ESTEEM Academic Journal
Vol. 13, December 2017, 118-128

Modified Shielding Function for Multi-biometric Authentication and Template Protection

Abayomi Jegede[1,2], Nur Izura Udzir[1] , Azizol Abdullah[1] and Ramlan Mahmod[1]
[1]*Faculty of Computer Science and Information Technology,Universiti Putra Malaysia, 43400 UPM Serdang, Selangor, Malaysia*
[2]*Department of Computer Science, University of Jos, Bauchi Road, Plateau State, Nigeria*
**Corresponding author: abayomi.jegede@ymail.com*

ARTICLE HISTORY

Received
18 September 2017

Received in revised form
1 December 2017

Accepted
8 December 2017

ABSTRACT

Biometrics provides a secure means of authentication because it is difficult to copy, forge, or steal biometric modalities. However, unprotected biometric data can be used to violate the security of the authentication system and the privacy of legitimate users. This paper proposes and implements a modified shielding function which provides multi-biometric authentication, template security and user privacy simultaneously. Experimental results based on face and iris datasets obtained from CASIA Near Infra-Red face database and CASIA Iris database version 2 respectively show that the approach has good recognition accuracy (false rejection rate of 0.65% and false acceptance rate of 0.035%). Security analysis shows that the method provides better security (key length of 120 bits) and user privacy compared to previous approaches based on the generic shielding function.

Keywords: *authentication; biometric; privacy; security; shielding function.*

1. INTRODUCTION

Multi-biometric systems authenticate users based on two or more biometric modalities. These systems use a process known as fusion to combine inputs from multiple sources into a single unit [1]. Some practical implementations of multi-biometric systems verify the identity of users by combining iris and palm-print [2], image and voice data [3], and face and iris [4]. The fusion of two or more biometric modalities generally provides improved recognition than when the modalities are applied individually. However, this does not exempt multi-biometric systems from issues related to template security and user privacy [5]. Such issues including the possibility of using reverse engineering can be used to reveal individual images in an unprotected multi-biometric image created using sensor (or image) level fusion. For instance, an attacker can also obtain the individual feature vectors comprising a multi-biometric feature data from a stolen or compromised template. In addition, impostors can spoof the matching scores of the sub-systems of a multi-biometric system based on matching score level fusion. To further exemplify, an intruder may fool the authentication system by altering the rule used for decision level fusion. Biometric cryptosystems or template protection schemes are used to overcome security and privacy challenges associated with the use of biometrics as a means of authentication. A biometric cryptosystem associates secret information with a biometric data before it is stored in the database. This makes it difficult for an intruder to obtain the original biometric data without knowing the secret information used to secure it. Template protection

p-ISSN 1675-7939; e-ISSN 2289-4934

systems also make it possible to revoke, update or replace biometric data in the event of loss or data corruption.

Shielding function [6] belongs to a class of biometric cryptosystems known as key binding schemes [7]. A previous implementation of shielding function was used to protect binary fingerprint templates which was obtained from Gabor filter [8]. The results from experiment show that this method has an EER (equal error rate) of 4.2% and a key length of 40 bits. A related work [9] used the shielding function to secure feature vectors which were extracted from fingerprint images using Wavelet Fourier-Mellin Transform. This method achieved sufficient key entropy and revealed only a small amount of information about users' biometrics. The helper data technique has also been used to secure binary face templates obtained by quantization of real-value feature vector [10]. Experimental results show that the scheme has good recognition accuracy (zero FAR – false acceptance rate and 0.8529% FRR - false rejection rate) and security (maximum key length of 63 bits). 3D face images were used to implement a helper data scheme in order to achieve better recognition performance [11]. This is because 3D face images generally contain a richer set of information than 2D face images. A two-factor authentication scheme known as biometric e-passport used the helper data technique to secure stored face templates [12]. Experimental results show that the approach has FARs of 0% and of 35% when applied to face images obtained from the FERET database. The application of the technique on Caltech database results in FAR and FRR of 0% and 35% respectively.

2. PROPOSED APPROACH

Previous implementations of the generic shielding function [9-11] extract real value features from fingerprints and face images. This requires the conversion of the real-value feature vectors to their binary equivalents using quantization and reliable bit selection. Quantization and reliable bit selection are complex and time-consuming processes which increase the overhead of the feature extraction phase. Quantization is prone to errors because actual feature values are replaced by either 0 or 1 depending on their relationship with the mean of all the feature set. This leads to loss of valuable information which may be useful in distinguishing one subject from the other. Reliable bit selection uses a subset of the quantized feature vector to represent a given biometric image. The bits which are discarded during the process may contain discriminating information about the images in the enrolment set. Thus bit selection is not only complex, error prone and time consuming, but also leads to loss of useful information. The generic shielding uses bit level error correction to handle background errors and natural intra-class variation among images of the same subject. This approach does not address burst error caused by an eyelash or specular reflection. Previous works produced biometric keys which fall short of the minimum requirement of 50 bits [12] and this makes them susceptible to brute-force attack. Moreover, none of these studies explored the application of the shielding function to multi-biometric modalities. This research proposes a modified shielding function which performs multi-biometric authentication and template protection simultaneously. It is a simple and efficient scheme which binary face and iris feature vectors are extracted directly from biometric images and does not require the additional pre-processing overhead of quantization and reliable bit selection. Extracted binary face and iris feature vectors are combined and modeled as the biometric modality of the same subject using a technique known as feature level fusion. The proposed scheme uses concatenated error correction method to address burst (block-level) and bit-level errors unlike the generic shielding function which handles only bit errors. The concatenated error correction method is able to handle errors in multiple blocks of data. It also addresses bit errors within each block. The goal is to provide good recognition accuracy as well as improved template security and user privacy.

3. METHODOLOGY

This section discusses the processes and procedures used for feature extraction, enrolment and authentication.

3.1 Feature Extraction

Binary feature vectors are extracted directly from pre-processed face images using rotation invariant neighbour-based invariant local binary pattern (RINLBP) technique. RINLBP improves on the generic local binary pattern [13] by addressing poor recognition performance due to image rotation. Rotation Invariant Neighbour-based LBP, $RINLBP_{R,P}$ is defined in equation 1 as

$$\sum_{p=0}^{P-1} s\left(g_p - g_{p+1}\right).2^{mod(p-\,d,P)} \qquad (1)$$

such that

$$s\left(g_p - g_{p+1}\right) = \begin{Bmatrix} 1 & g_p \geq g_{p+1} \\ 0 & g_p < g_{p+1} \end{Bmatrix} \qquad (2)$$

$$d = max\left|g_p - g_c\right| \qquad (3)$$

$$p \in (0,1 \ldots P-1)$$

(4)

where
g_p is gray scale value of a neighbour pixel
g_{p+1} is grayscale value of the next neighbour pixel
g_c is the value of the central pixel,
p is the index of the neighbour
R is the radius of the circular region
P is the number of sample points in the neighbour of the central pixel
d is the index of the neighbour pixel with the highest value, which defines the dominant direction in a neighbourhood.

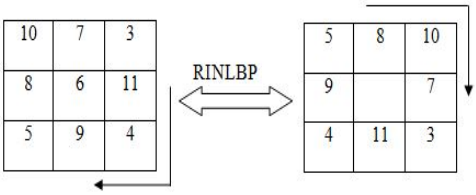

Figure 1: Rotation Invariant Neighbour-based LBP

The image in Figure 1 is rotated by through an angle of 90 degrees (90^0) but RINLBP obtained the same binary pattern from both the original image and the rotated image. This shows that image rotation does not affect the value of the binary pattern encoded by the RINLBP operator. Each face image is resized to 16×8 before applying the RINLBP in order to obtain a 1,024-bit binary representation of the image.

The first step in iris feature extraction is to break a 2D normalised iris image (see Figure 2) into a number of 1D signals.

Figure 2: Normalized Iris Image

The resultant 1D signals are then subjected to a convolution operation using 1D Gabor wavelets. A Log-Gabor filter is defined in equation 5 as

$$(f) = exp\left(\frac{-\left(log(f/f_0)\right)^2}{2\left(log(\sigma/f_0)\right)^2}\right) \tag{5}$$

where f_0 and σ are the frequency and the bandwidth of the filter respectively [14]. A given frequency value is quantized as 0 or 1 depending on the frequency response. This produces a binary template which represents the iris image. The total number of bits in the template is determined by multiplying 2 by the product of the angular resolution, the radial resolution, and the number of filters used.

A multi-biometric template is obtained by using feature level fusion to combine binary face and iris templates. This involves the transformation of the templates into row vectors and appending one at the end of the other. Feature concatenation, $FeatConc(x, y)$ is defined in equation 6 as

$$FeatConc(x, y) = Feat(x) \circ \quad Feat(y) \tag{6}$$

where
$Feat(x)$ is the binary face feature vector
$Feat(y)$ is the binary iris feature vector
$FeatConc(x, y)$ is the concatenated feature vector
°is the concatenation operator.

3.2 Enrollment and Authentication

The enrolment process involves the generation of a 120-bit random secret, S using multiplicative congruential random number generation method. The outer code (Reed-Solomon encoder) derives a 192-bit value from S and passes it to the inner code. The inner code uses the Hadamard encoder to obtain a 1,024-bit output by transforming each 6-bit block of the 192-bit value to 32 bits. The concatenated binary template extracted from the face and iris images and the 1,024-bit output of the Hadamard encoder are transformed into one dimensional column vectors. Helper data is computed by using an XOR operation to bind the 1,024-bit output of the Hadamard encoder with the 1,024-bit binary feature vector. The helper data and the hash value of the secret are stored in the database. The algorithm for enrolment is presented in Figure 3.

```
1. Generate a random secret, $S$
2. Perform concatenated encoding of $S$ as follows:
   Encode $S$ with Reed-Solomon encoder, $RS(S)$
   Encode the output of Reed-Solomon
    with Hadamard encoder $Had\ [RS(S)]$
3. Input reference biometric data, $X, Y$
4. Create a reference multibiometric template, $Z =$
$Featconc(X, Y)$
5. Compute helper data, $W = Had\ [RS(S)] \oplus Z$
6. Compute the hash of the secret, $hash(S)$
7. Save $W$ and $hash(S)$
```

Figure 3: Algorithm for Enrolment

During authentication, a 1,024-bit feature vector is extracted from a probe biometric image. A new secret S' (comprising 1,024 bits) is computed by performing XOR operation on the binary vector and the stored helper data. That is, $S' = W \oplus Z'$. The decoding process uses a concatenated approach in a way similar to encoding, but in a reverse direction. Hadamard decoder recovers a 192-bit value of the new secret from the computed 1,024-bit string, while Reed-Solomon decoder transforms the 192-bit value into 120 bits. A hash value of the recovered secret $hash(S')$ is computed and compared with the one stored in the database during enrolment. A successful authentication requires an exact match between the two hash values. The algorithm for authentication is presented in Figure 4.

```
1. Input probe biometric data, $X', Y'$
2. Create a probe multibiometric template, $Z' =$
$Featconc(X', Y')$
3. Retrieve helper data, $W$ from the database
4. Compute a new secret, $S' = W \oplus Z'$
5. Perform error correction decoding as follows:
   Decode $S'$ with Hadamard decoder, $Had(S')$
   Decode the output of Hadamard with Reed-Solomon
decoder, $RS[Had(S')]$
6. Compute the hash of the decoded secret, $hash\ (S')$
7. Compare $hash\ (S)$ with $hash(S')$
```

Figure 4: Algorithm for Authentication

4. RESULTS

The feasibility of the proposed approach is accessed using face and iris images obtained from CASIA Near Infra-Red face database and CASIA iris version 2 database respectively. The experiments were performed using 240 face images of 12 subjects (or classes), 240 iris images of 12 subjects and 480 multi-biometric (face and iris) images of 12 subjects. A multi-biometric modality was derived from the fusion of face and iris images. The concatenated feature vector was made up of 50% face bits and 50% iris bits. The two criteria used to measure the recognition accuracy of the system were of the false rejection rate (FRR) and false acceptance rate (FAR). False rejection was computed by comparing each of the images in the verification set with the corresponding images in the enrolment. The enrolment set for each subject contained 16 images while the verification set contained 4 images. The computation of FRR involved 64 comparisons for each class and a total of 768 comparisons for the entire dataset. The computation of false acceptance rate involved a one-to-one matching between the enrolment set for each class and the verification sets of the other classes. This resulted in 64∗11 or 704 comparisons for each class and a total of 12∗704 or 8,448 comparisons for the entire dataset.

4.1 Performance Evaluation

Table 1 shows the results of FRR based on the application of modified shielding function to face data. The total FRR for face (see Table 1) is 15.625% and the mean FRR is 1.302%. Classes 0008 and 0009 had high FRRs due to large intra-class variation among the biometric data of subjects in these classes. Other classes had very low FRRs (0%) because of the high degree of similarity among their biometric data. The results based on iris dataset show that the total FRR is 10.9375% and the mean FRR is 0.911%. Classes 0002, 0008 and 0012 have much higher FRRs compared to other classes. This is due to the high degree of dissimilarity among the biometric data of subjects in these classes. Other classes had 0% FRRs because of the high correlation among their biometric data. The total FRR and the mean FRR obtained using multi-biometric data were 7.875% and 0.65% respectively. All classes except 0001 and 0002 had 0% FRR. This implies that biometric data in Classes 0001 and 0002 had a high intra-class variation.

Table 1: Computation of FRR for Face, Iris and Multi-biometric Datasets

Class	No of Verification	False Rejection Rate (%)		
		Face	Iris	Multi-
0001	64	0	0	0
0002	64	0	6.25	1.625
0003	64	0	0	0
0004	64	0	0	0
0005	64	0	0	0
0006	64	0	0	0
0007	64	0	0	0
0008	64	14.0625	1.5625	0
0009	64	1.5625	0	0
0010	64	0	0	6.25
0011	64	0	0	0
0012	64	0	3.125	0

The FAR (see Table 2) is computed by verifying the enrolment set of each class or subject with the verification sets of the other classes.

Table 2: Computation of FAR for Face, Iris and Multi-biometric Datasets

Class	No of Verification	False Rejection Rate (%)		
		Face	Iris	Multi-
0001	11*64	0.142	0	0.142
0002	11*64	0.142	0.142	0.284
0003	11*64	0.142	0	0
0004	11*64	0.426	0	0
0005	11*64	0.	0	0
0006	11*64	0.142	0	0

0007	11*64	1.420	0	0
0008	11*64	0	0	0
0009	11*64	0	0	0
0010	11*64	1.420	0	0
0011	11*64	0	0	0
0012	11*64	0	0	0

The total FAR obtained for face data is 3.834% and the mean FRR is 0.32%. Classes 0007 and 0010 had the highest value of FAR because of the low inter-class variation between the biometric data of the class and those of the remaining classes. The classes with low FARs such as 0% and 0.1426% had high inter-class variation between their biometric data and those of the other classes. The results based on iris data show that Class 0002 has higher FAR (0.142%) than those of the remaining classes. This implies that classes with 0% had very little or no similarity between the data in their enrolment sets and those in the verification sets of the other classes. The total FAR for iris was 0.142% and the mean FAR was 0.012%. The results based on the multi-biometric dataset show that the total FAR is 0.426% while the mean FAR is 0.035%. False acceptance occurred in Classes 0001 and 0002 because of the collision among the biometric templates in these classes and those of Classes 0005, 0009 and 0012. The high inter-class distance made the FAR of the remaining classes to be 0%.

Figures 5 through 7 are the performance evaluation curves which depict the relationships between the FARs and FRRs for face, iris and multi-biometric modalities.

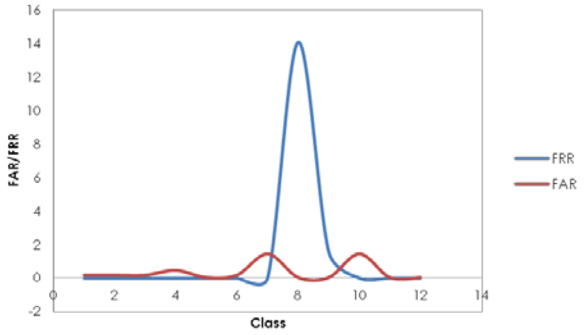

Figure 5: Performance Evaluation Curve for Modified Shielding Function (Face)

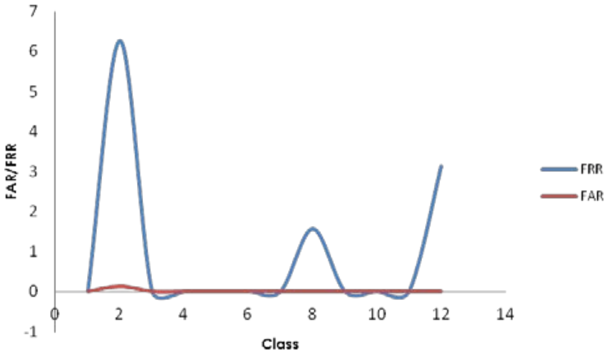

Figure 6: Performance Evaluation Curve for Modified Shielding Function (Iris)

p-ISSN 1675-7939; e-ISSN 2289-4934

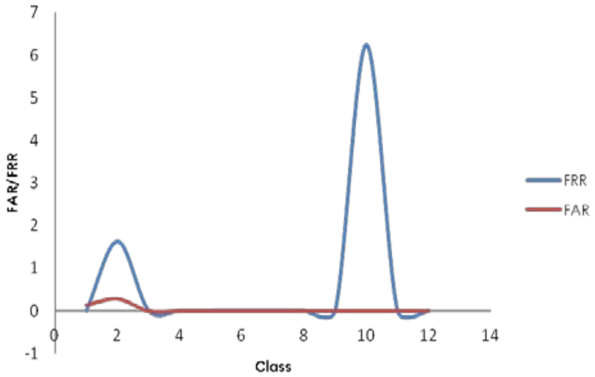

Figure 7: Performance Evaluation Curve for Modified Shielding Function (Multi-biometric)

The curves show that the FRRs are generally higher than (or at most equal to) the FARs for most of the classes. This implies that the proposed approach sacrifices user convenience for security.

4.2 Security Analysis

The security of the proposed scheme is analyzed to determine its resistance against guessing, key exhaustion, template sharing and cross matching attacks.

4.2.1 Key Length

Key length refers to the dimension of the extracted biometric key. The longer the length of a key, the less susceptible it is to guessing attack. Key length, $||K||$ is defined in equation 7 as

$$||K|| = m \times \left(\frac{n}{2^{m-1}}\right) - 2t \tag{7}$$

where n is the number of bits in the biometric data (1024 bits), m is the block size for Reed-Solomon encoding t is the block error correction capability of the RS decoder [15]. The respective values of n, m and t are 1024, 6 and 6.

$\therefore ||K|| = 6 \times \frac{1024}{2^{6-1}} - 2 * 6$ = 120 bits.

4.2.2 Key Space

Key space measures the level of resistance which the proposed scheme provides against brute force attack. Key space, k_s is defined in equation 8 as

$$k_s = 2^{||K||}$$

(8)

where

$||K||$ is the key length

$\therefore k_s = 2^{120} = 1.329 \times 10^{36}$.

4.2.3 Entropy

p-ISSN 1675-7939; e-ISSN 2289-4934

The entropy of a biometric key is used to determine its robustness to random guessing attack. It is measured in bits. Entropy, H is defined in equation 9 as

$$H = \log_2 N^K \tag{9}$$

where N is the symbol count and K is the key length [16]. The values of N and K are 2 and 120 respectively. Therefore $H = \log_2 2^{120}$ = 120 bits.

4.2.4 Probability of Correct Guess

This estimates the probability that an impostor will guess a biometric key correctly. It is computed as the inverse of key length. This is defined in equation 10 as

$$P_{guess} = {}^{1}/_{2^k} \tag{10}$$

where 2^k is the key space. $P_{guess} = {}^{1}/_{2^{120}}$ = 2^{-120} or 7.52×10^{-37}.

4.3 Summary of Findings

The results in Table 3 show that the proposed approach has better recognition accuracy for iris than it did for face. This is because of a little difference in the textural information in same person iris images while the irises of different persons had significant differences. Face modality, on the other hand, has large intra-class variation and low inter-class distance. These reasons also made the false acceptance rate for multi-biometric template to be higher than that of iris and lower than that of face. The table also shows that the approach provides equal level of security irrespective of the biometric modality used.

Table 3: Summary of Results

Modality	Performance (%)		Security Analysis			
	FRR	FAR	Key length	Key space	Entropy	Pr (guess)
Face	1.302	0.32	120	1.329×10^{36}	120	7.52×10^{-37}
Iris	0.911	0.012				
Multi-biometric	0.65	0.035				

The use of biometric features of long dimension results in a corresponding increase in the security of the system. However, this has an adverse effect on performance because of the increase in the overhead of error correction. The large key space (Pr =7.52×10^{-37}) and high entropy makes the approach less susceptible to random guessing and key exhaustion attacks. The large key space (2^{120} or 1.329×10^{36}) provides high level template renewability, diversity, revocability and resistance to cross matching attack.

Table 4: Comparison Between Our Approach and Previous Studies

Author	Modality	Technique	Performance (%)		Security Analysis		
			FRR	FAR	Key Length (Bits)	Key Space	Pr (Correct Guess)
Nandakumar & Jain, [17]	Fingerprint and Iris	Fuzzy Vault	98.2 (GAR)	0.01	49		
Kanade et al [18]	Left and Right Irises	Key Generation	0.18	0	147		
Geetika [5]	Iris, Retina and Fingervein	Fuzzy Vault			144		
Li et al [19]	Multiple Fingerprints	Hash + Fuzzy Vault	2.67	0	32		
Our approach	Face and Iris	Modified Shielding Function	0.65	0.0035	120	1.326×10^{36}	7.52×10^{-37}

It should be noted that one of the previous works [18] has better recognition performance, than the proposed approach. This is because it is based on left and right irises which are more reliable than face. However, the proposed approach provides higher level template security and user privacy. Only one of the previous studies [5] has better security than the proposed approach.

5. CONCLUSION

This paper proposed and implemented a multi-biometric authentication scheme which provides good recognition performance, template security and user privacy. The proposed scheme has a key length of 120 bits, which is higher than the minimum key of 50 bits required for secure biometric cryptosystems. The high level of resistance which the approach provides against security and privacy attacks will increase users' confidence in the authentication system.

ACKNOWLEDGMENTS

This material is based upon work supported by the Ministry of Higher Education Malaysia under Grant No. FRGS 08-01-15-1721FR.

REFERENCES

[1] M. Gudavalli, S.V. Raju, A.V. Babu and D.S. Kumar, “Multimodal biometrics - source, architecture and fusion techniques: an overview,” *2012 International Symposium on Biometrics and Security Technologies*, pp. 27-34, 2012.

[2] S. Hariprasath and T.N. Prabakar, “Multimodal biometric recognition using iris feature extraction and palmprint features,” *IEEE International Conference on Advances in Engineering, Science and Management*, pp. 174-179, 2012.

[3] T. Nishino, Y. Kajikawa and M. Muneyasu, “Multimodal person authentication system using features of utterance,” *IEEE International Symposium on Intelligent Signal Processing and Communication System*, pp. 43-47, 2012.

[4] A. Ratani and M. Tistarelli, “Robust multi-modal and multi-unit feature level fusion of face and iris biometrics,” *Lecture Notes in Computer Science*, vol. 5558, pp. 960-969, 2009.

[5] M.K. Geetika, “Multimodal-based fuzzy vault using iris, retina and fingervein,” *Fourth Internatioal Conference on Computing, Communication and Networking Technologies*, pp. 1-6, 2013.

[6] J.P. Linnartz and P. Tuyls, “New shielding functions to enhance privacy and prevent misuse of biometric templates”. *Lecture Notes in Computer Science*, vol. 2688, pp. 393-402, 2003.

[7] C. Rathgeb, A. Uhl and P. Wild, “Iris-Biometrics: From Segmentation to Template Security,” In *S. Jajodia, (ed.) Advances in Information Security*, Springer Science + Business Media LCC, 2013.

[8] P. Tuyls, A.H.M. Akkermans, T.A.M. Kavenaar, G.J. Schrijen, A.M. Bazen and R.N.J. Veldhuis, “Practical biometric authentication with template protection,” *Lecture Notes in Computer Science*, vol. 3546, pp. 436-446, 2005.

[9] L. Huixian, W. Man, P. Liaojun and Z. Weidong, “Key binding based on biometric shielding functions,”.*2009 5th International Conference on Information Assurance and Security*, pp. 19-22, 2009.

[10] H. Lu, K. Martin, F. Bui, K.N. Plataniotis and D. Hatzinakos, “Face recognition with biometric encryption for privacy enhancing self exclusion,” *16th International Conference on Digital and Signal Processing*, 2009.

[11] E.J.C. Kelkeboom, B. Gokberk, T.A.M. Kevenaar and A.H.M. Akkermans, "3D face: biometric template protection for 3D face recognition,” *Lecture Notes in Computer Science*, vol. 4642, pp. 566-573, 2007.

[12] M.V.D. Veen, T. Kavenaar, G.J Schrijen, T.A.H. Akkermans and F. Zuo, “Face biometrics with renewable templates,” *Proceedings of SPIE*, vol. 6072, pp. 1-12, 2006.

[13] T. Ojala, M. Pietikainen and T. Maenpaa, ”Multiresolution gray-scale and rotation invariant texture classification with local binary patterns,” *IEEE Transaction on Pattern Analysis and Machine Intelligence*, vol. 24 (7), pp. 971-987, 2002.

[14] D.J. Field, “Relations between the Statistics of Natural Images and the Response Properties of Cortical Cells”. *Journal of Optical Society of America*, vol. 4 (12), pp. 2379-2394, 1987.

[15] F. Hao, R. Anderson and J. Daugman, “Combining cryptography with biometrics effectively,” *IEEE Transaction on Computer*, vol. 55, no. 9, pp. 1081-1088, 2006.

[16] C.E. Shannon, “A mathematical theory of communication,” *Bell Systems Technical Journal*, vol. 27 (3), pp. 379-423, 1948.

[17] K. Nandakumar and A.K. Jain, “Multi-biometric template security using fuzzy vault,” *2nd International Conference on Biometrics: Theory, Application and Systems*, 2008.

[18] S. Kanade, D. Petrovska-Delecretaz and B. Dorizzi, “Multi-biometrics based cryptographic key generation scheme,” *3rd International Conference on Biometrics: Theory, Applications and Systems*, 2009.

[19] C. Li, J. Hu, J. Pieprzyk and W. Susilo, “A new biocryptosystem-oriented security analysis framework and implementation of multi-biometric cryptosystems based on decision level fusion,” *IEEE Transaction on Information Forensics and Security*, vol. 10 (6), pp. 1193-1206, 2015.

p-ISSN 1675-7939; e-ISSN 2289-4934