Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 154 (2019) 327–331

Procedia Computer Science

www.elsevier.com/locate/procedia

8th International Congress of Information and Communication Technology, ICICT 2019

Comparative Analysis of Crypto Systems Using Biometric Key

Zümrüt MÜFTÜOĞLU*, Tülay YILDIRIM

Yildiz Technical University, Department of Electronics & Communications Engineering, Istanbul, 34220, Turkey

Abstract

In digital world, the security of data is one of the most important issues. Biometric cryptosystems provide great convenience and security by combining biometrics and cryptography. The aim of this paper is to provide a good standpoint into the state-of-the-art and current research directions of crypto systems using biometric key, including theory and applications.

Keywords: *Biometrics; Key Generation; Cryptography*

1. Introduction

Towards the digital transformation age, information barter over the Internet and the storing of data on open networks has been widely increased. This also increases the importance of cryptography in computer science. Cryptography is designed to provide confidentiality and authenticity of a message. Generally; during the communication, encryption and decryption operations are performed for securing information through cryptographic key. Providing secure of this key is major concern, so key chose is essential. One should care that the keys are not estimated easily. At this point biometric cryptosystems provide great convenience and security by combining biometrics and cryptography. Cryptographic keys will be produced dynamically thanks to biometrics. What the thing makes it so popular is biometric data cannot be stolen or lost.

* Corresponding author. Tel.: +90 312 416 66 40.
E-mail address: zumrutmuftuoglu@gmail.com

10.1016/j.procs.2019.06.047

A variety of biometric traits has been used in many applications such as fingerprint, palm print, hand geometry, face, iris, vein, retina, and odour. Depending on the requirements of used application, each biometric has independently own advantages and disadvantages.

The first biometric-based encryption system is presented in Eurocrypt 2005 by Sahai and Waters. They called their system as "Fuzzy Identity-Based Encryption (IBE): Privacy for the Unprepared" [1].

Uludag et al. [2] have offered some techniques to solidly unify a cryptographic key with the biometric pattern, which is stored in the database. Their techniques do not allow cryptographic keys to be elicit unless an available biometric authentication is presented. In their study, they also handle assessment of key binding/generation algorithms using fingerprint biometric.

In [3], Lifang Wu et.al proposed a biometric cryptosystem using face biometrics. Firstly, at the time of encryption a 128- dimensional Principal Component Analysis feature vector is acquired through the face image. 128-bit binary vector is obtained by thresholding. After that the discernible bits were selected to generate bio-key. They also generated an error correcting code-using Reed –Solomon algorithm.

In [4], a proposal is presented to enable security of sensitive data stored in devices used in IoT by using fingerprint modality.

In [5]-[6] Soutar et al. studied on a key binding algorithm in an optical correlation-based fingerprint matching system. In their method, they produce a key using fingerprint images of user during enrolment. To retrieve the key, authentication should be successful.

Yen-Lung Lai et. al. [7] presented a novel biometric cryptosystem called symmetric keyring encryption (SKE). They deal with the biometric secret-binding problem as a fuzzy symmetric encryption problem by calling resilient vector pair.

In [8] Bansal et. al. focused on security problem while using the matrix to generate key in RSA. In their proposal, the matrix is forges using fingerprint and the matrix protection is provided using Fuzzy Vault.

In [9], Lifang Wu et.al initially acquired Principal Component Analysis (PCA) feature vector with 128-dimensional from the face image at the time of encryption. Afterward 128-bit binary vector is acquired by thresholding. Then, to generate bio-key, the distinguishable bits were selected. An error correcting code also is generated using Reed –Solomon algorithm.

2. Biometric Cryptosystems

With the increasing use of developing technology and information in digital media, the methods used for the storage of information safely have also improved over time. This requirement brings together biometrics and cryptography. As known, biometrics is portrayed as recognition of personal with respect to their behavioral and biological characteristics. And cryptography is all the techniques used to transform readable information into unreadable form. While a cryptographic operation is run, the original data is crypted and decrypted by using same key. By combining these keys with biometric features, biometric cryptosystems have been exposed.

In biometric cryptosystems, information is assured by using biometric features. Biometric cryptosystems are analogous to key generation systems using password. It is because they were developed to provide cryptographic key secure by using biometrics or directly producing a key from biometrics [10].

Since the biometric indications are different acquired during the registration and authentication, these features cannot be used to generate cryptographic key. The structures called as helper data or secure sketch are stored during registration to provide it. Accordingly, biometric cryptosystems are called helper data systems as well. Depending on how to obtain secure sketch or helper data, biometric cryptosystems are classified Key Binding Biometric cryptosystems and Key Generation Biometric cryptosystems.

2.1. Key binding biometric cryptosystems

As the name suggests Key binding cryptosystem binds a cryptographic key with a biometric template to ensure that only a legal user can access to encrypted data.

2.2. Key generation biometric cryptosystems

In key generation biometric cryptosystems, the secure sketch is reproduced from the template and the key is produced from helper data and user's biometric features. The stored secure sketch is used to revamp a key that is suspected to have been compromised.

To compare these two cryptosystems in terms of strengths and weakness, some basic considerations stand out [11]. In Key Binding Cryptosystems while the cryptographic keys are independent of biometric data, an adversary who knows the private key can capture the original biometric data from protected template. The biometric data is not stored directly in Key Generation Cryptosystems, so it is hard to recover biometric data from key string. But key generation designs which do not store helper data cannot provide retrievable keys and helper data based key generation designs using secure sketch are vulnerable to attack via registry multitude.

There are four types Key Binding Cryptosystem techniques: biometric encryption, fuzzy commitment scheme, fuzzy vault and shielding function [11]. Biometric encryption implements classic cryptography for generating secure biometric template. Fuzzy commitment uses error correcting techniques as well as cryptography. Fuzzy vault a set of biometric data disorderly to lock a private key in a vault. And shielding function produces a secure template from a random secret biometric data. Biometric encryption blocks to acquire secure template without algorithm and cryptographic key information [12]. In fuzzy commitment, the commitment is comprised from biometric data and private keys. It protects secure template and also protects key by hashing it [13].In fuzzy vault, the vault does not encode as long as the biometric data matches [14]. Looking at shielding function, the helper data protects the data and any biometric data cannot be obtained from secure template without private key information.

Key generation techniques are classified as private template schemes and quantization schemes [11].As the name suggests, biometric features are quantized in quantization schemes. And biometric keys are generated by helper data. In private template schemes, specific keys for users are acquired from reference biometric data directly [15].

3. Comparison of Biometric Traits

In literature, it has seen that various biometrics, such as fingerprints, iris, face, voice and so on, have been used to develop cryptographic algorithms. Each biometric trait has own pros and cons, depending on the application used on. So, some factors must be considered to choose an efficient trait [10]. These factors are briefly discussed below.

Universality: The application for each person should owns the trait. The failure to enroll rate (FTE) of the biometrics is determined according to this factor.

Uniqueness: Biometric trait should differ adequately among individuals covering all users. In other way, this will result in undesirably high mismatch ratio (FAR or FPIR) for biometric system.

Permanence: The biometric trait should be invariant enough over a period in accordance with the matching algorithm.

Performance: Speed, accuracy and robustness are distinguishing factors for performance.

Acceptability: People should be eager to submit their biometric feature.

Circumvention: It relates to facilitate with which a trait can be faked using an artifacts or substitute.

Measurability: The biometric trait should be gained and digitalized through appropriate devices.

In Table.1 Comparison of commonly used biometric traits with the above-mentioned characteristics are given [16].

Table.1. Comparison of biometric traits(High, Medium, Low denoted by H, M, and L, respectively) [11].

Biometric Identifier	Universality	Uniqueness	Permanence	Measurability	Performance	Acceptability	Circumvention
Face	High	Low	Medium	High	Low	High	High
Fingerprint	Medium	High	High	Medium	High	Medium	Medium
Hand geometry	Medium	Medium	Medium	High	Medium	Medium	Medium
Hand/finger vein	Medium	Medium	Medium	Medium	Medium	Medium	Low
İris	High	High	High	Medium	High	Low	Low
Signature	Low	Low	Low	High	Low	High	High
Voice	Medium	Low	Low	Medium	Low	High	High

In this table, looking the attributes of each biometric attitudes, suitable algorithms for usage have been developed in the literature. There are also multi-biometric solutions. Table.2 shows a comparison between unimodal and multimodal biometric systems [4].

Table.2. Comparison of modals

Parameters	Unimodal		Multimodal	
	Low	High	Low	High
Cost	√			√
Convenience		√	√	
Recognition accuracy	√			√
Security	√			√
Flexibility	√			√
Complexity	√			√

4. Conclusion

Biometrics is an important actor of any identity-based security system. Because it is the just technology which identifies the authorized person based on their native unique traits. Its invariance and portable properties make it preference. Integration of biometrics within a cryptographic system for influential user authentication makes responsive sensation. Even there are many exciting proposals for key generation or binding of biometric keys, there are also still some issues to the biometric field have not been convincingly solved yet. Future new methods will accelerate the development of biometric cryptographic systems. This paper discussed biometric cryptosystems types, review of their advantages, and disadvantages.

References

1. Sarier ND.Biometric Cryptosystems: Authentication, Encryption and Signature for Biometric Identities. Angefertigt mit Genehmigung der Mathematisch-Naturwissenschaftlichen Fakultät der Rheinischen Friedrich-Wilhelms-Universität Bonn.2011
2. Uludag U, Pankanti S, Prabhakar S, Jain AK. Biometric Cryptosystems: Issues and Challenges. Proceedings of the IEEE .Volume: 92, Issue: 6, June 2004.
3. Wu L, Liu X, Yuan S, Xiao P.A Novel key generation cryptosystem based on face features. IEEE 10th International Conference on Signal Processing Proceedings. DOI: 10.1109/ICOSP.2010.5656719, October 2010.
4. Belhadri A,Benyettou, M. New biometric cryptosystem to protect sensitive data in Internet of objects. Multiagent and Grid Systems. Vol. 14, no. 3, pp. 307-320, September 2018.
5. Soutar C, Roberge D, Stoianov A, Gilroy R, Kumar BVKV. Biometric Encryption (Chapter 22). In: Nichols RK, editor. ICSA Guide to Cryptography.McGraw-Hill New York, 1999
6. Wu L,Liu X,Yuan S,Xiao P. A Novel key generation cryptosystem based on face features.IEEE 10th International Conference on Signal Processing Proceedings.pp.1675-1678, DOI: 10.1109/ICOSP.2010.5656719, 2010
7. Lai YL, Hwang JY, Jin Z, S Kim, Cho S, Teoh ABJ. A Symmetric Keyring Encryption Scheme for Biometric Cryptosystems. ArXiv: 1809.11045 [cs.CV]. September 2018.
8. Bansal N, Mahto D, Yadav DK. Enhanced RSA Key Generation Modelling Using Fingerprint Biometric.Helix. Vol. 8(5): 3922- 3926, DOI 10.29042/2018-3922-3926, August 2018.
9. Wu L,Liu X,Yuan S,Xiao P. A Novel key generation cryptosystem based on face features.IEEE 10th International Conference on Signal Processing Proceedings.pp.1675-1678, DOI: 10.1109/ICOSP.2010.5656719, 2010
10. Jain AK, Ross AA, Nandakumar K. Introduction to Biometrics.Springer New York Dordrecht Heidelberg London; 2011, DOI 10.1007/978-0-387-77326-1.
11. Jegede A, Udzir NI, Abdullah A, Mahmod R. State of the Art in Biometric Key Binding and Key Generation Schemes. International Journal of Communication Networks and Information Security (IJCNIS). Vol. 9, No. 3, December 2017.
12. Juels A,Wattenberg M. A Fuzzy Commitment Scheme. CCS '99 Proceedings of the 6th ACM Conference on Computer and Communications Security.pp. 28 – 36, November 1999.

13. Juels A,Sudan M. A Fuzzy Vault Scheme. Designs, Codes and Cryptography.Vol. 38, pp. 237–257. Springer Science+Business Media, Inc. Manufactured in the United States, February 2006.
14. Sutcu Y, Li Q,Memon N. Protecting biometric templates with sketch: theory and practice. IEEE Transactions on Information Forensics and Security. Vol. 2, Issue. 3, Part 2, pp. 1825-1840, DOI: 10.1109/TIFS.2007.902022 September 2007.
15. Soutar C, Roberge D, Stojanov SA,Gilroy R, Kumar BVKV. Biometric encryption using image processing. Proceedings of the SPIE, Optical Security and Counterfeit Deterrence Techniques II.vol. 3314, pp. 178–188, 1998.
16. Dasgupta D, Roy A, Nag A. Biometric Authentication , Authentication through human characteristics, Springer International Publishing AG 2017.Advances in User Authentication, Infosys Science Foundation Series, DOI 10.1007/978-3-319-58808-7.