The 9th International Conference on Business Information Security (BISEC-2017), 18th October 2017, Belgrade, Serbia

SECURE MODULAR AUTHENTICATION SYSTEMS BASED ON CONVENTIONAL XOR BIOMETRICS

NEMANJA MAČEK
School of Electrical and Computer Engineering of Applied Studies, Belgrade and eSigurnost Association, Belgrade, macek.nemanja@gmail.com

MILAN MILOSAVLJEVIĆ
Singidunum University, Faculty of Technical Sciences, mmilosavljevic@singidunum.ac.rs

IGOR FRANC
Belgrade Metropolitan University, Faculty of Information Technologies and SECIT Security Consulting, igor.franc@metropolitan.ac.rs

MITKO BOGDANOSKI
Military Academy General Mihailo Apostolski, Skoplje, Macedonia, mitko.bogdanoski@ugd.edu.mk

MILAN GNJATOVIĆ
University of Novi Sad, Faculty of Technical Sciences, milangnjatovic@uns.ac.rs

BRANIMIR TRENKIĆ
School of Electrical and Computer Engineering of Applied Studies, btrenkic@viser.edu.rs

Abstract: *This paper presents an approach to designing secure modular authentication system based on conventional XOR biometrics. System consists of one or more clients, an authentication server and a trusted storage. Client is a device used to capture biometrics, obtain auxiliary data and create encrypted cancelable templates during the enrolment and verification phases. Authentication server manages encryption keys and verifies cancelable templates, while the trusted storage, which can be either distributed or centralized, stores the encrypted templates. Two important characteristics of the proposed system are that it keeps biometric templates encrypted or cancelable during all stages of storage, transmission and verification, and that it does not suffer from severe computational costs and large sizes of encrypted templates like systems based on homomorphic encryption. Additionally, system is general (i.e., it does do not depend on specific cryptographic algorithms) and modular, which allows a user enrolled on one client to verify his identity on another client connected to the same authentication server. Finally, security of the system is compared with the requirements of a cryptographically secured biometric system that provides strong privacy protection.*

Keywords: *Biometrics, Authentication, Security, Cryptography*

1. INTRODUCTION

Biometric authentication is the process of establishing user identity based on physiological or behavioral qualities of the person [1, 2]. Biometrics can be addressed as an ultimate authentication solution: users do not need to remember passwords or carry tokens and biometric traits are distinctive and non-revocable in nature [3], thus offering non-repudiation [4]. However, like any personal information, biometric templates can be intercepted, stolen, replayed or altered if unsecured biometric device is connected to a network or if a skilled attacker gains physical access to a device. A brief surveys of attacks on biometric authentication systems, such as replaying old data, stored template modification and communication chanell interception are given in [5, 6]. Due to non-revocability of biometric data aforementioned attacks and misuses may lead to identity theft. Having that said, it becomes clear that biometric systems operate with sensitive personal information and that biometric template security and privacy are important issues while designing such authentication systems. To counterfeit identity theft, one should not rely on administrative countermeasures or misuse identification upon successful attack [7], followed by erradiction and recovery from damages caused by illegimite access to the resources. Identity theft should be prevented with technological countermeasures that provide sufficient level of security and privacy while downgrading the performance of the system (computational costs and storage requirements) to the reasonable level.

One approach to biometric template security and privacy is cancelable biometrics. Cancelable biometrics refer to intentional distortion of biometric features with non-invertible transforms [8]. In this scenario, while verifying the user the same transform is applied to a given sample as in enrolment phase. If template is considered to be compromised, it's revoked, as large number of transforms are available. If a non-invertible transform operates with a key, template is revoked and only the key is changed during template update. Examples of cancelable transforms are given in [9-11]. Non-invertible transforms are, however, not a fail-safe solution to a problem. They may

be computationally expensive, partially reversible and they degrade overall accuracy of the system. Additionally, system is vulnerable to substitution attack if an adversary who knows how the transform operates creates a masquerade sample.

Another approach to providing template privacy is the application of homomorphic encryption schemes [12, 13]. Homomorphic encryption refers to cryptographic algorithms that allow some computations to be performed in the encrypted domain. These schemes appears to be suitable for application in conventional XOR biometric systems (for example, iris based systems) as these systems use bitwise XOR to calculate Hamming distance during verification. Although applicable in theory, there are two reasons why homomorphic encryption is not actually practical: the encrypted template is large and the system is computationally expensive. According to [13], calculating the Hamming distance between two encrypted 1024 bit templates would take approximately 10 minutes on 2GHz processor.

The main contribution of this paper is a general secure modular authentication architecture based on conventional XOR biometrics applicable to a variety of real-life scenarios. An approach presented in this paper employs public key cryptography, pseudorandom number generators and cancelable biometrics. Non-invertible transform operates with the key stored on a token, thus reassembling two-factor authentication. The system does not suffer from the drawbacks of homomorphic encryption as cryptographic operations are not computationally expensive and no large templates are created. As stated before, biometric templates are encrypted or at least remain cancelable during all stages of operation (excluding feature extraction) resulting in a system prone to variety of attacks. Also, the system satisfies the requirements of a cryptographically secured biometric system that provides strong privacy protection listed in [7].

2. AN OVERVIEW OF ATTACKS ON BIOMETRIC SYSTEMS

Biometric systems, as all traditional systems are susceptible to variety of threats: Denial of Service, circumvention, repudiation, contamination, coercion and collusion [14]. Aforementioned threats are used to make attacks on biometric authentication systems. Eight different attack on unimodal biometric authentication systems consisting of sensor, feature extraction, matching and decision making modules have been identified in [15]. These include: sensor attack, replay attack (bypassing the sensor), attack on the feature extraction module, attack on the channel between feature extractor and matcher, compromising the database, attack on the communication channel between template database and the matcher and overriding the result declared by the matcher module. More on the protection from these attacks can be found in [16]. Attacks on biometric encryption systems (such as hill-climbing attack [17], non-randomness attacks [18], re-usability attack [19], blended substitution attack [20] and linkage attack [21]) are usually more complex when compared to traditional biometric authentication systems. The goal of an adversary is to reduce the search space, obtain the key or to create a masquerade version of biometrics [7].

3. MODULAR BIOMETRIC SYSTEMS AND SECURITY REQUIREMENTS

As mentioned before, biometric authentication systems consisting of four modules that reside in one device are vulnerable to variety of attacks [15]. To prevent execution of these attacks, entire system is split into three high-level modules (residing on at least two devices) and both cancelable biometrics and strong cryptographic protection are introduced to the system. The modular system now contains of: one or more clients (devices used to capture biometrics, obtain auxiliary data from the user and create encrypted cancelable templates), an authentication server (device that manages encryption keys and verifies cancelable templates) and a trusted storage that stores the encrypted templates. If two or more clients are used within the system, and a user enrolled on one client should be allowed to verify his identity on another client connected to the same authentication server, template storage must be centralized. As the proposed system deals with the XOR biometrics, a transform that reassembles the one-time-pad cypher is used.

Aside from cryptographic security, system is expected to provide strong privacy protection, resulting in the following set of requirements: (1) biometric templates remain encrypted or at least cancelable during all stages of storage, transmission and verification (e.g. authentication server should never obtains unencrypted biometric templates) and (2) no client is allowed to access private keys stored on authentication server as it may compromise the security of the templates. Further, resilience to a template substitution attack and all low level attacks is expected, the system should not suffer from severe computational costs and cryptographic countermeasures should not degrade the overall accuracy (i.e. they should not increase false acceptance or false rejection rates).

4. SYSTEMS WITH DISTRIBUTED STORAGE

Systems with distributed storage store encrypted templates on the clients. In this scenario, during the enrolment phase, the system operates as follows:

- User provides a token carrying numeric user ID and non-invertible transform key K_t to the client.
- Hash of the user ID is calculated on the client and sent to the authentication server. Authentication server generates a keypair (K_{priv}, K_{pub}), stores the private key with hash of user ID (H(id), K_{priv}) and sends public key to the client.
- Client obtains biometrics, creates a template b_0 and generates cancelable binary template $b = K_t \oplus b_0$.
- Client generates random seed s_0 and encrypts it with the public key: $s_E = E(s_0 , K_{pub})$. Client generates a keystream s = PRNG (s_0) using pseudorandom number generator and given seed.
- Client calculates $s \oplus b$, stores (H(id), s_E, $s \oplus b$) and discards the rest of the data.

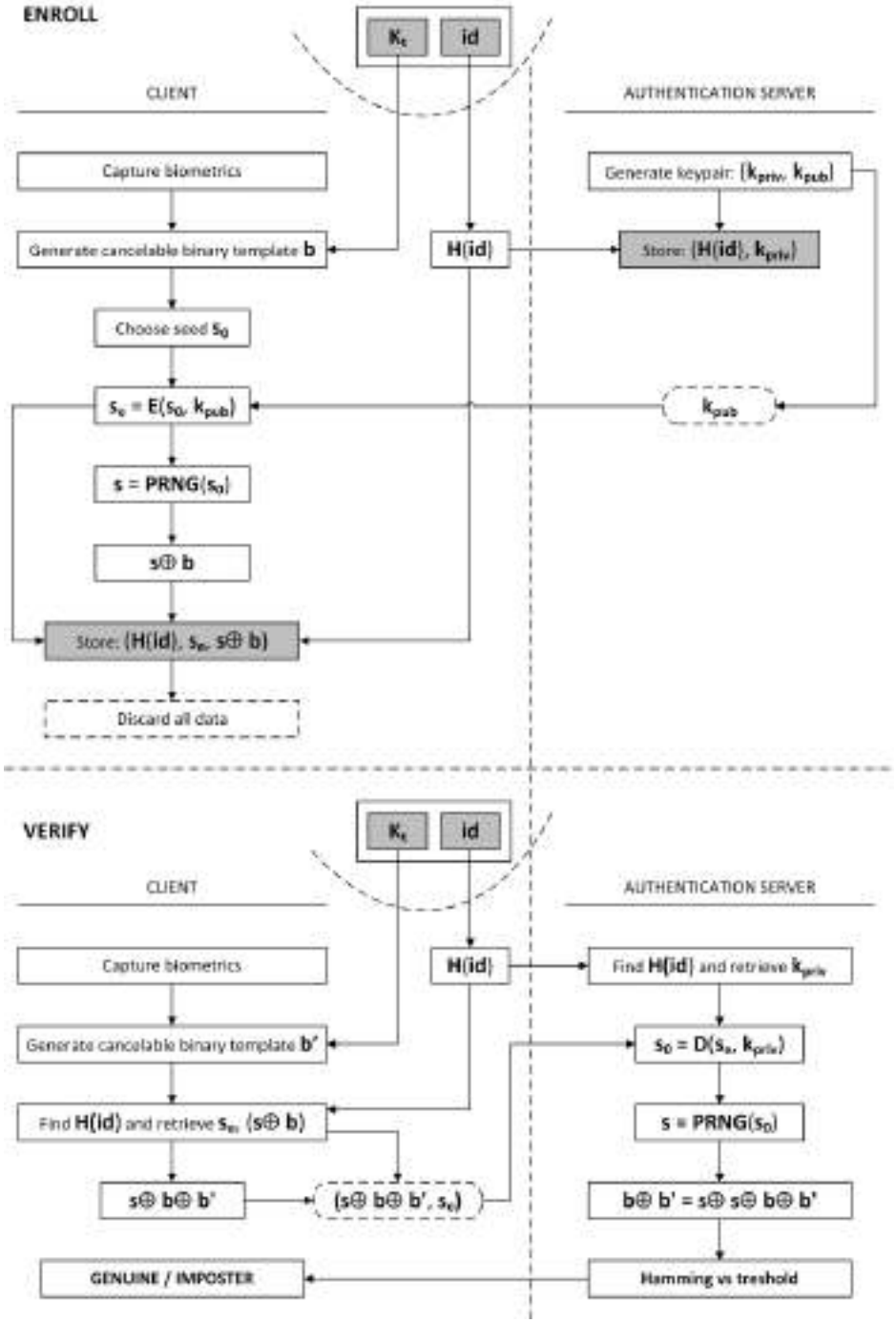

Image 1: Systems with distributed storage

During the verification phase, the system operates as follows:

- User provides a token carrying numeric user ID and non-invertible transform key K_t to the client.
- Client obtains biometrics, creates a template b_0' and generates cancelable binary template $b' = K_t \oplus b_0$'.
- Client calculates user ID hash and retrieves values s_E and $(s \oplus b)$ from stored record (H(id), s_E, $s \oplus b$) with the corresponding user ID hash.
- Client calculates $s \oplus b \oplus b'$ and sends it with the encrypted seed s_E to the authentication server.
- Hash of the user ID calculated on the client is sent to the authentication server. Authentication server retrieves private key from stored record (H(id), K_{priv}) with the corresponding user ID hash.
- Authentication server decrypts the seed with the private key $s_0 = E(s_E , K_{priv})$ and generates the keystream: $s = PRNG (s_0)$.
- Server calculates $b \oplus b' = s \oplus s \oplus b \oplus b'$ and compares the Hamming distance between cancellable templates b and b' with the treshold. According to that result, the decision is made (user is genuine or imposter) and sent back to the client.

The security of the system may be summarized as follows. Templates are encrypted or at least cancelable during all stages of storage, transmission and verification, and the client is not allowed to access private keys stored on authentication server, which satisfies the conditions set for an ideal biometric system. System employs two factor authentication thus making an imposter with auxiliary data virtually impossible to claim as genuine user. If templates stored on a client are somehow compromised, reenrolment with another transform key and encryption key-pair will remediate the situation. Substitution attacks cannot be performed, as the public key is discarded at the end of enrolment. As an adversary cannot recreate the keystream s from the encrypted seed s_E and the public key, system is resilient to most of the attacks on the biometric encryption systems. Regarding the usability of the system, the following conclusions can be made: system can be employed in one client – one server scenario. System can be employed in many clients – one server scenario only if users enrolled on one client are not expected to verify their identity on another. However, user may enrol on multiple clients, but this would require a client ID to be stored with the encryption keys and user ID on the server. In this case, user would have to re-enrol on each client if the transform key is lost or stolen. Another limitation to the usability is that system deals with conventional XOR biometrics, which is not applicable to all modalities.

5. SYSTEMS WITH CENTRALIZED STORAGE

Systems with centralized storage do not store encrypted templates on the clients. They are logical extension of distributed storage systems.

In this scenario, during the enrolment phase, the system operates similar to systems with the centralized storage, with two major differences (see image 2):

- Values (H(id), s_E, $s \oplus b$) are not stored on the client. After calculating these values, client asks authentication server to issue an request to storage to add a record containing (H(id), s_E, $s \oplus b$) into the database.
- Client discards all data, not just remaining ones (public keys, the unencrypted seed and original template). This means that no data is stored on a client.

The key point here is that encrypted seed should never be stored on the authentication server as the corresponding private key is stored on it. This enforces the usage of a database that is run on separate device which communicates with the authentication server via encrypted channel.

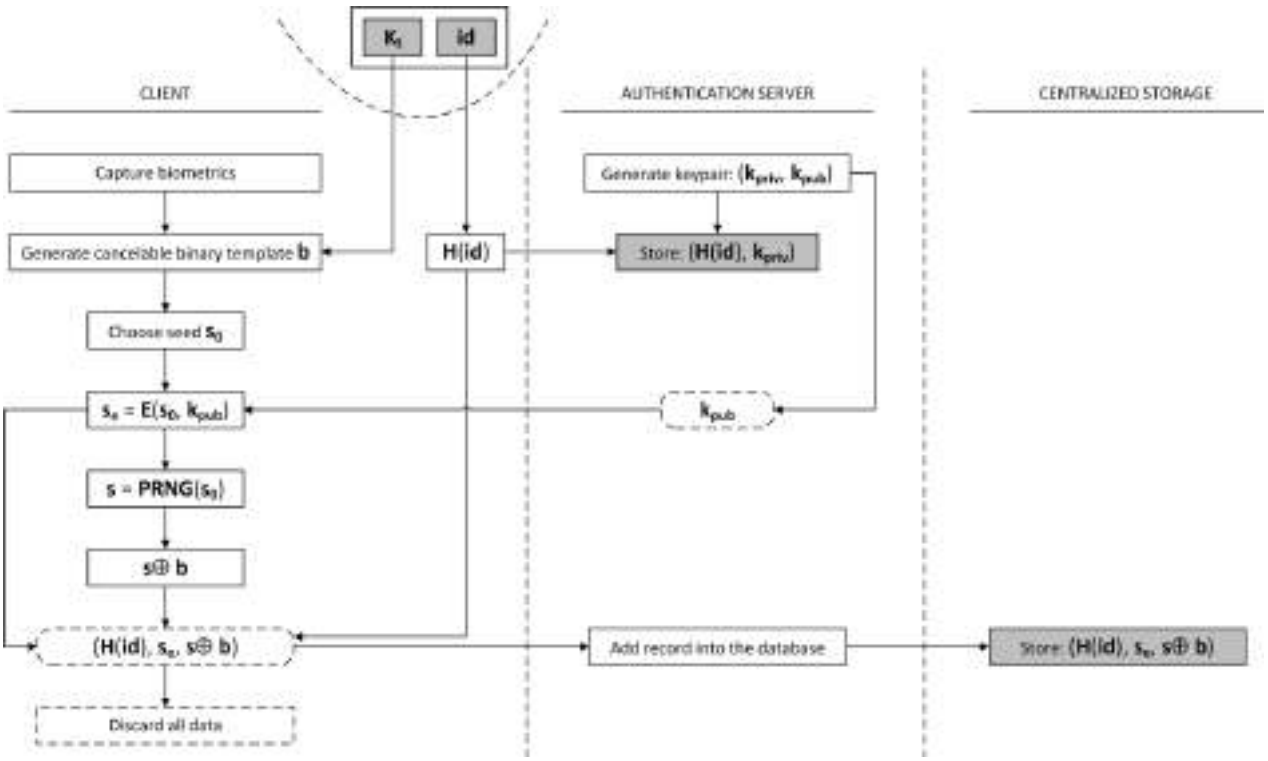

Image 2: Systems with centralized storage (enrolment phase)

During the verification phase, the system operates as follows:

- User provides a token carrying his numeric ID and non-invertible transform key K_t to the client.
- Client obtains biometrics, creates a template b_0' and generates cancelable binary template $b' = K_t \oplus b_0$'.
- Client calculates user ID hash and sends it to the authentication server.
- Authentication server contacts the centralized storage and retrieves values s_E and ($s \oplus b$) from corresponding (H(id), s_E, $s \oplus b$) stored on it.
- Authentication server sends value $s \oplus b$ to the client.

- Client calculates $s \oplus b \oplus b'$ and sends it back the authentication server.
- Authentication server retrieves private key from record (H(id), K_{priv}) with the corresponding user ID hash.
- Authentication server decrypts the seed with the private key $s_0 = E(s_E , K_{priv})$ and generates the keystream: $s = PRNG (s_0)$.
- Server calculates $b \oplus b' = s \oplus s \oplus b \oplus b'$ and compares the Hamming distance between cancellable templates b and b' with the treshold. According to that result, the decision is made (user is genuine or imposter) and sent back to the client.

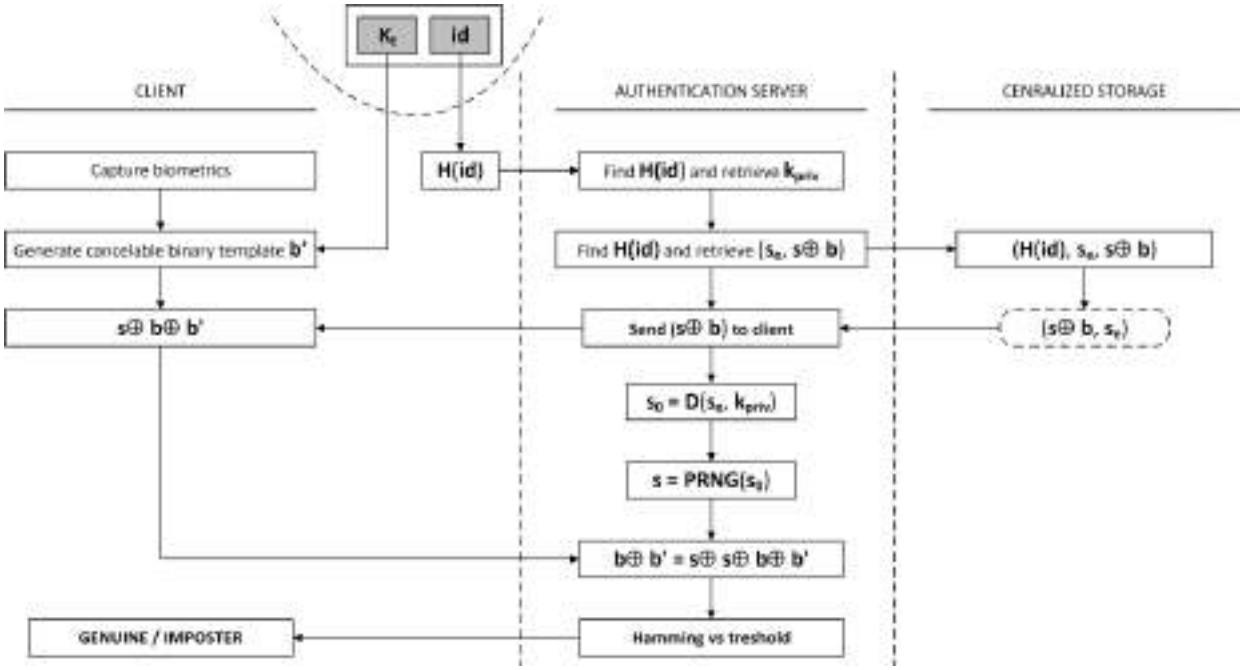

Image 3: Systems with centralized storage (verification)

The security of the system with centralized storage can be summarized as the security of the system with distributed one. However, additional cryptographic countermeasures are required to protect the communication channel between authentication server and centralized storage. The major difference between systems with distributed and centralized storage is the usability. One-to-many system does not require user to enrol on many clients as they share the stored templates on centralized storage. A user enrolled on one client can verify his identity on all clients connected to the same authentication server. These systems have a number of possible applications, ranging from facility entry control to securing mobile banking authentication.

6. CONCLUSION

This paper has introduced modular authentication systems architecture based on conventional XOR biometrics. The system keeps biometric templates encrypted or at least cancelable during all stages of storage, transmission and verification, and does not suffer from severe computational costs. Proposed architecture reassembles two factor authentication as the user who wants to verify identity must provide both biometrics and auxiliary data (non-invertible transform key). In further work we will explore the possible application of proposed authentication systems with centralized storage to secure mobile banking authentication.

REFERENCES

[1] A. K. Jain, A. Ross and S. Prabhakar, “An Introduction to Biometric Recognition”, IEEE Transactions on Circuits and Systems for Video Technology, Vol. 14, pp. 4-20, 2004.

[2] A. K. Jain and A. Ross, “Introduction to Biometrics”, in “Handbook of Biometrics”, A. Jain et al. (Eds), Springer, 2008.

[3] Y. C. Feng, P. C. Yuen and A. K. Jain, “A Hybrid Approach for Face Template Protection”, in Proceedings of SPIE Conference of Biometric Technology for Human Identification, Orlando, USA, Vol. 6944, pp. 325, 2008.

[4] P. Balakumar and R. Venkatesan, “A Survey on Biometrics-based Cryptographic Key Generation Schemes”, International Journal of Computer Science and Information Technology & Security, Vol. 2, No. 1, pp. 80-85, 2012.

[5] A. K. Jain, K. Nandakumar and A. Nagar, “Biometric Template Security”, EURASIP J. Adv. Signal Process, 2008:1-17, 2008.

[6] J. Galbally, C. McCool, J. Fierrez, S. Marcel and J. Ortega-Garcia, “On the Vulnerability of Face Verification Systems to Hill-Climbing Attacks”, Pattern Recognition, 43(3) pp. 1027-1038, 2010.

[7] A. Stoianov, “Cryptographically secure biometrics”, in SPIE Defense, Security, and Sensing, International Society for Optics and Photonics, 2010.

[8] N. Maček, B. Đorđević, J. Gavrilović and K. Lalović, “An Approach to Robust Biometric Key Generation System Design”, Acta Polytechnica Hungarica, Vol. 12, No. 8, pp. 43-60, 2015.

[9] N. K. Ratha, S. Chikkerur, J. H. Connell and R. M. Bolle, “Generating Cancelable Fingerprint Templates”, Pattern Analysis and Machine Intelligence, IEEE Transactions on, 29(4), pp. 561-572, 2007.

[10] J. Zuo, N. K. Ratha and J. H. Connell, “Cancelable iris biometric”, In Pattern Recognition, ICPR 2008, 19th International Conference on (pp. 1-4), IEEE, 2008.

[11] R. Ang, R. Safavi-Naini and L. McAven, “Cancelable Key-based Fingerprint Templates”, in C. Boyd & J. Gonzalez Nieto (Eds.), Australasian Conference on Information Security and Privacy, pp. 242-252, 2005.

[12] J. Bringer and H. Chabanne, “An authentication protocol with encrypted biometric data”, in International Conference on Cryptology in Africa, pp. 109-124. Springer Berlin Heidelberg, 2008.

[13] B. Schoenmakers and P. Tuyls, “Computationally secure authentication with noisy data”, in Security with Noisy Data, pp. 141-149. Springer London, 2007.

[14] A. K. Jain, A, Ross and U. Uludag, “Biometric template security: challenges and solutions”, in Proc. Europeon Signal processing conference, pp 1-4, September 2004.

[15] R. Jain and C. Kant, “Attacks on Biometric Systems: An Overview”, International Journal of Advances in Scientific Research, 1(07), pp. 283-288, 2015.

[16] B. Biggio, “Adversarial Pattern Classification”, Doctoral dissertation, University of Cagliari, Cagliari, Italy, 2010.

[17] A. Adler, “Vulnerabilities in Biometric Encryption Systems”, LNCS, Springer 3546, pp. 1100–1109, 2005.

[18] E.-C. Chang, R. Shen and F. W. Teo, “Finding the Original Point Set Hidden among Chaff” in Proc. ACM Symp. ASIACCS’06, Taipei, Taiwan, pp. 182–188, 2006.

[19] X. Boyen, “Reusable cryptographic fuzzy extractors”, in Proc. 11th ACM Conf. CCS, Washington, DC, pp. 82–91, 2004.

[20] W. J. Scheirer and T. E. Boult, “Cracking Fuzzy Vaults And Biometric Encryption”, Biometric Consortium Conference, Baltimore, September 2007.

[21] A. Cavoukian and A. Stoianov, “Biometric Encryption: The New Breed of Untraceable Biometrics,” in N.V Boulgouris et al., eds., “Biometrics: fundamentals, theory, and systems”, Wiley-IEEE Press, pp. 655-718, 2009.