ISSN 2278-3091
Volume 9, No.4, July – August 2020
International Journal of Advanced Trends in Computer Science and Engineering
Available Online at http://www.warse.org/IJATCSE/static/pdf/file/ijatcse44942020.pdf
https://doi.org/10.30534/ijatcse/2020/44942020

A Novel Multimodal Biometric System using Face and FKP

Komal[1], Dr. Chander Kant[2]
[1]Research Scholar, DCSA, KUK, Haryana, India, thakrankomal07@gmail.com
[2]Assistant Professor, DCSA, KUK, Haryana, India, ckverma@rediffmail.com

ABSTRACT

Single modality based biometric authentication systems are suffered from some security issues such as inter-class variation, spoof attacks and so on. A multimodal biometrics system overcomes these security issues by fusion of two or more modalities of an individual. In this paper, a novel multimodal biometric system is proposed that integrates face and Finger Knuckle Print (FKP) at the feature level. An image transformation algorithm is applied on the face and FKP images at sensor level. Scale Invariant Feature Transform (SIFT) algorithm is used to extract the feature vector of the transformed images. These transformed feature vectors are used for further processing. KNN and SVM classifiers are used for classification at matching level. An image transformation technique secures the original biometric modalities of a person. The experimental work has been performed on public dataset with the help of MATLAB 2017b and result shows that proposed multimodal system outperform as compared with other.

Key words: Face, Feature level fusion, FKP, Image transformation, Security

1. INTRODUCTION

Now a day biometrics is getting more attention for automated individual identification because of the intrinsic properties of biometric features of an individual to be indentified or authenticated. It requires no password to remember and no ID card to carry along [1]. Generally, a biometric recognition system works by acquiring raw biometric data from various biometric characteristics (iris, face image, fingerprint, hand geometry, gait, signature *etc.*,) that are possessed by the person to be authenticated. Relevant feature set is extracted from the acquired data and it is compared against the templates stored in the database with the aim of identifying the person or to verify the claimed identity [2].

The biometric systems are vulnerable to numerous attacks which declines their security. Attacks on biometric systems have been analyzed and classified into eight types. Figure 1 shows a typical biometric system with these attack points[3].

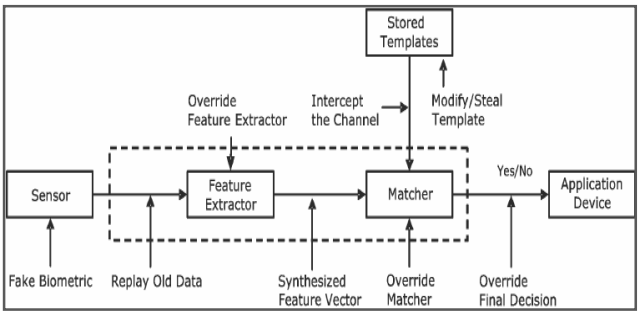

Figure 1: Attack points on biometric system

Type 1 attack is providing a fake biometric characteristic to the sensor module. Type 2 attack is submitting previously captured biometric data to the system. In type 3 attacks, the feature extraction module is forced to generate feature sets that are chosen by attacker. In type 4 attacks, genuine feature sets are replaced with those selected by the attacker. Type 5 attack is on the matcher module which is modified to produce a falsely high matching score. Type 6 attack is on the template database. In type 7 attacks, the transmission medium between template database and matcher module is attacked which results in modification of the send out templates. Type 8 attack is to override the result *i.e.*, accept or reject given by the decision module.

Among these attacks, the most damaging attack is on the template database [4]. Though biometrics provides an acceptable form of security but depending exclusively on that can be unsafe. Thus, it has necessitated the need to make templates secure by protecting the contents of the database with the help of some powerful techniques. Due to vulnerability to various types of attacks, biometrics is not safe as a primary authenticator [5]. If it is merged or used along with other security methods (such as steganography, watermarking, cancellable biometrics *etc.*,) then they will provide an extra layer of security to biometric information stored in databases [6].

Three pivotal parts of safety and security of biometric systems are authentication, verification, and identification. Authentication is most extreme significant since simply after verification, identification can be given. In verification mode, the questioned individual characteristics are compared with

the claimed individual characteristics available in template database where one to one matching is done. Though, in identification, the questioned individual characteristics are compared against all individual characteristics put away in template database where one to many matching is done. Identification is commonly utilized in the forensic offices for criminal record finding [7].

Rest of the paper is organized as follows: Section 2 discusses the related work for multimodal systems. Section 3 describes the methodology used in proposed work. Experimental work is demonstrated in section 4. Last section concludes the paper.

2. RELATED WORK

Imran et al. [8], proposed a multi-algorithm FKP verification scheme, which uses a combination of four different algorithms, LG (Log-Gabour) filters, PCA, LPP and LPQ (Local Phase Quantisation) to extract the features for FKP. Also numerous various techniques were used for feature normalisation: Median Absolute Deviation, Min-Max, Tangent-Estimator, and Z-Score. The investigations demonstrated that combining two algorithms delivered better result than a solitary algorithm, yet combining three algorithms doesn't give satisfactory results. It concludes that the chosen fusion method is the most important factor rather than the combination of two or three algorithms.

Long thai and hung [9], proposed a system that integrates face and fingerprint. ZM feature extraction and RBF neural networks (RBFNN) classification techniques is used. ZM technique is much more reliable than other techniques. An experimental result shows that proposed system is far better than unimodal systems.

Hossain and Chetty [10], proposed a multimodal system that integrate face and gait at feature level. PCA-LDA technique is used for feature extraction. For reducing the dimension of feature vectors, a new PDC-SSDR technique is used.

Almohhammad et al. [11], developed a multimodal system that combine face with gait modality to improve the performance of the system. facial acknowledgment has many problems because of ill-advised lighting conditions or low resolution camera, for example, a hallway, the recognition is a long way from exact. Research demonstrated that consolidating face recognition with gait recognition can improve the performance. Active Lines among Face Landmark Points (ALFLP) and Active Horizontal Levels (AHL) techniques are used for facial and gait feature extraction.

Kishu et al. [12], developed a multimodal authentication system for face and palm-print. Proposed system utilized isomorphic chart and K-medoids clustering for the face and palm-print. The system extracts key points highlighted by SIFT feature extraction algorithm and isolates these key points into clusters. An isomorphic chart is made corresponding to the clusters. Different graphs are made for face and palm-print. At later, these graphs are fused into one and then matching process is done.

Huang et al. [13], developed a multimodal system which comprises of palmprint and FKP. This plan utilizes a different strategy for the extraction of palmprint features called Monogenic Binary Coding (MBC). Two feature extraction algorithms SIFT and Finite Ridgelet Transform (FRIT) were used. The plan gives improved results than their unimodal and some multi-biometric modalities utilizing equivalent biometric characteristics.

Soruba Sree. and Radha [14], proposed a multimodal framework that utilized face and fingerprint biometric modalities. An image distortion algorithm is used for changing the original biometric modalities. After applying distortion, improve the quality of an image by pre-processing technique. The Crossing Number (CN) concept is used to extract features points from fingerprint and the Local Binary Pattern (LBP) algorithms are utilized to extract the facial features. Feature vectors of both modalities are fused at feature level. Fuzzy vault is added with the help of duplicate values which is containing a confidential key to open and lock the framework to give extra security to the proposed work. Both the techniques image distortion and Fuzzy vault goes about as an extra layer of security in proposed modal.

Hamd and Mohammed [15], developed a multi-modal system that integrates face and iris. The wavelet transform is used in feature extraction to generate a compact feature vector length of 128 bits; this technique reduces the computational time. The new called Phase-based Gabor Fisher Classifier (PBGFC) technique is used in facial feature extraction; this technique uses 16 Gabor filters, i.e. each filter has 2 scales and 8 orientations. This technique made very compact facial feature vector. Experiments are done on CASIA and ORL datasets for iris and face respectively. The results show that our multimodal biometric system achieves higher accuracy than both single biometric approaches and the other existing multi-biometric systems based on iris and face.

Abdellatef et. al [16], proposed a large number of multi-biometric framework which were based on different fusion strategies, cancellable biometrics and other Face recognition techniques. Also different region based and hybrid techniques were used. All the above techniques used the CNNs to extract the deep features called DFs from the biometric traits. The fusion technique helps to collaborate with the deep features to reach about a discriminative or different facial descriptor. In the region-based technique, DFs are extracted using various facial traits at different regions. Cancellable feature is provided with the help of bio-convolving method in the

framework. Multi-biometric method trains multiple CNNs with the help of different traits. The last hybrid features technique uses the advantage of both the hand crafted and deep-learned features to reach to a more efficient output. Also, a much more reliable and efficient architecture of the CNN is proposed.

3. METHODOLOGY

3.1 Image Transformation Algorithm

In this proposed work, image transformation algorithm is applied on captured images at sensor level. Transformation algorithm is based on changing the pixels locations in original input image. Figure 2 shows the sample of original and transformed image. Steps used in image transformation algorithm are as follows:-

step 1. Capture the original image of user.
step 2. Set the two locations for interchanging indices.
let
idx_0 = 150:190; idy_0 = 150:190;
idx_1 = 210:250; idy_1 = 210:250;
step 3. Move these pixels
let
$T_0 = I(idx_0, idy_0, :)$;
$T_1 = I(idx_1, idy_1, :)$;
step 4. Replace the pixels location.
$I(idx_0, idy_0, :) = T_1$;
$I(idx_1, idy_1, :) = T_0$;
step 5. Draw the transformed image after changing pixel locations.

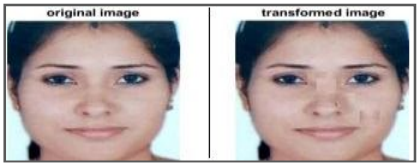

Figure 2: Sample of original image and transformed image

3.2 SIFT Based Feature Extraction Process

The main design of SIFT algorithm is to extract features from images to achieve reliable matching among the images. The SIFT feature extraction process can be described with the following steps shown in Figure 3.

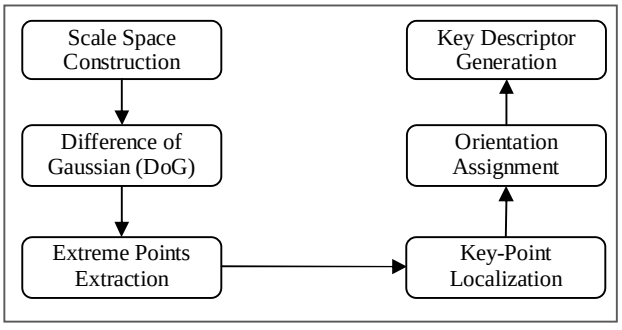

Figure 3: SIFT feature extraction

Lowe et al. [17] described the whole process of feature extraction by SIFT. The Initial step of SIFT algorithm is to build the scale space representation. Gaussian scale space of an input image can be acquired by convolving the image with bit by bit raised Gaussian changes. The Difference of Gaussian (DoG) is resolved based on the Gaussian scale space, by deducting adjoining image scales. Every pixel is compared with neighbouring pixels in the same level as well as lower or higher levels. Key points are found by considering whether the pixel is most extreme or least of every single neighbouring pixel. The locations which are unstable and low contrast along edges are discarded. Figure 4 & 5 shows the sample of selected transformed images with key points mapped onto it.

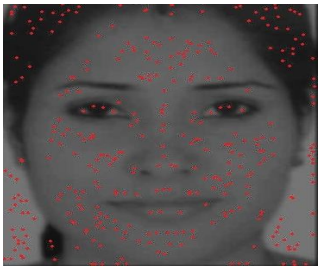

Figure 4: Key points mapped onto sample of transformed face image

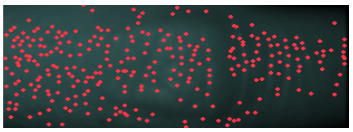

Figure 5: Key points mapped onto sample of transformed FKP image

Orientation is assigned to each of the resultant key points and obtains the feature vectors from the resultant key points. Whole region of the image is divided into 4×4 local regions to obtain the SIFT descriptor. Find out the histograms of gradient orientations for each region. Finally concatenate these histograms and normalized it to unit feature vector.

3.3 Fusion at Feature Level

Suppose individual feature vectors of face and FKP are F_{Face} = $\{p_1, p_2, p_3 \ldots\ldots p_m\}$ and F_{FKP} = $\{q_1, q_2, q_3 \ldots\ldots q_n\}$ respectively. These feature vectors may demonstrate significant variations in their range. Normalize function alter the mean and variation of original feature vectors and convert vectors into a common domain. Simple min-max normalization technique is used in this proposed system. Suppose F and F′ denote the original and normalized feature value respectively. Formula to compute F′ by min-max technique is shown below in equation 1[18]:-

$$F' = \frac{F - Min(F)}{Max(F) - Min(F)} \quad (1)$$

After normalization, $F'_{Face} = \{p'_1, p'_2, p'_3 \ldots\ldots p'_m\}$ and $F'_{FKP} = \{q'_1, q'_2, q'_3 \ldots\ldots q'_n\}$ becomes the new normalized feature vectors. New fused feature vector F_{Fused} is find out by concatenation of these two normalized feature vectors and resultant feature vector is represented as $F_{Fused} = \{p'_1, p'_2 \ldots p'_m, q'_1, q'_2 \ldots q'_n\}$. Now, fused feature vector (F_{Fused}) is used for further processing.

3.4 Matching Process

For the recognition, test data is compared with the template stored in the database. K Nearest Neighbour (KNN) and Support Vector Machine (SVM) are used to classify the images of the test data as genuine or imposter. If matching score (MS) of test data is greater than threshold (T) value, then it accept as genuine user else reject it as imposter.

3.5 Proposed Algorithms

Architecture of proposed work consists of two processes e.g, enrollment and authentication process as shown Figures 6 & 7. Proposed algorithms for both the processes are discussed below:

3.5.1 Algorithm for Enrollment Process:

step 1. Capture the face and FKP images with the help of suitable sensors

step 2. Apply transformation algorithm (as discussed in 3.1) on the captured images and obtained the transformed images.

step 3. Generate the transformed feature vector from both the modalities by using SIFT algorithm (as discussed in 3.2).

step 4. Perform the fusion of face and FKP feature vectors at feature level to obtain the secured fused feature vector.

step 5. Check the compatibility of both the feature vectors
   a) Normalization process
   b) Apply concatenation on normalized feature vectors.
   c) Store the fused feature vectors in template database.

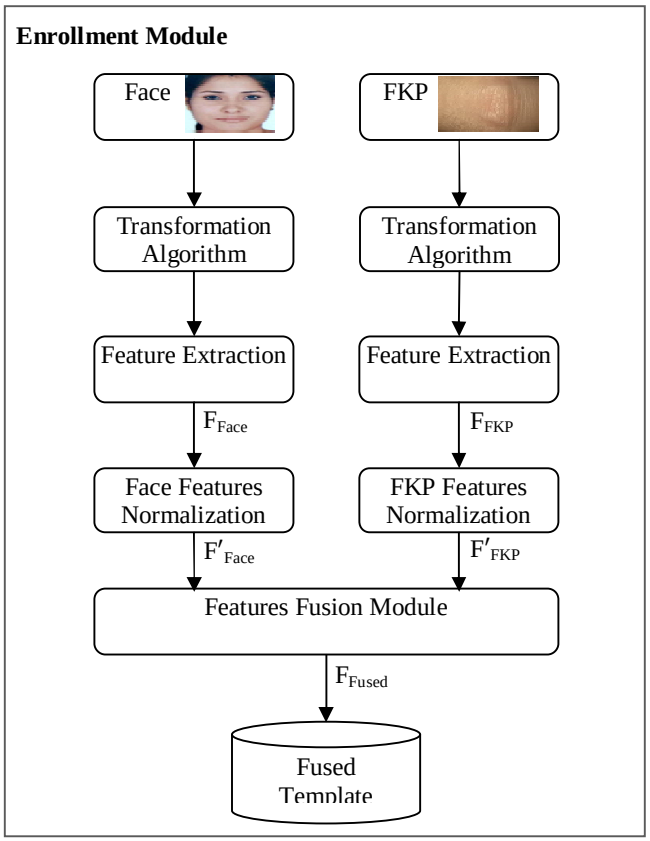

Figure 6: Enrollment Module of proposed multimodal system

3.5.2 Algorithm for Authentication Process:

step 1. Capture the face and FKP images with the help of suitable sensors

step 2. Apply elastic deformation algorithm (as discussed in section 3.1) on the captured images to obtain the transformed images.

step 3. Generate the transformed feature vector from transformed images corresponding to both modalities by using SIFT algorithm (as discussed in section 3.2).

step 4. Perform the fusion of face and FKP feature vectors at feature level to obtain the secured fused feature vector.

step 5. Check the compatibility of both the feature vector
   a) Normalization process
   b) Apply concatenation on normalized feature vectors.
   c) Perform matching of captured fused template with the template stored in database.

step 6. If (Matching score (MS) > Threshold (T)) then
   User is accepted as genuine user
   Else
   User is rejected as imposter

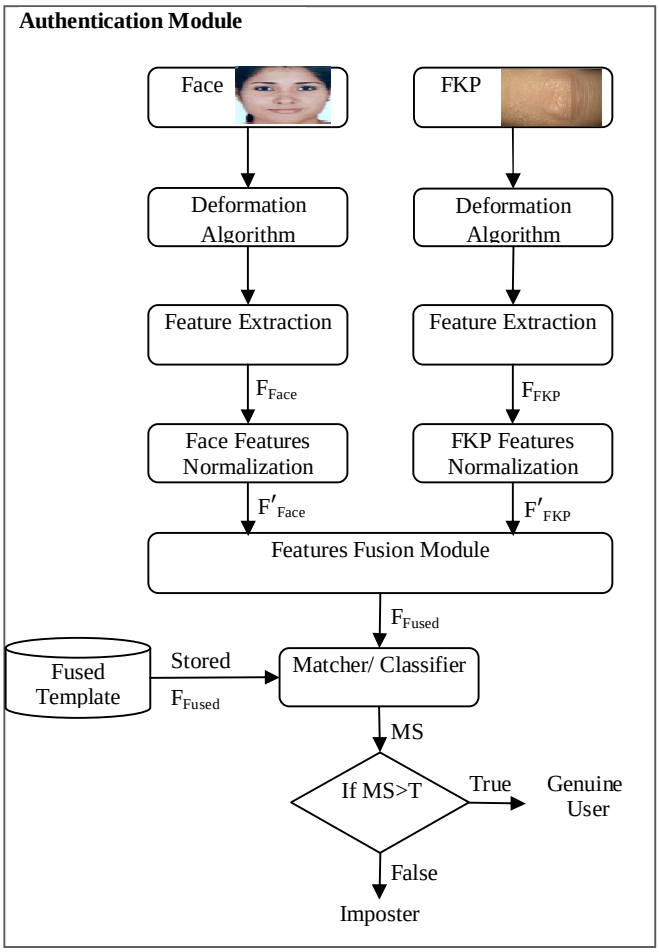

Figure 7: Authentication module of proposed multimodal system

4. EXPERIMENTAL RESULTS

4.1 Performance Metrics of Biometric Systems

The performance of the biometric verification system is estimated by measuring Genuine Acceptance Rate (GAR), False Acceptance Rate (FAR), and False Rejection Rate (FRR) [19]. Formula to calculate the FAR and FRR is given below:

$$FAR = \alpha / \beta \times 100$$

Where, α = Number of accepted imposter

β = Total number of imposter access

$$FRR = \gamma / \mu \times 100$$

Where, γ = Number of rejected clients

μ = Total number of client access

GAR is defined as a percentage of legitimate users accepted by the biometric system and formula to calculate GAR is as follows:

$$GAR = 1 - FRR$$

Equal error rate (EER) is the point where false acceptance rate and false rejection rate are optimal and formula to calculate EER is as follows:

$$EER = (FAR+FRR) / 2$$

The efficiency of the proposed method is computed by using the formula

$$Accuracy = 100 - (FAR+FRR) / 2$$

4.2 Result and Discussion

The proposed work has been done with publicly available Face and FKP datasets in MATLAB 2017b.. An image transformation algorithm is applied on the original images at sensor level to increase the security of the system. Transformed samples or images are used for further process. SIFT algorithm is used on transformed images to extract the transformed feature vectors.

The performance of proposed algorithm is evaluated with SVM and KNN classifier by measuring the error rates (FAR, FRR and GAR). Table 1 shows the performance parameters of unimodal and multimodal system with KNN and SVM classifier. By using KNN classifier, multimodal system (Face and FKP) yield highest GAR (99.76%) with lowest EER (0.26%) as compared to unimodal system with face and FKP. By using KNN classifier, multimodal system performs far better than unimodal systems. But as we compare both classifiers, KNN classifier outperforms SVM classifier.

Table 1: Performance parameters of unimodal and multimodal system with KNN and SVM classifier

Classifier	Modalities	FAR (%)	FRR (%)	EER (%)	GAR (%)	Accuracy (%)
KNN	Face	6.32	2.43	4.37	97.57	**95.63**
	FKP	3.51	2.13	2.82	97.87	**97.18**
	Face+FKP	0.28	0.24	0.26	99.76	**99.74**
SVM	Face	8.14	3.28	5.71	96.72	**94.29**
	FKP	4.02	2.52	3.27	97.48	**96.73**
	Face+FKP	0.45	0.36	0.41	99.64	**99.59**

Figure 9, 10, & 11 show the graph of GAR, FAR and FRR (%) of unimodal and multimodal systems. Multimodal system with KNN classifier has highest GAR with lowest FAR and FRR as compared with others. These graphs clearly show that multimodal system with KNN classifier outperforms SVM classifier.

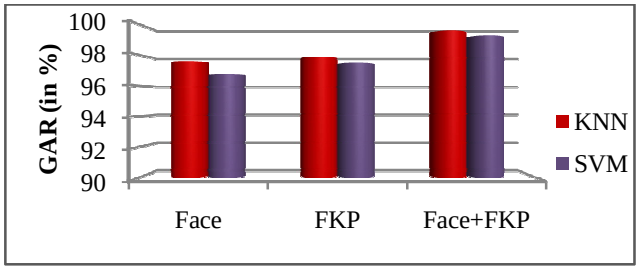

Figure 9: GAR (%) graph of unimodal and multimodal system

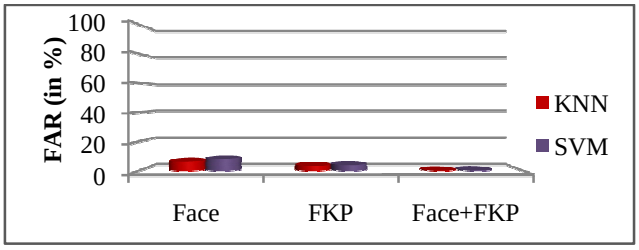

Figure 10: FAR (%) graph of unimodal and multimodal system

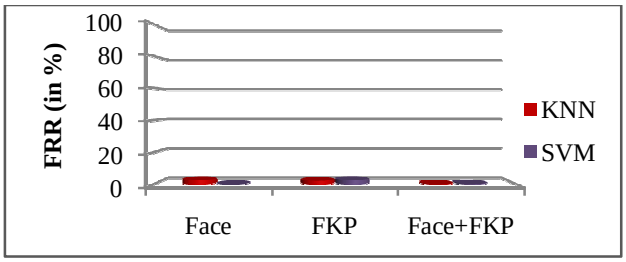

Figure 11: FRR (%) graph of unimodal and multimodal system

Accuracy of the biometric system is dependent on FAR (%) and FRR (%). Lowest the value of FAR and FRR, highest will be the accuracy of the system. Figure 12 shows the accuracy of unimodal and multimodal systems with SVM and KNN classifier.

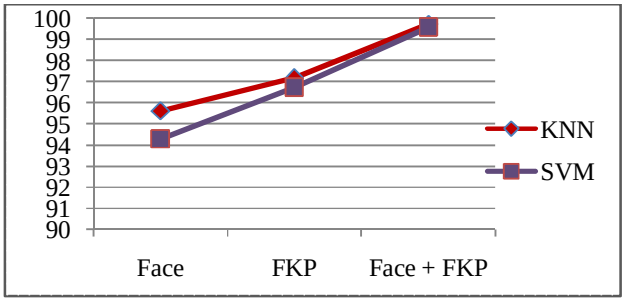

Figure 12: Accuracy (%) graph of unimodal and multimodal system

5. CONCLUSION

This paper presents a multimodal biometric system by integrating Face and Finger Knuckle Print (FKP) at the feature level. An image transformation algorithm is applied at sensor level to improve the security of system by transforming the original image into transformed image. Feature vector is extracted from the transformed image. This method of transforming an image is very simple and easy to implement. Performance of the proposed system is evaluated by using KNN and SVM classifier. Experimental result shows that proposed system outperform with KNN classifier as compared with other. Accuracy rate of proposed system is better than unimodal systems. Future work will be done on adaption of other security techniques e.g watermarking, steganography etc. to increase the security of multimodal biometric systems against spoof attacks.

REFERENCES

[1]. N. Ratha, J. Connell and R. Bolle, “Enhancing security and privacy in biometrics-based authentication systems”, IBM System Journal, vol. 40, no. 3, pp. 614-634, 2001. https://doi.org/10.1147/sj.403.0614

[2]. A. K. Jain, A. Ross and S. Prabhakar, “An Introduction to Biometric Recognition”, IEEE Trans. Circuits and Systems for Video Technology, vol. 14, No. 1 pp. 4-20, Jan 2004.

[3]. N. K. Ratha, J. H. Connell and R. M. Bolle, “An Analysis of Minutiae Matching Strength”, In Proceedings of the 3rd AVBPA, Halmstad, Sweden, pp. 223-228, June 2001. https://doi.org/10.1007/3-540-45344-X_32

[4]. W. Yang, S. Wang, J. Hu, G. Zheng and C. Valli, “A Fingerprint and Finger-vein Based Cancelable Multi-Biometric System”, Pattern Recognition, Vol. 78, pp. 242 – 251, Jun 2018.

[5]. N. Srivastava, “Fusion Levels in Multimodal Biometric Systems – A Review”, International Journal of Innovative Research in Science, Engineering and Technology, Vol. 6, No. 5 pp. 8874–8878, May 2017.

[6]. L. R. Haddada, B. Dorizzi, N. E. B. Amara, “A Combined Watermarking Approach for Securing Biometric Data”, Signal Processing: Image Communication, Vol. 55, pp. 23-31, Jul 2017. https://doi.org/10.1016/j.image.2017.03.008

[7]. M. S. Vinay Kumar and R. Srikantaswamy, “Comparative Analysis of distinct Fusion levels in Multimodal Biometrics”, International Journal of Computer Applications, Vol. 4, pp. 1–4, Sep 2015.

[8]. M. Imran, H. AlMahafzah, and H. S. Sheshadri, ‘‘Multi-algorithm feature level fusion using finger knuckle print biometric,’’ in Computer Applications for Communication, Networking, and Digital Contents (Communications in Computer and Information Science), vol. 350, T.-H. Kim, D.-S. Ko, T. Vasilakos, A. Stoica, and J. Abawajy, Eds. Berlin, Germany: Springer, pp. 302–311, 2012.

[9]. T. B. Long, L. H. Thai, and T. Hanh, ‘‘Multimodal biometric person authentication using fingerprint, face features,’’ in PRICAI 2012: Trends in Artificial Intelligenc (Lecture Notes in Computer Science), vol. 7458, P. Anthony, M. Ishizuka, and D. Lukose, Eds. Berlin, Germany: Springer, pp. 613–624, Sep. 2012.

[10]. E. Hossain and G. Chetty, ‘‘Multimodal face-gait fusion for biometric person authentication,’’ in Proc. IFIP 9th Int. Conf. Embedded Ubiquitous Comput. (EUC), pp. 332–337, Oct. 2011. https://doi.org/10.1109/EUC.2011.52

[11]. M. S. Almohammad, G. I. Salama, and T. A. Mahmoud, ‘‘Human identification system based on feature level fusion using face and gait biometrics,’’ in Proc. Int. Conf. Eng. Technol. (ICET), pp. 1–5, Oct. 2012.

[12]. D.R. Kisku, P. Gupta, and J. K. Singh, “Feature Level Fusion of Face and Palmprint Biometrics by Isomorphic Graph-Based Improved K-Medoids Partitioning,” AST/UCMA/ISA/ACN 2010, LNCS 6059, pp. 70–81, 2010.

[13]. M. I. Ahmad, W. L. Woo, and S. Dlay, ‘‘Non-stationary feature fusion of face and palmprint multimodal

biometrics,'' Neurocomputing, vol. 177, pp. 49–61, Feb. 2016.
https://doi.org/10.1016/j.neucom.2015.11.003

[14]. S.R.Soruba Sree, Dr. N. Radha, "Cancellable Multimodal Biometric User Authentication System With Fuzzy Vault,**"** International Conference on Computer Communication and Informatics (*ICCCI* -2016), Coimbatore, INDIA, Jan. 07 – 09, 2016.

[15]. M. H. Hamd, M. Y. Mohammed, "Multimodal Biometric System based Face-Iris Feature Level Fusion," I.J. Modern Education and Computer Science, 5, pp. 1-9, 2019.
https://doi.org/10.5815/ijmecs.2019.05.01

[16]. E. Abdellatef, N. A. Ismail, S. Eldin S. E. Abd Elrahman, K. N. Ismail, M. Rihan5 and F. E. Abd El-Samie, "Cancelable fusion-based face recognition," Springer Science +Business Media, pp. 1-25, May 2019.

[17]. D.G Lowe. "Distinctive image features from scale-invariant keypoints". International Journal of Computer Vision, vol. 60, No. 2, pp. 91–110, 2004.

[18]. P. Mote and P.H. Zope, "Multimodal Biometric System using Gabor Filter," IJATCSE, vol. 1, no. 2, pp. 67-72, May-June 2012.

[19]. G. Amirthalingam and H. Thangavel, "Multi-Biometric Authentication Using Deep Learning Classifier for Securing of Healthcare Data," IJATCSE, vol. 8, no. 4, pp. 1340-1347, 2020.
https://doi.org/10.30534/ijatcse/2019/48842019