Uniosun Journal of Engineering and Environmental Sciences (UJEES), Vol. 8 No. 2, Sept., 2026
DOI: 10.64980/ujees.v8i2.009 **Atoyebi et al.**
Published: September 30, 2026

ADAPTIVE FEATURE-LEVEL FUSION FOR TRI-MODAL BIOMETRIC RECOGNITION USING AN ENHANCED CLONAL MATCHING ALGORITHM

Jelili Olaniyi ATOYEBI[1]*, Nnamdi OKOMBA[2], Ibrahim Adepoju. ADEYANJU[3], Adebimpe ESAN[4], Bolaji OMODUNBI[5], Akeem Akande ATOYEBI[6], Michael Olumuyiwa ADIO[7] , Akinyemi Omololu AKINROTIMI[8]

[1]*Department of Computer Engineering, Adeleke University, Osun State, Nigeria.,*

[2,3,4,5]*Department of Computer Engineering, Federal University Oye-Ekiti, Ekiti State, Nigeria.*

[6]*Department of Building Technology, Osun State Polytechnic, Osun State, Nigeria.*

[7]*Department of Computer Engineering, Osun State University, Osun State, Nigeria.*

[8]*Department of Information Systems and Technology, Kings University, Osun State, Nigeria.*

[*]*Corresponding Author: atoyebi.jelili@adelekeuniversity.edu.ng*

Abstract
Over the past decade, biometric recognition systems have emerged as highly effective for identifying individuals and have attracted significant attention for their reliability and wide range of applications in authentication. However, unimodal biometric systems, which rely on a single biometric trait, often face limitations in terms of performance and accuracy. These shortcomings can be addressed by integrating multiple physiological or behavioral traits, thereby creating a multimodal biometric system that enhances both identification and verification. In this study, a tri-modal biometric recognition system was developed that incorporates facial, iris, and signature traits. Feature-level fusion was employed using an Enhanced Clonal Matching Algorithm (ECMA), while classification was performed through a parallel multi-Support Vector Machine (SVM) setup utilizing a quadratic kernel function. The decision-making process relied on thresholding techniques to finalize classifications. Implementation was carried out using multimodal biometric images of 200 participants on MATLAB platform. Performance evaluations of the system using Face, Iris, and Signature data were conducted at a threshold value of 0.75, comparing results from standard CMA and ECMA methods. The obtained result values for true positives, false negatives, false positives, true negatives, false positive ratio (%), accuracy (%), sensitivity (%), specificity (%), precision (%), and processing time (in seconds) were 173, 176; 7, 4; 4, 1; 56, 59; 6.67, 1.67; 95.42, 97.92; 96.11, 97.78; 93.33, 98.33; 97.74, 99.44; and 84.51 sec., 75.81 sec., respectively. The proposed ECMA demonstrated an adaptive matching rate strategy, contributing to its overall effectiveness, which ultimately could enhance secure access control to sensitive areas and valuable assets. 3D biometric images might be considered in the future.

Keywords
Fusion algorithm, Tri-modal, Sensitivity, Enhancement, Accuracy

1. INTRODUCTION

Biometrics has become a growing field in human identity recognition, focusing on the practical use of scientific and image processing technologies to achieve more accurate and dependable identification of individuals. This approach utilizes both physiological traits, such as fingerprints, palmprints, hand geometry, voice, and vascular patterns, and behavioral traits like gait, signature, and typing patterns. While behavioral characteristics may change gradually over time, physiological features tend to remain relatively stable. Among these, fingerprints are one of the oldest and most widely used physiological identifiers, often employed for purposes such as verifying personal information and assisting law enforcement in tracking criminals. Biometrics operates under two primary modes: verification and identification using fingerprint, face and iris recognition [1]. Multimodal biometrics offers a more secure authentication system by utilizing multiple biometric templates for verifying an individual's identity. The collected biometric data can be integrated into automated biometric systems and fused at various levels, including sensor, feature extraction, score matching, or final decision-making, to address the limitations found in unimodal biometric systems. This approach provides enhanced protection against spoofing, as generating fake data for multiple biometric

traits is significantly more difficult. In contrast, unimodal systems are more vulnerable to falsification. Therefore, multimodal systems deliver greater accuracy, reliability, and resistance to identity fraud. According to [2][3], it is crucial to integrate multiple biometric traits at a defined fusion level before proceeding with weighted score matching and comparing extracted features against the pre-existing templates stored in the database. [4] designed a multimodal biometric system that incorporated iris, finger vein, and fingerprint traits. By utilizing a single device, the system achieved optimal score-level fusion through the enhancement and suppression of concurrent classifiers while also addressing conflicts among disagreeing classifiers. The research suggests that the system has potential for further development, particularly in adapting to varying levels of security requirements. [5] integrated fingerprint and signature data at the feature extraction stage, employing the Sum rule as a standard method for performing the fusion. [6] combined iris, face, and fingerprint biometric templates at the matching score level by implementing a fusion approach that utilized multiple parallel Support Vector Machines (SVMs). [7] analyzed various techniques for combining different biometric traits to develop a multimodal biometric authentication system. Their study emphasized the significance of such systems in enhancing security measures and highlighted their role as a top-tier solution within network security frameworks through the integration of multiple biometric modalities. [8] presented an in-depth study of various unimodal and multimodal biometric sensing methods, discussing their respective benefits and drawbacks. A face-trait recognition system is a biometric technique that uses automated processes to authenticate or identify a person by analyzing the physiological characteristics of their facial image. Each individual is recognized based on the distinct structure of their face, which contains peaks and valleys at varying altitudes. The facial features are located at different latitudes and longitudes. This plate highlights unique human features that the biometric recognition system utilizes to distinguish between individual identities. Biometric-image processing techniques have impact on applications of multimodal and multisensor biometrics in smart factories [9]. Iris-scan biometric technology is a highly dependable form of biometric systems widely used for the identification and verification of a person's iris identity [10]. Iris image recognition falls under the category of human-eye biometrics, as it directly involves the individual's eye. The signature-trait recognition system is another biometric approach that uses automated methods to verify or identify an individual based on the unique characteristics of their signature. Typically, signatures are one of the most common ways organizations, including academic institutions, identify individuals, either through traditional pen-and-paper methods or electronic signatures on devices like mobile phones and tablets [11]. Signatures and handwriting are significant behavioral biometric traits in pattern recognition systems. Handwriting and signature-based technology, particularly for smaller devices, has become a preferred choice for biometric identification and verification in certain industries, gaining widespread acceptance. [12] employed the minutiae extraction method for fingerprint identification and the log-Gabor filtering technique for iris recognition. This biometric technology necessitates that the individual use an electronic input device (such as a writing instrument) to sign, enabling the capture of the signature image. The study aimed and presented a tri-modal biometric recognition system that integrated face, iris, and signature traits using feature-level fusion and an Enhanced Clonal Matching Algorithm (ECMA), with classification performed by a Support Vector Machine (SVM). At the feature extraction level, data from the three biometric modalities were combined to generate a unified matching score. ECMA served as the fusion mechanism to process these multimodal datasets. A parallel multiple SVM with a quadratic kernel function was employed as the final classifier, distinguishing between genuine users (authorized) and impostors (unauthorized) by comparing the final matching score of the new biometric input with that of the stored templates, using a thresholding (binarization) method. The developed system demonstrated promising performance during evaluation with acceptable results. Conclusively, this study focuses on the development of a trimodal biometric recognition system using an Enhanced Clonal Matching Algorithm (ECMA) to provide more secure, robust and accurate human traits authentication by implementing an adaptive mutation rate strategy (enhanced clonal matching algorithm) for solving the issues of affinity maturation (mutation) step, parent's affinity (as in standard clonal selection algorithm) and also maintenance of feature origin. Multimodal Biometric Recognition Systems are typical sophisticated automated authentication systems that leverage multiple biometric traits, such as iris, face, palmprint, fingerprint, and voice, to improve accuracy, robustness, and security in biometric identity verification systems [13]. [14] presented and evaluated the security of multimodal fusion levels using the Fast Gradient Sign Method (FGSM), concluding that input-level fusion demonstrated superior security, with attack success rates of 16.62% on DenseNet201 and 32.30% on ArcFace models. [15] introduced a border control biometric system integrating fingerprint and finger vein modalities using SIFT, FLANN, and CLAHE techniques. Their study showed that feature-level fusion yielded higher accuracy and reduced information leakage. [16] applied Dempster-Shafer Theory to combine face and signature biometrics, improving authentication performance. [17] proposed a deep learning framework using retina and fingerprint modalities, achieving a 99.94% accuracy with reduced error rates, thereby enhancing biometric data protection. [18] used a deep CNN with transfer learning for gait and facial recognition in surveillance videos, achieving 97.3% classification accuracy. [19] developed a Conditional Multimodal Biometrics Network (CMB-Net) to combine periocular and face biometrics with superior

identification results across multiple configurations. [20] explored flexible deployment using representation learning across unimodal and multimodal scenarios. Researchers scrutinized face traits, face traits conditioned with periocular and periocular-face configurations under the regimen of CMB. [21] explored quad-biometric systems for few-shot user identification, demonstrating notable improvements in accuracy and training speed. The research method consists of feature extraction from biometrics and fusion for multi-biometric user identification. Evaluation of user identification performance was achieved using data collected from CASIA-BIT, including face, iris, palmprint, and fingerprint biometric data. [22] focused on e exam authentication by integrating face and fingerprint with traditional methods, revealing challenges like impersonation and collusion. They further work on collaboration and external assistance, which pose significant challenges in the context of e exams, were also revealed by the findings. Their work was mainly aimed at designing a multimodal authentication method that will integrate face recognition and fingerprint recognition models in conjunction with traditional authentication schemes that use usernames and passcodes. [23] reviewed 3D biometrics and suggested future research in 3D algorithm generalization, anti-spoofing, and device enhancement. [24] developed the "Secure Sense" framework using face, iris, and fingerprint data via decision-level fusion, achieving 93% accuracy. [30] was aimed at enhancing the accuracy of person verification. Their approach integrated data from both web-based sources and real-time acquisitions. For web-based datasets, they utilized the Chicago Face dataset (facial recognition), MMU1 (iris recognition), and SOCOfing (fingerprint data). In real-time settings, facial images were captured using a Zebronics Zeb-Gem webcam, fingerprints with the Mantra MFS scanner, and iris data using the Mantra MIS scanner. The system employed a decision-level fusion strategy across all three biometric traits, achieving a notable accuracy rate of around 93%, demonstrating the effectiveness of its multimodal fusion approach. [25] conducted a study that involved comparing and integrating ear and face images within an appearance-based biometric framework, yielding encouraging and effective results. [26] explored the influence of multimodal and multisensor biometric systems within smart factory environments. Through extensive experimentation using commercial off-the-shelf (COTS) hardware, they demonstrated that their proposed approach was practical and scalable for large-scale smart factory deployment. Their work highlighted how integrating intelligent systems and ICT technologies significantly supports the advancement of Industry 4.0. The study emphasized that incorporating various sensors enhances the capabilities of smart factories, playing a vital role in driving technological growth and economic development in industrialized nations. [27] investigated the capabilities of ChatGPT in executing tasks like face verification, soft-biometric estimation, and providing explainable results. Their findings suggest that ChatGPT holds significant promise in enhancing the transparency and interpretability of automated decision-making in human-centered applications. The study included experiments using widely recognized public datasets and benchmarked ChatGPT's performance against leading methods in the field. Results indicated that large language models (LLMs) like ChatGPT can effectively contribute to face biometric systems, particularly in improving explainability. [28] introduced a cryptographic approach wherein a biometric trait, specifically, the palm vein which serves as a secure key to access the stored biometric template database. The core concept rests on the uniqueness of palm vein patterns, ensuring that no two individuals share the same vein structure. This inherent uniqueness makes it an ideal, non-replicable key, effectively safeguarding against theft or unauthorized use. [29] presented an overview of the biometrics field, highlighting its key advantages, limitations, challenges, and privacy implications. Their work covered potential applications of multimodal biometric systems, discussing feasible fusion levels, possible integration strategies, and methods to address issues such as spoofing attacks and the use of genetic algorithms for optimization. [30] presented Periocular Biometrics Enhancement through Multimodal Embeddings and Classifier Adaptation. The study made it clear that a multimodal biometric identification system that combined fingerprint, face, and iris recognition to accommodate large-scale user populations. He emphasized how image quality significantly influences the system's identification accuracy and highlighted the need for secondary human validation in some cases. For systems handling tens or hundreds of millions of enrolled identities and processing hundreds of thousands of identification requests, He pointed out that both identification performance and adequate staffing are critical for ensuring the system is effectively designed and managed. [31] introduced a secure, deep multimodal biometric authentication system that integrates online signature and facial features through feature-level fusion. This fused feature vector was utilized to train a Modified Mixed Sequence Deep Neural Network (MMS-DNN). The system demonstrated a significant enhancement in verification accuracy, achieving an equal error rate (EER) of just 0.5%, marking a notable improvement over prior methods. Additionally, the approach ensured greater data security, as only the fused feature vector from the raw biometric data was used during both training and verification processes. [32] released Multimodal biometric recognition using iris and face features. The study further explain an in-depth review of unimodal and multimodal fingerprint biometric authentication systems, with a focus on fusion techniques, attack vulnerabilities, and template protection methods. The study evaluated the strengths and limitations of various fingerprint recognition approaches through performance analysis. The review highlighted significant technological progress in both unimodal and multimodal fingerprint systems. However, the findings also revealed that while some systems employing dynamic

biometrics require enhancements in verification accuracy, many existing solutions still suffer from privacy and security shortcomings. [33] proposed a multimodal biometric recognition system that combines iris and facial features. They developed a novel feature extraction approach utilizing Discrete Wavelet Transform (DWT) and Singular Value Decomposition (SVD) to effectively extract key characteristics from both modalities. These extracted features were then fused to generate a unique biometric pattern for each individual in the dataset. The system was evaluated using the Faces94 and IIT Delhi Iris datasets. Experimental results demonstrated the effectiveness and robustness of the proposed approach in enhancing biometric recognition performance. [34] Introduced Sparse and Discriminative Multimodal Feature Codes (SDMFCs) for multimodal finger recognition, aiming to capture both shared and distinct features across different biometric modalities. Their approach began by constructing a local difference matrix to extract rich texture details from localized regions of finger images. Next, they learned compact and discriminative binary codes by jointly analyzing data from multiple modalities under specific constraints. These binary codes were then used to build a recognition framework that combined local histograms from each segmented block for accurate classification. Testing on three widely used finger biometric databases confirmed the robustness and efficiency of the proposed method in multimodal recognition scenarios. [35] presented a multimodal biometric authentication system that combines facial and voice data, utilizing FaceNet for face recognition and Gaussian Mixture Models (GMM) for voice processing. Their findings showed that the system effectively reduced the Equal Error Rate (EER), primarily due to FaceNet's ability to learn a compact Euclidean embedding of facial images, enabling precise similarity measurement. This approach achieved a high accuracy of 99.63%. However, the GMM-based voice recognition component did not achieve the lowest EER on its own, with the overall performance gains largely attributed to the use of FaceNet, a leading model in facial recognition. [36] proposed a multimodal biometric authentication system that integrates an Extreme Learning Machine (ELM) for classification, combined with feature reduction using Adaptive Particle Swarm Optimization (APSO). The ELM model was designed to enhance classification performance, and the use of APSO optimized the feature selection process. With 40 iterations and a population size of 30 in the optimization algorithm, the model achieved a sensitivity of 95.69%and specificity of 94.29%. The study's results highlight the system's potential for delivering efficient and reliable biometric security authentication. [37] introduced DeepFace-Attention, a multimodal face biometric system designed for attention estimation in e-learning environments. Their study showed that global features, when combined using score summation, were highly effective— particularly the combination of eyeblink and facial expressions, which achieved an accuracy of 83.34%. However, the highest performance was obtained using local features with score-level fusion via neural network training, which, while slightly less accurate than the full fusion model, required only 10% of the features, demonstrating a more resource-efficient alternative to unimodal biometric systems. [38] introduced a novel approach titled Flexible Biometrics Recognition: Bridging the Multimodality Gap through Attention, Alignment, and Prompt Tuning. In this work, the researchers proposed the MFA-ViT framework to tackle the complex challenges of flexible biometric recognition (FBR). This method utilizes Multimodal Feature Alignment (MFA) and Multimodal Prompt Tuning (MPT) to effectively capture and model dependencies across different biometric modalities. The MPT component plays a key role in establishing intermodal relationships, which are essential for improving both intra-modality and cross-modality recognition performance. [39] introduced a multi-modal recognition approach that integrated both the vein patterns and geometry of the forearm. The method involved extracting five key features from a Near-Infrared (NIR) image of the forearm: SURF, local line structures, global graph representations, forearm width, and forearm boundary features. These features were first matched individually and then combined at the score level using an Improved Analytic Hierarchy Process-entropy weight fusion method. Extensive experiments were conducted to assess the performance of the proposed recognition technique and its fusion strategy. The results demonstrated that this approach delivered strong performance in forearm recognition. [40] introduced a more robust and accurate BLD (Fingerprint Liveness Detection) strategy by utilizing weighted multimodal convolutional neural networks (MCNNs) to extract various deep features. Before detection, a Region of Interest (ROI) operation was applied to eliminate irrelevant background elements from the fingerprints. The researchers then proposed a multimodal feature fusion approach that leveraged the full learning potential of convolutional neural networks (CNNs) without requiring human intervention. Recognizing that directly combining features from different modalities for classification was inefficient, they explored a weighted summation strategy to improve the fusion process. Yuan's work was titled "MFFFLD: A Multimodal-Feature-Fusion Based Fingerprint Liveness Detection. [41] explored the impact of cosmetics on various fusion levels of face and iris biometrics, two widely recognized biometric traits. A face-iris cosmetic detection system was created to integrate shape, texture, and color information from individuals, utilizing Log-Gabor (L-Gabor) transform, Uniform Local Binary Pattern (ULBP), and Color Moments (CM) extractors in the proposed multimodal recognition system. The fusion of both modalities was carried out based on the outcomes of the detection scheme, using an optimized weighting system to assess the accuracy of the proposed multimodal method at both score and feature level fusions. [42] introduced an innovative fusion system combining iris and ear biometrics for e-exams. Their results showed that the system achieved a

recognition accuracy of 97%, with a 2% False Acceptance Rate (FAR), a 4% False Rejection Rate (FRR), a 94% Correct Recognition Rate (CRR), and a 96% Genuine Acceptance Rate (GAR). Furthermore, the proposed system outperformed other similar systems in terms of accuracy. In [43] developed a face-iris bimodal biometric recognition system was developed using match-level fusion with Support Vector Machines (SVMs), which achieved recognition accuracy of 96.2%, a False Rejection Rate (FRR) of 0.8%, and a False Acceptance Rate (FAR) of 2.2%. [44] Conducted an analytical study on users' awareness and acceptance of multimodal biometrics (MMB) for online transactions using a two-stage SEM-ANN approach. The study examined five key perspectives: User Acceptability, Cognizant Factors towards Biometrics, Technological Factors, Perceptional Factors (such as Fingerprints, Iris, Face Recognition, and Voice), and Data Privacy Factors. A questionnaire was distributed to 530 biometric users, and their responses were analyzed. This research paper offered a novel approach compared to previous studies by considering cognizant and perceptual factors in the proposed model, thus broadening the scope of MMB literature. Additionally, the research paper highlighted practical implications for adopting multimodal biometric systems, along with some limitations. [45] Performed the fusion of fingerprint and finger vein modalities. The implementation was done at feature-level, where feature level fusion demonstrates superior performance by effectively addressing compatibility issues between modalities and reducing information leakage and also to optimize feature extraction and matching. Leveraging Scale Invariant Feature Transform (SIFT) and Fast Library for Approximate Nearest Neighbors (FLANN) were used in MATLAB simulation environment. Fingerprint and finger vein traits were fused. The fused data of PLUSVein_CASIA achieved an EER of 0.13, FRR and FAR of 0.0, and an accuracy of 1 for feature level fusion. [46] reported that single biometric techniques have several problems, like non-universality, noisy data, unacceptable error rates, and spoof attacks. To solve these problems, multimodal biometrics were used to obtain secure authentication based on multiple modalities such as iris, retina, fingerprint, and face. The experimental analysis was evaluated with Python programming language. The researcher proposed multimodal secure biometrics (MSB) using a deep learning (DL) framework.

2. MATERIALS AND METHOD

This section outlines the overall methodology and research approach used in this paper. An experimental approach was adopted during the system development. The developed multimodal biometric system was developed through seven key phases: Data Acquisition (Image Capture), Pre-processing, Feature Extraction, Normalization of Extracted Features, Feature Level Data Fusion, Final Classification, and Evaluation/Validation, as illustrated in Figure 1. The incorporation of data fusion was essential in this system, as it integrates multiple biometric traits to enhance the accuracy and dependability of authentication and identification. Fusion can occur at various levels: sensor (data acquisition), feature extraction, matching score, and decision (classification), but this work focuses specifically on feature-level fusion. This choice is based on the structural incompatibility and dimensionality challenges encountered at the feature extraction stage, warranting deeper investigation. A parallel architecture was implemented for the image processing pipeline, allowing simultaneous processing of inputs to improve security during authentication. A block diagram explaining the components of the developed tri-modal biometric recognition system is presented in Figure 2. The fusion of extracted biometric features was achieved mainly using an Enhanced Clonal Matching Algorithm (ECMA), it was not Clonal Matching Algorithm (CMA). A locally collected multimodal biometric dataset was used for system testing. Performance evaluation of the system was conducted using five key biometric performance metrics: Accuracy, Sensitivity, Specificity, Precision, and Recognition time.

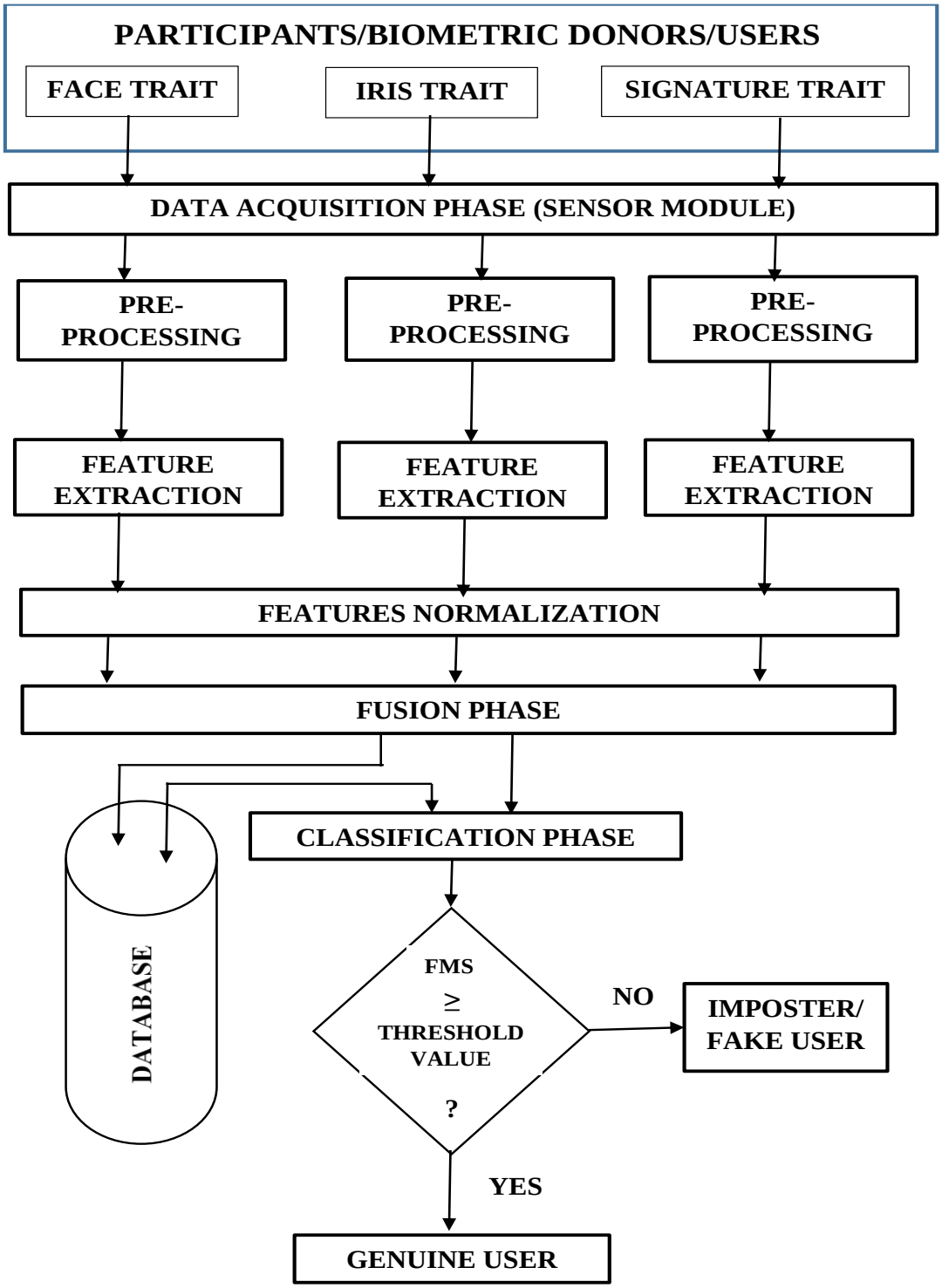


Figure 1: System Model Design for the Developed Tri-Modal Biometric Recognition

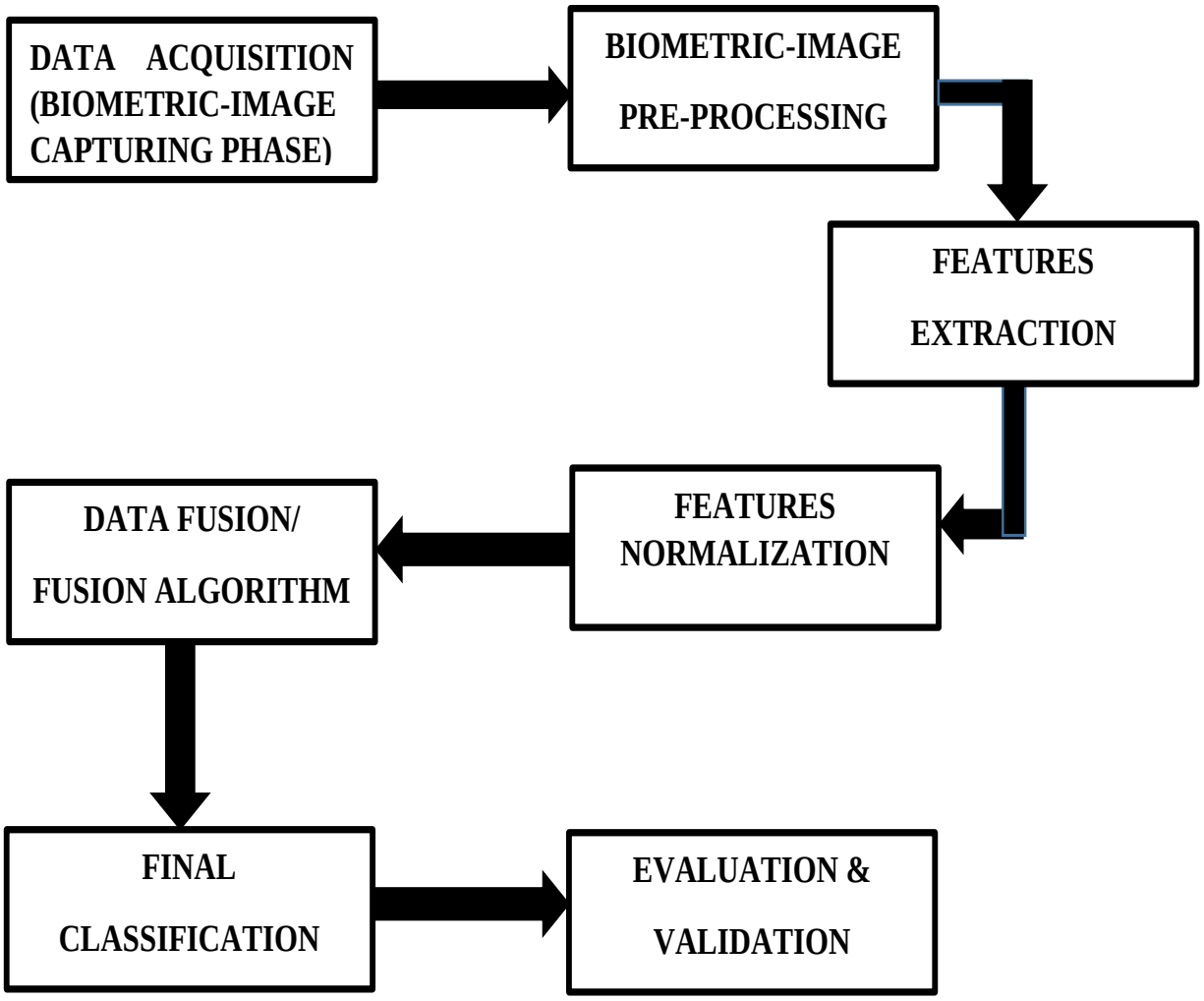


Figure 2: Block Diagram for the Developed Tri-Modal Biometric Recognition System

2.1 Data Acquisition

This first stage was responsible for collecting multiple biometric images from 200 targeted subjects/participants (as illustrated by plate 1 for face, plate 2 for iris part and plate 3 for signature). A total dataset of 800 non-chimeric biometric samples, stored in non-chimeric multimodal database, were collected from 200 participants. A non-chimeric multimodal database is a dataset where all collected data modalities (such as face, iris, and fingerprint, or different genomic layers) belong to the same real-world individual. Data acquisition was performed locally using these high-quality digital cameras and scanners, all without flash in natural day-time lighting with optimal image quality settings to get high-quality images:

i. Face image: A high-quality digital camera (Nikson D90 DSLR model).
ii. Iris image: A cross-match electronic camera (Hyundai Webcam – HYS 001 model).
iii. Signature image: A digitalizer tablet for digitalizing offline signatures (UV05003 model).



Plate 1: A sample of human face.



Plate 2: A sample of an open human eye with the iris part

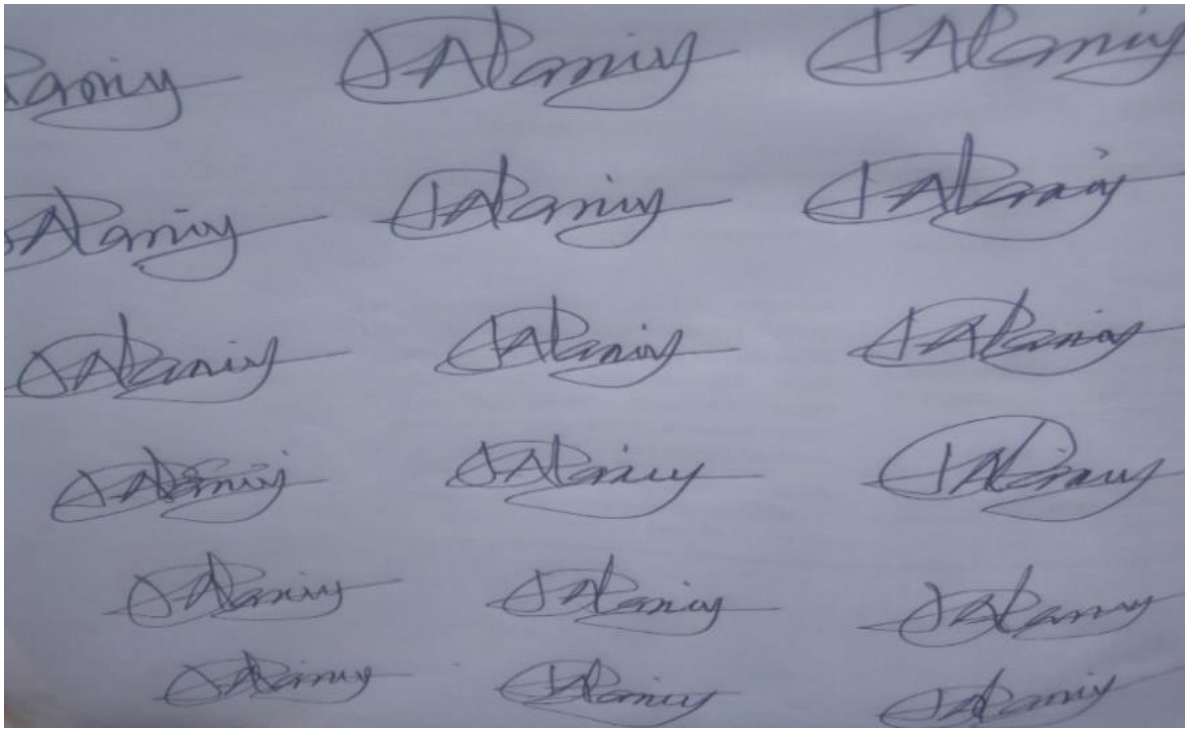


Plate 3: A sample of signature on white paper, digitalized using a digital camera.

2.2 Biometric-Image Preprocessing

The preprocessing stage was meant to extract the Region of Interest (ROI) from acquired biometric images and to correct the acquired image quality using possible algorithms for contrast improvement, noise removal, brightness correction, and extracting the region of interest. Basically, a normal image is a visual representation of a person or any other objects that is in two-dimensional form. The pixel is a set of the smallest elements with various colours in any digital image. The image resolution is the number of pixels present in a digital image, which is obtained by multiplying the number of pixel columns and pixel rows together. During the pre-processing phase, both hand and edge-level cropping techniques were used to crop the region of interest (ROI). These colored face images will then be converted to gray-scale images. The intensity range of the converted grayscale shall be stretched out using the Histogram equalization algorithm to enhance image brightness for a clearer view ahead of the extraction of biometric images' features. Histogram equalization causes uniformity in the intensity of pre-processed images. All three selected biometric images were subjected to Histogram Equalization Image Processing Algorithm with a simplified formula as represented in equation 1.

$$E(l) = \max\left(0, \text{round}\left(\left(\frac{L}{N*M}\right) * t(l)\right) - 1\right) \quad (1)$$

Where:
E(l) is an equalized histogram equalization function,
max is the maximum static range of biometric-image pixels,
round means round to the nearest integer (up or down),
L denotes the number of grey levels in the acquired biometric images,
N*M denotes the size of biometric images, and
t(l) is an accumulated histogram equalization frequency.

2.3 Feature Extraction

This stage was responsible for the representation and description of acquired biometric images using different algorithms for extracting and encoding the contents of the images in a concise feature template form and descriptive vector way. Feature sets extraction on acquired multiple images was performed using feature extraction techniques:

i. Face image: Eigen-face approach.
ii. Iris image: Gabor filtering technique.
iii. Signature image: Clustering extraction technique for local features.

Meanwhile, the Min-Max Normalization Technique, as shown in equation 2, was applied to every biometric score of extracted features of five selected traits to transform them into the common dataset format with score values ranging between 0 and 1. This score normalization method uses the minimum and maximum scores to generate normalized values for every selected trait, as shown in equations 3, 4, and 5.

$$N_{trait} = \frac{BS_{trait} - min_{trait}}{\max_{trait} - min_{trait}} \quad (2)$$

Where N is the normalized score value for the selected biometric trait, BS is the current biometric score of a trait, is the minimum biometric score, and is the maximum biometric score for the individual trait. Individually, normalized scores for the selected three traits are to be generated as follows:

$$N_{face} = \frac{BS_{face} - min_{face}}{\max_{face} - min_{face}} \quad (3)$$

$$N_{iris} = \frac{BS_{iris} - min_{iris}}{\max_{iris} - min_{iris}} \quad (4)$$

$$N_{signature} = \frac{BS_{signature} - min_{signature}}{\max_{signature} - min_{signature}} \quad (5)$$

2.4 Fusion of Extracted Biometric Features

A fusion of extracted biometric features from selected three (3) traits was achieved using an Enhanced Clonal Matching Algorithm since it has comparative advantages over most existing feature level fusion algorithms, such as Modified Clonal Selection Algorithm (MCSA), Standard Clonal Selection Algorithm (SCSA) and Standard Tournament Selection Method (STSM) that are less effective owing to their poor feature-balance maintenance and high computational complexity. Modified Clonal Matching Algorithm (MCMA) was realized by incorporating a segmented encoding scheme to Modified Clonal Selection Algorithm (MCSA) and Modified Tournament Selection Method (MTSM) into the selection phase. Meanwhile, initially, the Modified Tournament Selection Method (MTSM) was obtained by introducing a neighbourhood component into the Standard Tournament Selection Method (STSM). This developed Enhanced Clonal Matching Algorithm (ECMA) is characterized by an adaptive mutation rate strategy, which was good for the enhancement purpose, high feature-balance maintenance capability, and low computational complexity for the feature level of fusion. It was subjected to a classification stage for authentication purpose.

2.5 Classification with Support Vector Machine (SVM)

This stage involves the use of tried-and-true techniques for final recognition and interpretation of templates as a genuine or an impostor. A tried-and-true technique is a method, process, or approach that has been tested over time and proven to work reliably. Biometric features classification was achieved using a Support Vector Machine (Kernel-type) based on the thresholding technique. SVM has many comparative advantages over other supervised machine learning classifiers. SVMs are supervised machine learning classifiers with better accuracy than Euclidean distance, K-nearest neighbors (KNN), Decision Trees, and Naïve Bayes Classifier. SVMs can use the concept of mathematical planes. SVMs can also convert nonlinear to linear using the kernel trick. SVMs can use a kernel function to map the non-linear data to higher dimensions so that it becomes linear data. Overfitting can be avoided in SVM using Soft Margin. Last but not least, SVMs provide low complexity, high accuracy, and also work quite well for non-linear data. But SVMs require more training time compared to other algorithms, such as the Naïve Bayes classifier. In another literature, four SVM kernels were established: Radial Basis Function, Linear, Quadratic, and Polynomial, apart from Gaussian and Laplace. Quadratic function kernel type has a high success rate in terms of percentage accuracy, hence this kernel type was selected. Conclusively, the chosen SVM was adopted to perform the fusion of currently available biometric traits and generate the final matching score (FMS or MSfinal). The authenticated person was accepted as a legitimate user if the match scores were greater than the threshold value set for the decision-making. And, the authenticated person was rejected as an imposter if the match score is less than the decision threshold value.

2.6 Evaluation

Equations 6 – 14 revealed formulae for True Acceptance Rate (TAR), True Rejection Rate (TRR), False Acceptance Rate (FAR), False Rejection Rate (FRR), Equal Error Rate (EER), System Accuracy (SA), Sensitivity, Specificity and Precision. Equations 6 - 14 are notable system performance evaluation metrics. True Acceptance Rate refers to the proprtion of valid or correct inputs that a system accurately recognizes and accepts. True Rejection Rate is the proportion of invalid or incorrect inputs that a system correctly rejects. False Acceptance Rate is the proportion of invalid or incorrect inputs that a system incorrectly accepts. Equal Error Rate is where False Acceptance Rate equals False Rejection Rate. True Negatives (TN) is the calculated number of imposters identified precisely by the biometrics system, False Positives (FP) denotes estimated number of imposters that labeled as genuine users by the biometrics system and False Negatives (FN) denotes the known number of genuine users not identified by the biometrics system [12]. True Positives (TP) is the calculated number of genuine users precisely identified by the biometrics system, According to [12], system performance evaluation metrics are determined, in percentage, as follows, where:

i. $$TAR = \frac{\text{Total Number of Genuine Biometric Trait Accepted}}{\text{Total Number of Genuine Matching Tests Performed}} \quad (6)$$

ii. $$\text{TRR} = \frac{Total \text{ Number of Imposter Biometric Trait Rejected}}{\text{Total Number of Forgery Tests Performed}} \quad (7)$$

iii. $$\text{FAR} = \frac{\text{FP } (Total \text{ Number of Imposter Biometric Trait Accepted as Genuine})}{\text{TN+FP (Total Number of Forgery Tests Performed)}} \quad (8)$$

iv. $$\text{FRR} = \frac{\text{FN } (Total \text{ Number of Genuine Biometric Trait Rejected as Imposter})}{\text{TP+FN (Total Number of Genuine Matching Tests Performed)}} \quad (9)$$

v. $$\text{EER} = \text{It is an intersection point between FAR and FRR} \quad (10)$$

vi. $$\text{System Accuracy (SA)} = \frac{\text{TP+}TN}{\text{TP+TN+FP+FN}} \quad (11)$$

vii. $$\text{Sensitivity} = \frac{\text{TP}}{\text{TP+FN}} \quad (12)$$

viii. $$\text{Specificity} = \frac{\text{TN}}{\text{TN+FP}} \quad (13)$$

ix. $$\text{Precision} = \frac{\text{TP}}{\text{TP+FP}} \quad (14)$$

In the study, the performance of an Enhanced Clonal Matching Algorithm (ECMA) was developed. Recognition Time is the time taken by the biometric system to recognize a tested image. True Acceptance Rate, True Rejection Rate, False Acceptance Rate, False Rejection Rate, and Equal Error Rate were obtained using the above-listed equations 6, 7, 8, 9, and 10, respectively. Furthermore, the system recognition accuracy, sensitivity, specificity, and precision of the developed system were also evaluated using the above-listed equations 11, 12, 13 and 14, respectively.

2.7 Data Analysis for the Developed System

Training datasets and Test datasets, for each of the three 3 selected biometric traits, were used during the experimental setup of a developed system to draw relevant inferences. The dataset collected for the developed system was split into a training and a test dataset (percentage split). The training phase took 70 % of the datasets, while the test phase took 30 % of the remaining datasets. In addition, this locally collected dataset was used for the evaluation of the experiment to determine overall system performance. The Developed Enhanced Clonal Matching Algorithm (ECMA) was implemented using Matrix Laboratory (MATLAB) 8.1 (R2013a). Likewise, the Graphical User Interface (GUI) was designed using the GUI toolbox in the MATLAB development environment for simulating the multibiometric recognition system. A Graphical User Interface (GUI), which was designed, was used to handle data loading, training, testing, and result display in a user-friendly environment. A random sub sampling cross-validation was conducted to increase system reliability.

2.8 Participants/ Biometrics Donors

The multi-biometric recognition system requires that all prospective participants (system users or targeted subjects) are to enroll their biometric samples for authentications goals. To the best of research proposer knowledge, there is no freely available database that stores collectively datasets of the three (3) selected traits together after acquiring from the same person. In this research, the ages of 200 LAUTECH students are between 20 years and 60 years. The students of Ladoke Akintola University of Technology (LAUTECH), Nigeria, were used as participants (biometrics donators). The biometric-image capturing took place within the University for time-saving, and Easy and Accurate Data Acquisition.

2.9 Tri-Modal Biometric Images

Eight hundred multi-biometric sample images from two hundred students (4 samples per student), participants/biometrics donors among students of LAUTECH, Nigeria, were acquired and stored in a non-chimeric multimodal database as a multimodal dataset, and then used in the research work. Different high-quality electronic scanners, high-quality digital cameras, and other applicable image-capturing devices were used. Seventy percent (70%) of the datasets were used for training purposes, while the remaining thirty percent (30%) was used for testing purposes. These images were later pre-processed for uniformity in intensity using histogram equalization, while the extractions of the different features from the region of interest (ROI) of the multiple images were carried out using different feature extraction techniques that apply to each trait.

2.10 Resources Required for the Developed System

Personal Computer: A DELL laptop computer system was required during the development stage.
Library Resources: Visitation to the different universities' libraries, in addition to E-books from the internet, was made to get relevant on-site materials for knowledge elicitation. Different educational materials, such as textbooks on image processing techniques, Matrix Laboratory (MATLAB) usage, and Machine Learning Classifier, were used to get insightful information and in-depth knowledge about more advanced biometric algorithms, design concepts, and the mathematical constructs related to the developed multimodal research. Books, magazines, journals, and websites are the expected good resources for the research. In addition, modern computer laboratories, within and outside the LAUTECH campuses, were visited to implement an experimental setup using appropriate image processing techniques and programming learning facilities.

3. RESULTS AND DISCUSSION

The development of the existing Clonal Matching Algorithm (CMA) and the Enhanced Clonal Matching Algorithm (ECMA) for a Tri-Modal Biometric Recognition System was carried out using MATLAB. Enhancement of the traditional CMA was achieved through the integration of an Adaptive Matching Rate Strategy, which improved convergence speed and solution quality. The system utilized three biometric traits: face, iris, and signature, each with 4 images collected from 200 individuals (4 samples per person). A Graphical User Interface (GUI) was designed to handle data loading, training, testing, and result display in a user-friendly environment. The study illustrates the training process conducted on 70% of the dataset, using random sub sampling cross-validation for increased reliability. During training, the original CMA showed moderate recognition accuracy, while the ECMA demonstrated significantly better performance across the tri-modal dataset. The Adaptive Matching Rate enabled the ECMA to dynamically adjust the Matching intensity based on population diversity, promoting more effective exploration of the search space. As shown in Figure 4, the GUI displays biometric features such as face, iris, and signature during the training phase, along with intermediate recognition results. The threshold value was optimized dynamically, and the dataset was properly categorized before commencing the recognition process. The use of random sub-sampling ensured that the system was exposed to various combinations of data, improving its generalization capability. In the testing phase, represented in Figure 5, the performance difference between CMA and ECMA became more evident. Testing was performed on the remaining 30% of the data to validate the model's robustness and real-world applicability. The ECMA consistently outperformed the CMA, showing fewer false positives and false negatives in biometric matching results.

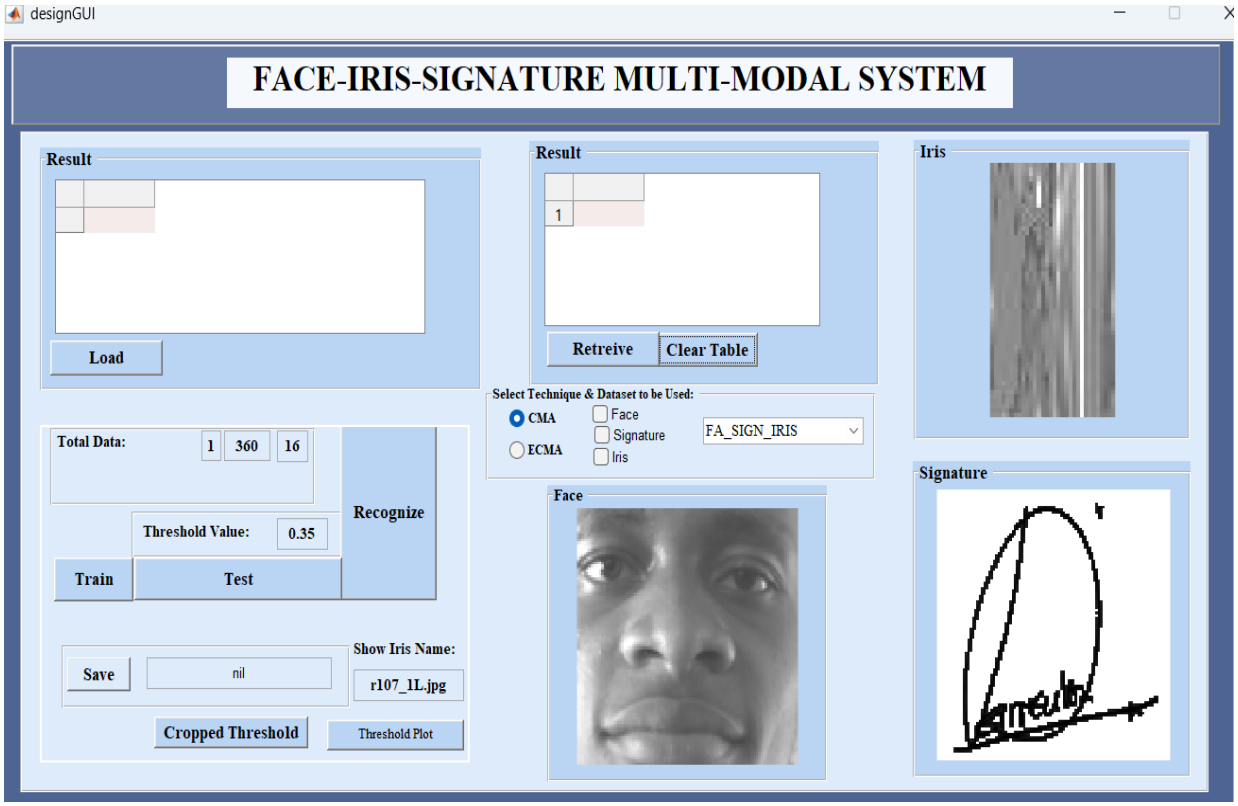


Figure 4: The Graphical User Interface of Tri-modal Training Process

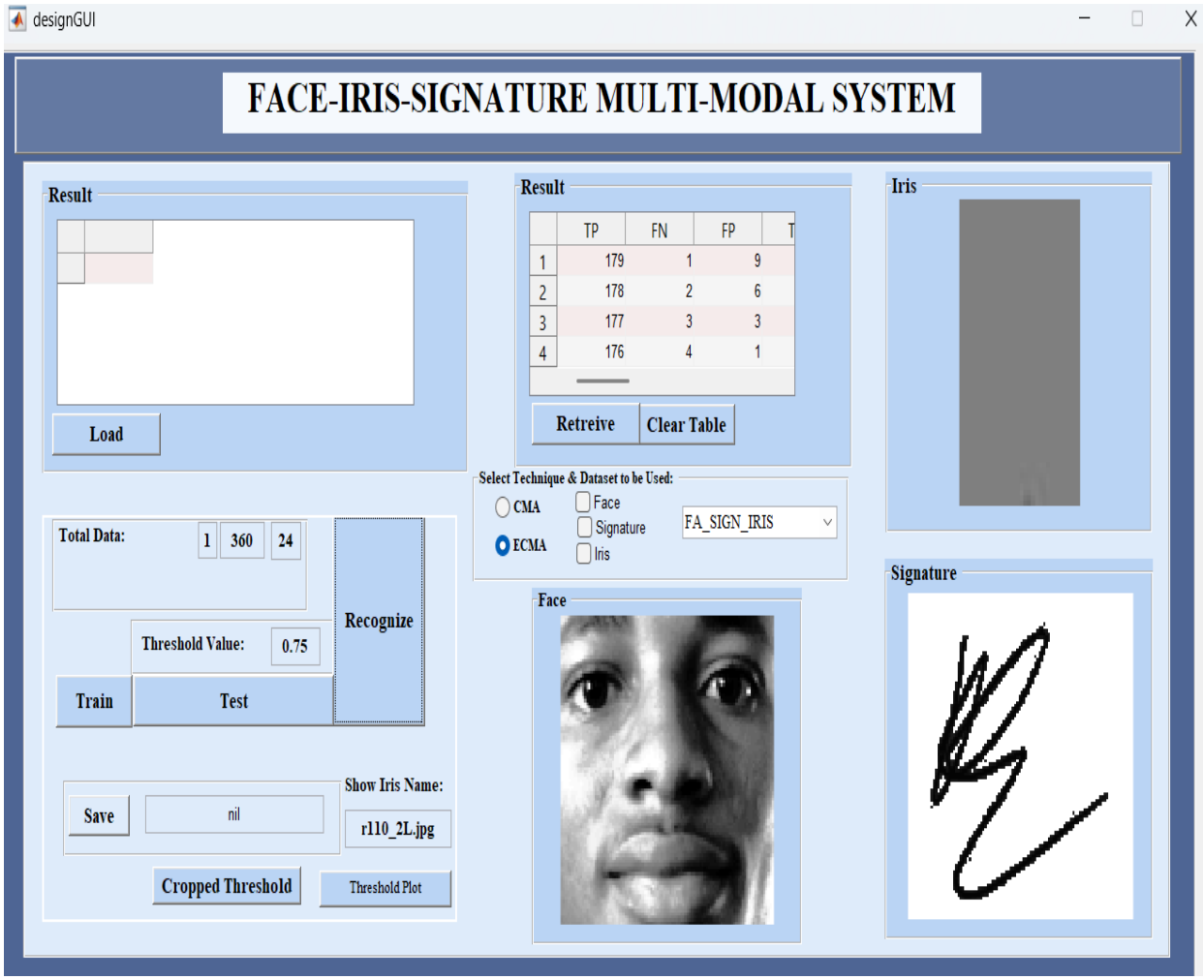


Figure 5: The Graphical User Interface of the Tri-Modal Recognition Process

Confusion matrix components such as True Positives (TP), False Negatives (FN), and False Positives (FP) were analyzed, with ECMA demonstrating superior matching rates. The GUI during testing clearly presents the recognition outcomes, with individual biometric traits displayed alongside the corresponding result metrics. The incorporation of an Adaptive Matching Rate into the Clonal Matching Algorithm enhanced the tri-modal biometric system's feature selection and fusion capabilities. The multi modal fusion was achieved at the feature level, improving the recognition rate by leveraging the complementary nature of the three biometric traits. Both training and testing processes confirmed the robustness and effectiveness of the Enhanced Clonal Matching Algorithm. The MATLAB-based GUI facilitated efficient experimentation and provided real-time feedback on system performance. The choice of threshold for the Enhanced Clonal Matching Algorithm (ECMA) in the Tri-Modal Biometric Recognition System was carefully determined by analyzing the recognition accuracy at various threshold values, as illustrated in Figure 6. From the graph, it is observed that the recognition accuracy improves steadily as the threshold value increases, reaching its peak performance at around a threshold of 0.75. Critical points at thresholds 0.20, 0.35, 0.45, and 0.75 show significant jumps in accuracy, which guided the selection of an optimal threshold. A threshold value of 0.75 was ultimately selected because it provided the highest recognition accuracy of approximately 98%, balancing the trade-off between True Positive and False Positive rates. This careful selection of the threshold was vital to maximizing the overall system performance during biometric recognition. The performance of the developed system was evaluated based on the following metrics: sensitivity (SEN), specificity (SPEC), precision (PREC), accuracy (ACC), and recognition time (Time).

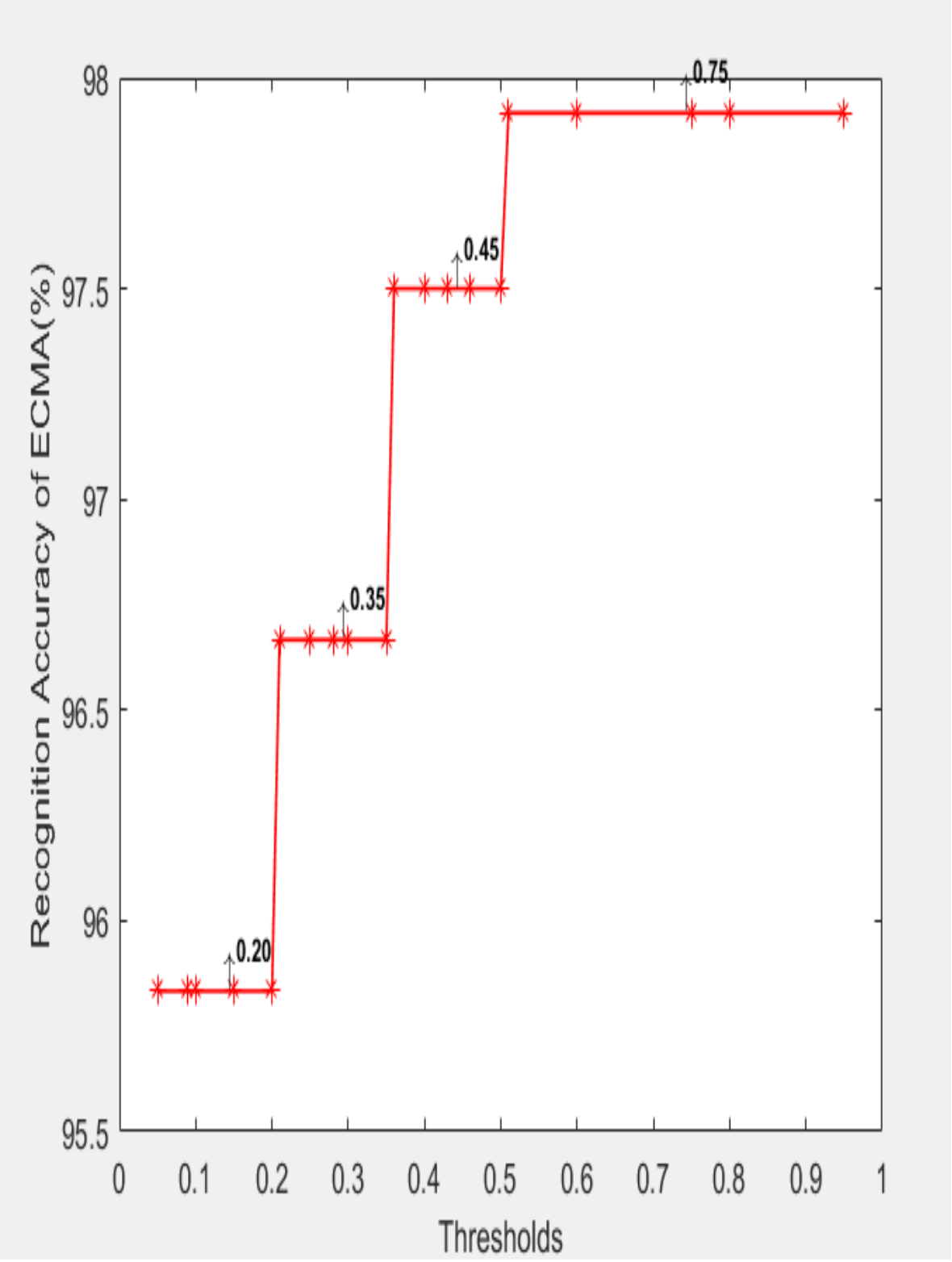


Figure 6: A Threshold Graph demonstrating the choice of thresholds

3.1 Results of CMA and ECMA using Face, Iris, and Signature

The Clonal Matching Algorithm (CMA) showed strong performance in the fusion of face, iris, and signature traits, especially at higher thresholds (Table 1). At a threshold of 0.2, CMA achieved a high True Positive (TP) count of 176 and a low False Negative (FN) of 4, resulting in a Sensitivity (SEN) of 97.78%. False Positive Rate (FPR) at this level was 18.33% with a True Negative (TN) of 49. As the threshold increased to 0.75, TP slightly decreased to 173, but FN increased only modestly to 7, while FP dropped to 4. This decline in false positives led to a lower FPR of 6.67% and improved Specificity (SPEC) of 93.33%. CMA's performance metrics across all thresholds showed consistent improvements in precision and accuracy as the threshold increased. Precision (PREC) improved from 94.12% at threshold 0.2 to 97.74% at 0.75, while

Accuracy (ACC) rose from 93.75% to 95.42%. This suggests that the fusion of three modalities at the feature level offers stronger reliability in distinguishing between genuine and impostor matches. The combination of the three biometrics helps stabilize performance even when one modality fluctuates slightly. The execution time for CMA remained steady across thresholds, averaging around 84.5 seconds. The Enhanced Clonal Matching Algorithm (ECMA) outperformed CMA in all measured aspects when used on the same fused dataset (Table 2). At a threshold of 0.2, ECMA recorded a TP of 179 and FN of just 1, giving an outstanding SEN of 99.44%. FP was also reduced to 9, and TN was 51, resulting in a lower FPR of 15.00%. As the threshold increased to 0.75, TP dropped slightly to 176, but FP decreased drastically to just 1, yielding a minimal FPR of 1.67%. These figures demonstrate ECMA's exceptional ability to reduce both false negatives and false positives simultaneously.

Table 1: Performance Evaluation Result using Face, Iris, and Signature with CMA

Threshold	**0.2**	**0.35**	**0.45**	**0.75**
TP	176.00	175.00	174.00	173.00
FN	4.00	5.00	6.00	7.00
FP	11.00	9.00	7.00	4.00
TN	49.00	51.00	53.00	56.00
FPR(%)	18.33	15.00	11.67	6.67
SEN(%)	97.78	97.22	96.67	96.11
SPEC(%)	81.67	85.00	88.33	93.33
PREC(%)	94.12	95.11	96.13	97.74
ACC(%)	93.75	94.17	94.58	95.42
Time(sec)	84.60	84.81	84.43	84.51

Table 2: Performance Evaluation Result using Face, Iris, and Signature with ECMA

Threshold	**0.2**	**0.35**	**0.45**	**0.75**
TP	179.00	178.00	177.00	176.00
FN	1.00	2.00	3.00	4.00
FP	9.00	6.00	3.00	1.00
TN	51.00	54.00	57.00	59.00
FPR(%)	15.00	10.00	5.00	1.67
SEN(%)	99.44	98.89	98.33	97.78
SPEC(%)	85.00	90.00	95.00	98.33
PREC(%)	95.21	96.74	98.33	99.44
ACC(%)	95.83	96.67	97.50	97.92
Time(sec)	74.74	75.67	75.83	75.81

The improvements in SPEC and PREC further emphasize the strength of ECMA over CMA. Specificity increased from 85.00% to 98.33% between thresholds 0.2 and 0.75, while Precision rose from 95.21% to 99.44%. Accuracy (ACC) also saw a steady climb, beginning at 95.83% and peaking at 97.92%. These results confirm ECMA's enhanced learning and adaptive capabilities, which are particularly effective in a multi-modal fusion scenario. By utilizing adaptive Matching, ECMA better navigates the feature space to optimize classification outcomes. A notable benefit of ECMA is its reduced processing time compared to CMA. ECMA's execution time ranged from 74.74 to 75.83 seconds—about 9 to 10 seconds faster than CMA across all thresholds. The processing time is a recognition time which is the time taken to process and recognize an individual biometric data. Despite being faster, ECMA maintained superior accuracy, precision, and error rates, indicating improved computational efficiency. This time advantage makes ECMA more suitable for large-scale or real-time biometric applications. The fusion of three traits with ECMA ensures robustness without compromising system responsiveness. The fusion of face, iris, and signature biometrics at the feature level of fusion significantly boosts recognition accuracy, especially when enhanced with ECMA. ECMA consistently outperforms CMA in sensitivity, specificity, precision, accuracy, and processing time at all thresholds. These results affirm the effectiveness of ECMA's adaptive learning strategy in complex multi modal biometric systems. The marked improvements across performance metrics validate ECMA as a superior choice for high security and high-reliability applications. Therefore, the ECMA approach is both efficient and highly reliable for tri-modal biometric recognition systems.

3.2 Discussion of Results of CMA and ECMA using Face, Iris, and Signature

This section analysed the results of the CMA and ECMA based on performance metrics. The fusion of face biometrics using CMA and ECMA clearly highlights the advantage of enhancing the Clonal Matching Algorithm with an Adaptive Matching Rate Strategy. The fusion of face, iris, and signature traits together (Figure 7) represents the strongest case for ECMA. ECMA recorded a minimal FPR and very high Sensitivity and Specificity, leading to superior Precision and the highest overall Accuracy among all tested fusions. Execution time was significantly improved compared to CMA. The comprehensive enhancement achieved with ECMA confirms the critical importance of adaptive Matching strategies during the affinity maturation stage. As highlighted in multiple studies, the integration of feature-origin-based adaptive rates fosters better solution diversity, higher convergence speed, and ultimately, more reliable biometric recognition systems.stage. As highlighted in multiple studies, the integration of feature-origin-based adaptive rates fosters better solution diversity, higher convergence speed, and ultimately, more reliable biometric recognition systems.

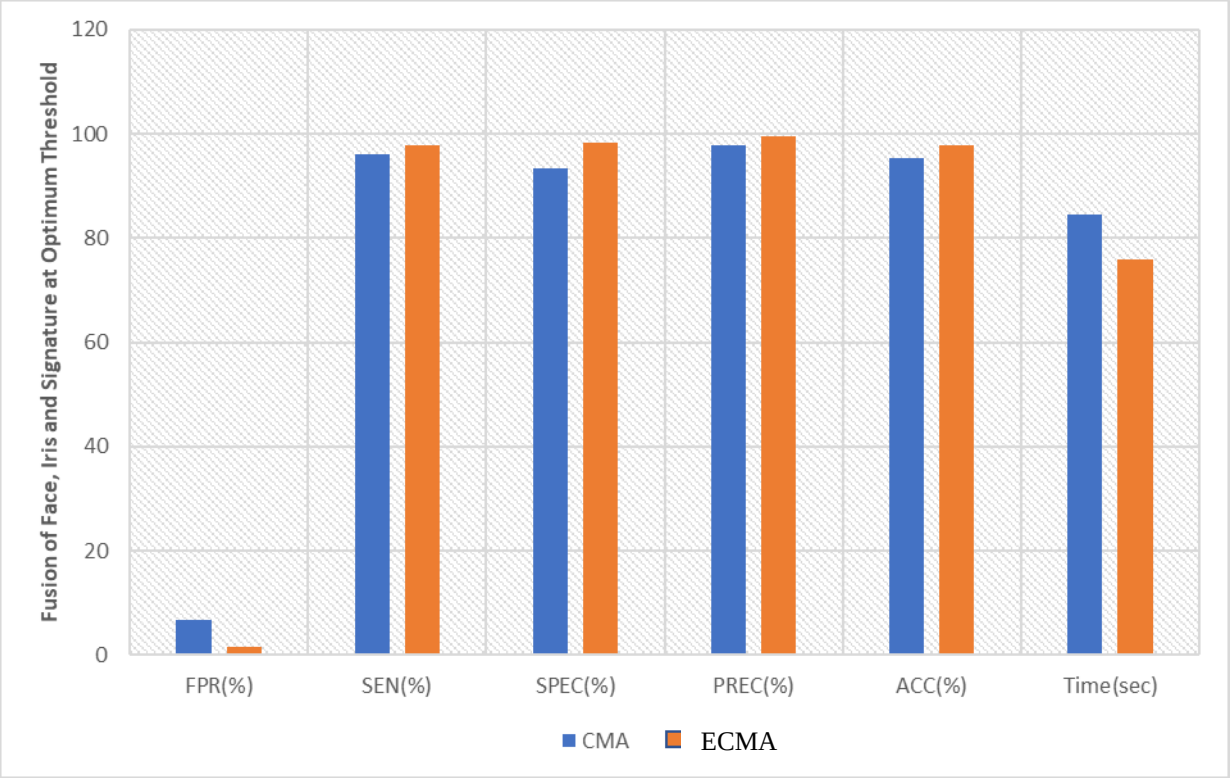


Figure 7: Fusion of Face, Iris, and Signature using CMA and ECMA at Optimum Threshold Value

3.3 ECMA Mathematical Approach

This section explains application of mathematical concept to the Enhanced Clonal Matching Algorithm developed. The developed tri-modal biometric recognition system integrates face, iris, and signature modalities to enhance recognition accuracy, robustness, and resistance to spoofing attacks. Each modality undergoes feature extraction using specialized algorithms suited to its biometric traits-facial texture and geometry features for the face, iris pattern features for the eye, and shape and stroke dynamics for the signature. These extracted feature vectors, denoted as F_f, F_i, and F_s, form the input to the Enhanced Clonal Matching Algorithm developed (ECMA), which is designed to fuse and optimize the combined features for improved classification performance. The first stage of the algorithm involves feature normalization and concatenation to ensure scale uniformity among the three biometric modalities. Each extracted feature vector is normalized using the min-max normalization formula, $F_x' = \big(F_x - \min(F_x)\big)/\big(\max(F_x) - \min(F_x)\big)$ for $x \in \{f, i, s\}$. This normalization process eliminates bias caused by differences in feature ranges. The normalized features are then concatenated to form an initial fused vector $F_{fused} = \left[F_f', F_i', F_s'\right]$. This fused vector serves as the baseline input for optimization through the ECSA, representing a comprehensive combination of the three modalities. In the next phase, the antibody population initialization step generates a set of candidate solutions represented as antibodies $\boldsymbol{Ab} = \{\boldsymbol{Ab}_1, \boldsymbol{Ab}_2, \ldots, \boldsymbol{Ab}_N\}$. Each antibody encodes a potential subset or weight distribution of the fused feature vector. The fitness of each antibody is evaluated using a classifier based criterion-typically a Support Vector Machine (SVM)-where the fitness value corresponds to recognition accuracy: Fitness $(Ab_i) = f(Ab_i) = \text{Accuracy}(Ab_i)$. This ensures that antibodies representing more discriminative fused features are assigned higher fitness scores, guiding the optimization process toward superior feature fusion. The algorithm proceeds to the cloning operation, in which each antibody is replicated in proportion to its fitness. The number of clones for the i^{th} antibody is determined as $n_i = \text{round}(\beta \times$ Fitness (Ab_i)/max (Fitness)), where β is the cloning rate. This biologically inspired step mimics the immune system's clonal expansion process, ensuring that highly fit antibodies produce more offspring, thereby increasing the likelihood of discovering an optimal feature fusion configuration. After cloning, an adaptive mutation process introduces controlled random variations into the cloned antibodies to promote population diversity and prevent premature convergence. The mutation rate for each antibody is adaptively adjusted based on its fitness using $\rho_i = \rho_0 \times e^{(-\alpha \times F\,\text{itness}(\,Ab_i\,)\,)}$, where ρ_0 is the initial mutation rate and α is the adaptation coefficient. Each clone is then mutated as $Cl'_{(i,j)} = Cl_{(i,j)} + \rho_i \times N(0,1)$, where $N(0,1)$ represents Gaussian noise. This adaptive approach allows poorly performing antibodies to explore the search space more aggressively, while fitter antibodies undergo finer adjustments. Following mutation, the selection and replacement phase evaluates all mutated clones and selects the best performing antibody from each clone group according to their fitness values. The new antibody population, $Ab^{\text{new}} = \{Ab_1^{\text{new}}, Ab_2^{\text{new}}, \ldots, Ab_N^{\text{new}}\}$ replaces the weakest antibodies from the previous generation to maintain a balance between exploitation of high-quality solutions and exploration of new possibilities. This ensures continuous improvement of the fused features across successive iterations. A memory update mechanism is employed to preserve the best antibodies across generations. A memory set $M = Top_k(Ab^{new})$ stores the top-performing antibodies, ensuring that optimal feature fusion configurations are not lost during population updates. The algorithm terminates when the maximum number of iterations $T_{\max}$ is reached or when the fitness convergence criterion is met-i.e., no significant improvement in recognition accuracy over several iterations. Finally, the antibody with the highest fitness value in the memory set is identified as the optimal fused feature vector, denoted as $F_{fused}^{\text{opt}} = Ab^* = \arg\max^{(Ab_i \in M)} \text{f}(Ab_i)$. This optimized fused vector represents the most discriminative combination of face, iris, and signature features. It is subsequently used for classification or matching within the recognition system, resulting in enhanced accuracy, reduced error rates, and improved reliability compared to unimodal or simple fusion approaches as defined as set of rules in Figure 8.

Enhanced Clonal Matching Algorithm

Inputs:

$\boldsymbol{F_f}$: Extracted feature vector from face

$\boldsymbol{F_i}$: Extracted feature vector from iris

$\boldsymbol{F_s}$: Extracted feature vector from signature

$\boldsymbol{N}$: Population size (number of antibodies)

$\boldsymbol{T}_{\max}$: Maximum number of iterations

$\boldsymbol{\beta}$: Cloning factor

$\boldsymbol{\rho_0}$: Initial mutation rate

$\boldsymbol{\alpha}$: Adaptive mutation coefficient

$\boldsymbol{f(\cdot)}$: Fitness function (e.g., classification accuracy or recognition rate)

Step 1: Feature Normalization and Concatenation

Each extracted feature vector is normalized using min-max normalization:

$$\boldsymbol{F'_x = \frac{F_x - \min(F_x)}{\max(F_x) - \min(F_x)}} \quad \text{for } \boldsymbol{x \in \{f, i, s\}}$$

Then, concatenate to form the initial fused vector:

$$\boldsymbol{F}_{\text{fused}} = \boldsymbol{[F'_f, F'_i, F'_s]}$$

Step 2: Initialize Antibody Population

Generate an initial antibody population:

$$\boldsymbol{Ab = \{Ab_1, Ab_2, \dots, Ab_N\}}$$

Each antibody $\boldsymbol{Ab_i}$ represents a candidate fused feature subset or weight vector for fusion.

Step 3: Fitness Evaluation

Evaluate the fitness of each antibody using a suitable criterion (e.g., recognition accuracy using an SVM classifier):

$$\boldsymbol{\text{Fitness}(Ab_i) = f(Ab_i) = \text{Accuracy}(Ab_i)}$$

Step 4: Cloning Operation

Clone each antibody in proportion to its fitness value:

$$\boldsymbol{n_i = \text{round}\left(\beta \times \frac{\text{Fitness}\,(Ab_i)}{\max(\,\text{Fitness}\,)}\right)}$$

where

$\boldsymbol{n_i}$: number of clones generated from antibody $\boldsymbol{i}$

$\boldsymbol{\beta}$: cloning rate (usually between 1 and 10)

The cloned population is:

$$\text{Clones} = \boldsymbol{\{Cl_{1,1}, Cl_{1,2}, \dots, Cl_{N,n_4}\}}$$

Step 5: Adaptive Mutation

Each clone undergoes mutation. The adaptive mutation rate is inversely proportional to its fitness:

$$\boldsymbol{\rho_i = \rho_0 \times e^{-\alpha \times \text{Fitness}\,(Ab_i)}}$$

where

$\boldsymbol{\rho_i}$: adaptive mutation rate for antibody $\boldsymbol{i}$

$\boldsymbol{\rho_0}$: initial mutation rate

$\boldsymbol{\alpha}$: adaptation coefficient controlling mutation decay rate

Then, the mutated clone is generated as:

$$\boldsymbol{Cl'_{i,j} = Cl_{i,j} + \rho_i \times \mathcal{N}(0, 1)}$$

where

$\boldsymbol{\mathcal{N}(0, 1)}$: Gaussian noise with mean 0 and variance 1

Mutation increases diversity among clones

Step 6: Selection and Replacement

Compute fitness for all mutated clones $Cl'_{i,j}$ and select the best antibody from each clone group:

$$Ab_i^{\text{new}} = \arg\max_j f(Cl'_{i,j})$$

Combine the selected antibodies to form a new population:

$$Ab^{\text{new}} = \{Ab_1^{\text{new}}, Ab_2^{\text{new}}, \ldots, Ab_N^{\text{new}}\}$$

Replace the worst-performing antibodies in the old population with the best new ones to maintain population diversity.

Step 7: Memory Update

Maintain a memory set M that stores the top-performing antibodies:

$$M = \text{Top}_k(Ab^{new})$$

where k is the memory size.

Step 8: Termination Condition

If $t \geq T_{\max}$ or the fitness has converged (no improvement for several iterations), stop; else, return to Step 3 with updated population.

Step 9: Optimal Fused Feature Vector

The antibody with the highest fitness in the memory set represents the optimized fused feature vector:

$$F_{fused}^{\text{opt}} = Ab^* = \arg\max_{Ab_i \in M} f(Ab_i)$$

Output:

$F_{\text{fused}}^{\text{opt}}$: Optimized fused feature vector

Figure 8: Algorithm for the ECMA

4. CONCLUSION

In this research paper, a face–face-iris-signature biometric recognition system was developed and presented with the promising results, which were not only based on feature-extraction level fusion and an enhanced clonal matching algorithm using support vector machine (SVM), but also the developed system was implemented in MATLAB environment. The developed tri-modal biometric recognition system is more secure, reliable, robust, and accurate than a unimodal biometric recognition system for authentication purposes. The developed system provided solutions to the necessity to solve the issues of affinity maturation (matching) step, parent's affinity (as in standard clonal selection algorithm), and also maintenance of biometric feature origin in multimodal biometric recognition systems. In a tri-modal biometric recognition system, it is extremely difficult for impostors to gain unlawful access to the restricted areas or valuable properties or expensive devices because it is extremely difficult to fraud three biometric traits that were integrated together at the same time.

REFERENCES

[1] T. Ko, "Multimodal biometric identification for large user population using fingerprint, face and iris recognition," in *Proc. IEEE 34th Annu. Int. Carnahan Conf. Security Technology (AIPR Workshop)*, 2005, p. 6.

[2] J. O. Atoyebi *et al.*, "A review of multimodal biometric recognition systems," in *Proc. 1st Int. Conf. Engineering (AUICONE 2025)*, Adeleke University, Nigeria, Apr. 2025.

[3] J. O. Atoyebi *et al.*, "Multibiometric recognition systems: A comprehensive review," *Adeleke Univ. J. Eng. Technol.*, vol. 8, no. 1, pp. 10–38, 2025.

[4] G. S. Walia, T. Singh, K. Singh, and N. Verma, "A robust multimodal biometric system based on optimal score level fusion model," *Expert Syst. Appl.*, vol. 116, pp. 364–376, 2019.

[5] S. Kataria and A. K. Goel, "A hybrid approach for biometric authentication using fusion of fingerprint and signature," *Int. J. Sci. Res. Eng. Technol.*, 2016.

[6] S. Chaudhary and R. Nath, "A robust multimodal biometric system integrating iris, face and fingerprint using multiple SVMs," *Int. J. Adv. Res. Comput. Sci.*, vol. 7, no. 2, 2016.

[7] S. Sheena and M. Sheena, "A study of multimodal biometric system," *Int. J. Res. Eng. Technol.*, 2014.

[8] M. O. Oloyede and G. P. Hancke, "Unimodal and multimodal biometric sensing systems: A review," *IEEE Access*, vol. 4, pp. 7532–7555, 2016.

[9] A. F. Abate, L. Cimmino, I. Cuomo, M. Di Nardo, and T. Murino, "On the impact of multimodal and multisensor biometrics in smart factories," *IEEE Trans. Ind. Informat.*, vol. 18, no. 12, pp. 9092–9100, 2022.
[10] A. Srinivasan and V. Balamurugan, "Occlusion detection and image restoration in the 3D face image," in *Proc. IEEE TENCON*, 2014, pp. 1–6.
[11] P. Kumar *et al.*, "Fusion of neuro-signals and dynamic signatures for person authentication," *Sensors*, vol. 19, no. 21, p. 4641, 2019.
[12] M. Elhoseny *et al.*, "Cascade multimodal biometric system using fingerprint and iris patterns," in *Proc. Int. Conf. Advanced Intelligent Systems and Informatics*, 2018.
[13] U. Sumalatha, K. K. Prakasha, S. Prabhu, and V. C. Nayak, "A comprehensive review of unimodal and multimodal fingerprint biometric authentication systems: Fusion, attacks, and template protection," *IEEE Access*, 2024.
[14] S. M. Alghamdi, S. K. Jarraya, and F. Kateb, "Enhancing security in multimodal biometric fusion: Analyzing adversarial attacks," *IEEE Access*, 2024.
[15] G. K. Kyeremeh *et al.*, "Fusion of hand biometrics for border control involving fingerprint and finger vein," *IEEE Access*, 2025.
[16] A. Achroufene, N. Slimani, and M. Sadi, "Multimodal biometric authentication using face and signature based on Dempster-Shafer theory," in *Proc. 2nd Int. Conf. Electrical Engineering and Automatic Control (ICEEAC)*, May 2024, pp. 1–6.
[17] T. S. Sasikala, "Multimodal secure biometrics using attention Efficient-Net hash compression framework," *Digit. Signal Process.* 2025.
[18] H. M. L. Aung, C. Pluempitiwiriyawej, K. Hamamoto, and S. Wangsiripitak, "Multimodal biometrics recognition using a deep convolutional neural network with transfer learning in surveillance videos," *Computation*, vol. 10, no. 7, p. 127, 2022.
[19] T. S. Ng, C. Y. Low, J. C. L. Chai, and A. B. J. Teoh, "Conditional multimodal biometrics embedding learning for periocular and face in the wild," in *Proc. 26th Int. Conf. Pattern Recognition (ICPR)*, 2022, pp. 812–818.
[20] T. S. Ng *et al.*, "On the representation learning of conditional biometrics for flexible deployment," *IEEE Access*, vol. 11, pp. 82338–82350, 2023.
[21] J. Yoon, C. Esposito, and C. Choi, "Quad-biometrics for few-shot user identification," in *Proc. 39th Annu. ACM/SIGAPP Symp. Appl. Comput. (SAC)*, 2024, pp. 560–564.
[22] D. R. Mdaka *et al.*, "A multimodal authentication method for electronic exams," in *Proc. 2024 Int. Conf. Artificial Intelligence, Big Data, Computing and Data Communication Systems (icABCD)*, Aug. 2024, pp. 1–5.
[23] G. G. Samatas and G. A. Papakostas, "Biometrics: Going 3D," *Sensors*, vol. 22, no. 17, p. 6364, 2022.
[24] J. Samatha and G. Madhavi, "Secure sense: Enhancing person verification through multimodal biometrics," *Scalable Comput.: Pract. Exp.*, vol. 25, no. 2, pp. 1040–1055, 2024.
[25] K. Chang, K. W. Bowyer, S. Sarkar, and B. Victor, "Comparison and combination of ear and face images in appearance-based biometrics," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 25, no. 9, pp. 1160–1165, 2003.
[26] A. F. Abate, L. Cimmino, I. Cuomo, M. Di Nardo, and T. Murino, "On the impact of multimodal and multisensor biometrics in smart factories," *IEEE Trans. Ind. Informat.*, vol. 18, no. 12, pp. 9092–9100, 2022.
[27] I. Deandres-Tame *et al.*, "How good is ChatGPT at face biometrics? A first look into recognition, soft biometrics, and explainability," *IEEE Access*, 2024.
[28] B. Prasanalakshmi *et al.*, "Biometric cryptosystem involving two traits and palm vein as key," *Procedia Eng.*, vol. 30, pp. 303–310, 2012.
[29] S. Shirke, N. Jadhav, S. Kapare, and N. Chaube, "Multimodal biometrics systems using iris scanning and face recognition," *Int. J. Early Childhood Special Educ.*, vol. 14, no. 3, 2022.
[30] J. Hwang and A. B. J. Teoh, "Periocular biometrics enhancement through multimodal embeddings and classifier adaptation," in *Proc. IEEE Int. Conf. Acoustics, Speech and Signal Processing (ICASSP)*, 2024, pp. 4665–4669.
[31] M. Singhal and K. Shinghal, "Secure deep multimodal biometric authentication using online signature and face features fusion," *Multimedia Tools Appl.*, vol. 83, no. 10, pp. 30981–31000, 2024.
[32] S. S. S. Reddy *et al.*, "Multi-modal biometric recognition for face and iris using Gradient Neural Network (Gen-NN)," *MATEC Web Conf.*, vol. 392, p. 01078, 2024.
[33] S. Alshebli, F. Kurugollu, and M. Shafik, "Multimodal biometric recognition using iris and face features," in *Advances in Manufacturing Technology XXXIV*, IOS Press, 2021, pp. 254–262.
[34] S. Li, B. Zhang, L. Fei, S. Zhao, and Y. Zhou, "Learning sparse and discriminative multimodal feature codes for finger recognition," *IEEE Trans. Multimedia*, vol. 25, pp. 805–815, 2021.

[35] B. Alharbi and H. S. Alshanbari, "Face-voice based multimodal biometric authentication system via FaceNet and GMM," *PeerJ Comput. Sci.*, vol. 9, p. e1468, 2023.
[36] C. Vensila and A. B. Wesley, "Multimodal biometrics authentication using extreme learning machine with feature reduction," *Visual Comput.*, vol. 40, no. 3, pp. 1383–1394, 2024.
[37] R. Daza *et al.*, "DeepFace-Attention: Multimodal face biometrics for attention estimation with application to e-learning," *arXiv preprint arXiv:2408.05523*, 2024.
[38] L. C. O. Tiong, D. Sigmund, C. H. Chan, and A. B. J. Teoh, "Flexible biometrics recognition: Bridging the multimodality gap through attention, alignment and prompt tuning," in *Proc. IEEE/CVF Conf. Comput. Vis. Pattern Recognit. (CVPR)*, 2024, pp. 267–276.
[39] C. Tang, M. Qian, R. Jia, H. Liu, and B. Wang, "Forearm multimodal recognition based on IAHP-entropy weight combination," *IET Biometrics*, vol. 12, no. 1, pp. 52–63, 2023.
[40] C. Yuan, S. Jiao, X. Sun, and Q. J. Wu, "MFFFLD: A multimodal-feature-fusion-based fingerprint liveness detection," *IEEE Trans. Cogn. Dev. Syst.*, vol. 14, no. 2, pp. 648–661, 2021.
[41] M. Eskandari, "Integrating a cosmetic detection scheme into face–iris multimodal biometric systems," *Signal, Image Video Process.*, vol. 18, pp. 809–823, 2024.
[42] S. A. Shaban, H. M. Ahmed, and D. L. Elsheweikh, "A novel fusion system based on iris and ear biometrics for e-exams," *Intell. Autom. Soft Comput.*, vol. 35, no. 3, 2023.
[43] J. Oyeniyi and O. Oyeniran, "Bimodal biometric recognition system based on score level fusion," *Int. J. Eng. Artif. Intell.*, vol. 1, no. 4, pp. 71–76, 2020.
[44] H. Purohit, M. Dadhich, and P. K. Ajmera, "Analytical study on users' awareness and acceptability towards adopting multimodal biometrics," *Multimedia Tools Appl.*, vol. 82, no. 9, pp. 14239–14263, 2023.
[45] G. K. Kyeremeh, M. Abdul-Al, R. Qahwaji, N. T. Ali, and R. A. Abd-Alhameed, "Fusion of Hand Biometrics for Border Control Involving Fingerprint and Finger Vein", *IEEE Access*, 2025.
[46] T. S. Sasikala, "Multimodal Secure Biometrics using Attention Efficient-Net Hash Compression Framework," Digital *Signal Processing*, 105018. 2025.