International Journal of Progressive Sciences and Technologies (IJPSAT)
ISSN: 2509-0119.

http://ijpsat.ijsht-journals.org
Vol. 28 No. 2 September 2021, pp.484-492

Comparative Analysis of Feature Level Fusion Bimodal Biometrics for Access Control

Adedeji O. T[1]*, Alo O.O.[2*], Akerele T. I[3*], Oguntoye J.P[4*], Makinde B.O[5*], Jooda J.O.[6*]

[1,2] Department of information Systems, Faculty of Computing and Informatics, Ladoke Akintola University of Technology (LAUTECH), Nigeria

[3]Department of Computer Science, Faculty of Computer Science, Southeast Missouri State University, USA

[4]Department of Computer Engineering, Faculty of Engineering and Technology, Ladoke Akintola University of Technology (LAUTECH), Nigeria

[5]Department of Computer Science, Faculty of Communication, Information and Technology (CIT), Osun State College of Technology, Esaoke

[6]Department of Computer Engineering, Igbajo Polytechnic, Igbajo,
Osun State. Nigeria.

Abstract—The increasing quest for dependable, robust and secure recognition systems led to combining two or more biometric modalities for improved performance of a biometric system. Bimodal biometric systems have proven to achieve obvious advantages over unimodal systems in various applications such as access control, surveillance, forensics, deduplication and border control etc. In this study, a comparative analysis of combination of three biometric trait at feature level of fusion was carried out. Face, fingerprint and iris images were acquired from LAUTECH biometric database. The bimodal setup consists of face-iris, face-fingerprint and iris-finger modalities. Principal Component Analysis (PCA) was employed for feature extraction, weighted sum technique was used to fuse the images at feature level while Support Vector Machine (SVM) was used for classification. Experimental result revealed that the bimodal biometric achieved an improved performance than the unimodal biometric. The performances of the bimodal systems indicated that combination of face and iris features achieved the best performance with FAR, FRR and accuracy of 0.00%, 1.42% and 99.00% at 38.15 seconds. Hence, a bimodal face-iris recognition system would produce a more reliable security surveillance system for access control than other combination compared in this study.

Keywords—Access Control, Bimodal Biometrics, Principal Component Analysis and Support Vector Machine.

I. Introduction

Access control is a security method that manages who can view or have access to computing resource and environment. It is a principal concept in security that limits risk to the businesses or association. The objective of access control is to limit the danger of unauthorized admittance to physical and intelligent systems (Gupta *et al.,* 2018). The use of biometrics for identification and ensuring information security has become a critical challenge in the information age (Ahmed *et al.,* 2021). Biometric recognition refers to the automatic recognition of persons based on their behavioral and biological characteristics such as fingerprint, face, palmprint, iris, palm/finger vein, iris, and voice (Jain *et al.,* 2016). It is regarded as a technology which does not identify people by either what they have or know but by who they are (Adetunji *et al.,* 2018).

The biometric recognition technology has played and will continue to play a significant role in everyday life role (De Keyser *et al.,* 2021). Biometric solutions have proven to achieve a clear-cut advantages over the use of tokens or passwords in various applications such as access control, surveillance, forensics, deduplication, border control etc. Unimodal and multimodal biometrics are the main types of biometric recognition systems. The unimodal system which uses a single biometric trait to recognize an individual are characterized with problems which includes noise in the sensed data, non-universality problems, vulnerability to spoofing attacks, intra-class, and inter-class similarity (Oloyede and Hancke, 2016; Alay and Al-Baity, 2020).

The problem associated with unimodal biometric system can be solve using multimodal biometric systems. Multibiometric systems collect evidence from more than one biometric trait (e.g., face, fingerprint, and iris) to recognize a person (Ross *et al.,* 2006, Elhoseny *et al.* 2015). The advantages of multimodal biometric systems over unimodal systems have led to its wide range of applications for secure recognition (Jain *et al.,* 2011). In a multibiometric system, information fusion can be implemented in four stages namely, the sensor stage, feature stage, score stage and decision stage. Feature level fusion is believed to consist of richer information about the raw biometric data compared to matching score or decision level fusion (Kulkarni and Namboodiri, 2014, Adedeji *et. al.,* 2019).

In view of the great performance of machine learning methods such as Principal Component Analysis (PCA) and Support Vector Machine (SVM) in various recognition tasks, this study aims to intensively investigate the use of the PCA and SVM techniques in recognizing a person from two combination of any of the three biometric traits: face, iris, and fingerprints. Performance evaluation of the bimodal combination of Iris-face, fingerprint-face and face-fingerprint biometric will be carried. PCA was used as feature extraction technique while SVM was employed for classification after fusion. This study seeks to know the best biometric trait combination for biometric authentication in access control. What informed the choice of face, iris, and fingerprint of a person in this study is that face is perhaps the most natural and, therefore, obvious individual recognition trait, while the unique and highly precise nature of recognition information contained in the iris makes it an effective option. Fingerprint is an essential biometric trait due to its uniqueness and invariant to every individual. The aforementioned limitations of poor performance imposed by unimodal system will be overcome by combining multiple sources of information for establishing the identity of a person. The specific objectives are:

i. To apply PCA for feature extraction of each biometric trait.

ii. To fuse the extracted features to achieve a bimodal scheme using the Weighted sum.

iii. To apply the Support vector machine for the classification of the fused features.

iv. To compare the performance of each biometric trait combinations based on accuracy, false-positive rate, false-negative rate, and computational time.

Next, section 2 showcases the detailed review of related works, section 3 depicts the research method while the results are given in section 4. Section 5 concludes the study and contains the recommendation for further studies.

II. Related Works

Kim *et al.,* (2012) proposed a multimodal biometric system that combines face and iris biometric. Support Vector Machine was used for classification. The experimental results show that the equal error rate for the proposed method is 0.131%, which is lower than that of face or iris recognition and other fusion methods.

Falohun *et al.* (2016) designed an access control system using bimodal biometrics. A door prototype was constructed with electric circuit design and an iris and fingerprint recognition software was developed using MATLAB. The application was interfaced with the door prototype. The developed system was tested widely with the pre-enrolled subjects as well as freshly introduced subjects for authentication. The design and construction were successfully achieved, that attained a more secured and foolproof access control system. Their work also emphasizes the uniqueness of bimodal biometrics in performance over the unimodal counterparts.

Adedeji *et al.* (2019) presented Clonal Selection Algorithm (CSA) for feature level fusion of multibiometric systems. Face, fingerprint and iris datasets were acquired from one hundred and fifty-four (154) randomly selected students and staff of Ladoke Akintola University of Technology (LAUTECH). The three (3) biometric traits were combined to achieve 3 bimodal biometric systems i.e. Iris-Fingerprint (IR-FI), Face-Iris (FA-IR) and Face-Fingerprint (FA-FI) biometric systems. Discrete Wavelet Transform (DWT) was used for feature extraction while fusion was performed at the feature selection phase using Clonal Selection Algorithm (CSA). Experiment result revealed that the bimodal combinations (IR-FI), (FA-IR) and (FA-FI) achieved an accuracy of 89.50%, 89.63% and 88.25% at 3.81s, 4.91s and 4.07s respectively.

Ammour, *et al.* (2020) proposed face–iris multimodal biometric identification system. The iris feature extraction was carried out using an efficient multi-resolution 2D Log-Gabor filter to capture textural information in different scales and orientations. On the other hand, the facial features were computed using the powerful method of singular spectrum analysis (SSA) in conjunction with the wavelet transform. The fusion process of relevant features from the two modalities were combined at a hybrid fusion level. The evaluation process was performed on a chimeric database and consists of Olivetti research laboratory (ORL) and face recognition technology (FERET) for face and Chinese academy of science institute of automation (CASIA) v3.0 iris image database (CASIA V3) interval for iris. Experimental results show the robustness of the proposed technique.

III. METHODOLOGY

The bimodal biometric system scheme proposed for identification is represented in figure 1. The functioning steps for the complete identification process are:

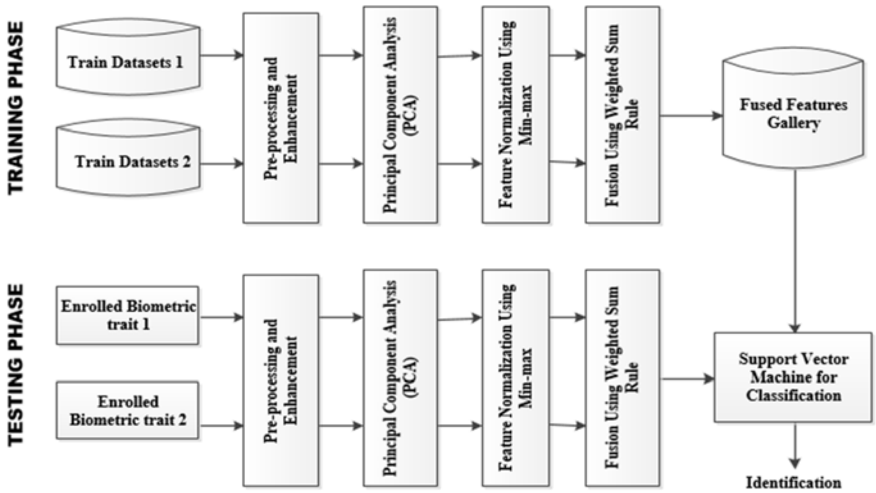

Figure 1: The Scheme of the bimodal biometric identification system

1. Acquisition of raw data from the biometric traits of the authentication subject (face, Iris, fingerprint);
2. Preprocessing of the acquired face, Iris and fingerprint datasets.
3. Extraction of feature of each biometric trait using PCA.
4. Normalization of extracted features using Min-max technique
5. Fusion of normalized features using weighted sum rule
6. Classification of fused features for identification using SVM technique.

3.1 Acquisition of raw data

The proposed systems were validated on a subset of LAUTECH Non-Chimeric Multimodal database. This database consists of 924 images each of faces, left and right eye, left and right thumbprints of 154 individuals taken in an uncontrolled condition. Each biometric trait contains five samples. For this study, 80 individuals were considered making a total of 480 images each for face, iris, and fingerprint database. The whole image database was randomly partitioned into training and testing set. For each of the subjects in each database, 3 images were randomly selected as training samples stored in training folders and the remaining 2 images as testing samples were stored in the testing folders.

3.2 Preprocessing of biometric traits

Various image processing techniques were used to enhance the captured images and their increase in the recognition rate. The quality of the obtained raw images might be low because the images can be blurred and noisy due to variations in environmental conditions, skin conditions, and acquisition devices. A set of tasks were applied to improve the clarity of the pattern structure of each image.

Pre-processing the Face datasets

Image normalization, de-nosing, filtering, histogram equalization, image resizing, and cropping were the operation performed on the face datasets.

Pre-processing the Iris datasets

The iris datasets were pre-processed by two-level segmentation technique combining Circular Hough Transform and Daugman's Integro-Differential Operator. The use of the operator was due to low contrast in the nature of the black eye´s irises used (Nigerian eyes). Its parameters are the centre coordinates x_c and y_c, and the radius r, which can define any circle according to equation (1).

$$x_c^2 + y_c^2 - r^2 = 0 \quad (1)$$

Equation (2) was used to detect eyelids, approximating the upper and lower eyelids with parabolic arcs.

$$\left(-(x - h_j)sin\Phi_j + (y - k_j)cos\Phi_j\right)^2 = a_j\left((x - h_j)cos\Phi_j + (y - k_j)sin\Phi_j\right) \quad (2)$$

Where a_j controls the curvature, (h_j, k_j) is the peak of the parabola and Φ is the angle of rotation relative to the x-axis. And because inner and outer iris boundaries are not concentric like the pupil, integro differential operator was performed around the pupil canter and the iris radius to find the iris canter according to equation (3).

$$max_{(r,x_0,y_0)} \left| G_\sigma(r) * \frac{\partial}{\partial r} \oint_{(r,x_0,y_0)} \frac{I(x,y)}{2\pi r} ds \right| \quad (3)$$

Where I(x, y) is the eye image, r is the radius to search for, $G_\sigma(r)$ is a Gaussian smoothing function, and s is the contour of the circle given by r, x_0, y_0. The operator searches for the circular path where there is maximum change in pixel values, by varying the radius and centre x and y position of the circular contour.

Pre-processing the Fingerprint datasets

The fingerprint images were converted to 8-bit gray image. A simple linear type of contrast stretching was applied to enhance the visual appearance of the image details. The dynamic range of pixels values were adjusted. This process was done using equation(4):

$$N(x,y) = \frac{N_{max} - N_{min}}{O_{max} - O_{min}} \left(O(x,y) - O_{min}\right) + N_{min} \quad (4)$$

A simple *mean smoothing filter* was used to reduce the noise and to integrate the white ROI. Mean filter of size 7x7, was applied four times to obtain an acceptable. Post- Processing which involves cleaning the gaps and pores, binarization and thinning was done.

3.3 Principal Component Analysis (PCA) Based feature extraction

PCA was employed to extract features from each of the pre-processed images. PCA compressed larger dimension into a set of lower dimensions, while retaining necessary information required for better classification. PCA is a mathematical tool used to extract principal components of original image data. These principal components may also be referred as Eigen images. The dimensionality reduction was achieved by transforming to a new set of variables, the principal components (PCs), which are uncorrelated, and are ordered so that the first few retain most of the variation present in all the original variables (Jolliffe, 2002). The mathematical concepts that were used for PCA are Standard Deviation, Variance, Covariance and Eigenvectors (Fadaei, and Sortrakul, 2014). This was employed to extract the facial features, fingerprint and iris regions features, given a set of N training samples of image $I_1, I_2, \ldots, I_N$. PCA algorithm is computed as follows:

1. Convert the set training Samples to row vectors $x_1, x_2, \ldots\ldots, x_N$
2. Compute the mean of the column vectors. The mean image of the training set is given as:

$$\mu = \frac{1}{N}\sum_{I=1}^{N} x_i \qquad (5)$$

3. Calculate the covariance matrix S

$$S = \frac{1}{N}\sum_{i=1}^{N} (x_i - \mu)\,(x_i - \mu)^T \qquad (6)$$

4. Compute the eigenvectors and eigenvalues of the covariance matrix S

$$S_{v_i} = \lambda_i v_i \qquad (7)$$

For i=1, 2, … N. Where v and λ are eigenvectors and eigenvalues respectively.

5. Select the eigenvectors or eigenfaces corresponding to the largest p eigenvalues.
6. Compute the projections or principal components Y

$$Y_I = \left[v_1, v_2, \ldots, v_p\right]^T (x_i - \mu) \qquad (8)$$

Where Y_i represent the feature vector of image I_i.

A feature vector of 1 × p dimension is obtained where $p <= N$ and N is the number of training set.

3.4 Feature Normalization

The features extracted by the PCA from each biometric trait was heterogeneous. The normalization of the images i.e., F'_{image} was achieved using Min-max. Min-max used because it retains distribution, sensitive to outliers and map the feature into common range. Normalization maps the raw biometric features to interval [0, 1] and retains the original distribution of the features. The normalization of the features of the biometric traits by the min-max rule are given by equation (9):

$$F'_{image} = \frac{F_{image} - \min\,(F_{image})}{\max\,(F_{image}) - \min\,(F_{image})} \qquad (9)$$

where F_{image} is the features extracted from each of the biometric trait, min (F_{image}) and max (F_{image}) are the minimum and maximum features for the trait.

3.5 Fusion at Feature-level using Weighted sum

Consider a multi-biometric system consisting of J modalities such that $k = 1,2, \ldots, J$ and $i = 1,2, \ldots, N$ where N is the number of probe samples of k modality. Let X_{ik} is the feature vector of the i^{th} sample for k^{th} modality and Z_i be the resulting feature vector after fusion for i^{th} sample. The approach used in this research work to obtain Z_i was weighted sum rule method.

$$Z_i = \sum_{k=1}^{j} w_k X_k \qquad (10)$$

$$where \sum_{k=1}^{j} w_k = 1$$

3.6 Classification of fused features using SVM

The fused features from the each of the bimodal combination were classified using SVM. The SVM classifier for the classification of the fused features was obtained using Equation (11). Values obtained from the combined biometric trait of both genuine and non-genuine users was used to determine a maximum margin hyper plane between the two classes.

$$f_{SVM}(Z_i) = W_t \varphi(Z_i) + b \tag{11}$$

Where W_t is the weight vector and φ is the mapping function used to map the input function to another dimension space. It was done for easy separation. The hyper plane was determined in such way that the distance from this hyper plane to nearest data points on each side called support vectors. SVM used the values of train images and using these values it was easy to classify the test images.

3.7 Performance Evaluation Metrics

The performance metrics considered in this study are False Acceptance Rate (FAR), False Rejection Rate (FRR), recognition accuracy and time. In a detection system, the following statistics are important: For enrolled users- **True Positives (TP)** and **False Negative (FN)**, for new users- **True Negative (TN)** and **False Positive (FP)**. **TP** represents the case that was positive and predicted as positive (persons are correctly identified) and **FP** means the case that was negative but predicted as positive (incorrect person identification). FAR, FRR and recognition accuracy were calculated using TP, FP, TN and FP as shown in equation 12, 13 and 14 respectively.

$$FAR = \frac{Wrongly\ accepted\ individuals}{Total\ number\ of\ wrong\ matching} = \frac{FP}{FP + TN} \tag{12}$$

$$FRR = \frac{Wrong\ rejected\ individuals}{Total\ number\ of\ correct\ matching} = \frac{FN}{FN + TP} \tag{13}$$

$$Accuracy(\%) = \left(100 - \left(FAR(\%) + FRR(\%)\right)/2\right) \tag{14}$$

IV. Experimental Results and Discussion

All implementations were executed on Windows 7 ultimate OS platform with Intel(R) Core (TM) i5-2540M CPU @ 2.60GHz and 6GB RAM, in which the performance of the proposed scheme is evaluated. The experimental results obtained for this research presented in Table 1. The biometric components face, iris and fingerprint features were extracted separately as unimodal system using PCA feature extraction methodology and then the fusion of these modalities is performed on different subsets of face, fingerprint, and iris image databases. The system was tested and evaluated in terms of recognition accuracy, FRR and FAR and computation time. All performance metrics were analyzed by using a square dimension pixel resolution 100 by 100 pixel.

Table 1: Summary of Experimental results obtained.

Biometric System	FAR (%)	FRR (%)	Accuracy (%)	Computation Time
Face Recognition	13.33	10.33	89.00	28.58
Iris Recognition	13.33	7.14	91.00	25.12
Fingerprint Recognition	16.67	11.42	87.00	23.94

Face-Iris Recognition	0.00	1.42	99.00	38.15
Face-Fingerprint Recognition	6.67	8.57	92.00	35.05
Iris- Fingerprint Recognition	6.67	4.28	95.00	32.54

The result obtainable from the table revealed that with the face biometric trait, the technique under study achieved a FAR, FRR and accuracy of 13.33%, 10.33% and 89.00% at 28.58 seconds while the corresponding values with Iris biometric trait were 13.33%, 7.14% and 91.00% at 25.12 seconds. Furthermore, with the fingerprint biometric trait, the technique under study achieved a FAR, FRR and accuracy of 16.67%, 11.42% and 87.00% at 23.94 seconds. Figure 2, depict the performance of each biometric trait based on recognition accuracy. The results depicts that each biometric trait has a unique performance for the same feature extraction and classification technique. This corroborates the findings of Bharadwaj et al. (2014) which postulate that face, iris and fingerprint biometric traits are of different quality and performance. Also, the findings depicts that the iris biometric trait has a better performance than the face and fingerprint biometric trait because the iris biometric has a more discriminating features for identification. This is also in line with the work of Adedeji et al., 2018 where iris biometric outperformed both finger and face biometric traits. The Face biometrics among others has the highest recognition time while the fingerprint had the least. This is because the face contains more features compared with iris and fingerprint.

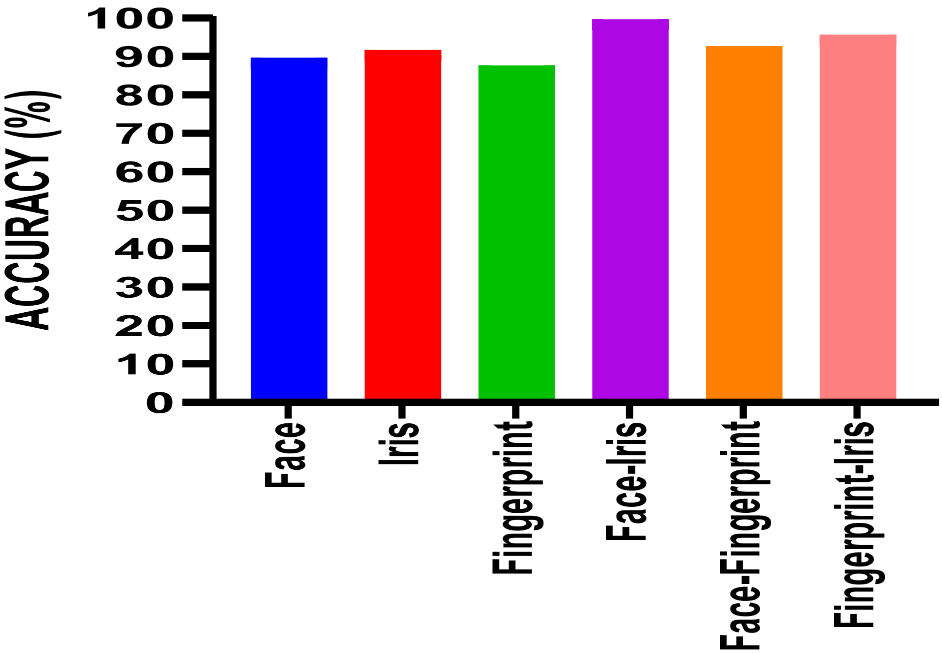

Figure 2: Performance of each biometric trait based on recognition accuracy.

Similarly, from Table 1, it was revealed that a bimodal biometric based on face and iris (Face-Iris) achieved a FAR, FRR and accuracy of 0.00%, 1.42% and 99.00% at 38.15 seconds while the corresponding values with bimodal biometric based on face and fingerprint (Face-fingerprint) were 6.67%, 8.57% and 92.00% at 35.05 seconds. Additionally, bimodal biometric based on iris and fingerprint (Iris-Fingerprint) achieved a FAR, FRR and accuracy of 6.67%, 4.28% and 95.00% at 32.54 seconds. The results obtainable in the table revealed that the bimodal biometric achieved an improved performance than the unimodal biometric. This implies that combining two or more modalities can improve the performance of a biometric system (Adedeji *et al.,* 2019). However, the bimodal biometric have an increased computation time due to the combination of features. This justifies the claims of Adetunji *et al.,* 2018 which stated that the more the features in the training sets the more the computation time.

The combination of face and iris features achieved the best performance. This may be because the face and iris biometric contains more discriminating features as postulated by Connaughton *et al.,* 2016 and Eskandari and Sharifi, 2017. In view of the results, the Face-Iris bimodal biometric is more accurate but with high computational cost. Also, it achieved minimal false acceptance rate (FAR) and false rejection rate (FAR) than other biometric sub-systems. This also corroborates the findings of Eskandari and Toygar, 2014. Furthermore, the results also revealed that the close bimodal biometric close to the Face-Iris biometric is the Finger-Iris biometric. This implies that among the trio of face, iris, and fingerprint biometric; the iris biometric seems to influence accurate performance. This is also evident in the work of Telgad, *et al.,* 2017 and Adedeji *et al.,* 2019. The outcome of the research shows that careful selection of biometric trait to combine for improved performance is highly essential. The combination of face and iris biometric trait would produce a more accurate security system.

V. Conclusion

In this work, comparative analysis of feature level fusion bimodal biometrics for access control was done to ascertain the biometric combination for improved performance. The experimental results obtained revealed that facial-iris biometric system gave the best performance in terms of recognition accuracy, FAR, FRR and computation time. In view of this, a facial-iris recognition system would produce a more reliable security surveillance system for access control than other combination compared in this study. The work also emphasizes the uniqueness of bimodal biometrics in performance over the unimodal counterparts. The proposed bimodal biometric model has contributed to existing works on assessments by integrating iris and face bimodal biometric to authenticate an individual. The work is exclusive as it can be employed in numerous enterprises to lessen and minimize impersonation. It is suggested that further study can be focused towards investigating the performance of the proposed framework on a huge database to establish the innumerable parameters like equal error rate, complexity of the system, user authentication cost, implementation cost, cost, true negative rate, etc. which are primarily the brain behind a result to endorse a validation model.

References

[1] Adedeji O. T., Falohun A. S., Alade O. M., Omidiora E. O., Olabiyisi S. O. 2018. Comparative Analysis of Face, Iris and Fingerprint Recognition Systems. *World Journal of Engineering Research and Technology* (WJERT). Vol. 4, No 4, pp. 160-167.

[2] Adedeji T. O., Falohun S. A., Alade M. O., Omidiora E. O., Olabiyisi S. O. 2019. Clonal Selection Algorithm for feature level fusion of multibiometric systems. *Anale. Seria Informatica.* Vol. 17, No 1, pp 69-75.

[3] Adedeji, O. T., Alade, O. M., Oguntoye, J. P., Awodoye, O. O. 2021. Comparative Analysis of Feature Selection Techniques for Fingerprint Recognition Based on Artificial Bee Colony and Teaching Learning Based Optimization. *LAUTECH Journal of Computing and Informatics*, Vol 2 No 1, pp 25-34.

[4] Adetunji, A. B., Oguntoye, J. P., Fenwa, O. D., Omidiora, E. O. 2018. Reducing the Computational Cost of SVM in Face Recognition Application Using Hybrid Cultural Algorithm. *IOSR Journal of Computer Engineering (IOSRJCE).* Vol 20, No 2, pp 76-85.

[5] Ahmed, D. M., Ameen, S. Y., Omar, N., Kak, S. F., Rashid, Z. N., Yasin, H. M., Ahmed, A. M. 2021. A State of Art for Survey of Combined Iris and Fingerprint Recognition Systems. *Asian Journal of Research in Computer Science*, pp 18-33.

[6] Alay, N., Al-Baity, H. H. 2020. Deep learning approach for multimodal biometric recognition system based on fusion of iris, face, and finger vein traits. *Sensors*, Vol 20 No 19, pp 5523.

[7] Ammour, B., Boubchir, L., Bouden, T., Ramdani, M. 2020. Face–iris multimodal biometric identification system. *Electronics*, Vol. 9, No. 1, pp. 1-18.

[8] Bharadwaj, S., Vatsa, M., Singh, R. 2014. Biometric quality: a review of fingerprint, iris, and face. *EURASIP journal on Image and Video Processing*, Vol 1, pp. 1-28.

[9] Connaughton, R., Bowyer, K. W., Flynn, P. J. 2016. Fusion of face and iris biometrics. In *Handbook of iris recognition* Springer, London. pp. 397-415.

[10] De Keyser, A., Bart, Y., Gu, X., Liu, S. Q., Robinson, S. G., Kannan, P. K. 2021. Opportunities and challenges of using biometrics for business: Developing a research agenda. *Journal of Business Research*, Vol 136, pp 52-62.

[11] Elhoseny, M., Elkhateb, A., Sahlol, A., Hassanien, A. E. 2018. Multimodal biometric personal identification and verification. In *Advances in Soft Computing and Machine Learning in Image Processing*. pp. 249-276.

[12] Eskandari, M., Sharifi, O. 2017. Optimum scheme selection for face–iris biometric. *Iet Biometrics*, Vol. 6, No. 5, pp. 334-341.

[13] Gupta, M., Patwa, F., Sandhu, R. 2018. An attribute-based access control model for secure big data processing in hadoop ecosystem. In *Proceedings of the Third ACM Workshop on Attribute-Based Access Control*. pp. 13-24.

[14] Jain, A. K., Nandakumar, K., Ross, A. 2016. 50 years of biometric research: Accomplishments, challenges, and opportunities. *Pattern recognition letters*, Vol 79, pp 80-105.

[15] Jain, A. K., Ross, A. A., Nandakumar, K. 2011. *Introduction to biometrics*. Springer Science & Business Media.

[16] Kim, Y. G., Shin, K. Y., Lee, E. C., Park, K. R. 2012. Multimodal biometric system based on the recognition of face and both irises. *International Journal of Advanced Robotic Systems*, Vol 9 No 3, pp 1-6.

[17] Kulkarni, R., & Namboodiri, A. 2014. One-time biometric token-based authentication. In *Proceedings of the 2014 Indian Conference on Computer Vision Graphics and Image Processing*. pp 1-7.

[18] Oloyede, M. O., Hancke, G. P. 2016. Unimodal and multimodal biometric sensing systems: a review. *IEEE access*, Vol 4, pp 7532-7555.

[19] Ross, A. A., Jain, A. K., Nandakumar, K. 2006. Levels of fusion in biometrics. *Handbook of multibiometrics*, pp 59-90.

[20] Telgad, R. L., Siddiqui, A., Lothe, S. A., Deshmukh, P. D., Jadhao, G. 2017. Development of an efficient secure biometric system by using iris, fingerprint, face. In *2017 1st International Conference on Intelligent Systems and Information Management (ICISIM)* pp. 100-104