Feature-Fusion Based Biometric Authentication System in Academic Library Access Control

Lukman Opeyemi Abimbola[1], Folasade Muibat Ismaila[2] Wasiu Oladimeji Ismaila[3], [4]Ganiyu Ojo Adigun, Abigail Bola Adetunji[5], Muhammed Okikiola Ismaila[6]
[1,3,5]Department of Computer Science, Faculty of Computing and Informatics,
Ladoke Akintola University of Technology, Ogbomoso, Oyo State, Nigeria
loabimbola@lautech.edu.ng, woismaila@lautech.edu.ng
[2]Department of Information Systems, Faculty of Computing and Informatics,
Osun State University, Osogbo, Osun State, Nigeria.
folaismaila@gmail.com
[4]Department of Library Information Systems, Faculty of Arts and Social Sciences,
Ladoke Akintola University of Technology, Ogbomoso, Nigeria.
goadigun@lautech.edu.ng
[6]Department of Nursing, Fountain University, Osogbo, Nigeria
moismaila@fuo.edu.ng

Abstract- Fingerprint-based authentication systems (FAS) play a crucial role in secure access control, including academic libraries. Conventional fingerprint recognition systems that rely on a single feature extraction technique often struggle to extract robust features, leading to high false positive rates and low accuracy. This research developed a feature-fusion authentication system for academic library access control using multi-feature extraction techniques. 324 university students fingerprint dataset from 81 subjects were captured. The acquired dataset was preprocessed (cropped, contrast adjustment, gray scale, binarization). The Cross Number Algorithm (CNA) and Principal Component Analysis (PCA) were used for feature extraction. The Weighted Sum Rule was used to fuse extracted features from CNA and PCA, generating a unified feature vector. Random Forest Classifier was employed for classification. The results show that CNA–PCA based system achieved accuracy of 96.91%, CNA achieved accuracy of 94.14% and PCA produced accuracy (92.59%).

Keywords Fingerprint-based authentication systems, Academic libraries, Cross Number Algorithm, Principal Component Analysis, Weighted Sum Rule

I. INTRODUCTION

Access control is a security technique that regulates who or what can view or use resources in a computing environment. It is a fundamental concept in security that minimizes risk to the business or organization [21]. Access control is applicable in Automated Teller Machines, Library management system, cybersecurity, etc. A library management system is automated software that streamlines a library's core functions, like cataloging, borrowing, returning books, managing members, and tracking inventory, acting as an integrated system to manage physical and digital resources for efficient, real-time data access, saving time for both librarians and users by automating processes and providing instant search capabilities. A typical Library management network diagram, figure 1, showing multiple computer Systems connected through a library network [6]. The increasing reliance on digital resources in academic libraries has heightened the need for secure and efficient authentication mechanisms to regulate access. Traditional methods, such as passwords and ID cards, are increasingly vulnerable to security breaches, including phishing, theft, and unauthorized duplication [34]. However, recently biometrics have gained the attention of researchers due to their robustness. The authors in [22] and [5] defined biometrics as the automatic recognition of individuals based on their physiological and/or behavioral characteristics.

Biometrics can be behavioral characteristics (e.g. voice, signature, and keystroke) and/or physiological biometrics (finger, Iris, retina, hand, and face) [24] [2]. Due to inadequacies of the traditional methods, biometric authentication has gained prominence as a more reliable alternative due to its inherent uniqueness and difficulty to replicate. Among the various

biometric modalities, fingerprint recognition remains one of the most widely adopted solutions due to its ease of use, cost-effectiveness, and high accuracy in most scenarios [13].

Figure1: Framework of a Library Management System [27]

Fingerprints (as shown in figure 2) are the patterns formed on the epidermis of the fingertip. Fingerprints are made up of a series of ridges and valleys (also called furrows) on the surface of the fingertip and have a core around which patterns like swirls, whorls, loops, or arches are curved to ensure that each print is unique. Fingerprints are the patterns formed on the epidermis of the fingertip. Fingerprints are made up of a series of ridges and valleys (also called furrows) on the surface of the fingertip and have a core around which patterns like swirls, whorls, loops, or arches are curved to ensure that each print is unique [12] [13] [28].

Figure 2: Sample of Fingerprint [12]

Despite its advantages, single algorithm-feature fingerprint authentication systems face several challenges that can compromise their effectiveness. Variations in fingerprint quality, such as dry or wet skin, scars, or partial prints, can lead to false rejections or acceptances [9]. Environmental factors, such as dirt on sensors or poor lighting conditions, and sensor limitations, including low-resolution imaging, further exacerbate these issues. These challenges highlight the need for more robust authentication systems capable of handling diverse conditions while maintaining high accuracy and security.

To address these limitations, feature-fusion authentication has emerged as a promising approach. This method integrates multiple feature extraction techniques to create a more comprehensive and reliable representation of biometric data. By combining features from different algorithms, feature fusion can mitigate the weaknesses of individual methods, resulting in improved recognition accuracy and security [38]. For instance, combining texture-based features with minutiae-based features can enhance the system's ability to handle low-quality fingerprints. Fusion compensates for these limitations by integrating additional biometrics or cascade or hybrid feature extraction techniques, resulting in a system with a higher recognition rate and greater resilience to variations [8]. Fusion in biometric systems, shown in Figure 3, can be categorized into four primary levels, *sensor-level fusion* occurs when raw data from multiple sensors or different biometric traits are combined before feature extraction [20], [25]; *feature-level fusion* which integrates feature sets from different biometrics or hybrid feature extraction methods before the matching process [26], *score-level fusion* in which individual match scores from different sensors or algorithms are combined into

a single score [35]; and *decision-level fusion* combines the final decisions (match or no match) from each modality to arrive at a single authentication decision [4], [16].

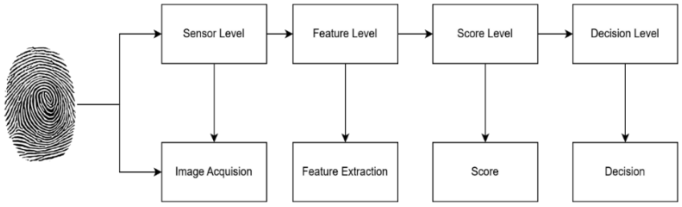

Figure 3. Levels of fusion in Biometric System [20]

This research proposes the development of a Feature-Fusion Authentication System (FFAS) specifically designed for academic library access control. Two primary algorithms are employed for feature extraction: Cross Number Algorithm (CNA) and Principal Component Analysis (PCA). The CNA is particularly effective in extracting minutiae points, such as ridge endings and bifurcations, which are critical for fingerprint recognition [42]. PCA is used to extract features by reduce the dimensionality of the features, ensuring efficient processing without compromising the distinctiveness of the fingerprint data [19]. And to combine the extracted features, the Weighted Sum Rule fusion technique is applied. This method assigns specific weights to each feature based on its reliability and contribution to the overall recognition process, ensuring a balanced and comprehensive representation of the fingerprint data [17].

The rest of the paper is organized as follows: section II contains the related works; section III contains the research materials and method; section IV entails the results and discussion while section V contains the conclusion.

II. Related Works

In recent years, biometric authentication systems have seen significant advancements, with a strong focus on multi-feature extraction and fusion techniques to improve accuracy, security, and reliability. In 2009, the researchers in [39] combined Kernel Principal Component Analysis (KPCA) or Kernel Fisher Discriminate Analysis (KFDA) algorithm, for feature fusion method which were presented and applied to multimodal biometrics based on fusion of ear and profile face biometrics. This system defines the Average rule, Product rule, Weighted-sum rule in kernel-based fusion feature method and USTB database is analyzed. The experimental shows that the recognition rate of KPCA is 94.52% and KFDA is 96.84%, and this method is efficient for feature fusion level. In 2011, authors in [18] proposed improve the accuracy by integrating multiple modal biometrics i.e face and palmprint. The both face and palmprint feature are represent by feature code, namely FPCode. FPCode uses fixed length 1/10 bits coding scheme that is very efficient in matching, and at the same time achieves higher accuracy than other fusion methods available. This approach compares with the Gabor plus PCA and Gabor plus KDRC. Experimental results show that both feature level and decision level strategies achieve much performance with the accuracy of 91.52% and 91.63%. in 2012, researchers in [38] discusses a new patron authentication approach in an automated and modern library based on the biometric recognition. The person working at the entrance or at the circulation desk of the library needs to either confirm or determine the identity of an individual requesting service in library. The purpose of such authentication system is to ensure that the rendered services are accessed only by a valid user, and not any. The authors of [32] in 2019 proposed system uses face recognition for entering and getting the details of an end user. Through this application, the book gets issued to the end-user by identifying the user with the help of face recognition and identifying the book using barcode capture. The proposed face recognition system gave 99.38% accurate.

In 2020, the researchers in [27] purposed secure library transaction supported on fingerprint recognition. The academic libraries can make use of the advantage of the fingerprint recognition technology. The registered person is identified by matching their fingerprint ridge and transaction details along with the due dates are sent to the registered mobile number. This

system is developed using fingerprint. Arduino Mega microcontroller. In 2021, [41] researchers proposed a multi-modal biometric authentication system that combined facial and iris recognition. The authors used a Convolutional Neural Networks for feature extraction and Recurrent Neural Networks for temporal feature fusion. The system was trained on two well-known datasets: the CASIA-IrisV4 dataset for iris images and the Celeb A dataset for facial images. The results showed an impressive accuracy of 98.7% in individual authentication. Also in 2021, [18] developed a biometric authentication system that fused fingerprint and palm print modalities at the feature level. The authors used a hybrid feature extraction technique, combining Gabor filters and Local Binary Patterns, to extract unique features from both fingerprints and palm prints. Support Vector Machine algorithm was employed for classification. The system was evaluated on the FVC2004 fingerprint dataset and the Poly U palm print dataset, achieving an accuracy of 97.3%. While a study by [23] in 2022 focused on developing a feature-fusion authentication system specifically for library access control. The system combined three biometric modalities: face, fingerprint and voice. The authors used a deep learning framework with Convolutional Neural Networks for feature extraction and a decision tree algorithm for classification. The system was trained on a custom dataset of 200 users, achieving an accuracy of 98.2%.

In 2022, authors in [30] introduced a continuous authentication system that relied on behavioral biometrics, such as keystroke dynamics and mouse movement patterns. The authors used a machine learning approach, with feature extraction based on time-series analysis and classification using Random Forest algorithms. The system was tested on a dataset of 100 users, achieving an accuracy of 96.8%. In 2024, the researches in [7] proposes a continuous authentication system using multimodal biometrics based on face and keystroke dynamics. A novel Adaptive Weighted Sum Score Fusion approach is introduced, which considers environmental factors and the user's profile in addition to the biometrics employed in the decision process. The proposed system is assessed and determined to be non-intrusive and user-friendly, achieving a 3.02% equal error rate. The authors in [37], 2025, proposed a large-scale feature extraction method based on the correlation analysis of two physicochemical properties of amino acids: hydrophobicity and hydrophilicity, as well as the correlation between amino acids. The new approach to feature extraction is OTE-24 approach and Random Forest is used for classification. The results of this research, evaluated using databases commonly utilized in previous studies, show an accuracy improvement of over 2.58% compared to existing methods.

III. Materials and Method

1. Materials

This section entails the techniques used for this work which include Principal Component Analysis (PCA), Cross Number Algorithm (CNA), weighted sum algorithm (WSA) and Random Forest (RF).

A. PCA

PCA is a widely used statistical technique for dimensionality reduction and feature extraction. It transforms high-dimensional data into a lower-dimensional space while preserving as much variance as possible. This is particularly beneficial in biometric systems, such as fingerprint and facial recognition, where data can be high-dimensional and computationally intensive to process [14]. Several researchers have used PCA for feature extraction in face recognition, computer vision etc. [10]; [1], [36]. The pseudocode of PCA algorithm is shown in algorithm 1.

The researches employed PCA for feature extraction because it lacks redundancy of data given the orthogonal components; reduced complexity in images' grouping with the use of PCA; produces smaller database representation since only the trainee images are stored in the form of their projections on a reduced basis and reduces noise since the maximum variation basis is chosen and so the small variations in the background are ignored automatically [29].

A. CAN

The CNA is a feature extraction technique particularly relevant in the context of biometric recognition systems. This algorithm is designed to capture distinct features from biometric data, such as fingerprints, through a methodical approach to pattern recognition and classification.

The CNA operates on the principles of spatial frequency analysis, which allows it to discern fine details in biometric patterns. [26]

Algorithm 1: Pseudocode of PCA [36]

Begin

Step 1: Normalize each feature independently to a scale of -1 to 1 using the mean and standard deviation of the values incurred for the feature; generate the $n(n\text{-}1)/2$ x 4 normalized dataset

Step 2: Determine the 4 x 4 Covariance matrix of the four features
The covariance matrix has entries corresponding to the Pearson's correlation coefficient for the features

Step 3: Determine the four Eigenvalues $\lambda_1, \lambda_2, \lambda_3, \lambda_4$ and the corresponding four Eigenvectors (one Eigenvector for each Eigenvalue). Each Eigenvector is of dimensions 4 x 1, where 4 corresponds to the number of features in the dataset. Let $\sigma_1^2, \sigma_2^2, \sigma_3^2, \sigma_4^2$ be the variances of these four Eigenvectors.

Step 4: Generate the four principal components PC_1, PC_2, PC_3 and PC_4
PC_1 = [$n(n\text{-}1)/2$ x 4 normalized dataset] X [4 x 1 Eigenvector corresponding to the Eigenvalue λ_1]
PC_2 = [$n(n\text{-}1)/2$ x 4 normalized dataset] X [4 x 1 Eigenvector corresponding to the Eigenvalue λ_2]
PC_3 = [$n(n\text{-}1)/2$ x 4 normalized dataset] X [4 x 1 Eigenvector corresponding to the Eigenvalue λ_3]
PC_4 = [$n(n\text{-}1)/2$ x 4 normalized dataset] X [4 x 1 Eigenvector corresponding to the Eigenvalue λ_4]

Step 5: Compute the principal components-based weighted average score for each of the $n(n\text{-}1)/2$ node pairs, by using the variances of the principal components as weights

$$LP_{Avg}^{PC} \quad v) = \frac{\sigma_1^2}{} \left(\frac{PC_1 \quad v + \sigma_2^2 \quad PC_2 \quad v + \sigma_3^2 \quad PC_3 \quad v + \sigma_4^2 \quad PC_4 \quad v)}{\sigma_1^2 + \sigma_2^2 + \sigma_3^2 + \sigma_4^2} \right.$$

return LP_{Avg}^{PC} scores for the node pairs

End

The core of the CNA lies in its ability to extract features from the preprocessed images. This is done by analyzing the orientation and frequency of patterns within the biometric data. Specifically, the algorithm utilizes the concept of cross-number features, which are calculated based on the pixel connectivity in the fingerprint. The cross-number for a pixel is defined as the number of neighboring pixels that meet a certain criterion, such as a specific intensity level [28]. This can be mathematically represented as:

$C(x, y) = \sum_{i=1}^{n} f(i, j)$ (2.5)

Where $\mathrm{C(x, y)}$ is the cross-number feature at pixel (x, y), and $f(i, j)$denotes the neighboring pixel values.

B. WSA

The Weighted Sum method is a widely used scalarization method in Multi-Objective Optimization (MOO) in Computer Science. It involves assigning positive real values, called weights, to each objective, and then taking the weighted sum of the objectives. This method is easy to implement and maintains the same level of complexity as the original MOO problem. However, the selection of weights requires expert knowledge and can introduce bias in the generated Pareto points. Alternatively, random weight vectors can be used to explore multiple search directions [7] Several researchers have employed WSM for feature fusion mechanism like [7] [39]. The pseudocode of WSM is in Algorithm 2.

C. Random Forest

A Random Forest (RF) classifier consists of multiple decision trees that operate as an ensemble to improve classification accuracy. Each tree in the forest independently classifies an input sample, and the final classification result is determined by aggregating the predictions from all trees [15], [33]. The pseudocode of RF is in Algorithm 3.

Random Forest has relevant features like handles missing data, works well with big and complex data; and can be used for different tasks which make it useful for classification problems [17] [11].

Algorithm 2: The pseudocode of WSM [7]

Inputs:
$votes$: array of votes from each source
W: array of weights for each source
Outputs:
$decision$: category voted by the algorithm
$W \leftarrow \alpha_0$; ▷ Initialize weights
for every new measure **do**
Weighted majority:
for all $s \in$ sources **do**
$contributions(s) \leftarrow W(s) * votes(s)$;
end for
$decision \leftarrow$ max_index($contributions$);
Update weights:
for all $s \in$ sources **do**
if $decision = votes(s)$ **then**
$W(s) = W(s) + \delta_+$;
else
$W(s) = W(s) - \delta_-$;
end if
end for
end for

Algorithm 3. The pseudocode of RF [40]

Input: *N - Quantitative amount of bootstrap samples*
M - Total number of features
m - Sample size
k - Next node
Output: A Random Forest (RF)
Steps:
*1. **Creates** N bootstrap samples from the dataset.*
2. Every node (sample) takings a feature randomly of size m where m<M.
3. Builds a split for the m features selected in Step 2 and detects the k node by using the best split point.
4. Split the tree iteratively until one leaf node is attained and the tree remains completed.
5. The algorithm is trained on each bootstrapped independently.
6. Using trees classification voting predicted data is collected from the trained trees (n).
7. The final RF model is build using the peak voted features.
*8. **return** RF*
End.

D. **Performance Evaluation**

The performance of the Library based FFAS system was evaluated based on metrics viz: as accuracy, precision, sensitivity, specificity, false positive rate, and recognition time [12].

$$Sensitivity = \frac{TP}{FN + TP} x\ 100 \quad (1)$$

$$Specificity = \frac{TN}{TN + FP} x\ 100 \quad (2)$$

$$False\ Positive\ Rate = \frac{FP}{TN + FP} x\ 100 \quad (3)$$

$$Precision = \frac{TP}{FP+TP} \times 100 \quad (4)$$

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN} x\ 100 \quad (5)$$

2. Method

This work involves a combination of image preprocessing, feature extraction using the Cross Number Algorithm (CNA) and Principal Component Analysis (PCA), feature fusion through the Weighted Sum Rule, and classification using a Random Forest Classifier. The architecture

of developed Feature-Fusion Based Fingerprint Authentication system (FFAS) is shown in figure 4.

The Architecture of FFAS

The development of the Fingerprint Fusion-Based Authentication System (FFAS) involve multiple stages designed to enhance accuracy, security, and reliability in academic library settings. These stages are as follows:

A. Fingerprint Acquisition

In this research, some students of Ladoke Akintola University of Technology, Ogbomoso, Nigeria were captured and used, which consists of 324 fingerprint images from 81 subjects. The dataset includes labels for gender, hand, and finger name, along with synthetically altered versions that incorporate three levels of alteration: obliteration, central rotation, and z-cut.

B. Fingerprint Preprocessing

The fingerprint images underwent preprocessing to enhance their quality and remove noise, ensuring accurate feature extraction. The preprocessing steps include:

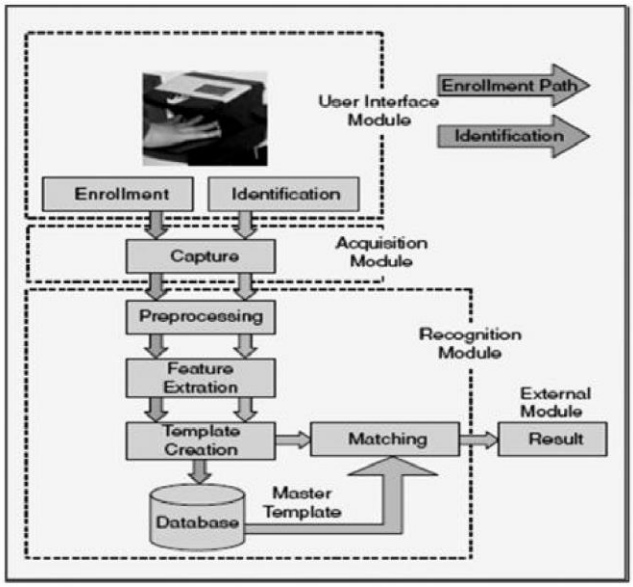

Figure 4: Architecture of the developed FFAS

Contrast Enhancement The contrast of fingerprint images was improved by using adaptive histogram equalization. This technique adjusts the brightness of pixels in small sections of the image, making it easier to see details like ridges and valleys.

Color Space Conversion The images were converted from RGB to YCbCr color space to emphasize fingerprint features without unnecessary color information. The Y (luminance) channel, which focused on brightness variations critical for distinguishing fine details in the fingerprint pattern.

Morphological Operations like erosion and dilation were removed. These processes preserved critical ridge details while removing isolated noise pixels, enhancing the fingerprint structure's integrity for more accurate analysis.

Binarization the grayscale images were converted into a binary format. This binarization step transformed each pixel value into either black or white, based on T, simplifying the image and highlighting essential fingerprint features. Mathematically, binarization is represented as follows.

$$I_b(x,y) = \begin{cases} 0, & if\ I(x,y) < T \\ 1, & if\ I(x,y) \geq T \end{cases} \qquad (6)$$

where $I(x,y)$ is the grayscale intensity at pixel location(x,y), and $I_b(x,y)$ represents the binary output. Otsu's algorithm may be employed to compute T, ensuring an optimal threshold based on the image histogram.

C. Feature Extraction

Relevant features of the fingerprint images were extracted using CNA and PCA. CNA feature extraction method was applied to analyze ridge patterns, bifurcations, and minutiae points in fingerprint images. These extracted features provide crucial biometric markers for authentication. After extracting features using CNA and PCA, the weighted Sum Rule was used to combine them into a unified feature vector.

Feature Extraction Using CNA

Feature extraction utilizes CNA, which is widely regarded as an effective approach to identifying ridge endings and bifurcations, or minutiae, in fingerprint images. This algorithm computes the number of transitions from 0 (background) to 1 (ridge) in each pixel's 8-neighborhood. Letting $p_1, p_2, \ldots . p_8$ represent these neighborhood pixels in a clockwise sequence, the cross number $CN(x, y)$ at pixel (x, y) is calculated as.

$$CN(x, y) = \frac{1}{2}\sum_{i=1}^{8} |p_i - p_i + 1| \qquad (7)$$

where $p_i + 1 = p_1$ completes the loop. This calculation yields a crossing number of one for ridge endings and three for bifurcations, allowing CNA to isolate these features effectively.

Feature Extraction Using PCA

Principal Component Analysis (PCA) reduces the dimensionality of the feature set while retaining the most significant information, streamlining the classification process Detail steps is as follows.

Step 1: Standardization of Features

Before PCA, it's essential to standardize the feature matrix $X = \{x_1, x_2, \ldots . , x_p\}$, ensuring each feature has a mean of zero and a unit variance (Duda *et al.*,, 2000). This standardized matrix Z is computed as:

$$Z = \frac{X - \mu}{\sigma} \qquad (8)$$

where μ and σ are the mean and standard deviation of each feature.

Step 2: Covariance Matrix Calculation

PCA relies on the covariance matrix Σ of Z , calculated as:

$$\sum = \frac{1}{N - 1} Z^T Z \qquad (9)$$

where N is the number of samples. This matrix captures feature correlations, providing the basis for variance maximization.

Step 3: Eigenvalue and Eigenvector Computation

Eigenvalues $\lambda_1, \lambda_2, \ldots . \lambda_p$ eigenvectors $\mathrm{v}_1, \mathrm{v}_2, \ldots \mathrm{v}_\mathrm{p}$ are then derived from Σ, with eigenvectors indicating principal component directions and eigenvalues representing variance contributions. The explained variance ratio for a principal component k is

$$Explained\ Variance\ Ratio = \frac{\lambda k}{\sum_{i=1}^{p} \lambda_i} \qquad (10)$$

Step 4: Selecting Principal Components

Principal components are selected to explain at least 95% of the total variance, ensuring that the essential feature variance is retained. This threshold is represented by:

$$\sum_{i=1}^{m} \lambda_i \geq 0.95 \cdot \sum_{i=1}^{p} \lambda_i \qquad (11)$$

where m is the number of components retained.

Step 5: Feature Transformation

The data matrix Z is then transformed into a new feature space using the selected eigenvectors V_m, yielding the transformed matrix Z_{new}

$$Z_{new} = Z \cdot V_m \quad (12)$$

where $V_m$contains the eigenvectors for the top mmm components. This reduced-dimensionality matrix Z_{new} is then ready for classification.

Fusion of CAN and PCA The Weighted Sum Rule is an effective method for fusing features in multi-modal biometric systems. This fusion technique combines features from different extraction methods to enhance recognition accuracy and system robustness. In this work, fuse features obtained from the Cross Number Algorithm (CNA) and Principal Component Analysis (PCA), balancing their contributions to achieve optimal fingerprint recognition.

After normalization, the Weighted Sum Rule is applied to combine features from CNA and PCA. Each feature set is assigned a weight, reflecting its contribution to the overall system performance. Let $F_{CNA}\ and\ F_{PCA}$ represent the feature vectors from Cross Number Algorithm and PCA, respectively. The weighted fusion feature $F_{fussion}$ is computed as.

$$F_{fussion} = \omega_{CNA} \cdot F_{CNA} + \omega_{PCA} \cdot F_{PCA} \quad (13)$$

where $\omega_{CNA}\ and\ \omega_{PCA}$ are weights assigned to the CNA and PCA feature sets, respectively, and $\omega_{CNA} + \omega_{PCA} = 1$. These weights can be chosen based on experimental results or system requirements, ensuring an optimal balance between the different features.

The weights are tuned by evaluating the recognition accuracy and other performance metrics of the system under different weight combinations. A common approach is to perform cross-validation on the training dataset, testing several values for $\omega_{CNA}\ and\ \omega_{PCA}$ and selecting the combination that maximizes performance metrics.

E. **Classification stage**

The fused fingerprint feature vector was classified using a Random Forest Classifier, a machine learning algorithm known for its high accuracy and robustness in biometric authentication tasks. The classification process involved training phase where the classifier was trained using the preprocessed and feature-fused fingerprint dataset, testing phase where the model was evaluated using acquired fingerprint samples to measure its recognition accuracy**,** sensitivity**,** and false positive rate. This classification step ensure that the FFAS system correctly identifies users based on their fingerprints.

E. Performance Evaluation of the Developed FFAS

To evaluate the effectiveness of the developed Fingerprint Fusion-based Authentication System (FFAS) for library applications, various performance metrics were calculated. These metrics include recognition accuracy, precision, sensitivity (or recall), specificity, false positive rate, and computation time. A confusion matrix was used to summarize the classification performance of the system, which consists of the following components; True Positive, TP, (*The number of cases where the system correctly identifies a fingerprint as belonging to a registered user;* False Positive, FP, (*Instances where the system incorrectly identifies an unregistered fingerprint as belonging to a registered user*); True Negative, TN, (*The number of cases where the system correctly identifies an unregistered fingerprint*); False Negative, FN, (*Cases where the system fails to recognize a registered fingerprint and incorrectly identifies it as unregistered*).

IV. Results and Discussion

Figure 5 presents the graphical user interface, GUI, of the developed Feature-Fusion Fingerprint Authentication System implemented in MATLAB R2024b. The interface was designed to provide an intuitive and user-friendly environment where fingerprint images could be trained, tested, and authenticated efficiently. It includes modules for loading and cropping fingerprint samples, selecting feature extraction methods, and displaying results of library access control systems.

The developed FFAS was implemented using a total fingerprint dataset of 1,080 images. Out of this, 70% of the dataset was used for training, while the remaining 30% was used for testing, employing a random sub-sampling cross-validation method.

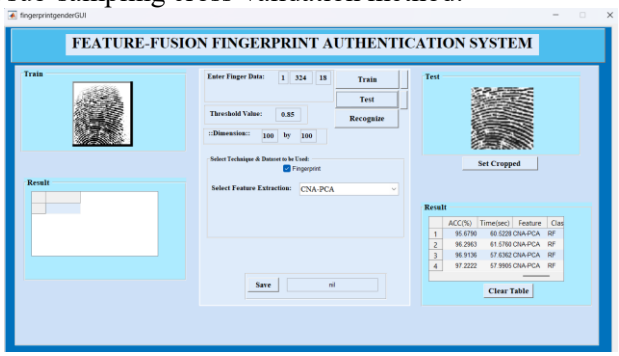

Figure 5: GUI of the developed FFAS

The results presented in Table 1 illustrate the performance of the developed Feature-Fusion Authentication System (FFAS) when using the Cross Number Algorithm (CNA) as the sole feature extraction technique. The results showed that at 0.20 threshold. the CNA-RF generated 12.96%, 96.76%. 87.04%, 93.72%,93.52%, in 77.93 msec for FPR, SEN, SPEC, PREC, ACC and C_time respectively; at threshold of 0.35, the CNA-RF generated 11.11%, 96.30%. 88.89%, 94.55%, 93.83%, in 74.65 msec for FPR, SEN, SPEC, PREC, ACC and C_time respectively; at 0.5 threshold, the CNA-RF generated 9.26%, 95.83%. 90.74%, 95.39%, 94.14%, in 74.24 msec for FPR, SEN, SPEC, PREC, ACC and C_time respectively; and at 0.85 threshold, the CNA-RF generated 6.48%, 95.37%. 93.52%, 96.71%, 94.75%, in 77.77 msec for FPR, SEN, SPEC, PREC, ACC and C_time respectively.

Table 1: Results of the CNA-RF based FFAS System

Threshold	FPR (%)	SEN (%)	SPEC (%)	PREC (%)	ACC (%)	C_Time (sec)
0.20	**12.96**	**96.76**	**87.04**	**93.72**	**93.52**	**77.93**
0.35	**11.11**	**96.30**	**88.89**	**94.55**	**93.83**	**74.65**
0.50	**9.26**	**95.83**	**90.74**	**95.39**	**94.14**	**74.24**
0.85	**6.48**	**95.37**	**93.52**	**96.71**	**94.75**	**77.77**

The results presented in Table 2 illustrate the performance of the developed Feature-Fusion Authentication System (FFAS) when using the Principal Component Analysis (PCA) as the sole feature extraction technique. The results showed that at 0.20 threshold. the PCA-RA generated 16.67%, 95.37%, 83.33%, 91.96%, 91.36%, in 82.06 msec for FPR, SEN, SPEC, PREC, ACC and C_time respectively; at threshold of 0.35, the PCA-RA generated 13.89%, 94.91%. 86.11%, 93.18%, 91.98%, in 80.78 msec for FPR, SEN, SPEC, PREC, ACC and C_time respectively; at 0.5 threshold, the PCA-RA generated 11.11%, 94.44%. 88.89%, 94.44%,92.59%, in 84.92 msec for FPR, SEN, SPEC, PREC, ACC and C_time respectively; and at 0.85 thresholds, the PCA-RA generated 9.26%, 93.98%. 90.74%, 95.31%, 92.90% in 84.11 msec for FPR, SEN, SPEC, PREC, ACC and C_time respectively.

Table 2: Performance of PCA-RF based FFAS

Threshold	FPR (%)	SEN (%)	SPEC (%)	PREC (%)	ACC (%)	C_Time (msec)
0.20	16.67	95.37	83.33	91.96	91.36	82.06
0.35	13.89	94.91	86.11	93.18	91.98	80.78
0.50	11.11	94.44	88.89	94.44	92.59	84.92
0.85	9.26	93.98	90.74	95.31	92.90	84.11

The results presented in Table 3 illustrate the performance of the developed Feature-fusion Authentication System (FFAS) when using CNA-PCA-RF with WSA as fusion feature

extraction technique. The results showed that at 0.20 threshold. the CNA-PCA-RF generated 10.19%, 98.61%, 89.81%, 95.09%, 95.68%, in 60.52 msec for FPR, SEN, SPEC, PREC, ACC and C_time respectively; at threshold of 0.35, the CNA-PCA-RF generated 7.41%, 98.15%. 92.59%, 96.36%, 96.30%, in 61.58 msec for FPR, SEN, SPEC, PREC, ACC and C_time respectively; at 0.5 threshold, the CNA-PCA-RF generated 4.63%, 97.69%. 95.37%, 97.69%, 96.91%, in 57.64 msec for FPR, SEN, SPEC, PREC, ACC and C_time respectively; and at 0.85 thresholds, the CAN-PCA-RA generated 2.78%, 97.22%. 97.22%, 98.59%, 97.22% in 57.99msec for FPR, SEN, SPEC, PREC, ACC and C_time respectively. Figures 6 – 11 show the graphs of FPR, Sensitivity, Specificity, Precision, Accuracy and Computational time of CNA-PCA-RF, CNA-RF and PCA-RF based FFAS techniques.

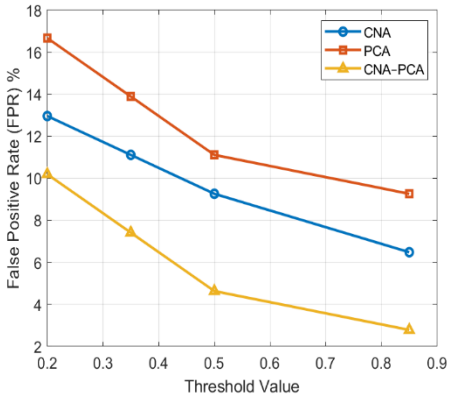

Figure 6: Graphs of FPR VS Thresholds

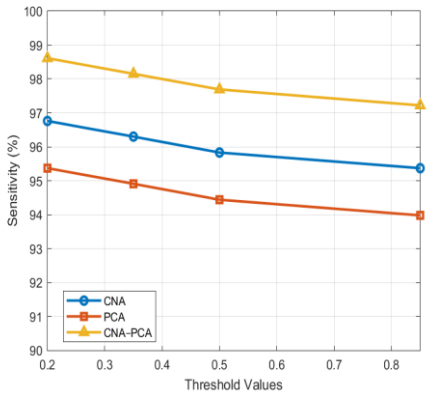

Figure 7: Graphs of Sensitivity Vs Thresholds

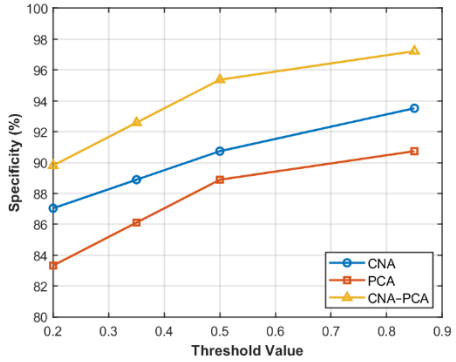

Figure 8: Graphs of Specificity Vs Thresholds

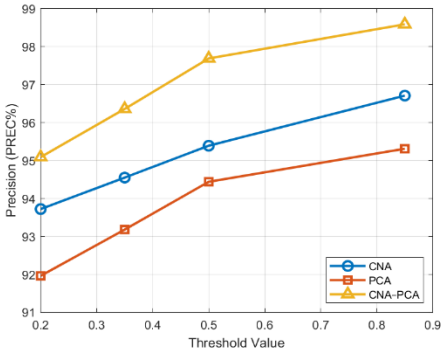

Figure 9: Graphs of Precision Vs Thresholds

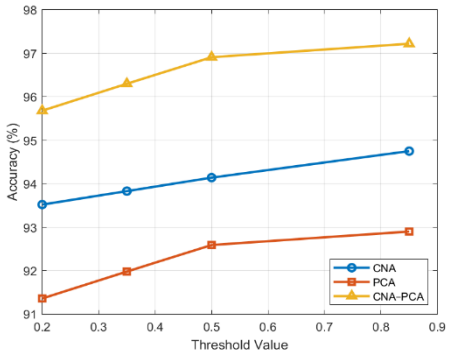

Figure 10: Graphs of Accuracy Vs Thresholds

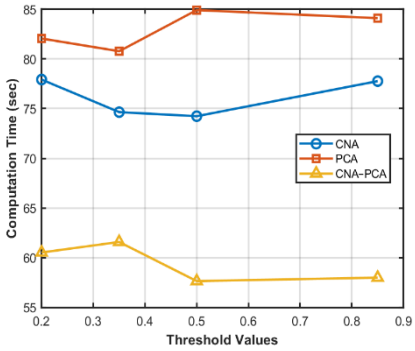

Figure 11: Graphs of Computation Time Vs Thresholds

Interpretation of results

As stated in Table 1, 2 and 3, adopting optimum values at 0.5 threshold, it could be deduced that:
(i) In case of FPR, the results showed that CNA-PCA-RF yielded a lesser FPR than CNA-RF and PCA-RF. this implies that CNA-PCA-RF is less prone to false positive error in than CNA-RF and PCA-RF.
(ii) In case of Sensitivity, the results showed that CNA-PCA-RF has higher recall than CNA-RF and PCA-RF which implies that CNA-PCA-RF has the ability to identify the presence of images (true positives) in the database.
(iii) In case of Specificity: the results showed that CNA-PCA-RF has higher specificity than CNA-RF and PCA-RF, which implies that CNA-PCA-RF has the ability to identify the absence of images (true negatives) in the database.;
(iv) In case of Precision: the results showed that CNA-PCA-RF produced higher precision than CNA-RF and PCA-RF, this implies that CNA-PCA-RF has better positive predictive capability.
(v) In case of Accuracy, the results showed that CNA-PCA-RF gave higher value than both CNA-RF and PCA-RF. this implies that CNA-PCA-RF has the ability to identify the presence and absence of images (true negatives and true positives) in the database.
(vi) In case of Computation Time, the results showed that CNA-PCA-RF gave lesser value than both CNA-RF and PCA-RF. this implies that CNA-PCA-RF has the ability to identify the presence and absence of images (true negatives and true positives) in the database in a shortest time.

V. Conclusion

This study successfully developed a Feature-Fusion Authentication System (FFAS) for library access control using a combination of Cross Number Algorithm (CNA) and Principal Component Analysis (PCA) techniques. The integration of these feature extraction methods significantly enhanced the system's performance by improving recognition accuracy, computational efficiency, and robustness against variations in fingerprint patterns. Experimental results demonstrated that the CNA–PCA fusion model consistently outperformed single-method approaches, achieving higher accuracy and faster processing time across multiple threshold values. Furthermore, the successful implementation of the FFAS underscores the potential of combining multiple feature extraction algorithms to overcome the limitations of individual techniques. The system's high recognition rate and reduced false acceptance and rejection rates make it suitable for practical deployment in real-world library systems and biometric related applications.

VI. Acknowledgement

I acknowledge the Tertiary Trust Fund (TETFUND) Nigeria for sponsoring this research work and publication.

References

[1] Afolabi A. O. and Adagunodo R. (2012). Implementation of an Improved Facial Recognition The algorithm in a Web-based Learning System, *International Journal of Engineering and Technology* 2(11), 1885-1892.
[2] Afolabi A.O., Falohun A.S., Adedeji O.T. (2019). Securing E-Library System with Bimodal Biometric Technique. Annal Biostatistics & Biometric Applications. Vol 3 Issue 5. 1-7.
[3] Ahmed, S., Rahman, T., and Khan, M. (2022). Multi-modal biometric authentication for library access control. *International Journal of Biometrics, 11*(4), 112-125.
4] Ahmad, T., Patel, R., and Khan, M. (2021). Decision-level fusion in biometric systems: A review. *Biometric Technology Today, 7*(3), 89-103.
[5] Al-juboori A. M, Bui W., Wu X. and Zhao Q. (2013). Palm Vein VerificationUsing Gabor Filter, *IJCSI International Journal of Computer Science Issues*, 10(1), 678-684.
[6] Atul M Gonsai And Nilesh N Soni (2007). Biometric Authenticated Library Network Model for Information Sharing. International Caliber -2007, Panjab University, Chandigarh, 08-10 491-499.
[7] Ayeswarya S. and John Singh K. (2024). FacekeyID: an adaptive weighted sum score based fusion framework for continuous user authentication, Engineering Research Express.
[8] Bhatia, R., and Purohit, S. (2020). Biometric systems: Physiological and behavioral traits. *International Journal of Security Studies, 9*(1), 23-37.
[9] Chen, X., Wang, Y., and Zhang, L. (2023). Fingerprint quality variations and their impact on authentication systems. *Biometric Technology Today, 8*(4), 112-125.
[10] Deepesh Raj (2011). A Realtime Face Recognition system using PCA and various Distance Classifiers, Computer vision and processing. 5(3), 15-22.
[11] Fangfang Dong (2024). Random Forest Algorithm for HR Data Classification and Performance

Analysis in Cloud Environments. *(IJACSA) International Journal of Advanced Computer Science and Applications,* Vol. 15, No. 11, 501-510.
[12] Ismaila W. O., Ismaila Folasade M, Falohun Adeleye S (2017): Soft Computing Approach to Multi-Modal Biometric System, American International Journal of Research In Science, Technology, Engineering & Mathematics, 20(1), 66-72. India.
[13] Johnson, R., and Lee, S. (2022). Fingerprint recognition: A cost-effective solution for secure access control. *Journal of Biometric Engineering, 7*(1), 23-37.
[14] Jain, A., Ross, A., and Prabhakar, S. (2020). Principal Component Analysis in biometric systems. *Journal of Computational Biometrics, 6*(3), 112-128.
[15] Jose-Luis S-R, Jimenez-Cruz R., Villuendas-Rey Y., Yanez-Marquez (2023). Random Forest algorithm for the classification of Spectral Data of Astrnomical Objects. Algorithms. 16(6), 293.
[16] Kisku, D., Nandakumar, K., and Jain, A. (2021). Template storage and encryption in biometric systems. *Journal of Biometric Engineering, 7*(4), 89-103.
[17] Kumar, P., and Singh, S. (2023). Weighted sum rule fusion for improved biometric recognition. *Biometric Systems Review, 11*(3), 45-60.
[18] Kumar, A., and Singh, R. (2021). Hybrid feature extraction for fingerprint and palmprint recognition. *International Journal of Biometrics, 10*(3), 67-82.
[17] Kumar, P., and Singh, S. (2023). Weighted sum rule fusion for improved biometric recognition. *Biometric Systems Review, 11*(3), 45-60.
[18] Linlin Shen, Li Bai, and Zzhen J.i. (2011). " FPCODE: An efficient approach for multi-modal biometrics", Intern.l Journal of Pattern Recognition and Artificial Intelligence, 25(2) 273-286.
[19] Li, H., Zhang, W., and Wang, Y. (2021). Dimensionality reduction in fingerprint feature extraction using PCA. *Journal of Computational Biometrics, 5*(2), 112-128.
[20] Malathi, R., and Sudha, V. (2019). Sensor-level fusion in biometric systems. *Journal of Biometric Research, 5*(1), 34-50.
[21]Margaret Rouse 2019: https://searchsecurity.techtarget.com/definition/biometrics.
[22] Mote P. and Zope P.H. (2012). Multimodal Biometric system using Gabor Filter, International *Journal of Advanced Trends in Computer Science and Engineering,* Volume 1, No.2,
[23] Ramesh M. R. (2012). Biometric Recognition: A New Approach for Library Patron Authentication. *International Journal of Library Science* 2012, 1(5): 72-74
[24]Patil, S., and Shinde, G. (2022). Biometric applications in academic libraries. *Library Hi Tech, 40*(2), 345-360.
[25] Patil, S., and Shinde, V. (2022). Cross Number Algorithm for fingerprint feature extraction. *Journal of Biometric Engineering, 8*(3), 112-125.
[26] Pandey, S., Thakur, R., and Kumar, A. (2021). Feature-level fusion using Principal Component Analysis. *Journal of Computational Biometrics, 7*(1), 23-37.
[27] Pandija S, Ramanathan N, Subashinee S, Vignesh J, Mythili E (2020). Library Management System Using Fingerprint Recognition, *International Journal of Innovative Research In Technology*, vol. 6 Issue 12. 566-570.
[28] Patil, S., and Shinde, V. (2022). Cross Number Algorithm for fingerprint feature extraction. *Journal of Biometric Engineering, 8*(3), 112-125.
[29] Phillips P. J., Flynn P. J., Scruggs T., Bowyer K. W., Chang J., Hoffman K., J. Marques, J. Min and W. Worek, "Overview of the Face Recognition Grand Challenge," *in Computer vision and pattern recognition,* 2005. CVPR 2005. IEEE Computer Society Conference on, 2005, pp. 947-954.
[30] Patel, R., Khan, M., and Alam, A. (2022). Continuous authentication using behavioral biometrics. *Biometric Technology Today, 9*(1), 67-82.
[31] Pratibha S. Yalagi and Prachi V. Mane (2021). Smart library automation using face recognition. *Journal of Physics: Conference Series*. 1854 (2021) 012041.
[32] Probst, P.; Wright, M.N.; Boulesteix, A.L. (2019). Hyperparameters and tuning strategies for random forest. *Wiley Interdisciplinary Rev. Data Mining Knowledge Discovery*. 9, 1301.
[33] Shweta Shirpurkar and R.A. Ingolikar (2018). Data Mining of Facial Features using Random Forest Algorithm for Person Classification. *IJCRT*, volume 6, Issue 1, 2112-2120.
[34] Smith, J., Johnson, R., and Lee, S. (2021). Security vulnerabilities in traditional authentication methods. *Journal of Cybersecurity, 6*(3), 112-125.
[35] Thakur, R., Pandey, S., and Kumar, A. (2021). Score-level fusion techniques in biometric systems. *Journal of Computational Biometrics, 6*(2), 67-82.
[36] Turk, M., and Pentland, A. (1991). Eigenfaces for recognition. *Journal of Cognitive Neuroscience, 3*(1), 71-86.
[37] Traore O. E., Kopoin N. C., N'takpe T. G. And Oumtanaga S. (2025). Optimization Of Feature

Extraction For The Prediction Of Macromolecular Interactions : Ote-24 Approach. International IEEE CS International Conference on Information Technology and Computer Science 13(03), 577-589.

[38]Wang, Y., Chen, X., and Zhang, L. (2023). Feature-fusion techniques for robust biometric authentication. *International Journal of Biometrics, 12*(1), 23-37.

[39]Xu Xiaona, Pan Xiuqin, Zhao Yue, Pu Qiumei, "Research on Kernel-Based Feature Fusion Algorithm in Multimodal Recognition", *IEEE CS International Conference on Information Technology and Computer Science*, 3-6, 2009.

[40] Xu, B.; Huang, J.Z.; Williams, G.; Wang, Q.; Ye, Y. (2012). Classifying very high-dimensional data with random forests built from small subspaces. Interl. Journal Data Warehouse, 8, 44–63.

[41] Zhang, L., Li, H., and Sun, Z. (2021). Multimodal biometric fusion. *IEEE Transactions on Cybernetics, 51*(3), 1450-1462.