Multi-Secure Authentication using Sift Algorithm in Biometric Cryptosystem

R. K. Rakesh Raja
University College of Engineering, Nagercoil

T. Viveka
Assistant Professor, TF, University College of Engineering, Nagercoil

Abstract – Most of the system breaches are caused by authentication errors during the login process and these failures are caused due to the limitations associated with existing authentication methods. The existing proxy-based biometric authentication methods are not user-centric and put the security and privacy of users in danger. A user-centered approach is proposed based on biometric authentication and this approach is secure and able to defend various attacks, thus the security of the user's biometrics is guaranteed and the user privacy is preserved. This method consists of introducing a reference subject that merges with user's biometrics, generating a BioCapsule(BC) and employing these BioCapsules for authentication. Such an approach is easy to use, identity bearing yet privacy-preserving, resilient and is revocable once the BioCapsule is compromised. The process of registration and verification of the biometric modality will take less time to produce the output. This method effectively reduces the processing time and increases the accuracy rate. The BC mechanism is generally applicable to typical biometric modules as it can be fed into newly designed biometric systems to continuously enhance the authentication accuracy.

Index terms – Authentication, cancelable biometrics (CB), biometric cryptosystem (BCS), BioCapsule (BC), secure fusion.

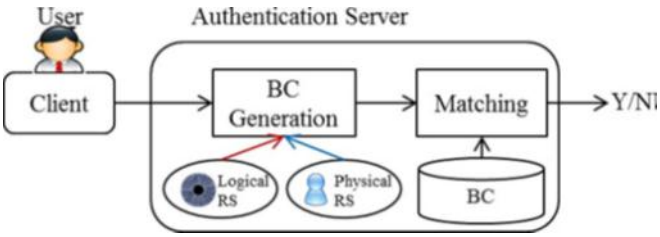
1. INTRODUCTION

User-proxy based authentication is well developed and widely used, it is also both effective and efficient in user authentication. However, the growth in user-credential theft in proxy based authentication and increased security requirements have prompted investigation of alternative authentication. The central theme of authentication is to authenticate users using characteristics intrinsically linked with human users rather than some external factors. A promising direction emerging from this effort is biometrics. Currently, the further adoption of biometrics is limited by the security of users' biometric templates extracted in the biometric authentication process: they are irreplaceable once compromised, and original biometric data can be reconstructed from the biometric templates.

A biometric template is derived from a user's biometric data and contains the user's private information, thus its compromise may divulge sensitive information (e.g., gender, possible disease). Intensive research has been conducted to address the security and revocability of biometrics, as well as user privacy; concepts such as biometric cryptosystem (BCS) have emerged from this research. There are limitations associated with both BCS and CB, compared to conventional biometric systems, BCS displays a noticeable decrease in performance this is due to the hardness of alignments of biometrics and a higher degree of quantization at feature level. Also for the BCS, the system performance and key entropy are highly related, and a direct relation between the maximum length of keys and the error rates has been identified, which is defined as k log2FAR, where FAR is the false acceptance rate (FAR). For a generic cryptographic purpose (e.g., with a 128-bit key) maintaining a FAR 2k is very difficult. For the CB, provable security (e.g., irreversibility and cross-matching resistance (CMR) is rarely done, and for some approaches it is extremely a sophisticated work. Similar to BCS, in the case of hardness of alignments of biometrics and the complexity of transformation, performance decrease is also observed. However, some such approaches have reported an increase in performance, especially when introducing a user-specific external factor (e.g., PIN/token). This performance gain is based on impractical assumptions during evaluation, and the user-specific transformation parameters must then be assumed compromised for such evaluation. An ideal secured biometric system possesses various properties: security, privacy-preservation, cross matching resistance, etc. And existing BCS and CB approaches cannot fully address one or more of these properties.

In this research, we propose a Bio Capsule (BC) and use the BC for user authentication (and identification as well) to address these issues in a comprehensive manner. The BC generation in is based on the difference of the user's biometric feature and that of a proposed reference subject (RS). There are, however, some limitations related to this difference based BC design. First, generation is at the feature level, thus scope is limited. Second, the formal security proof is difficult to obtain and it generally assumes that the RS is a physical entity and physically protected. In this paper, we present a unique BC generation method based on "secure fusion" of the user biometrics and the RS biometrics. The fusion process applies

to different stages of biometric processing such as signal, feature or template level. The fusion based BC construction is more usable and flexible, while also secure, resilient to different attacks, and tolerant to the disclosure of both the RS and BC.



.

Fig. 1 Authentication Process

An optimization framework for resource provisioning was developed. This framework considered multiple client QoS classes under uncertainty of workloads.

2. RELATED WORK

Emerging techniques for user authentication involve traditional biometric authentication, cognitive authentication, BCS, CB and the hybrid approach. Traditional biometrics binds users to their biological traits, either physiological traits (e.g., iris, palm print, sclera) or behavior traits (e.g., mouse dynamics, gait). As indicated previously, a limitation of traditional biometrics is security, user privacy risk and irreplaceability. Cognitive biometrics can be used to improve the revocability property. Cognitive biometrics represents a new approach which generates a "thought signature" of people using biological signals that characterize the brain's response to certain stimuli, giving a high degree of uniqueness to the individual. Revocability is provided by training a new thinking process and generating a new "thought signature" to replace the compromised one. However, catching brain signals requires special equipment. Also, the thinking process may change over time. Biometric cryptosystems can be used for user authentication by matching the exactness of the outputted keys. The majority of BCSs require some biometric-dependent public information (known as helper data), which is not supposed to reveal much information about the biometrics; with the helper data, the cryptographic key is retrieved or extracted from the query biometrics. The helper data are either obtained by binding a chosen key to biometrics or derived only from biometrics. BCSs use different techniques to deal with biometric variance; for example, some schemes apply error correction codes, while some others apply quantization. The introduction of helper data, in some circumstances (e.g., when multiple copy of helper data extracted from the single biometrics are obtained) may create vulnerabilities. However, without using helper data it is believed that extracting a sufficiently long and revocable key is not feasible because of the information entropy limitation of most biometric characteristics. Utilizing error-correction codes and cryptography, a concept secure sketch is generalized which allows error correction of a noisy input. Secure sketches can be used as primitives to build fuzzy extractors which extract a uniformly random string. Secure sketches and fuzzy extractors, as primitive formalisms, have been used in concrete BCSs. Quantization has also been used frequently in BCSs. In the BCS using quantization techniques, several enrollment samples are trained to derive appropriate intervals for feature quantization. As in, the authors apply a context-based reliable component selection and construct intervals for the most reliable features of each subject. Such approaches require multiple samples from each subject to reliably extract helper data. Cancelable biometrics applies a transformation on traditional biometrics and matches the biometrics in a transformed domain for authentication. Cancelable biometrics was first introduced, it presented a CB approach using random projections which embed biometrics from a higher dimensional space to a lower dimensional space; however, it is shown that the system is less secure if an attacker obtains both the random projection parameters and the transformed patterns.

3. PROPOSED MODELLING

The proposed authentication system contains two stages as shown in Fig. 1: registration and verification. For registration, user biometrics is sampled and fused with the RS biometrics; from the fused biometrics a user's BC is generated and stored (in the system database). Upon a verification request, user biometrics is re-sampled and fused with the RS biometrics. Again from the fused biometrics a user BC is derived which is further compared to the stored BC (of an individual). If the two BCs are close enough according to some distance metric, the user is authenticated as the individual. Selection and setting of RS in the system.

The RS can be a physical one or a logical one. A physical RS is some object from which RS biometrics can be sampled on-the-fly, and a logical RS can be a biometric image. RS is a system-wide object and managed by the authentication system, not by a user, which frees users' burden on carrying or memorizing something. Typically, RS is configured with the authentication server; since the compromised RS will not jeopardize the biometric security and users' privacy, the RS can also be located on client sites. For example, a RS can be configured on client computers at security check points which scan the RS and passenger biometrics and send then the computed BC to the authentication server for authentication.

A diagram of a system with the RS at the authentication server. The user's biometrics is captured via (built in) camera of the authentication client and sent to the authentication server. Through some preprocessing (omitted in the figure), the user biometrics is fused with the RS biometrics which is either sampled against a physical object on-the-fly or a logical one stored in the server. The server matches the generated BC against the BC stored in the BC database for an authentication

decision ("Y/N"). Where to locate and how to configure the RS in a system depends on the system's configuration, security, and application requirements, such as whether a secure transmission channel exists between the authentication server and the user client, and whether the computer used as the authentication server is powerful enough to sample and compute BC without becoming a performance bottleneck. In most critical environments such as military systems and nuclear power stations, a physically protected RS should be used, since a physical RS will prevent attackers from trying to compromise RS remotely. The RS can be considered as a (system-wide) salting mechanism. This mechanism needs the extracted key and features from the RS for salting. A random secret key may be directly used as the RS. It is not clear whether a random secret key has the characteristics of a biometric image such that the secret key and features can be extracted and then fused with the user biometrics. And it is worthy of further efforts to investigate if using a random secret key (as a logical RS) for salting can give us the same security strength and matching performance as does a biometric RS. Design criteria for the BC. To design an effective fusion and BC construction mechanism, there are following considerations:

1. What impact does the fused biometrics have on the matching performance? Are the users still representable by the fused biometrics? If the user biometrics is surpassed by the RS biometrics, the fused biometrics will be less discriminative thus will deteriorate matching performance.

2. Are the user biometrics and the fused biometrics correlated, or are the fused biometrics using different RSs correlated? If there is a strong correlation, there would be a vulnerability of cross-matching thus infringing user privacy.

4. RESULTS AND DISCUSSIONS

To create a personalized RS, a user-intrinsic key is extracted from the user's biometrics and used as the transformation parameters to the RS. We propose a lightweight key extraction considering the following criterion:

1. To facilitate usability, the key is directly generated from the user biometrics, thus avoiding the need for a user to memorize a password or carry a token to provide transformation parameters. Also, this key is directly generated from user biometrics and is user intrinsic, making its compromise significantly more difficult when compared to factors artificially bound to a user.

2. Since the keys are not used for authentication, the BC approach does not require 100 percent stable and user-distinct keys (as do some BCSs).

3. The conflict between key stability and distinguishability should be optimally balanced, since it will create further impact on the fusion of biometrics. Intuitively, completed stability will reduce distinguishability. Moreover, noisy features of different samplings of biometrics create constraints on stability, unless more helper data is used. On the other hand, complete distinguishability necessitates the use of complicated fuzzy handling techniques such as error correction codes. The compromised biometric credential needs to be revoked and replaced by a new one to prevent the attacker from injecting the compromised one directly into the system if the attacker is extremely powerful. Also the periodic update of biometric credentials is a useful practice which will enhance the security of the system and protect a user's privacy. The revocability is closely related to the diversity and cross-matching resistance of the system; based on the same biometrics a new credential can be generated, and the compromised biometric credential cannot be matched against the new one.

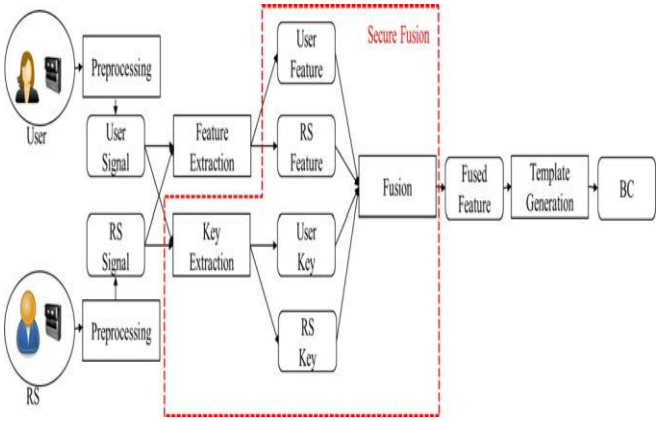


Fig. 2 Integration of the secure fusion (red box) with existing biometrics processes at feature level.

Preprocessing, feature extraction and template generation approaches without modification; it applies the "secure fusion" before the template generation and after the feature extraction. This property not only makes the proposed fusion more deployable but also keeps the same domain of inputs and outputs, thus theoretically enabling the fusion at other levels (e.g., signal, template) we illustrate the concrete integration of "secure fusion" with 2D Gabor. Through the integration of "secure fusion" with existing biometric procedures, a complete BC generation process is given as follows: preprocessing, feature extraction and template generation approaches without modification; it applies the "secure fusion" before the template generation and after the feature extraction. This property not only makes the proposed fusion more deployable but also keeps the same domain of inputs and outputs, thus theoretically enabling the fusion at other levels (e.g., signal, template). Next, we illustrate the concrete integration of "secure fusion" with 2D Gabor. Through the integration of "secure fusion" with existing biometric procedures, a complete.

4.1 Security Analysis

The system logically stores BCs and RS (if a logical RS is used). In this section, we prove the security of the users'

biometrics (i.e., privacy preservation) of the BC approach cons idering BCs and/or RS are compromised.

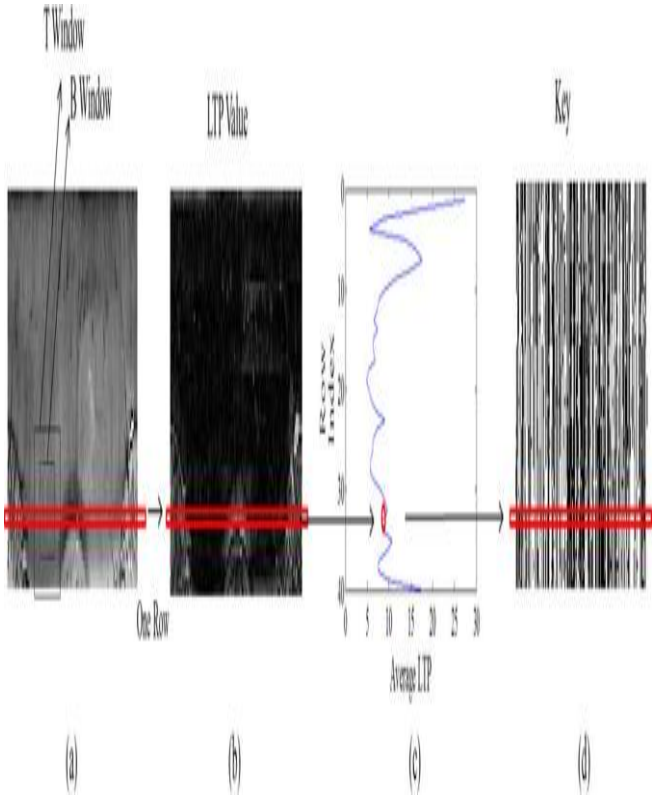
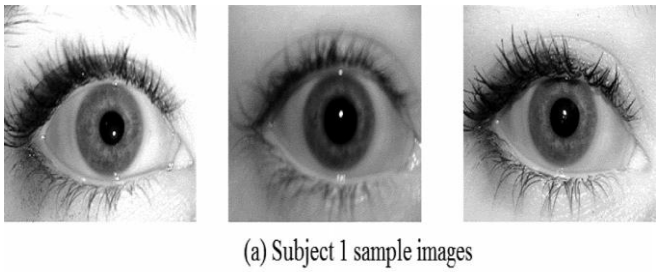
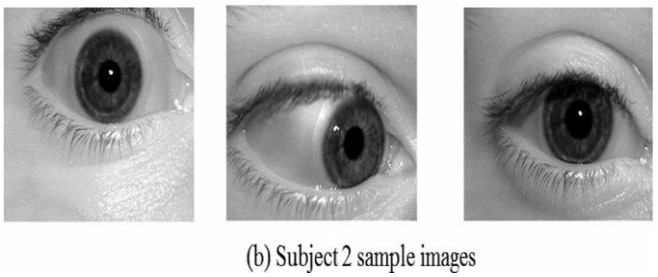


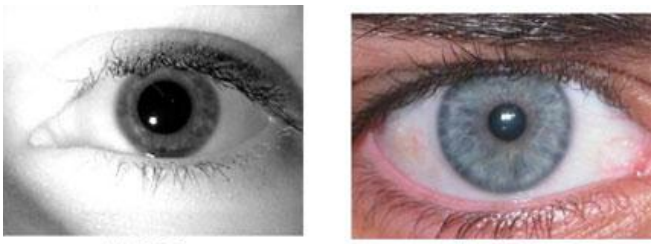
Fig 3. Key Extraction process



(a) Subject 1 sample images



(b) Subject 2 sample images



(a) RS 1 (b) RS 2

Fig. 4. Sample images of two subjects from NIST/ICE.

This is an interval linear system, and solving such a system is NP-hard, where the NP-hardness of solving the problem is due to the computational complexity of the problem itself. The running time to solve the problem grows exponentially with the number of unknowns. In our case, the number of unknowns is 12,000 (i.e., 12,000 features of RS). Such NP-hardness makes it practically infeasible to derive the RS, thus the system is resilient to the internal collusion attack. The above two attacks are against the RS. However, even if the RS is determinable, determining the RS helps no further if the attacker acquires another user's BC and tries to derive this user's biometrics. Following Theorem 2, user biometrics is secure against a lost RS and the user's BC. 5) Security against internal Cross-RS attack.

4.2 Experiment Setting

The performance of the proposed technique was tested on the ICE database which is provided by National Institute of Standards and Technology (NIST) for the Iris Challenge Evaluation (ICE) 2005. The ICE database contains 1,426 images from the right eye from 132 subjects, and 1,527 images from the left eye from 132 subjects. These images were collected with the LG EOU 2200 and intentionally represent a broader range of quality than the camera would normally acquire. This includes iris images that did not pass the quality control software embedded in the LG EOU 2200. And they were all used in our experiments.

The ICE 2005 is commonly used by academic institutions, research laboratories and companies and is a benchmark database used for system evaluation. Sample images from ICE 2005 database are provided in Fig. 4. We chose an iris image from the UBIRIS and one iris image from ICE as our RS iris image as shown in Fig. 8. If the RS is a logical one (e.g., an image stored in the system), it will display no image distortion. If the RS is a physical one, there will be some degree of image distortion on the obtained RS image for each sampling. To produce multiple distorted RS images for simulation, as suggested by Jung et al. we introduced random white Gaussian noise with signal-to noise ratio (SNR) 40 into a logical RS image considering that the International Organization for Standardization (ISO) suggests the SNR of an iris camera should be better than 40 db. Due to the fact that the physical RS was not a live person that demonstrates pupil focusing,

defocusing, head tilting and so on, we did not introduce defocus blurring in the sampled RS images. For the approach evaluation, using the physical RS setting we provide the receiver operating characteristic (ROC) as well as the probability distribution of inter-class and intra-class matching (Note: if we assume a stable RS, we get similar matching results, which are thus omitted). Fig. 4. Sample images of two subjects from NIST/ICE.

4.3 Key Stableness and Distinguishability

Key stableness and distinguishability were investigated; this experiment consisted of matching the extracted keys against each other. For example, in the ICE database with 2,953 images, 2; 953 _ 2; 952 matches are performed.

4.4 Identity-Bearing of the BC

This experiment tested the identity-bearing of the BC. To establish this, we constructed a BC for each image from the ICE database using the RS1 (i.e., Fig. 8a). For the BC generation, 1D Log-Gabor was used for feature extraction. To make a comparison, we also implemented 1D Log-Gabor Iris Code. The experimental results are shown In particular, compares the ROC, and Fig. 10b compares the intra-class and inter-class distribution. These curves are quite overlapped, which indicates that the BC mechanism maintains the identity-bearing of the original Iris Code quite well. From this experiment, we observe that when the keys are not as stable, their application in the fusion makes the "matching" of biometrics less similar. However, inter-class and intra-class matching follow the same trend as indicated by the left shifting from Iris Code curves to BC curves). As the inter-class and intra-class distributions are both left-shifted, the BC keeps the distribution as distinguishable as the original biometrics, while properly maintaining the system performance.

Applicability of the BC to Existing Biometric Modules This experiment tested the applicability of the BC to existing biometric modules. We implemented the BC approach using RS1), and either 1D Log-Gabor or 2D Gabor were used for the feature extraction. To make a comparison, we also implemented 1D Log-Gabor and 2D Gabor Iris Code. As the experimental results show in both generally applicable to existing biometric modules, e.g., 1D Log Gabor, 2D Gabor, and possibly others. 3.5 Effect of Image Quality on the BC Performance This experiment tested the effects of image quality on BC performance. We applied the BC approach on the entire image set and quality image of entire set can be observed that both IrisCode approaches and the BC approach perform better on quality images. Also the BC approach shows comparable performance to the Iris- Code, thus maintaining the performance of the traditional biometrics regardless of the image quality.

4.5 Revocability

To satisfy the property of revocability, BCs using different RSs, generated from a single user subject, have to appear random to themselves (like BCs of different subjects). To establish this, we constructed BCs using RS1 and BCs using RS2 (i.e., Fig.). The two sets of BCs are cross-matched. Fig. shows quite overlapped intra-class (genuine) andinter-class (impostor) distributions. The mixed distributions indicate that it is hard to determine whether or not two BCs (i.e., one from RS1, and the other from RS2) are from the same user. In this sense, we argue that the old BC cannot be used to identify or authenticate a user by comparing it to the new BC, and thus is revoked.

4.6 Cross-Matching Resistance of the BC

The purpose of this experiment is to test cross-matching resistance of the BC. We consider two cases: 1) system 1 uses the BC technique, and system 2 uses the IrisCode technique; and 2) system 1 and system 2 both use the BC technique, but with different RSs. To be cross-matching resistant, biometric credentials from different systems, generated for a single user subject, have to appear random to themselves (like BCs of different subjects). Further, the matchings have to appear random (inter-class and intra-class distributions are mixed). Fig. shows the genuine and impostor distribution of matching Iris Codes to BCs. The more mixed distribution indicates in distinguishability from Iris Code to BC, which also indicates good capability of defeating cross-matching attack. The cross-matching resistance of the BCs using different RSs is equivalent to the revocation, which is well established.

5. CONCLUSION

In this paper, a user-friendly, secure, privacy-preserving and revocable secure-fusion based biometric authentication method is used. The proposed approach involves key extraction: the extracted key is used in a "secure fusion" for mixing the user's biometrics and a reference subject's biometrics, and the fused biometrics is fed into an existing biometric system to generate a BioCapsule for authentication. The proposed BC mechanism has many desired features: 1. security analysis shows that the approach is secure and able to defeat various attacks, thus the security of the user biometrics is guaranteed and the user privacy is preserved; 2. experimental results prove the revocability of the proposed approach; 3. both security analysis and experimental results justify the cross-matching resistance of the proposed approach; 4. with existing approaches and the experimental results show comparable performance to traditional approaches and other BCS and CB systems; 5. the BC mechanism is generally applicable to typical biometric modules verified through experiments, thus, it can be fed into newly designed biometric systems to continuously enhance the authentication accuracy in the long run; 6. the cross matching resistance enables the interoperability of the BC system, and it

supports “one-click sign-on” across multiple systems by using a distinct RS; and 7. the system does not require user training, and is both easy to use and transparent to end-users since they are not required to remember a password or carry a token. These features make the proposed BC mechanism a user-centric authentication approach. We will continue to extend our study to other biometrics (e.g., face) and investigate the integration of the fusion at different biometric processing levels. We are also interested in extending the application of the proposed BC mechanism in a broader context, for instance, active and non-intrusive authentication.

REFERENCES

[1] http://en.wikipedia.org/wiki/Usability, 2013.
[2] http://iris.nist/gov/ice/, 2013.
[3] A. Ahmed and I. Traore, “A New Biometric Technology Based on Mouse Dynamics,” IEEE Trans. Dependable and Secure Computing, vol. 4, no. 3, pp. 165-179, July/Sept. 2007.
[4] T. Boult, “Robust Distance Measures for Face- Recognition Supporting Revocable Biometric Tokens,” Proc. Seventh Int’l Conf. Automatic Face and Gesture Recognition, pp. 560-566, Apr. 2006.
[5] T. Boult, W. Scheirer, and R. Woodworth, “Revocable Fingerprint Biotokens: Accuracy and Security Analysis,” Proc. IEEE Conf. Computer Vision and Pattern Recognition.
[6] X. Boyen, “Reusable Cryptographic Fuzzy Extractors,” Proc. 11th ACM Conf. Computer and Comm. Security (CCS ’04), pp. 82-91, 2004.
[7] J. Bringer, H. Chabanne, G. Cohen, B. Kindarji, and G. Zemor, “Theoretical and Practical Boundaries of Binary Secure Sketches,” IEEE Trans. Information Forensics and Security, vol. 3, no. 4, pp. 673-683, Dec. 2008.
[8] I. Buhan, J. Breebaart, J. Guajardo, K. de Groot, E. Kelkboom, and T. Akkermans, “A Quantitative Analysis of Indistinguishability for a Continuous Domain Biometric Cryptosystem,” Proc. 4th Int’l Workshop, and Second Int’l Conf. Data Privacy Management and Autonomous Spontaneous Security, pp. 78-92, 2010.
[9] I. Buhan, J. Doumen, P. Hartel, and R. Veldhuis, “Constructing Practical Fuzzy Extractors Using QIM,” Technical Report TRCTIT- 07-52 2007.
[10] R. Cappelli, A. Lumini, D. Maio, and D. Maltoni, “Fingerprint Image Reconstruction from Standard Templates,” IEEE Trans. Pattern Analysis and Machine Intelligence, vol. 29, no. 9, pp. 1489-1503, Sept. 2007.
[11] CASIA-IrisV1. http://biometrics.idealtest.org/, 2013.
[12] A. Cavoukian and A. Stoianov, “Biometric Encryption,” Encyclopedia of Biometrics. Springer, 2009.
[13] E. Chang, R. Shen, and F. Teo, “Finding the Original Point set Hidden among Chaff,” Proc. ACM Symp. Information, Computer and Comm Security (ASIACCS ’06), pp. 182-188, 2006.
[14] K. Cheung, A. Kong, D. Zhang, M. Kamel, and J. You, “Revealing the Secret of Facehashing,” Proc. Int’l Conf. Advances in Biometrics, pp. 106- 112, 2006.
[15] K. Cheung, A. Kong, D. Zhang, M. Kamel, J. You, and H. Lam, “An Analysis on Accuracy of Cancellable Biometrics Based on Biohashing,” Proc. Ninth Int’l Conf. Knowledge-Based Intelligent Information and Eng. Systems (KES ’05), pp. 1168-1172, 2010.