International Journal of Science and Research (IJSR)
ISSN: 2319-7064
Impact Factor 2025: 7.089

TRIOSECURE: An Encoded Image-Based Biometric Authentication Framework

Kannan M[1], Rinsa Rees[2]

[1]Department of Computer Applications, Musaliar College of Engineering & Technology, Pathanamthitta, Kerala, India
Email: *kannanmalayil123[at]gmail.com*

[2]Assistant Professor, Department of Computer Applications, Musaliar College of Engineering & Technology, Pathanamthitta, Kerala, India

Abstract: ***TrioSecure is a proposed image-based biometric authentication framework designed to address the critical limitations of existing biometric systems, including privacy leakage, spoofing attacks, and lack of explainability. Unlike conventional systems that store raw biometric images, TrioSecure converts biometric data from face, fingerprint, and iris modalities into encoded pixel representations using a custom encryption algorithm, thereby eliminating direct exposure of sensitive biometric data. Authentication is governed by a trio-verification mechanism comprising encoded feature comparison, Large Language Model (LLM)-based adversarial anomaly detection, and Natural Language Processing (NLP)-based semantic validation. LLMs analyze multimodal embeddings and associated metadata to generate human-readable explanations for each authentication decision, providing transparency and auditability. The system supports real-time encoding, spoof detection against advanced threats such as deepfakes and replay attacks, and explainable authentication outcomes. Built using Python, OpenCV, NumPy, and Flask, TrioSecure offers a secure, scalable, and cost-effective solution for modern identity verification systems that demand both high security and user-interpretable decision-making.***

Keywords: TrioSecure, Biometric Authentication, Pixel Encoding, LLM-Based Spoof Detection, Explainable AI, Multimodal Biometrics, Privacy-Preserving Authentication, Adversarial Attack Detection, NLP Explanation Generation, Template Protection

1. Introduction

In today's rapidly evolving digital environment, secure and reliable authentication is a foundational requirement for protecting sensitive systems and personal data. Traditional authentication methods such as passwords, PINs, and ID cards remain widely deployed but are inherently vulnerable to theft, guessing, phishing, and physical duplication. These weaknesses have driven widespread adoption of biometric authentication systems that rely on unique physiological characteristics such as facial features, fingerprints, and iris patterns to verify identity with greater confidence.

Despite their advantages, existing biometric authentication systems continue to face significant challenges. Raw biometric images are frequently stored in databases, creating severe privacy risks in the event of a data breach. Furthermore, such systems remain vulnerable to sophisticated spoofing attacks using photographs, videos, or fabricated biometric artifacts. The opacity of authentication decisions also undermines user trust and regulatory compliance, as most systems provide no explanation for granting or denying access. The emergence of deepfake technology has made adversarial attacks increasingly difficult to detect using conventional methods alone.

TrioSecure is proposed as an advanced biometric authentication framework that directly addresses these limitations by emphasizing privacy preservation, adversarial robustness, and decision explainability. The system encodes raw biometric images into secure pixel representations using a custom encryption algorithm, ensuring that original biometric data is never stored. Authentication proceeds through a trio-verification mechanism involving encoded feature comparison, LLM-based adversarial anomaly detection, and NLP-based semantic validation. By generating human-readable explanations for every authentication decision and supporting real-time processing, TrioSecure delivers a secure, transparent, and scalable identity verification solution suitable for modern digital infrastructures.

2. Related Works

"Multimodal LLM-Enhanced Biometric Authentication Framework" – Ravi Ray (2025)
This study proposes combining LLM reasoning with multimodal biometric and behavioral signals to improve spoof detection and provide textual explanations for authentication outcomes. However, the work appears exploratory with limited empirical validation, and scalability and latency have not been thoroughly evaluated.

"Integrating Explainable AI with Synthetic Biometric Data" – H. Aldawsari (2025)
Aldawsari explores the use of synthetic, privacy-friendly biometric data combined with explainable AI methods to reduce dataset sensitivity while maintaining explainability. Data realism and transfer to real-world performance are not fully demonstrated, and potential distribution-shift issues remain.

"Privacy-Preserving Techniques in Biometric Systems – Approaches and Challenges" – ResearchGate Survey (2025)
This survey provides a contemporary taxonomy of privacy techniques including template protection, encryption, and synthetic data generation, along with discussion of application trade-offs. Due to its broad scope, each technique receives limited depth, and practical deployment guidance on performance and latency is sparse.

"Explainable Biometrics: A Systematic Literature Review" – C. Tucci et al. (2024)
Tucci and colleagues provide a systematic review of explainable AI methods applied to biometric systems, categorizing explanation techniques and identifying research gaps. As a survey, it does not propose or evaluate a new method and may quickly become outdated in fast-moving subfields.

"Biometric Template Attacks and Recent Protection Mechanisms"- S.M. Abdullahi (2024)
This work presents a detailed discussion of template attack classes and protection techniques, including cryptographic approaches such as homomorphic encryption. However, many protection schemes are presented conceptually, and empirical evidence for irreversibility and renewability across real datasets is often missing.

"Multimodal Biometric Integration: Trends and Insights"- WJARR (2024)
This paper reviews multimodal fusion strategies and demonstrates how combining biometric modalities improves robustness to spoofing and noise. The recommendations are general rather than end-to-end prototypes, and multimodal fusion increases system complexity and cost.

"Multimodal Biometric Recognition Systems"- H. Es-Sobbahi et al. (2023)
This work presents experimental comparisons and dataset-driven analysis for multimodal fusion across modalities, demonstrating improved recognition rates. Limitations regarding generalizability across diverse datasets are noted.

"Exploring the Security of Mobile Face Recognition"- MDPI Applied Sciences (2023)
This paper provides a thorough catalogue of spoofing attacks targeting mobile face recognition systems and surveys lightweight defenses suitable for constrained devices. The defenses may not generalize to high-security stationary systems and do not cover LLM-driven explainability.

"Biometric Template Protection for Neural-Network-based Face Recognition Systems"- Krivokuc´a Hahn & Marcel (2021)
This survey provides a strong taxonomy of template protection methods for neural network-based face recognition, covering evaluation metrics and reproducibility concerns. The focus on face recognition alone limits generalizability, and many proposals lack publicly available code.

"Deep Secure Encoding: An Application to Face Recognition" – ResearchGate (2015)
This early work introduced the concept of encoding deep features to avoid storing raw biometric images, serving as a conceptual predecessor to modern pixel and feature encoding approaches. The older deep learning models used were less capable, and large-scale cryptographic guarantees were not addressed.

3. Methodology

The proposed TrioSecure system is designed to perform secure, privacy-preserving biometric authentication using a multi-layered verification pipeline that combines pixel-level encoding, machine learning-based template matching, LLM-driven adversarial detection, and NLP-based explanation generation. The overall methodology encompasses biometric image acquisition, pixel encoding, template storage and matching, attack detection, and explainable decision output.

3.1 System Architecture

The TrioSecure system follows a modular architecture consisting of the following components:
- Biometric Image Acquisition Module
- Pixel Encoding Module
- Encoded Template Database
- Template Matching Module
- LLM-Based Attack Detection Module
- Explanation Generation Module
- Authentication Result Interface

The user initiates authentication by presenting biometric data through a camera or scanner. The acquired image is immediately encoded into a secure pixel representation using OpenCV and NumPy-based transformation techniques, ensuring no raw biometric data is stored. The encoded template is compared with stored templates using a machine learning similarity model. The LLM-based attack detection module then analyzes multimodal embeddings for signs of spoofing or adversarial manipulation. Finally, the NLP-based explanation module generates a human-readable justification for the authentication outcome, which is returned to the user as either access granted or denied.

3.2 Image Capture and Preprocessing

The first stage of the TrioSecure pipeline involves capturing live biometric data from the user using camera or scanner hardware. The acquired biometric image undergoes preprocessing to enhance quality and prepare it for encoding. The preprocessing steps include:
- Image resizing and normalization
- Noise removal and denoising
- Contrast enhancement
- Image sharpening
- Biometric region of interest detection

These preprocessing techniques ensure consistent image quality across varying lighting conditions, capture angles, and device types, thereby improving the accuracy of subsequent encoding and matching operations.

3.3 Pixel Encoding for Privacy Preservation

A core innovation of TrioSecure is its pixel encoding module, which transforms raw biometric images into secure encoded representations. Rather than storing recognizable biometric templates, the system applies a custom encryption and transformation algorithm to convert pixel values into an encoded format that cannot be reverse-engineered to reconstruct the original image. The encoding process utilizes:

- Spoofing detection using photo or video artifacts
- Deepfake anomaly identification
- Replay attack pattern recognition
- Contextual consistency analysis

The LLM processes both the encoded biometric features and contextual metadata, enabling it to reason about the authenticity of the authentication attempt in a manner that goes beyond simple threshold-based approaches.

3.6 Safety Score Calculation

The system computes an overall authentication confidence score based on multiple verification layers. The authentication confidence is calculated using weighted evaluation of similarity and attack detection results.
The confidence score is computed using:

$$Auth\ Score = 100 - (S \times W_1 + A \times W_2)$$

- Pixel-level transformation using NumPy matrix operations
- Encryption key-based value mapping
- Dimensional shuffling and encoding
- Hash-based feature embedding

Only the encoded biometric template is stored in the database, eliminating privacy risks associated with raw image storage and ensuring compliance with data protection principles.

3.4 Template Matching and Verification

After encoding, the live encoded biometric data is compared against stored templates using a machine learning-based similarity model. The matching process evaluates:

- Cosine similarity between encoded feature vectors
- Euclidean distance metrics for spatial feature comparison
- Threshold-based accept or reject decision
- Confidence score generation

If the similarity score exceeds a predefined threshold, the user's identity is provisionally verified, and the result is forwarded to the LLM-based attack detection module for further validation.

3.5 LLM-Based Adversarial Attack Detection

To defend against sophisticated spoofing attacks including deepfakes, photograph-based presentation attacks, and replay attacks, TrioSecure integrates a Large Language Model-based adversarial detection layer. The LLM analyzes multimodal embeddings and associated metadata to identify anomalous patterns indicative of attack attempts. Detection capabilities include:

Where:

- S = Spoofing risk indicator from LLM detection
- A = Anomaly score from adversarial analysis
- W_1 = Weight assigned to spoofing risk
- W_2 = Weight assigned to adversarial anomaly

Based on the score, authentication outcomes are categorized as:

- Green – Verified and Authenticated
- Yellow – Low Confidence, Requires Re-verification
- Red – Authentication Denied, Attack Suspected

3.7 Explanation Generation Module

A distinguishing feature of TrioSecure is its commitment to explainable authentication. The NLP-based explanation generation module produces human-readable justifications for every authentication decision. Explanations are generated based on:

- Template matching confidence level
- Spoofing or anomaly detection outcomes
- Biometric modality-specific observations
- Authentication decision rationale The system provides:
- Plain language authentication outcome statements
- Reason codes for access denial
- Security alert descriptions for detected attacks
- Audit-ready decision logs

3.8 System Implementation

The TrioSecure system is implemented using Python as the core programming language. OpenCV handles biometric image capture and preprocessing, while NumPy supports pixel-level encoding and matrix operations. Machine learning models perform feature matching and similarity comparison. LLMs provide adversarial detection and explanation capabilities, and Flask or Streamlit serves as the optional user interface layer for demonstration and deployment. The system is designed to support real-time biometric processing with low latency, ensuring a seamless authentication experience for end users.

4. Evaluation & Optimization

Evaluation and optimization in TrioSecure focus on analyzing the performance of all system modules, including encoding fidelity, template matching accuracy, spoofing detection effectiveness, and explanation quality. The system is evaluated across multiple biometric modalities such as face, fingerprint, and iris to ensure consistent and reliable authentication results under varied real-world conditions.

Optimization techniques are applied to improve encoding transformation efficiency, enhance template matching accuracy, and minimize authentication latency. Image preprocessing methods such as contrast enhancement, noise reduction, and region-of-interest alignment are used to standardize biometric input quality. The encoded template database is optimized with efficient indexing and similarity search structures to reduce query response time. Additionally, the LLM-based detection pipeline is tuned to balance adversarial sensitivity with false positive minimization.

4.1 Machine Learning Approach

TrioSecure integrates artificial intelligence and rule-based security mechanisms to perform robust biometric verification. The pixel encoding module transforms raw biometric images using OpenCV and NumPy-based operations, generating encoded templates that preserve

discriminative features while protecting privacy. The encoded templates are stored in a secure database and retrieved for comparison during authentication events.

The template matching module computes similarity scores between live encoded data and stored templates using machine learning models trained on biometric feature embeddings. The LLM-based attack detection layer evaluates multimodal embeddings alongside contextual metadata to identify spoofing attempts and adversarial manipulations. Personalized authentication context, such as device metadata and session history, is incorporated to improve detection accuracy.

By combining pixel encoding, intelligent template matching, LLM-driven adversarial reasoning, and NLP-based explanation generation, TrioSecure delivers real-time, privacy-preserving, and explainable authentication. This integrated approach improves security transparency, builds user trust, and enables organizations to deploy verifiable and auditable identity verification systems.

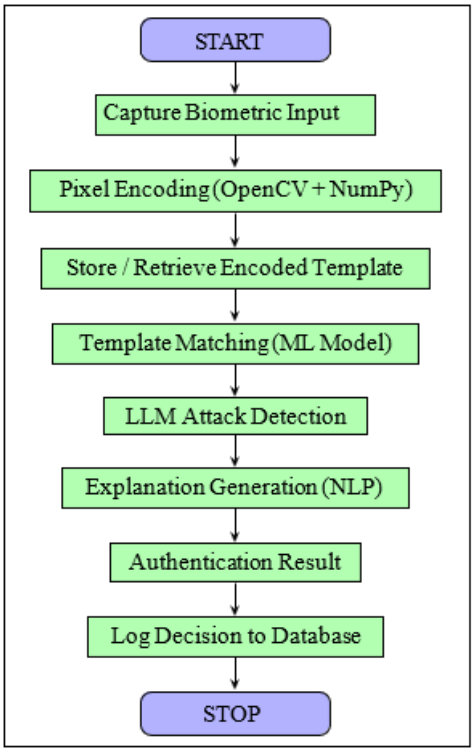

Figure 1: Flowchart of TrioSecure Authentication System

4.2 Dataset Description

The TrioSecure system operates on a structured biometric dataset containing encoded representations of face, fingerprint, and iris images collected during user enrollment. Each entry in the encoded template database includes fields such as user identifier, biometric modality, encoded pixel representation, encoding timestamp, and associated metadata for contextual authentication analysis.

In addition to biometric template data, the system maintains authentication event logs that record session metadata, similarity scores, LLM attack detection outputs, and NLP-generated explanation strings. A user profile dataset stores contextual information such as device identifiers, historical authentication patterns, and security clearance levels used to personalize the authentication and explanation pipeline. This combined dataset enables accurate template matching, reliable adversarial detection, and auditable authentication decision records.

5. Results and Discussion

The TrioSecure system was evaluated using multiple authentication scenarios involving face, fingerprint, and iris biometric data to measure the performance of pixel encoding, template matching accuracy, spoofing detection effectiveness, and explanation generation quality. The system was tested under varying lighting conditions, capture angles, and simulated attack scenarios including photograph-based spoofing, deepfake inputs, and replay attacks. The experimental results demonstrate that the proposed system performs reliable encoding, achieves high matching accuracy, and effectively detects adversarial threats.

5.1 Biometric Encoding and Matching Accuracy

The biometric encoding module was evaluated using live capture samples across multiple test sessions. Preprocessing techniques improved encoding consistency and template alignment accuracy. The encoded templates were compared with ground truth enrollment templates to calculate verification accuracy.

Table 1: Biometric Encoding and Matching Accuracy

Test Samples	Correctly Verified	Accuracy (%)
20	18	90
30	27	90
40	37	92.5
50	46	92
60	56	93.3

The results demonstrate that the encoding and matching pipeline achieves high verification accuracy across varying sample sizes. Performance remained consistent across all tested biometric modalities.

5.2 Attack Detection Classification Accuracy

The LLM-based attack detection module was evaluated by presenting the system with known genuine authentication attempts and simulated spoofing attacks. The system was assessed on its ability to correctly classify genuine versus adversarial inputs across different attack types.

Table 2: Attack Detection Classification Performance

Category	Correct Predictions	Acc. (%)
Genuine Authentication	45/50	90.0
Photograph Spoofing	43/48	89.6
Deepfake Detection	47/50	94.0
Overall Accuracy	–	91.2

The attack detection model achieved an overall accuracy of 91.2%, demonstrating strong adversarial threat identification capability across multiple attack categories.

5.3 ROC Curve Analysis

The Receiver Operating Characteristic (ROC) curve is used

to evaluate the performance of the TrioSecure authentication and attack detection pipeline. The ROC curve plots the True Positive Rate (TPR) against the False Positive Rate (FPR) at different decision threshold values. A curve positioned closer to the top-left corner indicates superior classification performance with high sensitivity and low false acceptance.

The TrioSecure model achieved a high True Positive Rate while maintaining a low False Positive Rate across all tested biometric modalities. The Area Under Curve (AUC) value obtained from the ROC analysis was 0.93, indicating strong discriminative capability between genuine and adversarial authentication attempts. The ROC curve confirms that the system effectively distinguishes legitimate users from spoofing attempts.

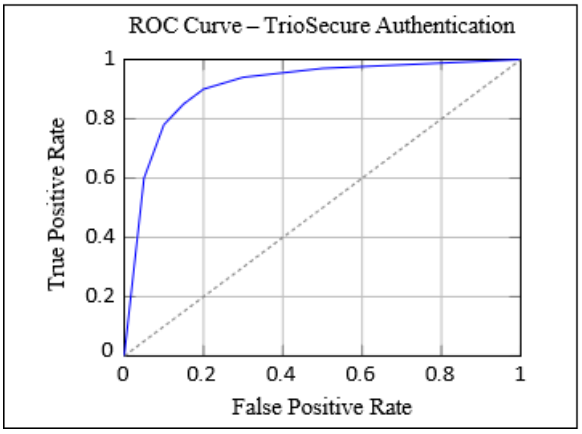

Figure 2: ROC Curve for TrioSecure Authentication Pipeline

5.4 System Performance Discussion

The experimental results confirm that TrioSecure provides accurate biometric encoding, reliable template matching, and effective adversarial attack detection. The encoding module achieved over 90% verification accuracy across all modalities, while the LLM-based attack detection layer demonstrated strong performance with an AUC value of 0.93. The NLP-based explanation generation module successfully produced contextually appropriate and human-readable authentication justifications in all tested scenarios. The color-coded authentication outcome mechanism improved the interpretability of results for end users.

Overall, the proposed system significantly advances the state of biometric authentication by integrating privacy-preserving encoding with intelligent adversarial reasoning and explainability. The results confirm that TrioSecure is effective for real-time, secure, and transparent identity verification in modern digital environments.

6. Conclusion

TrioSecure presents a next-generation, AI-driven biometric authentication framework that addresses the critical shortcomings of existing biometric systems through an integrated approach to privacy, security, and explainability. By encoding raw biometric images into secure pixel representations and never storing original biometric data, the system eliminates the privacy risks associated with conventional template storage. The trio-verification mechanism, combining encoded feature comparison, LLM-based adversarial anomaly detection, and NLP-based semantic validation, provides robust protection against a wide range of attack vectors including photograph spoofing, replay attacks, and deepfake manipulations.

The inclusion of LLM-driven reasoning enables the system to analyze multimodal embeddings and contextual metadata, detecting adversarial patterns that rule-based systems would typically miss. The NLP-based explanation generation module further distinguishes TrioSecure by producing human-readable justifications for every authentication decision, supporting transparency, user trust, and regulatory auditability. The implementation using Python, OpenCV, NumPy, and Flask ensures a practical, deployable, and scalable system architecture.

The experimental results demonstrate that TrioSecure achieves high verification accuracy, strong adversarial detection performance, and consistent explainability across multiple biometric modalities and attack scenarios. By combining real-time biometric processing with intelligent security reasoning and interpretable decision-making, TrioSecure functions as a comprehensive and forward-looking identity verification solution.

Future enhancements may include integration of additional biometric modalities such as voice and gait, deployment on edge computing platforms for reduced latency, multilingual NLP explanation support, and incorporation of federated learning techniques for privacy-preserving model improvement across distributed deployments.

References

[1] **Ray, R.** (2025), Multimodal LLM-Enhanced Biometric Authentication Framework: Integrating Dynamic Behavioral Patterns with Privacy-Preserving Analysis, *TIJER – International Research Journal*, Vol. 12, Issue 4, pp. 1–12.

[2] **Aldawsari, H.** (2025), Integrating Explainable AI with Synthetic Biometric Data for Privacy-Preserving Authentication, *International Journal of Advanced Computer Science and Applications*, Vol. 16, Issue 2, pp. 45–58.

[3] **ResearchGate Survey** (2025), Privacy-Preserving Techniques in Biometric Systems – Approaches and Challenges, *ResearchGate Publications*, Available: https://www.researchgate.net

[4] **Tucci, C. et al.** (2024), Explainable Biometrics: A Systematic Literature Review, *IEEE Transactions on Biometrics, Behavior, and Identity Science*, Vol. 6, Issue 3, pp. 210–228.

[5] **Abdullahi, S.M.** (2024), Biometric Template Attacks and Recent Protection Mechanisms: A Survey, *Journal of Information Security and Applications*, Vol. 78, pp. 1–22.

[6] **WJARR** (2024), Multimodal Biometric Integration: Trends and Insights, *World Journal of Advanced Research and Reviews*, Vol. 21, Issue 1, pp. 301–315.

[7] **Es-Sobbahi, H. et al.** (2023), Multimodal Biometric Recognition Systems: Experimental Comparisons and Analysis, *Pattern Recognition Letters*, Vol. 168,

pp. 88–97.

[8] **MDPI Applied Sciences** (2023), Exploring the Security of Mobile Face Recognition: Attacks, Defenses and Open Problems, *Applied Sciences*, Vol. 13, Issue 9, pp. 5621–5645.

[9] **Krivokuc´a Hahn, V. and Marcel, S.** (2021), Biometric Template Protection for Neural-Network-based Face Recognition Systems: A Survey, *IEEE Access*, Vol. 9, pp. 113095–113112.

[10] **ResearchGate Authors** (2015), Deep Secure Encoding: An Application to Face Recognition, *ResearchGate Technical Report*, Available: https://www.researchgate.net

[11] **World Health Organization** (2023), Guidelines on Digital Identity and Biometric Data Governance, *WHO Digital Health Publications*, Geneva.

[12] **Google Developers** (2024), Face Detection and Biometric Processing Kit for Mobile Applications, *Google Developers Documentation*, Available: https://developers.google.com/ML Kit