A Bimodal Biometric Student Attendance System

Atuegwu Charity, Kennedy Okokpujie, Noma-Osaghae Etinosa
Department of Electrical and Information Engineering
Covenant University, Ota
Ogun State, Nigeria
atuegwu.charity, kennedy.okokpujie, etinosa.noma-osaghae, (@covenantuniversity.edu.ng)

Abstract*— A lot of attempts have been made to use biometrics in class attendance systems. Most of the implemented biometric attendance systems are unimodal. Unimodal biometric systems may be spoofed easily, leading to a reduction in recognition accuracy. This paper explores the use of bimodal biometrics to improve the recognition accuracy of automated student attendance systems. The system uses the face and fingerprint to take students' attendance. The students' faces were captured using webcam and preprocessed by converting the color images to grey scale images. The grey scale images were then normalized to reduce noise. Principal Component Analysis (PCA) algorithm was used for facial feature extraction while Support Vector Machine (SVM) was used for classification. Fingerprints were captured using a fingerprint reader. A thinning algorithm digitized and extracted the minutiae from the scanned fingerprints. The logical technique (OR) was used to fuse the two biometric data at the decision level. The fingerprint templates and facial images of each user were stored along with their particulars in a database. The implemented system had a minimum recognition accuracy of 87.83%.

Keywords — biometrics; extraction; discrimination; minutiae; thinning; multimodal; unimodal.

I. INTRODUCTION

Biometric systems use unique physiological and behavioral traits for identification or verification. These traits include fingerprints, faces, irises, retinal patterns, hand geometry, hand writing, signature, palm printing and voice [1]. A bimodal biometric attendance system that uses a combination of facial and fingerprint traits for verification or identification is the focus of this paper [2]. It has all the benefits of any standard biometric system and has the additional advantage of an extra layer of authentication [3].

Attendance can be taken in two different forms and these are conventional and automated methods. The conventional method uses attendance book, time register and time clock to keep and track the attendance of students. The Automated method uses bar codes, magnetic stripes, radio frequency identification (RFID) and biometric attendance systems.

In biometric attendance systems, students' traits are enrolled and stored in a database which can be retrieved for recognition when taking attendance [4]. The facial image and fingerprint of each student in the class is taken. The facial image is taken under varying conditions of illumination and with different facial look.

The aim of this paper was achieved by designing an application that captures the facial image and fingerprint of all students of a class for the dual purpose of enrollment and authentication. A special provision is also made for analyzing the attendance record stored in the database.

Image capturing, image processing, feature extraction and classification were carried out using MATLAB® and MYSQL. The database holds the facial images and fingerprints of fifty students. Ten (10) facial Images and four finger prints are got from each student and stored in the database. Feature extraction was carried out by a combination of Principal Component Analysis (PCA) and Linear Discriminant Analysis (LDA). Facial recognition was done by the Support Vector Machine (SVM) Classifier. PCA (Principal Component Analysis) is one of the most effective face recognition techniques, which converts a correlated training set of variables into principal modes of variation through different orthogonal transformation procedure. Primarily, PCA reduces definition requirement of an image by analyzing the principal components (feature extraction). The feature extraction does not incorporate much physical details, as it is primarily driven by statistical characteristics.

Fingerprint recognition is done by matching minutiae scores. A minutia is the collection of ridge ending and ridge bifurcation features of a fingerprint. Ridges exclusively define the uniqueness of a fingerprint through their characteristics and relationship with their neighboring ridges. Extraction of these prominent features provides high efficiency in fingerprint recognition.

II. RELATED WORKS

In [17], iris and fingerprint biometrics were used to secure a door that granted access to only authorized personnel or persons. In the paper, the authors made use of MATLAB™ to develop the software that was used to implement the biometric door access system. The authors made use of voting techniques to fuse the biometric information from the iris and the fingers.

In [18], electrical activities got from the brain and the heart was fused using binaural brain entrainment. The authors declared that a greater stability and reliability was obtained from the fusion of the electrical signals emanating from the heart and brain over time.

In [19], the authors fused palm prints and iris biometrics and used a new extraction method to improve the accuracy and reduce the error rate. The basic for their accuracy test was the genuine acceptance rate.

In [20], the authors used a fusion of fingerprints and iris biometrics to protect digital images. The biometric protection

was applied to digital images in the form of watermarks. The authors employed the use of Independent Component Analysis to achieve it.

In [21], the authors fused the wavelet anchored face and signature biometrics and used hamming distance classifier for authentication.

In [22], the authors fused the two hands' shape and palm prints at the feature and decision level by employing cascade fusion and declared that they obtained a better result than what is obtainable from existing literature.

In [23], the authors reviewed the state of the art in multimodal biometrics with a strong focus on data fusion. They emphasized the milestones and challenges associated with multimodal data fusion.

In [24], the authors used the match score level technique to fuse the face and palm print biometrics.

III. FOUNDATION LITERATURE

A. Drawbacks of unimodal biometric systems

Unimodal biometric systems have a lot of drawbacks and some of them include:

a) Noise in collected data: Noisy data may produce error in matching. This could occur as a result of injuries, voice changes due to illness or cold, poor illumination and positioning during capture and faulty sensors[5][6].

b) Intra class variation: The physical or psychological makeup of users, wrinkles due to aging, beard or hair on the face and different facial expressions make unimodal biometric systems less reliable.

c) Inter class similarities: When there is no significant difference between two individuals, the false match rate increases.

d) Spoof attack: It entails the faking of one's biometric traits in order to get the identity of an authentic user.

e) Non universality: Inability of some individuals to use single biometric system due to deficiency in some of biological traits, physical abnormalities and culture.

B. Multimodal biometrics

This is a system that uses more than one biometric for recognition and authentication purposes. This has become an emerging trend due to increase in identification speed and accuracy. Using more than one biometric has made it possible to eliminate most of the drawbacks of unimodal biometric systems [7]. Sources of data in multi biometric systems can be categorized as follows:

a) Multi Sensor System: Here, more than one sensor is used to extract data from individuals. Examples include using a thermal infrared and a visible light camera to capture the face or using an optical and a capacitive sensor to capture the fingerprints[8].

b) Multi Modal: This entails the use of two or more physiological and behavioral trait for individual identification. For example, using fingerprint and iris [9].

c) Multi Instance: In this system, multiple instances of the physiological or behavioral trait like left and right index finger, left and right eyes are used.

d) Multi Algorithm: This is the process of processing biometric data using two or more algorithms for feature extraction to improve the matching and recognition performance. A good example is using Principal Component Analysis (PCA), Independent Component Analysis (ICA) and Linear Discriminant Analysis (LDA) for facial feature extraction.

e) Multi Sample: In this method, multiple samples of the same trait from an individual are acquired. An example is multiple dab prints of an individual's fingerprint.

C. Multimodal biometric fusion

A multi modal biometric system can be achieved using three different models and they are serial, parallel and hierarchical models. In the serial model, processing of data is done in sequential order. In the parallel model, data can be processed simultaneously and data is classified into a tree like structure in hierarchical models [10]. There are different level points in the fusion of biometric information and they include:

a) Fusion at sensor level: Here, multiple sensors are used or multiple snapshots of the same biometric trait are taken using a single sensor [11].

b) Fusion at feature extraction level: Here, multiple biometric algorithms are fused together to extract a simple feature by applying normalization, transformation and reduction techniques.

c) Fusion at matching score level: Here, combinations of several match scores are used to formulate a new match score [12].

d) Fusion at decision level: Here, final results of different biometric systems are merged using one of OR, AND or majority voting method.

D. Facial recognition technology

This is a systematic method of authenticating an individual by comparing selected facial features from the individual with the template stored in the database [13][27]. The facial image is used to discriminate an individual from others. The face comprises of the nose, mouth, eyes, lips, ears, chin, and forehead which are captured with a camera or other sensor technology. Facial recognition technology measures the entire facial structure, including distances between eyes, nose, mouth, and jaw edges. These measurements are retained in a database and are used for the purpose of comparison during verification. The face is a good biometric trait because of its numerous distinct features and some of the most notable ones

used by facial recognition technologies are:

- Distance between the eyes
- Width of the nose
- Depth of the eye sockets
- The shape of the cheekbones
- The length of the jaw line

These strategic nodal points are measured and used to create a face print (numerical code) that accurately represents the face image captured. This face print is stored in a database. A major advantage of facial recognition technologies is its non-intrusive nature. Individuals can be captured from a distance without being aware of it. This clearly overcomes the problems associated with biometric systems that use traits that require the user to touch or be in close proximity to the sensor.

E. Fingerprint recognition technology

This is a systematic method of authenticating an individual by comparing selected fingerprint features from the individual with the template stored in the database [16]. The fingerprint is used to discriminate an individual from others [25][26]. The fingerprint comprises of ridges and bifurcations which are captured with a scanner. The unique ways in which the ridges and bifurcations are formed on the fingerprint are used to create the thinned template of the fingerprint that is stored in the database. The processes followed by most fingerprint recognition technology in creating a fingerprint template are:

a) Image Capture: The image of the fingerprint is got using a scanner.

b) Image Preprocessing: The image captured is improved upon by filtering it using a wide range of filtering techniques. The contrast of the image is also improved and thinning is done. Thinning reduces the fingerprint image to a single pixel.

c) Feature extraction: Identified unique ridge ends, bifurcations and short ridge extracted and used to create a fingerprint template

F. Matching

Matching is the process of identifying the similarities between images taken from users and templates stored in the database. Based on the preset threshold, the biometric technology used could return a “true or false” for each match request.

IV. METHODOLOGY

This attendance system is a hybrid. It fuses facial and fingerprint recognition technologies. It is a MATLAB® GUI based solution. It covers all the steps of a typical attendance system. It registers students, takes attendance and stores all acquired information in a database. The students’ information and attendance details were stored in a MYSQL database using Apache Server.

A. System Components

Two different devices were used for the face and fingerprint recognition system and they are:

1) Fingerprint reader: A Digital Persona 4500 was used as the fingerprint image reader. It utilizes optical fingerprint scanning technology to achieve excellent image quality, a large capture area and superior reliability.

2) Face camera: A webcam embedded in personal computer was used to capture the facial images of the students.

B. Facial image database

Ten (10) images of 50 distinct individuals were taken. There were variations in facial expressions (opened/Closed eyes, smiling/non-smiling and has ones with/without glasses). All facial images were taken in an upright position, with tolerance for some tilting and rotation of about 15 degrees. The images are colored with minimum resolution of 110×160 and maximum of 130×160.

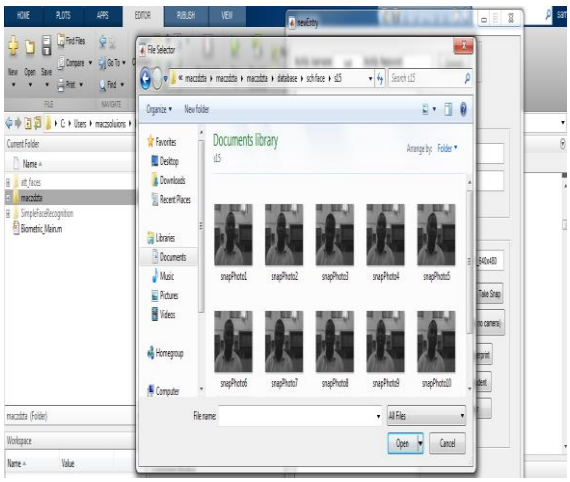

Fig. 1. Snapshot of ten (10) distinct images

C. Face recognition algorithm

To maintain an accurate result of taking the student attendance the following step was done for the student facial preprocessing using various preprocessing techniques before the feature was extracted using PCA and SVM was used as classifier.

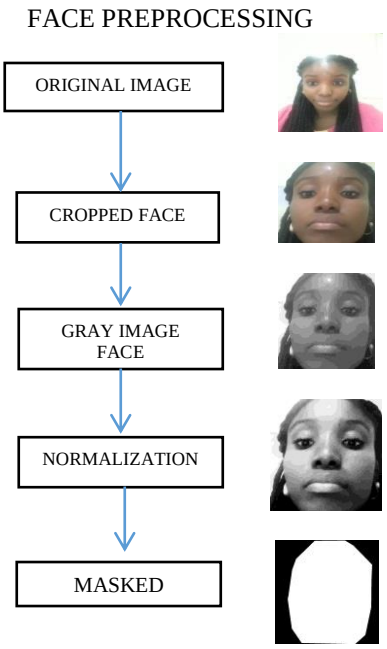

Fig. 2. Face recognition algorithm

D. *Face feature extraction*

The principle component analysis also known as vector recognition is used for face image distribution involving the entire image space length A2, describes an A x A image that defines subspace face image called "face space."

These vectors form the eigenvectors of the covariance matrix which is equivalent to the original face images and ghost face like in appearance are referred to as "eigenfaces." In PCA the entire image are group into two testing set of face images and the training set in which the average will be calculated and the vector will differentiate each image based on the average.

This set of large vector, with a set of M orthogonal vectors, Um when subjected to the PCA describing the distribution of the data. The kth vector, Uk, is chosen such that

$$\lambda k = 1/M \sum M\ n = 1\ (UkT\Phi n)2 \quad (1)$$

is a maximum, subjected to

$$UITUk = \delta lk = \{1, 0, if\ l=\} \quad (2)$$

Given Uk as a vectors and λk as a scalars the eigenvectors and eigenvalues of the covariance matrix respectively

$$C = 1M \sum Mn = 1\Phi n\Phi nT = AAT \quad (3)$$

E. *Fingerprint algorithm*

To maintain an accurate result of taking the student attendance the following step was done for the student finger preprocessing using various preprocessing techniques before the feature was extracted using minutiae extraction.

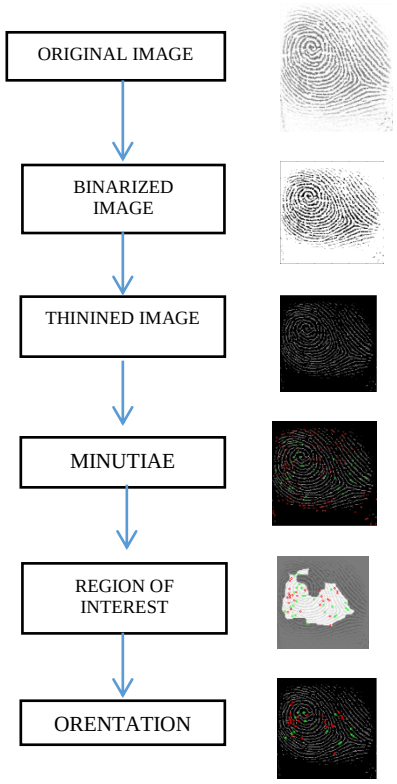

Fig. 3. Fingerprint extraction

F. *Fingerprint feature extraction*

False minutiae caused by ridge break or ridge cross connection due to the position of the finger can be removed using the following mechanism in order to make the fingerprint verification system accurate.

Taking F as the average inter-ridges width or distance between two parallel neighboring ridges.

If the distance between two bifurcations is less then F, the two bifurcations would be removed.

If two terminates are within a distance of F, it is taken as a false minutia and removed.

If the distance between one bifurcation and one termination is less than F, both would be removed.

If two terminations are in a short ridge with length less than F, they would also be removed.

$$M = \{x, y, \emptyset\} \quad (4)$$

Showing x and y coordinate and ø as minutia angle

Minutiae extracted formed a point pattern in a plane which are constructed formed a point pattern in a plane which are constructed only on (x,y) position in order to get distinct pattern, having enough points in each pattern provides the information needed for accurate matching results.

OR fusion method was used at decision level and high accuracy was obtained.

Fig. 4. Four sets of student's fingerprints

G. *Database*

A MySQL database was used to store all the images and particulars of the students. The Students' information was stored in a tabular form. The database is a table with six columns. The database was accessed through MATLAB®.

The process of updating and retrieving data from the database in MATLAB® is:

- Set username.
- Set password.
- Set online connection.
- Set JDBC (Java Database Connectivity) manager.
- Connect to the database.
- Execute SQL query.
- Update/Retrieve value from database.

The fingerprint and facial image capture is done by the MATLAB® GUI (Graphical User Interface) and used to update the database during students' registration.

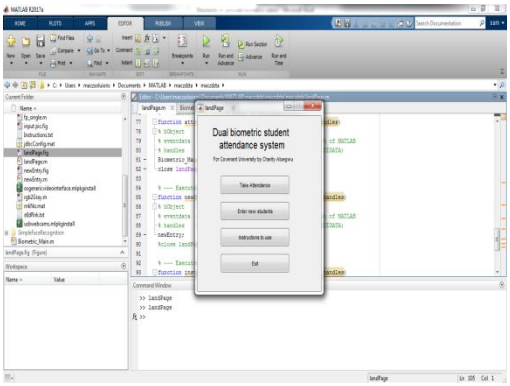

Fig. 5. Graphical User Interface

H. *Enrolling students*

The steps provided by the MATLAB® GUI for the registration of new students are as follows:

- Connect to the database.
- Enter student details (Name and Unique ID).
- Place student in front of the laptop and take snapshot (10 different images of the same person with different posture).
- Capture the student's fingerprint.
- Save new student image and particulars to the database
- To add more students, go to step two.

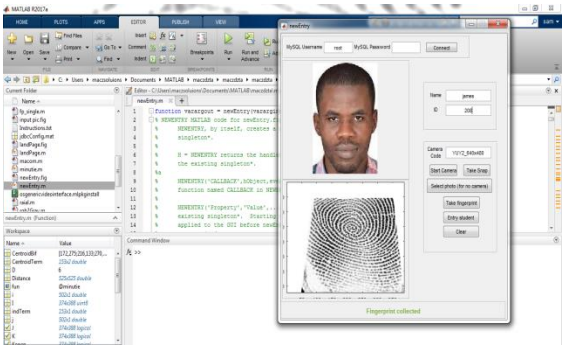

Fig. 6. Updating the database with new entries

I. *Taking attendance*

The "Take Attendance" button provided by the MATLAB ® GUI was used to take attendance and the process followed is:

- Connect to the database
- Click on "Take Attendance"
- Students' facial images and fingerprints are taken to ascertain whether there is a match (after comparison with templates stored in the database) for the facial and fingerprint image of each student present in class.
- The attendance file is automatically updated for the day.

V. RESULT AND DISCUSSION

The implemented student attendance system's performance was measured with the following criteria [16]:

a) False Rejection Rate (FRR): The probability that a system will fail to identify an enrollee. It is also called type 1 error rate. This is also known as *false nonmatch rate (FNMR).*

$$FRR = NFR \div NEIA$$
$$NFR = number\ of\ false\ rejection\ rates$$
$$NEIA = number\ of\ enrollee\ identification\ attempt$$

b) *False Acceptance Rate (FAR):* The probability that a system will incorrectly identify an individual or will fail to reject an imposter. It is also called as type 2 error rate. This is also known as false match rate (FMR).

$$FAR = NFA \div NIIA$$
$$NFA = number\ of\ false\ acceptances$$

$$NIIA = number\ of imposter\ identification\ attempt$$

c) *Response Time (RT):* The time period required by a biometric system to return a decision on identification of a sample. The average response time of the designed system was 1.5 seconds.

d) *Decision Threshold (DT):* the acceptance or rejection of a data is dependent on the match score falling above or below the threshold. The threshold is adjustable so that the system can be made more or less strict depending on the requirements of any given application.

e) *Enrollment Time (ET):* the time period a person must spend to have his/her reference template successfully created. The enrollment time of the designed system is one second ($1s$).

f) *False positive identification rate (FPIR):* this occurs when the system accept someone that is not enrolled in the system.

$$FPIR = 1 - (1 - FMR)N$$

g) *False Negative Identification Rate (FNIR):* occurs when it finds no hit or a wrong hit for a query image enrolled in the system. The relationship between these rates is defined by:

$$FNIR = 1 - (1 - FNMR)N$$
$$Where\ N\ is\ the\ number\ of\ users\ enrolled$$

h) Average time of transaction using the designed system, (Normal process time): 120 Seconds.

TABLE I. ACCURACY OF IMPLEMENTED BIMETRIC SYSTEM

S/N	Test Images	Recognized Images	Rejected Images	Recognition Accuracy
1	3	3	0	100.00
2	3	2	1	66.67
3	3	2	1	66.67
4	3	2	1	66.67
5	3	3	0	100.00
6	3	2	1	66.67
7	3	2	1	66.67
8	3	3	0	100.00
9	3	2	1	66.67
10	3	2	1	66.67
11	3	2	1	66.67
12	3	3	0	100.00
13	3	2	1	66.67
14	3	3	0	100.00
15	3	3	0	100.00
16	3	3	0	100.00
17	3	3	0	100.00
18	3	3	0	100.00
19	3	2	1	66.67
20	3	3	0	100.00
21	3	2	1	66.67
22	3	2	1	66.67
23	3	2	1	66.67
24	3	3	0	100.00
25	3	3	0	100.00
26	3	3	0	100.00
27	3	3	0	100.00
28	3	3	0	100.00
29	3	3	0	100.00
30	3	3	0	100.00
31	3	3	0	100.00
32	3	3	0	100.00
33	3	2	1	66.67
34	3	2	1	66.67
35	3	2	1	66.67
36	3	2	1	66.67
37	3	2	1	66.67
38	3	3	0	100.00
39	3	3	0	100.00
40	3	2	1	66.67
41	3	3	0	100.00

42	3	2	1	66.67
43	3	2	1	66.67
44	3	2	1	66.67
45	3	3	0	100.00
46	3	3	0	100.00
47	3	3	0	100.00
48	3	3	0	100.00
49	3	3	0	100.00
50	3	3	0	100.00
		Average Recognition accuracy		**87.83%**

CONCLUSION

The student attendance system was designed using bimodal recognition traits (Fingerprint and Face). A total of fifty (50) students were enrolled, but the database is large enough to accommodate hundreds of thousands of entries. For each student a total of ten (10) picture images (having different postures and facial expressions) and four (4) fingerprint images were captured for facial and fingerprint matching. MATLAB® GUI provided the interface between the database and the users of the implemented bimodal biometric system. A webcam was used for face image capturing and a Digital Persona 4500 scanner was used to capture fingerprints. MySQL database running on Apache server was used for student information storage. The implemented bimodal biometric student attendance system had a minimum accuracy of 87.83%.

FUTURE WORK

An enhanced multimodal biometric attendance system that can be deployed over a Local Area Network (LAN) instead of on a standalone computer would be designed and possibly implemented

ACKOWLEDGEMENT

This paper was sponsored by Covenant University, Ota, Ogun state, Nigeria.

REFERENCES

[1] P. V. Reddy, A. Kumar, S. M. K. Rahman, and T. S. Mundra, "A new antispoofing approach for biometric devices", IEEE Trans. Biomedical Circuits Systems., vol. 2, no. 4, pp. 328–337, Dec. 2008.

[2] Lucas D. Introna & Helen Nissenbaum, a Survey of Policy and Implementation Issues, Facial Recognition Technology.

[3]] Gaganpreet Kaur, Dheerendra Singh, Sukhpreet Kaur, "Pollination Based Optimization for Feature Reduction at Feature Level Speech & Signature Biometrics", ICRITO, AIIT, Amity University Uttar Pradesh, Noida, India, 8-10-2014.

[4] Ajay Kumar, Yingbo Zhou, "Human Identification using Finger Images", IEEE Transactions on Image Processing, vol. 21, pp. 2228-2244, April 2012.

[5] K. Ganapathi Babu & M.A.Rama Prasad (August 2013), an Effective Approach in Face Recognition using Image Processing Concepts, Volume 2, Issue 8, ISSN 2319 – 4847

[6] Sandeep Sonsanea, Siddhesh Thakura, Priyank Suthara and Jignesh Sisodiab (2015), Automated Attendance System, International Journal of Innovative and Emerging Research in Engineering, Vol 2, Issue 4, e-ISSN: 2394 - 3343 p-ISSN: 2394 - 5494

[7] Dapinder Kaur, Gaganpreet Kaur, Dheerendra Singh, " Efficient and Robust Multimodal Biometric System for Feature Level Fusion (Speech and Signature)", IJCA (0975 – 8887) Volume 75– No.5, August 2013.

[8] Stephen Mayhew (January 2015), History of Biometrics, http://www.biometricupdate.com/201501/history-of-biometrics

[9] Lucas D. Introna & Helen Nissenbaum, a Survey of Policy and Implementation Issues, Facial Recognition Technology

[10] M.Deepamalar, M.Madheswaran, "An Enhanced Palm Vein Recognition System Using Multi-level Fusion of Multimodal Features and Adaptive Resonance Theory", International Journal of Computer Applications (0975 - 8887) Volume 1 – No. 20, 2010.

[11] Shwethaks, Ashwihi A, C Neshwasalih, (Nov 2015), survey on attendance management system using face recognition, international journal of innovative research and computer and communication engineering, (2320 – 9798) vol 3 issue 11.

[12] Rishabi Rai (April 2013), Face Detection Using Matlab based on morphological processing algorithm, international journal of innovative research and development, (2278 - 0211) vol2 issue 4.

[13] T.Sheeba , M.Justin Bernard , "Survey on Multimodal Biometric Authentication Combining Fingerprint and Finger vein ", International Journal of *Computer Applications* (0975 – 8887) Volume 51– No.5, August 2012.

[14] Daramola, S.A. and Adefunmiyin, M., 2016. Personal Identification via Hand Feature Extraction Algorithm. International Journal of Applied Engineering Research, 11(7), pp.5148-5151.

[15] Majekodunmi, T.O. and Idachaba, F.E., 2011. A review of the fingerprint, speaker recognition, face recognition and iris recognition based biometric identification technologies.

[16] Okokpujie, K., Olajide, F., John, S. and Kennedy, C.G., 2016, January. Implementation of the Enhanced Fingerprint Authentication in the ATM System Using ATmega128. In Proceedings of the International Conference on Security and Management (SAM) (p. 258).

[17] Falohun, A.S., Fenwa, O.D. and Oke, A.O., 2016. An Access Control System using Bimodal Biometrics. International Journal of Applied Information Systems, Foundation of Computer Science-FCS, New York, USA, 10(5), pp.41-47.

[18] Palaniappan, R., Andrews, S., Sillitoe, I.P., Shira, T. and Paramesran, R., 2016. Improving the feature stability and classification performance of bimodal brain and heart biometrics. In Advances in Signal Processing and Intelligent Recognition Systems (pp. 175-186). Springer, Cham.

[19] Madane, M. and Thepade, S., 2016. Score Level Fusion Based Bimodal Biometric Identification Using Thepade's Sorted n-ary Block Truncation Coding with Variod Proportions of Iris and Palmprint Traits. Procedia Computer Science, 79, pp.466-473.

[20] Wójtowicz, W. and Ogiela, M.R., 2016. Digital images authentication scheme based on bimodal biometric watermarking in an independent domain. Journal of Visual Communication and Image Representation, 38, pp.1-10.

[21] Joshi, S.C. and Kumar, A., 2016, January. Design of multimodal biometrics system based on feature level fusion. In Intelligent Systems and Control (ISCO), 2016 10th International Conference on (pp. 1-6). IEEE.

[22] Charfi, N., Trichili, H., Alimi, A.M. and Solaiman, B., 2016. Bimodal biometric system for hand shape and palmprint recognition based on SIFT sparse representation. Multimedia Tools and Applications, pp.1-26.

[23] Zapata, J.C., Duque, C.M., Rojas-Idarraga, Y., Gonzalez, M.E., Guzmán, J.A. and Botero, M.B., 2017, September. Data Fusion Applied

to Biometric Identification–A Review. In Colombian Conference on Computing (pp. 721-733). Springer, Cham.

[24] Farmanbar, M. and Toygar, Ö., 2016. Feature selection for the fusion of face and palmprint biometrics. Signal, Image and Video Processing, 10(5), pp.951-958.

[25] K.O. Okokpujie, O. O. Uduehi, F. O. Edeko. "An Innovative Technique in ATM Security: An Enhanced Biometric ATM with GSM Feedback Mechanism" Journal of Electrical and Electronics Engineering (JEEE) 2015, 12 (2), Pages 68-81

[26] Okokpujie, K., Etinosa, N.O., John, S. and Joy, E., 2017, November. Comparative Analysis of Fingerprint Preprocessing Algorithms for Electronic Voting Processes. In International Conference on Information Theoretic Security (pp. 212-219). Springer, Singapore.

[27] Okokpujie, K., Noma-Osaghae, E., John, S. and Ajulibe, A., 2017, November. An Improved Iris Segmentation Technique Using Circular Hough Transform. In International Conference on Information Theoretic Security (pp. 203-211). Springer, Singapore.