International Journal of Engineering & Technology, 7 (4.29) (2018) 128-133

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research paper

Confidentiality and Integrity of the Biometric Fingerprint Template Protection

Taqiyah Khadijah Ghazali [1]*, Nur Haryani Zakaria [2]

[1,2]School of Computing, Awang Had Salleh Graduate School of Arts and Sciences,
Universiti Utara Malaysia, 06010 Sintok Kedah.
**Corresponding author E-mail:taqiyah_khadijah@ahsgs.uum.edu.my*

Abstract

Fingerprint is one of the most reliable biometric-based authentication methods for personal identification and providing access control to many applications. Due to its accuracy and convenience, it can never be forgotten or lost since biometric characteristics are biological parts of the users itself. However, previous studies have shown that, fingerprint template are exposed to threat in which the attackers can steal and modified the template to acquire illegal entree. Therefore, a technique to protect the biometric template is required. Biometric template protection consists of two categories, which are feature transformation and biometric cryptosystem. Thus, this paper will focus on biometric cryptosystem specialize in the key binding scheme, which is fuzzy commitment technique. In the key binding scheme, the helper data must not reveal any information concerning the biometric data, but previous studies have shown that it does certainly leak some crucial information. Hence, this paper intends to propose an enhancement to the existing fuzzy commitment technique. The enhancement will involve the key binding scheme of secret key with biometric template to generate AES-128 key algorithm, which is to provide confidentiality alongside with the Offset Codebook Mode (OCB), an authenticated encryption (AE) mode to provide integrity. The enhancement is expected to improve the technique, which will be more secure and robust while maintaining the existing performance.

Keywords: *Biometric Fingerprint; Biometric Template Protection; Lightweight Encryption; Authenticated-Encryption Mode; Biometric Cryptosystem*

1. Introduction

Biometric system is likely to be used in almost every operation is in need for authentication of personal identity as people realize that biometrics is really a viable procedure for protection of confidentiality and from deception [1, 2].

In addition, biometric can hamper the increases of identity thefts and are able to fulfil the rise of security concern to protect the network and databases [3]. It is now evident that security aspects are no longer similar to traditional methods such as using keys, pad-locks and password but it extends beyond physical security as such a good authentication mechanism is deemed important.

In biometric systems, templates are generated from feature extraction. However, since the biometric data are long lasting, a compromise to the biometric templates can result in eternal loss of individual's biometrics. This will result in spoofing or stealing of the biometric template to gain access illegally to any transaction [4]. Therefore, methods to protect the biometric template should never be seen trivial. The core purpose of biometric template protection is to avoid an imposter to steal the biometric data [1].

This paper intends to review the confidentiality and integrity, of biometric template protection and lightweight encryption. The objective of this paper will cover on biometric fingerprint system, its limitation and ways to prevent the limitation. Besides, this paper will also discuss on conceptual model of the biometric fingerprint template protection in the perspective of confidentiality, which is block cipher encryption, and integrity, which is an Authenticated-Encryption (AE) mode. Further, the author will insert some excerpt of the author's work, which is currently under implementation.

This paper will be organized as follows; Section 1 will discuss on introduction, followed by Sections 2 which is biometric systems, and Section 3 biometric systems and its limitations. Section 4 will brief on biometric template protection, while Section 5 will touch on confidentiality and integrity of biometric cryptosystem. This is further followed by discussion on Section 6. Last but not least, Section 7 is conclusion and future work.

2. Biometric Systems

General biometric fingerprint has three procedures, which consist of enrolment, verification, and identification. Most of these procedures utilize the accompanying components: capture, feature extraction, template creation, matching, and data storage. Figure 1 shows the procedure of general biometric fingerprint system. The functionalities of general biometric fingerprint system are described below [5].

a. Enrolment: The preliminary process of gathering from an individual biometric data samples as biometric template. This can be done by feature extraction of fingerprint to calculate the fingerprint minutiae.

b. Verification: Conduct a matching rate concerning the individual's biometric sample and the claimed identity's biometric template.
c. Identification: Determine the identity of an anonymous person by analyzing the user's biometric sample with templates kept in a database.

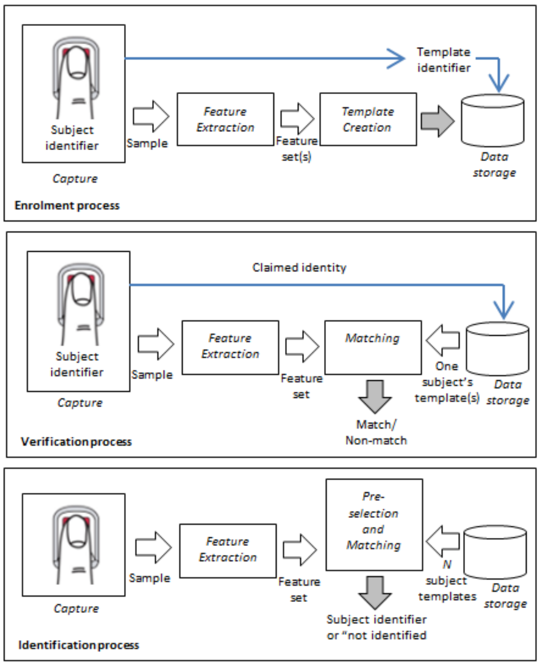


Fig. 1: Biometric Fingerprint System [5]

3. Biometric Systems Limitations

Biometric systems lack of some confidentiality and integrity concerns might somewhat reduce their pervasive use by recent vulnerabilities and threats that are targeted particular to biometric. Eight locations have been identified by [6] which are available for attacks in a general biometric system, as presented in figure 2 [7]. Point number one is that the attackers can alter, replace and steal the biometric template to gain to the application device illegally. While point number two, the biometric template can be used to make a physical spoof to acquire illegal access to any system that use same biometric traits. Apart from that, point number three, to gain unauthorized access, the attackers replayed the stolen biometric templates to the matcher to past the authentication vaults. Furthermore, point number four, the attackers can use cross matching between other databases secretly without user's acknowledgement. Next, point number five, the attackers can replace the matcher with a malware such as Trojan horse program to disguise the users. Point six affects the attacks on the template database. Then, point number seven, the attackers can manipulated or stole the templates throughout the communication between the template database and the matcher. While point number eight, the attacker can take-over the matcher's result.

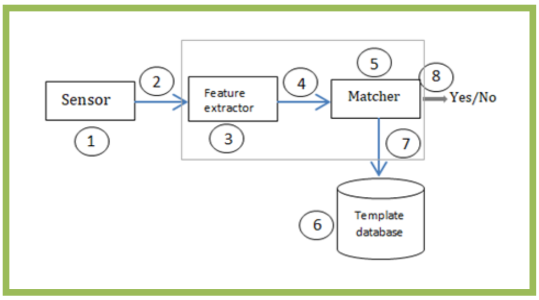


Fig. 2: Possible attacks in a generic biometric system [6, 8]

4. Biometric Template Protection

Biometric Information Protection, which is ISO/IEC Standard 24745, gives a standard direction for the protection of biometric information. Biometric template protection approaches can be generally categorized as feature transformation and biometric cryptosystems [9]. Figure 3 shows the categories of template protection schemes, which are feature transformation and biometric cryptosystem.

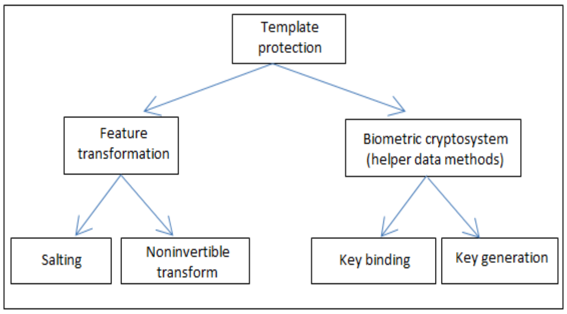


Fig. 3: Categorization of Template Protection Schemes [7]

Biometric template protection approaches must highlight the elements of diversity, revocability, security, and performance. The following are the desirable characteristics of template protection schemes [1, 4, 10].

a. Diversity: Assumed two protected templates produced from the similar biometric information, it should be computationally hard to distinguish whether they are gotten from the similar information or acquired from the initial biometric information.

b. Revocability: Template that has been compromised should be invalidated and it must be likely to reproduces a new template from the identical biometric data.

c. Security: Assumed a protected template, it must be computationally hard to discover a biometric feature set that will match from the given template.

d. Performance: The performance recognition of the biometric system must not be reduced by the operation of the protection approach.

Biometric template protection can be classified by two types, which are biometric cryptosystem and feature transformation.

4.1. Biometric Cryptosystem

There are two biometric cryptosystem approaches. First is key binding, in the case when randomly generated key is safely bound to the biometric feature. Second is key generation, when a key is adopted from the biometric data.

In key binding, helper data are acquired by binding a selected key to a biometric data. Therefor the binding process is a mixture of the secret key and the biometric template is kept as a helper data. By assigning a suitable key recovery process, keys are taken from the helper data during matching. Cryptographic keys are free from biometric data, which are revocable. However generating a new key usually needs to re-enrolment in order to obtained new helper data [11].

In key generation, helper data are obtained only from the biometric data. Keys are instantly created from the helper data and a given biometric sample. The storage of helper data is not compulsory but most of previous key-generation schemes do store helper data. Examples of key generation schemes are “fuzzy extractors” and “secure sketches” [11]. Figure 4 shows the basic concept of biometric encryption.

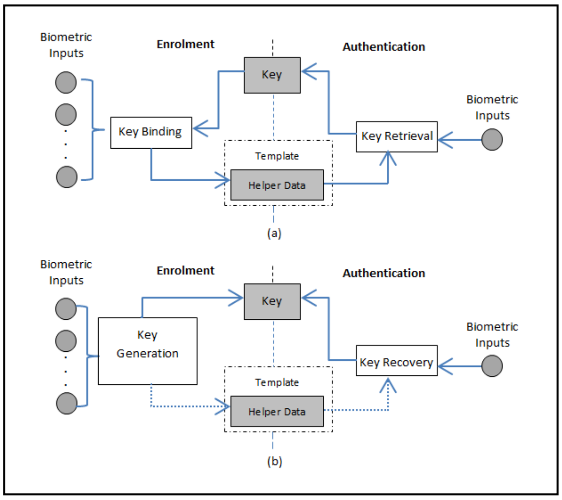


Fig. 4: The Basic Concept of Biometric Encryption (a) Key Binding and (b) Key Generation [11]

4.1. Approaches to Biometric Key-Binding

Techniques used in biometric key-binding are fuzzy commitment and fuzzy vault.

4.1.1. Fuzzy Commitment

In theory, it is uncomplicated, until now it is the most studied biometric cryptosystem approach. A biometric template must be designed in an organised bit string of a certain length. A key is plotted to an Error Correction Codeword of the equal length, *n*, as the biometric template. The codeword and the template are XORed, and the subsequent n-bit string is stored into helper data together with the hashed value of the key [12].

4.1.2. Fuzzy Vault

Fuzzy vault is appropriate for unordered data with random capacity, for example minutiae of a fingerprint. A key is denoted as constants of a polynomial in a Galois field, such as GF(2^{16}). Actual minutiae are stored in the fuzzy vault, although they are concealed inside the chaff points. This could turn into possible vulnerabilities [1, 12].

4.2. Approaches to Biometric Key-Generation

Techniques used in biometric key-generation are secure sketches and fuzzy extractor.

4.2.1. Secure Sketches and Fuzzy Extractor

The secure sketch can be recognized as helper data that releases only a few information of the template, but enables exact renewal of the template when accessible with a query that is close to the template. While the fuzzy extractor is a cryptographic primitive that generates a cryptographic key from the biometric features which designed to convert noisy data, for example biometric features, into cryptographic keys [7].

Key-generation has an abnormal state of entropy, which could let the construction of robust cryptographic keys. However, this situation has a major drawback, given by the variation of intra-class of the biometric data which are fingerprints from the identical fingers yet appear to be different from each other, which makes it impossible to recover precisely the same keys without fail, with a bit-level of accuracy. In the other hand, key-binding, is the most effectively utilized in bio-cryptography and represents the equivalent as part of the biometric cryptosystem [13]. Therefore, for this paper, the authors will utilize the approach of key-binding.

Another type of biometric template protection is feature transformation techniques, which convert the biometric template based on factors resulting from exterior information for example user’s passwords or keys. Readers can further read on these topics from [4, 14, 15].

5. Confidentiality and Integrity of Biometric Cryptosystem

Apparently, in key binding scheme the helper data must not reveal any information about the biometric data. Nevertheless, past study demonstrates that it does actually leak some important information about the data [16]. Besides, the traditional fuzzy commitment scheme cannot satisfy the hiding and binding scheme of biometric template and considered as insecure. This is because, the cryptographic hash function *h(c)* where the secret message c is concealed in the hash value *h(c)* is not sufficient enough to secure since the cryptographic hash functions like SHA and MD5 classification have already been demonstrated hypothetically and essentially susceptible to second pre-image attacks and collision [17].

Most in any IT framework, these necessities must be included such as confidentiality, integrity, availability and authenticity [18]. Therefore, in the biometric systems, confidentiality means to give the privacy to the expected users, whereas authentication is the central components of biometric systems. Data confidentiality and integrity are vital to assure that stored and transferred information is not available to illegal individuals, and that the information cannot be interfered. These conditions can be encountered by utilizing conventional cryptographic methods. To offer confidentiality, block or stream encryptions can be used.

However, there is a problem of key management by adopting the encryption. Various solutions can be implemented for this problem. In this case, if a custom-made key is used to protect the pseudonymous identifier (PI) and auxiliary data (AD) of a person and the key is managed by the data subject, the person has to show the key together with the biometric trait during matching. In contrast, if the authority who verifies the data subject manages the key, actions must be taken to keep every individual’s key safely. Data integrity can be delivered for example by a “signature” or a “Message Authentication Code (MAC)”. Alternatively, authenticated encryption (AE) mode can be endorsed which accordant to ISO/IEC 19772 [19]. Thus, in this paper confidentiality refers to lightweight encryption while integrity refers to authenticated encryption (AE) mode, which will be discussed on next section.

5.1. Lightweight Block Cipher

Concerning security issues in biometric sensor or any resource-constrained devices, a significant research effort has been carried out on cryptography designed for low-cost, low throughput, resource-constraint devices, etc. This area has been referred to as “lightweight cryptography”, and has resulted in a variety of new protocols that have been suggested for small devices, such as RFID tags and wireless sensor networks (WSNs) [20].

Block ciphers are better than stream ciphers because of the latter disadvantage in the long loading step before to initial usage. Furthermore, some protocol is not compatible with stream ciphers. Nevertheless, they are still in use because of their speed and ease in hardware. They are frequently designed to operate where the plaintext size is uncertain [21]. Thus, in this study the authors focus more on lightweight block cipher. There are several lightweight block ciphers that are used for constrained devices, such as

Present [22], Advance Encryption Standard (AES) [23], and Prince [24] to name a few.

Among these encryption techniques, AES is one of the most preferred encryptions due to its efficient performances and security reliability [25]. AES cipher has three different categories which are AES-128, AES-192 and AES-256, for which AES-128 complies with lightweight characteristic [21].

However, AES focuses on providing confidentiality but not authenticity. Existing encryption algorithm does not provide data authenticity [26] .Without covering the aspect of authenticity as suggested by NIST [27], AES cannot offer a complete protection to its users. Thus, this creates an opportunity for research to investigate further on improving the existing AES cipher and to improve its security [28].

5.2. Authenticated-Encryption (AE) Mode

Security needs are varied in different cryptographic functions. In addition, the strings to be handled by such applications generally have uncertain lengths. Therefore, a block cipher has to be properly designed to process such strings and also to achieve the exact security objectives. Techniques designed for doing these are known as modes of operations of a block cipher [28,29].

Thus, a few modes on random length of message are designed, such as "CBC (Cipher-block Chaining Mode), OFB (Output Feedback Mode), CFB (Cipher Feedback Mode) and ECB (Electronic Codebook Mode)." Nevertheless as some of these earliest modes, can only offer confidentiality or authenticity, but are not able to deliver both simultaneously [30, 31].

However, Galois/Counter Mode (GCM), variant of the Counter with CBC Mode (CCM), Offset Codebook Mode (OCB) and Carter-Wegman + CTR Mode (CWC), are some of the new advanced modes, designed to improved security which can perform confidentiality and authenticity simultaneously with the appropriate block ciphers, and thus are known as the Authenticated Encryption (AE) mode [30]. In this paper, OCB will be used alongside with AES, which provides both confidentiality and integrity security services for encryption and authentication.

OCB mode (Offset Codebook Mode) is one of the authenticated encryption modes of operation for cryptographic block ciphers. OCB mode was targeted to afford both confidentiality and integrity. It is technique to integrate a "Message Authentication Code (MAC) into the block cipher." Thus, OCB mode prevents the requirement to use two operations: a MAC for authentication and encryption for confidentiality. The outcome is lower in operational cost compared by using separate encryption and authentication process [32]. Next sub section will discuss on conceptual model of biometric fingerprint template protection.

5.3. Conceptual Model of Biometric Fingerprint Template Protection

For this sub section, the authors insert some excerpt of current works regarding the use of AES and OCB as a confidentiality and integrity for the protection of biometric fingerprint template.

Fingerprint recognition consists of enrolment of the fingerprint to the scanner to extract the features and store the template in the database. Second, fingerprint recognition will also do the verification and identification whereby to match the user's fingerprint and fingerprint's template stored in database, whether it is true or false. The templates kept in the database will be encrypted by the proposed technique upon verification and identification. Third, if the user is valid, access is granted. Figure 5 demonstrates the basic design of the conceptual model of fingerprint template protection. There are 4 phases included which are enrolment, binding, matching and integrate.

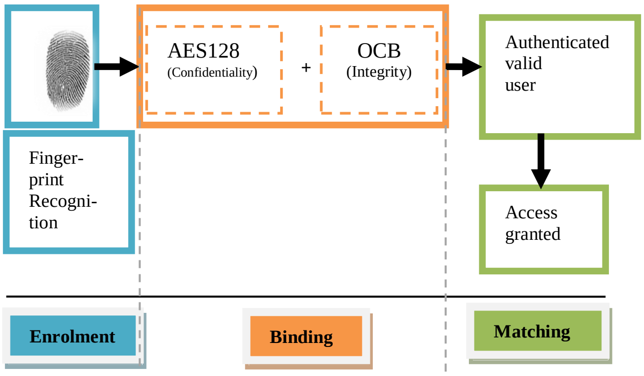


Fig. 5: Conceptual Model of Biometric Fingerprint Template Protection

5.3.1 Enrolment

During the enrolment phase, a fingerprint scanner produces a raw digital representation of the fingerprint of an individual. Then, a template is generated from feature extraction, which is situated at point number 3 in figure 2. Figure 6 shows the process of enrolment.

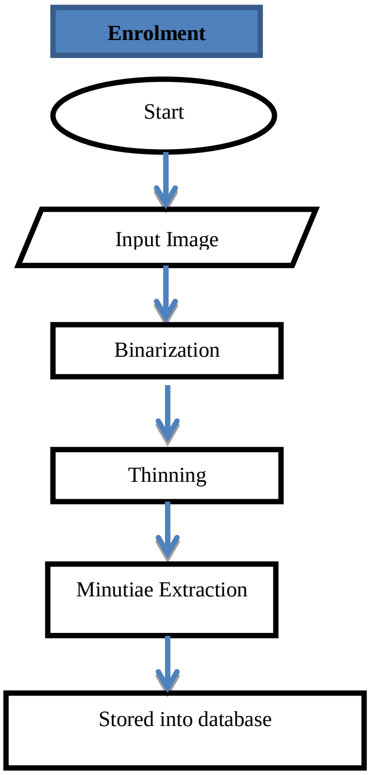


Fig. 6: Enrolment Flowchart

5.3.2. Binding

AES key *k* is plotted to an arbitrarily Error Correcting Code (ECC) knows as codeword *c*. The codeword will be bounded to the biometric template *b* (XORed) to produce the encrypted template *e* n-bit string. Using OCB authentication tag *t* to codeword and is stored into helper data along with *e*, which is kept in system database. Figure 7 shows the process of binding. By using OCB, the symmetric key is shared and authenticates to be from the original sender.

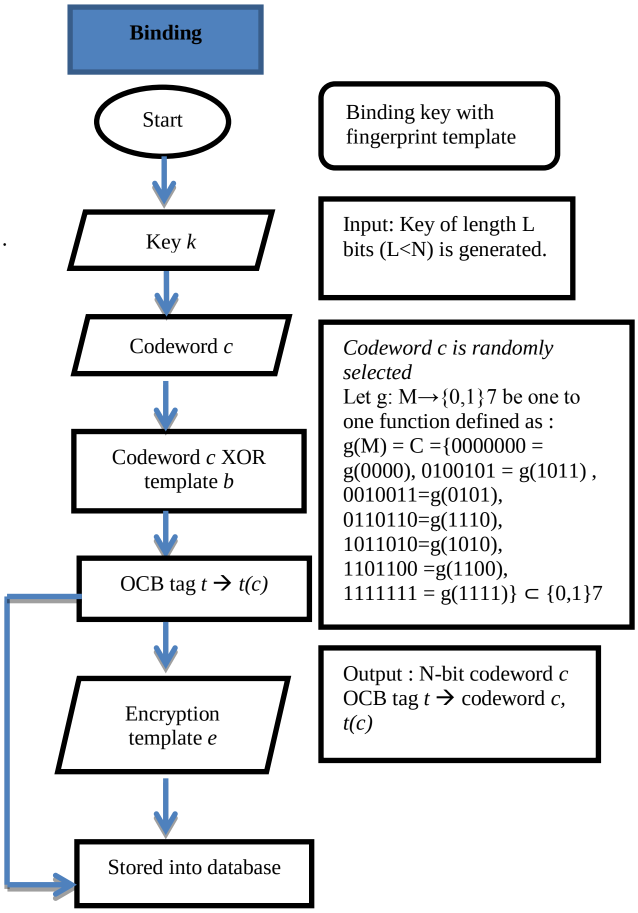

Binding
Start
Binding key with fingerprint template
Key *k*
Input: Key of length L bits (L<N) is generated.
Codeword *c*
Codeword c is randomly selected
Let g: M→{0,1}7 be one to one function defined as :
g(M) = C ={0000000 = g(0000), 0100101 = g(1011) , 0010011=g(0101), 0110110=g(1110), 1011010=g(1010), 1101100 =g(1100), 1111111 = g(1111)} ⊂ {0,1}7
Codeword *c* XOR template *b*
OCB tag *t* → *t(c)*
Encryption template *e*
Output : N-bit codeword *c*
OCB tag *t* → codeword *c*, *t(c)*
Stored into database

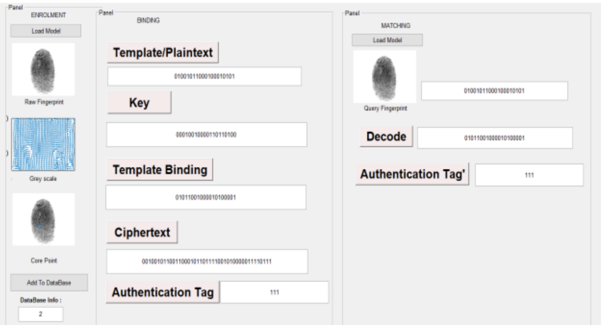
Fig. 7: Binding Flowchart

5.3.3. Matching

In matching phase, query biometric is acquired for feature extractor to produce a biometric template *b'*. The template is than XORed with e obtain from system database to get *e'*. In another word by decrypting *e'*, codeword *c'* is achieved. Therefore, if query image is similar as stored biometrics and within a definite threshold in terms of ECC measure, it can be said, $c = c'$. This can be verified by comparing OCB authentication code tag *t*, *t (k, c)* == *t (k, c')* and the k-bit key is revealed if the tag is same and thus it matched, otherwise it failed. Figure 9 shows the process of matching.

5.3.4. Integration

After these three phases have been done, the integration phase will complete a new prototype. Figure 8 shows the screen shot of the prototype interface.


Panel
ENROLMENT
Load Model
Raw Fingerprint
Grey scale
Core Point
Add To DataBase
DataBase Info : 2

Panel
BINDING
Template/Plaintext: 01001011000100010101
Key: 00010010000110110100
Template Binding: 01011001000010100001
Ciphertext: 0010010110011000101101111001010000011110111
Authentication Tag: 111

Panel
MATCHING
Load Model
Query Fingerprint: 01001011000100010101
Decode: 01011001000010100001
Authentication Tag': 111

Fig. 8: Prototype Interface

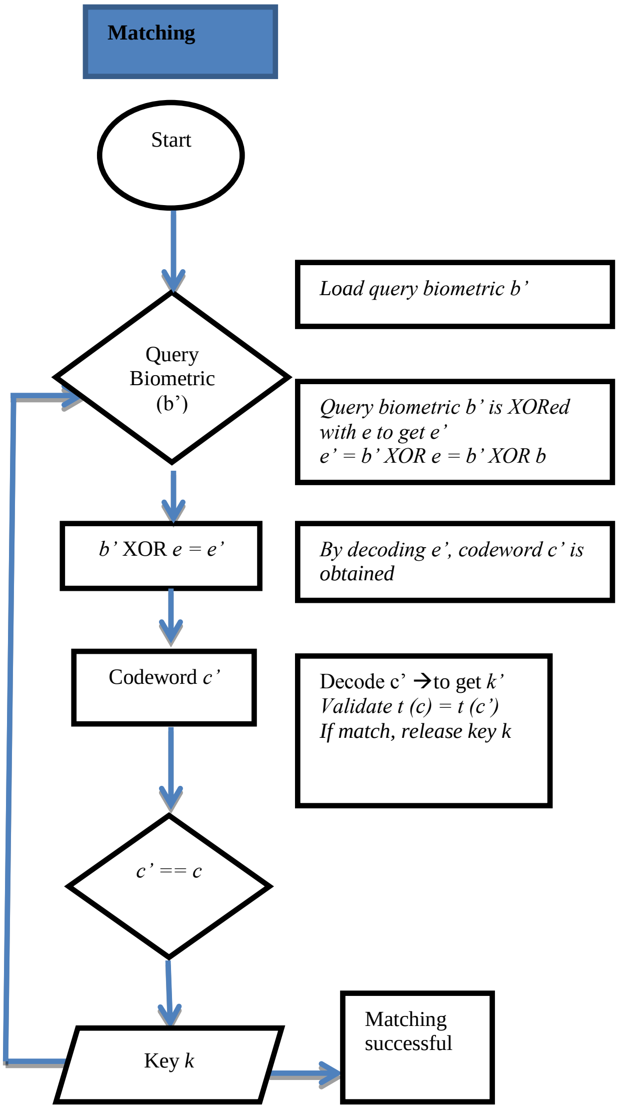


Fig. 9: Matching Flowchart

6. Discussion

Since biometric devices are resource-constraint, lightweight encryption should be used rather than non-lightweight encryption. Ultra-lightweight and lightweight encryption typically offers 80 to 128 bit security. Based on the review done on existing lightweight cipher, AES appears to be the highest alternative for software applications, since it is the best performer in a variety of accepted systems.

Besides, AES is one of the common and preferred encryption due to its efficient performances and security reliability. AES-128 complies with lightweight characteristic [25, 33].

Several authentication encryption (AE) modes mentioned demonstrate good, but inadequate, performance. Some types of attacks, such as an acknowledgement that is not from the true receiver of a message or even replay attacks carried out by sending an old message to start exchanging data by an intruder, can be prevented through message authentication code, named Message Authentication Code (MAC), which is an extraction of the message and approves its integrity. Encryption alone does not provide sufficient security [34].

Despite the advantages of using OCB and AES to protect the biometric encryption, some challenges might follow for example intrusion on the template is one of the viable imposter attacks on a biometric system. It is conceivable that determinations to secure the template may directly effect on the authentication itself. However, this research is currently on development, therefore there is no statistical result presented in this paper.

7. Conclusion and Future Work

In this study, biometric lightweight encryption technique for biometric fingerprint template protection is proposed. This technique incorporates both lightweight block cipher, which is AES-128, and authenticated encryption mode, which is OCB. The significant of this technique is that it covers two of the security objectives, which are confidentiality and integrity. Thus, the fingerprint templates will be well protected. Besides, this lightweight technique can minimize energy consumption and give better performance.

Furthermore, this research required further evaluation particularly in "energy saving, performance and security" which will be implemented in the nearest future works.

Acknowledgement

The "authors wish to thanks Awang Had Salleh Graduate School of Arts and Sciences, Universiti Utara Malaysia for funding this study under the Postgraduate Grant, S/O code: 16042.

The authors also wish to thanks the Ministry of Higher Education (Malaysia) for funding this study under the Trans Disciplinary Research Grant Scheme (TRGS), S/O code: 13164 and RIMC Universiti Utara Malaysia for administration of this study."

References

[1] [Sapkal S, Deshmukh RR. Biometric Template Protection with Fuzzy Vault and Fuzzy Commitment. Proceedings of the Second International Conference on Information and Communication Technology for Competitive Strategies. (2016);60:1--60:6. doi:10.1145/2905055.2905118.

[2] Ghazali T, Zakaria N. Security , Comfort , Healthcare , and Energy Saving : A Review on Biometric Factors for Smart Home Environment. Journal of Computers. (2018);29(1):189-208. doi:10.3966/199115992018012901017.

[3] Mehta G, Dutta MK, Karasek J, Kim PS, Union E. An Efficient and Lossless Fingerprint Encryption Algorithm Using Henon Map & Arnold Transformation. (2013);(Iccc):485-489.

[4] Mwema J, Kimwele M, Kimani S. A Simple Review of Biometric Template Protection Schemes Used in Preventing Adversary Attacks on Biometric Fingerprint Templates. International Journal of Computer Trends and Technology. (2015);20(1):12-18. doi:10.14445/22312803/IJCTT-V20P103.

[5] Maltoni D, Maio D, Jain AK, Prabhakar S. Handbook of Fingerprint Recognition. Annals of Physics. (2003);54(ISBN: 978-1-84882-253-5):494. doi:10.1109/MEI.2004.1342443.

[6] Ratha NK, Connell JH, Bolle RM. Enhancing security and privacy in biometrics-based authentication systems. IBM Systems Journal. (2001);40(3):614-634. doi:10.1147/sj.403.0614.

[7] Nandakumar K, Jain AK, Nagar A. Biometric template security. Eurasip Journal on Advances in Signal Processing.(2008). doi:10.1155/2008/579416.

[8] El-Abed M, Lacharme P, Rosenberger C. Privacy and security assessment of biometric systems. (2015).

[9] Nandakumar K, Jain AK. Biometric Template Protection: Bridging the performance gap between theory and practice. IEEE Signal Processing Magazine. (2015);32(5):88-100. doi:10.1109/MSP.2015.2427849.

[10] Pagnin E, Mitrokotsa A. Privacy-preserving biometric authentication : challenges and directions Preliminaries on Biometric Authentication Systems. (2017);1-11.

[11] Rathgeb C, Uhl A. A survey on biometric cryptosystems and cancelable biometrics. EURASIP Journal on Information Security. (2011);(1):1-25. doi:10.1186/1687-417X-2011-3.

[12] Cavoukian A, Stoianov A. Biometric Encryption. In: Encyclopedia of Biometrics. Springer; (2015);1-14.

[13] Velciu MA, Patrascu A, Patriciu VV. Bio-cryptographic authentication in cloud storage sharing. SACI 2014 - 9th IEEE International Symposium on Applied Computational Intelligence and Informatics, Proceedings. (2014);(May):165-170. doi:10.1109/SACI.2014.6840054.

[14] Ratha NK, Chikkerur S, Connell JH, Bolle RM. Generating cancelable fingerprint templates. IEEE Transactions on Pattern Analysis and Machine Intelligence. (2007);29(4):561-572. doi:10.1109/TPAMI.2007.1004.

[15] Nagar A, Nandakumar K, Jain AK. Biometric Template Transformation: A Security Analysis. Proceedings of SPIE - The International Society for Optical Engineering. (2010). doi:10.1117/12.839976.

[16] Sadhya D, Singh SK, Chakraborty B. Review of key-binding-based biometric data protection schemes. IET Biometrics. (2016);5(4):263-275. doi:10.1049/iet-bmt.2015.0035.

[17] Al-Saggaf AA, Haridas A. Statistical Hiding Fuzzy Commitment Scheme for Securing Biometric Templates. International Journal of Computer Network and Information Security. (2013);5(4):8-16. doi:10.5815/ijcnis.2013.04.02.

[18] Stallings W. Network Security Essentials. 5th ed. Pearson Education, Inc.; (2014).

[19] Breebaart J, Yang B, Buhan-Dulman I, Busch C. Biometric Template Protection: The need for open standards. Datenschutz und Datensicherheit. (2009);5:299-304. doi:10.1007/s11623-009-0089-0.

[20] Jacobsson A, Boldt M, Carlsson B. On the Risk Exposure of Smart Home Automation Systems. In: 2014 International Conference on Future Internet of Things and Cloud. ; (2014);183-190. doi:10.1109/FiCloud.2014.37.

[21] Manifavas C, Hatzivasilis G, Fysarakis K, Rantos K. Lightweight Cryptography for Embedded Systems - A Comparative Analysis. In: In Revised Selected Papers of the 8th International Workshop on Data Privacy Management and Autonomous Spontaneous Security. Springer-Verlag New York, Inc.; (2013);1-18. doi:10.1007/978-3-642-54568-9_21.

[22] Bogdanov A, Knudsen LR, Leander G, et al. PRESENT: An Ultra-Lightweight Block Cipher. In: Paillier P, Verbauwhede I, eds. Lecture Notes in Computer Science: Vol. 4727. Cryptographic Hardware and Embedded Systems - CHES 2007. Berlin, Heidelberg: Springer-Verlag; (2007);450-466.

[23] Daemen J, Rijmen V, Leuven KU. AES Proposal : Rijndael. Complexity. (1999);1-45. http://ftp.csci.csusb.edu/ykarant/courses/w2005/csci531/papers/Rijndael.pdf.

[24] Borghoff J, Canteaut A, Güneysu T, et al. PRINCE - A low-latency block cipher for pervasive computing applications. In: Lecture Notes in Computer Science: Vol. 7658. (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics). ; (2012);208-225. doi:10.1007/978-3-642-34961-4.

[25] Mohd BJ, Hayajneh T, Vasilakos A V. A survey on lightweight block ciphers for low-resource devices: Comparative study and open issues. Journal of Network and Computer Applications. (2015);58:73-93. doi:10.1016/j.jnca.2015.09.001.

[26] Cid C. Designs and Challenges in Authenticated Encryption. In: International Workshop on Cybersecurity. Kyushu University; (2016). http://staff.cs.kyushu-u.ac.jp/data/event/2016/02/160107_Carlos_Cid.pdf.

[27] Stallings W, Brown L. Computer Security Principles and Practice.; (2012).

[28] [28]Ghazali TK, Zakaria NH. An Enhancement Of Lightweight Encryption For Security Of Biometric Fingerprint Data For Smart Home Environment. In: Proceedings of the 6th International Conference on Computing and Informatics, ICOCI 2017 25-27April, 2017 Kuala Lumpur. ; (2017);1-6.

[29] Chakraborty D, Sarkar P. On modes of operations of a block cipher for authentication and authenticated encryption. Cryptography and Communications. (2016);8(4):455-511. doi:10.1007/s12095-015-0153-6.

[30] Chen H. Authenticated Encryption Modes of Block Ciphers, Their Security and Implementation Properties. (2009). http://www.emsec.rub.de/media/crypto/attachments/files/2011/03/chen.pdf.

[31] Krovetz T, Rogaway P. The software performance of authenticated-encryption modes. In: Lecture Notes in Computer Science: Vol. 6733 (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics). ; (2011):306-327. doi:10.1007/978-3-642-21702-9_18.

[32] Rogaway. OCB: Background. http://web.cs.ucdavis.edu/~rogaway/ocb/ocb-faq.htm. Published (2015).

[33] Law YW, Doumen J, Hartel P. Survey and benchmark of block ciphers for wireless sensor networks. ACM Transactions on Sensor Networks. (2006);2(1):65-93. doi:10.1145/1138127.1138130.

[34] Mehran N, Reza Khayyambashi M. Performance Evaluation of Authentication-Encryption and Confidentiality Block Cipher Modes of Operation on Digital Image. International Journal of Computer Network and Information Security. (2017);9(9):30-37. doi:10.5815/ijcnis.2017.09.04.