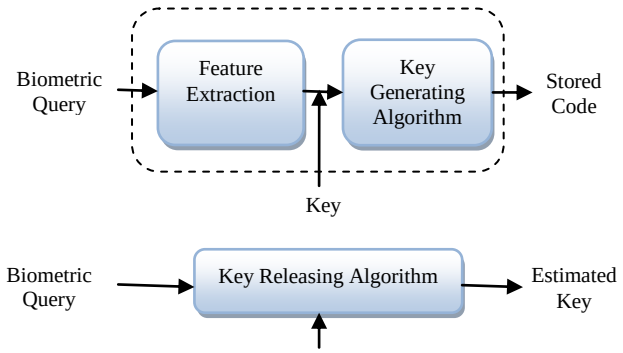

Fig. 5 Generic Key Generating Biometric Cryptosystem

C. Watermarking:

Watermarking refers to approaches that hide a watermark into a cover work, in a way that makes the watermark imperceptible to humans.

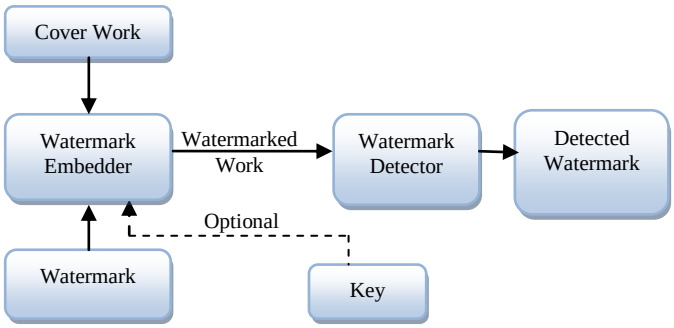

Fig. 4 Generic Watermarking System [30]

Watermarking can also be used to hide one template into another, which accomplishes template security as well as multi-biometric authentication. Watermarking is the art of embedding or hiding critical data into unsuspected multimedia content, so that it's imperceptible for humans and hence doesn't affect the quality of the multimedia content [2]. The main components of a watermarking system are an *embedder* and a *detector* (See fig. 5).

Watermarking systems can be designed to use keys in an analogous manner to encryption. The key is used to cast, detect and remove a watermark [17]. The idea is to make it impossible to detect the presence of a watermark in a work without knowledge of the key, even if the watermarking algorithm is known. Further, by restricting the access to the key, it is extremely difficult, if not impossible, for attackers to remove the watermark without causing significant degradation in the fidelity of the cover work.

Although watermarking algorithms were first developed to protect multimedia from illegal use, or sharing, it has recently emerged as one of the ways to protect iris templates. Besides offering secure transmission and storage of iris templates, it also provides a means for proving ownership by using a specific cover for every organization and/or application. If the iris template is "hidden" within another biometric representation, it also offers a way for multimodal biometric authentication as well as iris template protection. In recent years there has been some attempts to protect iris templates by watermarking them, so as to detect any tampering with the original template [20].

Hybrid Iris Template Security Scheme

Hybrid Iris Template Security Scheme is a system that combines a key binding biometric cryptosystem using revocable iris codes with a watermarking algorithm. This system has multi-layers of security, which decreases the chance of the database being compromised even if one of the keys is revealed. The combination of these methods aims to benefit from the strengths of each method, as well as complexity in trying to breach the security of the iris templates.

Haptic-biometric Iris Template Protection

With recent advances in both the hardware and software for three dimensional applications, virtual environments are growing in popularity. Haptic devices offer a more immersed interaction between users and the virtual environments; and

with the growing use of the internet to connect more users and arises the need to authenticate their identity in a secure manner. Identifying users by their interaction with haptic devices is an emerging research field that is proving promising, but like all biometric based authentications relies on the uniqueness of the stored template, which poses a risk if the iris template is compromised, because unlike passwords and pins, iris templates are irrevocable. Virtual environments have long exploited the visual and hearing senses of the users and recently haptic devices that offer tactile/force feedback have greatly enhanced the user experience in those virtual environments. Haptic devices also offer a means to authenticate users by their behavioral interaction with such devices [3] [12] in a similar way to keystroke dynamics [13] and two dimensional handwritten signatures [9]. These behavioral biometrics not only provide initial authentication like passwords, but they also provide continuous authentication throughout the duration of the interaction if desired.

V. Summary And Conclusion

Here, we have discussed various types of attacks that can be launched against an iris recognition system. We have discussed various types of iris template protection techniques that can be used for a secure iris recognition system. We have specifically highlighted techniques that can be used to protect the contents of an iris template and secure the system for personal authentication.

References

[1] A. Adler, "Images can be Regenerated from Quantized Biometric Match Score Data," in Proceedings Canadian Conference on Electrical and Computer Engineering, Niagara Falls, Canada, May 2004, pp. 469–472.
[2] A. Edler, "Can sample images be regenerated form biometric templates", Proceeding of Biometrics consortium conference 2003, Hyatt Regency Crystal City, Arlington, VA, USA.
[3] A. El Saddik, M. Orozco, Y. Asfaw, S. Shirmohammadi, A. Adler. "A Novel Biometric System for Identification and Verification of Haptics Users". IEEE Transaction on Instrumentation and Measurement, June 2007, Vol.56, No. 3.
[4] A. Juels and M. Wattenberg, "A fuzzy commitment scheme", CCS 1999: Proceedings of the 6th ACM conference on Computer and communications security,1999, pp. 28-36.
[5] A. K. Jain, K. Nanda Kumar and A. Nagar, "Biometric Template Security", EURASIP Journal on Advances in Signal Processing, Special Issue on Advanced Signal Processing and Pattern Recognition Methods for Biometrics, January 2008.
[6] A. K. Ross, J. Shah, and A. K. Jain, "From Templates to Images: Reconstructing Fingerprints From Minutiae Points," IEEE Transactions on Pattern Analysis and Machine Intelligence, 2007, Vol. 29, No. 4, pp. 544–560
[7] A. Vetro and N. Memon, "Biometric System Security," Tutorial presented at Second International Conference on Biometrics, Seoul, South Korea, August 2007.
[8] C. S. Chin, A. B. J. Teoh, and D. C. L. Ngo, "High Security Iris Verification System Based On Random Secret Integration", Computer Vision and Image Understanding, May 2006, Vol. 102, No. 2, pp. 169–177.
[9] E. Maiorana, P. Campisi, A. Neri, "Feature Selection and Binarization for On-line Signature Recognition", 3rd IAPR/IEEE International Conference on Biometrics (ICB 2009), June 2009, Alghero , Italy.
[10] E. S. Reddy, I. R. Babu, "Authentication Using Fuzzy Vault Based on Iris Textures", Second Asia International Conference on Modeling & Simulation, AICMS 08, 2008, pp. 361 – 368.
[11] E.S. Reddy, I.R. Babu; "Performance of Iris Based Hard Fuzzy Vault", IEEE 8th International Conference on Computer and Information Technology Workshops, July 2008, pp. 248 – 253.
[12] F. A. Alsulaiman, J. Cha, A. El Saddik, M. Ferre, "User Identification Based on Handwritten Signatures with Haptic Information", Haptics: Perception, Devices and Scenarios, Springer Berlin / Heidelberg, 2008, pp. 114-121.
[13] F. Monrose, A. Rubin, "Authentication via keystroke Dynamics", in the proceedings of 4th ACM Conference of Computer and Communication Security. 1997. pp. 48-56.
[14] F. Petitcolas, R. Anderson, M. Kuhn, "Information Hiding – A Survey", in the proceedings of the IEEE Conference, July 1999, Vol. 87, No.7, pp. 1062–1078.
[15] G. I. Davida, Y. Frankel, B. J. Matt, "On enabling secure applications through online biometric identification" in the proceedings of IEEE Symposium on Privacy and Security, May 1998, pp. 148–157.
[16] G. I. Davida, Y. Frankel, B. J. Matt, R. Peralta, "On the relation of error correction and cryptography to an offline biometric based identification scheme", in the proceedings of the Workshop of Coding and Cryptography, 1999, pp. 129–138.
[17] G. Voyatzis, N. Nikolaidis, I. Pitas, "Digital Watermarking: An Overview", 9th European Signal Processing Conference (EUSIPCO'98), 1998.
[18] J. Bringer, H. Chabanne, G. Cohen, B. Kindarji, G. Zémor, "Optimal iris fuzzy sketches", IEEE First International Conference on Biometrics: Theory, Applications and Systems, BTAS'07, 2007.
[19] J. Zuo, N.K. Ratha and J.H. Connell , "Cancelable iris biometric", 19th International Conference on Pattern Recognition (ICPR), December 2008, pp.1-4.
[20] M. Vatsa, R. Singh, P. Mitra, A. Noore, "Comparing robustness of watermarking algorithms on biometrics data", in the proceedings of the Workshop on Biometric Challenges from Theory to Practice – ICPR Workshop, 2004, pp. 5–8.
[21] N. K. Ratha, J. H. Connell, and R. M. Bolle, "Enhancing security and privacy in biometrics-based authentication systems", IBM Systems Journal, 2001, Vol. 40, No. 3, pp. 614-634.
[22] N. Ratha, and J. Connell, "Cancelable Biometrics", presented at Biometric Consortium 2000 Conference, Sept. 2000.
[23] Rajeev Gupta and Ashok Kumar, "Noisy Iris Recognition & its importance", Journal of Ultra Scientist of Physical Sciences International Journal of Physical Sciences, Aug. 2013, Vol 25(2)B, pp. 229-234
[24] S. Kanade, D. Camara, E. Krichen, D. Petrovska-Delacretaz, B. Dorizzi; "Three factor scheme for biometric-based cryptographic key regeneration using iris", Biometrics Symposium, BSYM '08, Sept. 2008, pp. 59-64.
[25] S.Kanade, D. Petrovska-Delacretaz, B. Dorizzi,; "Cancelable iris biometrics and using Error Correcting Codes to reduce variability in biometric data", IEEE Conference on Computer Vision and Pattern Recognition, CVPR 2009, June 2009, pp. 120 – 127.
[26] U. Uludag and A. K. Jain, "Attacks on biometric systems:a case study in fingerprints", in the proceedings of SPIE, Security, Steganography and Watermarking of Multimedia.
[27] Y. Dodis, R. Ostrovsky, L. Reyzin, and A. Smith, "Fuzzy Extractors: How to Generate Strong Keys from Biometrics and Other Noisy Data", EUROCRYPT 2004, February 2006.
[28] A. K. Jain, S. Pankanti, R. Bolle, "BIOMETRICS: Personal Identification in Networked Society", Kluwer Academic Publishers, 1999.
[29] C. Soutar, D. Roberge, A. Stoianov, R. Gilroy, B.V.K. Vijaya Kumar, "Biometric Encryption™", Chapter 22 in ICSA Guide to Cryptography, edited by Randall K. Nicholls, McGraw Hill, pp. 649-675, 1999.
[30] D. Maltoni, D. Maio, A. K. Jain, S. Prabhakar, "Handbook of Fingerprint Recognition", Springer-Verlag,2003.
[31] I.J. Cox, M. Miller, J. Bloom, "Digital Watermarking", Morgan Kaufmann Publishers, 2002.