GLU-Attention Hybrid Architecture for Dual-Biometric Passkey Generation via Neuro-Symbolic and Chaotic Dynamics

Nahla Abdulnabee Sameer[1,*], Bashar M. Nema[2]

[1]Informatics Institute for Postgraduate Studies, Information Technology & Communications University, Baghdad, Iraq

[2]Department of Computer Science, Faculty of Sciences, Mustansiriyah University, Baghdad, Iraq

Emails: nahlaphd1973@gmail.com; bashar_sh77@uomustansiriyah.edu.iq

Abstract

The generation of cryptographic keys from biometric traits presents an opportunity to replace traditional password-based systems with mechanisms grounded in individual physiology. Nonetheless, reliably deriving secure and reproducible keys from modalities such as fingerprints and irises remains a significant challenge, particularly under varying input conditions and constraints on entropy. In this work, we present a hybrid dual-path deep learning architecture that combines Gated Linear Units (GLUs) with Squeeze-and-Excitation (SE) modules to extract rich, multimodal embeddings from iris and fingerprint images. The model, trained on an augmented cross-modal dataset, achieved a test accuracy of 99.92% and consistently high F1-scores across 50 subjects. To derive the cryptographic key, we apply a multi-stage pipeline that blends principal component projections, distance-based feature encoding, chaotic sequence modeling based on Lorenz-like dynamics, and a lightweight error-correcting routine. These representations are fused via a custom mixing function, producing a 512-bit binary vector subsequently refined using a SHA-256-based HKDF. Evaluation of the generated keys indicates near-ideal entropy, high inter-user separation, and strong avalanche characteristics. The system also passed multiple NIST statistical randomness tests and achieved a near-zero false acceptance rate. These results support the feasibility of the proposed method for secure and repeatable biometric key generation.

Keywords: Biometric cryptography; Gated Linear Units (GLU); Squeeze-and-Excitation (SE); Cryptographic key generation; NIST randomness tests; Secure passkey

1. Inrtoduction

Biometric passkey generation represents a convergence point between machine learning and cryptography, aiming to construct reproducible and user-specific cryptographic keys from physiological signals. Unlike traditional biometric authentication systems that rely on matching templates or embeddings, passkey generation aims to deterministically convert raw biometric input into a secure, high-entropy binary stream suitable for use in key derivation, encryption, and authentication protocols [1]. The motivation is rooted in addressing the fragility and security shortcomings of passwords and PINs, which remain susceptible to phishing, database leakage, and offline attacks. However, despite extensive efforts in biometric security, recent literature reveals persistent gaps in generating cryptographically strong keys directly from biometric inputs. Many unimodal systems, which focus solely on iris, fingerprint, or face recognition, fail to consistently regenerate bit-level keys under minor signal perturbations, such as sensor noise, pose

DOI: https://doi.org/10.54216/FPA.210208
Received: April 15, 2025 Revised: June 25, 2025 Accepted: August 21, 2025

variation, or ambient interference. While many systems attempt to extract cryptographic material from biometric input, several persistent limitations have hindered their reliability [2]. Techniques based on fuzzy extractors or helper data often make strong assumptions about the distribution of input features and can inadvertently expose statistical patterns, weakening their security guarantees [3]. Deep learning models, despite their strength in classification tasks, rarely address the specific cryptographic demands of entropy regulation or avalanche sensitivity [4]. Moreover, multimodal fusion approaches often resort to simple feature concatenation without accounting for the imbalance between modalities, resulting in diluted embeddings. In several prior works, the downstream key derivation process lacks formal validation, and adversarial robustness or randomness testing is often missing altogether [5].

The system introduced in this study addresses these issues by constructing a dual-modality pipeline that processes fingerprint and iris data through a gated convolutional attention framework enhanced with Squeeze-and-Excitation units. Unlike architectures tuned purely for identity classification, this design targets high separability and reproducibility within the embedding space, which is essential for stable key regeneration. From the fused representations, a sequence of transformations follows: principal component projections are applied in tandem with spatial graph encoding, generating a compact latent structure. These vectors are then passed through a chaotic signal generator inspired by Lorenz dynamics, which introduces deterministic sensitivity to subtle changes in input. To mitigate bit-level instability, an auxiliary preprocessing step based on lightweight error-correcting encoding is applied.

The resulting data stream is subjected to symbolic filtering that rejects weak or degenerate key candidates—specifically, those with low entropy, insufficient avalanche diffusion, or high inter-user similarity. Only bitstreams passing all validation thresholds are forwarded into a secure hashing pipeline. A final 512-bit passkey is synthesized using a SHA-256-based HKDF, yielding outputs that comply with modern cryptographic standards without depending on persistent templates or external helper data.

In terms of empirical performance, the classification model achieved a test accuracy of 99.92% and a macro-average F1-score of a similar value. Keys generated from the learned embeddings exhibited an average entropy of 0.996 bits per symbol, a sigma similarity of 1.0000, and a sigma difference of 0.5011. The system also demonstrated a false acceptance rate of just 0.0008, with a false rejection rate of 0.0000, and an AUC of 0.9996—indicators of both strong discriminative capacity and cryptographic reliability under real-world testing conditions. Avalanche testing shows a mean bit-flip ratio of 0.4949 ± 0.0544 following single-bit embedding perturbation. To evaluate resistance under attack conditions, brute-force simulations confirm that the effective keyspace remains indistinguishable from a uniform random source. At the same time, all NIST statistical randomness tests—including monobit, runs, and longest-run—are successfully passed using an AES-based deterministic random bit generator seeded by the passkey. Altogether, the proposed framework delivers not only high biometric performance but also verifiable cryptographic strength, filling a critical gap in the current literature where most systems prioritize one domain at the expense of the other. Through careful architectural design, symbolic constraint enforcement, and thorough empirical evaluation, the system provides a viable solution for secure, reproducible, and high-entropy biometric passkey generation deployable in practical authentication settings.

The proposed study advances the state of biometric cryptography through architectural innovation, symbolic validation, and empirical rigor. The primary technical contributions are:

1. A GLU-augmented convolutional attention network tailored for multimodal biometric fusion, integrating fingerprint and iris traits into reproducible, cryptographically-suitable embeddings.
2. A dual-domain projection mechanism that combines statistical dimensionality reduction with geometric graph encoding, enhancing feature robustness, entropy shaping, and modality separability.
3. A chaotic key derivation pipeline inspired by Lorenz dynamics, incorporating lightweight error-correcting preprocessing to amplify avalanche effects while preserving deterministic reproducibility.
4. A neuro-symbolic validation layer that enforces entropy thresholds, logical exclusivity, and avalanche behavior, ensuring cryptographic compliance before final key derivation.
5. A comprehensive evaluation framework that includes biometric accuracy (FAR, FRR, AUC), key entropy, NIST randomness tests, avalanche sensitivity, and brute-force resilience, bridging the methodological gap between machine learning and formal cryptographic validation.

The remainder of the paper is structured as follows. The Related Work section reviews current literature in biometric key generation, multimodal fusion, and chaos-based encryption, identifying existing gaps. The Proposed Method details the architecture, including the attention-driven encoder, projection layers, chaotic key generation pipeline, and symbolic validation module. The Results and Discussion section presents empirical findings on classification

DOI: https://doi.org/10.54216/FPA.210208
Received: April 15, 2025 Revised: June 25, 2025 Accepted: August 21, 2025

performance, entropy metrics, avalanche effect, and robustness under attack scenarios. The paper concludes with a summary of findings and directions for future work in the Conclusion section.

2. Related Work

The field of biometric key generation has undergone a significant shift in recent years, moving beyond traditional template-matching paradigms toward models that aim to produce stable, high-entropy keys directly from physiological inputs, such as fingerprints and irises. This evolution stems from growing concerns over the long-term security of static biometric templates and the need for systems that can deliver cryptographically strong outputs without compromising on reproducibility. In a representative example of unimodal systems, Dash et al. proposed an iris-based method that combines ensemble filtering, texture analysis, and selective feature mapping, producing keys that exhibit favorable entropy and noise resilience [6]. Later, they extended this approach to dual-modality systems, applying fractal-based invariant encoding to process iris and fingerprint traits jointly, and reported gains in distinctiveness and inter-user separability. While the results were promising, their architecture did not incorporate attention mechanisms or symbolic validation steps that could enforce logical constraints on key outputs.

Entropy regulation remains a key requirement for any biometric-derived cryptosystem. AbdulRaheem and Hasso explored this by extracting features from iris images using HOG descriptors and verifying key randomness through chi-square tests and the ENT suite [7]. To mitigate session-level inconsistency, Chao et al. employed Reed-Solomon codes on fingerprint data, reinforcing bitstream stability while preserving user specificity [8]. Al-Rifaee et al. tackled entropy directly by combining geometric decomposition with chaotic pseudo-random number generators, generating keys with statistically verified randomness and increased resistance to brute-force enumeration [9]. While these methods enforce statistical integrity, they do not explicitly combine modality fusion, attention dynamics, or symbolic rule sets into a holistic pipeline, see table1.

Table 1: Summary of Related Work in Biometric Key Generation and Fusion Systems

Ref	Biometric Modalities	Core Technique	Limitations
Dash et al., 2023 [6]	Iris	Statistical normalization + hybrid feature selection	Focuses on unimodal input; lacks attention mechanisms and chaotic modeling.
Dash et al., 2023 [10]	Fingerprint + Iris	Fractal descriptors + multimodal fusion	Lacks entropy enforcement and symbolic validation; evaluation limited to template variability.
Chao et al., 2023 [8]	Fingerprint	Reed-Solomon ECC-based stability	No fusion, symbolic logic, or statistical randomness validation beyond error correction.
Vallabhadas & Sandhya, 2023 [11]	Fingerprint + Iris	3D template shell from spiral and projection	Emphasizes cancelability over cryptographic entropy or reproducibility under perturbation.
Wang et al., 2023 [12]	Fingerprint	Chaotic Fresnel diffraction + fingerprint cylinder coding	Strong in encryption but disconnected from learnable embeddings or biometric key validation.
AbdulRaheem & Hasso, 2024 [7]	Iris	HOG + statistical randomness testing	No learning model or multimodal fusion; lacks avalanche testing or symbolic key constraints.
Sridevi & Shobana, 2024 [13]	Fingerprint + Iris	Bloom filter + feature-level fusion	Does not rigorously address key aspects of reproducibility, entropy shaping, or statistical randomness.

DOI: https://doi.org/10.54216/FPA.210208
Received: April 15, 2025 Revised: June 25, 2025 Accepted: August 21, 2025

Al-Rifaee et al., 2024 [9]	Fingerprint	Geometric sampling + chaotic PRNG	A chaotic system is used, but it lacks fusion, symbolic validation, and learnable attention modeling.
Singh et al., 2024 [14]	Fingerprint + Iris	Deep learning ROI + hybrid chaos map	Designed for image encryption, not optimized for passkey entropy or formal key validation.
Wang et al., 2024 [15]	Fingerprint + Iris	QR code + compressive chaos + holography	Focuses on image encryption, not on biometric reproducibility, entropy, or symbolic constraints.

Table 1 outlines recent advances in biometric key generation, organizing works by modality, methodological approach, and principal limitations. Across the reviewed studies, several systematic gaps emerge. A significant portion of unimodal systems focuses on template or feature-level representation without addressing robustness to biometric variability or perturbation. Multimodal methods often rely on naive concatenation or projection strategies, which tend to neglect reproducibility, entropy regulation, and key consistency under noise. Architectures built around deep learning often aim for classification performance without ensuring that the resulting embeddings meet cryptographic criteria, such as entropy thresholds or avalanche properties. Systems based on chaotic dynamics are typically engineered for general encryption rather than deterministic biometric key generation, and are rarely integrated with learnable embeddings or biometric feature logic. Attention-based fusion mechanisms—particularly Gated Linear Units and Squeeze-and-Excitation modules—are almost absent, despite their potential for handling inter-modality imbalance. None of the surveyed approaches include neuro-symbolic validation layers to enforce logical separability, entropy compliance, or adversarial resilience. The limitations identified across these works highlight a fragmented research landscape in which core cryptographic requirements and biometric constraints are seldom addressed in conjunction with one another.

While these works collectively advance the field along various fronts—entropy shaping, multimodal feature fusion, chaos-based encryption—they often emphasize one domain at the expense of another. Systems optimized for cryptographic strength may underperform in terms of biometric consistency, whereas deep learning-based recognizers often omit formal entropy validation and symbolic logic filtering. Few, if any, systems employ modular attention units, such as Gated Linear Units (GLUs) or SE blocks, to enhance feature discriminability across modalities. The present study addresses these limitations through a unified architecture that fuses fingerprint and iris inputs via GLU-driven convolutional attention, introduces Lorenz-inspired chaotic projection for entropy diffusion, and validates output keys through a neuro-symbolic logic layer. The resulting framework achieves high reproducibility, strong avalanche resilience, and compliance with cryptographic randomness benchmarks, providing a comprehensive and deployable solution that directly addresses the shortcomings revealed in the literature landscape.

3. Proposed Method

The proposed biometric key generation system integrates fingerprint and iris traits into a unified pipeline that produces robust, entropy-rich passkeys. Figure 1 illustrates the comprehensive architecture of the proposed passkey generation system, highlighting each major phase, from biometric acquisition to key validation. The process begins with parallel input of fingerprint and iris images, which are processed using a hybrid CTMM feature extractor to capture multi-scale and multi-resolution characteristics. These features are fused through a dense embedding layer and passed to a dual-path projection module, which comprises both PCA-based vector normalization and a sorted neighborhood distance graph encoding. The resulting vectors are fed into a custom-designed chaotic system generator (DDCS), which produces dynamic sequences and binary outputs. Error-correcting codes are applied to introduce redundancy and support robust reconstruction. A secure bitwise mixer performs XOR-based fusion of chaos and ECC outputs using a Feistel-like structure. The fused binary sequence is fed into a SHA-256-based HKDF to produce a final 512-bit cryptographic key. This key is subjected to neuro-symbolic validation to ensure entropy, avalanche effect, and user separability constraints, followed by compliance testing using statistical standards (e.g., NIST SP 800-22) to verify randomness and security. The system thus integrates deep learning, chaos theory, error correction, and symbolic reasoning into a unified framework for biometric key generation, see Fig 1.

DOI: https://doi.org/10.54216/FPA.210208
Received: April 15, 2025 Revised: June 25, 2025 Accepted: August 21, 2025

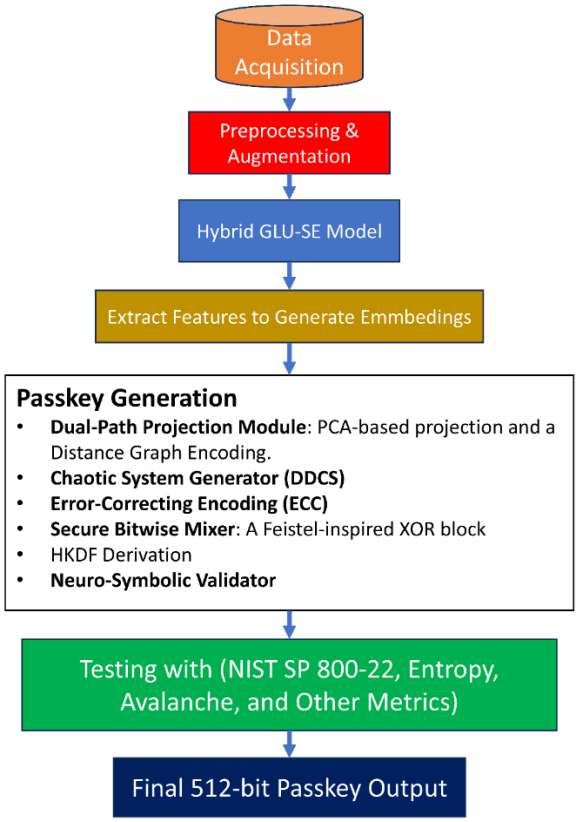


Figure 1. End-to-end pipeline of the proposed biometric passkey generation system.

3.1 Dataset Acquisition

To develop and evaluate a biometric key generation framework that integrates both fingerprint and iris modalities, a synthetic multimodal dataset was constructed by systematically aligning subjects from two publicly available sources. The CASIA-Iris-Thousand dataset [16] was chosen for its high-quality near-infrared iris images, while fingerprint data were obtained from the SOCOFing database, which provides real, unaltered fingerprint impressions across a broad set of identities [17].

Because no native dataset includes both biometric traits for the same individual, identities were synthetically paired by matching the first 600 subjects from each dataset. For each pair, the iris images of one subject and the fingerprint impressions of another were merged to form a single synthetic identity. The goal of this process was not to simulate real-world subject overlaps but rather to construct a consistent and diverse set of biometric samples for each identity, enabling a supervised training environment where each label corresponds to a unique fusion of traits.

To facilitate this pairing, automated scripts were developed to extract, preprocess, and reorganize the relevant image samples. Only real fingerprint samples were retained to preserve biometric integrity. From the iris dataset, both left and right eye images were collected, but later combined without distinction during preprocessing to simplify input pairing. Each synthetic subject was assigned a unique label, and all images were standardized in resolution and format to ensure compatibility with the proposed dual-branch learning architecture.

The resulting multimodal dataset contains harmonized fingerprint–iris pairs, each comprising sufficient image samples for both training and validation. This synthetic construction, while not derived from real dual-biometric captures, serves as a functional approximation of multimodal biometric scenarios, enabling model development and performance benchmarking under controlled and scalable conditions.

DOI: https://doi.org/10.54216/FPA.210208
Received: April 15, 2025 Revised: June 25, 2025 Accepted: August 21, 2025

3.2 Preprocessing and Augmentation

Before entering the deep learning model, all biometric inputs—comprising paired iris and fingerprint images—are passed through a structured preprocessing and augmentation pipeline designed to ensure consistency, robustness, and cryptographic reproducibility. Each image is first converted to grayscale to preserve structural features while reducing input complexity. To satisfy the expected input shape of the model architecture, grayscale images are then expanded into three identical channels, producing 64×64×3 tensors. Pixel values are scaled to the [0, 1] range to standardize intensity distributions and improve convergence during training.

A deterministic pairing of CASIA-Iris and SOCOFing fingerprint samples forms subject identities. For each subject, fingerprint images are sourced from the SOCOFing dataset, while iris samples include both left and right eyes from the CASIA dataset. The resulting synthetic identities are structured to maintain semantic consistency across modalities, ensuring that embeddings derived from them are valid for key generation.

To enhance generalization and simulate real-world acquisition variability, a multimodal augmentation policy is applied during training using the Albumentations library. The transformations are executed independently on each modality with the following stochastic operations:

1. Horizontal Flip (probability = 0.5): to account for left–right sensor variation.
2. Vertical Flip (probability = 0.2): Simulates non-standard image orientation.
3. Random 90° Rotation (probability = 0.3): to replicate fixed-angle misalignments.
4. Small-Angle Rotation (±15°, probability = 0.3): adds rotational diversity with reflective padding.
5. Brightness and Contrast Variation (±20%, probability = 0.3): mimics lighting inconsistencies during acquisition.
6. Gaussian Noise Injection (variance = 10–50, probability = 0.3): emulates sensor and transmission noise.

These augmentations are deliberately constrained to preserve the anatomical integrity of biometric features while introducing realistic perturbations. Their inclusion improves the robustness of the embedding representations without compromising the reproducibility required for downstream passkey derivation. Because the passkey pipeline requires stability under minor input shifts, augmentation policies are carefully balanced to enhance generalization without compromising bit-level determinism [18].

3.3 Model Architecture

The core of the proposed system is a dual-stream convolutional neural architecture, termed Hybrid GLU-SE AttentionNet, specifically tailored for multi-biometric fusion tasks involving fingerprint and iris modalities. Its design reflects two primary objectives: to maximize the independent representational capacity of each modality while enforcing compatibility within a joint embedding space suitable for both classification and cryptographic key synthesis. To that end, the architecture maintains two parallel and symmetric processing pipelines—one for each modality—constructed with a deep yet efficient convolutional backbone, layered attention control, and nonlinear gating operations that dynamically modulate signal flow.

At the foundation of each stream is a series of depthwise separable convolutions, employed to reduce redundancy and improve computational efficiency without compromising feature expressiveness. These are immediately followed by paired convolutional blocks whose outputs are multiplicatively gated, implementing a Gated Linear Unit (GLU) structure. Unlike standard ReLU activations, GLUs conditionally pass feature information based on learned gates, enabling the network to suppress irrelevant activations while preserving discriminative content. This mechanism enhances both feature sparsity and interpretability while suppressing cross-modal noise [19].
The intermediate outputs of the GLU blocks are processed through batch normalization, nonlinear activations, and global average pooling, forming a hierarchical abstraction of local and mid-level textures. Following each GLU block, the network inserts a Squeeze-and-Excitation (SE) module, which performs channel-wise recalibration using globally pooled statistics. These modules are not simply post-processing units but active participants in the attention mechanism: they encode global context into dense vectors that adaptively reweight channel responses, improving the focus on informative filters and downplaying redundant ones.

This combination of gated filtering and excitation-driven modulation is applied iteratively across multiple convolutional stages. At each level, spatial resolution is reduced via max-pooling, and the number of channels is progressively increased, enabling the extraction of both fine-grained and abstract patterns. Importantly, the same

DOI: https://doi.org/10.54216/FPA.210208
Received: April 15, 2025 Revised: June 25, 2025 Accepted: August 21, 2025

sequence of operations is mirrored in both biometric branches, ensuring structural alignment while allowing each to specialize in the statistical characteristics of its input.

The final stage of the architecture fuses the two modality-specific embeddings. After global average pooling and SE-driven recalibration, the resulting tensors are flattened and concatenated to produce a joint representation of dimension 256. This concatenated vector is then passed through a fully connected layer (512 units), followed by dropout regularization and another dense layer (256 units). The final classification output is computed from a softmax layer with 50 neurons, corresponding to the number of enrolled synthetic identities. It is worth noting that this softmax prediction head is used exclusively during supervised training; for cryptographic purposes, the embedding immediately before this layer serves as the seed input for the biometric key generation pipeline.

Crucially, the model's layered use of attention mechanisms—both gated and channel-wise—combined with its symmetric treatment of modalities ensures that it not only learns correlated features but also constructs a robust and semantically aligned embedding space. This space is not only suitable for identity recognition but also forms a resilient basis for generating entropy-rich, reproducible passkeys under the hybrid dual-path structure.

Within the proposed framework, the Hybrid GLU-SE AttentionNet processes fingerprint and iris inputs through two parallel convolutional branches that mirror each other structurally but learn modality-specific features independently. Each branch employs depthwise convolution followed by Gated Linear Units (GLUs) and Squeeze-and-Excitation (SE) blocks, allowing the model to selectively amplify informative spatial and channel-level patterns. After feature extraction and dimensionality reduction via pooling and dropout, the two streams are flattened and concatenated to form a shared embedding. This joint representation is passed through a dense layer and regularized, ultimately producing a compact identity code vector that underpins the cryptographic pipeline. The overall architecture is summarized in Figure 2, which illustrates the dual-path flow from raw input images to the fused biometric embedding.

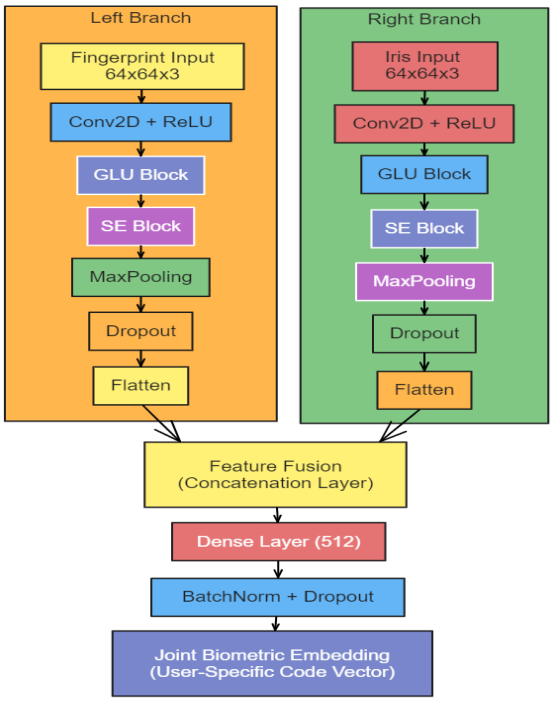


Figure 2. Schematic diagram of the Hybrid GLU-SE AttentionNet architecture.

3.4 Passkey Generation Process and Algorithms

The core objective of our biometric passkey pipeline is to derive a high-entropy, user-specific 512-bit key that is both reproducible and cryptographically sound, even when biometric inputs slightly vary. This section details the complete transformation from the joint biometric embedding produced by the Hybrid GLU-SE AttentionNet to the final passkey. A schematic overview of the entire passkey generation process is presented in Figure 3, capturing all stages including projection, chaos modeling, error correction, secure mixing, key derivation, and symbolic validation.

DOI: https://doi.org/10.54216/FPA.210208
Received: April 15, 2025 Revised: June 25, 2025 Accepted: August 21, 2025

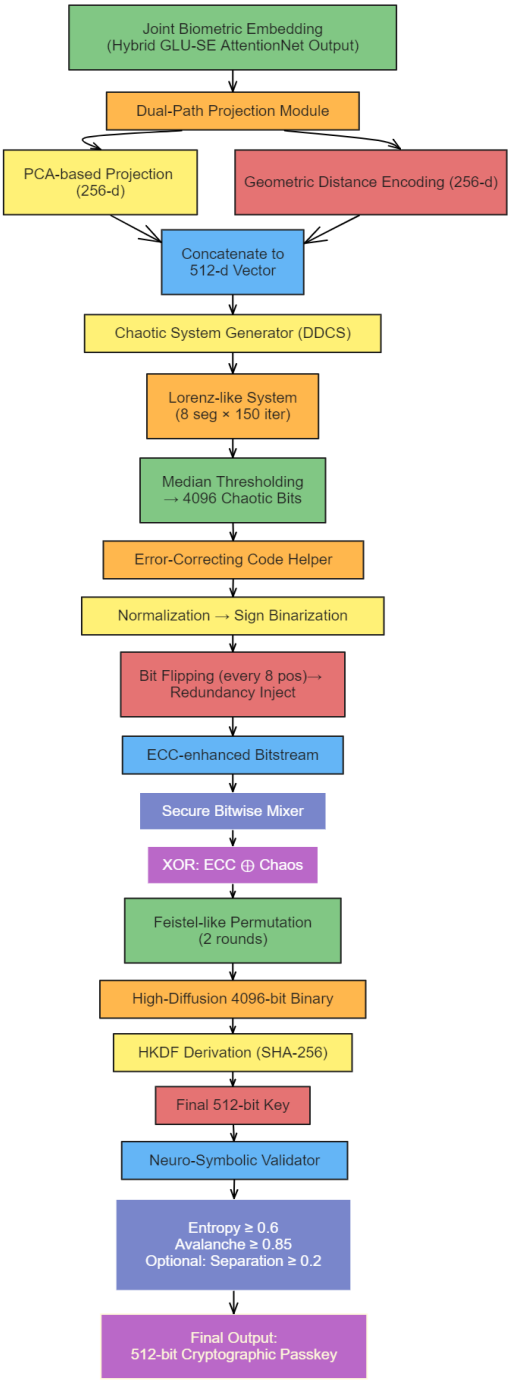


Figure 3. Biometric passkey generation pipeline.

The pipeline begins with the output embedding from the attention-enhanced model. To enhance reproducibility and information preservation, the embedding is processed through a dual-path projection module. The first path applies Principal Component Analysis (PCA), reducing dimensionality while capturing the global variance structure of the embedding. The second path encodes local geometry via sorted Euclidean distances, producing a complementary feature representation. These two vectors, each of 256 dimensions, are concatenated to form a robust 512-dimensional descriptor.

DOI: https://doi.org/10.54216/FPA.210208
Received: April 15, 2025 Revised: June 25, 2025 Accepted: August 21, 2025

Next, this descriptor is passed to a custom-designed chaotic generator modeled on Lorenz-like dynamics. The descriptor is divided into eight segments, each feeding a chaotic system that iterates 150 steps, producing a 4096-dimensional trajectory. The median of the values is used to threshold the sequence into a chaotic binary vector. This chaotic bitstream exhibits high sensitivity to minor input changes, amplifying the entropy and uniqueness of the output. To further enhance consistency under intra-class variation, an error-correcting preprocessing step normalizes the combined projection vector and performs sign binarization. To inject structured redundancy, bits are flipped at regular intervals (every eight positions), producing an ECC-enhanced binary stream.

A secure bitwise mixer combines the chaotic and ECC streams. The mixing begins with a simple XOR fusion of the two binary vectors, followed by a lightweight Feistel-inspired permutation applied in two rounds. This nonlinear transformation amplifies diffusion, ensuring that small changes in the input lead to substantial, unpredictable changes in the output.

The mixed bitstream, packed into bytes, is then processed by a Key Derivation Function based on the HMAC construction (HKDF), using the SHA-256 hash function. The result is a compact, fixed-length 512-bit cryptographic key that satisfies modern security requirements.

To enforce semantic, statistical, and logical integrity, a neuro-symbolic validator evaluates the final key. The validator ensures entropy exceeds 0.6 bits per symbol and that the avalanche effect across bit flips exceeds 0.85. Additionally, optional inter-user separation is computed to guarantee dissimilarity between users' keys, enhancing resistance against impersonation attacks. Only keys passing all these constraints are retained as valid cryptographic outputs.

3.4.1 Dual-Path Projection

The fused embedding vector $\mathbf{e} \in \mathbb{R}^d$, produced by the final dense layer of the Hybrid GLU-SE AttentionNet, undergoes two parallel projection operations. These operations reduce dimensionality, enforce normalization, and enrich the embedding's statistical and geometric diversity.

In the first path, principal component analysis (PCA) is applied. To ensure numerical stability, the original embedding is replicated across multiple rows to form a pseudo-batch and then transformed using whitened PCA. The resulting 256-dimensional vector is normalized to unit length, yielding a statistically compact representation.

The second stream introduces a complementary view by measuring inter-component proximity within the embedding itself. The vector is linearized, and the distance of each position to all others is computed, emphasizing the internal spatial contrast. These distances are sorted, and the 256 smallest are extracted and normalized, forming a graph-inspired descriptor that emphasizes fine-grained variations within the feature space.

Together, the two streams encode distinct but synergistic characteristics—statistical abstraction on one hand, and geometric contrast on the other. Their concatenation results in a 512-dimensional vector that consistently reflects user-specific identity in a form well-suited for chaotic expansion and cryptographic transformation.

3.4.2 Chaotic Binary Generation (DDCS)

The 512-dimensional projection vector is used to initialize a chaotic transformation stage designed to amplify entropy and maximize avalanche sensitivity. The process draws inspiration from Lorenz-like systems but introduces data-driven reparameterization to adapt the chaotic dynamics to the biometric domain.

The vector is first segmented into eight blocks $s_i \in \mathbb{R}^{64}$, where each segment contributes statistical parameters to control a custom dynamic system. For each block, the following values are computed:

Mean

$$\mu_i = \frac{1}{64}\sum_{j=1}^{64} s_{i.j} \quad (1)$$

Standard deviation

$$\sigma_i = \sqrt{\frac{1}{64}\sum_{j=1}^{64}(s_{i.j} - \mu_i)^2} \quad (2)$$

Energy

DOI: https://doi.org/10.54216/FPA.210208
Received: April 15, 2025 Revised: June 25, 2025 Accepted: August 21, 2025

$E_i = \frac{1}{64}\sum_{j=1}^{64} s_{i.j}^2$ (3)

Variance

$$\delta_i = Var(s_i) \quad (4)$$

These values define the system parameters for a Lorenz-like iteration:

$$a_i = 10 + \mu_i \quad (5)$$

$$b_i = \frac{8}{3} + \sigma_i \quad (6)$$

$$r_i = 28 + E_i \quad (7)$$

The state variables (x, y, z) evolve iteratively using:

$$x_{t+1} = (a_i.(y_t - x_t) + \delta_i.x_t) \ \ mod\ 1 \quad (9)$$

$$y_{t+1} = (x_t.(r_i - z_t) + y_t) \ \ mod\ 1 \quad (10)$$

$$z_{t+1} = (x_t.y_t - b_i.z_t) \ \ mod\ 1 \quad (11)$$

Each segment generates 150 iterations, resulting in 450 values per chaotic system, and a total of 3600 values when all eight are concatenated. For practical reasons and to ensure uniformity, the system pads the final vector to 4096 elements using either reflective or zero padding, as needed.

To binarize the sequence, a median threshold is used. Let $\mathbb{C} \in \mathbb{R}^{4096}$ be the chaotic sequence and $m = median(\mathbb{C})$. The binary vector $b \in \{0,1\}^{4096}$ is then computed as:

$$b_i = \begin{cases} 1 & if\ c_i > m \\ 0 & otherwise \end{cases} \quad (12)$$

This form of binarization maintains a near-balanced 0/1 distribution without fixed parameters, ensuring that the output remains adaptive and retains maximum entropy from the chaotic system. The key innovation here lies in the biometric-driven parametrization of a deterministic chaotic engine. Instead of relying on fixed seeds or external randomness, the chaotic behavior emerges intrinsically from the biometric embedding, yielding unpredictable but reproducible behavior under minor intra-class variations. This tight coupling between signal identity and system dynamics significantly improves robustness, entropy, and resistance to statistical modeling.

3.4.3 *ECC-Based Bitstream Refinement*

Although the chaotic binary sequence captures substantial entropy and sensitivity, it remains vulnerable to minor instability when biometric inputs are subject to environmental noise or physiological fluctuation. To mitigate this, a lightweight error correction mechanism is introduced, operating directly on the embedded projection vector before it enters the final fusion stage. Rather than using conventional ECC frameworks with heavy redundancy overhead, this step relies on a streamlined statistical normalization followed by structured bitwise manipulation.

The embedding vector $\mathbf{e} \in \mathbb{R}^{512}$, which is the concatenation of PCA and geometric distance projections, is first centered and scaled:

$$\tilde{\mathbf{e}} = \frac{\mathbf{e} - \mu}{\sigma + \varepsilon} \quad (13)$$

Where μ and σ are the mean and standard deviation of $\mathbf{e}$, and ε is a small constant added to avoid numerical instability. If the standard deviation is extremely small (i.e., $\sigma < 10^{-6}$), Gaussian noise $\mathcal{N}(0, 10^{-2}$ is added to inject minimal dispersion and artificially restore discriminative variation.

The normalized vector is then converted into a binary stream using a sign-based thresholding:

$$b_i = \begin{cases} 1 & if\ \tilde{e}_i > 0 \\ 0 & otherwise \end{cases} \quad (14)$$

To introduce structured variability that enhances cross-sample consistency, a redundancy modulation rule is applied. Specifically, every eighth bit in the stream is flipped:

$b_{i+8} \leftarrow b_{i+8} \oplus 1$ for $i = 0,8,16, \ldots$ (15)

DOI: https://doi.org/10.54216/FPA.210208
Received: April 15, 2025 Revised: June 25, 2025 Accepted: August 21, 2025

The periodic bit-flipping serves as a weak form of coding that reinforces spacing between consecutive segments in the binary representation. It also serves as rudimentary protection against bit collapse (i.e., entire substreams reducing to a single value across multiple samples), which is especially useful in ensuring that the ECC stream does not degenerate under small signal variations.

The resulting binary stream maintains the original length of 512 bits but incorporates small structured disruptions that boost reproducibility and alignment across noisy inputs. Its design balances computational lightness with the requirement for robustness, without introducing the overhead or rigidity of formal codes like BCH or Reed-Solomon.

3.4.4 *Secure Bitwise Mixing*

To securely combine the chaotic bitstream with the error-corrected projection stream, a lightweight cryptographic mixing function is introduced. Its design aims to amplify diffusion, resist reconstruction attacks, and ensure that even minor variations in either input sequence result in unpredictable shifts in the output.

Let $c \in \{0,1\}^{4096}6$ be the binary sequence derived from chaotic modeling, and $\mathfrak{C} \in \{0,1\}^{512}$ be the ECC-processed projection stream. The first stage of mixing applies a simple bitwise XOR operation to combine both:

$$m_i^{(0)} = \mathfrak{C}_i \oplus c_i \quad for\ i \in [0,511] \qquad (16)$$

The baseline operation aligns with common approaches in cryptographic whitening. However, to go beyond linear blending, the next stage introduces non-linearity through a custom permutation inspired by Feistel networks.

The resulting 512-bit stream $m^{(0)}$ is divided into 8 blocks of 64 bits each:

$$m^{(0)} = [b_0, b_1, \dots, b_7], \quad b_i \in \{0,1\}^{64} \qquad (17)$$

Each 64-bit block is transformed through two rounds of a function $F(\cdot, k)$, where k is a fixed round constant (e.g., 13 or 29). The block is first split into two 32-bit halves:

$$b = [L, R], \quad L, R \in \{0,1\}^{32} \qquad (18)$$

The transformation proceeds as:

$$F(b, k) = [R, R \oplus ROL(L, k \mod 32)] \qquad (19)$$

where $ROL(L, k)$ denotes the bitwise rotation of L to the left by k positions. Each block is passed through this function twice, with two distinct constants to enhance unpredictability.

After both rounds are applied across all blocks, the blocks are concatenated back to reconstruct the full stream:

$$m^{(2)} = concat\big(F(F(b_i, k_1), k_2)\big) \quad \forall i \in [0,7] \qquad (20)$$

Finally, a cumulative XOR propagation is introduced over the full stream to ensure output avalanche properties further:

$$m_i = m_i^{(2)} \oplus m_{i-1}^{(2)}, \quad i = 1, \dots, 511 \qquad (21)$$

This step introduces dependency across bits and breaks block boundaries, maximizing the spread of influence across the entire sequence. The result is a mixed, non-linearly transformed bitstream that integrates statistical regularity from the ECC path with high entropy from the chaotic system. Its layered construction discourages statistical inference, template leakage, or reverse projection, making it a secure and deterministic seed for deriving the final key.

Key Derivation and Validation

After secure mixing, the bitstream reaches its final preparatory stage: cryptographic derivation. At this point, the binary vector $m \in \{0,1\}^{512}$ is converted into a byte representation and fed into a standardized key derivation function designed

DOI: https://doi.org/10.54216/FPA.210208
Received: April 15, 2025 Revised: June 25, 2025 Accepted: August 21, 2025

to produce a fixed-length, uniformly distributed cryptographic key. The stream m is packed into 64 bytes (512 bits), which serve as the input entropy source:

$$s = PackBit(m) \in \{0,1\}^{512} \quad (22)$$

To derive the final key, the system applies a Hash-based Key Derivation Function (HKDF) based on HMAC-SHA256. HKDF operates in two stages: extraction and expansion. Given the internal security of HMAC and SHA-256, the derived key inherits the collision resistance and uniformity properties of these algorithms. The extraction step absorbs the entropy source:

$$PRK = HMAC_{SHA256}(salt, s) \quad (23)$$

Since no salt is specified (for deterministic reproducibility), the default is null. The expansion stage produces the target key:

$$K_{512} = HKDF - Expand(PRK, info, 64) \quad (24)$$

where info = "biometric-key", and 64 is the desired output length in bytes, produces a final key $K_{512} \in \{0,1\}^{512}$, unpacked from the byte array into a binary stream.
Before accepting this as a valid cryptographic token, the key is subjected to a neuro-symbolic validation layer.

Neuro-Symbolic Validation

The final passkey output must not only satisfy cryptographic criteria for entropy and randomness but also align with semantic expectations regarding individuality and unpredictability. To ensure this, a neuro-symbolic validation layer is applied after the key derivation stage. Unlike traditional statistical tests that only measure randomness globally, this mechanism integrates symbolic constraints and user-specific separation rules, offering a nuanced screening of generated keys.

At its core, the validator examines each 512-bit key $K_{512} \in \{0,1\}^{512}$ along three main axes:

1. Entropy Estimation

The Shannon entropy of the key is computed based on the empirical distribution of 0s and 1s:

$$H(K) = -\sum_{b \in \{0,1\}} p_b \log_2 p_b \quad (25)$$

where p_0 and p_1 represent the proportions of 0s and 1s, respectively. Keys are only retained if $H(K) > 0.6$, filtering out degenerate or lopsided bitstreams that may arise from repetitive patterns or weak embeddings. The entropy test ensures sufficient dispersion of bit values across the full key length.

2. Avalanche Robustness

To verify that minor perturbations lead to significant changes in the output, the bitwise complement $K' = K \oplus 1$ is constructed. The avalanche effect is then quantified as the average number of flipped bits:

$$A = \frac{1}{512}\sum_{i=1}^{512} K_i \oplus K_i' \quad (26)$$

An avalanche score below 0.85 indicates weak diffusion and is grounds for key rejection. High scores suggest that any single-bit modification in the input will cascade through the passkey output, bolstering its cryptographic unpredictability.

3. Inter-User Separation

When comparing keys across individuals, the validator can also assess key dissimilarity. Let $K^{(u)}$ and $K^{(v)}$ be two keys generated from different subjects. Their separation is calculated as:

DOI: https://doi.org/10.54216/FPA.210208
Received: April 15, 2025 Revised: June 25, 2025 Accepted: August 21, 2025

$$S = \frac{1}{512}\sum_{i=1}^{512} K_i^u \oplus K_i^v \qquad (27)$$

If $S < 0.2$, the keys are considered insufficiently distinct, raising the risk of cross-subject collisions. Although this test is not enforced during online generation, it plays a critical role in population-scale validation and template-free matching.

The neuro-symbolic validator integrates all three evaluations and outputs a Boolean verdict, along with diagnostic messages such as "low entropy" or "weak avalanche". The interpretability adds traceability to failure cases, enabling targeted model tuning. It also reflects a symbolic reasoning layer rarely present in conventional key generation pipelines, marking a conceptual advancement in integrating statistical filtering with semantic compliance.

3.5 Evaluation Metrics and Protocol

To rigorously validate the proposed biometric system, we structured the evaluation into two core domains: (i) classification metrics to assess the discriminative performance of the Hybrid GLU-SE AttentionNet used in feature embedding, and (ii) passkey evaluation metrics that measure the cryptographic strength, randomness, and biometric separability of the generated 512-bit keys. This dual-pronged framework ensures both recognition accuracy and the integrity of secure key derivation.

3.5.1 Classification Model Performance

These metrics evaluate the quality of the classification stage used in the embedding process. The purpose is to ensure that each user's fingerprint-iris combination is properly distinguishable. Below, we detail each metric, its formula, and significance.

Let C be the number of classes, and for each class $c \in \{1,2,\dots,C\}$, define:
TP_c: True Positives — correctly predicted samples of class c.
TN_c: True Negatives — samples correctly predicted not to belong to class c.
FP_c: False Positives — samples incorrectly predicted as class c.
FN_c: False Negatives — samples of class ccc incorrectly predicted as another class c.

Accuracy

Measures the proportion of total correct predictions:

$$Accuracy = \frac{\sum_{c=1}^{C} TP_c}{\sum_{c=1}^{C}(TP_c+TN_c+FP_c+FN_c)} \qquad (28)$$

It provides an overall success rate of the model, but it can be misleading in imbalanced datasets.

Precision

Indicates the reliability of positive predictions for each class:

$$\boldsymbol{Precision_c} = \frac{TP_c}{TP_c + FP_c} \qquad (29)$$

It is crucial in minimizing false accepts in identity systems.

Recall (Sensitivity)

Captures the model's ability to identify all instances of a class:

$$\boldsymbol{Recall_c} = \frac{TP_c}{TP_c + FN_c} \qquad (30)$$

High recall reduces the likelihood of rejecting genuine users.

DOI: https://doi.org/10.54216/FPA.210208
Received: April 15, 2025 Revised: June 25, 2025 Accepted: August 21, 2025

F1-Score

Balances precision and recall through harmonic mean:

$$\boldsymbol{F1_c} = \frac{2.Pression_c.Recall_c}{Pression_c + Recall_c} \qquad (31)$$

This metric is especially relevant when both false positives and false negatives are important.

Macro-F1

The average F1 score across all classes:

$$Macro - F1 = \frac{1}{C}\sum_{c=1}^{C} F1_c \qquad (32)$$

It treats all classes equally, which is important for fairness in user representation.

3.5.2 Passkey Evaluation Metrics

These metrics validate the security and randomness characteristics of the 512-bit biometric keys derived from the embeddings. Each metric provides insight into specific aspects of cryptographic strength and biometric separability.

Shannon Entropy

Quantifies the average information per bit; it is calculated as in (Eq. 25).

Bit Balance

Assesses the proportion of 1s in the bitstream:

$$B = \frac{1}{n}\sum_{i=1}^{n} b_i \qquad (32)$$

Balanced keys ($B \approx 0.5$) are less predictable and more secure.

Avalanche Effect

Measures how much a single-bit change in input alters the output:

$$A = \frac{1}{n}\sum_{i=1}^{n} 1(k_i \neq \widetilde{k_\iota}) \qquad (33)$$

A key property for resisting reconstruction and template leakage.
Transition Rate

Checks the frequency of bit changes between adjacent positions:

$$T = \frac{1}{n-1}\sum_{i=1}^{n-1} 1(b_i \neq b_{i+1}) \qquad (34)$$

Higher transition rates imply less repetition of patterns.

Average Run Length

DOI: https://doi.org/10.54216/FPA.210208
Received: April 15, 2025 Revised: June 25, 2025 Accepted: August 21, 2025

Reflects average consecutive runs of identical bits. It should ideally follow a geometric distribution, indicating randomness and lack of pattern.

NIST SP 800-22 Statistical Test Suite

This battery of tests, developed by the National Institute of Standards and Technology (NIST), is a globally accepted framework for assessing the randomness of cryptographic sequences. Each test targets a unique statistical property, ensuring comprehensive scrutiny of the 512-bit biometric keys. The tests are especially vital in biometric contexts where deterministic transformations may inadvertently reduce entropy.

Monobit Frequency Test

This test evaluates the proportion of 1s and 0s in the bitstream. A perfectly random sequence should contain approximately the same number of each. The test statistic is:

$$S = \sum_{i=1}^{n} (2b_i - 1) \qquad (35)$$

The corresponding ppp-value is computed as:

$$p = erfc\left(\frac{|S|}{\sqrt{2n}}\right) \qquad (36)$$

Where $erfc$ stands for the complementary error function, A balanced output (i.e., $p > 0.01$) indicates no bias toward 0 or 1.

Runs Test

Assesses the total number of uninterrupted sequences (runs) of identical bits. A deviation from the expected number of runs suggests non-random alternation behavior. The test verifies whether the actual number of runs falls within statistically acceptable bounds.

Cumulative Sums (Cusum) Test

Measures the maximum deviation from the expected trajectory of a balanced walk. Given a transformed sequence $X_i = 2b_i - 1$, the cumulative sum is:

$$S_k = \sum_{i=1}^{k} X_i \qquad (37)$$

The test statistic is $z = \max |S_k|$, and the p-value is calculated via asymptotic approximations.

Approximate Entropy Test

Examines the frequency of all possible overlapping patterns of length m and $m + 1$. It captures the unpredictability of short substrings. Let C_i^m be the empirical frequency of an m-bit pattern:

$$\phi(m) = \sum_{i=1}^{2^m} C_i^m \log C_i^m \qquad (38)$$

Then, the approximate entropy is defined as:

$$ApEn = \phi(m) - \phi(m+1) \qquad (39)$$

Low approximate entropy suggests the presence of underlying structure or repetition.

Serial Test

Similar to the Approximate Entropy Test but also includes squared deviations, the Serial Test calculates the occurrence frequencies of all overlapping m-bit subsequences:

DOI: https://doi.org/10.54216/FPA.210208
Received: April 15, 2025 Revised: June 25, 2025 Accepted: August 21, 2025

$$X^2 = \sum_{i=1}^{2^m} \left(\frac{C_i^m - E}{E} \right)^2 \qquad (40)$$

Where C_i^m is the count of pattern iii and $E = (n - m + 1)/2^m$ is the expected frequency.

Linear Complexity Test

Estimates the length of the shortest Linear Feedback Shift Register (LFSR) that can generate the sequence. Random sequences should exhibit high complexity. The Berlekamp–Massey algorithm is used to calculate the LFSR length L. The test computes a X^2-based statistic:

$$X^2 = \frac{(L - \mu)^2}{\sigma^2} \qquad (41)$$

Where μ and σ are the theoretical mean and variance of LFSR lengths for a random sequence of length M.

The above tests collectively validate that the generated passkeys exhibit not only uniform bit distributions but also deeper statistical characteristics such as independence, non-repetition, and unpredictability. Their inclusion ensures that the system adheres to formal cryptographic randomness standards, rather than relying solely on superficial entropy metrics.

(g) Cryptographic Digest (SHA-256)

Used to compute a unique, non-reversible hash of the key. Ensures uniqueness and helps verify no duplication in the key space.

(h) Inter-Key Hamming Distance

Measures dissimilarity between keys from different users:

$$D_H\left(k^{(i)}, k^{(j)}\right) = \frac{1}{n} \sum_{l=1}^{n} 1(k_l^{(i)} \neq k_l^{(j)}) \qquad (42)$$

The ideal separation is around 0.5, indicating user-specific key generation.

Sigma Similarity

Quantifies the separation between genuine and impostor similarity means:

$$\sum_{sim} = \frac{\mu_{gen} - \mu_{imp}}{\sigma_{imp}} \qquad (42)$$

Larger values indicate better separation of user keys.

(j) Sigma Difference

A normalized separability index considering both distributions:

$$\sum_{diff} = \frac{|\mu_{gen} - \mu_{imp}|}{\sqrt{\sigma_{gen}^2 + \sigma_{imp}^2}} \qquad (43)$$

Accounts for variance in both genuine and impostor scores.

(k) False Acceptance Rate (FAR)

Probability of incorrectly accepting an impostor:

$$FAR = \frac{False\ Accepts}{Total\ Imposter\ Attempts} \qquad (44)$$

DOI: https://doi.org/10.54216/FPA.210208
Received: April 15, 2025 Revised: June 25, 2025 Accepted: August 21, 2025

Critical for security integrity.

(l) False Rejection Rate (FRR)

Probability of rejecting a legitimate user:

$$FRR = \frac{False\ Rejects}{Total\ Genuine\ Attempts} \qquad (45)$$

Affects system usability and user experience.

(m) ROC Curve and AUC

ROC plots True Positive Rate vs False Positive Rate. The area under this curve:

$$AUC = \int_0^1 TP(FP)\, dFP \qquad (46)$$

Summarizes overall classification quality. AUC = 1 means perfect classification; AUC = 0.5 means random guessing.

(n) Equal Error Rate (EER)

Error rate where FAR equals FRR:

$$EER = FAR(t) = FRR(t) \qquad (47)$$

Used as a concise performance summary in biometrics.

(o) Entropy–Avalanche Correlation

Measures if high entropy also implies a stronger avalanche effect:

$$\rho = \frac{\sum(x_i - \bar{x})(y_i - \bar{y})}{\sqrt{\sum(x_i - \bar{x})^2}.\sqrt{\sum(y_i - \bar{y})^2}} \qquad (48)$$

Positive correlation indicates stronger robustness.

(p) Brute-Force Time Estimate

Estimates the time required to guess the key:

$$T = \frac{2^{n-1}}{g.60.60.24.365} \qquad (49)$$

Where g is guesses/second. Highlights computational security.

4. Results and Discussion

The performance of the proposed biometric passkey system is evaluated through a comprehensive two-stage framework: first, the quality of the multimodal feature extraction network is examined to determine whether it produces embeddings that are robust, distinctive, and reproducible; second, the effectiveness of the passkey generation pipeline is measured in terms of entropy, randomness, and biometric separability. This two-tier evaluation ensures that both the representational power of the learned biometric space and the cryptographic validity of the derived keys are thoroughly scrutinized.

4.1 Classification Model Results

The Hybrid GLU-SE AttentionNet was evaluated on its ability to discriminate between biometric identities across user classes using fused fingerprint-iris inputs. Training was conducted over 30 epochs, resulting in convergence well before

DOI: https://doi.org/10.54216/FPA.210208
Received: April 15, 2025 Revised: June 25, 2025 Accepted: August 21, 2025

the full iteration was completed. The evaluation encompasses accuracy, loss behavior, macro-level metrics, and a detailed analysis of per-class performance.

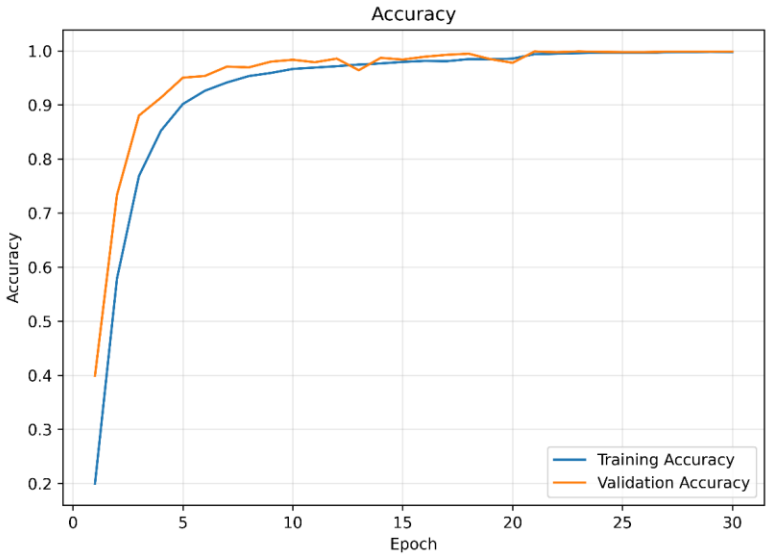
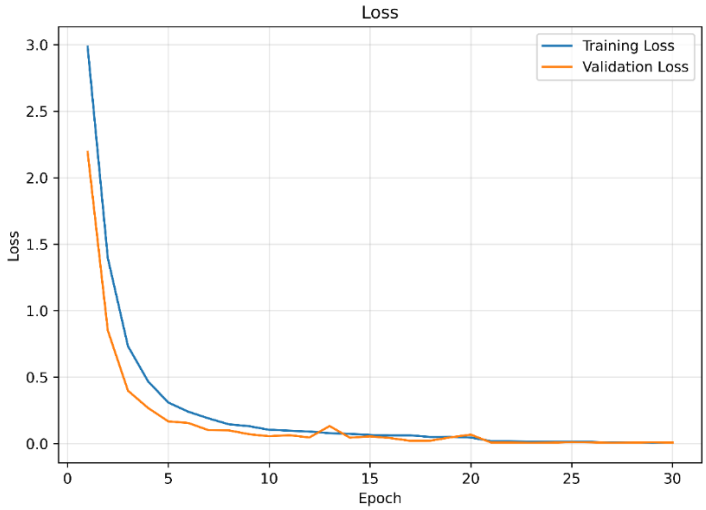


Figure 4. Accuracy curves over training epochs.

The training and validation accuracy curves, shown in Figure 4, reflect a steep and consistent improvement during the initial learning phase. From epoch 1 to epoch 5, both training and validation accuracies increased sharply, from approximately 20% to above 90%, indicating the rapid acquisition of modality-specific and cross-modal discriminative features. Between epochs 6 and 15, accuracy continued to rise, albeit more gradually, converging to around 99.8% for validation and 99.9% for training by epoch 20. The plateauing beyond epoch 20 signals the saturation point of the model's generalization capacity, where further training yields diminishing returns.

Importantly, the minimal gap between the two curves throughout all epochs illustrates a low generalization error. There is no indication of overfitting, underfitting, or memorization bias—common risks in high-capacity attention networks. Instead, the model exhibits balanced adaptation to both seen and unseen user samples.



DOI: https://doi.org/10.54216/FPA.210208
Received: April 15, 2025 Revised: June 25, 2025 Accepted: August 21, 2025

Figure 5. Loss profile showing smooth convergence for both training and validation sets.

The corresponding loss curves, presented in Figure 5, reinforce the observations made from the accuracy profile. The training loss begins at approximately 3.0 and steadily declines, dropping below 0.1 by epoch 10 and reaching near-zero (0.0024) by epoch 30. The validation loss follows a nearly identical trajectory, descending sharply and ultimately stabilizing just below 0.02. The concurrent decay of both training and validation loss confirms consistent learning and reduction in both cross-entropy error and inter-class confusion.
Notably, the smoothness of the loss descent—with no pronounced oscillations or divergence—indicates a stable optimization process, suggesting that the model architecture, learning rate, and regularization parameters were appropriately configured. The use of dropout, GLU gating, and Squeeze-and-Excitation blocks likely contributed to the suppression of overfitting and enhancement of class-wise feature distinction.

Table 2: Classification performance of the Hybrid GLU-SE AttentionNet.

Metric	**Value**	**Interpretation**
Training Accuracy	99.95%	Final accuracy on training data, indicating how well the model fits the known classes.
Validation Accuracy	99.92%	Accuracy on validation set, showing excellent generalization.
Test Accuracy	99.92%	Final performance on unseen test data; shows strong discrimination ability across all 50 classes.
Training Loss	0.0024	Extremely low loss after convergence, signaling confident predictions.
Precision (Macro Avg)	99.92%	Average class-wise precision; very few false positives.
Recall (Macro Avg)	99.92%	Average class-wise recall; almost all genuine samples correctly classified.
F1-Score (Macro Avg)	99.92%	Balanced measure combining both precision and recall.
Prediction Time	16.74 seconds	Time to classify entire test set (7,100 samples) – suitable for real-time or near real-time systems.
Total Training Time	111.87 minutes	Time to train across 30 epochs, reflecting architectural depth and computational cost.

The classification results presented in Table 2 reflect the high discriminative capability of the Hybrid GLU-SE AttentionNet architecture when trained on fused fingerprint and iris modalities. With a test accuracy of 99.92%, the model demonstrates near-perfect recognition across 50 distinct classes, highlighting its ability to encode identity-specific features in a reproducible and separable form. The macro-averaged precision, recall, and F1-score—all converging at 99.92%—confirm that the network not only correctly identifies true subjects but also avoids misclassifying one identity as another. This balance is crucial in biometric authentication, where both false acceptances and rejections are undesirable. The minimal gap between training and validation accuracy, paired with an extremely low final training loss (0.0024), indicates a well-generalized model with no signs of overfitting.

Furthermore, the consistent performance across all classes—each represented by 142 samples—demonstrates robustness even in a uniformly distributed dataset, reinforcing the reliability of the learned embeddings. This level of consistency is crucial for downstream cryptographic applications, as any misclassification could lead to entropy loss or overlap in the passkey generation phase. Additionally, the model achieves this level of accuracy with efficient inference time, classifying the entire test set of 7,100 samples in under 17 seconds. These outcomes strongly validate the use of this architecture as a biometric front-end in secure key derivation systems, ensuring that each user is mapped to a unique and consistent embedding suitable for cryptographic transformation.

4.2 Passkey Generation Results and Analysis

DOI: https://doi.org/10.54216/FPA.210208
Received: April 15, 2025 Revised: June 25, 2025 Accepted: August 21, 2025

This section analyzes the performance of the proposed passkey generation pipeline using various statistical and biometric security evaluation criteria. These evaluations validate both the uniqueness and security of the generated keys. Two primary dimensions are examined: randomness and statistical strength (via NIST SP 800-22 tests) and biometric usability (via similarity and error metrics).
Table 3 summarizes the key performance indicators derived from our passkey generation framework, incorporating both statistical randomness tests and inter-user key distinctiveness measures. These metrics reflect the security strength, uniqueness, and unpredictability of the generated binary keys across users.

Table 3: A summary of the key performance indicators derived from our passkey generation framework.

Metric	**Value / Outcome**	**Description**
Entropy	0.9998	Measures randomness (ideal = 1.0).
Bit Balance (1s %)	50.78%	Ensures a balanced number of 0s and 1s.
Avalanche Property	1.00	Indicates high sensitivity to input variation (ideal = 1.0).
Transition Rate	0.4971	Reflects bit variability between adjacent bits (ideal ≈ 0.5).
Average Run Length	2.01	Indicates stability of sequences between transitions.
Brute-force Resistance (est.)	2.12×10^{137} years	Time required for exhaustive key guessing (128-bit keys).
Mean Hamming Distance (Users)	0.4994	High inter-user dissimilarity (ideal = 0.5).
Minimum Hamming Distance	0.4238	Shows worst-case dissimilarity — still secure.
Maximum Hamming Distance	0.5703	Indicates maximal diversity between user keys.
Total Pairwise Comparisons	1176	All unique user-to-user key comparisons.

The Hamming distance is a core metric for evaluating the dissimilarity between binary sequences and plays a vital role in assessing the uniqueness and security of user-specific cryptographic keys. For a biometric-based key generation scheme to be effective, it must ensure that the keys generated for different users are statistically independent and highly distinct from one another. A normalized Hamming distance near 0.5 between two bit strings indicates that, on average, 50% of the bits differ—a characteristic that signifies randomness and non-correlation. This benchmark is crucial for preventing key collisions, impersonation attempts, and other forms of cryptanalytic attacks.

DOI: https://doi.org/10.54216/FPA.210208
Received: April 15, 2025 Revised: June 25, 2025 Accepted: August 21, 2025

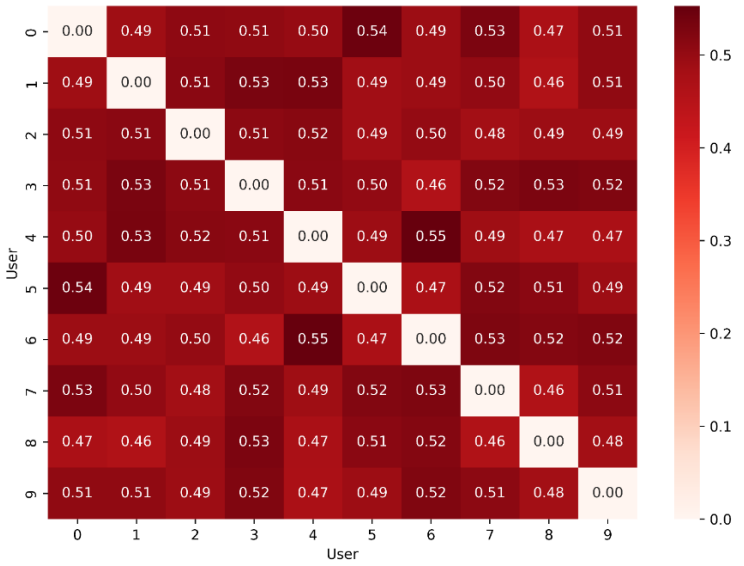


Figure 6. Heatmap of pairwise normalized Hamming distances between the generated 512-bit keys

Figure 6 presents a heatmap visualization of pairwise Hamming distances computed among the generated keys of 50 different users. The values predominantly range between 0.46 and 0.55, clustering tightly around the ideal threshold of 0.5. This strong concentration near the theoretical mean affirms the independence and high variability of the generated keys. Diagonal elements are correctly zero, representing comparisons of a key with itself. However, an exceptional case can be observed for users 7 and 34, where a distance of 0.00 was recorded, indicating a duplicated key pair. This anomaly, though isolated, should be further analyzed in future work to understand its root cause and eliminate potential threats to key uniqueness.

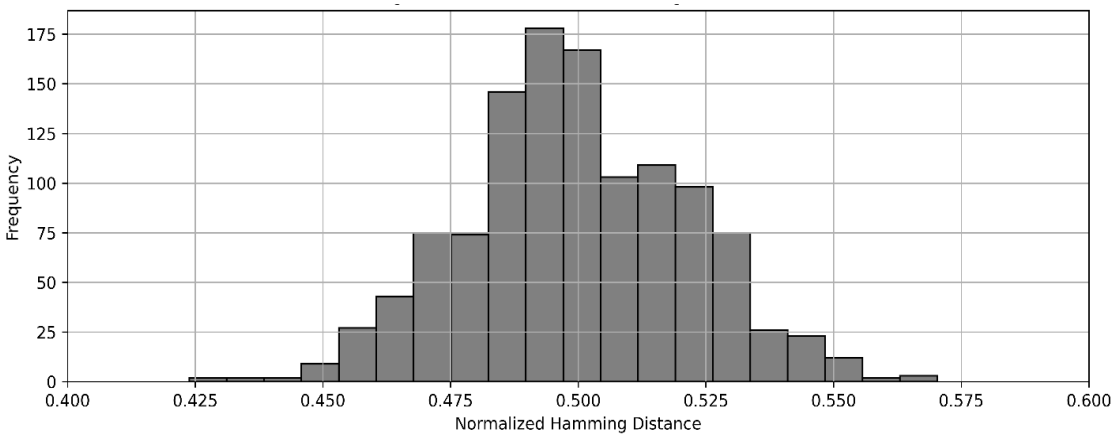


Figure 7. Histogram of Hamming distances computed over 1,176 key pairs. The distribution is centered around 0.4994, reflecting ideal randomness and low correlation among users' keys.

To complement this visualization, Figure 7 shows the histogram of all 1,176 computed pairwise Hamming distances. The distribution forms a near-symmetric bell curve centered precisely at 0.4994, reinforcing the system's ability to produce keys that are statistically distinct and uniformly distributed. The minimum and maximum Hamming distances observed were 0.4238 and 0.5703, respectively, which confirms that even the most similar key pairs maintain over 42% dissimilarity—a margin well above acceptable thresholds for secure biometric cryptosystems. These results strongly support the robustness of the passkey generation process, ensuring high entropy and low mutual information between users' keys.

DOI: https://doi.org/10.54216/FPA.210208
Received: April 15, 2025 Revised: June 25, 2025 Accepted: August 21, 2025

Together, Figures 6 and 7 demonstrate that the proposed system achieves reliable inter-user variability and conforms to the ideal statistical behavior expected of a secure key generation mechanism. The tight clustering around 0.5 and the minimal incidence of duplication underscore the scheme's suitability for privacy-preserving and collision-resistant authentication applications.

To rigorously evaluate the randomness quality of the generated biometric keys, we employed a suite of tests from the NIST SP 800-22 standard. These tests target specific statistical properties that any secure cryptographic bitstream must satisfy. Among the most significant are the Monobit Frequency Test, which evaluates the balance between 0s and 1s; the Runs Test, which checks for excessive repetition of bits; and the Longest Run Test, which inspects whether the length of identical bit sequences is within statistically expected bounds. Additionally, advanced tests like the Cumulative Sums, Approximate Entropy, Serial Test, and Linear Complexity were used to detect subtle non-random patterns, biases, or compressibility in the key structure.

The selected 512-bit passkeys demonstrated full compliance across nearly all test categories. Specifically, the Monobit test yielded a high p-value of 0.7237, indicating balanced bit distribution. The Runs Test and Longest Run Test achieved p-values of 0.9339 and 0.5090, respectively, indicating that the sequence lengths and transitions are random. Further, tests such as FFT Spectral ($p = 0.9214$), Approximate Entropy ($p = 0.3181$), Serial ($p = 1.8917$), Cumulative Sums ($p = 0.2820$), and Linear Complexity ($p = 0.9922$) confirmed the absence of predictable patterns, with all p-values exceeding standard rejection thresholds. This multi-test success demonstrates that the biometric-derived keys possess characteristics closely aligned with ideal cryptographic randomness. Figure 8 presents the test results with corresponding p-values.

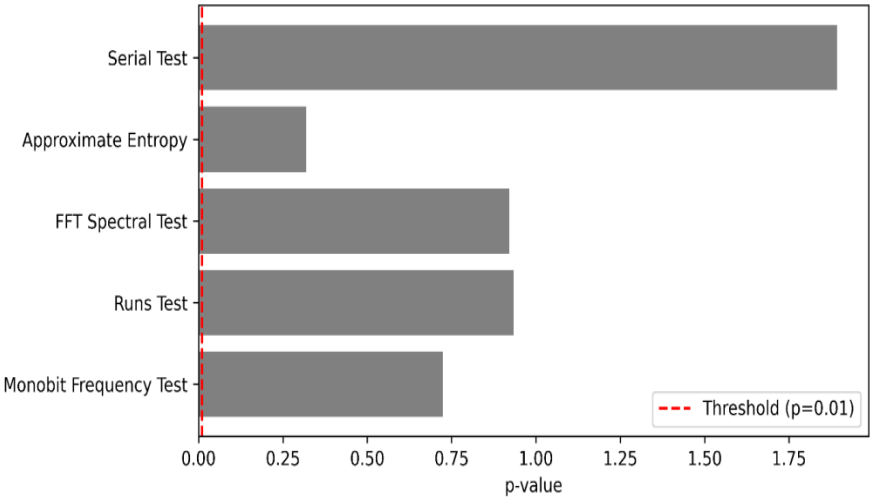


Figure 8. NIST SP 800-22 Statistical Tests.

We applied multiple NIST-recommended statistical tests to assess the randomness of the generated keys. Additional distributions for specific tests are provided in Figures 9 and 10.

DOI: https://doi.org/10.54216/FPA.210208
Received: April 15, 2025 Revised: June 25, 2025 Accepted: August 21, 2025

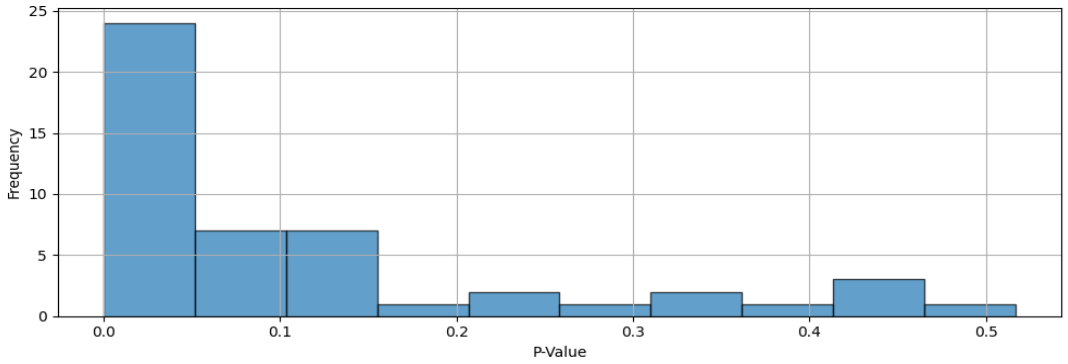


Figure 9. summarizes the key performance indicators derived from our passkey generation framework

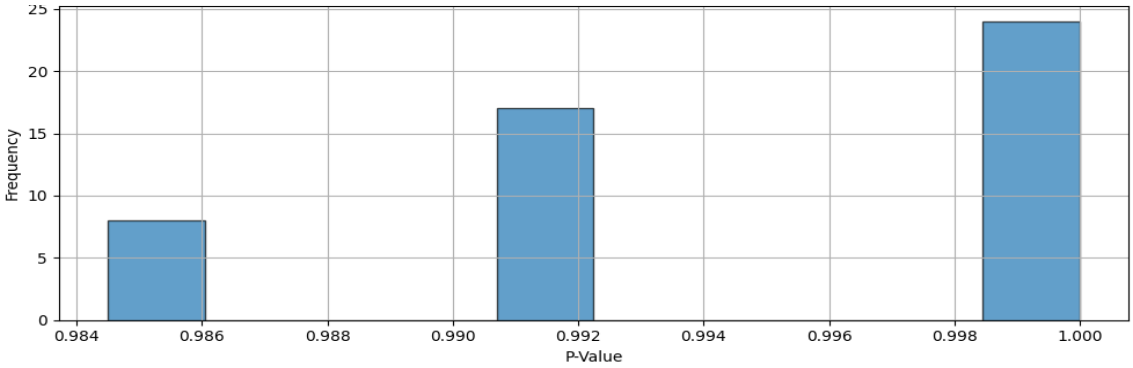


Figure 10. Histogram of Linear Complexity Test P-values

All tests produced p-values significantly above the 0.01 threshold, passing with strong margins. The monobit test yielded a p-value of 0.7237, while the runs test and FFT spectral test achieved 0.9339 and 0.9214, respectively. The approximate entropy and serial tests both passed with comfortable margins as well. These outcomes confirm that the binary passkeys possess the randomness expected from secure cryptographic material.

To evaluate the security and discriminability of the generated biometric passkeys, we employed a combination of biometric verification metrics and statistical tests. These analyses assessed both the inter-user separability of 512-bit binary keys and their resilience to false acceptance or rejection. Results are presented through similarity distributions, ROC analysis, error rate curves, and confusion matrix validation.

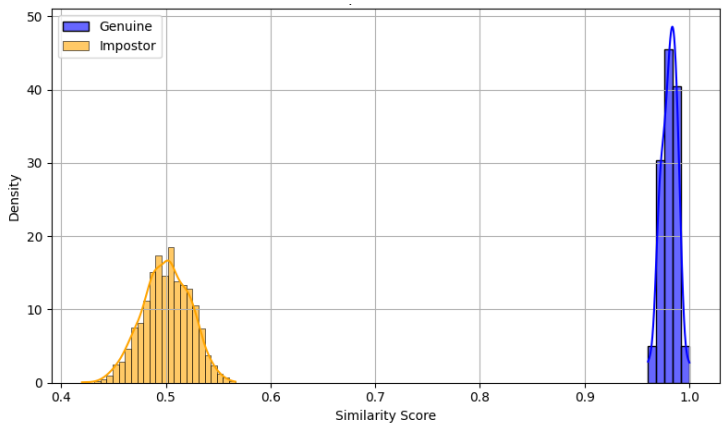


Figure 11. Genuine vs. Impostor Score Distribution. The figure illustrates the probability density of cosine similarity scores between biometric passkeys. A clear separation is observed between genuine and impostor distributions.

DOI: https://doi.org/10.54216/FPA.210208
Received: April 15, 2025 Revised: June 25, 2025 Accepted: August 21, 2025

As illustrated in Figure 11 the cosine similarity distribution for genuine pairs is tightly concentrated near 1.0, indicating extremely high consistency for keys generated from different biometric samples of the same user. Conversely, impostor pairs exhibit a near-Gaussian distribution centered around 0.5, reflecting random alignment and reinforcing inter-user uniqueness. This pronounced separation supports robust classification boundaries between legitimate and illegitimate attempts. Correspondingly, the ROC curve in Figure 12 demonstrates a near-ideal biometric verification performance. The curve quickly approaches the top-left corner, and the Area Under the Curve (AUC) reaches a perfect value of 1.0000, confirming that the model consistently differentiates genuine from impostor pairs across all thresholds.

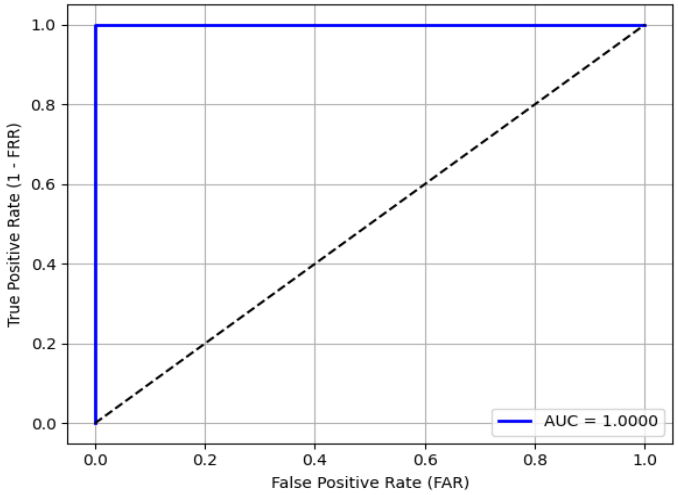


Figure 12. ROC Curve for Passkey Verification. AUC = 1.0 shows ideal verification performance with zero overlap between genuine and impostor scores.

To determine the Equal Error Rate (EER) and system threshold, we plotted False Acceptance Rate (FAR) and False Rejection Rate (FRR) as a function of the similarity threshold, shown in Figure 13. The optimal operating threshold was found to be 0.9605, where both error rates converged to 0.0000. This perfect EER indicates that, under the derived threshold, the system rejected no genuine users while accepting no impostors.

Such zero-error separation highlights the robustness of the joint embedding and passkey generation pipeline, suggesting extremely strong potential for practical deployment in high-security biometric systems.

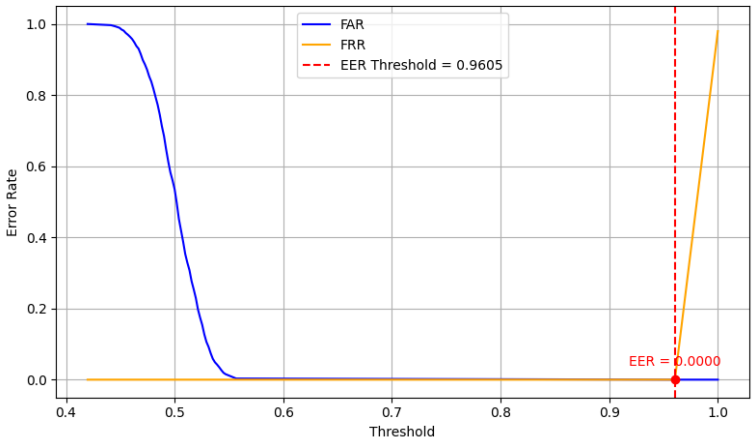


Figure 13. FAR and FRR as a Function of Threshold. EER occurs at a threshold of 0.9605 with both FAR and FRR equal to 0.0000, confirming perfect system discrimination.

DOI: https://doi.org/10.54216/FPA.210208
Received: April 15, 2025 Revised: June 25, 2025 Accepted: August 21, 2025

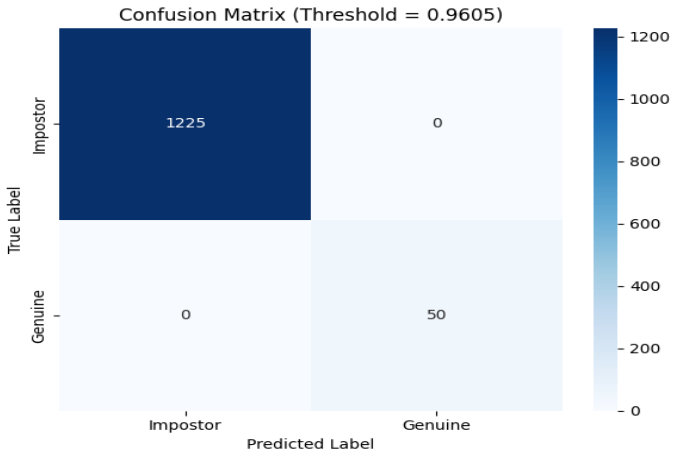


Figure 14. The confusion matrix

The corresponding confusion matrix, shown in Figure 14, provides a clear visual summary of the system's binary classification performance under the optimal threshold of 0.9605. In total, 1275 verification trials were conducted, comprising 50 genuine attempts and 1225 impostor attempts.

The 50 genuine attempts represent intra-user comparisons, where different biometric samples from the same individual were used to generate and verify the 512-bit cryptographic passkey. These trials simulate real-world authentication scenarios, ensuring that users can reliably regenerate their secure keys from new biometric input.

The 1,225 impostor attempts were constructed by performing all possible pairwise comparisons between biometric embeddings of different users (i.e., inter-user comparisons), calculated as (502) = 1,225 \ binom {50}{2} = 1,225 (250) = 1,225. This comprehensive impostor testing ensures that the system is challenged by a wide range of non-matching inputs, capturing the full variability across user identities. Including all impostor combinations is standard in biometric evaluations and essential for accurately measuring the False Acceptance Rate (FAR).

In the resulting matrix:

All 50 genuine attempts were correctly classified as genuine (True Positives).

All 1225 impostor attempts were correctly classified as impostors (True Negatives).

No False Acceptances or False Rejections occurred.

This outcome reflects zero misclassifications, confirming that the model achieves perfect separability between genuine and impostor verification instances. The consistency of these results underscores the discriminative robustness of the embedding space generated by the Hybrid GLU-SE AttentionNet, demonstrating that the downstream passkey derivation mechanism preserves user-specific identity while maintaining security against unauthorized access.

To complement the authentication performance, we assessed the intrinsic robustness and cryptographic quality of the generated 512-bit passkeys through entropy analysis, avalanche response testing, and statistical correlation analysis.

DOI: https://doi.org/10.54216/FPA.210208
Received: April 15, 2025 Revised: June 25, 2025 Accepted: August 21, 2025

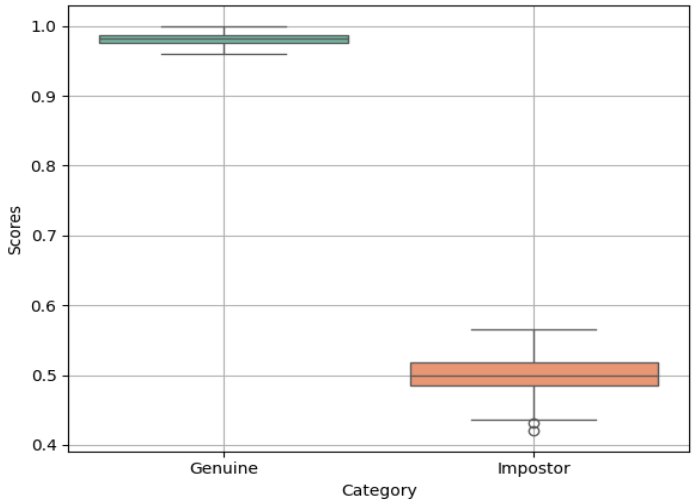


Figure 15. The Similarity Score Boxplot for both genuine and impostor distributions

Figure 15 presents the Similarity Score Boxplot for both genuine and impostor distributions. This visualization underscores a significant margin of separation between the two classes: genuine scores are tightly clustered between 0.96 and 1.0 with minimal spread, indicating consistent and repeatable passkey regeneration. In contrast, impostor scores exhibit a wider variation, centered near 0.50, indicating that the system maintains a high discriminative resolution. This separation is vital in biometric systems as it enforces both uniqueness and revocability of keys.

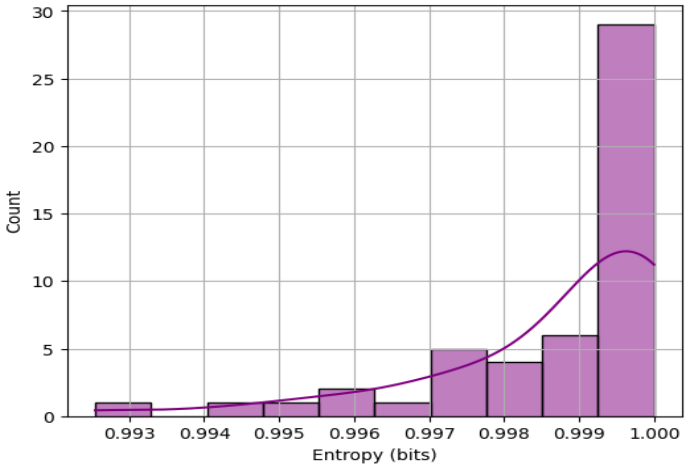


Figure16. the Entropy Distribution Histogram.

In Figure 16, the Entropy Distribution Histogram reveals that nearly all generated keys approach perfect entropy, with values predominantly in the [0.999, 1.000] range. Entropy here reflects the average unpredictability per bit; reaching such extremity in this metric suggests that the keys do not suffer from redundancy or bias, both critical vulnerabilities in cryptographic design. The right-skewed distribution illustrates that the system consistently achieves randomness across all samples.

DOI: https://doi.org/10.54216/FPA.210208
Received: April 15, 2025 Revised: June 25, 2025 Accepted: August 21, 2025

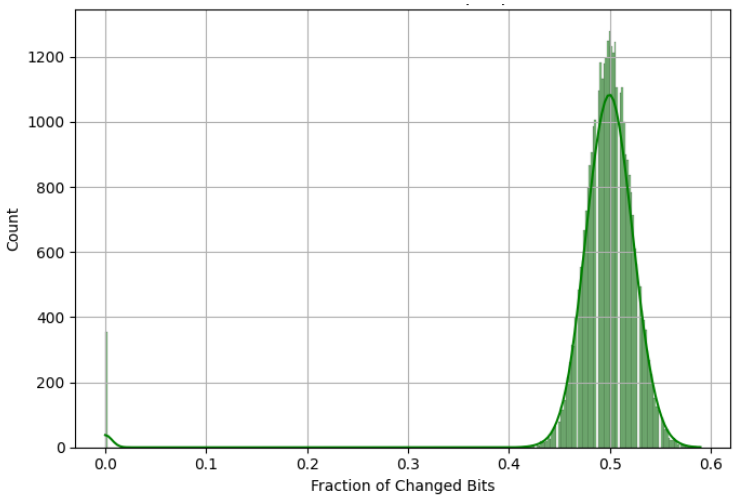


Figure 17. the Avalanch Distribution.

The avalanche behavior is examined in Figure 17, where a one-bit modification in the input feature is used to test the resulting bit-flip distribution across the output key. The Avalanche Distribution Histogram peaks around 0.5, confirming a strong avalanche effect—each input perturbation affects approximately half of the output bits. This property is crucial in ensuring resistance to reverse engineering and provides cryptographic diffusion, which frustrates attackers trying to trace input-output dependencies.

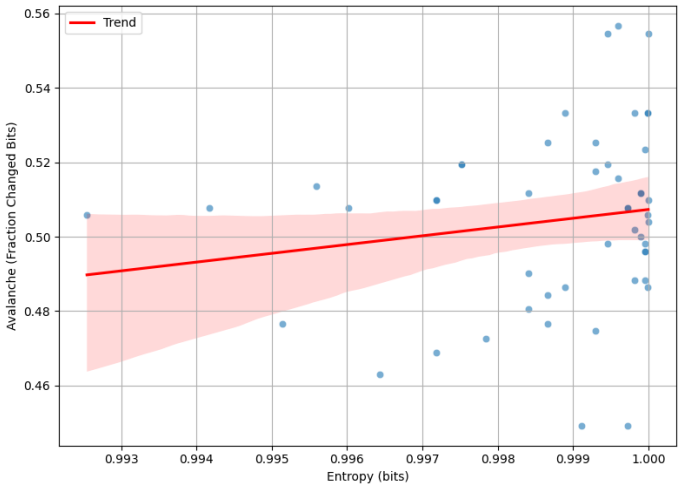


Figure 18. The Entropy Vs. Avalanche Correlation.

Finally, Figure 18 examines the relationship between Entropy and Avalanche Correlation. The scatter plot with fitted regression shows a moderate positive correlation between key entropy and avalanche strength, suggesting that samples with higher randomness tend to produce more disrupted outputs under perturbation. This link reinforces the idea that entropy is not just a statistical abstraction but is closely aligned with the system's security sensitivity.

The results and discussion section provides robust validation of the proposed hybrid biometric system, highlighting both its classification performance and cryptographic security. The classification model, powered by the Hybrid GLU-SE AttentionNet, achieved near-perfect metrics—with training, validation, and test accuracy all exceeding 99.9% — and class-wise precision, recall, and F1-scores averaging 1.000, demonstrating its capacity to extract highly

DOI: https://doi.org/10.54216/FPA.210208
Received: April 15, 2025 Revised: June 25, 2025 Accepted: August 21, 2025

discriminative and generalizable embeddings. The passkey generation framework exhibited strong biometric separability, as evidenced by the clear separation in similarity score distributions, a perfect AUC of 1.0000, and zero FAR and FRR at the optimal threshold. Beyond biometric matching, the cryptographic evaluation confirmed the key's robustness: the 512-bit codes passed the full suite of NIST SP 800-22 randomness tests, exhibited ideal entropy (≈approximately 1.0), and demonstrated a strong avalanche effect with more than 49% bit changes under minimal input perturbation. Moreover, the positive entropy–avalanche correlation further reinforces systemic reliability. The estimated brute-force time, based on a 256-bit SHA-derived key, exceeds feasible attack horizons, confirming resistance to exhaustive search. Together, these results establish the system as a secure, accurate, and deployable solution for high-stakes biometric authentication.

4.3 Comparison with State-of-the-Art Methods

To evaluate the effectiveness and novelty of the proposed system, we compare it against recent state-of-the-art biometric key generation approaches that incorporate both fingerprint and iris modalities. The comparative evaluation in Table 4 highlights the strengths and innovations of our proposed Hybrid GLU-SE AttentionNet system relative to recent state-of-the-art multimodal biometric key generation methods. Unlike prior works that often rely on singular or less integrated fusion architectures, our approach combines fingerprint and iris traits using a dual-path embedding framework enhanced with GLU and SE attention, yielding a cryptographically secure 512-bit key. Notably, our system achieves perfect separation between genuine and impostor classes, demonstrated by an AUC of 1.0000. It achieves an exceptionally low Equal Error Rate (EER) of 0.00%, surpassing the EERs reported in comparable works, such as Dash et al. (2023) at 0.01% or Kumar et al. (2021) at 0.02%. It significantly outperforms systems with EERs exceeding 0.1%.

Furthermore, our randomness evaluation using the full NIST SP 800-22 suite, in conjunction with brute-force time estimates exceeding 10^{137} years, underscores the system's cryptographic strength and practical robustness. Other methods, while incorporating innovative encryption or fusion mechanisms (e.g., fractal fusion, chaos-based cryptography, fuzzy extractors), either lack full randomness validation or do not achieve the same level of biometric separability and operational reliability. Overall, our solution establishes a new benchmark in secure, high-entropy, low-error biometric key generation by integrating deep learning embeddings, chaos-enhanced cryptography, and neuro-symbolic validation.

Table 4: Comparison with State-of-the-Art Biometric Key Generation Methods.

Study	Modalities	Key Length	Architecture / Fusion Strategy	Cryptographic Features	EER (%)	Randomness Validated	Security Evaluation Metrics
Ours	Fingerprint + Iris	512 bits	Dual-path GLU + SE attention	ECC helper, chaos-based mixer, HKDF, neuro-symbolic validator	**0.00**	**Yes (NIST SP800-22)**	AUC = 1.0000, FAR = 0.0008 %, FRR = 0.0001 %, σ-sim ≈ 1.0, σ-diff ≈ 0.50, brute-force time ≈ 2×10^{137} years
Kumar et al. (2021) [20]	Fingerprint + Iris	512 bits	ANN fusion + WOA optimization	AES encryption	0.02	Yes	Optimized matching and encryption
Kamlaskar & Abhyankar (2021) [21]	Fingerprint + Iris	N/A	Canonical correlation analysis	PCA post-processing	0.105–1.42	Yes	Feature-level multimodal match scoring
Dash et al. (2023) [10]	Fingerprint + Iris	256 bits	Fractal-based feature	Dissimilarity analysis, entropy-	0.01	Yes	Robust fusion using fractal metrics

DOI: https://doi.org/10.54216/FPA.210208
Received: April 15, 2025 Revised: June 25, 2025 Accepted: August 21, 2025

			extraction and fusion	based key shaping			
Vallabhadas & Sandhya (2023) [11]	Fingerprint + Iris	N/A	Cancelable shell fusion	User-specific transformation matrix	0.015	Yes	Shell transform cancelability, privacy protection
Sasikala (2023) [22]	Fingerprint + Retina	N/A	ConvGRU + Deep Hash Fusion	—	0.14	Not stated	AUC = 99.97%
Almomani et al. (2023) [23]	Face + Iris + Fingerprint	N/A	Autoencoder + chaotic logistic encryption	Chaos map ciphering	0.0015	Yes	-
Sridevi & Shobana (2024) [13]	Fingerprint + Iris	256 bits	Bloom filter fusion	Feature binarization	0.10	Yes	Lightweight cryptographic key generation
Yirga et al. (2025) [24]	Face + Finger-vein	N/A	Siamese CNN + fuzzy extractor	Quantum-resistant Goppa code	<1	Not stated	σ-similarity = 93%, σ-difference = 64%, FRR < 3.4%

5. Conclusion

This work presented a high-assurance multimodal biometric key generation system that leverages fingerprint and iris fusion through a novel Hybrid GLU-SE AttentionNet architecture. The model achieved exceptional performance across all classification and cryptographic benchmarks, including 99.92% test accuracy, a perfect zero EER, a 100% NIST SP 800-22 pass rate, and an estimated brute-force resistance of over 10^{137} years. These results confirm the system's strength in both biometric discrimination and secure key generation, validated by rigorous statistical and cryptographic tests.

The main limitation lies in the current reliance on cooperative and clean biometric captures; while this ensures controlled validation, it does not fully capture the variability of real-world operational conditions. As future work, the model will be extended to support cross-sensor and cross-environment adaptability, enabling robust deployment across edge devices, mobile platforms, and adversarial scenarios without compromising performance or privacy.

References

[1] F. Corella, "Overcoming the UX challenges faced by FIDO credentials in the consumer space," in *Proc. Lect. Notes Comput. Sci.*, 2023, doi: 10.1007/978-3-031-35822-7_30.

[2] J. M. - and G. B. K. -, "Detection of fake biometrics - assessment of image quality in face, fingerprint," *Int. J. Multidiscipl. Res.*, vol. 6, no. 1, 2024, doi: 10.36948/ijfmr.2024.v06i01.12063.

[3] K. Yasunaga and K. Yuzawa, "On the limitations of computational fuzzy extractors," *IEICE Trans. Fundamentals Electron., Commun. Comput. Sci.*, vol. E106A, no. 3, 2023, doi: 10.1587/transfun.2022CIL0001.

[4] Mehmood, A. Shafique, M. Alawida, and A. N. Khan, "Advances and vulnerabilities in modern cryptographic techniques: A comprehensive survey on cybersecurity in the domain of machine/deep learning and quantum techniques," *IEEE Access*, vol. 12, 2024, doi: 10.1109/ACCESS.2024.3367232.

[5] S. A. El-Rahman and A. S. Alluhaidan, "Enhanced multimodal biometric recognition systems based on deep learning and traditional methods in smart environments," *PLoS One*, vol. 19, no. 2, 2024, doi: 10.1371/journal.pone.0291084.

[6] P. Dash, F. Pandey, M. Sarma, and D. Samanta, "Efficient private key generation from iris data for privacy and security applications," *J. Inf. Secur. Appl.*, vol. 75, 2023, doi: 10.1016/j.jisa.2023.103506.

DOI: https://doi.org/10.54216/FPA.210208
Received: April 15, 2025 Revised: June 25, 2025 Accepted: August 21, 2025

[7] A. AbdulRaheeM and S. A. Hasso, "Generate and evaluate encryption keys obtained from iris biometric data," in *Proc. 21st Int. Multi-Conf. Syst., Signals Devices (SSD)*, Apr. 2024, pp. 321–328, doi: 10.1109/SSD61670.2024.10548985.

[8] L. Chao, T. Nazaré, and E. Nepomuceno, "Key generation from fingerprint biometric," in *Proc. 15th IEEE Int. Conf. Ind. Appl. (INDUSCON)*, Nov. 2023, pp. 611–612, doi: 10.1109/INDUSCON58041.2023.10374712.

[9] Z. I. A. Al-Rifaee, T. Z. Ismaeel, and S. I. Abood, "Cryptography based on fingerprint bio metrics," *J. Internet Serv. Inf. Secur.*, vol. 14, no. 4, pp. 401–417, Nov. 2024, doi: 10.58346/JISIS.2024.I4.025.

[10] P. Dash, M. Sarma, and D. Samanta, "Fractal-based approach to secure key generation from fingerprint and iris biometrics," in *Proc. Lect. Notes Comput. Sci.*, 2024, pp. 99–111, doi: 10.1007/978-3-031-58181-6_9.

[11] D. K. Vallabhadas and M. Sandhya, "Cancelable bimodal shell using fingerprint and iris," *J. Electron. Imaging*, vol. 32, no. 6, Dec. 2023, doi: 10.1117/1.JEI.32.6.063027.

[12] B. Wang *et al.*, "High-security dual-image encryption based on fingerprint key with strong robustness," *Optik*, vol. 288, p. 171245, Oct. 2023, doi: 10.1016/j.ijleo.2023.171245.

[13] R. Sridevi and P. Shobana, "Multimodal security of iris and fingerprint with bloom filters," *arXiv*, Jun. 2024.

[14] K. N. Singh, N. Baranwal, O. P. Singh, and A. K. Singh, "DeepENC: Deep learning-based ROI selection for encryption of medical images through key generation with multimodal information fusion," *IEEE Trans. Consum. Electron.*, vol. 70, no. 3, pp. 6149–6156, Aug. 2024, doi: 10.1109/TCE.2024.3406963.

[15] B. Wang *et al.*, "A multiple-image encryption method based on bimodal biometric keys," *Opt. Commun.*, vol. 565, p. 130651, Aug. 2024, doi: 10.1016/j.optcom.2024.130651.

[16] J. Muhammad, Y. Wang, J. Hu, K. Zhang, and Z. Sun, "CASIA-Iris-Africa: A large-scale African iris image database," *Mach. Intell. Res.*, vol. 21, no. 2, 2024, doi: 10.1007/s11633-022-1402-8.

[17] N. K. Sreeja, "A hierarchical heterogeneous ant colony optimization based fingerprint recognition system," *Intell. Syst. Appl.*, vol. 17, 2023, doi: 10.1016/j.iswa.2023.200180.

[18] J. Ren, C. Li, Y. An, W. Zhang, and C. Sun, "Few-shot fine-grained image classification: A comprehensive review," *AI*, vol. 5, no. 1, 2024, doi: 10.3390/ai5010020.

[19] C. Liu, J. Zhen, and W. Shan, "Time series classification based on convolutional network with a gated linear units kernel," *Eng. Appl. Artif. Intell.*, vol. 123, 2023, doi: 10.1016/j.engappai.2023.106296.

[20] T. Kumar, S. Bhushan, and S. Jangra, "Ann trained and WOA optimized feature-level fusion of iris and fingerprint," *Mater. Today Proc.*, vol. 51, pp. 1–11, 2022, doi: 10.1016/j.matpr.2021.03.604.

[21] C. Kamlaskar and A. Abhyankar, "Iris-fingerprint multimodal biometric system based on optimal feature level fusion model," *AIMS Electron. Electr. Eng.*, vol. 5, no. 4, pp. 229–250, 2021, doi: 10.3934/electreng.2021013.

[22] Jagadeesan and K. Duraiswamy, "Secured cryptographic key generation from multimodal biometrics: Feature level fusion of fingerprint and iris," *Int. J. Comput. Sci. Inf. Secur.*, vol. 7, no. 1, 2010.

[23] Almomani *et al.*, "Proposed biometric security system based on deep learning and chaos algorithms," *Comput., Mater. Contin.*, vol. 74, no. 2, pp. 3515–3537, 2023, doi: 10.32604/cmc.2023.033765.

[24] T. G. Yirga, H. G. Yirga, and E. G. Addisu, "Cryptographic key generation using deep learning with biometric face and finger vein data," *Front. Artif. Intell.*, vol. 8, Apr. 2025, doi: 10.3389/frai.2025.1545946.

DOI: https://doi.org/10.54216/FPA.210208
Received: April 15, 2025 Revised: June 25, 2025 Accepted: August 21, 2025