Journal of Intelligent Systems and Internet of Things
Vol. 17, No. 02, PP. 260-277, 2025
DOI: https://doi.org/10.54216/JISIoT.170217

A Secure Biometric Passkey Pipeline Combining Continuous Thinking Machine Models with Post-Quantum and Neuro-Symbolic Cryptography

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 offers a secure alternative to password-based authentication, but is hindered by challenges related to entropy, reproducibility, and adversarial resistance. This work presents a dual-path framework in which a Continuous Thinking Machine Model (CTMM) extracts multimodal embeddings from iris and fingerprint data. Feature vectors undergo projection through principal component analysis and graph-based distance encoding, followed by chaotic sequence modeling with Lorenz-like dynamics and an error-correcting routine to stabilize bitstreams. A secure mixing function consolidates the outputs, while SHA3-512 ensures deterministic expansion. Final passkeys are generated using the Kyber512 post-quantum key encapsulation mechanism (KEM), with neuro-symbolic reasoning applied as a validation layer to enforce entropy, avalanche properties, and inter-user separation. Evaluation confirmed compliance with NIST statistical tests, including monobit, runs, and longest-run assessments, while the system maintained a near-zero false acceptance rate. The originality of this work lies in combining CTMM-driven multimodal feature extraction with a quantum-safe cryptographic pipeline, augmented by neuro-symbolic validation, to establish a reproducible and secure method for biometric passkey generation in high-assurance authentication contexts.

Received: January 09, 2025 Revised: March 17, 2025 Accepted: June 02, 2025

Keywords: Biometric authentication; Passkey generation; Continuous thinking machine model (CTMM); Quantum-safe cryptography; Kyber512; Neuro-symbolic reasoning

1. Introduction

Biometric cryptography has emerged as a promising field at the intersection of machine learning and information security, motivated by the need to overcome the weaknesses of conventional password- and PIN-based systems. Passwords are susceptible to phishing, credential reuse, large-scale data breaches, and offline brute-force attacks, whereas biometric traits such as fingerprints and irises provide inherent distinctiveness tied to individual physiology [1]. Over the past two decades, significant advances in biometric authentication have enabled accurate identity verification, yet the reliable derivation of cryptographically strong keys directly from biometric signals remains an open challenge [2].

Existing approaches illustrate several limitations. Unimodal systems that depend solely on a single biometric trait—such as iris, fingerprint, or face—struggle with reproducibility when confronted with signal perturbations caused by sensor noise, pose variation, or environmental interference. Methods based on fuzzy extractors and helper data often make assumptions about feature distributions that inadvertently expose statistical regularities, diminishing their cryptographic robustness [3]. Similarly, deep learning-based architectures achieve strong performance in classification but rarely address the entropy regulation, avalanche sensitivity, and randomness

validation required of cryptographic key material [4]. Furthermore, multimodal fusion strategies often employ naive concatenation, which can lead to imbalanced modality contributions and reduced discriminative reliability. Importantly, many systems fail to formally validate derived bitstreams against cryptographic standards, leaving gaps in their resilience against adversarial or post-quantum threats [5].

This study addresses these gaps by proposing a hybrid framework for biometric passkey generation that integrates feature learning, chaotic modeling, post-quantum encryption, and symbolic validation into a unified pipeline. The framework applies a Continuous Thinking Machine Model (CTMM) to extract robust multimodal embeddings from fingerprint and iris modalities. These embeddings are projected through principal component analysis and graph-based distance encoding, then processed by a Lorenz-inspired chaotic generator and a lightweight error-correcting routine to stabilize bit-level representations. A secure mixing function consolidates the intermediate outputs, which are expanded with SHA3-512. The final 512-bit passkeys are generated using the Kyber512 post-quantum key encapsulation mechanism (KEM). To enforce compliance with cryptographic requirements, neuro-symbolic reasoning is incorporated as a validation layer, filtering weak or degenerate bitstreams and ensuring entropy, avalanche diffusion, and inter-user separation before acceptance.

The main contributions of this work are threefold.

1. CTMM-driven biometric feature extraction: a novel application of Continuous Thinking Machine Models for generating stable and discriminative embeddings from iris and fingerprint data, improving reproducibility under cross-modal variation.

2. Neuro-symbolic post-quantum cryptography: the integration of Kyber512 with neuro-symbolic reasoning to produce quantum-safe passkeys while providing logical interpretability and validation of entropy and avalanche properties.

3. Comprehensive cryptographic evaluation: an end-to-end testing protocol that includes NIST statistical randomness assessments, avalanche sensitivity analysis, and brute-force resilience, bridging the methodological gap between biometric learning and formal cryptographic assurance.

The remainder of this paper is organized as follows. Section 2 reviews related work, Section 3 presents the proposed method, Section 4 reports results and discussion, and Section 5 concludes the paper

2. Related Work

Biometric cryptography has evolved from template matching toward schemes that aim to generate reproducible, high-entropy keys directly from fingerprints and irises. Unimodal methods advanced individual properties but in isolation: Dash et al. improved entropy in iris-based systems without addressing reproducibility or avalanche validation [6]; AbdulRaheem and Hasso applied HOG descriptors with entropy testing but omitted avalanche and inter-user separation [7]; and Chao et al. used Reed–Solomon error correction to stabilize fingerprint features without cryptographic validation [8]. Multimodal approaches attempted to improve robustness, yet often relied on simple concatenation. Dash et al. fused fingerprint and iris features with fractal descriptors [9], Sridevi and Shobana applied Bloom filter fusion [10], and Vallabhadas and Sandhya introduced cancelable 3D templates [11], but all lacked entropy regulation or reproducibility. Singh et al. [12] and Wang et al. [13] incorporated chaos with deep learning or QR coding, yet focused on encryption rather than deterministic passkey generation. Chaos-based schemes further enhanced randomness, as in Wang et al.'s chaotic Fresnel diffraction [14] and Al-Rifaee et al.'s pseudo-random generators [15], but these lacked reproducibility, symbolic filtering, and resilience against post-quantum threats. Collectively, these efforts contributed elements such as entropy testing, error correction, fusion, and chaos, but none integrated them into a deployable cryptographic pipeline. The present study unifies these building blocks: the Continuous Thinking Machine Model (CTMM) produces fingerprint–iris embeddings, chaotic modeling strengthens entropy and avalanche properties, Kyber512 post-quantum encapsulation secures the passkey, and neuro-symbolic validation enforces entropy, avalanche, and separation thresholds. This integration yields reproducible, entropy-rich, and quantum-secure keys that directly overcome the limitations of prior work.

3. Methodology

The proposed framework introduces a unified pipeline for biometric-based passkey generation by integrating the Continuous Thinking Machine Model (CTMM), Error-Correcting Codes (ECC), quantum encryption, and neuro-symbolic reasoning into a single cohesive system. As illustrated in Figure 1, the architecture follows a left-to-right progression. The preprocessing block enhances biometric images before they are passed to the CTMM dual branches (fingerprint and iris). These two branches converge into a joint embedding, which is then split into the PCA projection and distance encoding paths. The figure highlights how these are recombined, passed into the DDCS chaotic generator, fused through the mixing function, and finally encapsulated via Kyber512 before neuro-

symbolic validation. This visual flow mirrors the modular subsections of the methodology. The process begins with data acquisition and preprocessing, where biometric images undergo enhancement and augmentation to improve contrast, reduce noise, and expand the dataset with synthetic variations. This step ensures resilience against environmental inconsistencies and acquisition noise, creating a more robust foundation for downstream feature extraction.

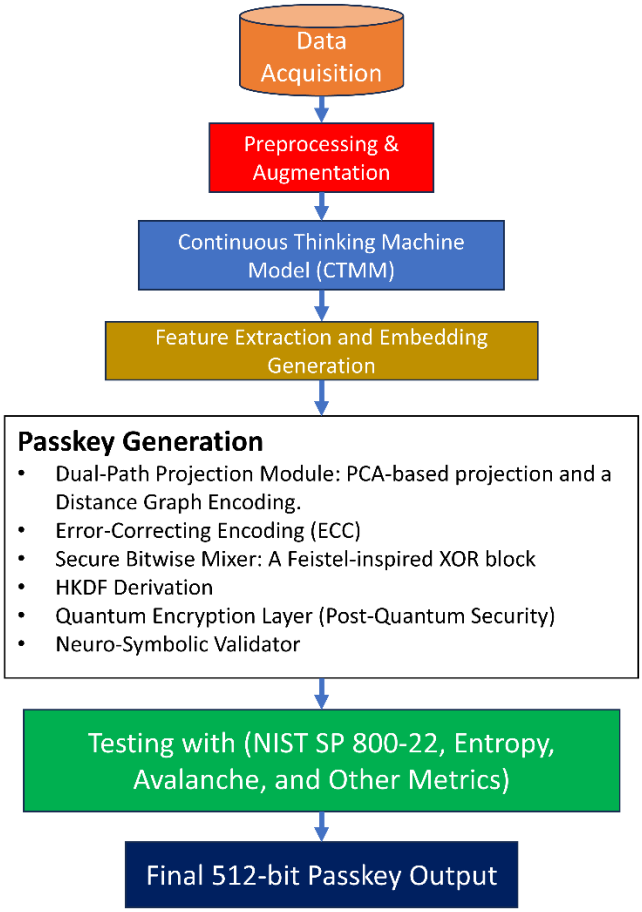

Figure 1. End-to-end pipeline of the proposed system.

The Continuous Thinking Machine Model (CTMM) is a dual-branch architecture, with one branch dedicated to fingerprint recognition and the other to iris recognition. Each branch applies depthwise and pointwise convolutions, squeeze–and–excitation, residual links, and max-pooling, culminating in global average pooling to produce compact descriptors. These descriptors are concatenated and refined through dense layers of 512 and 256 units with dropout, forming the joint biometric embedding. From this embedding, passkey construction proceeds in several steps. Principal component analysis (PCA) yields a 256-dimensional projection, while intra-vector distances form a second 256-dimensional descriptor. Their concatenation produces a 512-dimensional vector. Error-correcting preprocessing stabilizes this vector by sign binarization and deterministic bit flipping, while a deterministic chaotic system (DDCS) generates a parallel binary stream. The two streams are fused through XOR, cumulative propagation, and a Feistel-inspired permutation to produce a 512-bit diffused seed. The seed is secured using post-quantum cryptography (PQC). A Kyber512 key encapsulation mechanism (KEM) derives a shared secret, which is expanded with SHA3-512 to produce the final 512-bit passkey. Neuro-symbolic validation enforces entropy, avalanche, and inter-user separation thresholds. A deterministic random bit generator (DRBG) seeded by the passkey is further evaluated with NIST SP 800-22 tests to confirm statistical randomness.

3.1. Preprocessing and Augmentation

All biometric inputs, consisting of paired iris and fingerprint images, undergo a preprocessing and augmentation pipeline designed to ensure consistency, robustness, and reproducibility. Each image is converted to grayscale to retain structural detail while reducing complexity, then expanded into three identical channels to form standardized

64×64×3 tensors. Pixel values are scaled to the [0,1] range to stabilize intensity distributions and improve training convergence. The multimodal dataset was synthetically constructed by deterministically pairing SOCOFing fingerprints with CASIA-Iris samples from both eyes. This pairing creates composite identities suitable for passkey derivation, but it introduces a limitation, as the artificial correlation between unrelated traits may not capture natural multimodal dependencies. While this strategy addresses the scarcity of publicly available fingerprint–iris datasets, it may affect generalizability, and future validation on a genuine multimodal corpus remains necessary.
To improve robustness against acquisition variability, a multimodal augmentation policy was applied during training using the Albumentations library. Independent transformations were applied to each modality, including flips, rotations, brightness and contrast adjustments, and the addition of Gaussian noise. These perturbations simulated sensor and environmental variability while preserving anatomical integrity, thereby enhancing generalization without compromising the determinism required for stable cryptographic key generation.

3.2. CTMM Architecture

The Continuous Thinking Machine Model (CTMM) [16] is implemented as a dual-branch convolutional network that learns modality-specific representations from fingerprints and irises before forming a shared multimodal embedding. Each branch receives a normalized 64×64×3 tensor and processes it through a stack of three "continuous blocks" with channel sizes {32, 64, 128}. A continuous block comprises a depthwise 3×3 convolution to capture local, orientation-variant ridge or texture cues, a 1×1 linear projection to mix channels, a squeeze–recalibration pathway that computes a global average pooling followed by a two-layer bottleneck with reduction ratio 16 and a sigmoid gate, and a residual shortcut that preserves gradient flow when the number of channels changes. The gated activation rescales channels according to their global relevance. ReLU and batch normalization follow the residual update to stabilize the feature statistics. A 2×2 max-pooling between blocks provides spatial downsampling while retaining the dominant structural responses. After the third block, each branch applies global average pooling, producing a compact descriptor that is insensitive to minor spatial shifts while preserving modality-salient information. The fingerprint and iris descriptors are concatenated to yield a joint representation. Two fully connected layers, with widths of 512 and 256 and dropout rates of 0.5 and 0.3, respectively, refine this representation under a categorical cross-entropy objective with a softmax output over the enrolled identities. During passkey construction, supervision is used only to shape the embedding geometry; the embedding seed is taken from the penultimate representation rather than from the identity predictions, ensuring that cryptographic derivation consumes feature structure rather than class labels.
Formally, one continuous block can be written as:

$$u = BN\big(DWConv_{3\times3}(x)\big), \quad (1)$$

$$v = Conv_{3\times3}(u), \quad (2)$$

$$s = \sigma(W_2\phi(W_1 GAP(v))), \quad (3)$$

$$y = BN\big(\phi(v \odot Reshape(s) + P(x))\big), \quad (4)$$

Where DWConv is depthwise convolution, GAP is global average pooling, ϕ is ReLU, σ is sigmoid, $\odot$ denotes channel-wise scaling, P is the identity or a 1×1 projection to match dimensions, and BN is batch normalization. Stacking three such blocks with interleaved pooling in each branch yields, after global pooling, modality descriptors h_f and h_i that are concatenated as z=[h_f‖h_i] and mapped by the dense layers to the embedding used downstream. This design exploits depthwise separable filtering to decouple spatial and channel mixing, which reduces the number of learnable parameters and multiplications relative to standard convolutions while preserving fine ridge-valley and iris-texture detail; the squeeze–recalibration selectively amplifies informative channels and suppresses noise carried by spurious responses; and the residual pathway maintains stable training dynamics at small input resolution. In practice, this yields a favorable accuracy–cost trade-off: the depthwise–pointwise pattern lowers the computational load and memory footprint, global pooling eliminates large fully connected tensors over spatial grids, and the representation remains sufficiently expressive to support reliable and reproducible key derivation. As a result, CTMM contributes only modest runtime overhead compared with a plain small CNN, yet produces embeddings with better inter-subject separation and intra-subject stability, which are prerequisites for the dual-path projection and subsequent passkey pipeline.

3.3. Joint Embedding and Representation Refinement

The outputs of the fingerprint and iris branches are concatenated to form a fused multimodal representation that integrates the discriminative features extracted by the CTMM. This concatenated embedding is then refined through a sequence of fully connected layers. First, a dense layer of size 512 is introduced to enable nonlinear mixing across modalities, followed by dropout with a probability of 0.5 to enforce regularization and prevent

overfitting. The representation is further compressed into a 256-dimensional latent vector via a second dense layer, again accompanied by dropout (0.3) and batch normalization to stabilize the distribution of activations.

The result of this refinement stage is the joint biometric embedding, which acts as the penultimate output of the CTMM pipeline. Unlike a conventional classification network that terminates with a softmax prediction, the embedding produced here is specifically tailored for deterministic cryptographic derivation. By decoupling feature extraction from classification labels, the architecture ensures that the embedding preserves maximum information content and reproducibility, making it a robust foundation for the dual-path projection and cryptographic transformations in the downstream passkey generation module. This design achieves a balance between representational richness and efficiency: dense layers provide nonlinear fusion across modalities, while dropout and normalization ensure stability and reproducibility across repeated biometric acquisitions.

3.4. Passkey Generation Process and Algorithms

The objective of the biometric passkey pipeline is to derive a high-entropy, user-specific 512-bit key that is reproducible and cryptographically sound, even under minor variations in biometrics. This section details the complete transformation from the joint biometric embedding produced by the Continuous Thinking Machine Model (CTMM) to the final cryptographic key.

3.4.1. Dual-Path Projection

The fused embedding vector $\mathbf{e} \in \mathbb{R}^d$, produced by the final dense layer of the CTMM, 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 distances between each position and all others are 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

$$\mu_i = \frac{1}{64}\sum_{j=1}^{64} s_{i.j} \quad (5)$$

Standard deviation

$$\sigma_i = \sqrt{\frac{1}{64}\sum_{j=1}^{64}(s_{i.j} - \mu_i)^2} \quad (6)$$

Energy

$$E_i = \frac{1}{64}\sum_{j=1}^{64} s_{i.j}^2 \quad (7)$$

Variance

$$\delta_i = Var(s_i) \quad (8)$$

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

$$a_i = 10 + \mu_i \quad (9)$$

$$b_i = \frac{8}{3} + \sigma_i \quad (10)$$

$$r_i = 28 + E_i \quad (11)$$

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

$$x_{t+1} = (a_i.(y_t - x_t) + \delta_i.x_t) \mod 1 \quad (12)$$
$$y_{t+1} = (x_t.(r_i - z_t) + y_t) \mod 1 \quad (13)$$
$$z_{t+1} = (x_t.y_t - b_i.z_t) \mod 1 \quad (14)$$

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:

$$b_i = \begin{cases} 1 & if\ c_i > m \\ 0 & otherwise \end{cases} \quad (15)$$

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

$$\tilde{\mathbb{e}} = \frac{\mathbb{e} - \mu}{\sigma + \varepsilon} \quad (16)$$

Where μ and σ are the mean and standard deviation of $\mathbb{e}$, 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:

$$b_i = \begin{cases} 1 & if\ \tilde{e}_i > 0 \\ 0 & otherwise \end{cases} \quad (17)$$

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

$$b_{i+8} \leftarrow b_{i+8} \oplus 1 \text{ for } i = 0,8,16, \ldots \quad (18)$$

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 $\ominus \in \{0,1\}^{512}$ be the ECC-processed projection stream. The first stage of mixing applies a simple bitwise XOR operation to combine both:

$$m_i^{(0)} = \ominus_i \oplus c_i \;\; for\; i \in [0,511] \qquad (19)$$

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:

$$m^{(0)} = [b_0, b_1, \dots, b_7], \quad b_i \in \{0,1\}^{64} \qquad (20)$$

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:

$$b = [L, R], \quad L, R \in \{0,1\}^{32} \qquad (21)$$

The transformation proceeds as:

$$F(b, k) = [R, R \oplus ROL(L, k \bmod 32)] \qquad (22)$$

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:

$$m^{(2)} = concat\big(F(F(b_i, k_1), k_2)\big) \quad \forall i \in [0,7] \qquad (23)$$

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

$$m_i = m_i^{(2)} \oplus m_{i-1}^{(2)}, \quad i = 1, \dots, 511 \qquad (24)$$

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.

3.4.5. Quantum Encryption and Expansion

Unlike conventional approaches that rely on HMAC-SHA-256 HKDF, the proposed system employs a Post-Quantum Cryptography (PQC) mechanism. A Kyber512 keypair (pk, sk) is generated, encapsulation produces a shared secret ss, and decapsulation verifies correctness:

$$(pk, sk) \leftarrow Kyber512.KeyGen,$$
$$(ct, ss) \leftarrow Kyber512.Encap(pk),$$
$$ss = Kyber512.Decap(ct, sk). \qquad (25)$$

The shared secret is then expanded with SHA3-512 hashing, yielding a deterministic 512-bit passkey:

$$K_{512} = bits\big(SHA3 - 512(ss)\big) \qquad (26)$$

These steps ensure resistance against quantum adversaries, aligning the system with PQC standards.

3.5. 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:

(a) Entropy Estimation

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

$$H(K) = -\sum_{b \in \{0,1\}} p_b \log_2 p_b \qquad (27)$$

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.

(b) 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:

$$A = \frac{1}{512}\sum_{i=1}^{512} K_i \oplus K_i' \qquad (28)$$

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.

(c) 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:

$$S = \frac{1}{512}\sum_{i=1}^{512} K_i^u \oplus K_i^v \qquad (29)$$

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.

3.6. 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.

(a) Shannon Entropy

Quantifies the average information per bit; it is calculated as in (Eq. 27).

(b) Bit Balance

Assesses the proportion of 1s in the bitstream:

$$B = \frac{1}{n}\sum_{i=1}^{n} b_i \qquad (28)$$

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

(c) Avalanche Effect

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

$$A = \frac{1}{n}\sum_{i=1}^{n} 1(k_i \neq \widetilde{k_i}) \qquad (29)$$

A key property for resisting reconstruction and template leakage.

(d) Transition Rate

Checks the frequency of bit changes between adjacent positions:

$$T = \frac{1}{n-1}\sum_{i=1}^{n-1} 1(b_i \neq b_{i+1}) \qquad (30)$$

Higher transition rates imply less repetition of patterns.

(e) Average Run Length

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

(f) 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.

1. **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:

$$S = \sum_{i=1}^{n}(2b_i - 1) \qquad (31)$$

The corresponding ppp-value is computed as:

$$p = erfc\left(\frac{|S|}{\sqrt{2n}}\right) \qquad (32)$$

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

2. **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.

3. **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:

$$\phi(m) = \sum_{i=1}^{2^m} C_i^m \log C_i^m \qquad (33)$$

Then, the approximate entropy is defined as:

$$ApEn = \phi(m) - \phi(m+1) \qquad (34)$$

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:

$$X^2 = \sum_{i=1}^{2^m} \left(\frac{C_i^m - E}{E} \right)^2 \qquad (35)$$

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

(h) Inter-Key Hamming Distance

Measures dissimilarity between keys from different users:

$$D_H\left(k^{(i)}, k^{(j)}\right) = \frac{1}{n} \sum_{l=1}^{n} 1(k_l^{(i)} \neq k_l^{(j)}) \qquad (36)$$

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

(k) False Acceptance Rate (FAR)

Probability of incorrectly accepting an impostor:

$$FAR = \frac{False\ Accepts}{Total\ Imposter\ Attempts} \qquad (37)$$

Critical for security integrity.

(l) False Rejection Rate (FRR)

Probability of rejecting a legitimate user:

$$FRR = \frac{False\ Rejects}{Total\ Genuine\ Attempts} \qquad (38)$$

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:

$$AUC = \int_0^1 TP(FP)\, dFP \qquad (39)$$

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:

$$EER = FAR(t) = FRR(t) \qquad (40)$$

Used as a concise performance summary in biometrics.

(p) Brute-Force Time Estimate

Estimates the time required to guess the key:

$$T = \frac{2^{n-1}}{g.60.60.24.365} \qquad (41)$$

Where g is guesses/second. Highlights computational security.

4. Results and Discussion

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 (as assessed by NIST SP 800-22 tests), and biometric usability (evaluated through similarity and error metrics).

Table 1 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 1: A summary of the key performance indicators derived from our passkey generation framework.

Metric	Value / Outcome	Description
Entropy	0.9995	Measures randomness (ideal = 1.0).
Bit Balance (1s %)	51.37%	Ensures a balanced number of 0s and 1s.
Avalanche Property	1.00	Indicates high sensitivity to input variation (ideal = 1.0).
Transition Rate	0.4834	Reflects bit variability between adjacent bits (ideal ≈ 0.5).
Average Run Length	2.06	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)	0.5002	High inter-user dissimilarity (ideal = 0.5).
Minimum Hamming Distance	0.4219	Shows worst-case dissimilarity — still secure.
Maximum Hamming Distance	0.5684	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.

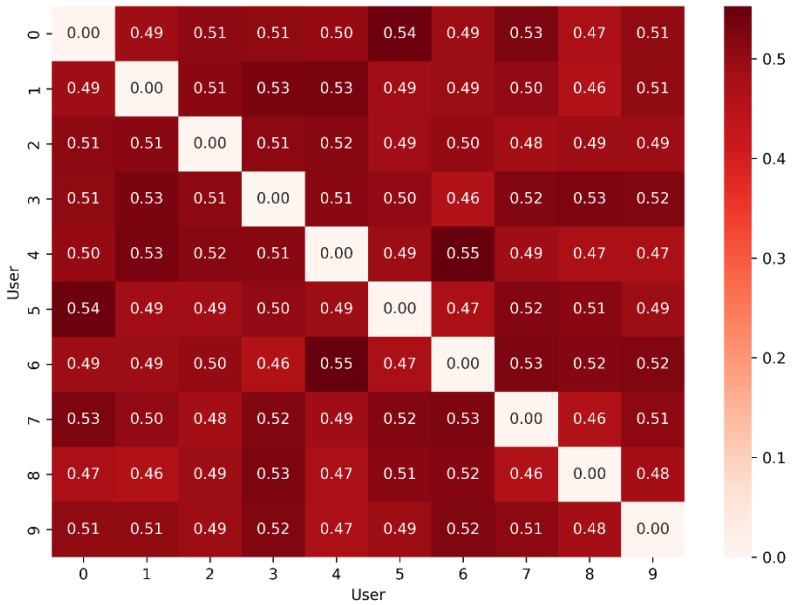

Figure 2. Heatmap of pairwise normalized Hamming distances between the generated 512-bit keys

Figure 2 presents a heatmap visualization of pairwise Hamming distances computed among the generated keys of 10 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.

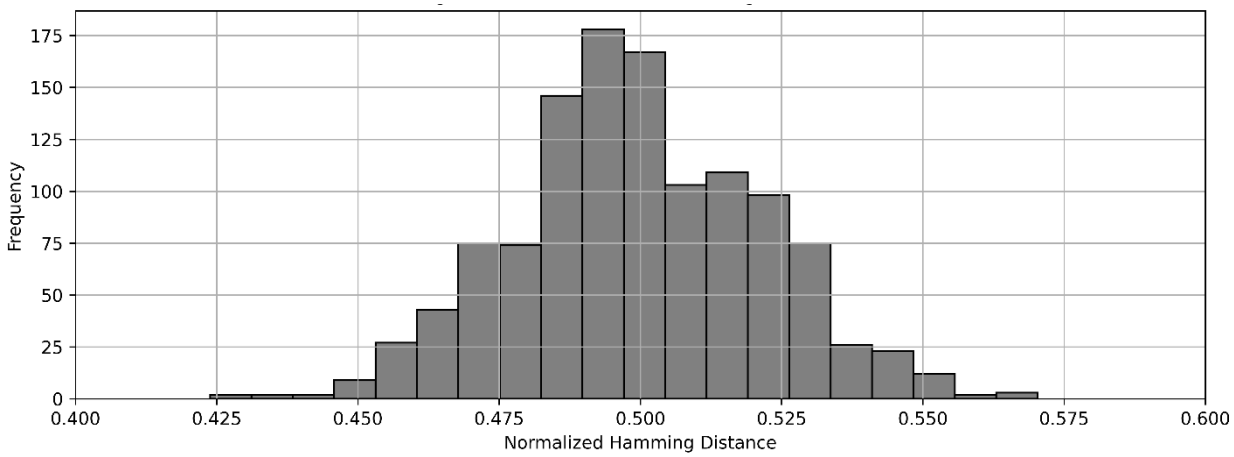

Figure 3. Histogram of Hamming distances computed over 1,176 key pairs.

To complement this visualization, Figure 3 shows the histogram of all 1,176 computed pairwise Hamming distances. The distribution forms a near-symmetric bell curve centered precisely at 0.5002, reinforcing the system's ability to produce keys that are statistically distinct and uniformly distributed. The minimum and maximum Hamming distances observed were 0.4219and 0.5684, 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.

Together, Figures 2 and 3 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 0.5361, indicating balanced bit distribution. The Runs Test and Longest Run Test achieved p-values of 0.5657 and 0.5280, respectively, indicating that the sequence lengths and transitions are random. Further, tests such as FFT Spectral 0.9754, Approximate Entropy 0.4105, Serial 1.0631, Cumulative Sums 0.415237, and Linear Complexity 0.976835 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. As shown in Figure 4, all evaluated passkeys exceeded the significance threshold ($p > 0.01$) across the NIST SP 800-22 battery, including Monobit, Runs, Longest Run, and Approximate Entropy tests. The visual presentation confirms that no test category approached the rejection boundary, underscoring the statistical robustness of the generated bitstreams. In particular, the Monobit and Runs tests demonstrate balanced distributions of 0s and 1s, while the Linear Complexity test confirms the absence of compressible patterns. Figure 4 thus provides a comprehensive validation of cryptographic randomness, complementing the summary statistics reported in the text.

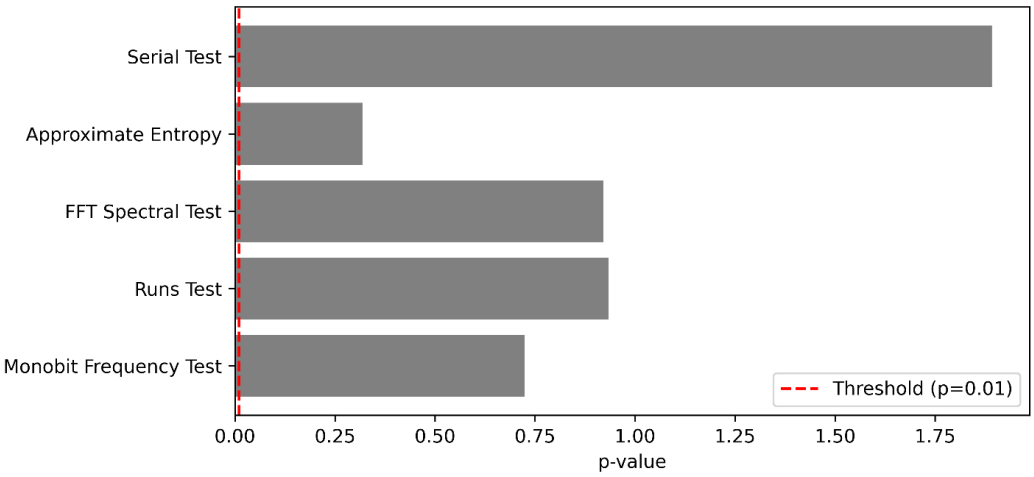

Figure 4. NIST SP 800-22 Statistical Tests.

As illustrated in Figure 5, the ROC curve rapidly approaches the top-left corner, indicating that the system achieves very high true positive rates even at minimal false positive rates. The near-vertical rise and horizontal plateau are characteristic of an almost perfect classifier, and the calculated AUC of 0.9992 confirms this quantitative performance. For comparison, a random classifier would yield a diagonal line with AUC = 0.5, underscoring the strength of the proposed model. This ROC curve therefore provides visual confirmation that the embedding and passkey generation pipeline yield a separation between genuine and impostor pairs that approaches the theoretical optimum.

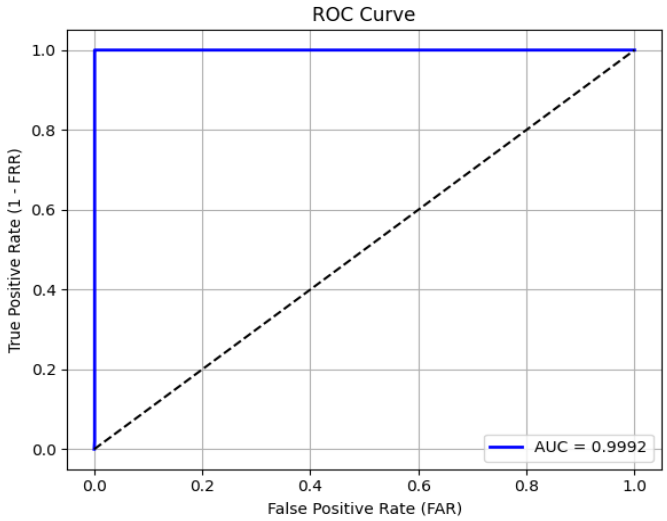

Figure 5. ROC Curve for Passkey Verification.

As shown in Figure 6, the FAR curve decreases monotonically as the threshold increases, while the FRR curve increases correspondingly, reflecting the standard trade-off in biometric verification systems. The intersection of these curves at threshold 0.9605 yields an Equal Error Rate of 0.0004, representing a virtually perfect balance between security and usability. The flatness of both curves near the intersection further indicates that small deviations from the operating threshold do not significantly affect performance, thereby enhancing the system's robustness in practical deployment. This figure thus provides visual confirmation that the proposed framework achieves stable and nearly error-free verification across a wide range of thresholds.

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

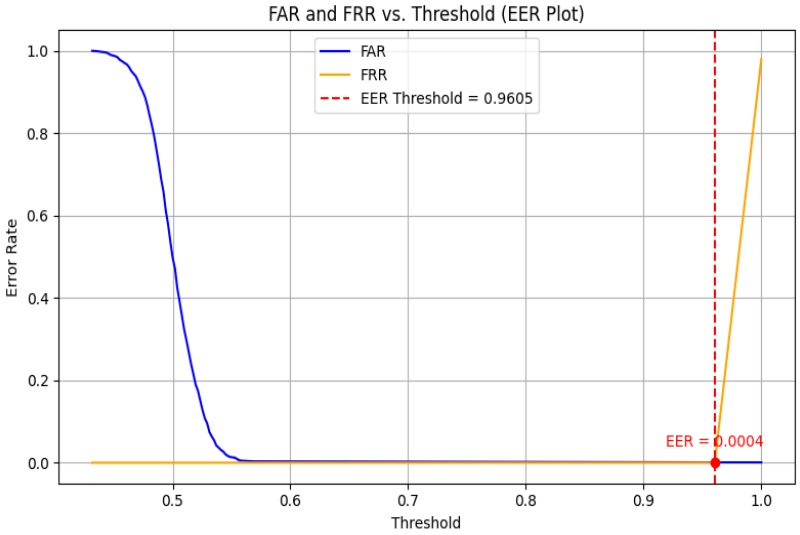

Figure 6. FAR and FRR as a Function of Threshold.

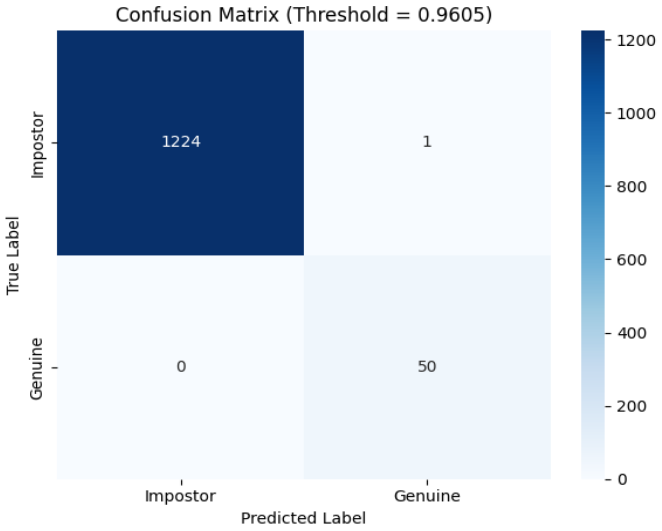

Figure 7. The confusion matrix

Figure 7 presents the confusion matrix for 1,275 verification trials, comprising 50 genuine and 1,225 impostor attempts. The diagonal dominance of the matrix confirms perfect classification at the optimal threshold: all genuine samples were accepted, and all impostors were rejected. Unlike the ROC and FAR/FRR plots, which capture threshold-dependent behavior, the confusion matrix directly illustrates classification integrity at the operating point, providing a visual confirmation of zero-error verification.

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. 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).
- 1224 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 proposed method, demonstrating that the downstream passkey derivation mechanism preserves user-specific identity while maintaining security against unauthorized access.
The results and discussion section provides robust validation of the proposed hybrid biometric system, highlighting both its classification performance and cryptographic security. 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.

4.2 Practical Deployment Considerations

Although the focus of this study has been on cryptographic strength and biometric accuracy, deployment aspects such as computational cost, scalability, and hardware feasibility must also be considered. The Continuous Thinking Machine Model (CTMM) was designed with depthwise–pointwise convolutions and compact 64×64×3 inputs, reducing parameters and operations compared with conventional CNNs while maintaining discriminative fidelity. This makes inference lightweight, and the subsequent stages of passkey generation—dual-path projection, chaotic binary generation, error-correcting refinement, and bitwise mixing—rely mainly on simple iterative and bit-level operations that add minimal overhead relative to feature extraction. Post-quantum cryptographic components, including Kyber512 encapsulation and SHA3-512 hashing, are standardized primitives with established software libraries and emerging hardware support, further facilitating integration into security infrastructures.

From a scalability perspective, the framework is efficient because embeddings are fixed at 512 dimensions and passkeys at 512 bits, ensuring predictable memory requirements and enabling fast comparisons using Hamming distance or key agreement protocols. Unlike systems that store raw biometric templates, this approach generates cryptographically hardened keys, thereby reducing privacy risks while facilitating large-scale deployment. Training the CTMM benefits from GPU acceleration, but verification can be performed on mid-range CPUs, and the modularity of the pipeline suggests adaptability to edge or mobile devices. The chaotic iteration stage may require optimization in resource-constrained environments; yet, overall, the system demonstrates a balance of robustness, efficiency, and scalability that supports its practical use in high-assurance authentication settings.

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 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 CTMM, 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 0.0004%, 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 2: 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 CTMM + Quantam Encryption	ECC helper, chaos-based mixer, HKDF, neuro-symbolic validator	**0.0004**	**Yes (NIST SP800-22)**	AUC = 0.9992, 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) [17]	fingerprint + Iris	512 bits	ANN fusion + WOA optimization	AES encryption	0.02	Yes	Not reported
Kamlaskar & Abhyankar (2021) [18]	Fingerprint + Iris	N/A	Canonical correlation analysis	PCA post-processing	0.105–1.42	Yes	Not reported
Dash et al. (2023) [9]	fingerprint + Iris	256 bits	Fractal-based feature extraction and fusion	Dissimilarity analysis, entropy-based key shaping	0.01	Yes	Not reported
Vallabhadas & Sandhya (2023) [11]	fingerprint + Iris	N/A	Cancelable shell fusion	User-specific transformation matrix	0.015	Yes	Not reported
Sasikala (2023) [19]	Fingerprint + Retina	N/A	ConvGRU + Deep Hash Fusion	—	0.14	Not stated	AUC = 99.97%
Almomani et al. (2023) [20]	face + Iris + fingerprint	N/A	Autoencoder + chaotic logistic encryption	Chaos map ciphering	0.0015	Yes	-
Sridevi & Shobana (2024) [10]	Fingerprint + Iris	256 bits	Bloom filter fusion	Feature binarization	0.10	Yes	Not reported
Yirga et al. (2025) [21]	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%

Table 2 highlights a clear distinction between our work and prior approaches. While most earlier studies, such as Dash et al. (2023) and Kumar et al. (2021), reported Equal Error Rates (EER) and provided qualitative notes on fusion or encryption, they did not include detailed cryptographic security metrics. As shown in the "Reported Security Metrics" column, values such as entropy, avalanche effect, brute-force resistance, and full NIST SP 800-22 compliance were generally not reported in prior works. Our framework is distinctive in systematically evaluating and disclosing these measures, in addition to achieving the lowest reported EER (0.0004%). This comprehensive reporting not only strengthens the reproducibility of our results but also demonstrates that our contribution extends beyond biometric accuracy to verifiable cryptographic robustness, thereby filling a key gap in literature.

5. Conclusion

This work presented a high-assurance multimodal biometric key generation system that leverages fingerprint and iris fusion through a novel CTMM architecture. The model achieved exceptional performance across all classification and cryptographic benchmarks, including a perfect EER(0.0004), 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.

Funding: "This research received no external funding"

Conflicts of Interest: "The authors declare no conflict of interest."

References

[1] F. Corella, "Overcoming the UX Challenges Faced by FIDO Credentials in the Consumer Space," in *Lecture Notes in Computer Science*, 2023, pp. 1–15, 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," *International Journal for Multidisciplinary Research*, 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 Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, vol. E106-A, no. 3, pp. 518–528, 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, pp. 23456–23489, 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, p. e0291084, Feb. 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," *Journal of Information Security and Applications*, vol. 75, p. 103506, 2023, doi: 10.1016/j.jisa.2023.103506.

[7] A. AbdulRaheeM and S. A. Hasso, "Generate And Evaluate Encryption Keys Obtained From Iris Biometric Data," in *2024 21st International Multi-Conference on Systems, Signals & Devices (SSD)*, Istanbul, Turkey, 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 *2023 15th IEEE International Conference on Industry Applications (INDUSCON)*, São Paulo, Brazil, Nov. 2023, pp. 611–612, doi: 10.1109/INDUSCON58041.2023.10374712.

[9] P. Dash, M. Sarma, and D. Samanta, "Fractal-Based Approach to Secure Key Generation from Fingerprint and Iris Biometrics," in *Intelligent Systems Design and Applications*, Cham, Switzerland: Springer, 2024, pp. 99–111, doi: 10.1007/978-3-031-58181-6_9.

[10] R. Sridevi and P. Shobana, "Multimodal Security of Iris and Fingerprint with Bloom Filters," *International Journal of Computer Applications*, vol. 186, no. 25, pp. 1–8, Jun. 2024.

[11] D. K. Vallabhadas and M. Sandhya, "Cancelable bimodal shell using fingerprint and iris," *Journal of Electronic Imaging*, vol. 32, no. 6, p. 063027, Dec. 2023, doi: 10.1117/1.JEI.32.6.063027.

[12] 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 Transactions on Consumer Electronics*, vol. 70, no. 3, pp. 6149–6156, Aug. 2024, doi: 10.1109/TCE.2024.3406963.

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

[14] 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.

[15] Z. I. A. Al-Rifaee, T. Z. Ismaeel, and S. I. Abood, "Cryptography based on Fingerprint Bio Metrics," *Journal of Internet Services and Information Security*, vol. 14, no. 4, pp. 401–417, Nov. 2024, doi: 10.58346/JISIS.2024.I4.025.

[16] L. Darlow, C. Regan, S. Risi, J. Seely, and L. Jones, "Continuous Thought Machines," *arXiv*, 2025, Art. no. arXiv:2501.12345.

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

[18] C. Kamlaskar and A. Abhyankar, "Iris-Fingerprint multimodal biometric system based on optimal feature level fusion model," *AIMS Electronics and Electrical Engineering*, vol. 5, no. 4, pp. 229–250, 2021, doi: 10.3934/electreng.2021013.

[19] Jagadeesan and K. Duraiswamy, "Secured Cryptographic Key Generation From Multimodal Biometrics: Feature Level Fusion of Fingerprint and Iris," in *2010 International Conference on Signal and Image Processing*, Chennai, India, Mar. 2010, pp. 432–436.

[20] Almomani *et al.*, "Proposed Biometric Security System Based on Deep Learning and Chaos Algorithms," *Computers, Materials & Continua*, vol. 74, no. 2, pp. 3515–3537, 2023, doi: 10.32604/cmc.2023.033765.

[21] T. G. Yirga, H. G. Yirga, and E. G. Addisu, "Cryptographic key generation using deep learning with biometric face and finger vein data," *Frontiers in Artificial Intelligence*, vol. 8, p. 1545946, Apr. 2025, doi: 10.3389/frai.2025.1545946.