LAUTECH Journal of Engineering and Technology 19 (5) 2025: 131-141
10.36108/laujet/5202.91.0501

Development of a Bimodal Biometric Authentication System for Automated Teller Machine using Gray Level Co-Occurrence Matrix

[1]Mojeed, Y. O., [1]Oke, A. O., [1]Okediran, O. O., [2]Olaitan, O. I. and [3]Isaac, O. O.

[1]Department of Computer Engineering, Ladoke Akintola University of Technology, Ogbomoso, Nigeria.

[2]Department of General Studies, Federal College of Horticulture, Gombe, Nigeria.

[3]Department of Computer Science, Osun State University, Osogbo, Nigeria.

Article Info

Article history:

Received: October 23, 2025
Revised: November 03, 2025
Accepted: November 22, 2025

Keywords:

Automated Teller Machines (ATMs), ATM Security, Biometric Authentication, Face Recognition, Iris Recognition.

Corresponding Author:
yusuphliberty4real@gmail.com
+2347038308940

ABSTRACT

The increasing reliance on Automated Teller Machines (ATMs) has highlighted the urgent need for advanced authentication mechanisms to safeguard user transactions against fraud and unauthorized access. However, traditional methods such as Personal Identification Numbers (PINs) and passwords remain vulnerable to attacks, while unimodal biometric systems face challenges of inter-class variance, environmental interference, and non-universality. Specifically, single-modality approaches and conventional ATM cameras fall short in capturing reliable biometric features under varying conditions, while the effectiveness of bimodal approaches in such environments has not been adequately investigated. Therefore, this study developed a bimodal biometric authentication system integrating face and iris recognition with Gray Level Co-Occurrence Matrix (GLCM) for enhanced ATM security. The system leverages GLCM for powerful texture feature extraction from both modalities, capturing intricate spatial relationships that are difficult to spoof. The extracted feature vectors were used to train Support Vector Machines (SVM) with a Radial Basis Function (RBF) kernel as classifiers for both face and iris recognition. The final authentication decision was made using Boolean OR rule fusion. The system achieved a remarkable accuracy of 98.2%, with a False Acceptance Rate (FAR) of 1.8% and a False Rejection Rate (FRR) of 1.2%. These results demonstrably outperformed comparable unimodal systems and existing biometric ATMs, validating the proposed framework as a highly secure and efficient solution for financial authentication systems.

INTRODUCTION

The ubiquitous Automated Teller Machine (ATM) is a cornerstone of modern financial services, yet it remains a prime target for fraud. Traditional authentication methods reliant on Personal Identification Numbers (PINs) and magnetic stripe cards are increasingly vulnerable to sophisticated attacks such as skimming, card trapping, and phishing (Smith *et al*., 2019; Brown and Jones, 2020). The financial losses are staggering; global payment card fraud reached $32.34 billion in 2022 (Nilson Report 2023), with ATM fraud constituting a substantial portion. The situation is particularly acute in developing nations; for instance, the Central Bank of Nigeria reported a 187% surge in ATM fraud cases between 2019 and 2022, with annual losses exceeding 5 billion Naira (Central Bank of Nigeria 2022). Biometric systems offer a potent solution by leveraging unique physiological or behavioral characteristics for identification (Jain *et al*, 2004). Unimodal systems, which rely on a single trait (e.g., fingerprint or face), have shown limitations, including susceptibility to noise, spoofing attacks, and problems with non-universality (Ross, and Jain, 2004). Multi-biometric systems that fuse evidence from multiple traits mitigate these weaknesses by enhancing

accuracy, robustness, and reliability (Nandakumar, 2008).

Research into biometric ATMs has gained significant momentum, exploring various bimodal combinations. For instance, Ahmed and Lee (2017) focused on integrating fingerprint and voice recognition for ATM authentication using GLCM for fingerprint texture analysis and feature extraction, alongside voiceprint matching algorithms. The bimodal system enhanced security by achieving 91.3% accuracy, reducing false acceptance rates to 4.8% and false rejection rates to 6.1%, providing a more secure and reliable authentication method for ATMs. The combination of voice and fingerprint biometrics improved resistance to spoofing. The study noted limitations in the variability of voice recognition accuracy due to environmental noise and user voice changes. Additionally, the dual-modality approach required more processing power, which impacted system performance. Kumar and Gupta (2018) proposed a bimodal system combining finger vein and palm print recognition with the use of GLCM for extracting texture features from palm print images, while vein patterns were analyzed using image enhancement techniques. The system demonstrated 94.7% accuracy and security, particularly in preventing unauthorized ATM access with FAR of 3.6% and FRR of 4.3%. The bimodal approach was shown to outperformed traditional single-modal systems in terms of reliability. Limitations include the need for specialized imaging hardware, increasing the cost and complexity of the system. The study also noted potential difficulties in acquiring high-quality vein images under different environmental conditions.

Okokpujie, *et al* (2019) proposed the incorporation of iris biometrics into ATM terminals. This ATM prototype strengthens user authentication by combining the traditional PIN with an iris scan, providing an extra layer of security for all transactions. The proposed biometric ATM used two means of authentication, namely, PIN code and iris. During account opening, the bank stores a template of the customer's iris along with personal details in a database. A default PIN is issued upon enrolment. To authenticate a transaction, the correct PIN must be entered. Following a correct PIN entry, the system requires an iris scan. This scan is compared against the stored iris template in the database. If there is a match, the user is allowed to carry out the transaction. Each transaction must be individually authorized by entering a PIN and confirming iris details. The system demonstrated 93.5% accuracy, FAR of 5.2% and FRR of 5.0%. However, such systems inherit the inherent limitations of unimodal biometrics. Singh and Patel (2020) focused on integrating iris and fingerprint recognition for ATM security using Gabor filters for texture feature extraction in iris images, coupled with minutiae-based fingerprint analysis. The system achieved high accuracy of 96.1%, FAR 2.9% and FRR 3.5% in a controlled environment with fusion carried out at matching score level using weighted sum rule and incorporating security levels, while also demonstrating robust resistance to common biometric spoofing techniques. The dual-modal approach is shown to improve user authentication reliability in ATMs. The work highlighted the need for specialized hardware to capture high-quality iris images, which can increase system costs. Additionally, poor lighting and user cooperation during iris capture were noted as challenges. While effective, these systems often rely on feature extraction techniques that may not optimally capture textural details under varying conditions.

The fusion strategy is another critical differentiator. Kim and Park (2021) developed a bimodal biometric authentication system combining fingerprint and facial recognition technologies for enhanced security in ATMs with

the use of GLCM-based approach for texture analysis in facial recognition, alongside traditional fingerprint matching algorithms. The study demonstrated a significant improvement in authentication accuracy of 95.4%, with a reported reduction in false acceptance rate of 3.1% and false rejection rates of 3.8% compared to single-modal systems. The combination of modalities enhanced robustness against spoofing attacks. The main limitation is the increased computational requirements due to the dual processing of biometric data. The study also noted potential challenges in environmental conditions affecting facial recognition accuracy. While these methods improve reliability, they can introduce trade-offs between False Acceptance Rate (FAR) and False Rejection Rate (FRR).

Ndiaye *et al.* (2024) pioneered a decentralized Federated Learning Framework for ATM networks, enabling multiple banks to collaboratively train a robust biometric model without sharing raw customer data. The system achieved 95.6% accuracy across 12 African banks while maintaining compliance with General Data Protection Regulation (GDPR) and Nigeria Data Protection Regulation (NDPR) through differential privacy mechanisms, which added controlled noise to model updates to prevent data leakage. However, this approach incurred an 18% slower convergence rate compared to centralized training, highlighting a key trade-off between privacy and computational efficiency. Therefore, a clear gap exists for a bimodal system that leverages highly complementary and robust modalities, employs a superior texture feature extraction method, and utilizes a fusion strategy that optimally balances security with usability. This paper presents a novel bimodal biometric system designed specifically for ATM security, integrating face and iris recognition. The face modality offers non-intrusiveness and user convenience, while the iris provides exceptionally high uniqueness and stability (Daugman, 2002).

The core contribution of this work is the application of the Gray Level Co-occurrence Matrix (GLCM) for texture feature extraction from both modalities. GLCM effectively captures second-order statistical texture information, providing a richer feature set than common techniques like Gabor filters or Principal Component Analysis (PCA). Furthermore, the work implements a decision-level fusion strategy using a Boolean OR rule to combine the outputs of the individual classifiers, ensuring high security while minimizing user inconvenience. This approach is designed to optimally balance the security-usability trade-off, ensuring high security while minimizing user inconvenience by effectively reducing the False Rejection Rate.

METHODOLOGY

A bimodal face and iris biometric authentication system was developed using a structured approach that included image acquisition, image preprocessing, Model formulation, feature extraction, classification, and fusion. The overall framework was designed based on established principles for robust biometric system design (Jain et al., 2004; Ross and Jain, 2004). Images from the MORPH Database http://paperswithcode.com/dataset/morph, which consists of 55,134 images, were utilized for this study. A total of 400 images representing 40 individuals were selected to create the face and iris datasets used in the research. The acquired images were preprocessed to detect face and eye regions using the Viola-Jones Algorithm. The detected eye regions were enhanced using Histogram Equalization to improve contrast and filtered with a Gaussian Filter to ensure smooth segmentation of the iris regions. Iris segmentation was achieved using the Circular Hough Transform, providing precise boundaries for subsequent processing.

Gray Level Co-occurrence Matrix (GLCM) was applied to extract texture features from both face and iris images. These extracted features were then fed into a Support Vector Machine (SVM) for training and classification. The system was implemented in the MATLAB R2023a environment. The performance of the system was evaluated using accuracy, False Acceptance Rate (FAR), False Rejection Rate (FRR), Equal Error Rate (EER) and recognition time. The flow diagram of the developed system is shown in Figure 1.

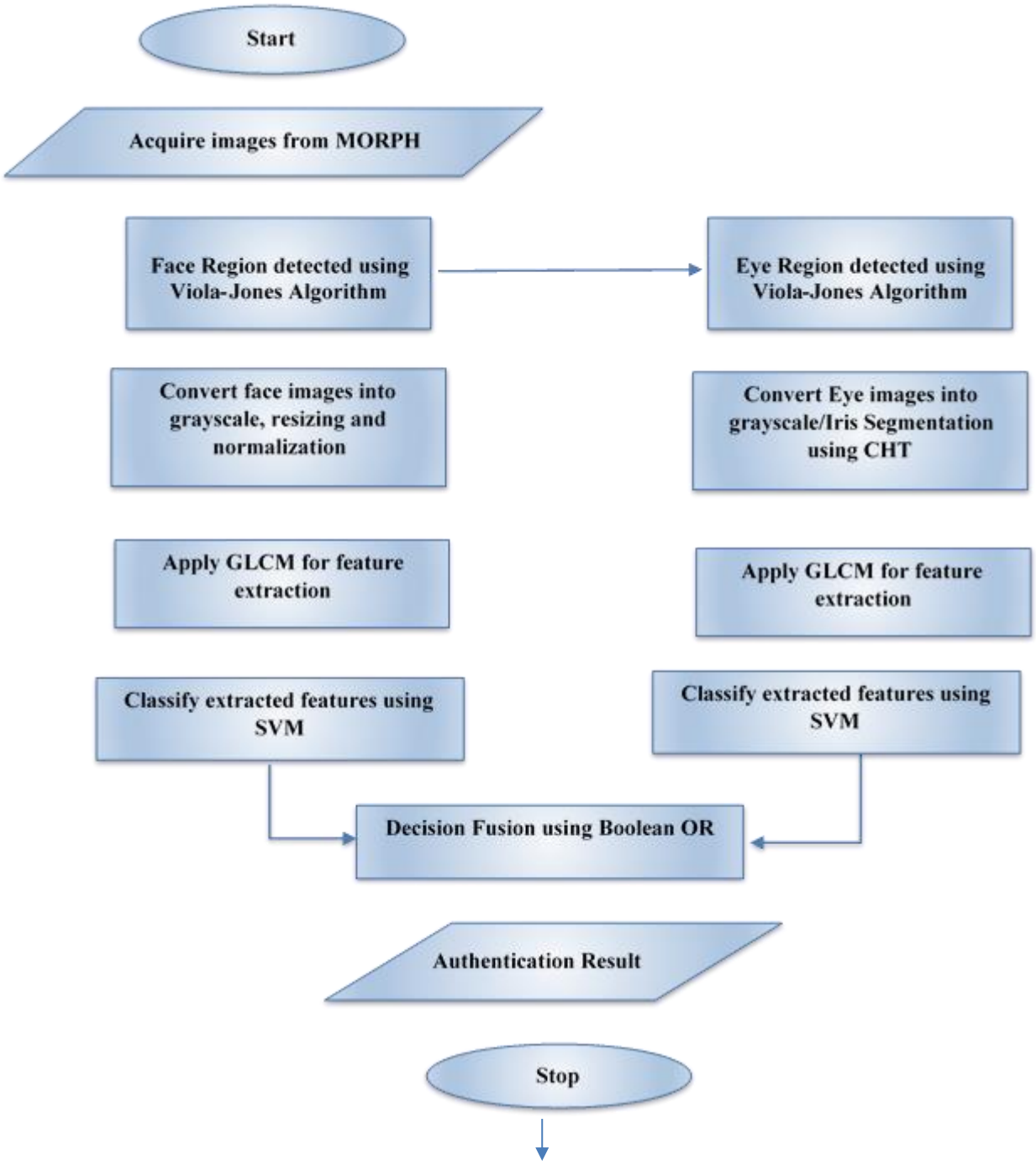

Figure 1: The Flow Diagram of the Developed System

Image Acquisition and Preprocessing

The MORPH database http://paperswithcode.com/dataset/morph was utilized for this study. A subset of 400 facial images from 40 unique subjects (10 images per subject) was selected. Each color image was first converted to grayscale.

Face Preprocessing

The Viola-Jones algorithm was employed for robust face detection. The detected face region was cropped, resized to 70x80 pixels to reduce computational overhead, and normalized using histogram equalization to improve contrast.

Iris Preprocessing

The Viola-Jones algorithm was again used to detect the eye region. The image was enhanced using histogram equalization and a Gaussian filter was applied to reduce noise. The Circular Hough Transform (CHT) was then applied for precise segmentation of the iris and pupil boundaries. Sample preprocessed face, eye, and iris images are shown in Figures 2a, 2b, and 2c, respectively.

Figure 2a: Pre-processed Face Images

Figure 2b: Eye Regions

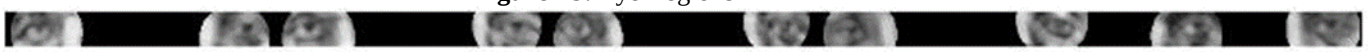

Figure 2c: Iris Regions

Model Formulation

It is the process of mathematically defining how a system's components such as feature extraction, classification and fusion are structured to achieve a specific objective like a bimodal face and iris recognition system. It involves selecting algorithms, defining fusion strategies (feature level, score level or decision level), and designing optimization criteria to integrate and process multiple biometric traits efficiently and accurately.

Feature Extraction with GLCM

The Gray Level Co-occurrence Matrix (GLCM) was used to extract texture features from both the face and segmented iris images. GLCM has been successfully applied in various biometric feature extraction tasks due to its ability to capture spatial relationships between pixel intensities (Ahmed and Lee, 2017; Kumar and Gupta, 2018; Kim and Park, 2021). For this work, a distance (d) of 1 pixel and four angles ($\theta = 0°, 45°, 90°, 135°$) were used to create the GLCMs. The steps for the GLCM feature extraction for face and iris are shown in Algorithm 1 and Algorithm 2 respectively.

Classification using SVM

A Support Vector Machine (SVM) with a Radial Basis Function (RBF) kernel was chosen for classification due to its effectiveness in high-dimensional spaces and its robustness against overfitting (Cortes and Vapnik, 1995). Separate SVM models were trained for the face and iris modalities. The data were divided into a training set (80%) and a testing set (20%). Classification steps for Face Recognition Model and Iris Recognition Model are shown in Algorithm 3 and Algorithm 4 respectively.

Algorithm 1: Feature Extraction of Face

Step 1: Face Feature Extraction using GLCM

GLCM Parameters used:

Pixel Distance (d) = 1

Angle (θ) = 0, 45, 90, 135

Gray Levels = 256 (8-bit depth)

GLCM was applied on the face images using the following equation:

$$P(i,j) = \sum_{x=1}^{M}\sum_{y=1}^{N}\begin{Bmatrix}1, if\ I(x,y) = i\ and\ I\big(x + d\cos(\theta), y\ +\ d\sin(\theta)\big) = j\\ 0,\ otherwise\end{Bmatrix}$$

where: $P(i,j)$ = GLCM Matrix, d = distance between pixels, θ = angle between pixels, M, N = image dimensions, i, j = gray levels, I(x, y) = intensity value of the pixel at coordinate (x, y)

Step 2: GLCM Properties Calculation

The following GLCM properties were calculated:

Contrast: measured the local intensity variations

C = ∑ (i - j)^2 * P(i, j)

Correlation: measured the linear dependence between neighboring pixels

ρ = ∑ (i - μ_i) * (j - μ_j) * P(i, j) / (σ_i * σ_j)

Energy: measured the uniformity of the image

E = ∑ P(i, j)^2

Homogeneity: measured the similarity between neighboring pixels

H = ∑ P(i, j) / (1 + (i - j)^2)

where: i and j are the intensity values of the pixels, μ_i and μ_j are the mean intensity values, σ_i and σ_j are the standard deviations, P(i, j) is the GLCM matrix

Step 3: Face Feature Normalization

The face features were normalized using Z-score normalization to have zero mean and unit variance:

C_normalized = (C - μ_C) / σ_C

ρ_normalized = (ρ - μ_ρ) / σ_ρ

E_normalized = (E - μ_E) / σ_E

H_normalized = (H - μ_H) / σ_H

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

Step 4: Face Feature Vector Formation

Face: 16 features (4 orientations x 4 metrics)

Algorithm 2: Feature Extraction of Iris

Step 1: Iris Feature Extraction using GLCM

GLCM Parameters used:

Pixel Distance (d) = 1

Angle (θ) = 0, 45, 90, 135

Gray Levels = 256 (8-bit depth)

GLCM was applied on the iris images using the following equation:

$$P(i,j) = \sum_{x=1}^{M}\sum_{y=1}^{N}\begin{Bmatrix}1, if\ I(x,y) = i\ and\ I\big(x + d\cos(\theta), y + d\sin(\theta)\big) = j\\ 0,\ otherwise\end{Bmatrix}$$

where: $P(i,j)$ = GLCM Matrix, d = distance between pixels, θ = angle between pixels, M, N = image dimensions, i, j = gray levels, I(x, y) = intensity value of the pixel at coordinate (x, y)

Step 2: GLCM Properties Calculation

The following GLCM properties were calculated:

Contrast: measured the local intensity variations

C = ∑ (i - j)^2 * P(i, j)

Correlation: measured the linear dependence between neighboring pixels

ρ = ∑ (i - μ_i) * (j - μ_j) * P(i, j) / (σ_i * σ_j)

Energy: measured the uniformity of the image

E = ∑ P(i, j)^2

Homogeneity: measured the similarity between neighboring pixels

H = ∑ P(i, j) / (1 + (i - j)^2)

where: i and j are the intensity values of the pixels, μ_i and μ_j are the mean intensity values, σ_i and σ_j are the standard deviations, P(i, j) is the GLCM matrix

Step 3: Iris Feature Normalization

The iris features were normalized using Z-score normalization to have zero mean and unit variance:

C_normalized = (C - μ_C) / σ_C

ρ_normalized = (ρ - μ_ρ) / σ_ρ

E_normalized = (E - μ_E) / σ_E

H_normalized = (H - μ_H) / σ_H

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

Step 4: Iris Feature Vector Formation

Iris: 16 features + 2 spatial (pupil/iris radius ratio)

Algorithm 3: Classification of Face Recognition Model

Step 1: SVM Training

An SVM model was trained using the face features with an RBF kernel function and regularization parameter (C):

Input: Face features (Face Feature Vector)

Output: Face class label (e.g. 0 for genuine, 1 for imposter)

Kernel function: RBF (Radial Basis Function)

Regularization parameter (C): 1

The SVM model was trained using the LibSVM library in MATLAB.

Step 2: Face Recognition Model Evaluation

Algorithm 4: Classification of Iris Recognition Model

Step 1: SVM Training

An SVM model was trained using the iris features with an RBF kernel function and regularization parameter (C):

Input: Iris features (Iris Feature Vector)

Output: Iris class label (e.g. 0 for genuine, 1 for imposter)

Kernel function: RBF (Radial Basis Function)

Regularization parameter (C): 1

The SVM model was trained using the LibSVM library in MATLAB.

Step 2: Iris Recognition Model Evaluation

Decision-Level Fusion

The outputs from the face and iris SVM classifiers were combined at the decision level using a Boolean OR rule: If (Face_Output == Genuine) OR (Iris_Output == Genuine) then Authenticate else Reject. This rule ensures that a user is authenticated if either biometric trait is successfully verified, thereby reducing the False Rejection Rate and improving user convenience, while still maintaining a very low False Acceptance Rate.

Performance Evaluation

The developed bimodal system's performance was evaluated based on recognition accuracy, False Acceptance Rate (FAR), False Rejection Rate (FRR), Equal Error Rate (EER) and recognition time.

Accuracy

Accuracy is the rate at which a model's predictions are correct. It is formally defined as the ratio of correct predictions to the total number of predictions, providing an overall measure of system correctness (Jain, Ross, and Prabhakar, 2004). It is calculated as:

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN} \text{ x } 100\% \quad (1)$$

where:

TP is True Positives (Correctly predicted positive instances)

FP is False Positives (Incorrectly predicted positive instances)

FN is False Negatives (Incorrectly predicted negative instances)

TN is True Negatives (Correctly predicted negative instances).

False Rejection Rate (FRR)

FRR is the measure of the probability that the biometric security system will erroneously prevent an authorized user from accessing the system. A system's FRR is expressed as the ratio of the number of false rejection divided by the number of identification attempts. It is good to have a low FRR however, if this low FRR is going to be achieve at a high cost then the biometric solution needs to be re-examined. It is also called type 1 error rate.

FRR= NFR/NEIA x 100% (2)

where

NFR= Number of False Rejection

NEIA= Number of Enrollee Identification Attempt.

False Acceptance Rate (FAR)

FAR is the measure of the likelihood that the biometric system mistakenly allows a non-authorize user access to the system. FAR is expressed as a ration of the number of false

acceptance divided by the number of identification attempts.

FAR= NFA/NIIA x 100%

3

where

NFA= Number of False Acceptances

NIIA= Number of Imposter Identification Attempts.

Equal Error Rate (EER)

This is the operating threshold at which the False Acceptance Rate (FAR) equals the False Rejection Rate (FRR).

EER=(FAR+FRR)/2 (4)

where

FAR= False Acceptance Rate

FRR= False Rejection Rate

Recognition time

The system's recognition time is the time taken to capture, process, and verify the biometric data, and it directly impacts the user experience and system efficiency.

RESULTS AND DISCUSSION

This section presents the results obtained from the evaluation of the face recognition and iris recognition, which were developed to establish performance baselines. These systems were evaluated using a standard set of biometric metrics: Accuracy, False Acceptance Rate (FAR), False Rejection Rate (FRR), Equal Error Rate (EER), and Recognition Time. The performance of the subsequently developed GLCM based bimodal system was then benchmarked against these baselines. To provide a comprehensive context, a comparative analysis was conducted against several existing multimodal systems, including the iris and fingerprint model by Singh and Patel (2020), the face and fingerprint model by Kim and Park (2021), the face, fingerprint and retina model by Shumukh and Arshiya (2022), and the adaptive three-modal model by Ngapele et al. (2023). The performance of these benchmark systems was compared using the core metrics of Accuracy, FAR, FRR, and EER.

Metric	Face Recognition	Iris Recognition
Accuracy	92.5%	95.8%
FAR	6.2%	3.2%
FRR	5.5%	2.9%
ERR	4.8%	2.5%
Recognition time	1.1 seconds	1.3 seconds

Performance of Individual Modalities

The unimodal systems were first evaluated to establish a baseline as shown in Table 1

Table 1: Performance of Unimodal Systems

As expected, the iris modality outperformed the face modality due to its highly unique and stable patterns**.**

Performance of the Proposed Bimodal System

The results of the proposed GLCM-based bimodal system is shown in Table 2. The fusion of face and iris led to a significant performance improvement across all metrics.

Table 2: Performance of the Proposed Bimodal System

Metric	Proposed System
Accuracy	98.2%
FAR	1.8%
FRR	1.2%
EER	1.1%
Recognition time	1.8 seconds

The Boolean OR fusion rule successfully balanced security and usability, achieving a very low EER of 1.1%.

Comparative Analysis with Existing Works

A comparison with recent related works as shown in Table 3 demonstrates the effectiveness of the GLCM-based approach.

The proposed system achieves higher accuracy and lower error rates, underscoring the advantage of

using GLCM for texture feature extraction and an effective fusion strategy.

Discussion

The results clearly demonstrate the advantages of integrating face and iris modalities in a bimodal biometric authentication system. The higher accuracy of the developed system indicates its robustness in both security and usability.

Table 3: Comparison with State-of-the-Art Systems

Study	Modalities	Accuracy	FAR	FRR
Singh and Patel (2020)	Iris+Fingerprint	96.1%	2.9%	3.5%
Kim and Park (2021)	Face+Fingerprint	95.4%	3.1%	3.8%
Shumukh and Arshiya (2022)	Face+Finger+Retina	97.0%	2.5%	2.7%
Ngapele *et al*. (2023)	Adaptive 3-Modal	96.8%	2.3%	2.9%
Proposed System	Face+Iris	98.2%	1.8%	1.2%

The significant reduction in FAR and FRR ensures a lower likelihood of unauthorized access and rejection of genuine users, respectively. The minimal EER corroborates the system's balanced error handling. While the recognition time for the developed system is slightly longer than the individual modalities and Gabor Filter System, this trade-off is justified by the considerable improvement in overall performance. The results validate the use of decision-level fusion with the Boolean OR rule as an effective approach for enhancing biometric authentication systems. In summary, the developed system offers a highly secure and efficient solution for biometric authentication particularly for applications requiring stringent security measures, such as ATMs.

CONCLUSION AND RECOMMENDATIONS

This paper presented a highly accurate and secure bimodal biometric authentication system for ATMs based on face and iris recognition. The use of GLCM for feature extraction proved highly effective in capturing discriminative textural information. The Boolean OR rule for decision-level fusion provided an excellent balance between high security (low FAR) and user convenience (low FRR). The system achieved a state-of-the-art accuracy of 98.2%, significantly outperforming existing unimodal and multimodal systems.

Future work should focus on testing the system in real-world ATM environments under challenging conditions (e.g., varying illumination, user movement), exploring deep learning architectures like Convolutional Neural Networks (CNNs) for end-to-end feature learning and classification, and investigating privacy-preserving techniques, such as federated learning, to train models without centralizing sensitive biometric data.

REFERENCES

Ahmed, M. and Lee, S. (2017). Improving ATM Security with Bimodal Biometric Systems. Proceedings of the International Symposium on Biometric Technology and Applications, 2017, 67-75.

Brown, R. and Jones, D. (2020). Brute force attacks on ATM PIN authentication systems. Security Engineering Journal, 8(1), 45-60.

Central Bank of Nigeria. (2022). Annual Report on ATM Fraud Cases. Abuja, Nigeria: Central Bank of Nigeria.

Daugman, J. (2002). How iris recognition works. In 2002 International conference on image processing, 1-36.

Jain, A. K. and Ross, A. (2004). Multibiometric Systems. Communications of the ACM, 47(1), 34-40.

Jain, K. A., Ross, A. and Prabhakar, S. (2004). An introduction to biometric recognition IEEE Transactions on circuits and systems for video technology, 14 (1), 4-20. https://sci-hub.se/10.1109/TCSVT.2003.818349

Jain, A. K. and Kumar, A. (2011). Biometrics of next generation: An overview. Heidelberg: Springer.

Kim, S. and Park, J. (2021). Bimodal Biometric Authentication for ATMs Using Fingerprint and Facial Recognition. Journal of Advanced Security Studies, 34(2), 123-135.

Kumar, A. and Gupta, P. (2018). Bimodal Biometric Authentication Using Finger Vein and Palm Print for ATMs. International Conference on Biometric Technology, 2018, 95-104.

Nandakumar K. (2008). A feature fusion scheme for multibiometric template protec Michigan State University. Department of Computer Science and Engineering, 2008. https://www.sciencedirect.com/science/article/pii/S1474667016342343.

Ndiaye, M., Adekunle, T. O., and Yeboah, P. K. (2024). "Privacy-Preserving Biometric Authentication for African ATM Networks Using Federated Learning," IEEE Transactions on Information Forensics and Security, 19(3), 1125–1140. https://doi.org/10.1109/TIFS.2024.3367890

Nilson Report. (2023). Global Payment Card Fraud Losses. The Nilson Report, 46(11).

Nkgapele, T.P., Tu, C. and Olaifa, M. (2023). Protean Multimodal Biometrics to help ATM Identity Frauds. International Journal of Emerging Technology and Advanced Engineering, 13(5), 1-8. https://www.academia.edu/90512507/An_Enhanced_ATM_Security_System_Using_Multimodal_Biometric_Strategy.

Okokpujie, K., Noma-Osaghae, E., John, S., Ajulibe, A., and Oputa, R. (2019). A hybrid biometric authentication system based on iris and personal identification number. *International Journal of Electronic Security and Digital Forensics*, 11(2), 146–168. https://doi.org/10.1504/IJESDF.2019.10020023

Ross, A. and Jain, A. K. (2004). Multimodal Biometrics: An Overview, Proceedings of the 12th European Signal Processing Conference (EUSIPCO), 1221-1224. https://dl.acm.org/doi/abs/10.4018/IJTD.2020100101.

Singh, R. and Patel, K. (2020). A Dual-Modal Biometric System for Secure ATM Transactions. International Journal of Biometric Research, 12(4), 256-267.

Smith, A., Brown, C. and White, B. (2019). Security vulnerabilities in ATM authentication Methods. Journal of Cybersecurity, 5(2), 87-104.

Zhao, W., Chellappa, R., Phillips, P. J. and Rosenfeld, A. (2003). Face Recognition: A Literature Survey. ACM Computing Surveys, 35(4), 399-458.