ISSN:1991-8178

Australian Journal of Basic and Applied Sciences

Journal home page: www.ajbasweb.com

A New Hybrid Approach for Securing Multibiometric Templates Based on Cancelable and Fuzzy Commitment Scheme

Suzwani Ismail, Fakariah Hani Hj Mohd Ali, Syed Ahmad Aljunid

Faculty of Computer and Mathematical Sciences, Universiti Teknologi MARA Shah Alam, 40450 Shah Alam, Malaysia.

ARTICLE INFO

Article history:
Received 13 June 2015
Accepted 5 August 2015
Available online 12 August 2015

Keywords:
Adaptive Bloom Filters, Fuzzy Commitment Scheme, Cancelable Biometrics,FAR, FRR, Iris Recognition System

ABSTRACT

Biometric template protection is one of the most important issues in biometric authentication system. It is vital because once the biometric template is being attacked, the intruder could introduce him/her into the system without following the proper enrolment procedures. Therefore, to combat this attack many researchers have proposed methods and algorithms in over 20 years. In this paper, a hybrid approach based on Adaptive Bloom Filters and Fuzzy Commitment schemes for securing multibiometric templates is proposed. Right and left irises of a single individual will be used as input templates. The experiment will be carried out using CASIA-v3 iris database to verify the soundness of the proposed system. This research is expected to show that the proposed hybrid template protection scheme can satisfy all template protection requirements without degrading the iris recognition performance.

ToCite ThisArticle: Suzwani Ismail, Fakariah Hani Hj Mohd Ali, Syed Ahmad Aljunid., A New Hybrid Approach for Securing Multibiometric Templates Based on Cancelable and Fuzzy Commitment Scheme. ***Aust. J. Basic & Appl. Sci.,*** *9(26): 72-76, 2015*

INTRODUCTION

Biometric authentication system is an automatic identification of an individual, offers many advantages over conventional authentication systems. It could increase convenience, reliability and universality of the authentication systems. However, they are vulnerable against attacks that can diminish their security considerably. According to Satyavarapu *et al.* (2014), attacks on biometric authentication system can be generally divided into four categories. There are attacks at the user interface, attacks at interfaces between modules, attacks on the modules and also attacks on the template database.

From these four categories of attacks, attack on the template database is considered as the most dangerous attack on the biometric authentication system (Satyavarapu *et al*., 2014). It is because the template database stores biometric templates of authorized users which are unique and permanent to each person. Once the biometric data is compromised, it cannot be cancelled of revoked (De L Oliveira Filho *et al*., 2013). This leads to several vulnerabilities such as spoofing (Rathgeb *et al*., 2014), stolen and changed template by adversaries (Satyavarapu *et al*., 2014). Therefore the protection of biometric template gaining primary concern (Ghouzali and Abdul, 2013).

To protect biometric template, there are several template protection schemes have been proposed by previous researchers. It can be divided into two major categories, which are biometric cryptosystem based and feature transformation based (Nandakumar and Jain, 2015). A number of template protection schemes based on biometric cryptosystem have been proposed including Key Generation scheme (Chi *et al*., 2014), Key Release scheme (Wencheng *et al*., 2013), Fuzzy Vault scheme (Tams *et al*., 2015) and Fuzzy Commitment scheme (Xuebing and Busch, 2012). There are also a number of template protection schemes based on feature transformation based including robust hashing approach (Barman *et al*., 2015) and biohashing approach (Jain *et al*., 2013).

A template protection scheme should satisfy several properties in order to ensure the security of biometric template. There are non-invertibility, revocability, non-linkability and performance (Nandakumar and Jain, 2015), (Jain *et al*., 2013). However, by applying one type of template protection scheme is not sufficient enough to satisfy all the properties mentioned above. It is due to the weaknesses of each scheme having. For instance, it is not easy to achieve non-linkability in biometric cryptosystem based template protection scheme. While in feature transformation based, finding

Corresponding Author: Suzwani Ismail, Faculty of Computer and Mathematical Sciences, Universiti Teknologi MARA Shah Alam, 40450 Shah Alam, Malaysia.
E-mail: suzwani89@gmail.com

appropriate transformation function that provides non-invertibility is a main challenge.

As a solution for achieving non-linkability and non-invertibility, a combination of feature transformation and biometric cryptosystem approach can be applied. This solution also gives advantage in revocability property since feature transformation approach is capable of ensuring revocability of the template protection. However, there is trade-off between invertibility and recognition performance of biometric authentication system. This limitation can be solved by implementing multibiometric template protection system (Nandakumar and Jain, 2015).

Thus, this paper proposes a hybrid approach based on Bloom Filters and Fuzzy Commitment schemes for securing multibiometric templates in terms of non-invertibility, revocability and non-linkability. Both right and left irises of a single individual are used to provide a better recognition performance. The remainder of the paper is organized as follows: In section 2, related works regarding Fuzzy Commitment scheme and Bloom Filters are explained briefly. Section 3 presents the methods that will be used for the proposed framework of hybrid multibiometric template protection based algorithm. Expected results will be justified in Section 4. Finally, section 5 concludes the paper and section 6 explained on the Future works.

2. Related Work:

The related work had been reviewed in order to determine the best and suitable methods to be studied in terms of non-invertibility, revocability, non-linkability and recognition performance of biometric template protection.

2.1. Fuzzy commitment scheme:

Fuzzy commitment scheme (FC) is one of biometric cryptosystem based template protection, which uses error correcting codes to construct commitments from noisy information. It has been first introduced by Juels and Wattenberg (1999). A number attempts have been made regarding this scheme. There are several previous works applied this scheme in their proposed approach. For instance, Feng *et al*. (2010) proposed a three-step hybrid approach based on fuzzy commitment scheme, random projection and discriminability-preserving (DP) transform. Face recognition system is used to evaluate the proposed scheme. In Nagar *et al*. (2012) a multibiometric feature level fusion based on fuzzy vault and fuzzy commitment scheme has been proposed. Three biometric modalities have been used to evaluate the proposed method. Both previous works mentioned above are not considering about the speed of recognition performance.

2.2. Adaptive Bloom filters:

Bloom Filter is a set of space-efficient probabilistic data structure used to support membership queries. It provides several properties which benefits to biometric authentication system including template protection, biometric data compression and efficient identification. In Gomez-Barrero *et al*. (2014), in order to achieve irreversible face biometric templates the original concept of Bloom filters is adapted. Rathgeb *et al*. (2014) also applied Bloom Filters in their proposed approach in order to compress biometric template, improve the biometric performance and at the same time could provide rotation-invariant cancelable templates hence secure the biometric templates. Both previous works mentioned above implemented only one type of template protection technique instead of proposing hybrid approach.

3. Methods:

Section 3.1 will shows the summarization of overall proposed framework and explanation about feature level fusion framework, Bloom Filter algorithm and Fuzzy Commitment algorithm that will be implemented. A hybrid Bloom Filters and Fuzzy commitment scheme template protection is proposed in order to achieve all requirements of template protection methods. While, the performance metrics that will be evaluated are False Acceptance Rate (FAR) and False Rejection Rate (FRR).

3.1. Proposed Methodology:

Fig. 1 shows the summarization of overall proposed framework. The experiment of the methods will be carried out using Matlab7.4 as simulator. For experimentation, iris images from CASIA Iris Image Database v4 collected by Institute of Automation, Chinese Academy of Science will be used.

Based on Fig. 1, the proposed scheme starts with image acquisition of both right and left irises of a single person using sensor. Next, segmentation takes place where the iris region is located from a given eye to determine the iris boundaries. Active Contour method will be implemented for segmentation stage as being applied by previous work (Sinduja *et al*., 2012). The iris region is transformed from Cartesian to polar form in normalization using Daugman's Rubber Sheet Model in order to allow comparisons. Subsequently, feature extraction takes place to extract iris features from the normalized iris. 2D Gabor Wavelet is applied in this phase. Then biometric template is produced (Kovendan and Eldose, 2014).

According to Nagar *et al*. (2012), ISO/IEC TR 24722:2007 has distinguished three possible level of fusion: (1) fusion at feature level, (2) fusion at score level, and (3) fusion at decision level. In this proposed work, the features of both right and left irises will be fused at feature level in order to generate a single multibiometric template. We will adapt feature level fusion method proposed by Nagar *et al*. (2012). It is mainly due to the security properties it provides which could secure multiple

templates of a single individual. In addition, this method is compatible with the fuzzy commitment scheme that will be implemented in this proposed work.

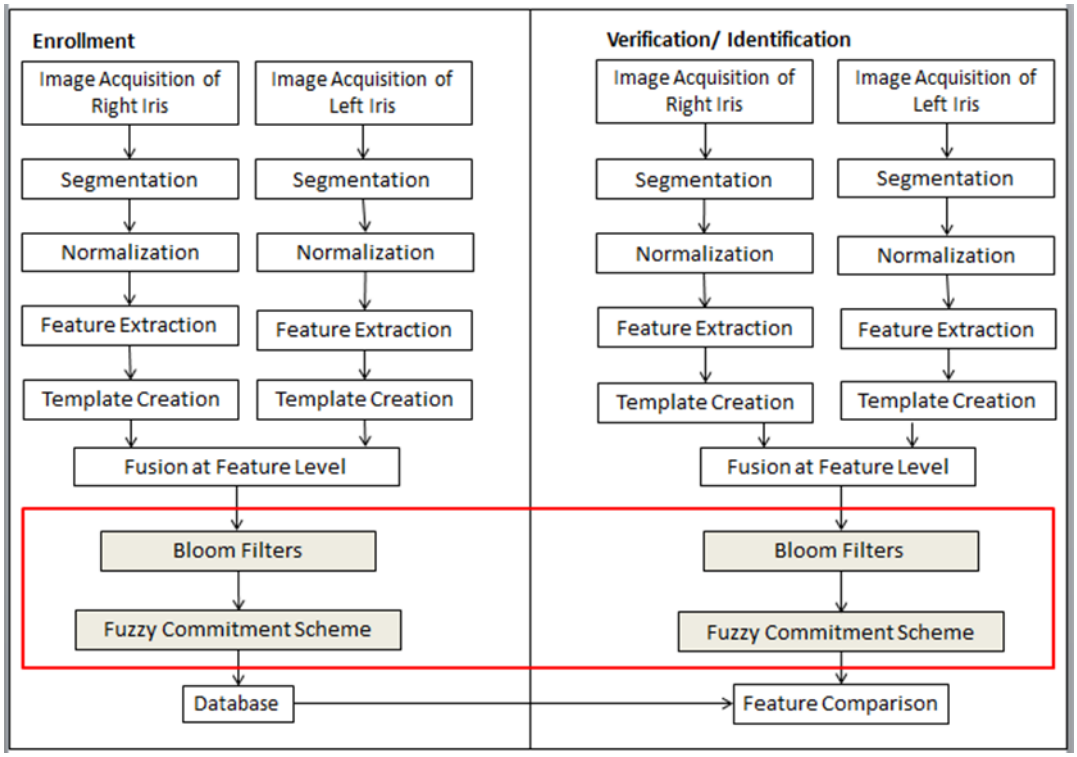

Fig. 1: The summarization of overallprocesses of proposed work.

Once a multibiometric template is generated, hybrid template protection method will be implemented. In order to solve the limitation of non-linkability in template protection, Adaptive Bloom Filters is applied. Adaptive Bloom Filters is a cancelable biometrics technique that meets non-linkability and irreversibility/ non-invertibility properties of template protection method (Rathgeb *et al*., 2014). It also gives additional advantages for template protection due to its capability to compress biometric template, improve the biometric performance and at the same time could provide rotation-invariant cancelable templates hence secure the biometric templates. Fig. 2 shows basic operation mode of Adaptive Bloom Filters.

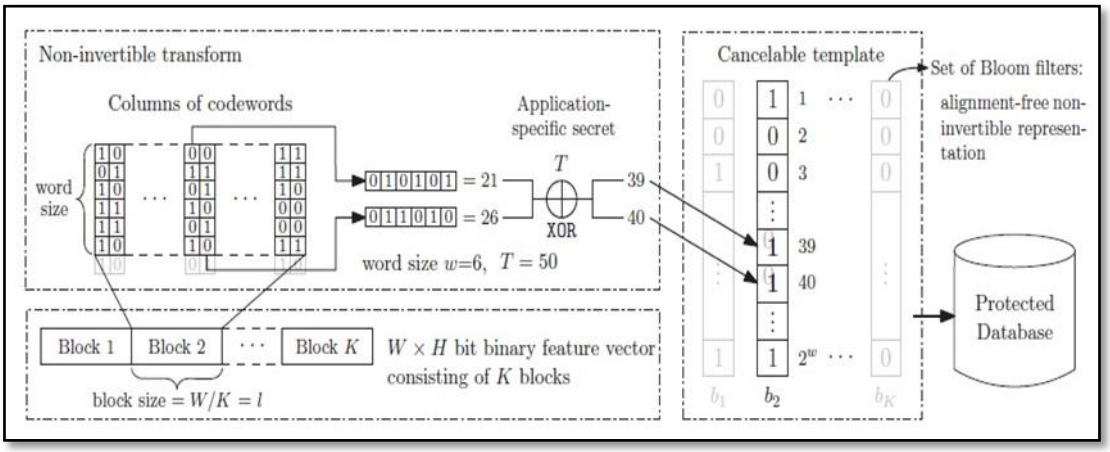

Fig. 2: Basic operation mode of Adaptive Bloom Filters (Rathgeb *et al*., 2014).

When Adaptive Bloom Filters is applied, a transformed template is generated. Fuzzy Commitment scheme is applied to protect the binary template of irises and generate a secure template. Fuzzy Commitment scheme is chosen because it is easy to evaluate the security of a secure sketch due to

the presence of error correcting code (ECC) (Nagar *et al*., 2012). Fig. 3 shows a Fuzzy Commitment scheme.

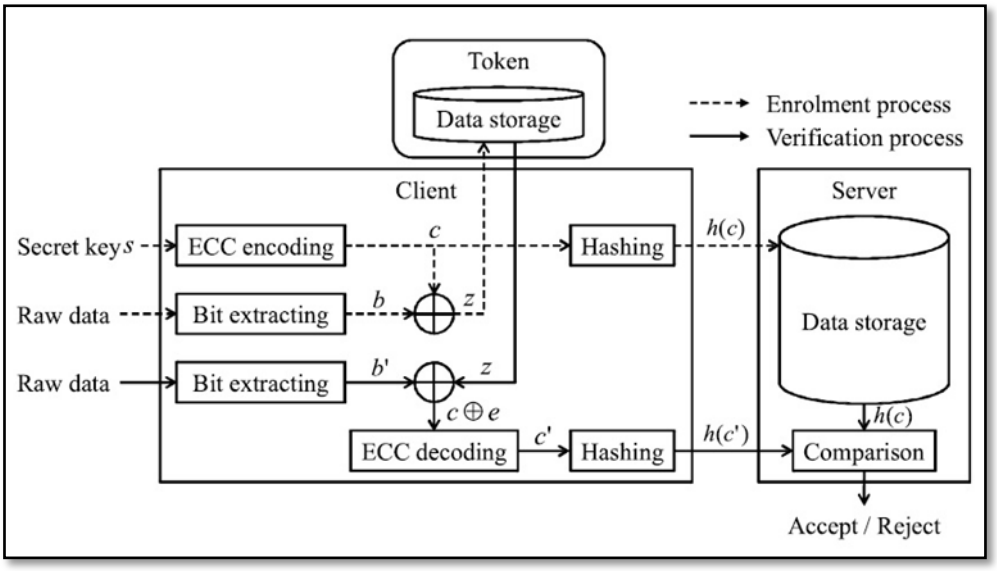

Fig. 3: Fuzzy Commitment scheme(Hidano, Ohki, & Takahashi, 2012).

By combining both categories of template protection methods, several limitations in terms of non-invertibility, revocability and non-linkability of template protection methods can be reduced. However, according to Nandakumar and Jain (2015) there is trade-off between invertibility and recognition performance of biometric authentication system. Hence, multibiometric template is applied which can solve this limitation (Nandakumar and Jain, 2015). Besides can improve the recognition performance, applying multibiometric template protection can lead to stronger non-invertibility due to higher inherent entropy of the template. A secure multibiometric template is then stored in the database for further classification process during authentication.

4. Expected Results:

From the previous works, we know that a hybrid approach of multibiometric template protection method based on robust hashing and secure sketch proposed by E.Durgadevi *et al*. (2014) can provide all requirements needed. However, applying three types of multimodal biometrics can increase the complexity of the system; hence lower the speed of the overall system. Another previous work proposed by Feng *et al*. (2010) applied hybrid approach of Fuzzy Commitment scheme and random projection. This approach enhanced security for template protection. However, it did not concern about the compression of the template and the speed of the overall system. Based on these two previous works, there has gap that needed to be solved. A template protection scheme should satisfy not only these three properties of non-invertibility, revocability and non-linkability, it also should provide a better recognition performance so that it can be applied in practise. Thus, by implementing Adaptive Bloom Filters and Fuzzy Commitment scheme on both irises of a single individual, all requirements of template protection method are expected to be improved.

Conclusion:

This paper had identified the standard requirements of biometric template protection in the related work. Several limitations also have been identified based on the previous works. Therefore, a hybrid approach based on Adaptive Bloom Filters and Fuzzy Commitment scheme is proposed. This proposed work is applied on both right and left irises images which applied fusion at the feature level. This paper expected that the implementation of Adaptive Bloom Filters and Fuzzy Commitment scheme on both irises templates of a single individual might work to achieve non-invertibility, revocability, non-linkability, and also could enhance the performance of biometric recognition system.

ACKNOWLEDGEMENT

This research was supported by the Research Management Institute, UniversitiTeknologi MARA and registered under the Research Acculturation Grant Scheme (RAGS) #600-RMI/RAGS 5/3 (77/2012) by the Ministry of Education Malaysia.

REFERENCES

Barman, S., *et al*., 2015."Fingerprint-based crypto-biometric system for network security." EURASIP Journal on Information Security, 2015(1): 1-17.

Chi, C., *et al*., 2014. Optional multi-biometric cryptosystem based on fuzzy extractor. Fuzzy Systems and Knowledge Discovery (FSKD), 2014 11th International Conference on.

De L. Oliveira Filho, I. *et al*., 2013. A Comparative Analysis of Cryptographic Algorithms and Transformation Functions for Biometric Data.Machine Learning and Applications (ICMLA), 2013 12th International Conference on.

Durgadevi, M., *et al*., 2014. "A Combined Robust Hashing and Secure Sketch Algorithm for Multi-Biometric Template Security." International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering, 3(4): 9179-9186.

Feng, Y.C., *et al*., 2010. "A Hybrid Approach for Generating Secure and Discriminating Face Template." Information Forensics and Security, IEEE Transactions on 5(1): 103-117.

Ghouzali, S. and W. Abdul, 2013. Private chaotic biometric template protection algorithm. Image Information Processing (ICIIP), 2013 IEEE Second International Conference on.

Gomez-Barrero, M., *et al*., 2014. Protected Facial Biometric Templates Based on Local Gabor Patterns and Adaptive Bloom Filters. Pattern Recognition (ICPR), 2014 22nd International Conference on.

Hidano, S., T. Ohki, K. Takahashi, 2012. Evaluation of security for biometric guessing attacks in biometric cryptosystem using fuzzy commitment scheme. Paper presented at the Biometrics Special Interest Group (BIOSIG), 2012 BIOSIG - Proceedings of the International Conference of the.

Jain, A.K., *et al*., 2013. "Fingerprint Template Protection: From Theory to Practice." Security and Privacy in Biometrics, P. Campisi (ed.), Springer, 2012: 1-29.

Juels, A. and M. Wattenberg, 1999. A fuzzy commitment scheme.Proceedings of the 6th ACM conference on Computer and communications security. Kent Ridge Digital Labs, Singapore, ACM: 28-36.

Kovendan, V. and G. Eldose, 2014. SBBSCS: SHA based biometric smartcard security. Information Communication and Embedded Systems (ICICES), 2014 International Conference on.

Nagar, A., *et al*., 2012. "Multibiometric Cryptosystems Based on Feature-Level Fusion." Information Forensics and Security, IEEE Transactions on 7(1): 255-268.

Nagar, A., *et al*., 2012. "Technical Report: Multibiometric Cryptosystems." Under review for IEEE TIFTS 7(1).

Nandakumar, K. and A.K. Jain, 2015. "Biometric Template Protection: Bridging the Performance Gap Between Theory and Practice." IEEE Signal Processing Magazine - Special Issue on Biometric Security and Privacy: 1-12.

Rathgeb, C., *et al*., 2014. "On application of bloom filters to iris biometrics." Biometrics, IET, 3(4): 207-218.

Satyavarapu, S., *et al*., 2014. "Multimodal Biometric Template Access Control Using Fingerprint Data Encrypted By Iris Data." Proceedings of 13th IRF International Conference, 16-21.

Sinduja, R., *et al*., 2012. Sheltered iris attestation by means of Visual Cryptography (SIA-VC).Advances in Engineering, Science and Management (ICAESM), 2012 International Conference on.

Tams, B., *et al*., 2015."Security Considerations in Minutiae-Based Fuzzy Vaults." Information Forensics and Security, IEEE Transactions on 10(5): 985-998.

Wencheng, Y., *et al*., 2013. Biometrics for securing mobile payments: Benefits, challenges and solutions. Image and Signal Processing (CISP), 2013 6th International Congress on.

Xuebing, Z. and C. Busch, 2012. Measuring privacy and security of iris fuzzy commitment.Security Technology (ICCST), 2012 IEEE International Carnahan Conference on.