*International Journal of Applied Information Systems (IJAIS) – ISSN : 2249-0868*
*Foundation of Computer Science FCS, New York, USA*
*Volume 12 – No. 5, August 2017 – www.ijais.org*

# Trimodal Biometric Authentication System using Cascaded Link-based Feed forward Neural Network [CLBFFNN]

Benson-Emenike Mercy E.
Dept. of Computer Science
Abia State Polytechnic, Aba
Abia State, Nigeria

Sam-Ekeke Doris C.
Dept. of Computer Science
Abia State Polytechnic, Aba
Abia State, Nigeria

## ABSTRACT

The beginning of the 21st century was rich in events that turned the world’s attention to public security. Increase in technological advancement gave people possibilities of information transfer and ease of physical mobility unseen before. With those possibilities comes risk of fraud, theft of personal data, or even theft of identity. One of the ways to prevent this is through biometric authentication system. This paper considers a multi-biometric system involving a combination of three biometric traits: iris, fingerprint and face in order to make authentication cheaper and more reliable. When the images are captured using optical scanner and webcam, image pre-processing is done using Enhanced Extracted Face (EEF), Plainarized Region of Interest (PROI) and Advanced Processed Iris Code (APIC) methods for face, fingerprint and iris images respectively. These are fed into a Cascaded Link-Based Feed Forward Neural Network (CLBFFNN) which is a classifier trained with back-propagation algorithm. CLBFFNN comprises of CLBFFNN(1) used for training and CLBFFNN(2) used as the main classifier. Fusion of outputs from face, fingerprint and iris recognition systems is done at decision level using AND operation. With the use of the improved pre-processing methods, Optical Character Recognition (OCR) with intelligent barcode and CLBFFNN, the proposed intelligent multibiometric system is proved to be cheaper, more secure and efficient than the existing methods.

## Keywords

Authentication, Enhanced Extracted Face (EEF), Plainarized Region Of Interest (PROI), Advanced Processed Iris Code (APIC), Cascaded Link-Based Feed Forward Neural Network (CLBFFNN), Optical Character Recognition (OCR), Multibiometric, Back propagation Algorithm, Adaptive Principal Component Analysis (APCA), Multilayer Perceptron (MLP), Relevant Vector Machine (RVM), and Support Vector Machine (SVM).

## 1. INTRODUCTION

Biometrics is a division of science that uses computer knowledge to establish human identification or authentication, based on a person’s behavioral or physical characteristics. Biometrics is a constituent of two Greek words, ‘bio’ and ‘metrics’. ‘Bio’ in the word biometrics has to do with natural life and refers to the quantifiable physical or biological traits while ‘metrics’ literally means ‘to measure’ and refers to the quantitative or measurable analysis for accurate authentication of a person.

It has been observed from the definition of biometrics that the use of biometrics in person’s authentication yields better results than traditional methods. However, no single biometric technology can guarantee 100% accuracy; this means that every biometric technology has both advantages and disadvantages in terms of accuracy, cost, ease of use, intrusiveness, ease of deployment. Secondly, none can be perfectly used in all applications. Therefore, unimodal biometric systems (biometric technology involving only one biometric trait) have a lot of problems such as noise, false rejection, etc.; which could be solved by employing the use of more than a biometric attribute. Any biometric system that uses more than one biometric trait or identifier in a personal authentication is called a multibiometric system. It solves the problems of unimodal biometrics such as false rejection, noisy data, intra-class variations, restricted degrees of freedom, non-universality and spoof attacks (Farhat and Zede, 2008; Singh et al, 2012; Rashmi et al, 2012). This is because multi-biometric systems incorporate and fuse proofs obtainable from different traits and guarantee significant development in the biometric system matching accuracy. This depends on the traits that are being merged and the merging approach.

To overcome these difficulties multi-biometric systems are used [13], [42], [28]. Many of these limitations can be addressed by deploying multi-modal biometric systems that integrate the evidences presented by multiple sources of information [20], [38], [25], [47].

This paper is arranged in seven sections consisting of the Introduction, Reviewed Literatures, the proposed method, CLBFFNN, OCR with Intelligent 2D Barcode, Biometric Fusion and Matching, Implementation and Evaluation.

## 2. REVIEWED LITERATURES

Nayak & Narayah (2013) in their work “Multimodal Biometric Face, Fingerprint and Iris Recognition Using Adaptive Principal Component Analysis and Multilayer Perception” combined ridge-based and eigen face approach for parallel execution. They used APEX algorithm, Multilayer Perceptron (MLP) with back propagation learning technique and combined various fusion levels. Their major shortcoming was on the speed of face recognition system. They had a low recognition rate.

Long & Thai, (2015) in their work ‘Person Authentication using Relevance Vector Machine (RVM) for Face, Fingerprint and Iris, extracted both face and fingerprint features using Zernike Moment. This moment is invariant to rotation, scaling and noise image, while authentication is done using RVM. Their preprocessing involves image normalization, noise elimination, and illumination normalization. Their system encountered noise reduction but had low recognition rate.

Wilson & Lenin, (2014) in their work, 'An Efficient Biometric Multimodal Face, Iris and Finger Fake Detection using an Adaptive Neuro Fuzzy Inference System (ANFIS) used Singularity Points detection method for fingerprint detection and an Anisotropic Gaussian filtering and Hough Transform. They employed four phases in iris image detection: image scanner, preprocessing, feature extraction and identification; employed median filter and canny edge detection algorithm and used Daugman's rubber sheet model to normalize the iris model and Gabor filter for feature extraction. Median filter and Canny Edge detection algorithm were used for face detection preprocessing, and also used vertical and horizontal sober operator. They used an Adaptive Neuro Fussy Inference System (ANFIS) classifier, which is a fuzzy inference system implemented in a framework of adaptive network.

Annis et al., (2013) in their work, ' Person Authentication System with Quality Analysis of Multimodal Biometrics employed Orientation Field Methodology (OFM) for fingerprint preprocessing and Hough transform for detection of ROI. Gabor transform and Independent Component Analysis (ICA) were used for iris and face feature extraction respectively. They used score level fusion using weighted average approach. They also employed Block Independent Component Analysis (BICA), Discrete Cosine Transform with Fisher Linear Discriminant Classifier and Kalman Filter.

# 3. OUR PROPOSED METHOD

In our approach, we adopted an intelligent trimodal Multi-biometric Authentication System using a Cascaded Link Feed-Forward Neural Network [CLFFNN] as a classifier. The preprocessing methods used for fingerprint, face and iris are Plainarized Region of Interest Method (PROI), Enhanced Extracted Face (EEF) and Advanced Processed Iris Code (APIC) methods for face, fingerprint and iris images respectively. Our method involves two phases: Enrollment phase and Verification phase. Each of these phases consists of four steps such as: Image Acquisition, Preprocessing, Feature extraction, and Training and matching.

When each of the biometric traits or images is captured, it undergoes image preprocessing and feature extraction. Feature vectors for face, fingerprint and iris are produced and then passed into CLBFFNN classifier for network training and authentication. Image acquisition, preprocessing and feature extraction of these three biometric traits are done in parallel. This is shown in Figure 1.

## 3.1 Face Modality

We employ a method called Enhanced Extracted Face Method as shown in figure 2. This involves Image Acquisition using webcam, Face Image Preprocessing, Image Resizing and Cropping, ROI Detection, Feature Extraction, and Post Processing with Biometric Feature Quality Checker. Preprocessing is the process of screening the input image so as to obtain a better-quality output image before passing it on to the next stage of the authentication system [Benson-Emenike and Nwachukwu, (2015)]. Preprocessing is an important phase in face recognition that makes the quality of face image standard and ready for feature extraction. It involves some Image Enhancement processes such as Image Conversion, Morphological Dilation, Thinning, and Binarization. In our feature extraction, we adopted a 2-D Gabor filter kernel which we defined as follows:

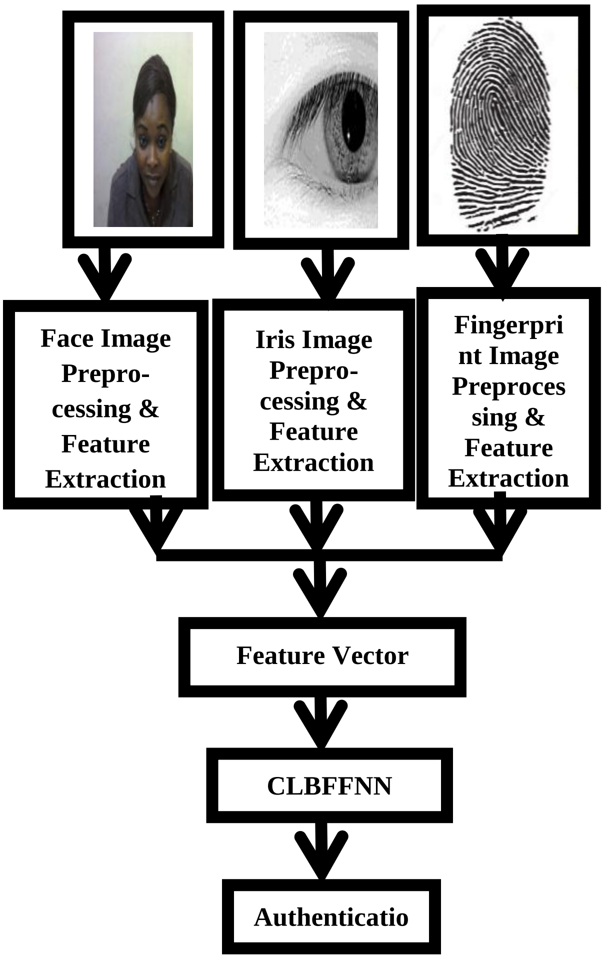

Face Image Prepro-cessing & Feature Extraction
Iris Image Prepro-cessing & Feature Extraction
Fingerpri nt Image Preproces sing & Feature Extraction
Feature Vector
CLBFFNN
Authenticatio

**Figure 1: Intelligent Face Preprocessing and Detection**

$$f(\alpha,\beta,\theta_{r\,,},\eta) = exp\left[-\frac{1}{2}\left\{\frac{T_1^2}{\sigma_\alpha^2}+\frac{T_2^2}{\sigma_\beta^2}\right\}\right] exp\left\{P\frac{2\pi T_1}{\eta}\right\}$$

**(1)**

Where $T_1 = \alpha cos\theta_r + \beta sin\theta_r$ **(2)**

$$T_2 = -\alpha sin\theta_r \quad \textbf{(3)}$$

$\sigma_\alpha$ *and* $\sigma_\beta$ are the Gaussian envelope standard deviations along the $\alpha$ and $\beta$ dimensions while $\eta$ and $\theta_r$ are the wavelength and orientation of sinusoidal plane wave respectively. The sinusoidal plane wave orientation $\theta_r$ is defined by

$$\theta_r = \frac{\pi(r-1)}{k}, \qquad r = 1, 2, \ldots, k \qquad (4)$$

where k equals the number of orientations (in degrees) that are taken into consideration. A convolution of the image with the filter kernel obtained by Eq. (1) gives a Gabor filter response. For sampling point ($\alpha$,$\beta$), the filter response is given by:

$$\boldsymbol{u(\alpha,\beta,\theta_r,\eta) = \sum_{g=-(K-\alpha)}^{K-\alpha-1} \sum_{q=-(K-q)}^{K-\beta-1} J(\alpha+g,\beta+ qf(g,q,\theta r,\eta)} \quad \textbf{(5)}$$

where $J(\alpha,\beta)$ signifies a 16x16 grayscale image.

After these stages, the resultant image is passed into CLBFFNN classifier for training and recognition.

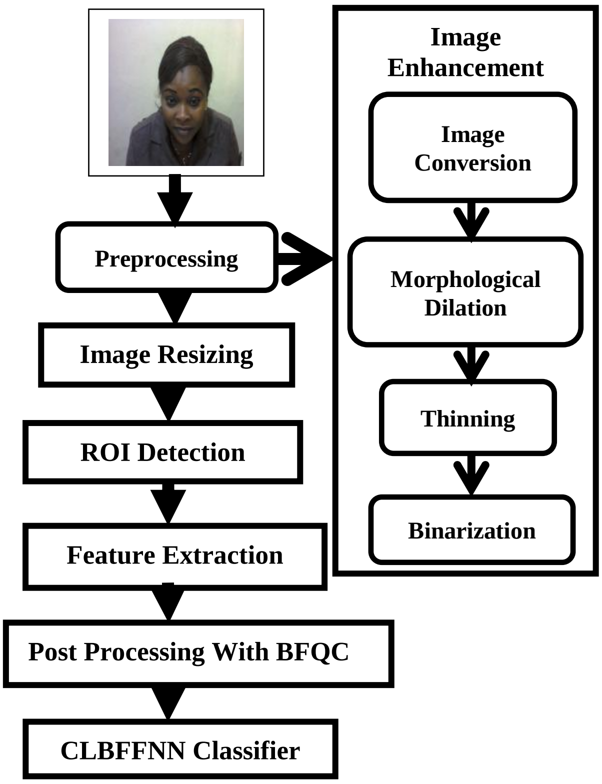


**Figure 2: Enhanced Extracted Face Method (EEF) of Face Image Preprocessing**

## 3.2 Fingerprint Modality

We employ a method called Plainarized Region of Interest (PROI) which involves the following stages: Fingerprint Image Acquisition, Preprocessing, Image Enhancement, Binarization, Denoising, Thinning, Minutiae Extraction, Post Processing and Biometric Feature Quality Checker, as seen in figure 3. After these stages, the resultant image vector is passed into CLBFFNN classifier for training and recognition.

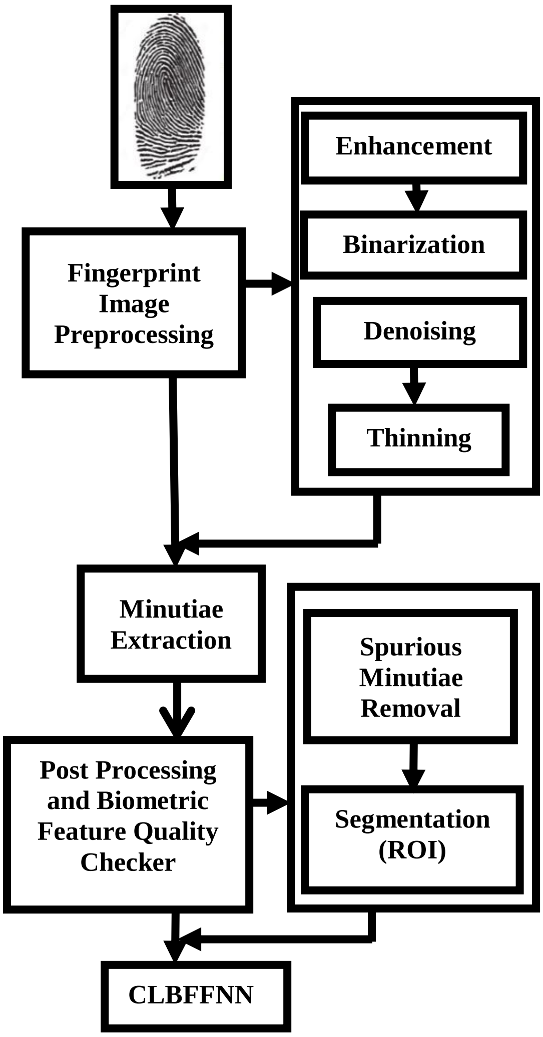

Enhancement
Binarization
Denoising
Thinning
Fingerprint Image Preprocessing
Minutiae Extraction
Spurious Minutiae Removal
Segmentation (ROI)
Post Processing and Biometric Feature Quality Checker
CLBFFNN

**Figure 3: Plainarized Region of Interest (PROI) Method of Fingerprint Image Preprocessing**

## 3.3 Iris Modality

We adopt a method called Advanced Processed Iris Code (APIC) which involves stages such as Iris Image acquisition, Preprocessing (involving Iris Segmentation, Normalization, Enhancement and Denoising), Iris Code Generation and Feature Extraction, Post Processing and Biometric Feature Quality Checker. After these stages, the resultant image is passed to CLBFFNN classifier for classification and matching, as seen in Figure 4.

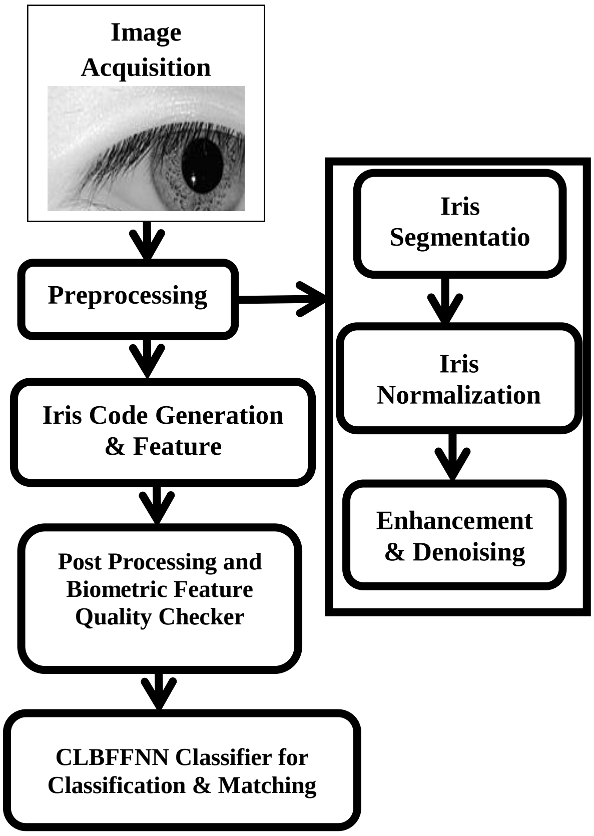


Image Acquisition
Preprocessing
Iris Code Generation & Feature
Post Processing and Biometric Feature Quality Checker
CLBFFNN Classifier for Classification & Matching
Iris Segmentatio
Iris Normalization
Enhancement & Denoising

**Figure 4: Advanced Processed Iris Code (APIC) Method for Image Preprocessing**

## 4. CASCADED LINK-BASED FEED FORWARD NEURAL NETWORK (CLBFFNN)

After preprocessing, feature extraction and quality assessment, the next stage is verification or authentication which is done by a CLBFFNN classifier. CLBFFNN is an ordered cascade of two neural networks CLBFFNN(1) and CLBFFNN(2), as seen in Figure 5.

Their designed arrangement guarantees reduction in computation cost, increases system's detection accuracy and efficiency. The network components are interconnected with layers and flow of information via these network components is not interrupted in any way. Apart from learning and training of CLBFFNN with back propagation algorithm, it makes decisions on final association between its inputs.

### 4.1 CLBFFNN(1)

CLBFFNN(1) is a neural network that uses Back Propagation algorithm. It is composed of an input layer, a single hidden layer and an output layer with a sigmoid activation function. The feature vectors from APIC, EEF and PROI for iris, face and fingerprint respectively; form the input into CLBFFNN(1). The CLBFFNN (1) has three cascaded stages as seen in Figure 6. The first stage ensures that the feature patterns that are entering into the network are life-scanned features, i.e. facilitating further liveness detection. The second stage filters the non-face from face feature, distorted or incomplete minutiae from fingerprints and blurred iris pattern from iris images. Lastly, the third stage determines the image width and height and calculates the time complexity of face, fingerprint and iris detection. These sub windows are passed through each section of image and minimizes the false positive rate (i.e. non-faces for example) and detects the face. This method reduces false rejection and false acceptance errors to their barest minimum and increases system verification accuracy. The simulated results from CLBFFNN(1) is fed into CLBFFNN(2) for the function approximation.

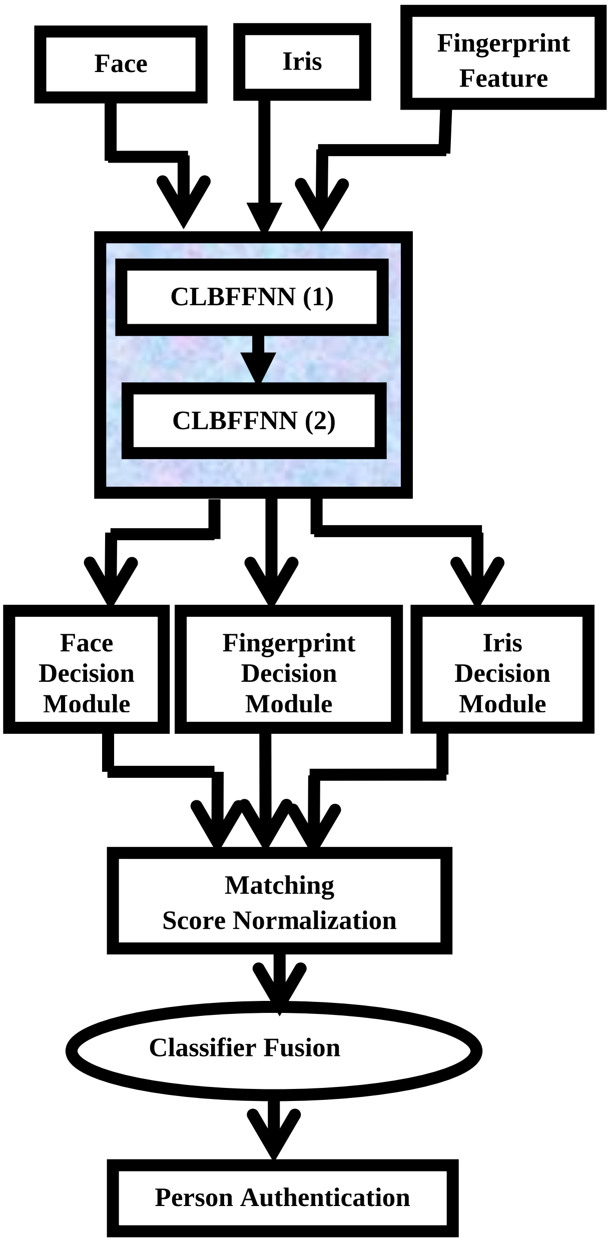


**Figure 5: CLBFFNN Classifier**

### 4.2 CLBFFNN(2)

Network learning and training, template matching, comparison and decision making take place in CLBFFNN(2). Output from CLBFFNN(1) is approximated since it is connected with CLBFFNN(2). CLBFFNN(2) are universal approximators and have a very compact topology. CLBFFNN(2) is also composed of an input layer, a single hidden layer and an output layer with fast locally regulated neurons; and also has a feed-forward design. With this arrangement, false rejection must be totally eradicated if adequate data are made available to the network during training session. The output from the CLBFFNN(2) is considered as the recognition result.

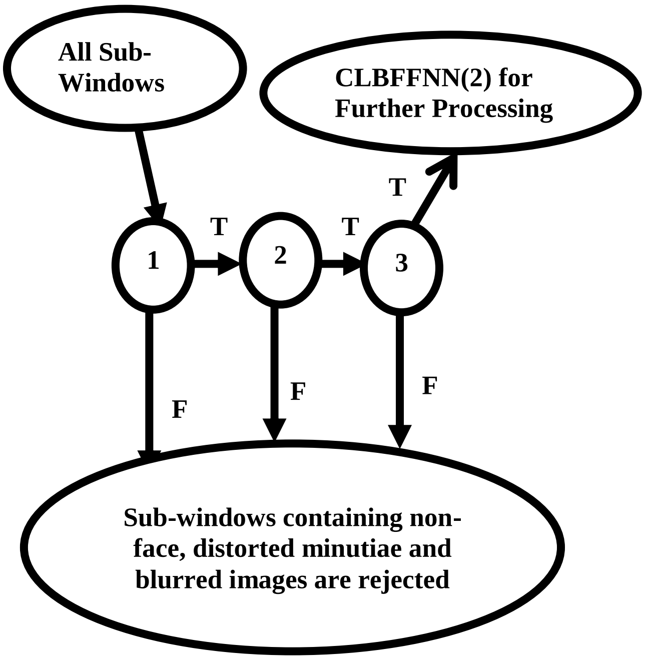

All Sub-Windows
CLBFFNN(2) for Further Processing
T
T
T
1
2
3
F
F
F
Sub-windows containing non-face, distorted minutiae and blurred images are rejected

**Figure 6: The Three Cascaded Stages of CLBFFNN(1)**

## 5. OPTICAL CHARACTER RECOGNITION (OCR) WITH INTELLIGENT 2D BARCODE

OCR is a technology that converts various documents (whether digital, scanned, or PDF files) into data that can be edited or searched. OCR automatically scans a document and provides a full alphanumeric recognition of printed or handwritten characters at electronic speed (Pranob et al., 2012).

OCR with Intelligent 2D Barcode has been used in conjunction with the intelligent trimodal biometric system and has been seen to greatly increase the throughput, effectiveness, accuracy and efficiency of the system.

## 6. BIOMETRIC FUSION AND MATCHING

During enrolment stage, an individual's biometric sample is extracted and converted to biometric feature using the proposed preprocessing algorithms; and is stored as template in the template database. When the individual later comes for authentication, he submits his biometric sample again, and the whole process repeats. At template match, his template already saved in the memory is extracted and compared with the current template and a match score is obtained which is then matched with a set threshold. A "match" or "non-match" output is obtained. Feature extraction and matching scores for the three biometric traits are done independently, thereafter the output from the three recognizers are fused at decision level using AND rule.

### 6.1 Fusion

Fusion is a method designed to obtain a combination of multiple pieces of biometric data; in our case, face, fingerprint and iris biometric features. Fusion is normally performed when there are multiple samples, multiple modes, or multiple algorithms; and it is more informative than any of the input images. Good combination of these traits improves the overall decision accuracy.

The score vector is formed with the scores obtained from each of the biometric trait at matching score level using sum rule. MSiris, MSfinger and MSface, being the matching scores generated by iris, fingerprint and face recognizers respectively are obtained. Combining match scores is a challenging task because the scores of different matchers are heterogeneous i.e. have dissimilar nature and scale.

### 6.2 Score Normalization

Since the three traits used are dissimilar in nature and have un-identical geometric range; score normalization of the three scores becomes inevitable. Normalization means transforming the marks obtained from each of the separable matchers into a mutual province prior to their combination. Here, we adopt min-max normalization pattern, as given in equations (6), (7) and (8):

$$\mathbf{N_{Iris}} = \frac{\mathbf{MS_{Iris} + min_{Iris}}}{\mathbf{max_{Iris} + min_{Iris}}} \qquad \textbf{(6)}$$

$$\mathbf{N_{finger}} = \frac{\mathbf{MS_{finger} + min_{finger}}}{\mathbf{max_{finger} + min_{finger}}} \qquad \textbf{(7)}$$

$$\mathbf{N_{face}} = \frac{\mathbf{MS_{face} + min_{face}}}{\mathbf{max_{face} + min_{face}}} \qquad \textbf{(8)}$$

The $\max_{iris}$, $\max_{face}$, $\max_{finger}$ are the maximum scores for iris, face and fingerprint recognition respectively while the $\min_{iris}$, $\min_{face}$, $\min_{finger}$ are the minimum scores for iris, face and fingerprint recognition respectively. $N_{iris}$, $N_{face}$, and $N_{finger}$ are the normalized matching scores of iris, face and fingerprint respectively. The output of an iris matcher, fingerprint and face matchers are given as a distance score, a similarity score and a distance score, respectively.

### 6.3 Combination of Normalized Scores

Before combining the normalized scores, the three normalized scores $N_{iris}$, $N_{face}$, and $N_{finger}$ are converted to likeness domain. This is achieved by finding its difference from 1, as shown in Equation 9.

$$\begin{aligned}\mathbf{NSS_{iris}} &= \textbf{Unity - } \mathbf{N_{iris}} \\ \mathbf{NSS_{finger}} &= \textbf{Unity - } \mathbf{N_{finger}} \qquad \textbf{(9)} \\ \mathbf{NSS_{face}} &= \textbf{Unity - } \mathbf{N_{face}}\end{aligned}$$

where Unity = 1

Therefore the addition of the obtained normalized similarity score, $\mathbf{NSS}_{\text{iris}}$, $\mathbf{NSS}_{\text{finger}}$, and $\mathbf{NSS}_{\text{face}}$ gives the final matching score, $\mathbf{MS_{final}}$; this is obtained by Equation (10).

$$\mathbf{MS_{final}} = \mathbf{1/3}\ [\boldsymbol{\alpha} * \mathbf{NSS_{iris}} + \boldsymbol{\beta} * \mathbf{NSS_{finger}} + \boldsymbol{\gamma} * \mathbf{NSS_{face}}] \qquad \textbf{(10)}$$

Where α, β, $\gamma$ are the threshold weights for the individual traits: iris, fingerprint and face features respectively.

### 6.4 Matching

α, β and $\gamma$ are individually apportioned the value of one, so that the classifiers will have a common domain. Matching involves the assessment of similarity and difference between the final matching score ($MS_{final}$) and the set threshold. Hence, the output obtained is verifying an individual as a true or an impersonator.

**$MS_{Final}$ Vs Threshold ➡ Authentication (Accept / Reject)**

## 7. IMPLEMENTATION AND EVALUATION

When the training begins, all the weights of the neurons are aggregated and stored in a weight file. After the first set of data is trained, an error is calculated, which is based on the difference between the computed output and the target output, as seen in figure 7. This aims at reducing this error and ensuring that the final output obtained is equal to the target output; by series of network training and weight adjustments.

### 7.1 Experimental Details

The experiment involves two major phases: Enrolment and Authentication. During enrolment, the user is expected to enter his name, address, date of birth and gender. After this, he clicks to have his face, iris and fingerprint captured, as seen in Figure 8. In the case of fingerprint, he is expected to choose from the left or right finger index, pinkie, middle finger or thumb. Four samples of the selected choice are taken. Each of these traits, when captured, is used to obtain feature matrices which are stored in the database. These feature matrices are then fed into CLBFFNN for training and learning purposes. The learning rate of the network is set to $\eta_1 = \eta_2 = 0.6$ and spread factor is $K_1 = K_2 = 0.7$. When training is completed, the updated weights and threshold values are stored in a database (Auth_sys), which are used in the iris, face and fingerprint verification process.

During authentication, the enrollee is expected to resubmit the same biometric data he submitted during enrolment. When this is done, the features are extracted from a feature matrix and compared with those pre-stored in the database. Authentication is done and access is either guaranteed or denied. When access is guaranteed, the user is given an ID card which has an OCR barcode on it with the user's picture. This ensures more secure and efficient system.

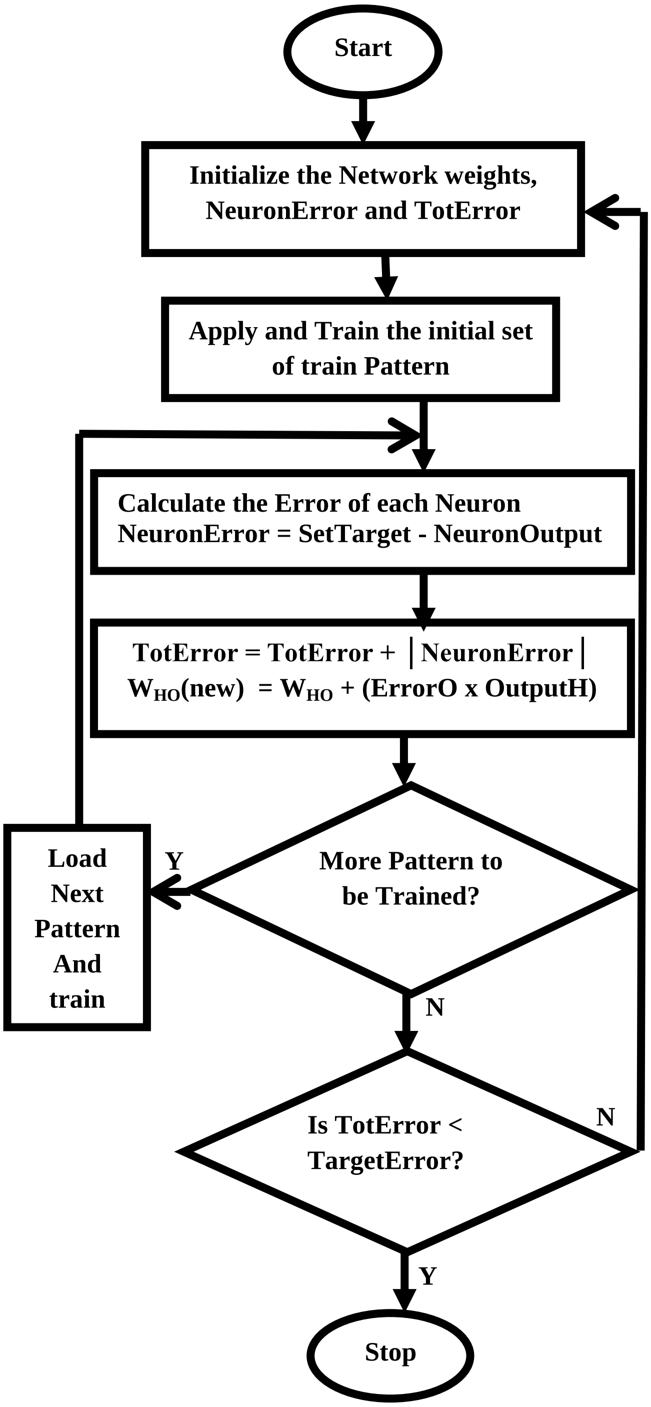
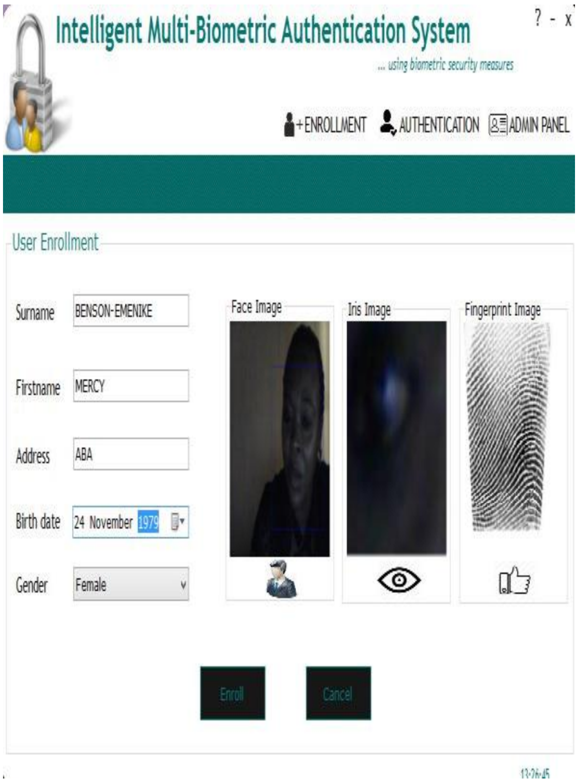

Start
Initialize the Network weights, NeuronError and TotError
Apply and Train the initial set of train Pattern
Calculate the Error of each Neuron
NeuronError = SetTarget - NeuronOutput
TotError = TotError + │NeuronError│
W_HO(new) = W_HO + (ErrorO x OutputH)
More Pattern to be Trained?
Y
Load Next Pattern And train
N
Is TotError < TargetError?
N
Y
Stop

**Figure 7: Network Learning and Training**



Surname: BENSON-EMENIKE

Firstname: MERCY

Address: ABA

Birth date: 24 November 1979

Gender: Female

**Figure 8: Enrolment Phase**

## 7.2 System Testing and Results

To test the multi-biometric system, iris, fingerprints and face features were obtained from 20 persons. Four samples of face, fingerprint and iris features were collected from each person. The experimental result of the verification process as seen in Table 1 proves the authenticity of our proposed system.

**Table 4.1: Result of Verification using Trimodal Biometrics**

| Experimental Data | Face Alone | Iris Alone | Finger-print Alone | Multi-modal Result |
|---|---|---|---|---|
| **No. of Persons** | **50** | **50** | **50** | **50** |
| **Samples for each Person** | **4** | **4** | **4** | **4** |
| **Total No. of Samples** | **200** | **200** | **200** | **200** |
| **False Acceptance** | **4** | **4** | **2** | **0** |
| **Unrecognized Samples** | **3** | **3** | **4** | **2** |
| **Misclassified Images** | **4** | **5** | **2** | **1** |
| **Impostors obtained** | **1** | **1** | **2** | **0** |
| **Recognized Samples** | **195** | **193.75** | **190** | **199** |
| **System Accuracy** | **97.5** | **96.875** | **95** | **99.5** |

### 7.2.1 System Percentage Recognition Accuracy

Accuracy is the measure of a system's correctness, effectiveness and reliability. The following were computed based on the experiment conducted:

$$\%\text{Accuracy}=\frac{\text{Total No.of Recognized Samples}}{\text{Total No.of samples}}\text{ x }100$$

$$\%\ \text{Accuracy (Iris)} \quad = \frac{193.75}{200}\text{ x }100$$
$$= \ 96.875$$

$$\%\ \text{Accuracy (Fingerprint)} = \frac{190}{200}\text{ x }100$$
$$= \ 95$$

$$\%\ \text{Accuracy (Face)} \quad = \frac{195}{200}\text{ x }100$$
$$= \ 97.5$$

$$\%\ \text{Accuracy (Face + Iris + Fingerprint)}$$
$$= \frac{199}{200}\text{ x }100$$
$$= \ 99.5$$

It is observed that our proposed system gives a better Recognition Rate and Accuracy, as seen in Table 2; and its superiority over unimodal applications is proved.

The error rate is calculated by finding the ratio between the number of misclassified images and the total number of images in the testing set. The accuracy is precisely the opposite of the error rate, that is, the percentage of correctly classified images.

**Error rate of our proposed system**

$$= \frac{\text{Misclassified images}}{\text{Total number of images}}\text{ x }100\%$$

$$= \ \frac{1}{200}\text{ x }100\% = \ 0.5\%$$

$$\text{Accuracy} \quad = 100\% - \text{Error Rate}$$
$$= 100 - 0.5$$
$$= \ 99.5$$

This multi-biometric system gives a recognition rate of 99.474. This is shown in Table 2.

**Table 2: Recognition Rate of our Proposed System**

| Test | Recognition Rate |
|---|---|
| A | **99.54** |
| B | **99.65** |
| C | **99.31** |
| D | **99.35** |
| E | **99.52** |
| **Average** | **99.474** |

### 7.2.2 Evaluation

Two types of evaluation are considered: System Performance Evaluation and Recognition Performance Evaluation. In our system performance evaluation, we considered the following metrics: security, data quality and usability. Security has to do with the biometric system robustness. Here, the devices, architectures and algorithms are secured against attacks by mounting appropriate checks (such as liveness checks, biometric data quality checks and overtraining check facilities) at appropriate quarters. With the aid of the biometric quality checking, bad quality samples are removed during enrolment while some are rejected during verification. This, if not done, would definitely increase the enrollment failure rate; and consequently lead to a lower system performance quality. The proposed biometric system usable since it guarantees efficiency, effectiveness and user satisfaction with little or no specific training. In our Recognition Performance Evaluation, we calculated FAR, FRR, FTE, FTA, GAR, TER and Recognition rate

**False Acceptance Rate**

**FAR (%) =**

$$\frac{\text{False Acceptance Number}}{\text{Number of Impostors Obtained}} \text{ X } 100\%$$

$$= \frac{0}{0} \text{ x } 100\%$$

$$= 0\%$$

**False Rejection Rate**

$$\text{FRR}(\%) = \frac{\text{False Rejection Number}}{\text{Number of Approved User Obtained}} \text{X } 100$$

$$= \frac{1}{199} \text{ x } 100\%$$

$$= 0.00502513 \text{ x } 100$$

$$= 0.5025\%$$

**Failure-To-Enrol Rate**

**FTE = 0.**

**Failure-To-Acquire Rate**

**FTA = 0.**

**Genuine Acceptance Rate**

**GAR(%) = 100 – FRR(%) = 100 – 0.5025**

**= 99.498%**

**Total Error Rate (TER)(%)**

**= FAR(%) + FRR(%)**

**= 0 + 0.502**

**= 0.5025%**

### 7.2.3 Comparison of our Method with Others

The proposed classifier, CLBFFNN is compared with Adaptive Principal Component Analysis (APCA) and Multilayer Perceptron (MLP) (Nayak and Narayah (2013)) methods as seen in Figure 9; and is seen to have a better recognition performance. The second comparison shows the superiority and efficiency of multimodality over unimodality, as shown in Figure 10. Comparison was also done with that of Long & Thai (2015) who used RVM in their approach. CLBFFNN gives better performance than their approach as seen in Figure 12. If the user is verified to be true, he gets an output message granting him an access, as seen in figure 13. Then an ID card with an OCR Barcode is issued to him, as seen in figure 14.

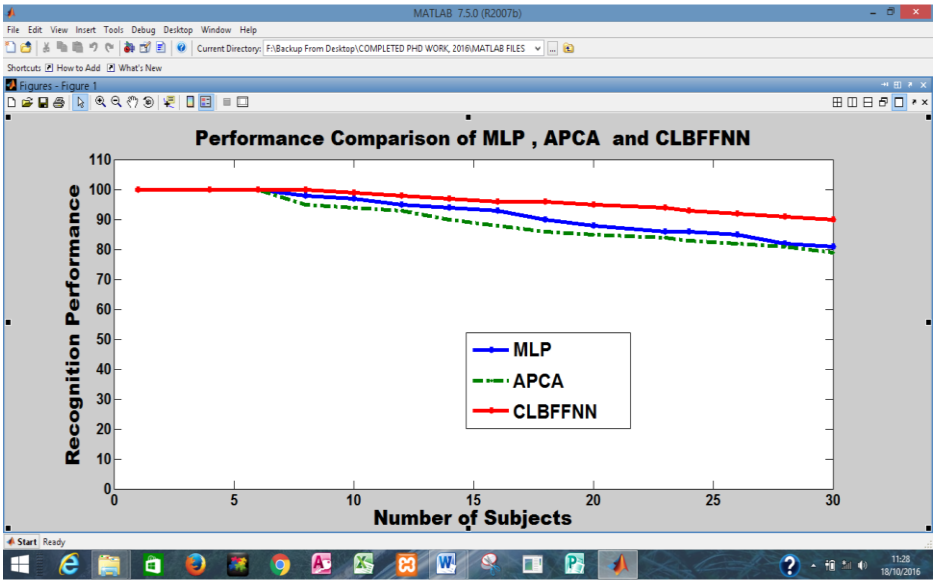


**Figure 9: Performance Comparison MLP, APCA and CLBFFNN**

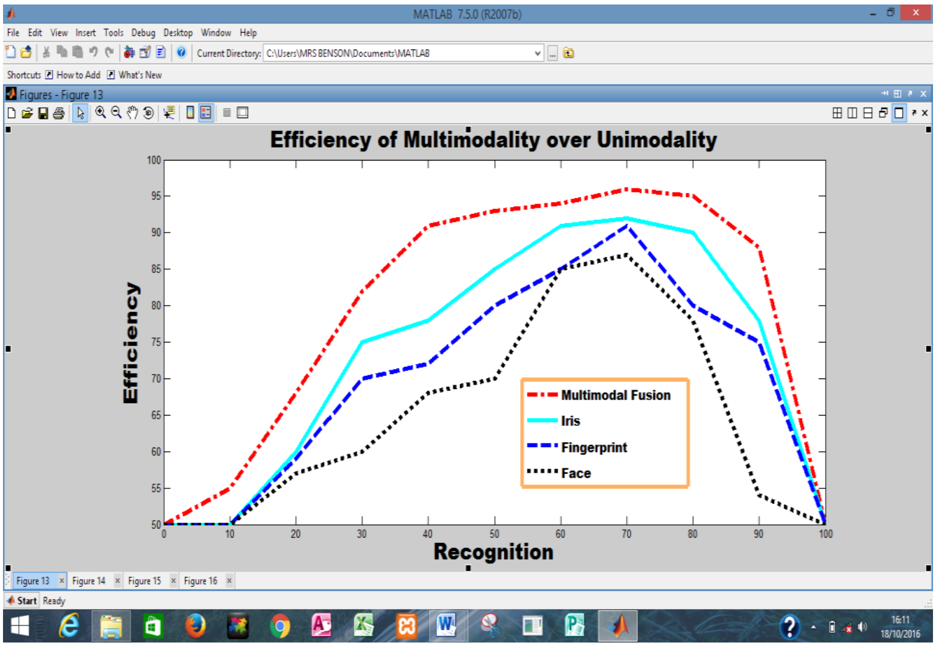


Figure 10: The Proof of Effectiveness of Multimodality over Unimodality

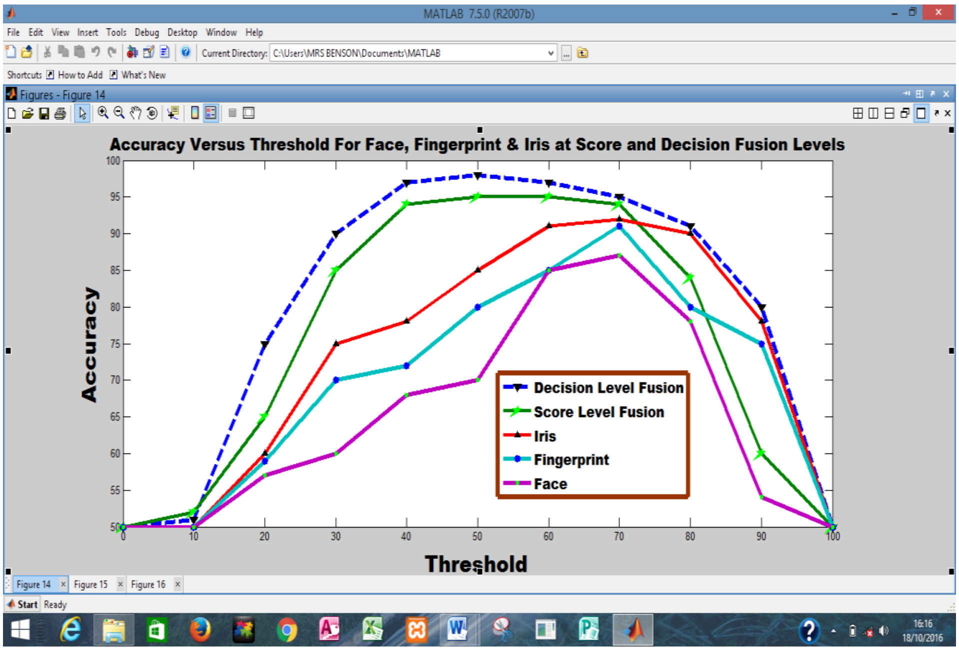


Figure 11: Comparison of Accuracy levels obtained

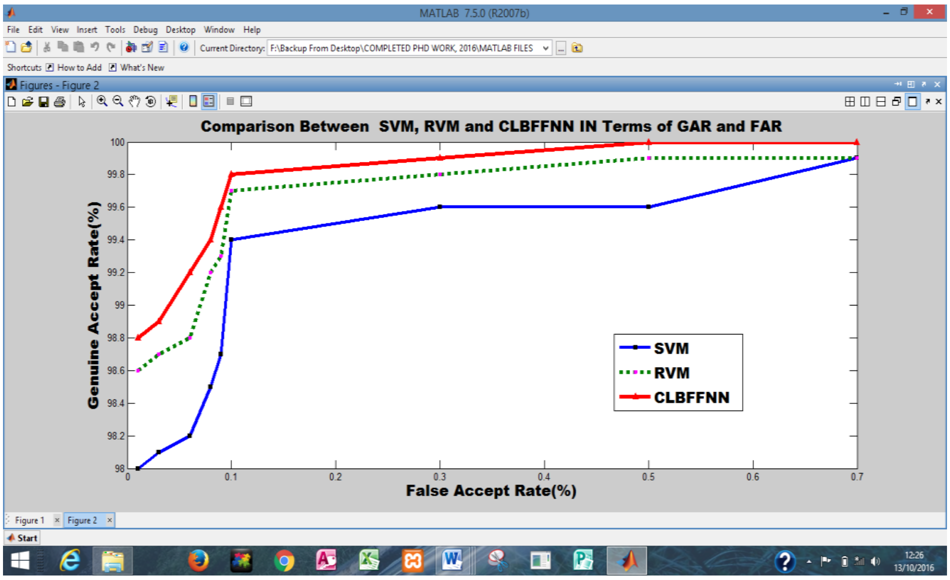


Figure 12: Comparing SVM and RVM Classifiers with CLBFFNN

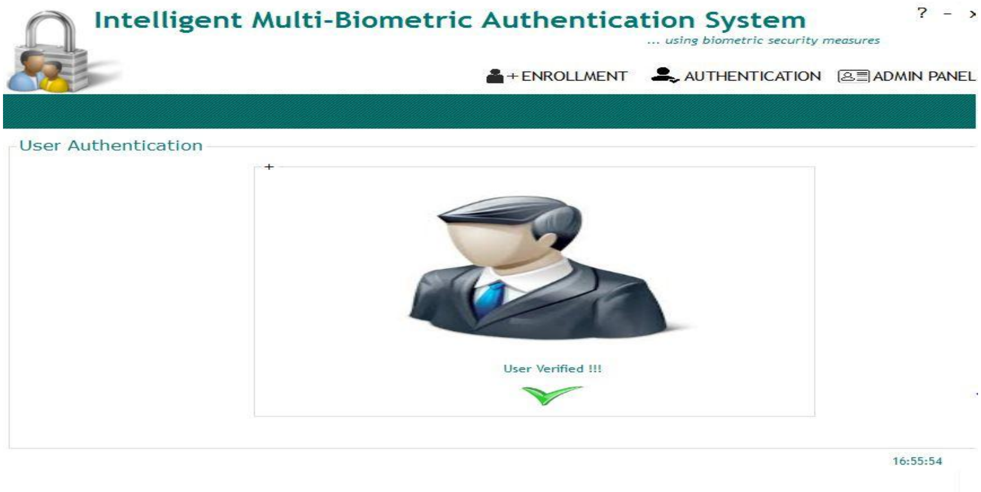
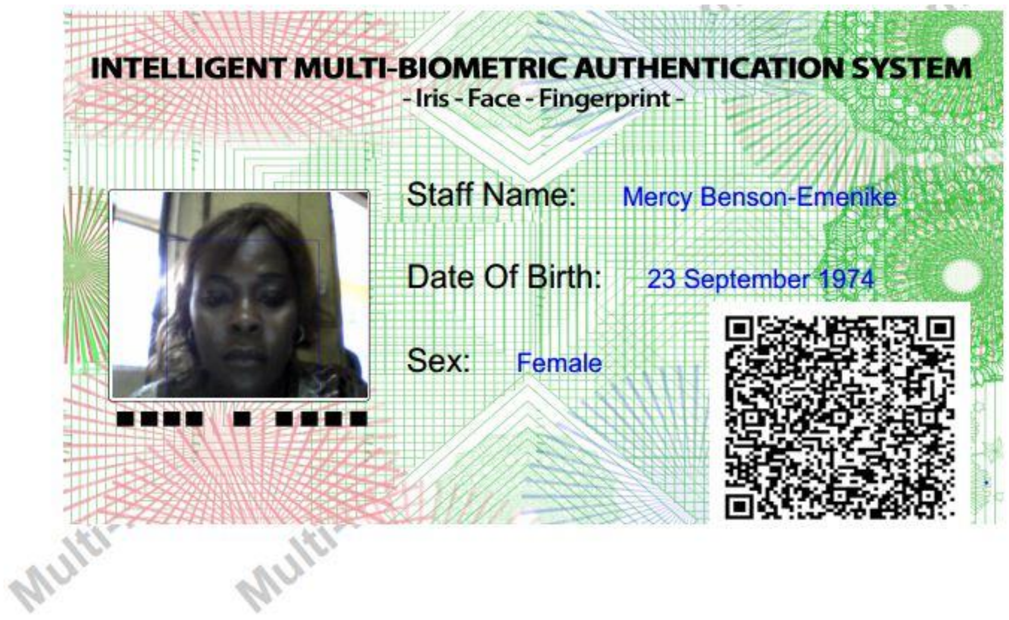

Intelligent Multi-Biometric Authentication System
... using biometric security measures
? – ›
+ ENROLLMENT
AUTHENTICATION
ADMIN PANEL
User Authentication
User Verified !!!
16:55:54

Figure 13: Authentication showing access guaranteed



INTELLIGENT MULTI-BIOMETRIC AUTHENTICATION SYSTEM
- Iris - Face - Fingerprint -

Staff Name: Mercy Benson-Emenike

Date Of Birth: 23 September 1974

Sex: Female

**Figure 14: The ID card with an OCR Barcode**

## 8. CONCLUSION

Security is an all-important phenomenon in the establishment, growth and sustenance of any establishment, organization and society. The use of biometrics has substantially superseded the traditional techniques which have some shortcomings such as one could forget, misplace, lose or steal tokens, since they are not based on natural traits. Biometrics is a division of science that uses computer knowledge to establish human identification or authentication, based on a person's behavioral or physical characteristics.

For secure authentication, this research considers a trimodal multi-biometric authentication system with fingerprint, iris, and face modalities. The implementation involves image capture (i.e. capturing of face poses and iris using webcam and fingerprints using Optical fingerprint scanner); application of efficient pre-processing techniques and neural network training.

A classifier, Cascaded Link-Based Feed Forward Neural Networks (CLBFFNN), which is a feed-forward neural network trained with back propagation algorithm is used. The APIC, PROI and EEF methods were used for iris, fingerprint and face image capture and processing respectively. The system and general recognition performance were evaluated using the following metrics: security, data quality, usability, accuracy, FAR, FRR, FTE, GAR, and throughput. Also, OCR with intelligent barcodes is used to make the system more secure and efficient. Finally, the system when compared with other existing system gives a better recognition performance and accuracy.

## 9. RECOMMENDATIONS

For further study, I recommend, that a special sensor that could combine the image capturing and preprocessing of the three traits simultaneously should be built. This will further increase the recognition time and throughput of the biometric system.

## 10. REFERENCES

[1] *Anissa*, B., Naouar, B., Arsalane, Z., and Jamal, K. (2011). Face detection and recognition using back propagation neural network and Fourier Gabor filters. *Signal & Image Processing:* 2(3): 15-21.

[2] Anjana, P., Revathi, N., and Merlin, M. (2013). Neural network based matching approach for iris recognition. *International Journal of Advanced Research in Computer Science and Software Engineering.* 2(2):618

[3] Annis A. F., Vasuhi S., Teena M. T., Naresh B. N.T., and Vaidehi V. (2013). Person authentication system with quality analysis of multimodal biometrics, 10(6): 2224-3402.

[4] Avinash, P., and Sushma, L. (2010). MERIT: Minutiae Extraction using Rotation Invariant Thinning. International Journal of Engineering Science and Technology 2(7): 3225-3235. csjournals.com/IJCSC/PDF5-1/46.%20komal.pdf

[5] Belghini, N., Zarghili, A., Kharroubi, J., and Majda, A., (2011). Sparse random projection and dimensionality reduction applied on face recognition. *Proceedings of International Conference on Intelligent Systems & Data Processing*, 78-82.

[6] Benson-Emenike, M. E., and Nwachukwu, E.O. (2015): An efficient image preprocessing in an improved intelligent multi biometric authentication system. *International Journal of Applied Information Systems (IJAIS) – ISSN : 2249-0868 Foundation of Computer Science FCS, New York, USA 9 (6): 37-42.*

[7] Chatterjee A., Mandal S., Atiqur Rahaman G. M., and Arif A. M. (2010). Fingerprint identification and verification system by minutiae extraction using artificial neural network. *Signal Processing: Image Communication*, 18, (9), 123-140

[8] Chirchi, E.R., and Waghmare, L.M. (2011). Iris biometric recognition for person identification in security systems. *International Journal of Computer Applications*, 24(9): 0975 – 8887.

[9] Dapinde, K., and Gaganpreet, K. (2013). Level of fusion in multimodal biometrics: A Review. *International Journal of Advanced Research in Computer Science and Software Engineering* 3(2): 242-246.

[10] Daugman, J. (1992). High Confidence Visual Recognition of Persons by a Test of Statistical Independence. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 15, (11), 1148-1161.

[11] Daugman, J. (2012). KeyNote on Iris Recognition. *International Conference on Biometrics(ICB), New Delhi*, 34-40.

[12] Devika, C., Amita, S. and Manish, G. (2013). Recapitulation on Transformations in Neural Network Back Propagation Algorithm. *International Journal of Information and Computation Technology* 3(4): 323-328

[13] Farhat, A., and Zede, H. (2008). Multibiometric systems based verification technique. *Faculty of Engineering, Department of ECE International Islamic, University Malaysia.* 11, (8), 123-135.

[14] Fei, Z. (2006). Embedded face recognition using cascaded structures. Thesis, Technische Universiteit Eindhoven, China.

[15] Gayathri, D., and Uma, R., (2013). Multimodal biometric system: An overview. *International Journal of Advanced Research in Computer and Communication Engineering*, 2(1), 898-902.

[16] Iwasokun, G. B., Akinyokun, O.C., Alese B.K., and Olabode O., (2012). Fingerprint image enhancement: Segmentation to thinning. *(IJACSA) International Journal of Advanced Computer Science and Applications,* 3 (1) 212-269.

[17] Jain, A. K., Bolle, R., Pankanti, S., Ross, A. A., and Nandakumar, K. (2011). Introduction to Biometric. Springer. *IEEE Spectrum*, 22-27.

[18] Khedkar, M. M., and Ladhake, S. A. (2013). Robust human iris pattern recognition system using neural network approach. *IEEE Trans. Patt. Anal. Mach. Int.* 19: 1280-1295

[19] Kirby, M., and Sirovich, L. (1990). Application of Karhunen-Loeve procedure for the characterization of human face. 12(1): 103-108.

[20] Krishna Prasad P. E. S. N., Pavan Kumar K, Ramakrishna M. V. and Prasad B. D. C. N. (2013) Fusion Based Multimodal Authentication In Biometrics Using Context-Sensitive Exponent Associative Memory Model : A Novel Approach Computer Science & Information Technology (CS & IT)Jan Zizka (Eds) : CCSIT, SIPP, AISC, PDCTA – 2013 pp. 81–90, 2013. ©CS & IT-CSCP

[21] Le Cun, V., Bottou, L., Bengio, Y., and Haffner, P., (2012). Handwritten digit recognition with a back propagation network. *Neural Information Processing Systems*, 2: 396-404.

[22] Lee, H. C., and Gaensslen, R.E. (1991). Advances in fingerprint technology. New York: Elsevier. www.worldcat.org/title/advances-in-fingerprint.

[23] Li, S. Z., Hou, X.W., Zhang, H. J. and Cheng, Q. S. (2001). Learning spatially localized, parts-based Representation. *In Proceedings of IEEE Conf. Computer Vision and Pattern Recognition*. 207-212.

[24] Lin-Lin, H., Akinobu, S., Yoshihiro, H., and Hidefumi, K. (2003). Face detection from cluttered images using a polynomial neural network. *Neuro Computing*, 51: 197-211.

[25] Long, B.T., and Thai, H. L., (2015). Person authentication using relevance vector machine (RVM) for face and fingerprint. *I. J. Modern education and Computer Science,* 5, 8-15.

[26] ManiRoja, M., SudhirSawarkar, D. (2013). Iris recognition using orthogonal transform. International Journal of Engineering and Technology (IJET), Dec 2012- Jan. 2013 4(6).

[27] Mohammad, A., Abdelfatah T.and Omaima A., (2013). Integrated system for monitoring and recognizing students during class session. *AIRCC's: International Journal of Multimedia & Its Applications (IJMA),* 5(6): 45-52. Airccse.org/journal/ijma.html

[28] Muhammad, I. R., Rubiyah Y. and Marzuki K. (2010). Multimodal face and finger veins biometric authentication. *International journal of scientific research and essays*, 5(17): 2529-2534.

[29] *Nandakumar, K, Chen, Y, Jain A .K., and Dass, S. C.* (2006). *Quality based score level fusion in multibiometric systems. In Proceedings of IEEE International Conference on Pattern Recognition. Hong Kong; 20 (24): 473-476.*

[30] Nayak, P.K. and Narayan, D., (2013). Multimodal biometric face and fingerprint recognition using adaptive principal component analysis and multilayer perception. *International Journal of Research in Computer and Communication Technology*, 2(6).

[31] Omaima N. A. A. (2014) Review of face detection systems based artificial neural networks algorithms. *The International Journal of Multimedia & Its Applications (IJMA)* 6(1), DOI: 10.5121/ijma.2013.6101 1.

[32] Prakash, N. K. (2010). Face detection using neural network. *International Journal of Computer Applications* (0975 – 8887), 1(14): 36-39.

[33] Pravin, S. P. (2012). Iris recognition based on Gaussian Hermite movement. *International Journal on Computer Science and Engineering (IJCSE),* 4 (11).

[34] Rakesh, T., and Khogare, M. G. (2012). Survey of biometric recognition system for iris. International

Journal of Emerging Technology and Advanced Engineering. 2(6): 2250-2459.

[35] Ratha, N.K. (2010). Privacy protection in high security biometrics applications. In: Ethics and Policy of Biometrics: Lecture Notes in Computer Science #6005, 62–69. Springer-Verlag Berlin Heidelberg.

[36] Reetu, A. and Ingolikar, R. A. (2013). A study of biometrics security system. *International Journal of Innovative Research & Development* April, 2 (4).

[37] Ritu, M. G. (2014). A review on fingerprint-based identification system. *International Journal of Advanced Research in Computer and Communication Engineering* 3(3). Copyright to IJARCCE www.ijarcce.com 5849.

[38] Rashmi, S. and Payal, J., (2012). Multi biometric system: Secure security system. *IJREAS International Journal of Research in Engineering & Applied Sciences* 182 2(2), 2249-3905. http://www.euroasiapub.org

[39] Sawarkar, S.D., Shubhangi V., Shila H., and Taruna S. (2009). Minutiae extraction from ingerprint images. *IEEE International Advance Computing Conference*, 691-696.

[40] Shilbayeh, N. and Al-Qudah, G. (2008). Face detection system based on MLP neural network. *Recent Advances in Neural Networks, Fuzzy Systems & Evolutionary Computing*, 3(8), 238-243.

[41] Shubhangi, D. C., and Manohar, B. (2012). Multi biometric approaches to face and fingerprint biometrics. *International Journal of Engineering Research & Technology* 1(5), 213-229.

[42] Singh, H. and Gayathri, R., (2012). Image authentication technique using Fsim algorithm. *International Journal of Engineering Research and Applications (IJERA)* ISSN: 2248-9622, 2(2), 1129-1133.

[43] Tran B. L., and Le Hoang T. (2012). Hybrid multi-biometric person authentication system. *Proceedings of the World Congress on Engineering and Computer Science, I WCECS*, October 24-26, San Francisco, USA.

[44] Vijaya, S. (2012). A study on the neural network model for finger print recognition. *International Journal of Computational Engineering Research (ijceronline.com)*2 (5).

[45] Virginia, R. A. (2010). Iris-based automatic recognition system based of SIFT features, MSc Thesis, Universidad Autónoma de Madrid Escuela politécnica superior.

[46] Wilson S. and Lenin F. A. (2014). An efficient biometric multimodal face, iris and finger fake detection using an Adaptive Neuro Fuzzy Inference System (ANFIS). *Middle-East Journal of Scientific Research* 22 (6): 937-947.

[47] Yan, Y. and Zang, Y. (2011). Multimodal biometrics fusion using correlation filter bank. *IEEE*, 4(5), 130-148.

[48] Zhang, Q. and Zhang, X. (2010). Research of key algorithm in the technology of fingerprint identification. *Second IEEE International Conference on Computer Modeling and Simulation*, 282-284.

[49] Zhang, D. (2000). Automated biometrics: Technologies and systems. Kluwer and Academic Publishers, USA. ISSN: 1566-0710; 7.

[50] Zhang, Q. and Yan, H. (2004). Fingerprint classification based on extraction and analysis of singularities and pseudo ridges. *Pattern Recognition*, 37 (11): 2233-2243.

[51] Zhao, W., Chellappa, R, and Rosenfeld, A. (2000). Face recognition: A literature survey. Technical Report CAR-TR-948, University of Maryland.

[52] Zhao, W., Chellappa, R., Phillips, P. J., and Rosenfeld, A. (2003). Face recognition: A literature survey. *ACM Computing Surveys*, 35(4): 399-458.