Article

Dual Chaotic Diffusion Framework for Multimodal Biometric Security Using Qi Hyperchaotic System

Tresor Lisungu Oteko * and Kingsley A. Ogudo

Posted Date: 22 May 2025

doi: 10.20944/preprints202505.1756.v1

Keywords: biometric security; template protection; Qi hyperchaotic map; multi-modal biometrics; image encryption; facial recognition; iris recognition

Article

Dual Chaotic Diffusion Framework for Multimodal Biometric Security using Qi Hyperchaotic System

Tresor Lisungu Oteko * and Kingsley Ogudo

University of Johannesburg, department of Electrical and Electronics Engineering

* Correspondence: lisungu.tresor1@gmail.com

Abstract: The proliferation of biometric authentication systems across critical domains such as financial services, healthcare, security, law enforcement, and border control necessitate robust protection mechanisms for sensitive biometric data. This paper introduces a novel dual-layer cryptographic framework leveraging four-dimensional Qi hyperchaotic dynamics for securing face and iris biometric templates. The proposed system's cryptographic foundation demonstrates exceptional randomness properties, validated through comprehensive NIST Statistical Test Suite analysis, achieving statistical significance across all 15 NIST tests suite with p-values consistently above the 0.01 threshold across all test categories. Our architecture implements a distinctive two-tier encryption mechanism, where each layer independently utilizes the Qi hyperchaotic map to generate unique encryption parameters, ensuring template-specific encryption patterns that significantly enhance resistance against chosen-plaintext attacks. Implementation and testing were conducted using MATLAB software. Rigorous security analysis reveals outstanding cryptographic metrics: entropy values exceeding 7.99 bits, an expansive key space of 10^{320}, negligible correlation coefficients ($< 10^{-2}$), and robust differential attack resistance with Number of Pixels Change Rate (NPCR) of 99.6% and Unified Average Changing Intensity (UACI) of 33.45%. Empirical evaluation conducted on standard CASIA face and iris databases demonstrates practical computational efficiency, achieving average encryption times of 0.630551 seconds per template for 252x252 images size. The framework's superior plaintext sensitivity, coupled with its comprehensive resistance to various cryptographic attacks, positions it as a viable solution for high-security biometric applications. Our findings contribute to the advancement of biometric template protection methodologies, offering a balanced approach between security robustness and operational efficiency in real-world deployment scenarios.

Keywords: biometric security; template protection; Qi hyperchaotic map; multi-modal biometrics; image encryption; facial recognition; iris recognition

1. Introduction

Biometric systems, which emerged in the early 1960s with the first semi-automated face recognition system and fingerprint verification in the 1970s, represent a significant advancement in biometric authentication technology. These solutions exploit intrinsic physiological or behavioral attributes of individuals for identification and verification purposes. The field gained substantial momentum in the 1990s with the development of more sophisticated algorithms and improved sensor technologies, leading to widespread adoption across various sectors contemporary biometric systems offer several distinct advantages over traditional authentication methods such as passwords, PINs, or ID cards. Unlike knowledge-based authentication (passwords) or token-based systems (ID cards) that can be forgotten, stolen, or shared, biometric traits are inherently linked to an individual, providing stronger binding between the authenticator and the person's true identity. Moreover, biometric characteristics cannot be easily transferred between individuals and generally require the physical presence of the person being authenticated, significantly enhancing security against impersonation attacks.

The applications of biometric systems have expanded significantly, now encompassing law enforcement, border control, healthcare, financial services, and consumer electronics. For instance, smartphones increasingly incorporate fingerprint and facial recognition for device unlock and payment authorization, while governments employ biometric passports and national ID systems for enhanced security. In healthcare, biometric systems ensure accurate patient identification and secure access to medical records, while financial institutions utilize them for secure transactions and fraud prevention. However, despite these advantages, biometric systems face unique challenges, including privacy concerns, template security, and the irrevocability of biometric traits[1,2]. Unlike passwords that can be changed if compromised, biometric characteristics are permanent and cannot be reset, necessitating robust security measures for template protection and storage. These challenges have driven continuous innovation in the field, leading to the development of more sophisticated multimodal systems and advanced security frameworks.

The remainder of this paper is structured as follows: Section 2 provides a comprehensive review of extant literature, examining the inherent vulnerabilities in both unimodal and multimodal biometric systems, while emphasizing the pivotal role of cryptographic security in enhancing system robustness. Section 3 delineates the methodological framework, focusing on the analytical characterization of Qi Hyperchaotic systems and their application in encryption-decryption protocols. Section 4 presents empirical findings, including comparative analyses against state-of-the-art algorithms and offers a fair discussion of the results, while in Section 6, we present conclusive insights and directions for future research endeavors.

2. Related Works

In this section, we briefly introduced a short literature survey on the related biometric security works. The landscape of biometric authentication systems presents complex security challenges that demand sophisticated solutions. This review examines the evolution, challenges, and emerging solutions in multimodal biometric security, with particular emphasis on the integration of cryptographic techniques and advanced security frameworks. Biometric authentication systems face vulnerabilities at four critical junctures that fundamentally impact their security architecture: sensor-level susceptibility to presentation attacks utilizing synthetic biometrics, data transmission vulnerability between system components, template database exposure to unauthorized access, and decision module vulnerability to result falsification [1,2]. Building upon the aforementioned elements, we can categorize the attacks on biometric authentication systems into two major classifications: unauthorized acquisition of raw biometric data and malicious attempts to manipulate the templates databases. To mitigate these vulnerabilities, robust cryptographic mechanisms must be integrated into the biometric system architecture, ensuring protection against both biometric data falsification and stored templates tampering. The complexity of these challenges necessitates comprehensive security measures to maintain system integrity while ensuring practical usability in real-world applications.

The vulnerability of biometric systems to presentation attacks represents a particularly significant challenge in authentication security. Contemporary research demonstrates that sensor-level susceptibility to synthetic biometric presentations can fundamentally compromise system integrity, especially when sophisticated counterfeit characteristics circumvent traditional detection mechanisms [1,3,4]. This vulnerability becomes more pronounced when attackers possess detailed knowledge of system architecture, enabling them to exploit inherent limitations in distinguishing between genuine and fraudulent or fake biometric presentations.

Contemporary unimodal biometric authentication systems, despite their recent development, demonstrate significant vulnerabilities to sophisticated spoofing attacks. Modern attackers have developed techniques to generate false positive authentications, fundamentally compromising these systems' accuracy and reliability in user verification, thus undermining the core integrity of the authentication mechanism. A fundamental question that one might ask is how vulnerable are biometric systems to fake biometric information, and how is it accomplished? A targeted review of recent literature examines the scope and implications of biometric spoofing techniques.

For example, facial recognition systems and fingerprint authentication mechanisms exhibit significant vulnerabilities to presentation attacks (spoofing). While numerous scholars have advanced liveness detection protocols to mitigate face-based spoofing threats [3–5], the susceptibility of fingerprint biometric systems to artificial reproductions remains a pressing concern [6–9]. This vulnerability has catalyzed extensive research into countermeasure development, particularly focusing on the detection, identification, and prevention of synthetic fingerprint attacks [6,9,10]. The proliferation of these security challenges underscores the critical importance of robust anti-spoofing mechanisms in biometric authentication systems.

Although iris patterns offer unique identification markers independent of genetic factors, making them among the most reliable biometric identifiers, they remain susceptible to spoofing attacks. Recent research has explored various methodologies for both detecting and counterfeiting iris biometrics during authentication procedures. Notable contributions include Saranya et al. (2016) [9] who developed an Image Quality Assessment (IQA) framework to enhance biometric security systems, particularly for iris and fingerprint verification. Building on this foundation, He et al. (2008) [10] integrated Fast Fourier Transform (FFT) analysis with IQA techniques to detect fake iris data. Their research specifically addressed photographic and printed iris replicas, employing IQA to filter low-quality forgeries while utilizing Fourier frequency patterns to detect sophisticated fake iris samples.

In response to the inherent limitations of unimodal biometric systems, multimodal biometric authentication has emerged as a sophisticated countermeasure. These systems integrate multiple biometric modalities—either heterogeneous (combining different biometric traits) or homogeneous (utilizing multiple instances of the same trait, such as bilateral iris patterns or multiple fingerprints). The integration of multiple modalities substantially elevates the system’s security threshold, as it necessitates the successful spoofing of multiple independent biometric traits simultaneously. Recent scholarly work has demonstrated that this architectural approach significantly mitigates the vulnerabilities inherent in single-modal systems while enhancing authentication robustness [11–15].

A novel authentication mechanism leveraging multiple biometric traits—face, eye region, and iris patterns—was introduced in [16]. The researchers successfully adapted the OSIRIS v4.1 segmentation framework for smartphone implementation, with experimental validation confirming its viability on Android smart devices.

Smartphone-based recognition solutions incorporating face, iris, and periocular characteristics have achieved Equal Error Rates (EER) of 0.68% [14], demonstrating the potential for highly accurate multimodal authentication. Similarly, Research by Raj G et al. [17] introduced a comprehensive biometric authentication system that synthesizes three distinct modalities - facial features, iris patterns, and palm vein characteristics. Their implementation in banking environments demonstrated heightened security measures while yielding improved identification precision. These advancements highlight the practical viability of multimodal approaches in real-world applications. However, research has shown that even multimodal systems are not impervious to sophisticated attacks, particularly when attackers can simultaneously compromise multiple biometric modalities [18,19].

Research by Rodrigues et al. [18] explored vulnerabilities in dual-trait authentication systems combining facial recognition and fingerprint analysis. Their investigation across four distinct attack scenarios revealed that even combined biometric measures remain susceptible to sophisticated spoofing attempts. These findings highlight the necessity of integrating cryptographic protocols with multi-factor biometric systems to achieve comprehensive security.

The security and data protection paradigm represents a fundamental consideration in biometric solution architectures. While multimodal biometric systems inherently incorporate security enhancement through their multifaceted nature, the implementation of robust cryptographic frameworks becomes imperative to fortify these systems against presentation attacks and ensure data privacy preservation. The system's capability to discriminate between genuine and fraudulent or fake biometric presentations is particularly crucial, given that contemporary spoofing methodologies can produce highly convincing synthetic biometric artifacts [11,12]. The rising frequency of cyberattacks has accelerated the adoption of biometric security measures, offering enhanced protection for enterprises and individuals in today's digital ecosystem. The integration of cryptographic techniques with multimodal biometric systems has emerged as a crucial development in enhancing security frameworks.

Researchers have proposed various approaches to secure biometric data both at rest and in transit. Notable among these is the implementation of DNA QR coding combined with face and fingerprint authentication, achieving detection performance rates of 98.58% while significantly enhancing resistance to identity compromise attempts [44]. This approach demonstrates the potential for innovative security solutions that combine traditional biometric methods with advanced cryptographic techniques.

The fundamental challenges in biometric security extend beyond mere technical vulnerabilities. The intrinsic nature of biometric data presents unique privacy and security considerations that traditional authentication methods do not encounter [32,33]. Unlike passwords or security tokens, biometric characteristics cannot be revoked or replaced if compromised, creating a permanent security vulnerability. This irrevocability of biometric data necessitates exceptionally robust protection mechanisms from the outset of system design and implementation.

Contemporary research has identified multiple attack vectors that must be addressed in comprehensive security solutions. These include presentation attacks at the sensor level, replay attacks utilizing previously captured legitimate signals, feature extraction compromise, and template storage attacks [34]. Each of these vulnerability points requires specific security measures, leading to the development of layered security approaches that combine multiple protection mechanisms. However, they have overlooked the practicability of the multistage encryption in real-work applications.

In their research, [20] A. Rahik and C. Priya developed an integrated authentication framework combining DNA QR encoding with EXOR operations, utilizing DNA sequences as cryptographic keys. This system incorporates facial and fingerprint biometrics for enhanced cybersecurity. Their novel fusion methodology achieved 98.58% accuracy while strengthening defenses against identity theft.

In [21], Eid and Mohamed developed a multimodal biometric system integrating iris and facial recognition, secured through 2D Henon chaotic mapping. Their approach implemented encryption at three critical stages: pre-feature extraction, pre-matching, and database storage. The combination of Henon and 2D Logistic maps provided efficient encryption, while fuzzy logic fusion of face and iris matching scores achieved a FAR of 0.0345% and FRR of 0.001%.

Singh K et al. in [22] developed a multimodal biometric framework for cloud security, integrating steganographic and cryptographic techniques in a triple-authentication system. Their approach enables secure smartphone-based file operations while mitigating unauthorized access risks

Arulalan et al. in [23] proposed a multi-modal biometric encryption framework, integrating palmprint and fingerprint characteristics to generate 256-bit cryptographic keys for document security. The system's strength lies in leveraging physiological traits, making key prediction computationally infeasible for adversaries. While their empirical validation demonstrated system effectiveness, the research notably omitted crucial randomness assessments of the biometric-derived bit sequences through standardized testing protocols such as FIPS or NIST suites.

Yagiz S. et al. in [24] propose a biometrics-based cryptography scheme for E-Health systems that has two main components: Biometrics-based Fuzzy Authentication and Key Negotiation (BFAKN) for secure authentication and key exchange between system components, and Fingerprint-based Authority Access Mechanism (FAAM) for managing access control and data permissions. The key particularity is that it leverages biological signals and fingerprint biometrics to establish secure communications and granular access control within E-Health systems, achieving high security (99.6% impostor rejection) while maintaining usability for legitimate users (93.5% acceptance rate).

The work in [25] introduced a cryptographic system combining facial and iris biometrics, utilizing dual chaos mechanics through 2G Logistic Sine-coupling and Tent Logic Cosine maps. Their adaptive approach implements six rotation diffusion techniques that vary based on input images, enhancing resistance to plaintext attacks. The system demonstrated robust security metrics with entropy exceeding 7.99, NPCR >99.6%, and UACI >33.4%.

3. Theoretical Framework

3.1.4. D Qi Hyperchaos Map

The Qi hyperchaotic system, initially formulated by authors in [26], exhibits remarkable dynamical complexity characterized by two substantial positive Lyapunov exponents ($l_1 \approx 13.46$ and $l_2 \approx 3.48$), demonstrating exceptional ergodicity and sensitive dependence on initial conditions. This intrinsic characteristic establishes the system's superior randomness properties and makes it particularly suitable for cryptographic applications. The system's high-dimensional nature, coupled with its multiple control parameters (a, b, c, d, e, f), provides an extensive key space of approximately 10^{140} significantly enhancing its cryptographic robustness against brute-force attacks[27]. The mathematical model of this four-dimensional dynamical system, which serves as our pseudo-random number generator, is expressed by the following coupled differential equations $Eq.(1)$:

$$\dot{x} = a(y - x) + yz,$$

$$\dot{y} = b(y + x) - xz,$$

$$\dot{z} = -cz - ew + xy,$$

$$\dot{w} = -dw + fz + xy. (1)$$

where (x, y, z, w) represent the state variables, and (a, b, c, d, e, f) are the control parameters that determine the system's dynamical behavior. The system demonstrates hyperchaotic characteristics when $a, b \in R: (a, b)|\ 50 \le a \le 555; 20 \le b \le 26, c = 13,\ d = 8,\ e = 33\ and\ f = 30$ producing complex, aperiodic trajectories with exponential divergence in multiple directions of the phase space as depicted in Figure 1.

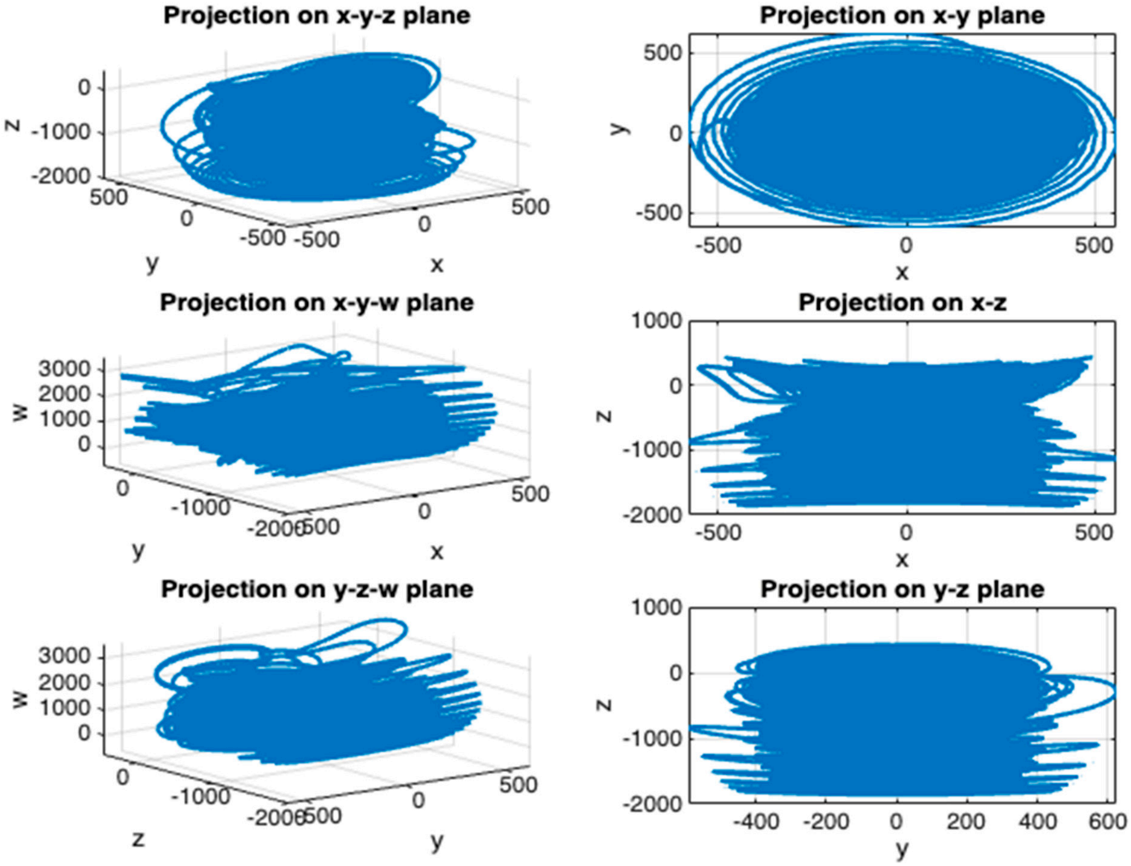

Figure 1. Qi Hyperchaos attractors.

3.2. Key Generation and Binary Sequence transformation

The encryption framework utilizes Qi hyperchaotic dynamics to produce entropy-rich random sequences. These undergo binary conversion, generating cryptographic keys for securing facial and iris biometric templates. The key $\mathrm{k_i}$, derived through quantization of chaotic outputs per Eq. (2), exhibits robust statistical characteristics, including uniformity and randomness.

$$\mathrm{k_i} = \mathrm{dec2bin}\left(\mathrm{mod}\left(\mathrm{Abs}\left(10^8 \mathrm{x_1(i)}\right), 256\right)\right) \quad (2)$$

where $x_1(i)$ represents the pseudorandom number generated from Qi Hyperchaos system and $i = 1,2,3,4 \ldots \ldots, n$. n represents the key length. The transformed bit sequences exhibit robust statistical characteristics, validated through NIST randomness tests (see Figure 6). We validated the algorithm's pseudo-random number generation capabilities through comprehensive testing using the NIST Statistical Test Suite. The results, detailed in Section 4.1, demonstrate that the generator passed all test categories with p-values consistently above the 0.01 significance threshold, confirming its statistical randomness

3.3. A Novel Secure Biometric Protection Framework

This research addresses biometric authentication vulnerabilities through an innovative cryptographic framework. Our approach transforms conventional template storage by implementing homomorphic encryption for biometric data protection. The system converts biometric features into secure ciphertext while maintaining essential discriminative properties for authentication, preventing template reconstruction and presentation attacks.

The security architecture leverages a multimodal approach, combining facial and dual iris recognition with a two-tier encryption mechanism based on 4D Qi hyperchaotic mapping. This integration of multiple biometrics enhances system reliability through redundancy and cross-validation protocols. The hyperchaotic encryption introduces high-dimensional complexity, creating unpredictable pixel distributions that significantly increase computational resistance to brute force attacks.

The enrollment process depicted in Figure 2 captures facial and dual iris data, processes the inputs, and extracts distinct feature templates. These templates undergo encryption using Qi Hyperchaos-generated bit streams before secure database storage, ensuring robust template protection through non-linear cryptographic transformations

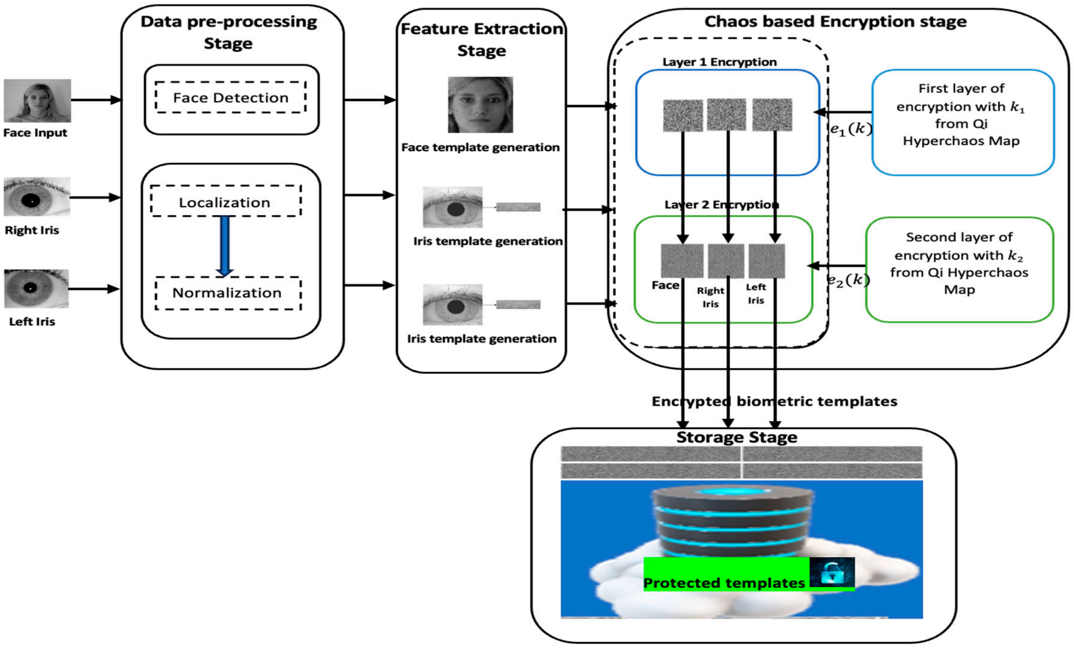

Figure 2. Multimodal Biometric enrollment framework.

Figure 3. depicts a secure biometric verification framework where incoming biometric data undergoes data pre-processing followed by feature extraction to generate comparison-ready templates. These newly generated templates are then matched against decrypted versions of previously stored encrypted templates from the database. This architecture maintains security by storing only encrypted templates in the database, decrypting them only during the verification process. The cryptographic protocols employed for template protection are elaborated in Section 3.4.

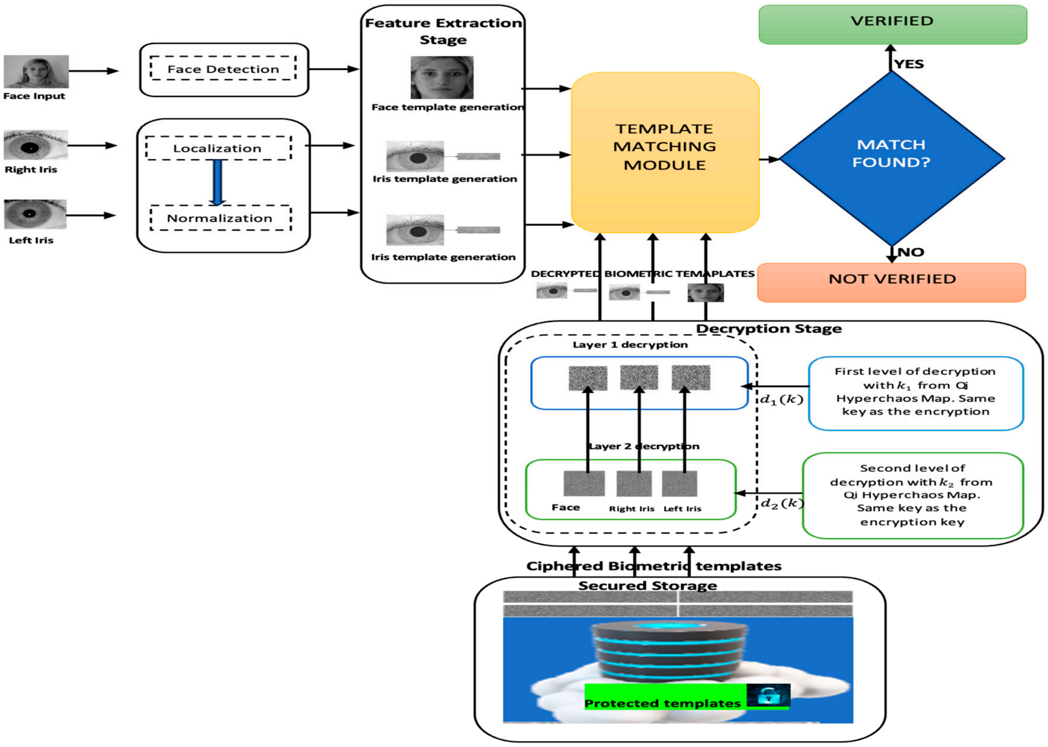

Figure 3. Biometric Verification framework.

3.4. Encryption Algorithm

The proposed scheme introduces an enhanced cryptographic architecture for biometric template protection, leveraging a sophisticated dual-encryption protocol based on 4D Hyperchaotic dynamics. The security framework implements a two-phase encryption methodology, where initially extracted biometric features undergo primary encryption using keys generated from the Qi Hyperchaotic framework (Eq. 1). Prior to cryptographic operations, both the key sequences and biometric data are transformed into standardized binary formats of equivalent length to facilitate precise encryption procedures. The primary security phase employs an XOR transformation between the standardized Qi Hyperchaotic sequence and the digitized biometric data, generating an intermediate protected template. This intermediate result undergoes secondary encryption through another XOR operation, utilizing an independent key sequence derived from the Qi Hyperchaotic system. The resulting dual-encrypted template is subsequently preserved in a secured repository, establishing a robust defense mechanism against unauthorized database manipulation and security breaches. This multi-layered cryptographic approach substantially reinforces the integrity of stored biometric data. The peusecode for the proposed encryprion algorithm is shown in Algorithm 1.

Algorithm 1: Encryption algorithm pseudocode

```
Input: Read the extracted biometric image, Bin_I of size M × N pixels
    1. System Initialization
        Define Qi system parameters for key1: $a_1, b_1, c_1, d_1, e_1, f_1$
        Define Qi system parameters for key2: $a_2, b_2, c_2, d_2, e_2, f_2$
        Define initial conditions for key1: $x_{10}, y_{10}, z_{10}, w_{10}$
    Define initial conditions for key2: $x_{20}, y_{20}, z_{20}, w_{20}$
    2. Calculate total number of pixels, $L = M \times N$
    3. Key Generation Process Generate $key1$ sequence:
        $for\ l = 1\ to\ L$
    $x_1[l\,] = a_1(y^1[l-1]) + b_1(w_1[l-1]) + c_1$
            $y_1[l] = d_1(x_1[l-1]) + e_1(z_1[l-1]) + f_1$
            $z_1[l] = x_1[l-1]y_1[l-1] - w_1[l-1]$
            $w_1[l] = z_1[l-1] + x_1[l-1]w_1[l-1]$
            $key1[l] = round\big(mod(abs(x_1[l]) * 10^8, 256)\big)$
        $end$
    4. Key Generation Process Generate $key2$ sequence:
                        $for\ l = 1\ to\ L$
    $x_2[l] = a_2(y_2[l-1]) + b_2(w_2[l-1]) + c_2$
            $y_2[l] = d_2(x_2[l-1]) + e_2(z_2[l][l-1]) + f_2$
            $z_2[l] = x_2[l-1]y_2[l-1] - w_2[l-1]$
            $w_2[l] = z_2[l-1] + x_2[l-1]w_2[l-1]$
          $key2[n] = round\big(mod(abs(y_2[l]) * 10^8, 256)\big)$
     $end$
    5. Reshape keys to match image dimensions
        $key1 = reshape(key1, [M, N])$
  $key2 = reshape(key2, [M, N])$
    6. First Encryption Layer
        $C1 = zeros(M, N)$
            $for\ m = 1\ to\ M$
                $for\ n = 1\ to\ N$
                    $C1[m, n] = XOR(Bin\_I[m, n], key1[m, n])$
                          $\boldsymbol{end}$
                        $\boldsymbol{end}$
    7. Second Encryption Layer
        $C2 = zeros(M, N)$
            $for\ m = 1\ to\ M$
                $for\ n = 1\ to\ N$
                    $C2[m, n] = XOR(C1[m, n], key2[m, n])$
                $end$
            $end$
    8. Output: Encrypted image $C2$ of size $M \times N$
```

As evidenced in Figure 4, the visual analysis presents unprocessed biometric images alongside their corresponding cryptographic transformations at First and Second encryption layers. The resultant encoded matrices manifest as stochastic distributions, effectively nullifying any characteristic patterns inherent to the source data. This transformation demonstrates the system's efficacy in achieving comprehensive visual obfuscation.

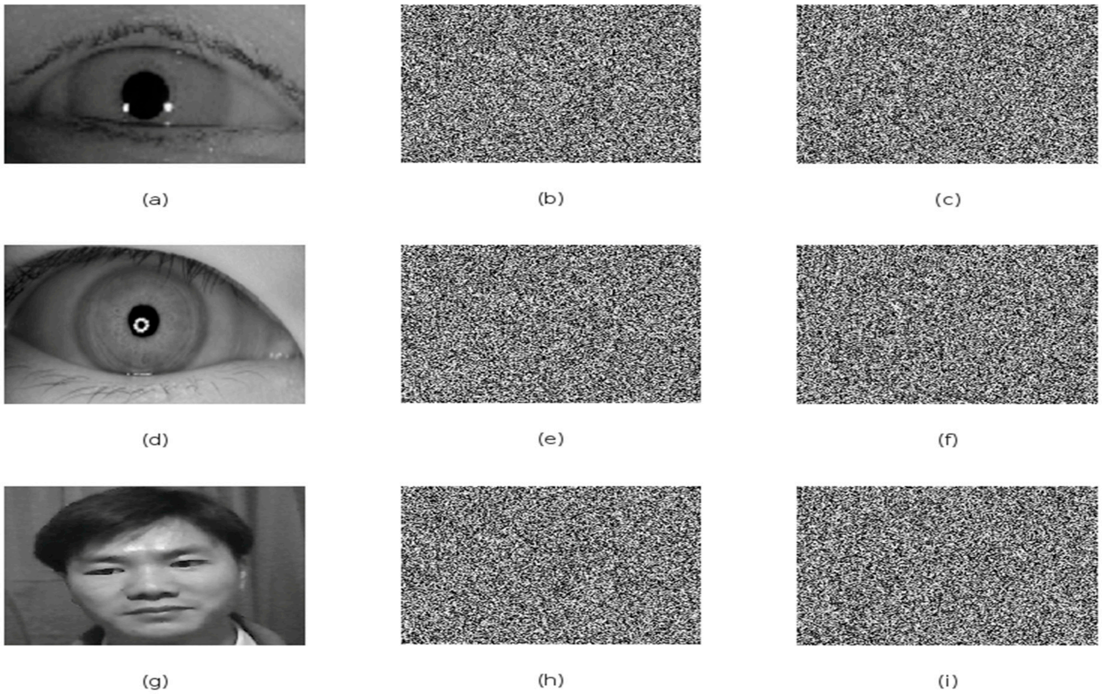

Figure 4. Biometric encryption stages for Left Iris, Right Iris, and Face images. (a)(d)(g) Original plaintext images; (b)(e)(h) First-layer encryption results using key1; (c)(f)(i) Second-layer encryption results using key2.

3.5. Decryption Algorithm

The decryption process depicted in Figure 5 recovers the original biometric template through a two-layer decryption mechanism utilizing the 4D Hyperchaotic map. The process begins with retrieving the encrypted biometric template from the database. The first stage of decryption uses the second set of keys used during the encryption, generated by Qi Hyperchaos in Eq. (1), performing an XOR operation with the encrypted template. The output from this initial decryption becomes the input for the second decryption stage. In this stage, another XOR operation is executed using the first set of keys (also generated by Qi Hyperchaos), where both the keys and intermediate decrypt result are in binary format of matching sizes. This dual-layer decryption process effectively reverses the encryption sequence, ultimately revealing the original biometric template. The successful decryption relies on using identical initial conditions and parameters from the Qi Hyperchaotic system that were used during encryption. The peusecode for the proposed decryprion algorithm is shown in Algorithm 2.

Algortihm2: Decryption algorithm pseudocode

```
Input: $Read\ the\ encrypted\ biometric, C2$
    1. Use the exact same keys with the same parameters and initial conditions as in
       Algortihm1: $key1$ and $key2$
    2. Reshape keys to match image dimensions
           $key1 = reshape(key1, [M, N])$
           $key2 = reshape(key2, [M, N])$
    3. First Decryption Layer (Reverse Second Encryption)
           $C1 = zeros(M, N)$
           $for\ m = 1\ to\ M$
               $for\ n = 1\ to\ N$
                   $C1[m, n] = XOR(C2[m, n], key2[m, n])$
               $end$
           $end$
    4. Second Decryption Layer
           $Bin\_I = zeros(M, N)$
           $for\ m = 1\ to\ M$
               $for\ n = 1\ to\ N$
                   $Bin\_I[m, n] = XOR(C1[m, n], key1[m, n])$
               $end$
           $end$
    5. Output: Decrypted image $Bin\_I$ of size $M \times N$
```

As illustrated in Figure 5, the encrypted biometric images were successfully restored to their original form through the application of identical cryptographic keys used in the encryption process, demonstrating the algorithm's symmetry.

doi:10.20944/preprints202505.1756.v1

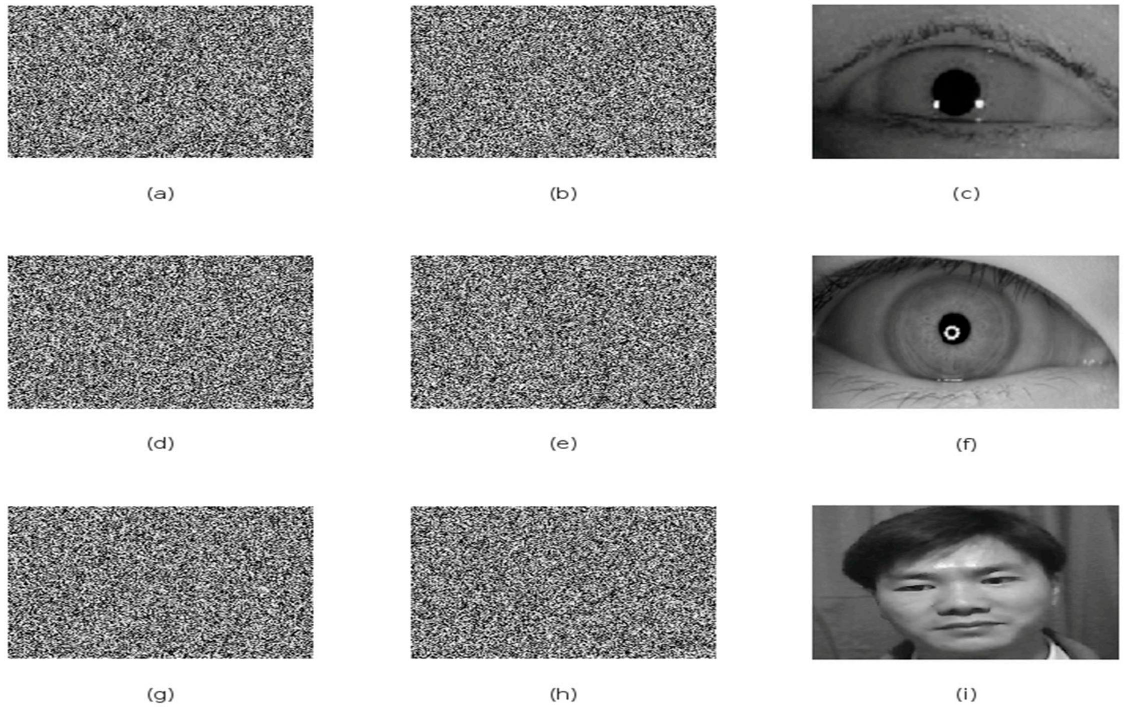

Figure 5. Two-layer decryption process using encryption-corresponding keys: (a)(d)(g) Second-layer encrypted images; (b)(e)(h) First-layer decryption results using key2; (c)(f)(i) Complete decryption results using key1.

4. Experimental and Performance Analysis

4.1. Qi Hyperchaos Randomness test

A chaotic map must generate highly random sequences to ensure unpredictability and sensitivity to initial conditions, which are crucial for robust cryptographic systems[27–29]. However, many chaotic maps suffer from periodic behavior, limited key space, or non-uniform distribution, creating vulnerabilities in cryptographic applications[30]. The National Institute of Standards and Technology (NIST) Statistical Test Suite addresses these concerns by providing 15 statistical tests that evaluate various aspects of randomness, including frequency patterns, runs, entropy, and complexity measures. The suite helps detect deviations from truly random behavior by analyzing binary sequences and producing P-values for each test, where values above 0.01 indicate sufficient randomness[31,32]. A chaotic map must pass all these tests to be considered cryptographically secure, ensuring no statistical patterns can be exploited by attackers. While traditional chaotic maps like logistic and tent maps often fail several NIST tests due to their inherent limitations, multi-dimensional hyperchaotic systems, hybrid chaotic maps or enhanced chaotic systems are designed to overcome these shortcomings by combining multiple maps or incorporating additional randomization techniques[27,33–35].

Figure 6. presents a comprehensive flow diagram depicting the NIST statistical test suite implementation for evaluating the randomness properties of the 4D Qi hyperchaotic map employed in our proposed algorithm. The statistical analysis results, summarized in Table 1, demonstrate that the bit sequences generated by the Qi hyperchaotic system satisfy the NIST criteria for randomness with P-values exceeding the standard threshold of 0.01. These findings substantiate that the generated sequences possess sufficient entropy and statistical randomness properties, rendering them suitable for deployment in robust cryptographic applications.

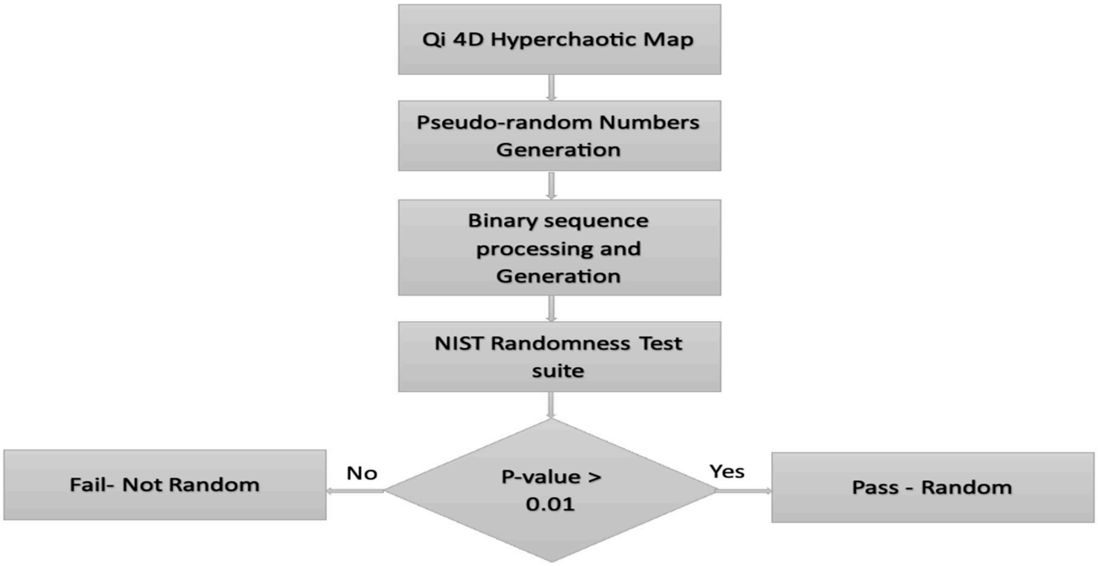
Qi 4D Hyperchaotic Map
Pseudo-random Numbers Generation
Binary sequence processing and Generation
NIST Randomness Test suite
P-value > 0.01
No
Yes
Fail- Not Random
Pass - Random

Figure 6. Framework for Randomness Evaluation.

Table 1. NIST 800-22 Test Results for Qi Hyoerchaos System.

Test Name	$P - value_{Qi\_Key1}$	$P - value_{Qi\_Key2}$	Result
Frequency (Monobit) Test	0.0375	0.8103	Pass - Random
Block Frequency Test	0.7509	0.3084	Pass - Random
Runs Test	0.7632	0.4023	Pass - Random
Longest Run of Ones in a Block Test	0.4252	0.0215	Pass - Random
Binary Matrix Rank Test	0.6883	0.5895	Pass - Random
Discrete Fourier Transform (Spectral) Test	0.5318	0.7420	Pass - Random
Non-overlapping Template Matching Test	0.4654	0.8026	Pass - Random
Overlapping Template Matching Test	0.6917	0.9102	Pass - Random
Maurer’s Universal Statistical Test	0.4965	0.5782	Pass - Random
Linear Complexity Test	0.8346	0.7831	Pass - Random
Serial Test	0.0491	0.1749	Pass - Random
Approximate Entropy Test	0.9704	0.1690	Pass - Random
Cumulative Sums (Cusum) Test	0.9998	0.1045	Pass - Random
Random Excursions Test	0.9992	0.0916	Pass - Random
Random Excursions Variant Test	0.9985	0.8342	Pass - Random

4.2. Key Space Analysis

Key Space Analysis in chaotic cryptography evaluates the possible combinations of system parameters and initial conditions that generate valid chaotic behavior. While theoretical key space encompasses all parameter values within defined ranges, effective key space considers only parameter combinations yielding genuine chaos, verified through positive Lyapunov exponents. Security standards require an effective key space exceeding 2^{100} to prevent brute-force attacks, with high sensitivity to parameter perturbations. This analysis is fundamental for ensuring cryptographic security and system viability [27,35,36].

doi:10.20944/preprints202505.1756.v1

In our implementation, the final encryption represents the composite product of the two encryption keys ($e_1(k)$, $e_2(k)$) employed in the successive encryption layers. Each key is characterized by four initial conditions ($x_{1e(k)}(0)$, $y_{1e(k)}(0)$, $z_{1e(k)}(0)$, $w_{1e(k)}(0)$) and six control parameters (a, b, c, d, e, f). Assuming a computational precision of 10^{16}, the key space magnitude, K_s, for our proposed dual-layer encryption algorithm can be expressed as :

$$\boldsymbol{K_s = 10^{16x(N_{ic}+N_p)}} \ \textbf{(3)}$$

where N_{ic} represents the total number of initial conditions and N_p denotes the total number of parameters. Given that the algorithm employs eight initial conditions and twelve parameters in total, the resultant key space is calculated as $10^{16\times20} = 10^{320}$. This value substantially exceeds the minimum-security threshold of 2^{100}, demonstrating the algorithm's robust resistance to brute-force cryptanalytic attacks. The proposed scheme demonstrates an expanded key space, suggesting enhanced cryptographic robustness. Comparative analysis with existing algorithms reveals superior key space dimensions in our proposed system, as shown in Table 2.

Table 2. Key Space performance Analysis.

Chaotic System	Precision	Number of parameter and Initial conditions	Key Space
Ours	10^{16}	20	10^{320}
Ref-[37]	10^{16}	8	10^{128}
Ref-[27]	10^{16}	10	10^{140}
Ref-[25]	10^{16}	5	10^{80}
Ref-[38]	10^{16}	14	10^{224}

4.3. Key Sensitivity Analysis

Key sensitivity analysis demonstrates that a minor alteration in the encryption key should result in a completely different ciphertext, even when encrypting the same plaintext. In our evaluation, we modified a single bit in the original key and performed encryption with both the original and modified keys, resulting in two distinct ciphertexts. Statistical comparison between these ciphertexts yielded a correlation coefficient near zero (approximately 0.0042) indicating that the proposed algorithm exhibits strong key sensitivity. This characteristic ensures that an adversary cannot derive meaningful relationships between ciphertexts even with minimal variations in encryption keys, thus confirming the algorithm's robustness against key-based attacks. Figure 8. illustrates the encrypted images generated using the original encryption keys $e_1(k)$ and $e_2(k)$, with initial conditions defined as follows: $x_{1e1(k)}(0) = -2.510$, $y_{1e1(k)}(0) = 11.3215$, of $z_{1e1(k)}(0) = -8$, of $w_{1e1(k)}(0) = -8.7$ and $x_{1e2(k)}(0) = -2.510$, $y_{1e2(k)}(0) = 11.3215$, of $z_{1e2(k)}(0) = -8$, of $w_{1e2(k)}(0) = -8.7$. To assess the system's sensitivity to initial conditions, the encryption keys were modified by introducing a perturbation of 10^{-15} while maintaining all other parameters constant. As depicted in Figure 7, a minimal perturbation in the initial conditions yielded significantly different encryption outcomes, with a statistical divergence of 99.227% between the images encrypted using the original and modified keys, thereby demonstrating the system's high sensitivity to initial conditions.

doi:10.20944/preprints202505.1756.v1

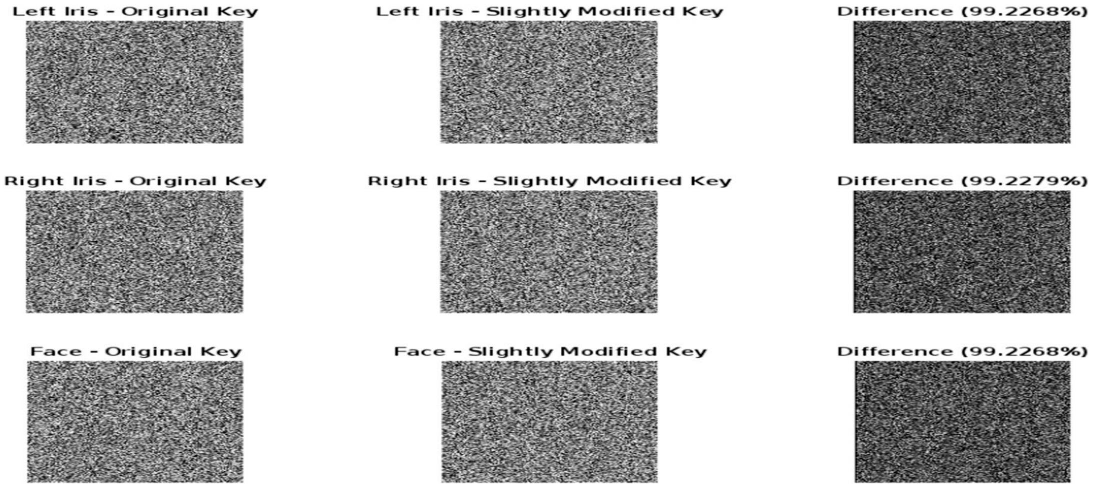
Left Iris - Original Key
Left Iris - Slightly Modified Key
Difference (99.2268%)
Right Iris - Original Key
Right Iris - Slightly Modified Key
Difference (99.2279%)
Face - Original Key
Face - Slightly Modified Key
Difference (99.2268%)

Figure 7. key sensitivity original key, slightly modified key 10^{-15} and the difference between the encrypted images with original and the modified ones.

4.4. Histogram Analysis

Histogram analysis serves as a fundamental statistical tool for evaluating the strength of encryption algorithms by examining the frequency distribution of pixel values or character occurrences in both plaintext and ciphertext. In secure encryption systems, the ciphertext histogram should demonstrate a uniform distribution, effectively masking the statistical patterns present in the original data[26,38]**.**

Significant deviations from uniformity may indicate statistical vulnerabilities that could be exploited through cryptanalysis techniques. This analysis provides quantifiable metrics for assessing the algorithm's resistance to statistical attacks and its effectiveness in achieving confusion and diffusion properties as defined by Shannon's principles of cryptography[35,39].

Figure 8 illustrates the frequency distribution histograms, depicting pixel intensity values of the original plaintext images and their corresponding first- and second-layer encrypted variants for the left iris, right iris, and facial biometric samples, respectively. The resultant histogram patterns demonstrate that the proposed dual-layer encryption algorithm effectively transforms the initial pixel distribution into a uniform distribution in the encrypted templates. This uniformity in pixel distribution indicates the algorithm's robust resistance to statistical attacks, as it eliminates discernible patterns between the plaintext and ciphertext, thereby enhancing the security of the encrypted biometric templates against cryptanalysis[26,34,40].

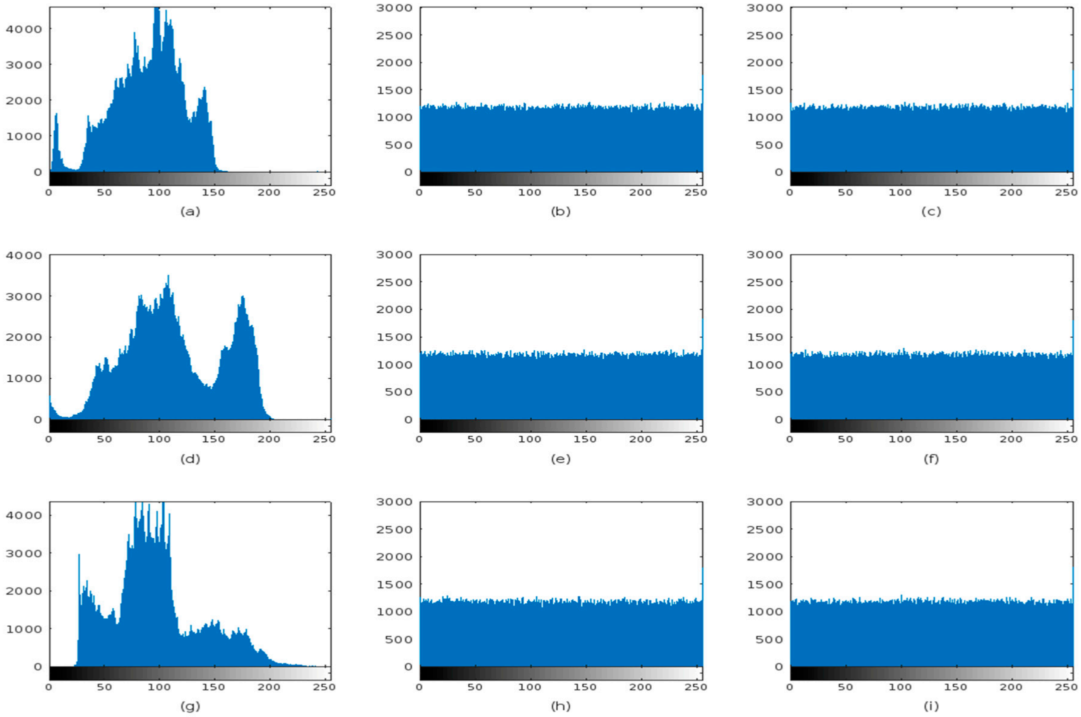

Figure 8. Histograms of Original Plaintext image, first layer encryption and second layer encryption for Left Iris, Right Iris and Face images respectively.

The decryption sequence illustrated in Figure 9 presents the progressive restoration stages, depicting the transformation from second-tier encryption through first-tier decryption, culminating in the retrieval of the original plaintext image. Comparative analysis of the histogram distributions between Figures 8 and 9 reveals consistent pixel intensity patterns, validating the successful reconstruction of the initial biometric data through the decryption protocol. This correlation in pixel distribution characteristics confirms the algorithm's ability to accurately reverse the encryption process, preserving the integrity of the biometric information.

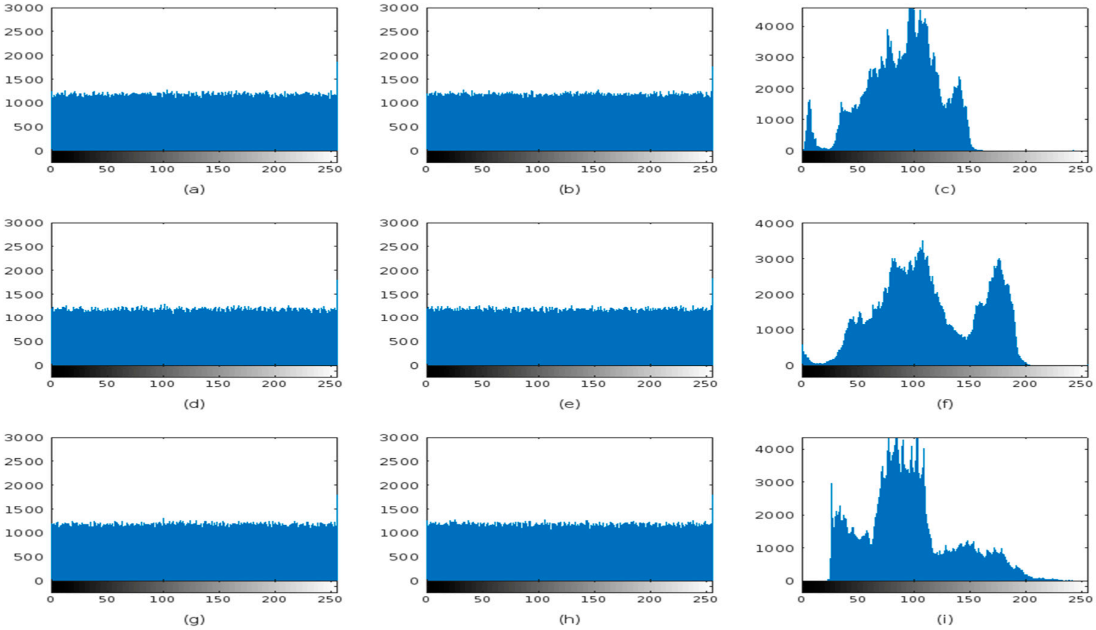

Figure 9. Decryption process using the same set of keys used for encryption process.

4.4. Pixels Correlation Analysis

The correlation coefficient (ϱ) serves as a crucial metric in evaluating the strength of encryption algorithms by measuring the statistical relationship between plaintext and its corresponding ciphertext. In a robust cryptographic system, the correlation coefficient should approach zero, indicating minimal statistical similarity between the original and encrypted data[42,43]. The correlation coefficient is expressed as:

$$\boldsymbol{\rho(x,y)} = \frac{\boldsymbol{N\sum_{j=1}^{N}(x_j * y_j) - \sum_{j}^{N} x_j \sum_{j}^{N} y_j}}{\boldsymbol{\sqrt{\left(N\sum_{j=1}^{N} {x_j}^2 - \left(\sum_{j=1}^{N} x_j\right)^2\right) * \left(N\sum_{j=1}^{N} {y_j}^2 - \left(\sum_{j=1}^{N} y_j\right)^2\right)}}} \quad \boldsymbol{(4)}$$

where x and y represent the gray-level intensity values of adjacent pixel pairs within the biometric image, where N represents the total quantity of image pixels selected for computational analysis. For an ideal encryption algorithm, ϱ ≈ 0 signifies that the relationship between plaintext and ciphertext is effectively random. Higher absolute values of ϱ (approaching ±1) may indicate potential vulnerabilities in the encryption scheme, as they suggest a detectable pattern between input and output data streams. This mathematical property is fundamental in cryptanalysis and serves as a quantitative measure of an algorithm's resistance to statistical attacks[27,35,37].

Figures 10, 11, and 12 present the pixel correlation analysis for left iris, right iris, and facial biometric images, respectively, examining adjacent pixel relationships across horizontal, vertical, and diagonal orientations. The analysis encompasses three sequential phases: (a) original plaintext images exhibiting strong intrinsic spatial correlations, (b) intermediate outputs following first-level encryption showing substantial decorrelation, and (c) final ciphertext aftersecond-level encryption demonstrating further randomization of pixel relationships. This progressive decorrelation validates the encryption algorithm's efficacy in disrupting the inherent spatial redundancy of biometric data.

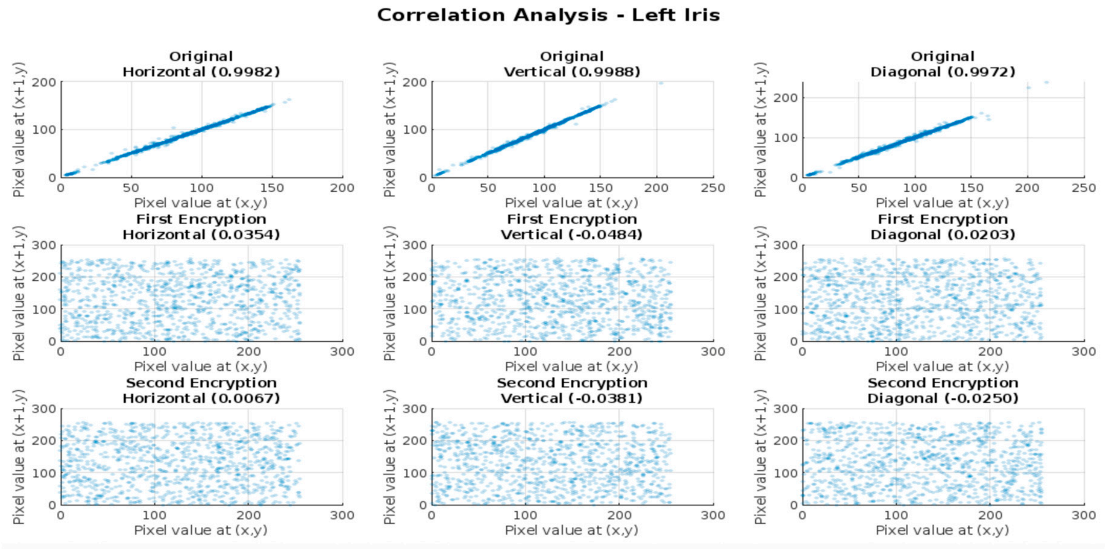

Figure 10. Adjacent pixel correlations in (a) original left iris image, (b) first-level encrypted image, and (c) second-level encrypted image, shown in horizontal, vertical, and diagonal directions.".

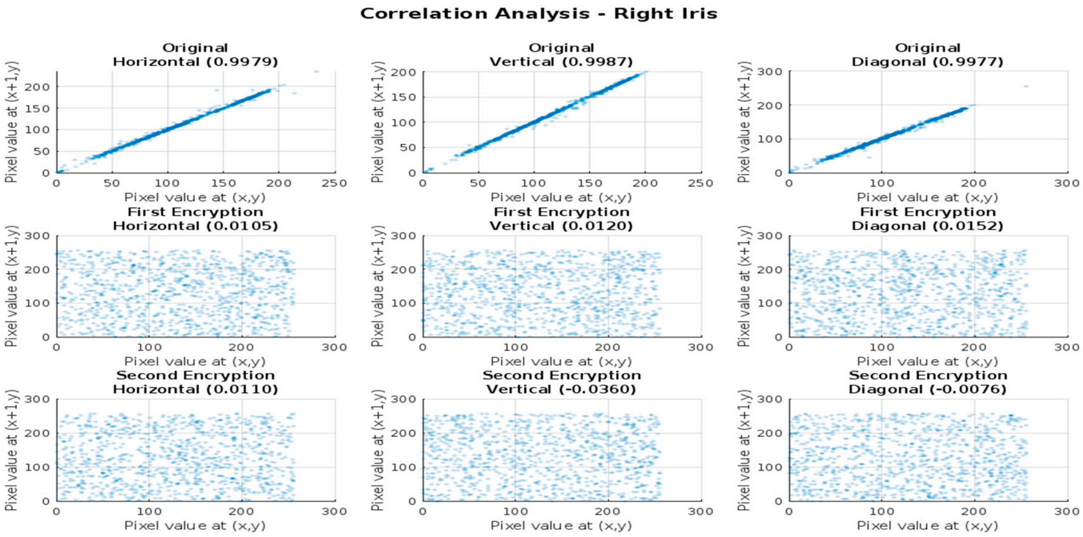

Figure 11. Adjacent pixel correlations in (a) First row - original Right iris image, (b)middle row - first-level encrypted image, and (c) bottom row - second-level encrypted image, shown in horizontal, vertical, and diagonal directions.

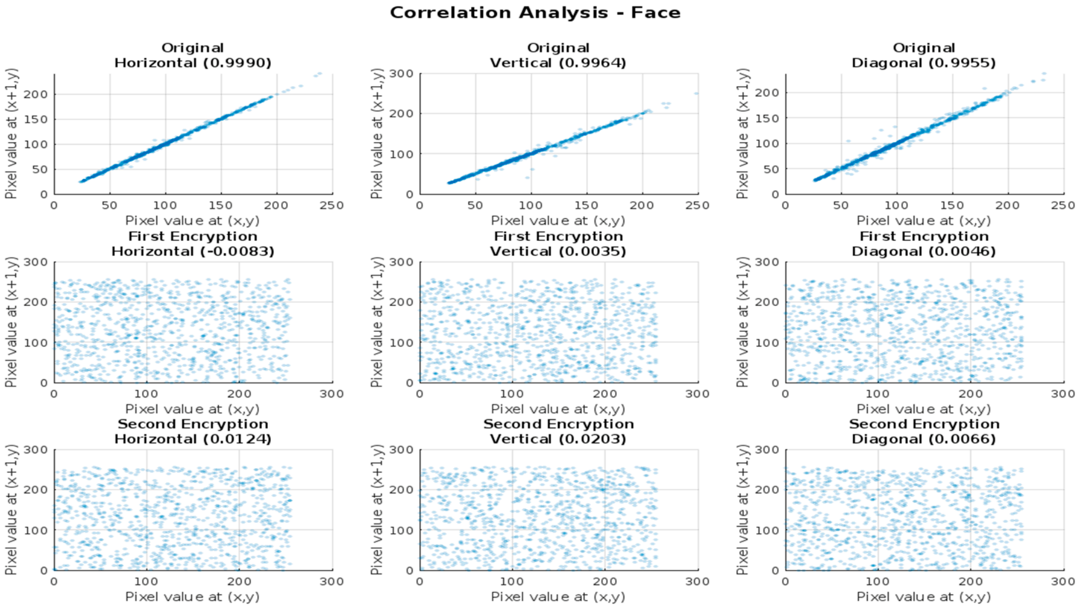

Figure 12. Adjacent pixel correlation distributions in horizontal, vertical, and diagonal directions for: Top row (a): Original face image; middle row (b): First-level encrypted image; bottom row (c): Second-level encrypted image. Correlations shown in horizontal, vertical, and diagonal directions.

As illustrated in Table 3, the correlation coefficient analysis shows the comparative performance between our proposed algorithm and existing state-of-the-art methodologies using lena image as reference. The simulation results indicate that our novel cryptosystem exhibits robust statistical properties, achieving correlation coefficients close to 0 that suggest strong resistance against statistical attacks. These findings validate the cryptographic strength of the proposed encryption scheme.

Table 3. Comparative Analysis of Adjacent Pixel Correlation Coefficients Across Three Directional Planes with Existing Cryptographic Schemes.

Chaotic System	Correlation Coefficients		
	Horizontal	**Vertical**	**Diagonal**
Ours	0.0072	0.0046	0.0063
Ref-[27]	0.0105	-0.0019	-0.0019
Ref-[37]	0.0206	0.0003	-0.0141
Ref-[38]	-0.0082	0.0073	0.0089
Ref-[44]	0.0003	0.0009	0.019
Ref-[45]	0.0011	0.0012	0.016
Ref-[46]	0.004	0.007	0.037

4.5. Information Entropy Analysis

Information Entropy Analysis quantifies the randomness and unpredictability of encrypted data through Shannon's entropy measure:

$$H(m) = -\sum_{i-=0}^{2^N-1} P\,(m_{\mathrm{i}}) log_2 P(m_{\mathrm{i}}) \; (5)$$

where m represents gray image, $P(m_{\mathrm{i}})$ represents the probability distribution of pixel values. For 8-bit grayscale images, the theoretical optimum of 8 bits indicates perfect uniformity in pixel distribution. Modern encryption algorithms must demonstrate entropy values approaching this theoretical maximum, signifying minimal information leakage and robust resistance to statistical attacks. The convergence of measured entropy to this theoretical bound, combined with uniform pixel distribution analysis, serves as a critical benchmark for evaluating the cryptographic strength and statistical independence of the encryption scheme. Table 4. presents a comparison of information entropy performance between our proposed method and existing algorithms. A value close to the ideal value of eight indicates that the system randomness is satisfactory and the proposed schemed has the capabilities to resist entropy-based attacks.

Table 4. Performance Analysis of Entropy of Encrypted with Lena Image by existing schemes.

Proposed	Ref-[27]	Ref-[37]	Ref-[42]	Ref-[47]	Ref-[48]	Ref-[49]
7.9988	7.9983	7.9998	7.9996	7.9993	7.9971	7.7795

Figure 13 presents the information entropy analysis across three stages our proposed system showing: original plaintext biometric images (blue), first-level encryption (orange), and second-level encryption (yellow) for Left iris, Right iris, and Face images. The entropy for first and second layer of encrypted biometric display satisfactory values close to the the idea value of 8, this indicate that our proposed cryptosystem is robust enough and can resit brute force attacks.

doi:10.20944/preprints202505.1756.v1

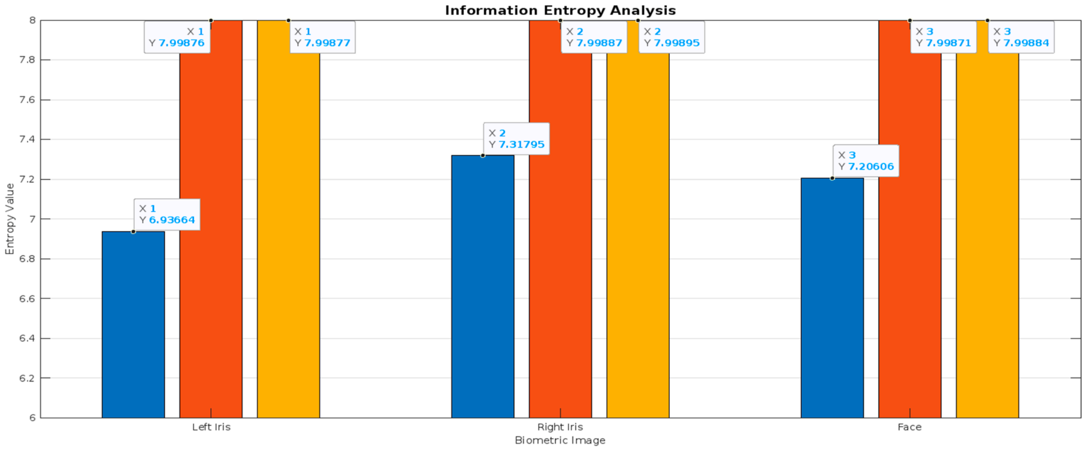

Figure 13. Information Entropy for Biometric Left Iris, Right Iris and Face, plaintext, Ciphertext level1 and Ciphertext level2.

4.6. Histogram Analysis I Cryptographic Assessment

NPCR and UACI serve as fundamental metrics for evaluating an encryption algorithm's resilience against differential attacks. NPCR quantifies the percentage change in pixel values between two encrypted images when their original images differ by a single pixel, with an ideal value approaching 99.6%[35,50,51]. Its mathematical formular is expressed as follows:

$$NPCR = \frac{\sum_{i,j} D(i,j)}{MXN} \times 100\% \; (6)$$

where $D(i,j)$ equals 0 if pixel values are identical and 1 if different, and $N \times M$ represents the image dimensions.

Complementing this, UACI measures the average intensity difference between two encrypted images, targeting an ideal value of around 33.4%.[46] It's calculated as:

$$UACI = \frac{1}{MXN}\left[\sum_{i,j} \frac{|C1(i,j) - C2(i,j)|}{255}\right] \times 100\% \; (7)$$

where $C1$ and $C2$ represent the encrypted images. Together, these metrics assess an algorithm's diffusion properties and its ability to resist chosen-plaintext attacks, with values closer to their theoretical ideals indicating stronger security characteristics in image encryption algorithms. Figure 14 illustrates the NPCR and UACI performance metrics for the first and second levels of encryption in the proposed algorithm, as applied to left iris, right iris, and facial biometric images.

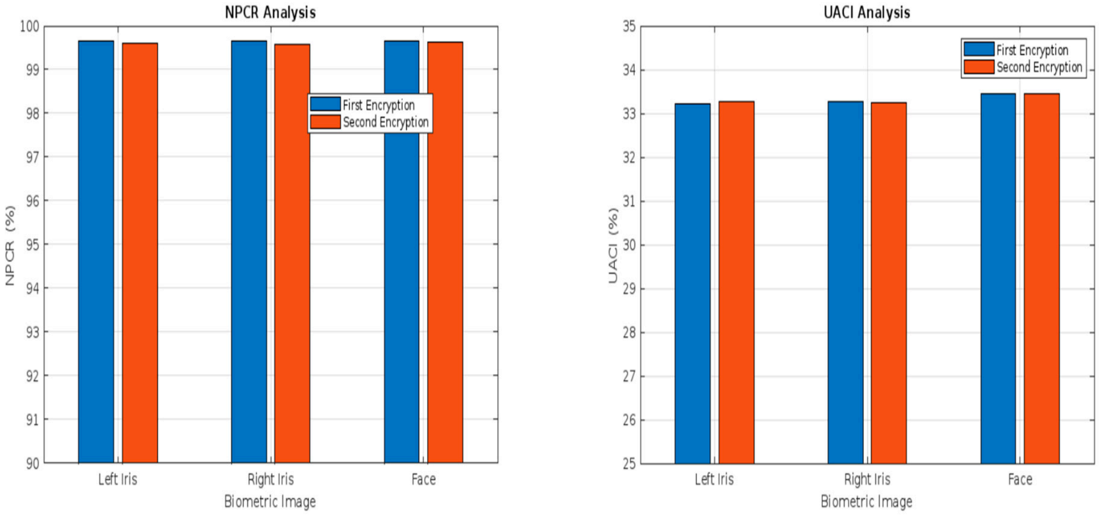

Figure 14. NPCR and UACI performance Analysis for Left iris, Right Iris and Face biometric images.

Table 5 presents a comparative analysis of NPCR and UACI performance between our proposed scheme and existing algorithms using Lena as the reference benchmark input. The results demonstrate that our proposed algorithm exhibits high sensitivity to slight pixel value changes in the original biometric image, thereby providing robust encryption against differential attacks. When compared with existing algorithms, our proposed scheme present equally satisfactory results while outperforming some existing schemes.

Table 5. NPCR and UACI performance and comparison with existing Methods using Lena image.

	Proposed	Ref-[25]	Ref-[27]	Ref-[37]	Ref-[44]	Ref-[45]	Ref-[47]	Ref-[49]	Ref-[52]
NPCR (%)	99.629	99.658	99.810	99.715	99.603	99.611	99.614	99.510	99.630
UACI (%)	33.441	33.459	33.400	33.511	33.692	33.692	33.466	33.160	33.480

4.8. Time Efficiency Analysis

The time efficiency of encryption algorithms is crucial in modern cryptographic systems, directly impacting their practical implementation and real-world performance. In resource-constrained environments and high-throughput scenarios, the computational complexity of encryption operations significantly affects system performance and resource utilization. Therefore, optimizing the balance between security strength and computational efficiency remains a fundamental consideration in cryptographic algorithm design[37,53]. For our proposed algorithm, we leveraged Matlab online to conduct our experimental simulations. Matlab online uses cloud-based environment with 1 Virtual CPU (vCPU) and 4GB RAM, 2.5GHz. The results demonstrate that the proposed scheme offers several advantages over existing algorithms. Table 6. illustrates the performance of encryption and decryption times across 512x512 and 256x256 image sizes.

Table 6. Comparison analysis of encryption time with existing algorithms with Lena image.

Algorithms	Image size	Encryption time in s	Decryption time in s
Ours	512x512	2.1439	2.1081
	256x256	0.61158	0.6094
Ref-[25]	512x512	2.727	2.708
	256x256	0.941	0.902
Ref-[37]	512x512	3.17	--
	256x256	1.23	--

Ref-[44]	512x512	0.5156	--
	256x256	0.1272	--
Ref-[45]	512x512	25.3077	--
	256x256	6.3849	--
Ref-[54]	512x512	16.43	--
	256x256	8.2	--
Ref-[55]	512x512	25.867	24.564
	256x256	6.494	6.471

5. Conclusions

This paper presented a novel dual-layer cryptographic framework for securing multimodal biometric templates using 4D Qi hyperchaotic dynamics. During identification and matching processes, the system employs a comprehensive traversal mechanism to navigate recognition codes and decrypt corresponding ciphertext data. This robust approach ensures the integrity and confidentiality of stored biometric information against unauthorized access, tampering, and destruction. The proposed double chaotic-based diffusion encryption method leverages dual chaos properties to enhance scrambling effectiveness, while plaintext-related control parameters govern the algorithm's diffusion dynamics, demonstrating strong resistance to selected plaintext attacks. The proposed system demonstrates superior performance across multiple security metrics compared to existing schemes. The algorithm achieved exceptional randomness properties, validated by comprehensive NIST testing with p-values consistently above 0.01 across all 15 NIST test categories. Security analysis revealed robust cryptographic metrics including entropy values exceeding 7.99 bits, correlation coefficients approaching zero ($<10^{-2}$), and strong differential attack resistance with NPCR of 99.6% and UACI of 33.45%. The expansive key space of 10^{320} significantly exceeds the minimum-security threshold of 2^{100}, providing robust resistance to brute-force attacks. Comparative analysis demonstrates that our approach outperforms some existing schemes in both security metrics and computational efficiency. This framework represents a significant advancement in biometric template protection, offering a balanced solution between security robustness and operational efficiency for practical deployment in high-security multimodal biometric applications. Future research directions will explore the implementation of multilayered encryption protocols across various authentication phases, extending beyond the current focus on template storage security. This comprehensive approach aims to enhance the biometric authentication system's robustness by integrating cryptographic mechanisms throughout the authentication pipeline, thereby addressing potential vulnerabilities in data transmission and processing stages.

References

1. S. K. Singla, M. Singh, and N. Kanwal, "Biometric system - Challenges and future trends," *Proceedings of the 2021 8th International Conference on Computing for Sustainable Global Development, INDIACom 2021*, pp. 647–651, 2021, doi: 10.1109/INDIACom51348.2021.00114.
2. "Security and Cryptographic Challenges for Authentication Based on Biometrics Data - cryptography-02-00039".
3. J. Yan, Z. Zhang, Z. Lei, D. Yi, and S. Z. Li, "Face liveness detection by exploring multiple scenic clues," *2012 12th International Conference on Control, Automation, Robotics and Vision, ICARCV 2012*, vol. 2012, no. December, pp. 188–193, 2012, doi: 10.1109/ICARCV.2012.6485156.
4. D. Gafurov, E. Snekkenes, and P. Bours, "Spoof attacks on gait authentication system," *IEEE Transactions on Information Forensics and Security*, vol. 2, no. 3, pp. 491–502, 2007, doi: 10.1109/TIFS.2007.902030.
5. Y. Kim, J. H. Yoo, and K. Choi, "A motion and similarity-based fake detection method for biometric face recognition systems," *IEEE Transactions on Consumer Electronics*, vol. 57, no. 2, pp. 756–762, 2011, doi: 10.1109/TCE.2011.5955219.
6. M. Espinoza, C. Champod, and P. Margot, "Vulnerabilities of fingerprint reader to fake fingerprints attacks," *Forensic Sci Int*, vol. 204, no. 1–3, pp. 41–49, 2011, doi: 10.1016/j.forsciint.2010.05.002.

7. R. Cappelli, A. Lumini, D. Maio, and D. Maltoni, “from Standard Templates,” *Analysis*, vol. 29, no. 9, pp. 1489–1503, 2007.
8. N. A. Kulkarni and L. J. Sankpal, “Efficient Approach Determination for Fake Biometric Detection,” *2017 International Conference on Computing, Communication, Control and Automation, ICCUBEA 2017*, pp. 1–4, 2018, doi: 10.1109/ICCUBEA.2017.8463715.
9. S. Saranya, S. Vinitha Sherline, and M. Maheswari, “Fake biometric detection using image quality assessment: Application to iris, fingerprint recognition,” *2016 2nd International Conference on Science Technology Engineering and Management, ICONSTEM 2016*, pp. 98–103, 2016, doi: 10.1109/ICONSTEM.2016.7560931.
10. X. He, Y. Lu, and P. Shi, “A fake iris detection method based on FFT and quality assessment,” *Proceedings of the 2008 Chinese Conference on Pattern Recognition, CCPR 2008*, pp. 316–319, 2008, doi: 10.1109/CCPR.2008.68.
11. B. Ammour, T. Bouden, and S. Amira-Biad, “Multimodal biometric identification system based on the face and iris,” *2017 5th International Conference on Electrical Engineering - Boumerdes, ICEE-B 2017*, vol. 2017-Janua, pp. 1–17, 2017, doi: 10.1109/ICEE-B.2017.8191981.
12. T. Barbu, A. Ciobanu, and M. Luca, “Multimodal biometric authentication based on voice, face and iris,” *2015 E-Health and Bioengineering Conference, EHB 2015*, pp. 19–22, 2016, doi: 10.1109/EHB.2015.7391373.
13. A. Tharwat, A. F. Ibrahim, and H. A. Ali, “Multimodal biometric authentication algorithm using ear and finger knuckle images,” *Proceedings - ICCES 2012: 2012 International Conference on Computer Engineering and Systems*, pp. 176–179, 2012, doi: 10.1109/ICCES.2012.6408507.
14. B. Ammour, T. Bouden, and L. Boubchir, “Face-Iris Multimodal Biometric System Based on Hybrid Level Fusion,” *2018 41st International Conference on Telecommunications and Signal Processing, TSP 2018*, pp. 298–302, 2018, doi: 10.1109/TSP.2018.8441279.
15. T. Ko, “Multimodal biometric identification for large user population using fingerprint, face and iris recognition,” *Proceedings - 34th Applied Image Pattern Recognition Workshop, AIPR 2005*, pp. 218–223, 2005, doi: 10.1109/AIPR.2005.35.
16. K. B. Raja, R. Raghavendra, M. Stokkenes, and C. Busch, “Multi-modal authentication system for smartphones using face, iris and periocular,” *Proceedings of 2015 International Conference on Biometrics, ICB 2015*, pp. 143–150, 2015, doi: 10.1109/ICB.2015.7139044.
17. R. Gusain, H. Jain, and S. Pratap, “Enhancing bank security system using Face Recognition, Iris Scanner and Palm Vein Technology,” *Proceedings - 2018 3rd International Conference On Internet of Things: Smart Innovation and Usages, IoT-SIU 2018*, no. 3, pp. 3–7, 2018, doi: 10.1109/IoT-SIU.2018.8519850.
18. R. N. Rodrigues, N. Kamat, and V. Govindaraju, “Evaluation of biometric spoofing in a multimodal system,” *IEEE 4th International Conference on Biometrics: Theory, Applications and Systems, BTAS 2010*, 2010, doi: 10.1109/BTAS.2010.5634531.
19. “Handbook of Multibiometrics,” *Handbook of Multibiometrics*, 2006, doi: 10.1007/0-387-33123-9.
20. A. Rashik and C. v Priya, “MULTI-BIOMETRIC RECOGNITION AND QR,” 2022.
21. M. M. Eid and M. A. Mohamed, “A secure multimodal authentication system based on chaos cryptography and fuzzy fusion of iris and face,” *ACCS/PEIT 2017 - 2017 Intl Conf on Advanced Control Circuits Systems and 2017 Intl Conf on New Paradigms in Electronics and Information Technology*, vol. 2018-Febru, pp. 163–171, 2018, doi: 10.1109/ACCS-PEIT.2017.8303037.
22. K. Singh, A. K. Sajnani, and S. Kumar Khatri, “Data Security Enhancement in Cloud Computing Using Multimodel Biometric System,” *Proceedings of the 3rd International Conference on Electronics and Communication and Aerospace Technology, ICECA 2019*, pp. 175–179, 2019, doi: 10.1109/ICECA.2019.8821976.
23. V. Arulalan, K. S. Joseph, and V. Premanand, “Securing Digital Data using 256-bit Multimodal Biometrics based Cryptographic Key,” 2016.
24. Yagiz Sutcu, Qiming Li, and Nasir Memon, “Secure Biometric TemplatesFrom Fingerprint-Face Features.”
25. “Biometric information security based on double chaotic rotating diffusion - 1-s2.0-S0960077923005155-main”.

26. G. Qi, M. A. van Wyk, B. J. van Wyk, and G. Chen, “On a new hyperchaotic system,” *Physics Letters, Section A: General, Atomic and Solid State Physics*, vol. 372, no. 2, pp. 124–136, Jan. 2008, doi: 10.1016/j.physleta.2007.10.082.
27. L. O. Tresor and M. Sumbwanyambe, “A selective image encryption scheme based on 2D DWT, henon map and 4D Qi hyper-chaos,” *IEEE Access*, vol. 7, pp. 103463–103472, 2019, doi: 10.1109/ACCESS.2019.2929244.
28. H. Zhu, Y. Zhao, and Y. Song, “2D Logistic-Modulated-Sine-Coupling-Logistic Chaotic Map for Image Encryption,” *IEEE Access*, vol. 7, pp. 14081–14098, 2019, doi: 10.1109/ACCESS.2019.2893538.
29. “A chaotic image encryption algorithm based on coupled piecewise sine map and sensitive diffusion structure - s11071-021-06576-z”.
30. P. K. RAJAN and H. C. REDDY, “Hyper chaos- laboratory experiment and numerical confirmation,” *IEEE Trans Circuits Syst*, vol. CAS-33, Nov. 1986.
31. A. Rukhin et al., “A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications Lawrence E Bassham III Special Publication 800-22 Revision 1a.”
32. T. O. Lisungu, “CHAOS BASED IMAGE CRYPTOGRAPHY SYSTEM USING DISCRETE WAVELET DECOMPOSITION,” 2019.
33. M. Jiang and H. Yang, “Image Encryption Using a New Hybrid Chaotic Map and Spiral Transformation,” 2023.
34. M. A. Al-Khasawneh, S. M. Shamsuddin, S. Hasan, and A. A. Bakar, “An Improved Chaotic Image Encryption Algorithm,” *2018 International Conference on Smart Computing and Electronic Enterprise, ICSCEE 2018*, pp. 1–8, 2018, doi: 10.1109/ICSCEE.2018.8538373.
35. T. Lisungu and M. Sumbwanyambe, “Image Compression-Encryption Scheme Based on 2D,” *2019 Southern African Universities Power Engineering Conference/Robotics and Mechatronics/Pattern Recognition Association of South Africa (SAUPEC/RobMech/PRASA)*, no. 1, pp. 177–182, 2019.
36. C. Zhu, G. Wang, and K. Sun, “Cryptanalysis and improvement on an image encryption algorithm design using a novel chaos based s-box,” *Symmetry (Basel)*, vol. 10, no. 9, Sep. 2018, doi: 10.3390/sym10090399.
37. JHARNA TAMANG et al., “Dynamical Properties of Ion-Acoustic Waves in Space Plasma and Its Application to Image Encryption,” Jan. 2020. doi: 10.1109/ACCESS.2021.3054250.
38. E. Inzunza-González and C. Cruz-Hernández, “Double Hyperchaotic Encryption for Security in Biometric Systems,” 2013.
39. NESTOR TSAFACK et al., “A New Chaotic Map With Dynamic Analysis and Encryption Application in Internet of Health Things,” Jul. 2020.
40. L. Liu, Z. Zhang, and R. Chen, “Cryptanalysis and Improvement in a Plaintext-Related Image Encryption Scheme Based on Hyper Chaos,” *IEEE Access*, vol. 7, pp. 126450–126463, 2019, doi: 10.1109/ACCESS.2019.2938181.
41. L. Liu, Z. Zhang, and R. Chen, “Cryptanalysis and Improvement in a Plaintext-Related Image Encryption Scheme Based on Hyper Chaos,” *IEEE Access*, vol. 7, pp. 126450–126463, 2019, doi: 10.1109/ACCESS.2019.2938181.
42. J. D. D. Nkapkop, J. Y. Effa, M. Borda, and R. Terebes, “A novel fast and secure chaos-based algorithm for image encryption,” in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, Springer Verlag, 2015, pp. 87–101. doi: 10.1007/978-3-319-27179-8_7.
43. Yong Wang, Kwok-Wo Wong, Xiaofeng Liao, and Guanrong Chen, “A new chaos-based fast image encryption algorithm,” *Appl Soft Comput*, vol. 11, pp. 514–522, Dec. 2009.
44. Moatsum Alawida, Je Sen Teh, Azman Samsudin, and Wafa’ Hamdan Alshoura, “An image encryption scheme based on hybridizing digital chaos and finite state machine - 1-s2.0-S0165168419302221-main,” Jun. 2019.
45. Zhongyun Hua and Yicong Zhou, “Image encryption using 2D Logistic-adjusted-Sine map,” *Inf Sci (N Y)*, vol. 339, pp. 237–253, Jan. 2016.
46. K. Gupta and S. Silakari, “New Approach for Fast Color Image Encryption Using Chaotic Map,” *Journal of Information Security*, vol. 02, no. 04, pp. 139–150, 2011, doi: 10.4236/jis.2011.24014.

doi:10.20944/preprints202505.1756.v1

47. “A fast and efficient multiple images encryption based on single-channel encryption and chaotic system - s11071-021-07192-7”.
48. X. Wang and Q. Wang, “A novel image encryption algorithm based on dynamic S-boxes constructed by chaos,” *Nonlinear Dyn*, vol. 75, no. 3, pp. 567–576, Feb. 2014, doi: 10.1007/s11071-013-1086-2.
49. Nalini M K and Dr. Radhika K R, “Encryption on Multimodal Biometric using HyperChaotic Method and Inherent Binding Technique,” vol. 12, Jul. 2021.
50. T. Nestor, N. J. De Dieu, K. Jacques, E. J. Yves, A. M. Iliyasu, and A. A. Abd El-Latif, “A multidimensional hyperjerk oscillator: Dynamics analysis, analogue and embedded systems implementation, and its application as a cryptosystem,” *Sensors (Switzerland)*, vol. 20, no. 1, Jan. 2020, doi: 10.3390/s20010083.
51. Z. Man et al., “A novel image encryption algorithm based on least squares generative adversarial network random number generator,” *Multimed Tools Appl*, vol. 80, no. 18, pp. 27445–27469, Jul. 2021, doi: 10.1007/s11042-021-10979-w.
52. M. Gupta, V. P. Singh, K. K. Gupta, and P. K. Shukla, “An efficient image encryption technique based on two-level security for internet of things,” *Multimed Tools Appl*, vol. 82, no. 4, pp. 5091–5111, Feb. 2023, doi: 10.1007/s11042-022-12169-8.
53. H. Bao, Z. Y. Hua, W. B. Liu, and B. C. Bao, “Discrete memristive neuron model and its interspike interval-encoded application in image encryption,” *Sci China Technol Sci*, vol. 64, no. 10, pp. 2281–2291, Oct. 2021, doi: 10.1007/s11431-021-1845-x.
54. K.C. Jithin and Syam Sankar, “Colour image encryption algorithm combining Arnold map, DNA sequence operation, and a Mandelbrot set,” Dec. 2019.
55. Kaiyun Ma, Teng Lin, Wang Xingyuan, and Meng Juan, “Color image encryption scheme based on the combination of the fisher-yates scrambling algorithm and chaos theory,” Apr. 2021

Disclaimer/Publisher’s Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.