International Journal of Engineering & Technology, 7 (4) (2018) 2609-2613

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET
doi: 10.14419/ijet.v7i4.11485
Research paper



Multi biometric Template Protection using Hybrid Technique

G. Karthi [1] *, M. Ezhilarasan [2]

[1] Research Scholar, Department of Computer Science and Engineering, Pondicherry Engineering College, Puducherry, India
[2] Department of Information Technology, Pondicherry Engineering College, Puducherry, India
**Corresponding author E-mail:karthi.govindharaju@gmail.com*

Abstract

Recently, multi-biometrics system has been the important identification system for providing authentication mechanism. In this pa-per, the multi-biometric recognition system uses multiple traits (face, iris and fingerprint) for authentication. The features are extracted from the traits and feature level fusion technique is applied to the individual features traits to form a fused feature. Protection of these biometrics features against various attacks points is an important concern for authentication process. One such attack is the modification of stored template, which largely affects the performance of biometric recognition system. This paper addresses this concern, by apply-ing template protection algorithm to the biometric features. An improved hybrid template protection algorithm is proposed to protect the biometric template.The experimental results show that the proposed algorithm works better than the existing algorithms available. The proposed algorithm provides better protection to the template. Further, attacks are performed on the proposed system which provide strong resistant against the attacks.

Keywords: *Template Protection; Biometric Hashing; Pin; Multimodal Biometrics; Uni-modal Biometrics and Authentication.*

1. Introduction

Authentication is an act of providing information to get authorized to access the resources. The conventional authentication system uses information like password/pin to authorize the individual. The conventional system suffers from stealing and guessing the information (password/pin). The biometric system which avoids the problem of conventional system is recently used for authentication. The biometric system uses traits like palm-print, fingerprint, iris, face etc. as information for authentication. The biometric system which uses single trait for authentication is known as uni-biometric system. Further, multi-biometrics system is used for authentication to get better performance for personal authentication system. The multi-biometrics relies on multiple sources of information. The disadvantages of uni-modal biometric system are as follows:

Noise in sensed data: The sensed data from sensor can have noise due to improper maintenance of sensors or due to sensor defectiveness. For example, accumulation of residual remains on a fingerprint sensor can result in sensing noisy fingerprint image. Non-universality: Every individual in the target population has to posses the trait that can be used for recognition. For example, according to National Institute of Standards and Technology (NIST) has reported that it is not possible to obtain a good quality fingerprint from approximately two percent of the population.

Lack of individuality: Features extracted from different individuals can be quite similar. For example, facial features of father and son are similar due to genetic factors.

Lack of invariant representation: The biometric data acquired from a user can't match the same users template during verification due to improper presentation of biometric trait to the sensor. This is known as intra-class variation. For example, changes in pose and expression when the user stands in front of a camera.

Susceptibility to circumvention: There always a possibility that the biometric trait can be spoofed to circumvent the biometric system. For example, a fake finger, a copy of signature, a face masks.

Motivation for Multimodal biometric system

- To have choice of biometric modality for authentication based on the application we use.
- To increase population coverage by reducing the failure to enroll rate. For example Failure To Enroll (FTE) for iris is approximately 7%
- To enhance performance of the biometric system.

In this paper, the multi-biometric system is employed for authentication. Multi-biometric system refers to two or more traits for a verification or identification system. Multi-biometric system potentially plays a vital role in wide range of security applications like banking login, credit card transactions, resources access and login privileges. Multi-biometric system overcomes the issues of noisy data, non-universality, intra class variations, interclass similarity etc. faced by the uni-modal biometric system. The performance measures of the biometric system include False Acceptance Rate (FAR), Genuine Acceptance Rate (GAR), and False Rejection Rate (FRR). The multi-biometric system uses multiple information for personal identification, in order to improve the performance compared to the uni-modal biometric system.

The multi-biometric system could be categories as multiple sensors with an individual trait, multiple instances of an individual trait, multiple algorithms applied on an individual trait, multiple samples from a single senor, multiple traits and hybrid system. Various multi-biometrics scenarios are as follows.

Various sensors- single trait: Different sensors are used to capture the information of the individual trait. Normally more than two sensors are used to capture the information. During acquisition, if the information capture from one sensor is not proper, so the same information acquired from other sensor is used.

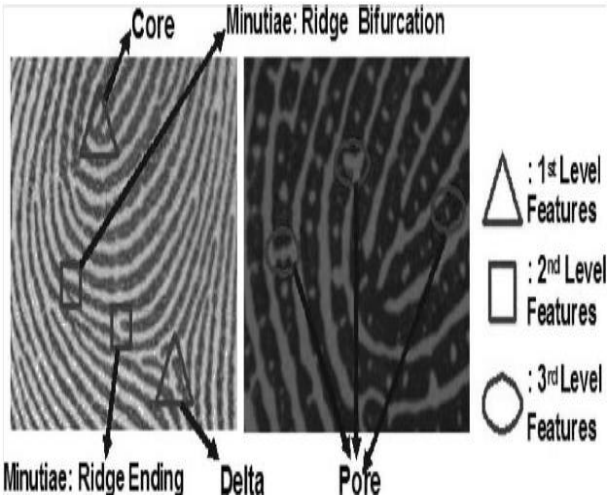
Copyright © 2018 G. Karthi, M. Ezhilarasan. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Multiple instances – single trait: Multiple instances of the same biometric trait is used to extract the feature for authentication. For instance, index finger and thumb of an individual are used for authentication process.
Multiple algorithms – single trait: Multiple algorithms are used for feature extraction, matching process etc. for the same biometric trait. For instance, multiple matching algorithms may be applied for single biometric trait to get better results.
Multiple samples – Single trait: Multiple samples of the same biometric trait is captured using single sensor. For instance, multiple sample of the index finger is taken for feature extraction.
Multiple traits: Multiple traits of an individual are used for authentication and it is also referred as multimodal biometrics. For example, fingerprint and face may be used for authenticating an individual identity.
Hybrid system: These systems work with more than one combination of above said scenario for the recognition process. For instance, the recognition system uses multiple algorithms with multiple samples.
In this paper, multiple trait scenario is used which uses fingerprint, face and iris for recognition process. These traits are fused to get combined feature set before matching process. The feature level fusion method is used which combines the features of multiple traits. The feature level fusion combines the features obtained from different biometric modalities together to get combined feature set.

1.1. Fingerprint

Fingerprint biometric is the most predominantly used biometric modality to identify the individual. The fingerprint is basically the combination of ridges and valleys pattern. The fingerprint features could be classified as level1, level2 and level3 features as shown in Fig. 1(a). Level 1 feature is the global features of the fingerprint such as singular points, orientation and ridge frequency. Level 1 features are mainly used for categorization rather than recognition as shown in figure. The level 2 features are minutiae points like ridge ending and bifurcation of ridge as shown in Fig. 1(b) and the level 3 features are finer details of the fingerprint features related to the ridges such as ridge width, ridge contours, sweat pores and incipient ridges. Level 3 features provide more accurate and finer data for robust fingerprint recognition.

(A)



(B)

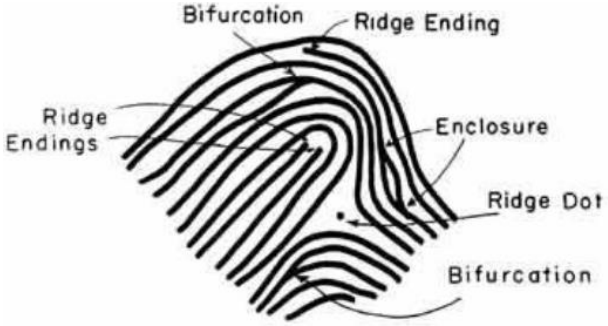


Fig. 1: Fingerprint Features A) All Three Levels of Feature B) Level [2] Features.

Among these level [3] features, pores are predominantly used and reliable feature for recognition.

1.2. Face

Face recognition is probably the most common biometric features used by humans to recognize one another. The applications of facial recognition range from a static, to a dynamic, uncontrolled face identification in a cluttered background. The most popular approaches to face recognition are based on either (i) the location and shape of facial attributes, such as the eyes, eyebrows, nose, lips, and chin and their spatial relationships, or (ii) the overall (global) analysis of the face image that represents a face as a weighted combination of a number of canonical faces. Face biometric is easily acceptable trait for the users. Limitation is, in recognizing face images captured from two different views, under different illumination conditions, and at different times is very difficult.

1.3. Iris

Iris is the most important biometric trait used for identifying the individual identity. Iris recognition requires pre-processing before extracting features from iris image. The iris pre-processing includes segmentation and normalization. After the pre-processing phase, the features are extracted from the iris image. In the segmentation process, the region between pupil and sclera is isolation from the iris image using segmentation algorithm. In this project, circular Hough transform algorithm is used to segment the iris image. In the segmentation phase, the noise and light illumination which are added during enrollment phase are removed. The Hough transform is the most popular segmentation algorithm which is used to determine any image using geometrical objects like line, circle and other shapes. Here, a circular Hough transform is applied to the iris image as follows:

$$r^2 = (x - a)^2 + (y - b)^2 \quad (1)$$

Where r is the radius of the circle and a, b are the coordinates points of the center. The x, y are the coordinates points on the circle given in the equation 2 and 3.

$$x = a + r\cos\theta (2)$$

$$y = b + r\sin\theta (3)$$

The circular Hough transform is computed by drawing circles with a given radius. The radius can be defined by minimum radius r_{min} to maximum radius denoted as r_{max}. For every drawn circle using the radius, the coordinates points x and y of the circle will be incremented by 1 until it reaches the maximum radius of the circle. For each radius tested, the coordinates which has the highest peak values are the most likely the radius.
Iris segmentation algorithm works as follows:

Input: Iris image I, radius r_{min} and r_{max}, Pupil center points c_{px}, c_{py} and pupil radius p_r. Search window of the image S × S.
Output: Segmented image.

1) $M_{diff} \leftarrow 0$, the maximum change in the coordinate's values.
2) for all points $c_x, c_y \varepsilon$ S × S do
3) $prev_{sum} \leftarrow 0, flag \leftarrow 0$
4) for $r = r_{min}$ to r_{max} do
5) $c_{sum} \leftarrow 0$, current summation value
6) for all θ do
7) $c_{sum} \leftarrow c_{sum} + I(c_x - r\sin\theta, c_y + r\cos\theta)$
8) end for
9) $D_{sum} \leftarrow c_{sum} - prev_{sum}$
10) $prev_{sum} \leftarrow c_{sum}$
11) if $D_{sum} > M_{diff}$ and flag $\neq 0$ then
12) $c_{ix} \leftarrow c_x, c_{iy} \leftarrow c_y, i_r \leftarrow r$; Updating the parameters
13) end if
14) $flag = 1$
15) end for
16) end for

The organizations of the papers is as follows, the first section gives the introduction of the work, the section two covers the related works done and the section three discuss about the proposed algorithms needed for template protection. The evaluation parameters for the algorithms are defined in the section four. The section five gives the experimental results and finally conclusion of the work.

2. Literature survey

In this section, various works on multi-biometric systems, fusion techniques and template protection algorithm are studied. In [1, 2] employs a multi-biometric system which uses face and fingerprint as trait. In this system feature, level fusion technique is applied and the results show that the multi-biometric system gives better results than the uni-modal biometric system. Ross et al [3] discuss about various fusion techniques at various levels namely sensor, feature, matching and decision. Ross et al [4] proposes a feature level fusion techniques using face and hand features. Zion et al [5] uses face and gait as features for multi-biometric system and fusion of traits are done at feature level and also various works [6-9] done in multi-biometric system which uses face and gait.

The template protection algorithm could be categories as key binding and key generating algorithms. Effective combination of fuzzy extractor with cryptographic key is proposed by Yang et al [10]. Here, the delaunay triangulation based fuzzy extractor is used to mitigate biometric uncertainty. Herder et al [11], proposed a stateless cryptographically secure Physical Unclonable Function (PUF) which mitigates attacks against PUF via tampering. Moreover, they describe the proof of the computational security and stateless construction of template. Chen et al [12] proposed a effective optional multi-biometric cryptosystem combined with fuzzy extractor with a random key to improve the performance of the system compared to the uni-biometric cryptosystem. A stable key generation method is proposed by Taniguchi et al [13]. This method utilizes the fuzzy extractor along with the given PUF and produces the stable key for cryptographic authentication.

Connie et al [14] proposed the salting technique for palmprint. In their work, the palmprint template is secured by applying bio-hash function. Nanni et al [15] proposed a bio-hash system using random subspace to create a reliable bio-hash code for face templates. Patrick [16] investigates the security of bio-hashing technique. Moreover, he proves that unlinkability and irreversibility decides the security of the bio-hashing not the statistical analysis. Yang et al [17] in their work describes a machine learning hash based approach for the biometric template protection. Punithavathi et al [18] proposes a new dynamic sectored random projection for biometric template protection. The method projects the iris template to a new domain using projection matrix.

3. Proposed system

The proposed system works with different modules from data acquisition to storing the biometric data to database. There are various modules to exercise in this proposed model as illustrated in Fig. 2.

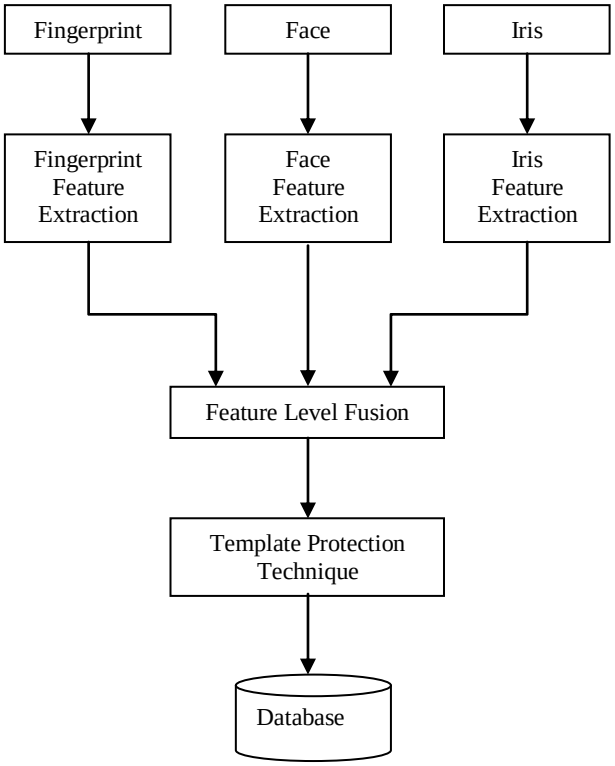


Fig. 2: Various Modules of Multi-Biometrics Template Protection.

3.1. Data acquisition module

The ability of biometric systems for providing high quality information at the very first stage by the use of sensors. The acquisition module interprets the biometric data into digital form. This component acquires the raw biometric data of an individual by scanning and reading. For example, In case of fingerprint recognition, an optical fingerprint sensor may be used to image the ridge pattern of the fingertip. The quality of raw data is influenced by the scanning or camera device that is used.

3.2. Feature extraction module

For further processing, the quality of the acquired raw data is first assessed. The raw data is subjected to signal enhancement algorithm to improve its quality. This data is then processed and a set of salient features extracted to represent the underlying trait. This feature set is stored in the database and is referred as template. For example, the position and orientation of minutia in a fingerprint image is extracted by the feature extraction module in finger print biometric system.

3.3. Feature level fusion module

In a biometric recognition system, the levels of fusion could be categories into the fusion before matching and the fusion after matching as shown in the figure. In this paper, fusion level fusion is applied to the biometric trait which falls in the fusion before matching category. In this feature level fusion module, the information/feature extracted from each biometric trait is concatenated to form a multi-biometrics feature template as shown in the Fig. 3. For fusion process, face, iris and fingerprint trait are taken.

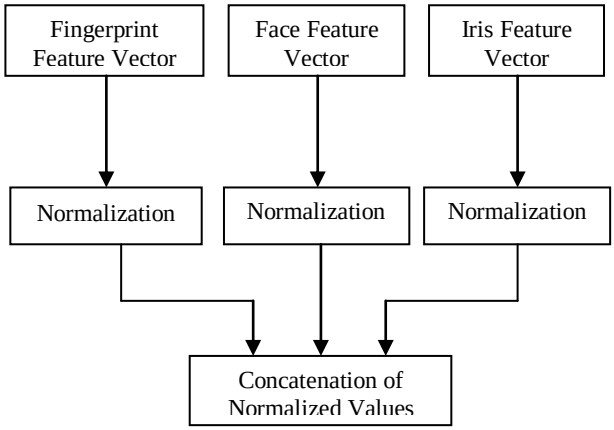


Fig. 3: Multi-Biometric Feature Level Fusion.

In feature level fusion, the features are extracted individually from different biometric traits/sensor by applying pre-processing methods and for these features vectors normalization techniques are applied. The purpose of normalization technique is to transform the individual feature vector into a common feature vector. The feature vector can be normalized using various normalization techniques such as min-max, z-score and mean-median. The min-max normalization technique is applied to normalize the individual feature vector and it is computed as follows:

$$x' = \frac{x - min(F_x)}{max(F_x) - min(F_x)} \quad (4)$$

Where x' and x denotes a feature vector before and after normalization. After normalization process the normalized values are concatenated using feature selection algorithm.

3.4. Template protection module

In this module based on the features, the biometric template protection algorithm is selected. Basically template protection algorithms are broadly classified into two categories namely biocrytosystem and cancellable biometrics. Here, a hybrid template protection algorithm is the combination of both the biocryptosystem and cancellable biometrics which are used for the fused feature set. The hybrid algorithm combines two different algorithms, one generates a key and another binds the key to the template.
The hybrid system uses key generation algorithm to generate the key and key binding algorithm bio-hashing to bind the key to the template as shown in Fig. 4.
Key Generation Module:
The key generation module is the process of producing a key from the biometric features. The features set used for the process is a fused feature set with normalized value. The following steps are performed in the key generation module:
Input: The Binary Fingerprint Vector (i.e.) BFV
Step 1: The input BFV is Xored with the Random Number generated by the Random Function.
Step 2: The output from step 1, is applied to two-process Hash function (SHA – 3) to produce 512-bit key k. In addition, BCH Encoder to produce a encoded output.
Step 3:The BCH Encoder output is Xored with the BFV to produce helper data S for the Key generation process.
Step 4: The helper data S, Random number R, and the Key k are stored in the Database for verification or identification.

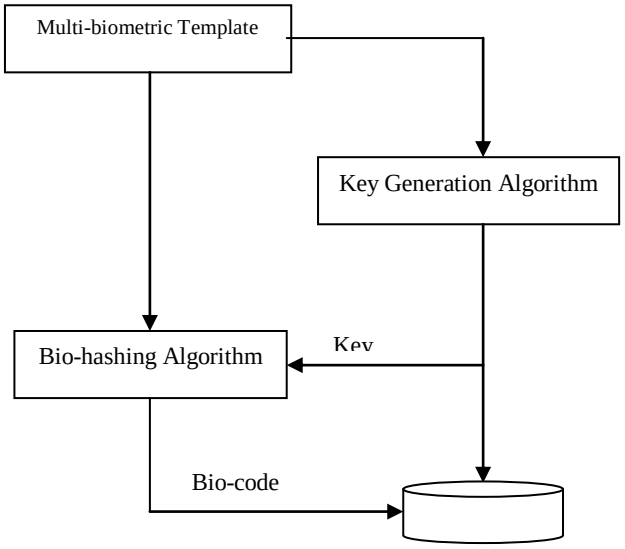


Fig. 4: Multi-Biometric Template Protection Process.

For the Key Regeneration process the following process is applied
Input: The Query Binary Fingerprint Vector (i.e.) QBFV
Step 1: The input QBFV is Xored with the helper data S,
Step 2: The output from step 1, is applied to BCH Decoder to produce a decoded output.
Step 3:The BCH decoder output is Xored with the BFV Random Number
Step 4: The output of the Step 3, is applied to the Hash function (SHA – 3) to produce 512 bit key
Step 5: The key is matched with the key, if match is found then it is authentic otherwise not.
The output of the key generation process is applied to the bio-hashing module which produces bio-code as the output. The bio-hashing algorithm binds a key to the biometric template. The key used here is obtained from the key generation algorithm. The following are the steps of bio-hashing algorithm.

1) Generate a random matrix R, based on a secret key or a secret seed K (key) obtained from the key generation algorithm.
2) Generate a sequence of real numbers to produce a set of Pseudo-random vectors p_i, where i = 1,……,m by applying Gram-Schmidt process.
3) Apply the Gram-Schmidt ortho-normalization procedure to transform the basis p_i, into an orthonormal set of vectors o_i, where i = one, 2, 3… m.
4) Compute the inner product between the biometric feature vector x and o_i, where i = 1,2,3,…..,m and compute bio-code b_i, where i = 1,2,3,…..,m.

The output bio-code is stored in the database along with the key as the transformed template.

4. Results and discussions

In this section, the evaluation of multi-biometric system is provided. The fingerprint, face and iris are the traits used for evaluation. The dataset taken for performance evaluation are FV2006 for fingerprint, ORL for face and CASIA for Iris. In FVC 2006, the DB3 dataset is used which has a total number of 680 images. For ORL face database 400 images of 40 users are taken. In case of Iris CASIA database a total of 600 images are taken for performance. To calculate the recognition rate of the system, FAR (false Acceptance Rate) and FRR (False Rejection Rate) is used.
The False Acceptance Rate (FAR) was identified by equation 5.

$$FAR = \frac{\sum_{n=1}^{N} FAR(n)}{N} \quad (5)$$

In addition, the Genuine Acceptance rate (GAR) was identified by equation 6,

$$FRR = \frac{\sum_{n=1}^{N} FRR(n)}{N} \quad (6)$$

Table 1: Performance of the Proposed System

Method	False Acceptance Rate	False Rejection Rate
Fingerprint Vector	2.57	1.73
Face Vector	4.56	6.75
Iris Vector	1.73	1.95
Fused Vector	1.05	1.25

The table 1 results show that the multi-biometric system performs better than the uni-modal biometric system. When compared with the face, the proposed system produces four times better results. When compared to the Iris the performance is slightly better.

5. Conclusion

From the experimental analysis, it is found that proposed hybrid algorithm provides security as well as performance to the biometric recognition system. The given biometric transformed template is protected with hybrid algorithm before storing it in the database. The hybrid approach enhances the security and privacy of the biometric system. In this paper, the proposed hybrid method takes the advantages of both cancelability and biocryptosystem. Here, the transformed template stored in the database is more secure since it does not store any helper data or any key for the authentication process. In all other template protection algorithm either the helper data or the token or key will be stored in the database. So, in the existing algorithms the transformed template can be compromised if either the helper data reveal some information about the template or if the key is stolen, the transformed template is not secured. Experimental results were conducted on two databases and the performance of the different approaches is tabulated with the metrics. The proposed system produces better results in performance as well as the security of the system. The performance of the system is improved by feature level fusion method.

References

[1] K.Sasidhar, Vijaya L Kakulapati, Kolikipogu Ramakrishna, K. KailasaRao, "Multimodal Biometric Systems - Study to Improve Accuracy and Performance", *International Journal of Computer Science & Engineering Survey (IJCSES)*, Vol.1, No.2, pp.54-61, November 2010.https://doi.org/10.5121/ijcses.2010.1205.

[2] A. Rattani, D.R. Kisku, M. Bicego, M. Tistarelli, "Robust Feature-Level Multibiometrics Classification", *In: Proc. of IEEE Biometric Consortium Conference, Biometrics Symposium*, pp. 1-6, 2006.

[3] A. Ross and A.K. Jain, "Information Fusion in Biometrics", *Pattern Recognition Letters*, vol. 24, No. 13, pp. 2115-2125, 2003. https://doi.org/10.1016/S0167-8655(03)00079-5.

[4] A. Ross and R. Govindarajan, "Feature Level Fusion Using Hand and Face Biometrics", *In:Proc. of SPIE Conference on Biometric Technology for Human Identification II*, Orlando, USA, pp. 196-204, March 2005. https://doi.org/10.1117/12.606093.

[5] X. Zhou and B. Bhanu, "Feature fusion of face and Gait for Human Recognition at a distance in video", *In: Proc. ofInternational Conference on Pattern Recognition*, Hongkong, pp. 529-532, 2006.

[6] Xianglei Xing, Kejun Wang, ZhuowenLv, "Fusion of Gait and Facial Features using Coupled Projections for People Identification at a Distance", *Signal Processing Letters IEEE*, vol. 22, pp. 2349-2353, 2015.https://doi.org/10.1109/LSP.2015.2481930.

[7] Martin Hofmann, Stephan M. Schmidt, A N. Rajagopalan, Gerhard Rigoll, "Combined face and gait recognition using alpha matte preprocessing", *In: Proc.* of *IAPR International Conference on Biometrics (ICB)*, pp. 390-395, 2012.https://doi.org/10.1109/ICB.2012.6199782.

[8] Qi-Shen Li, Zhi-Tian Lu, Dan-Dan Zhang, "Integration of Gait and Side Face for Human Recognition in Video", *Electronic Commerce and Security 2009. ISECS '09. Second International Symposium on*, vol. 2, pp. 65-69, 2009.

[9] MdWasiur Rahman, FatemaTuz Zohra, Marina L. Gavrilova, "Rank level fusion for kinect gait and face biometrie identification", *In Proc. ofIEEE Symposium Series onComputational Intelligence (SSCI)*, pp. 1-7, 2017.

[10] W. Yang, J. Hu and S. Wang,"A Delaunay Triangle-Based Fuzzy Extractor for Fingerprint Authentication", *In: Proc. of IEEE International Conference on Trust, Security and Privacy in Computing and Communications*, pp. 66-70, June 2012.

[11] Charles Herder and Ling Ren and Marten van Dijk and Meng-Day (Mandel) Yu and Srinivas Devadas, "A Stateless Cryptographically-Secure Physical Unclonable Function", *IEEE Transactions on Dependable and Secure Computing*, Vol. 14, No. 1, pp. 65-82, 2016.

[12] C. Chen, C.Wang, T. Yang, D. Lin, S.Wang and J. Hu,"Optional multi-biometric cryptosystem based on fuzzy extractor," *In: Proc of International Conference on Fuzzy Systems and Knowledge Discovery*, pp. 989-994, August 2014.

[13] M. Taniguchi, M. Shiozaki, H. Kubo and T. Fujino,"A stable key generation from PUF responses with a Fuzzy Extractor for cryptographic authentications," *In: Proc. of IEEE second Global Conference on Consumer Electronics*, pp. 525-527, October 2013.

[14] Tee Connie, Andrew Teoh, Michael Goh, David Ngo,"Palm Hashing: a novel approach for cancelable biometrics", *Information Processing Letters*, vol. 93, no. 1, pp. 1-5, January 2005.https://doi.org/10.1016/j.ipl.2004.09.014.

[15] L. Nanni, and A. Lumini,"Random subspace for an improved BioHashing for face authentication," Journal of Pattern Recognition Letters, vol. 29, no. 3, pp. 295- 300, February 2008.https://doi.org/10.1016/j.patrec.2007.10.005.

[16] P. Lacharme, "Revisiting the accuracy of the biohashing algorithm on fingerprints," *in IET Biometrics*, vol. 2, no. 3, pp. 130-133, September 2013.

[17] B. Yang and E. Martiri,"Using Honey Templates to Augment Hash Based Biometric Template Protection," IEEE 39th Annual Computer Software and Applications Conference, pp. 312-316 July 2015.

[18] P. Punithavathi and S. Goethe,"Dynamic sectored random projection for cancelable iris template," *In: Proc. of IEEE International Conference on Advances in Computing, Communications and Informatics (ICACCI)*, pp. 711-715, September 2016.