Research Article

International Journal of Advanced Computer Research, Vol 9(43)
ISSN (Print): 2249-7277 ISSN (Online): 2277-7970
http://dx.doi.org/10.19101/IJACR.PID49

Security performance evaluation of biometric lightweight encryption for fingerprint template protection

Taqiyah Khadijah Ghazali[1*] and Nur Haryani Zakaria[2]
Research Scholar, School of Computing, College of Arts and Sciences, Universiti Utara Malaysia[1]
Senior Lecturer, School of Computing, College of Arts and Sciences, Universiti Utara Malaysia[2]

Received: 13-September-2018; Revised: 30-November-2018; Accepted: 30-January-2019

Abstract
Due to its accuracy and convenience, the fingerprint is one of the most reliable biometric-based authentication methods for personal identification and providing access control to many applications. However, previous studies have shown that, the fingerprint template is exposed to threat in which the attackers can steal and modified the template to acquire illegal authorization. Therefore, a technique to protect the biometric template has been proposed. The proposed technique involved the biometric template binding by advanced encryption standard (AES-128) key algorithm, which is to provide confidentiality alongside with the offset codebook mode (OCB), an authenticated encryption (AE) mode to provide integrity. Hence, this paper intends to evaluate the security performance of the proposed technique. Three parameters will be analysed which are peak signal to noise ratio (PSNR), correlation coefficient and histogram. The efficiency of the proposed technique is measured by the standard of its capability to hide all the information by correlating the relationship between the original and encrypted biometric image using PSNR, correlation coefficient and histogram analysis. The experimental results show good security performance in the given parameters.

Keywords
Fingerprint template protection, Biometric cryptosystem, Key-binding, Security performance, Lightweight block cipher, Authenticated-encryption mode.

1.Introduction
Biometric system is likely to be used in almost every operation which is needed for authentication of personal identity as people realized that biometrics is considered as a viable procedure for the protection of confidentiality and fraud [1, 2]

However, users need to securely transmit their biometric data throughout the network. The information transmitted through computer networks may be intercepted, modified, fabricated or even interrupted by an unauthorized third party. While transferring the essential data over communication channels, security is an important element to be measured [3]. Due to the increasing number of Internet of Things (IoT) applications, it is essential to protect confidential biometric data against unauthorized access by third parties.

Biometric systems' lack of some confidentiality and integrity concerns might reduce their pervasive use of recent vulnerabilities and threats that are targeted particularly towards biometric applications. Eight locations have been identified by [4] which are available for attacks in a general biometric system, as presented in *Figure 1*. Based on *Figure 1*, point number one is that the attackers can alter, replace and steal the biometric template to gain to the application device illegal. 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 a Trojan horse program to disguise as the users. Point six affects the attacks on the template

*Author for correspondence

database. Then, point number seven, the attackers can manipulate or steal the templates throughout the communication between the template database and the matcher. Finally, point number eight, the attacker can take over the matcher's result.

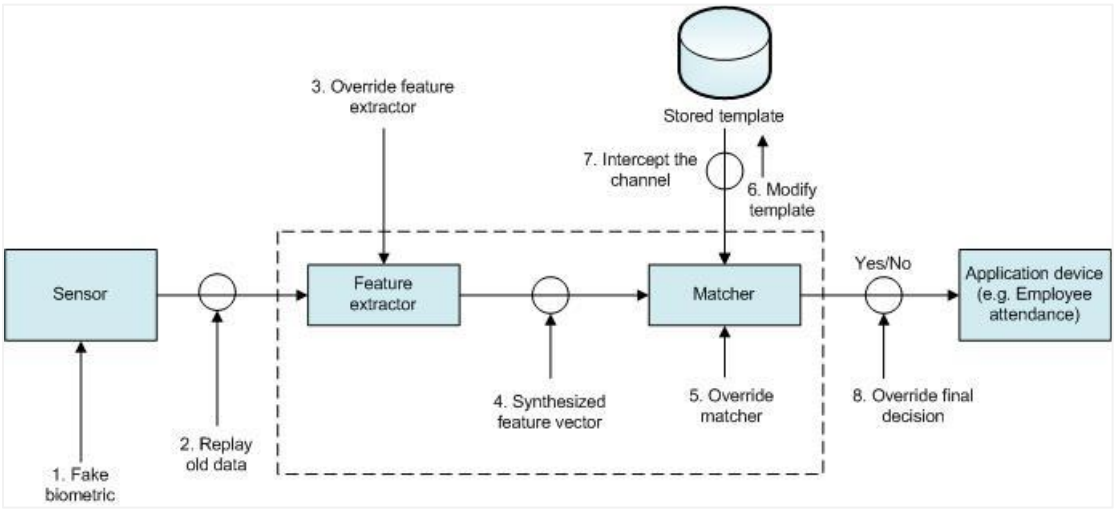


Figure 1 Point of attack on a generic biometric system (adapted from [4])

In order to solve this problem, several schemes were created to protect the fingerprint information from attackers which commonly known as *biometric template protection based on the point of attack*. These schemes will be discussed further in the related work sections. This study was designed based on an ongoing work – a biometric lightweight encryption technique for fingerprint template protection which is proposed recently [5, 6]. The study proposed a conceptual model that comprises of a technique which covers points of attack (i.e. point no 5 and 6). Further discussion on this concept will be discussed in the conceptual model of biometric fingerprint template protection technique section. This technique applies that the biometric data bind with the block cipher encryption in the perspective of confidentiality, and Authenticated-Encryption (AE) mode, in the perspective of integrity. However, the study did not provide any evidence on the evaluation perspective. Thus, this study intends to extend the study by analysing the confidentiality of biometric cryptosystem by performing the security performance of the protected template image.

This paper will be organized as follows; the next section will discuss on related work, followed by the conceptual model of biometric fingerprint template protection technique. Further, the next section will touch on methodology. This is further followed by results and findings, discussion and last but not least, conclusion and future work.

2.Related work

This section presents previous work regarding biometric template protection schemes, lightweight block cipher and Authenticated Encryption (AE) Mode.

Biometric template protection schemes

A standard direction for the protection of biometric information is ISO/IEC Standard 24745. Biometric template protection approaches can be generally categorized as feature transformation and biometric cryptosystems [7]. *Figure 2* shows the categories of template protection schemes, which are feature transformation and biometric cryptosystem.

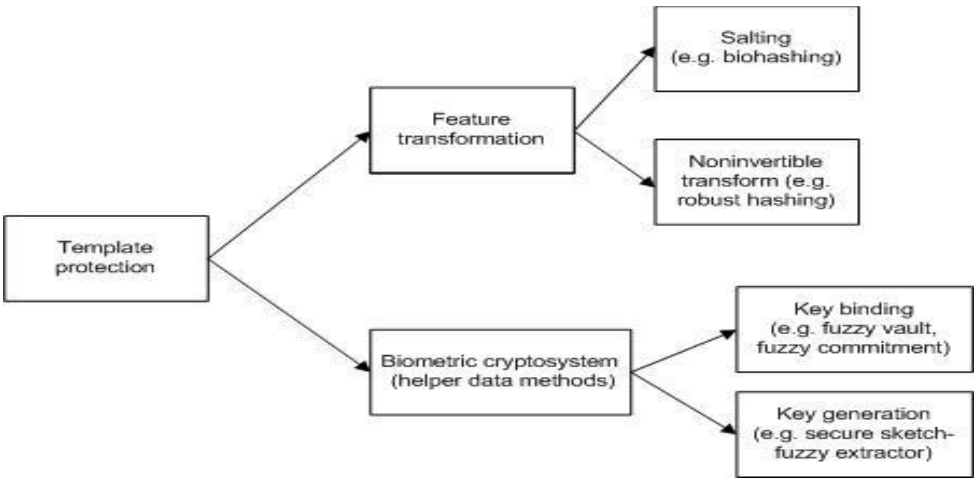


Figure 2 Categorization of template protection schemes (adapted from [7])

There are two biometric cryptosystem approaches. First is key-binding, in the case when a randomly generated key is safely bound to the biometric feature. Therefore, the binding process is a mixture of the secret key and the biometric template is kept as a helper data. Techniques used in biometric key-binding are fuzzy commitment and fuzzy vault. Second is key-generation, which a key is adopted from the biometric data. Keys are instantly created from the helper data and a given biometric sample. Examples of key-generation schemes are fuzzy extractors and secure sketches. *Figure 3* shows the basic concept of biometric encryption, key-binding and key-generation**.** This research will focus more on key-binding technique as the proposed technique is enhanced from the key-binding [8].

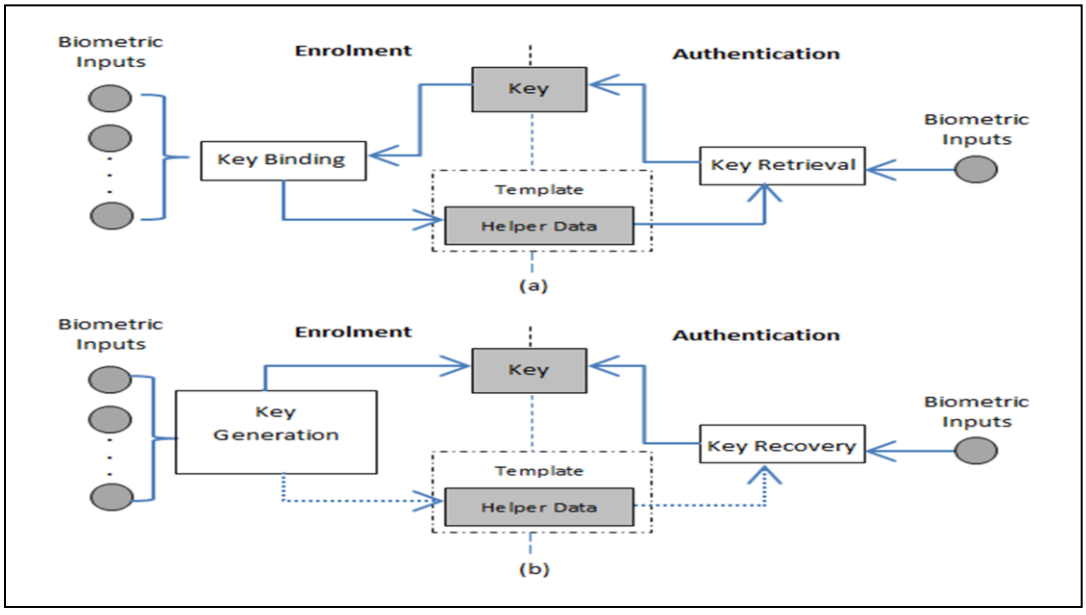


Figure 3 The basic concept of biometric encryption (a) key-binding and (b) key-generation (adapted from [8])

Approaches to biometric key-binding, in concept, fuzzy commitment is unsophisticated. To date it is the most studied biometric cryptosystem approach. In fuzzy commitment, 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 same length, *n*, as the biometric template. The codeword and the template are XORed, and the subsequent n-bit string is kept into helper data together with the hashed value of the key [9].

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, 9].

Lightweight block cipher

Significant research effort has been carried out on cryptography designed for low-cost, low throughput and resource-constraint devices. This area known as lightweight cryptography, and has resulted in a variety of new protocols that have been suggested for small devices, such as Radio-Frequency Identification (RFID) tags and wireless sensor networks (WSNs) [10].

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 [11]. 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 [12], advance encryption standard (AES) [13], and PRINCE [14] to name a few.

Among these encryption techniques, AES is one of the most preferred encryptions due to its efficient performance and security reliability [15]. AES cipher has three different categories which are AES-128, AES-192 and AES-256, for which AES-128 complies with lightweight characteristic [11].

However, AES focuses on providing confidentiality but not authenticity. Existing encryption algorithm does not provide data authenticity [16]. Without covering the aspect of authenticity as suggested by NIST [17], AES cannot offer a complete protection to its users. Thus, this creates an opportunity for researchers to investigate further on improving the existing AES cipher and to improve its security by using authenticated encryption (AE) mode [5].

A few researchers have been using AES in biometric environment. A novel fingerprint encryption scheme was proposed by [18] which uses the bit plane encryption and the random block feedback (RBF). "RBF is a mode for the block ciphers which use an unknown random block as a feedback. The mode makes the differential/linear cryptanalysis require at least the complexity of an exhaustive key search, maintaining the original safety of the block cipher." In implementing the fingerprint RBF mode encryption, they use AES as a primary block cipher. Based on this study, they successfully implemented the security objective which is confidentiality. However, security objectives such as integrity are not applied whereby it will cause the possibility compromise of the data is higher.

Another related work by [19] proposes a protocol to transfer fingerprint images. To lessen the computational task on the resource-constrained sensor, they apply the "encryption algorithm to a nonce for integrity and to a specific bitplane of each pixel of the fingerprint image" for confidentiality. They also use AES encryption to encrypt the biometric data. Their protocol can reduce the execution time of full encryption by a factor of six.

Authenticated Encryption (AE) mode

Some 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) [20]. For example, Galois/Counter Mode (GCM), a variant of the counter with CBC Mode (CCM), offset codebook mode (OCB) and Carter-Wegman + CTR Mode (CWC). 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 a technique to integrate a message authentication code (MAC) into the block cipher. Thus, OCB mode removes the requirement to use two operations: a MAC for authentication and encryption for confidentiality. The outcome is lower in operational

cost compared to using separate encryption and authentication process [20]. OCB mode, offers both privacy and authenticity; that is to say, this scheme provides data authenticity without increasing the cost of encryption [21, 22].

A comprehensive search of the relevant literature returned only one related article although it is not from biometric area. The closest research is from [23], which have been proposed AE mode to protect digital image. Their results show that the model based on OCB scheme, by both AES and Serpent algorithms, exhibits good performance on a digital image compared to the models based on other modes. OCB-AES based scheme, associated with its own authentication, has considerable speed in comparison with other confidentiality only modes.

3.Conceptual model of biometric fingerprint template protection technique

In this section, the authors insert some excerpt of current works regarding the use of AES and OCB as a confidentiality and integrity of the protection of the 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 match the user's fingerprint and fingerprint 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 4* demonstrates the basic design of the conceptual model of fingerprint template protection. There are three phases included which are enrolment, binding, matching. These three phases will be integrated to produce a prototype.

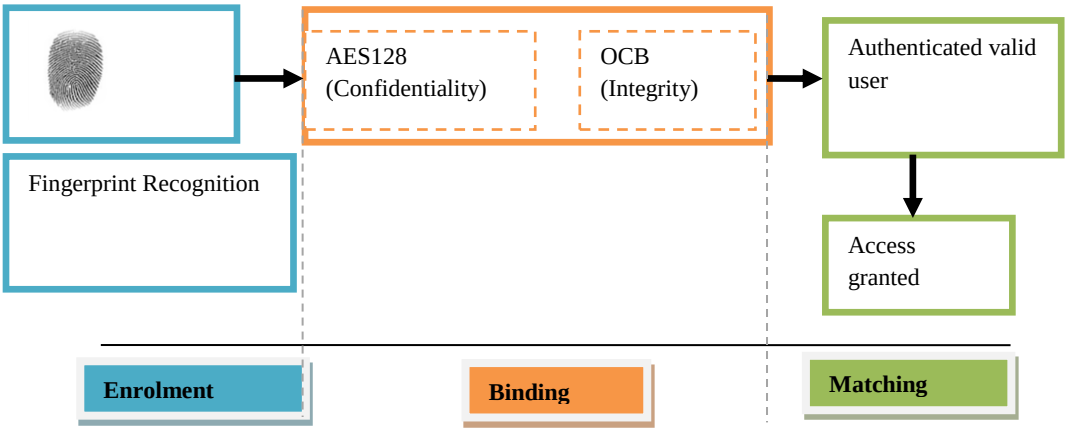


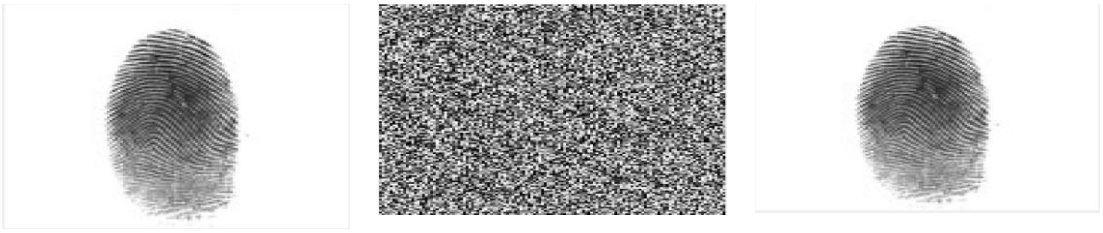
Figure 4 Conceptual model of biometric fingerprint template protection

4.Methodology

This section presents the methodology which will be carried out to conduct security performance evaluation of encrypted template. In order to conduct the evaluation, several standard measurements are used to evaluate which focus on confidentiality [23, 24]. The measurements are 1) peak signal to noise ratio (PSNR), 2) correlation coefficient and 3) histogram.

In this research, the encryption algorithms, the security analysis and the test parameters, were implemented and designed using the MATLAB R2017a environment, on a machine with Intel (R) Core (TM) i7 ~2.50GHz CPU and an 8-GB of RAM.

The tests are applied to a fingerprint database for fingerprint verification competition (FVC2004). The FVC2004 consist of four databases, three real and one synthetic. Each database consists of 80 fingerprints whereby total of four databases is 320 fingerprints. Each database is collected by using various sensors. Database 1 and database 2 are collected using optical sensor with a different brand. Meanwhile, database 3 is collected using thermal sweeping sensor and database 4 is collected using synthetic fingerprint generation. For this work, database 1 was used which consist of 80 fingerprints [25]. *Figure 5* shows the template encrypted and decrypted by the proposed technique.



(a) Original (b) Encrypted (c) Decrypted

Figure 5 Template image: (a) original, (b) encrypted and (c) decrypted images with OCB-AES128

Peak signal to noise ratio (PSNR)

The peak signal-to-noise ratio (PSNR) is the most common criterion used to measure the similarity between the original plain image and the cipher image [26]. It is to show that encrypted template's images are fully meaningless and make it difficult for the attackers to retrieve any important data relating to the original image. Therefore, 28 dB is the maximum threshold of PSNR value needed for similarity between original and encrypted biometric template [27]. Low PSNR (Peak Signal to Noise Ratio) indicates a high variation between the encrypted template and original. The major advantage of this measure is that is does not require complex computations [28].

PSNR calculates the peak signal-to-noise ratio for any given image (*e.g.* image *x)* which is the encrypted template, with the image (*ref)* which is original template as the reference. *X* and *ref* must be of the same size and type. The PSNR function implements the following Equation (1) To calculate the Peak Signal-to-Noise Ratio (PSNR), where *peakval* is either specified by the user or taken from the range of the image data type (*e.g.* for *uint8* image it is 255). MSE is the mean square error, that is to say MSE between *x* and *ref* [29].

$$PSNR = 10\log_{10}(peakval^2/MSE) \quad (1)$$

Correlation coefficient

Correlation Coefficient is a performance metric used to measure the amount of similarity between two objects. It has been used as a significant parameter to evaluate the quality of a cryptosystem [23]. In the perspective of the proposed technique, if the encrypted template image and original image are totally dissimilar, thus the correlation factor will be very low or very close to zero.

In contrary, if the correlation factor is equivalent to one, then the two images are same and the encryption process is considered to be unsuccessful [26]. For example, correlation coefficients should ensure the value is between 0.75 – 1.00 for the original image and less than 0.1 for the encrypted image. If the correlation is zero, the original and encrypted images are totally not the same [27]. A negative correlation shows that for any two variables *x* and *y*, an increase in *x* is associated with a decrease in *y*. Hence it means the relationship between two images are the same way a positive correlation coefficient does [30]. That is to say, a correlation coefficient of -0.0054 shows the same strength as a correlation coefficient of 0.0054. Correlation coefficient in terms of the covariance of x and y in Equation (2) [31]:

$$Pxy = \frac{\mathrm{Cov}(rx,\ ry)}{\sigma x\ \ \sigma y} \quad (2)$$

Histogram analysis

A histogram is a graph that displays the distribution of data values or the repetition of each pixel in an image. The histogram of an encrypted template image demonstrates that the correlation between two adjoining pixels and in all directions, is insignificant and there are numerous pixels in the encrypted image; hence, the attacker can barely achieve any important information [23].

5.Results and findings

The low PSNR value achieved by the proposed algorithm (below than 10dB) proves that the two images are uncorrelated, and thus confidentiality is achieved. *Table 1* shows the experimental results of PSNR and correlation coefficient taken from five different fingerprints.

The correlation factor measured between the original and encrypted template's images is very low, which is less than 0.1 and also means close to zero. This point out that the proposed technique is capable to protect all aspects of the transferred image, hence achieving the essential confidentiality. *Table 2* shows the correlation factor measured between the original and encrypted template's images.

Apart from that, the histogram of the original image does not have different values; for example, a pixel with a value of 250 is not practical. On the other hand, the encrypted image does have a wide range of pixels, showing diffusion in the encryption algorithm. Two examples are given in *Figure 6* that displays the histogram image. As can be seen, a histogram of the encrypted image is constant and significantly different from the histogram of the original image. Therefore, any statistical analysis attack on the encrypted image is impossible to the attackers to perform since no valuable information can be decided. As a matter of fact, the extensive difference between the histograms of the two images apparently shows that the images are highly uncorrelated. Thus, it can be concluded that the proposed technique does acquire the confusion and diffusion characteristics.

6.Discussion

In this paper, a biometric template protection scheme which is biometric cryptosystem has been proposed. The proposed technique comprises the fingerprint image template binding with the algorithm which is AES128 block cipher encryption and the authenticated-encryption mode which is OCB. The security performance of the proposed technique is analysed according to three parameters. The PSNR value between original and encrypted template of the proposed technique is less than 10 dB whereby it displays that there is no resemblance between these two images. Besides, correlation coefficient has been tested on the proposed technique and the outcome demonstrations that the algorithm delivers high resistances towards statistical attacks.

Therefore, it is a strong and efficient method to secure biometric data. Histogram analysis shows that encrypted template image makes the intruders complicated to search any probable connection between the original and its equivalent encrypted image.

Apart from that, confidential is ensured if the encrypted image is highly uncorrelated to the original plain image [26]. Confidentiality concerns with secrecy and privacy which means message should be invisible to unauthorized persons [32]. Thus, these 3 measurements show that the proposed algorithm is capable to conceal the information of the transferred image, hence accomplishing the recommended confidentiality.

Besides confidentiality, integrity means the identity of the sender should be verified on delivering the message weather the information is coming from authentic sender, from whom we are expecting [32]. Therefore, from this encryption algorithm which is OCB, the integrity element has been taken into measure to provide the tag value upon decryption which, if the tag value is same with encryption, thus the authentication is successful.

7.Conclusion and future work

This paper presented the evaluation of security performance of biometric lightweight encryption for fingerprint template protection. The objective of this paper is to measure the confidentiality of the encryption technique to hide all the attributes of the original image. Thus, this objective has been archived using the three measurements stated in this paper.

Besides, the proposed technique also contributes some benefits, for example efficiency, lightweight and secure. The proposed technique has considerable speed and energy efficiency. Further, it has low requirements to essential resources of target devices as well as lowering in operational cost. In addition, the proposed technique targeted to afford both confidentiality and integrity.

Future work may include working on other performance evaluation such as algorithm and biometric performance. Besides, the authors also will test on different data sets. This proposed technique also will focus on the possibility of the other biometric image based.

Acknowledgment

The “authors wish to thank 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 thank 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.”

Conflicts of interest

The authors have no conflicts of interest to declare.

References

[1] Sapkal S, Deshmukh RR. Biometric template protection with fuzzy vault and fuzzy commitment. In proceedings of the second international conference on information and communication technology for competitive strategies 2016 (p. 60). ACM.

[2] Ghazali TK, Zakaria NH. Security, comfort, healthcare, and energy saving: a review on biometric factors for smart home environment. Journal of Computers. 2018; 29(1):189-208.

[3] 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):12-8.

[4] Ratha NK, Connell JH, Bolle RM. An analysis of minutiae matching strength. In international conference on audio-and video-based biometric person authentication 2001 (pp. 223-8). Springer, Berlin, Heidelberg.

[5] Ghazali TK, Zakaria NH. An enhancement of lightweight encryption for security of biometric fingerprint data for smart home environment. In proceedings of the international conference on computing and informatics 2017 (pp. 1–6).

[6] Ghazali TK, Zakaria NH. Confidentiality and integrity of the biometric fingerprint template protection. International Journal of Engineering and Technology. 2018; 7(4.29):128-33.

[7] Jain AK, Nandakumar K, Nagar A. Biometric template security. EURASIP Journal on Advances in Signal Processing. 2008.

[8] Rathgeb C, Uhl A. A survey on biometric cryptosystems and cancelable biometrics. EURASIP Journal on Information Security. 2011; 2011(1):3.

[9] Soutar C, Roberge D, Stoianov A, Gilroy R, Kumar BV. Biometric encryption. In ICSA guide to Cryptography 1999. New York, NY: McGraw-Hill.

[10] Jacobsson A, Boldt M, Carlsson B. On the risk exposure of smart home automation systems. In international conference on future internet of things and cloud 2014 (pp. 183-90). IEEE.

[11] Manifavas C, Hatzivasilis G, Fysarakis K, Rantos K. Lightweight cryptography for embedded systems–a comparative analysis. In data privacy management and autonomous spontaneous security 2013 (pp. 333-49). Springer, Berlin, Heidelberg.

[12] Bogdanov A, Knudsen LR, Leander G, Paar C, Poschmann A, Robshaw MJ, et al. PRESENT: an ultra-lightweight block cipher. In international workshop on cryptographic hardware and embedded systems 2007 (pp. 450-66). Springer, Berlin, Heidelberg.

[13] Daemen J, Rijmen V. AES proposal: Rijndael.1999:1-45.

[14] Borghoff J, Canteaut A, Güneysu T, Kavun EB, Knezevic M, Knudsen LR, et al. Prince–a low-latency block cipher for pervasive computing applications. In international conference on the theory and application of cryptology and information security 2012 (pp. 208-25). Springer, Berlin, Heidelberg.

[15] Mohd BJ, Hayajneh T, Vasilakos AV. 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.

[16] https://cs.kyushu-u.ac.jp/icsg/wp-content/uploads/sites/2/2017/09/160107_Carlos_Cid.pdf. Accessed 22 June 2018.

[17] Stallings W, Brown L, Bauer MD, Bhattacharjee AK. Computer security: principles and practice. Upper Saddle River (NJ: Pearson Education; 2012.

[18] Kim Y, Yoon J, Joo JH, Yi K. Robust lightweight fingerprint encryption using random block feedback. Electronics Letters. 2014; 50(4):267-8.

[19] Moon D, Chung Y, Pan SB, Moon K, Chung KI. An efficient selective encryption of fingerprint images for embedded processors. ETRI Journal. 2006; 28(4):444-52.

[20] Chen H, Paar IC. Authenticated encryption modes of block ciphers, their security and implementation properties.2009.

[21] Rogaway P, Bellare M, Black J. OCB: a block-cipher mode of operation for efficient authenticated encryption. ACM Transactions on Information and System Security. 2003; 6(3):365-403.

[22] Krovetz T, Rogaway P. The software performance of authenticated-encryption modes. In international workshop on fast software encryption 2011 (pp. 306-27). Springer, Berlin, Heidelberg.

[23] Mehran N, Khayyambashi MR. 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):30-7.

[24] Khandelwal SS. Multitier biometric template security using cryptographic salts and personal image identification. ELCVIA Electronic Letters on Computer Vision and Image Analysis. 2014; 13(3):28-40.

[25] FVC2004. http://bias.csr.unibo.it/fvc2004/default.asp. Accessed 25 May 2018.

[26] Al-Haj A. Providing integrity, authenticity, and confidentiality for header and pixel data of DICOM images. Journal of Digital Imaging. 2015; 28(2):179-87.

[27] Mehta G, Dutta MK, Karasek J, Kim PS. An efficient and lossless fingerprint encryption algorithm using Henon map & Arnold transformation. In international conference on control communication and computing 2013 (pp. 485-9). IEEE.

[28] Shankar K, Eswaran P. Sharing a secret image with encapsulated shares in visual cryptography. Procedia Computer Science. 2015; 70:462-8.

[29] MathWorks. PSNR. https://www.mathworks.com/help/images/ref/psnr.html. Accessed 25 May 2018.

[30] Investopedia. What does a negative correlation coefficient mean? https://www.investopedia.com/ask/answers/041015/w

hat-does-negative-correlation-coefficient-mean.asp. Accessed 25 April 2019.
[31] Investopedia. Correlation Coefficient. https://www.investopedia.com/terms/c/correlationcoefficient.asp. Accessed 25 May 2018.
[32] Abtoy A, Aknin N, Sbihi B, El Moussaoui A, El Kadiri KE. Towards a framework for a validated content management on the collaborative Web: Blogs case. International Journal of Computer Science Issues. 2011; 8(3):96-104.

Taqiyah Khadijah Ghazali is a Ph.D student at School of Computing, College of Arts and Sciences, Universiti Utara Malaysia. Her research interests include, Biometric Fingerprint, Biometric Encryption and Lightweight Encryption. Currently she is working on her research in Lightweight Encryption for Biometric Fingerprint Template Protection. She received her Bachelor of Information Technology in Computer E-Commerce from Malaysia Institute of Information Technology, Universiti Kuala Lumpur and Master of Science in Information Technology from Universiti Utara Malaysia.
Email: taqiyah_khadijah@ahsgs.uum.edu.my

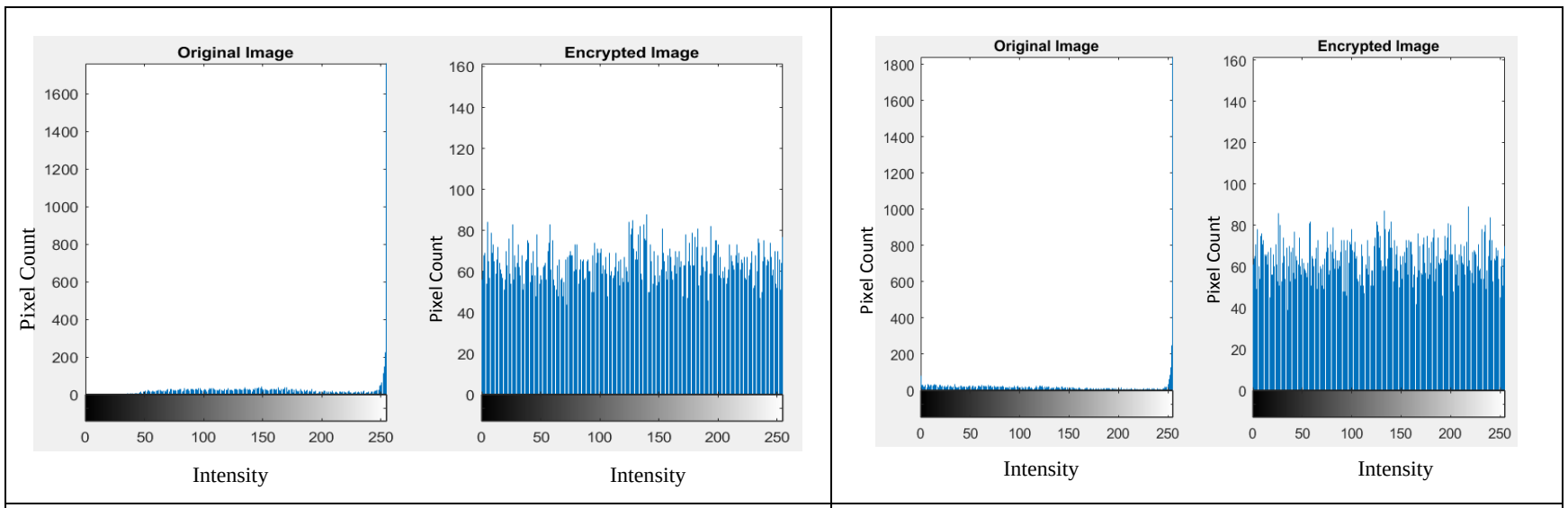
Nur Haryani Zakaria received her PhD in Computing Science from Newcastle University, United Kingdom. She is currently a Senior Lecturer at School of Computing, College of Arts and Sciences, and also Deputy Dean of Awang Had Salleh Graduate School, Universiti Utara Malaysia. Her research interests include Usable Security, Information Security, Network Security, Password Compliance and Single Sign-On. She received her Bachelor of Information Technology from Universiti Utara Malaysia and Master of Science in Computer Science (Information Security) from Universiti Teknologi Malaysia.
Email: haryani@uum.edu.my

Table 1 PSNR value between encrypted and original image

Image	**PSNR** (DB)	Image	PSNR (DB)	Image	PSNR (DB)	Image	PSNR (DB)	Image	PSNR (DB)
Fingerprint 1	5.5923	Fingerprint 17	5.2189	Fingerprint 33	5.0092	Fingerprint 49	5.2236	Fingerprint 65	5.4996
Fingerprint 2	5.3641	Fingerprint 18	5.2644	Fingerprint 34	5.7594	Fingerprint 50	4.9848	Fingerprint 66	5.0113
Fingerprint 3	5.2455	Fingerprint 19	5.2571	Fingerprint 35	5.2484	Fingerprint 51	5.8104	Fingerprint 67	5.5186
Fingerprint 4	5.4486	Fingerprint 20	5.0073	Fingerprint 36	5.3431	Fingerprint 52	5.4366	Fingerprint 68	5.4027
Fingerprint 5	5.3986	Fingerprint 21	5.7727	Fingerprint 37	5.2963	Fingerprint 53	5.4091	Fingerprint 69	5.4154
Fingerprint 6	5.0404	Fingerprint 22	5.3514	Fingerprint 38	5.1676	Fingerprint 54	5.5645	Fingerprint 70	5.1477
Fingerprint 7	5.2416	Fingerprint 23	5.4908	Fingerprint 39	5.6732	Fingerprint 55	5.0978	Fingerprint 71	5.0665
Fingerprint 8	5.1387	Fingerprint 24	5.1269	Fingerprint 40	5.8191	Fingerprint 56	5.7203	Fingerprint 72	5.4473
Fingerprint 9	5.2826	Fingerprint 25	5.3488	Fingerprint 41	5.1944	Fingerprint 57	5.1952	Fingerprint 73	5.5608
Fingerprint 10	5.2119	Fingerprint 26	5.4223	Fingerprint 42	5.7341	Fingerprint 58	5.1123	Fingerprint 74	5.5522
Fingerprint 11	5.3271	Fingerprint 27	5.2802	Fingerprint 43	5.2468	Fingerprint 59	5.4056	Fingerprint 75	5.4811
Fingerprint 12	5.0632	Fingerprint 28	5.0389	Fingerprint 44	5.4447	Fingerprint 60	5.5620	Fingerprint 76	5.5511
Fingerprint 13	5.5900	Fingerprint 29	5.8172	Fingerprint 45	5.4120	Fingerprint 61	5.5916	Fingerprint 77	5.4212
Fingerprint 14	5.3880	Fingerprint 30	5.6099	Fingerprint 46	5.1587	Fingerprint 62	5.3575	Fingerprint 78	5.1932
Fingerprint 15	5.6111	Fingerprint 31	5.4091	Fingerprint 47	5.2896	Fingerprint 63	5.4234	Fingerprint 79	5.1777
Fingerprint 16	5.5982	Fingerprint 32	5.3642	Fingerprint 48	5.5923	Fingerprint 64	5.6602	Fingerprint 80	5.3865

Table 2 Correlation Coefficient value between encrypted and original image

Image	**Correlation coefficient**	Image	**Correlation coefficient**	Image	**Correlation coefficient**	Image	**Correlation coefficient**	Image	**Correlation coefficient**
Fingerprint 1	0.0049	Fingerprint 17	0.0033	Fingerprint 33	0.0118	Fingerprint 49	0.0048	Fingerprint 65	-0.0058
Fingerprint 2	0.0090	Fingerprint 18	-0.0054	Fingerprint 34	0.0169	Fingerprint 50	-0.0033	Fingerprint 66	-0.0125
Fingerprint 3	0.0117	Fingerprint 19	0.0093	Fingerprint 35	0.0011	Fingerprint 51	-0.0033	Fingerprint 67	-0.0008
Fingerprint 4	0.0128	Fingerprint 20	-0.0011	Fingerprint 36	0.0027	Fingerprint 52	0.0040	Fingerprint 68	-0.0026
Fingerprint 5	0.0036	Fingerprint 21	0.0020	Fingerprint 37	0.0089	Fingerprint 53	0.0051	Fingerprint 69	0.0103
Fingerprint 6	0.0073	Fingerprint 22	0.0068	Fingerprint 38	0.0171	Fingerprint 54	0.0153	Fingerprint 70	-0.0062
Fingerprint 7	0.0020	Fingerprint 23	0.0063	Fingerprint 39	0.0214	Fingerprint 55	0.0006	Fingerprint 71	-0.0065
Fingerprint 8	0.0142	Fingerprint 24	0.0179	Fingerprint 40	0.0168	Fingerprint 56	-0.0076	Fingerprint 72	0.0082
Fingerprint 9	0.0181	Fingerprint 25	-0.0025	Fingerprint 41	-0.0008	Fingerprint 57	0.0052	Fingerprint 73	0.0045
Fingerprint 10	-0.0043	Fingerprint 26	-0.0039	Fingerprint 42	0.0162	Fingerprint 58	-0.0026	Fingerprint 74	0.0020
Fingerprint 11	0.0060	Fingerprint 27	0.0014	Fingerprint 43	-0.0095	Fingerprint 59	0.0218	Fingerprint 75	0.0052
Fingerprint 12	0.0137	Fingerprint 28	0.0052	Fingerprint 44	0.0153	Fingerprint 60	0.0039	Fingerprint 76	0.0023
Fingerprint 13	-0.0058	Fingerprint 29	0.0082	Fingerprint 45	0.0102	Fingerprint 61	0.0096	Fingerprint 77	0.0102
Fingerprint 14	0.0008	Fingerprint 30	-0.0019	Fingerprint 46	-0.0041	Fingerprint 62	-0.0061	Fingerprint 78	-0.0005
Fingerprint 15	0.0039	Fingerprint 31	0.0069	Fingerprint 47	0.0133	Fingerprint 63	0.0196	Fingerprint 79	-0.0077
Fingerprint 16	-0.0052	Fingerprint 32	0.0020	Fingerprint 48	0.0013	Fingerprint 64	-0.0004	Fingerprint 80	0.0079



(a) Fingerprint 1 **(b) Fingerprint 2**

Figure 6 Examples of histogram of original