CHAOS
Theory and Applications
in Applied Sciences and Engineering

e-ISSN: 2687-4539
RESEARCH ARTICLE
Vol.8 / No.2 / 2026 / pp.117-134
https://doi.org/10.51537/chaos.1900590

An Efficient Information Confidentiality Scheme Based on Genesio-Tesi Map and Deoxyribonucleic Acid Sequencing

Majid Khan [*,1] **and Iqra Ishaque** [α,2]

[*]Department of Mathematics, College of Science and Humanities in Alkharj, Prince Sattam Bin Abdulaziz University, Al-Kharj 11942, Saudi Arabia,
[α]Department of Applied Mathematics and Statistics, Institute of Space Technology, Islamabad, Pakistan.

ABSTRACT This study develops an advanced image encryption system which combines Deoxyribonucleic Acid (DNA) cryptography, chaotic behavior, and compressive sensing into multi-stage design. The approach differs from previous techniques in that it uses DNA encoding on chaotic sequences instead of encoding image pixel values directly. Thus, this method significantly increases the amount of confusion and diffusion effects produced by the overall technique. Additionally, the technique includes the use of a highly secure SHA-512 based key derivation system coupled with Blum Blum Shub randomization. These two mechanisms introduce several additional layers of high entropy randomness to the overall system and provide high sensitivity to variations in the plaintext. An analysis of the performance and statistics of the overall system shows that the system is more resistant to statistical attacks, differential attacks, and brute force attacks than other systems previously developed.

KEYWORDS
DNA cryptography
Compressive sensing
Chaotic systems
Image encryption
SHA-512

INTRODUCTION

The current era of advanced computing using intelligent technology, which is characterized by the creation, transmission, and storage of large amounts of sensitive data within interconnected computer systems, relies upon cryptography as its foundation for both trust and security. As a result of improvements in areas such as Artificial Intelligence (AI), Internet of Things (IoT) and Cloud Computing, the boundaries protecting the security of these systems are becoming increasingly permeable; thus, it is imperative to employ data encryption methods to protect confidentiality, ensure authenticity, and defend against cyber-attacks.

Cryptography enables secure real-time communication, private artificial intelligence (AI) computation and long-term data storage. Cryptography is therefore necessary for creating secure smart infrastructure. DNA-based cryptography offers an alternative approach using nucleotide bases to represent, encode, and compute digital information. It has the ability to operate in parallel; store large amounts of information per unit area; and create random elements. The application of DNA coding as an encoding system and chaos theory along with the use of additional cryptographic concepts make it a candidate for strong encryption in smart and future quantum resistant environments.

Modern encryption systems have evolved to provide high levels of protection against various types of cyber threats. As our reliance on automation continues to grow within both local and global infrastructures and systems, we require stronger measures than previously implemented to safeguard vast amounts of sensitive data. Because data can include anything from simple usernames to complex training data sets for AI applications, there exists a need for evolving encryption methodologies to remain one-step-ahead of present-day cyber threats and those that may exist in the future. Encryption also provides protection against theft, unauthorized access and malicious modification of AI models, training datasets, algorithms, and live outputs. In addition, advanced techniques such as homomorphic encryption and secure multiparty computation enable AI to learn and make decisions directly upon encrypted data. As the use of AI becomes increasingly prevalent, the ability to perform secure computations on sensitive data will be necessary for the development of ethical-AI applications that protect end-user privacy and enable the creation of autonomous, decentralized and trusted intelligent network architectures. With the emergence of smart technologies, encryption has moved beyond its traditional role of providing intermediate level security for sensitive data and now serves as a means to preserve the integrity of artificial intelligence (AI) models.

Additionally, innovative techniques such as homomorphic en-

Manuscript received: 1 March 2026,
Revised: 4 July 2026,
Accepted: 11 July 2026.

[1]mk.cfd1@gmail.com (**Corresponding author**)
[2]iiqra962@gmail.com

cryption and secure multi-party computation now provide the capability for AI systems to learn and generate decision-making output using sensitive data that remains encrypted at all times. These capabilities enable organizations to create ethical-AI applications that protect end-user privacy while facilitating the future of autonomous, decentralized and trusted intelligent networks. In addition to encrypting an images content through pixel shuffling, or scrambling, other encryption methods also utilize diffusion and confusion to protect against unauthorized viewing of the encrypted image. Although the previous methods have proven effective in protecting the privacy of large volumes of image data, they also provide several technical challenges. Image data, by nature, can be very voluminous and has a strong correlation with its neighboring pixels. As such, many standard cryptographic methods, which include Data Encryption Standard (DES) (NIST 1999), Advanced Encryption Standard (AES) (Rijmen and Daemen 2001), Triple DES (3-DES) (Barker and Mouha 2017), International Data Encryption Algorithm (IDEA) (Chang 2004), and others are specifically designed to handle textual data rather than images.

Therefore, when applying these common encryption methods to large amounts of multimedia data, they suffer from two major drawbacks; first, a higher amount of computation is required and second, they do not effectively hide the inherent statistical redundancy of the image pixels themselves. This issue has generated academic interest in developing new cryptosystems that will allow the efficient encryption/decryption of multimedia data in real-time. To help meet this challenge, researchers have developed and published several different types of multimedia encryption techniques using both DNA and Chaos Theory-based encryption techniques (Vidhya and Brindha 2020).

DNA cryptography is becoming a new field in which cryptography has emerged from the DNA computing area. In addition to being conducted as laboratory experiments (using biology), DNA computing research can also be conducted as simulated by computational and mathematical processes using pseudo-DNA. The use of DNA-based computers will possibly take over the role of today's computers, or alternatively there is some evidence suggesting that the most successful computer systems in the years ahead are those that combine both types of processing (Gearheart et al. 2010). Compressive sensing (CS) is a latest form of sampling (sample breaking), as per the Nyquist sampling theorem. Signals are able to be sampled at the same time. A method of CS has a structure similar to that of symmetric encryption in which the key is the measurement matrix (Li et al. 2017). An example of an image encrypting system was developed by Huang et al. (Huang et al. 2014). Zhen et al. (Li et al. 2021) developed a compressive sensing-based, plain text related, chaotic image encryption method.

There have been many methods of encryption described in literature that use chaos. Qayyum et al. (2020), for example, developed a method of encryption employing both dynamic substitution and chaos. In another study an image encryption scheme has been designed using compressed sensing along with a discrete hyperchaotic system. Also, Ponuma and Amutha (2018) employed a 1-D chaotic system to obtain an equilibrium matrix as well as to construct a chaotic sequence which was then used. Similarly, Chai et al. (2017) employed both compressive sensing and chaos. Furthermore, Yu et al. (2020) presented a similar scheme but used a chaotic measurement matrix mapping and a sequence generator. Wang et al. (2021), however, implemented a DNA coding algorithm combined with Fisher-Yates shuffling. Finally, Xu et al. (2020) similarly developed an encrypted scheme based upon 2-D slim; while Luo et al. (2019) similarly applied compressive sensing and similarly a similar encrypting scheme employing a hyper-chaotic map was used in (Gong et al. 2019).

The logistic-tent map was utilized in (Li et al. 2021), for both compressive sensing as well as chaos based encryption schemes. Gong et al. (2019) applied combination of compressive sensing and the RSA algorithm. Quantum genetic algorithm (QGA) utilizing a hyperchaotic map has also been developed by (Cheng et al. 2020) for compression based techniques. Another form of compression is the S-box based method which has been described in (Zhu et al. 2020). Cellular Neural Network (CNN)-based methods have also been described by Lin et al. (2018). A five dimensional (5D) chaotic system with cap-like trajectories based on a tangent hyperbolic memristive model, enhanced with fractional calculus for improved encryption performance is proposed in (Qureshi et al. 2024a). The methodology used by these researchers demonstrates strong aspects of security and chaotic behavior that are beneficial in application as an image encryption process. The authors Yan et al. (2023) have developed a new type of fractional-order (FO) 5-dimensional memristive chaotic system that demonstrates extreme multistability (EM), which improves the ability to be unpredictable or complex for use in encryption schemes. This FO 5-dimensional memristive chaotic FO system has been successfully implemented in image encryption and demonstrated to provide both high diffusion and confusion. A 3D chaotic system with a clown-face attractor using memristor based electronic systems, DNA encoding, and fractional calculus is presented in (Qureshi and Khan 2024b).

Recent algebraic-SPN encryption frameworks employ substitution–permutation network (SPN) constructions defined over algebraic residue domains such as Gaussian, quaternion, and Eisenstein integer rings (Alammari et al. 2025; Sajjad and Alqwaifly 2025; Sajjad et al. 2025). These schemes achieve confusion and diffusion primarily via algebraic substitutions and ring-based permutations that exploit ring arithmetic for structured mixing. By contrast, our method integrates three orthogonal mechanisms (i) continuous hyperchaotic dynamics (Genesio–Tesi) to produce high-entropy, parameter-sensitive pseudorandom sequences, (ii) DNA-style symbolic encodings applied to chaotic streams (not to pixels directly) to amplify diffusion via rule variability, and (iii) compressive sensing to reduce ciphertext bandwidth while preserving reconstruct ability.

Mathematically, SPN on residue rings is based on discrete algebraic transforms $x \mapsto \pi(x)$ inside finite rings $\mathbb{Z}[\iota]/\pi$ that produce deterministic, structure-preserving mixing, whereas our approach uses real-valued chaotic maps $s_{t+1} = F(s_t; p)$ whose Lyapunov spectrum and exponential divergence introduce continuous nonlinearity and statistical unpredictability prior to discrete DNA mapping. Practically, this leads to two main differences: (a) confusion–diffusion origin algebraic-SPN builds diffusion from multiple algebraic rounds with compact state representation, while our design achieves diffusion via chaotic sensitivity + per-block DNA rule variation, and (b) efficiency trade-off SPN schemes are often computationally compact for purely integer arithmetic, but they do not reduce ciphertext size; our hybrid scheme adds an explicit compression stage (measurement matrix Φ) so that encrypted payloads are smaller at comparable security metrics.

We provide an empirical comparison (Table 12) of the proposed DNA–chaos-compressive scheme against standard schemes of comparable diffusion ability and entropy. In this comparison, we show that the proposed DNA–chaos-compressive scheme provides reductions of 30–50% in the amount of space required to store its ciphertexts relative to these standard schemes with a mod-

erate increase in the time needed to perform decryption due to reconstruction using OMP on the part of the decryptor. Unlike the previous models within the family of DNA-chaos-compressive models, which utilized ring arithmetic as their means of generating uniformly distributed keys through deterministic operations, our DNA-chaos-compressive model generates high-quality keys through the use of chaotic dynamics and applies two methods of creating cryptographically strong encodings, namely symbolic encoding based upon the properties of DNA and compressive sensing. From a conceptual standpoint, the primary goal of all members of the family of DNA-chaos-compressive models is to create keys that are statistically uniform, have a high degree of nonlinearity and are sensitive to variations in their keys. However, unlike those models that utilize modular algebraic substitution to achieve such goals, the proposed model achieves them using analytical nonlinearity and sequence randomness.

We propose here an RGB image compression/encryption algorithm that utilizes Genesio–Tesi hyper chaos and compressive sensing techniques. For added protection against plaintext attacks we have taken 512-bits from a SHA-512 function as input. To further ensure no correlation exists among the pixels of the image, we use the Blum Blum Shub (BBS) scrambling algorithm. The approach developed here differs in that it uses DNA encoding on chaotic sequences rather than the raw pixels of images when compared to other recent frameworks (Cardona-López et al. 2024; Alghafis et al. 2021; Tariq et al. 2020; Waseem and Khan 2018; Xu et al. 2020; Rahul et al. 2023; Wen et al. 2024; Pourasad et al. 2021).

While Luo et al. (2023) discussed hyperchaotic maps to encrypt images, they did not include compressive sensing into their research, nor provide a more complete or efficient solution than what was provided in this paper. In (Chai et al. 2020a), an image encryption method utilizing DNA encoding is developed; however, our research combined both DNA encoding with chaos driven compressive sensing and therefore can be said to offer greater levels of security and efficiency. Additionally, our research includes a larger security evaluation framework to protect against both differential and statistical attacks.

Unlike many previously published studies (Wen et al. 2024; Pourasad et al. 2021; Rahul et al. 2023; Luo et al. 2023; Chai et al. 2020a) that apply DNA operations directly to image data, our scheme applies DNA encoding to chaotic sequences. Therefore, our approach offers improved encryption diffusion without generating redundancy through pixel-level operations. By integrating compressive sensing, chaos, and DNA at the structural level instead of the surface level, we develop a fundamentally new encryption model.

The motivation of the study: In an era of rapid digital advancement, secure image data transmission and storage have emerged as critical challenges in fields such as healthcare, military communications, and private data sharing. In addition to being highly secure from a theoretical standpoint, standard cryptographic primitives such as AES can have significant performance issues and be computationally expensive to operate on large image databases. Additionally, images contain redundant information (due to high pixel correlation) which makes images more vulnerable to statistical or differential attacks if a non-optimal cipher mode is used with traditional block ciphers. As a means of overcoming both the structural and performance shortcomings associated with current block ciphers, the present paper will describe an experimental hybrid encryption method that combines DNA encoding, chaotic system encodings, and compressive sensing. The primary purpose of this work is to create a scalable framework that is capable of achieving both high levels of security and high speed performance using compressive sensing to eliminate redundant data in images. The combination of chaotic systems providing high sensitivity based upon their initial conditions; DNA encoding complex diffusion; and compressive sensing to reduce the amount of data that needs to be encrypted, provide a comprehensive encryption approach that is suitable for real time applications. The final contribution of this study is to connect the two areas of performance and security so as to provide a secure cryptographic solution that can be applied to real world applications within demanding environments for image processing.

There is still a substantial gap of investigation in terms of comparison between algebraic (SPN) based and chaotic based encryption paradigms. Although recent number theoretic (Gaussian, quaternion and Eisenstein) ring based SPN schemes (Alammari et al. 2025; Sajjad and Alqwaifly 2025; Sajjad et al. 2025) have exhibited excellent results in terms of confusion-diffusion properties they are computationally expensive for larger scale images and also do not inherently provide any form of compression. On the other hand, although several chaos based DNA encryption algorithms show great randomness properties most of them map pixel level mapping into DNA sequences resulting in redundant information as well as increase in the size of the cipher-text. The proposed work therefore will utilize a hybrid approach that utilizes compressive sensing along with Genesio–Tesi hyperchaos to develop a compact encryption algorithm which has good security features. Compressive sensing provides sparse representation and dimensionality reduction and hence improves transmission efficiency whereas Genesio–Tesi hyperchaos systems contribute multiple dimensional hyperchaotic sequences having multiple positive Lyapunov exponents and hence increases key sensitivity and diffusion. Hence this hybrid approach fills the gaps existing among the above mentioned three approaches i.e. providing analytical nonlinearities, computational efficiency and establishes a new trade-off between theoretical analysis, randomness and feasibility for secure real time image communication.

Contribution of the study: Our study has made major enhancements and innovative contributions to prior studies in the area of image encryption using the methods of DNA coding, chaos and compressive sensing. The primary differences of our proposed system are as follows:

i. Compressive sensing (CS) along with DNA encoding and chaotic sequences have been used in order to improve both the effectiveness and performance of this encryption system.

ii. The use of DNA-based encoding of chaotic sequences provides increased unpredictability and complexity to generate the encryption process, making it very difficult to withstand a number of different types of attacks.

iii. By adding CS into the encryption process, we reduce redundant data and maintain high-quality reconstruction to make it suitable for real-time applications.

iv. A 384-bit key was generated from SHA-512 hashing function to provide extreme resistance to brute force attacks and overall improve security.

v. Statistical, differential and key-sensitivity tests were performed extensively to validate the robustness of our proposed method against all types of cryptanalysis attacks.

The remainder of the paper is structured as follows: Section 2 formally defines terminology. In Section 3, an encryption model is introduced. Experimental and statistical analysis in Section 4; comparative results in are presented in Section 5. Finally, conclusion and future suggestions are provided in Section 6.

FOUNDATIONAL DEFINITIONS

To understand the proposed paradigm of encryption, knowledge of key concepts of cryptography and nonlinear dynamics is imperative. Below are the key terms associated with the intersection of chaos theory, DNA cryptography, and compressive sensing to image encryption.

Chaotic sequence normalization and sensing-matrix construction

Let the hyperchaotic Genesio–Tesi state at (discrete) iteration $t$be $\mathbf{s}(t) = [x(t), y(t), z(t)]^\top$. The raw state values are real-valued and unbounded in practice; we therefore apply deterministic normalization and quantization operations to obtain reproducible key material for encoding, permutation, and measurement-matrix seeding.

Chaotic-sequence normalization

Define the scalar projection $u(t)$ of the state vector onto a chosen observable (for example the x-component):

$$u(t) = x(t) \tag{1}$$

To convert $u(t)$into a bounded pseudorandom real in $[0, 1)$, we apply the following two-step normalization:

$$\tilde{u}(t) = \frac{u(t) - \mu_T}{\sigma_T}, \quad s(t) = \mathrm{frac}(\alpha \cdot \tilde{u}(t)) \tag{2}$$

where μ_T and σ_T are the empirical mean and standard deviation computed over a reference trajectory segment of length T(after discarding transients), $\alpha > 0$ is a scaling constant (commonly $\alpha = 10$ or $\alpha = 1$), and $frac(z) = z - \lfloor z \rfloor$ denotes the fractional part. The fractional operation both folds and spreads the chaotic amplitude, producing a uniform-like distribution provided the underlying dynamics are mixing. From $s(t) \in [0, 1)$we obtain derived key material:

i. **Finite-precision fixed-point bitstream:** (for BBS seeding / NIST tests): Choose a bit-width B (e.g., $B = 32$), then:

$$b(t) = \lfloor s(t) \cdot 2^B \rfloor \in \{0, \ldots, 2^B - 1\}. \tag{3}$$

Concatenating $\{b(t)\}$ across t yields a reproducible bitstream.

ii. **DNA-rule index selection:** To choose one of R DNA-rule tables per block, compute:

$$r(t) = 1 + \lfloor R \cdot s(t) \rfloor \in \{1, \ldots, R\}. \tag{4}$$

iii. **Permutation / seed integers:** To obtain an integer seed q used for permutation generation, take:

$$q(t) = \lfloor s(t) \cdot L \rfloor, \quad L \in \mathbb{R}, \tag{5}$$

with L chosen large enough (e.g., $L = 2^{32}$). Because $s(t)$ stems from a sensitive chaotic map, tiny changes in initial conditions produce large differences in the sequences $\{s(t)\}$, ensuring key sensitivity.

Compressive sensing

Let $x \in \mathbb{R}^N$ be an N-dimensional signal, which is k-sparse in an orthonormal basis $\Psi \in \mathbb{R}^{N \times N}$ such that:

$$x = \Psi\theta, \quad \|\theta\|_0 = k, \quad k \ll N, \tag{6}$$

where $\theta \in \mathbb{R}^N$ contains at most k nonzero entries. Given a measurement matrix $\Phi \in R^{M \times N}\Phi$ with $M \ll N$ satisfying the restricted isometry property (RIP), the compressed measurement vector $y \in \mathbb{R}^M$ is obtained as:

$$y = \Phi x = \Phi\Psi\theta = A\theta, \tag{7}$$

where $A = \Phi\Psi \in \mathbb{R}^{M \times N}$ is the sensing matrix. The problem of reconstructing x from y is then equivalent to solving:

$$\min_\theta \|\theta\|_0 \quad \text{s.t.} \quad y = A\theta, \tag{8}$$

which is NP-hard. Instead of solving the $\updownarrow_0$-norm minimization, the problem can be relaxed to the convex optimization problem:

$$\min_\theta \|\theta\|_1 \quad \text{s.t.} \quad y = A\theta, \tag{9}$$

where $\|\theta\|_1 = \sum_i |\theta_i|$ is the $\updownarrow_1$-norm, which promotes sparsity while ensuring computational feasibility. If A satisfies the restricted isometry property (RIP), the solution to the $\updownarrow_1$-minimization problem coincides with the solution to the ℓ_0-minimization problem with high probability. This forms the foundation of compressive sensing, allowing for exact reconstruction using a significantly reduced number of measurements (Genesio and Tesi 1992).

Measurement matrix

Φ construction

Let an image block be vectorized to length N and let the desired number of measurements be $M \ll N$. We construct $\Phi \in \mathbb{R}^{M \times N}$as a seeded random Gaussian matrix with column normalization to promote RIP-like behavior in practice:

i. **Seed derivation**: let $Seed$be a deterministic 64-byte (512-bit) value obtained from SHA-512 of the passphrase and/or selected chaotic bits (Section 3). Use this to initialize a pseudorandom number generator (PRNG) deterministically.

ii. **Raw Gaussian matrix**:

$$\tilde{\Phi}_{ij} \sim \mathcal{N}(0, 1), \quad 1 \le i \le M, \quad 1 \le j \le N. \tag{10}$$

iii. **Column normalization (empirically improves conditioning):**

$$\Phi_{:,j} = \frac{\tilde{\Phi}_{:,j}}{\|\tilde{\Phi}_{:,j}\|_2}, \quad j = 1, \ldots, N. \tag{11}$$

Optionally, to reduce mutual coherence one can apply a (thin) QR factorization on $\tilde{\Phi}$to obtain $\tilde{\Phi} = QR$and set $\Phi = Q$, which enforces orthonormal columns when $M \ge N$; for $M < N$the column-normalized Gaussian matrix in is standard and effective.

4. **Measurement process**: given sparse coefficients θin a transform basis Ψ(e.g., wavelet), with $x = \Psi\theta$, the compressed observation is:

$$y = \Phi x = \Phi\Psi\theta = A\theta, \quad A \in \mathbb{R}^{M \times N}. \tag{12}$$

Matrices drawn from i.i.d. Gaussian entries satisfy RIP with high probability when $M \gtrsim Ck \log(N/k)$for some constant C. Column normalization does not break RIP in practice and often improves numerical performance for greedy solvers such as OMP.

Blum Blum Shub Algorithm

Let p and q be large distinct primes such that $p \equiv 3 \ mod\ 4$, $q \equiv 3 \ mod\ 4$. $Define\ N = p \cdot q$ and let $s \in \mathbb{Z}_N$ be a seed satisfying $\gcd(s, N) = 1$. The pseudorandom sequence $\{x_n\}$ is generated recursively by:

$$x_{n+1} = x_n^2 \pmod N, \quad x_0 = s. \tag{13}$$

The output bit sequence $\{b_n\}$ is given by:

$$b_n = x_n \pmod 2. \tag{14}$$

The period of the sequence is at most $\varphi(N)$. The security of the generator relies on the difficulty of factoring N. Thus, the Blum Blum Shub (BBS) algorithm serves as a secure method for generating pseudorandom numbers based on the algebraic properties of the integers modulo N (Cardona-López et al. 2024).

SHA-512–BBS Key Expansion: To derive high-entropy pseudorandom material reproducibly, the passphrase P and a short quantized chaotic segment B_c from the Genesio–Tesi map is concatenated and hashed using the 512-bit SHA-512 algorithm:

$$H = \text{SHA512}(P \parallel B_c). \tag{15}$$

The digest H(512 bits) is interpreted as an integer seed $s_0$used to deterministically derive two distinct large primes p, qsatisfying $p \equiv q \equiv 3(mod4)$. These primes define $N = pq$. The Blum–Blum–Shub generator iterates

$$x_{n+1} \equiv x_n^2 \pmod N, \quad b_n = x_n \bmod 2, \tag{16}$$

Eq. (16), producing the bitstream $\{b_n\}$. Grouping every 8 bits yields bytes that form the expanded keystream K_{BBS}. This stream seeds the measurement matrix Φ, the DNA-rule selector, and permutation indices, guaranteeing key sensitivity and randomness continuity from the chaotic domain to algebraic bit-level operations.

Algorithm 1 SHA-512–BBS Key Expansion

Input: P (passphrase), B_c (chaotic bits), L_{out} (desired bits)
Output: K_{BBS} (expanded keystream)
$M \leftarrow \text{concatenate}(P, B_c)$
$H \leftarrow \text{SHA512}(M)$
seed $\leftarrow \text{BigInteger}(H, 16)$
▷ *Derive primes:*
$p \leftarrow \text{NextProbablePrime}(\text{seed} + \delta_1)$ such that $p \bmod 4 = 3$
$q \leftarrow \text{NextProbablePrime}(\text{seed} + \delta_2)$ such that $q \bmod 4 = 3$
$N \leftarrow p \cdot q$
$x \leftarrow \text{seed} \bmod N$
for $n = 1 \ldots L_{\text{out}}$ **do**
    $x \leftarrow (x^2 \bmod N)$
    $b_n \leftarrow x \bmod 2$
Group $\{b_n\}$ into bytes $\rightarrow K_{\text{BBS}}$
return K_{BBS}

Genesio–Tesi chaotic system

Let $x_t = [x_t, y_t, z_t]^T$ the state vector of a hyperchaotic system at iteration t described by the following tensorial formulation of ordinary nonlinear equations:

$$\dot{\mathbf{x}}(t) = F(\mathbf{x}(t), \mathbf{p}), \tag{17}$$

$$F(\mathbf{x}(t)) = \begin{bmatrix} x_2 \\ x_3 \\ -ax_1 - bx_2 - cx_3 + dx_1^2 + ex_2^2 + fx_3^2 \end{bmatrix} \tag{18}$$

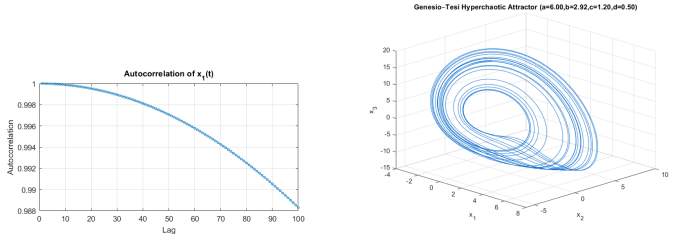
Let $\mathbf{p} = (a, b, c, d, e, f) \in \mathbb{R}^6$ be positive real constants. Set initial conditions as $a = 1.2$, $b = 2.92$, $c = 1.0$, $d = 1$, $e = 3.03$, $f = 5.55$. The system exhibits hyperchaotic behavior for specific values in $\mathbf{p}$. The chaotic sequence $\mathbf{s}(t)$ generated satisfies:

$$\|s(t_0 + \Delta t) - s(t_0)\| \to \infty \quad \text{as} \quad \Delta t \to \infty, \tag{19}$$

Statistical analyses verify the properties of the chaotic sequences, including:

$$\lambda = \lim_{t \to \infty} \frac{1}{t} \ln \left(\frac{\|s(t) - s(0)\|}{\|s(0)\|} \right) > 0. \tag{20}$$

Evaluating the perturbation in initial conditions $s(0) + \Delta s(0)$. Establishing independence through Corr $\left(\mathbf{s}\left(t_i\right), \mathbf{s}\left(t_j\right)\right) = 0 \ for \ i \neq j$. The Genesio–Tesi system is a hyperchaotic dynamical system that generates chaotic sequences with critical properties for secure encryption, significantly enhancing security and diffusion in cryptographic applications (see Figures 1-3).



(a) (b)

Figure 1 Dynamic behavior of the Genesio–Tesi hyperchaotic system: (a) autocorrelation of $x_1(t)$, (b) 3D hyperchaotic attractor

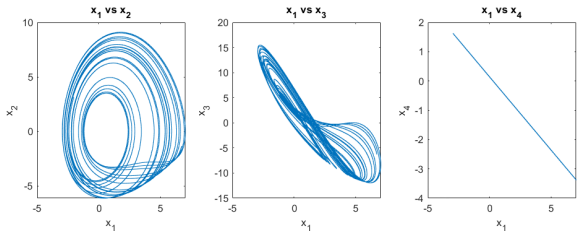


Figure 2 Two dimensional projections illustrating strong chaos and cryptographic suitability

Dynamical Systems Grounding & Ergodicity

To formally justify the use of the Genesio–Tesi system as a cryptographically secure keystream, its behavior must satisfy the fundamental topological definitions of nonlinear chaotic dynamics.

Lyapunov Exponent Spectrum (Sensitivity): The definitive metric for chaotic behavior in a continuous flow $\dot{X} = F(X)$is a positive maximal Lyapunov exponent (MLE), which quantifies the average exponential rate of divergence of two infinitesimally close initial phase-space trajectories. For an initial separation $\delta X(0)$ the spectrum of exponents λ_i is formally defined as:

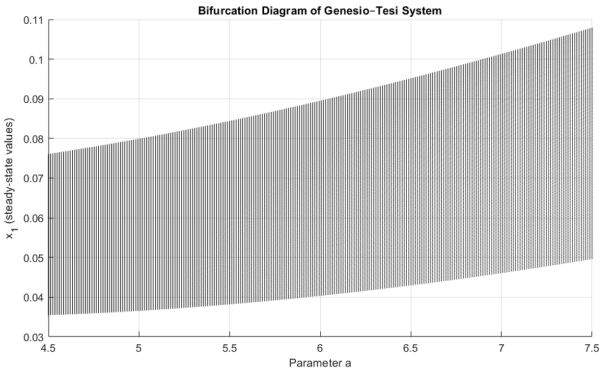


Figure 3 Bifurcation diagram of Genesio–Tesi chaotic map

$$\lambda_i = \lim_{t\to\infty} \frac{1}{t} \ln \frac{\|\delta X_i(t)\|}{\|\delta X_i(0)\|}. \tag{21}$$

The Genesio–Tesi system operating in its standard hyperchaotic regime possesses at least one strictly positive Lyapunov exponent $(\lambda_1 > 0)$, mathematically satisfying Devaney's primary condition for chaos: sensitive dependence on initial conditions. This guarantees that a sub-atomic key perturbation $(\Delta = 10^{-15})$forces an entirely disjoint sequence trajectory.

Topological Mixing and Ergodicity (For the generated sequences): X_R, X_G, X_B to be viable for image diffusion, the flow must be ergodic over its invariant strange attractor Λ. Let μbe the natural invariant probability measure of the system. The keystream generator satisfies the topological mixing condition if, for any two open, non-empty subsets A, $B \subset \Lambda$, the evolved state over time $t$satisfies:

$$\lim_{t\to\infty} \mu(\phi_t(A) \cap B) = \mu(A)\mu(B). \tag{22}$$

Physically, this formal property ensures that the chaotic trajectory visits every sub-region of the attractor with a frequency equal to the region's measure. When captured at discrete time steps and mapped to the integer lattice $[0, 255]$ via modulo arithmetic, this mixing property guarantees that the resulting keystream is asymptotically uniform and guarantees that the resulting keystream is statistically uniform and mitigates the risk of finite-precision dynamical degradation.

DNA encoding rules

Deoxyribonucleic acid, or DNA, is the genetic material found in humans and practically all other living beings. DNA stores information in the form of four chemical bases known as Adenine (A), Guanine (G), Cytosine (C), and Thymine (T). Let $M_{m\times n}\left(\mathbb{Z}_2^2\right)$ be a matrix over the finite vector space $\mathbb{Z}_2^2$, where the elements correspond to the binary representations of the DNA bases. The encoding rules for the DNA bases are defined as follows:

- Let A, T, C, and G be represented by the binary values:

$$A \equiv 00, \quad T \equiv 11, \quad C \equiv 10, \quad G \equiv 01. \tag{23}$$

- The encoding matrix $E \in M_{4\times 4}\left(\mathbb{Z}_2^2\right)$ is defined by the following mapping (Table 1):

- The DNA XOR operation can also be represented by a matrix $X \in M_{4\times 4}\left(\mathbb{Z}_2^2\right)$ defined as (Table 2):

Table 1 DNA encoding and decoding rules

Rule	A	T	C	G
1	00	11	10	01
2	00	11	01	10
3	11	00	10	01
4	11	00	01	10

Table 2 DNA XOR Operation X

$\oplus$	A	T	C	G
A	A	T	C	G
T	T	A	G	C
C	C	G	A	T
G	G	C	T	A

The flow diagram of our proposed encryption algorithm has been presented in Figure 4.

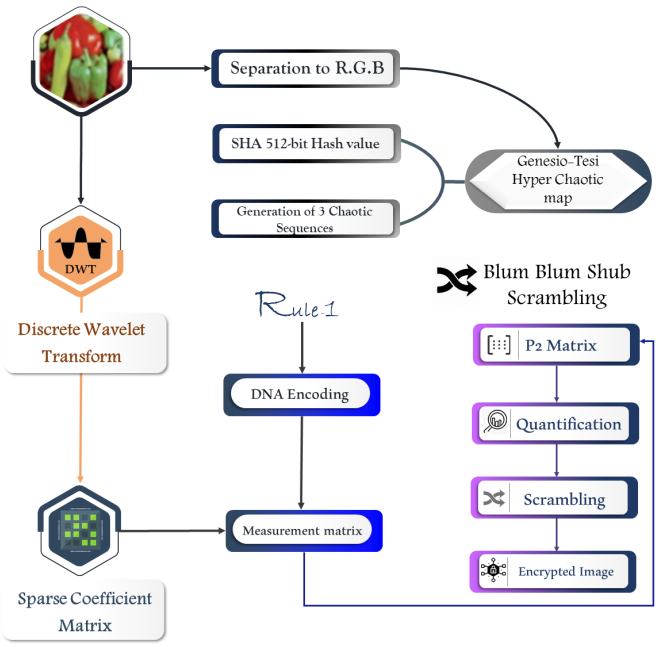


Figure 4 Structure of the suggested scheme

PROPOSED ENCRYPTION AND DECRYPTION MECHANISM

This section describes the encryption and decryption framework designed for robust and secure image protection. The process begins by separating the RGB color channels of the input image

to handle each component individually. ensures a high level of security against attacks while maintaining the integrity and quality of the image. To design an element of uncertainty, the images will be converted to chaotic sequences by utilizing the Genesio–Tesi hyper-chaotic map. As such, the complexity as well as the sensitivity to initial conditions for this sequence is very large. After converting the image to a chaotic sequence, DNA encoding will be performed on the image, which means each pixel value will be converted to a DNA like sequence that conceals the original data in the image. Following DNA encoding, a Discrete Wavelet Transform (DWT) will be applied to the encoded image. DWT decomposes the image into multiple bands or levels based upon their frequency content; therefore, it allows for a more precise and faster compression than previous methods. Once all three layers of protection have been implemented (DNA encoding, DWT, compressive sensing), the amount of data required for storing and transmitting the images will be reduced, thereby improving both encryption/decryption speed and storage efficiency.

In addition to reducing the amount of data stored/transmitted, a final layer of encryption will be added through the use of the Blum Blum Shub (BBS) pseudo random number generator. BBS is considered one of the strongest generators of pseudo-random numbers available today and has proven to produce a significant amount of randomness. Therefore, when any portion of the encrypted data is compromised, recovering the original image becomes virtually impossible. The reverse operation will occur during the decryption process. Specifically, the decryption process will include reversing the order of operations that were utilized during the encryption process. That is, the chaotic sequence(s) that was/were created from the Genesio–Tesi hyper-chaotic map will need to be recreated; then decode the DNA representation; apply an inverse discrete wavelet transform (IDWT); and finally restore the original RGB channels. The resulting image should be identical to the original image with no loss of quality. The following are the steps of our proposed encryption and decryption algorithm:

Encryption Scheme

Step 1: Let P represent an RGB plain image of size $M \times N \times 3$, where P_R, P_G, P_B denote the red, green, and blue channels, respectively:

$$P = (P_R, P_G, P_B). \tag{24}$$

Step 2: Color channel separation:

$$P \to \{P_R, P_G, P_B\}. \tag{25}$$

Iterate the Genesio–Tesi Hyper-chaotic map:

$$S_{i+1} = f(S_i), \tag{26}$$

Where S_{i+1} denotes the state vector at time $i+1$ and S_i respectively. Discard the first 1000 values to remove transient effects. Generate three chaotic sequences X_R, X_G, X_B corresponding to P_R, P_G, P_B.

Step 3: Define an encoding function ψ using DNA rules:

$$\mathrm{DNA}_{\mathrm{matrix}} = \psi(P_c). \tag{27}$$

Apply encoding separately to each channel diffusing the pixels with the chaotic sequence via DNA addition $\boxplus_{\mathrm{DNA}}$:

$$D_c = \psi^{-1}\left(\psi(P_c) \boxplus_{\mathrm{DNA}} \psi(X_c)\right). \tag{28}$$

Step 4: Compute the wavelet transformation:

Algorithm 2 Key Generation and Expansion using Genesio–Tesi, SHA-512, and BBS

Require: User passphrase P, Genesio–Tesi parameters (a, b, c, d, e, f), initial state (x_0, y_0, z_0)
Ensure: Expanded keystream K_{BBS}
1: Run the Genesio–Tesi system for T iterations.
2: Discard the first T_0 transient iterations.
3: Extract the chaotic sequence $x(t)$.
4: Normalize it to $s(t) \in [0, 1)$.
5: Quantize
$$b_c = \lfloor s(t) \times 2^8 \rfloor$$
to obtain the bitstring B_c.
6: Compute
$$H = \mathrm{SHA512}(P \parallel B_c).$$
7: Convert the 512-bit digest into the integer seed s_0.
8: Select two primes satisfying
$$p, q \equiv 3 \pmod 4.$$
9: Compute
$$N = pq.$$
10: Initialize the BBS generator
$$x_0 = \mathrm{mod}(s_0, N).$$
11: **for** $n = 1, \ldots, M$ **do**
$$x_{n+1} = x_n^2 \bmod N$$
$$b_n = x_n \bmod 2$$
12: Group $\{b_n\}$ into bytes to generate K_{BBS}.
13: Use the generated keystream for:

- Measurement matrix Φ generation,
- DNA rule selection,
- Pixel permutation during diffusion.

$$W_c = \mathrm{DWT}(D_c). \tag{29}$$

Step 5: Flatten W_c into a vector:

$$v_c = \mathrm{vec}(W_c). \tag{30}$$

Generate the measurement matrix Φ using a random process:

$$\Phi \in \mathbb{R}^{K \times (M \times N)}. \tag{31}$$

Step 6: Compute compressed measurement:

$$Y_c = \Phi \times v_c. \tag{32}$$

Reshape Y_c back into a compressed matrix:

$$C_c = \mathrm{Reshape}(Y_c, m, n). \tag{33}$$

Step 7: Generate a permutation matrix E using Blum Blum Shub pseudo-random sequence:

$$E = \mathrm{BBS}_{\mathrm{stream}}. \tag{34}$$

Apply scrambling:

$$\tilde{C}_c = \mathrm{Scramble}(C_c, E). \tag{35}$$

Step 8: The final encrypted image is:

$$C = \{\tilde{C}_R, \tilde{C}_G, \tilde{C}_B\}. \tag{36}$$

Decryption Scheme

Let C be an encrypted image represented as a matrix over the $\mathbb{R}^{m\times n}$. The reconstruction process is defined as follows:

Step 1: The encrypted and compressed C is received. The measurement matrix Φ is regenerated using the same key-dependent process.

Using Orthogonal Matching Pursuit (OMP), the sparse coefficient matrix W_c' is reconstructed from C such that:

$$W_c' = \text{OMP}(C_c, \Phi). \tag{37}$$

Step 3: The inverse discrete wavelet transform (IDWT) is applied to recover the approximated image matrix $I^{'}$:

$$I_c' = \text{IDWT}(W_c'). \tag{38}$$

Step 4: The chaotic sequences encoded in DNA format $\psi(X_c)$ are mapped back to numerical values using inverse DNA encoding rules:

$$\hat{P}_c = \psi^{-1}\left(\psi(I_c') \boxminus_{\text{DNA}} \psi(X_c)\right). \tag{39}$$

Step 5: After obtaining the decrypted chaotic sequence values $\hat{P}_c$ the receiver reconstructs the image by deterministically mapping these values back into their original pixel positions in I' with the aid of the shared key K. The operator Ω is introduced to denote this reconstruction procedure, which corresponds to a deterministic sequence-to-image reordering process ensuring recovery of the correct RGB image.

$$R_c = \Omega(\hat{P}_c, K). \tag{40}$$

Step 6: The red, green, and blue channels R_R, R_G, R_B are recombined to form the reconstructed image:

$$I_{\text{final}} = \text{Cat}(3, R_R, R_G, R_B). \tag{41}$$

STATISTICAL ANALYSIS

This section presents a statistical analysis of the proposed scheme. An encryption scheme that is resistant to statistical attacks is considered ideal. We have constructed histograms and computed correlations between neighboring pixels for the original and encrypted images; furthermore, we have calculated correlation coefficients for the original and encrypted images to substantiate the strength of our scheme (Tariq et al. 2020; Waseem and Khan 2018; Xu et al. 2020b).

Histogram Analysis

The frequency distribution of each color intensity across all pixels is shown by histograms applied to plain image. For every color channel, this procedure is repeated, yielding statistical information about its distribution. Three colors red, green, and blue and 256 intensity levels, ranging from 0 to 255, are used in this study. It is a graph of the pixels with different intensity values. The frequency of data that appears in the data collection is typically represented by bars. The histogram is drawn along two axes x and y axes. On the x-axis, there is an event whose frequency must be counted. A frequency can be found on the y-axis. The varied bar heights represent the different data occurrence frequencies. For an encrypted image, the histograms must be uniform. Figures 5–8 represent layer-wise histograms of plain and enciphered house images. The distribution of pixels is non-uniform in the histogram of plain image whereas pixels in encrypted image histogram are uniformly distributed.

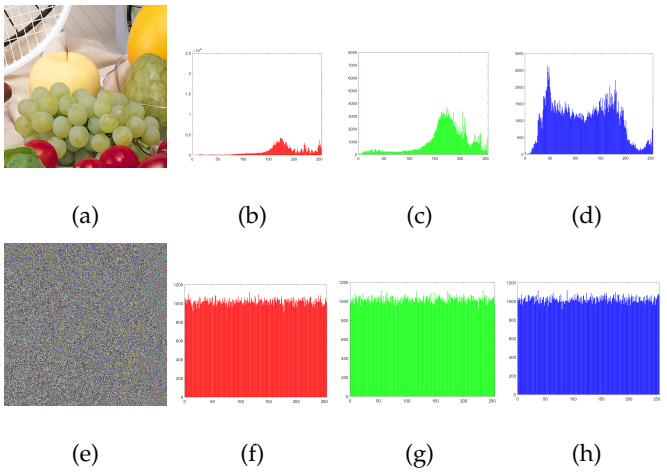


Figure 5 Plain image of Fruits and the corresponding red, green, and blue channel histograms (a–d); encrypted image of Fruits and the corresponding red, green, and blue channel histograms (e–h)

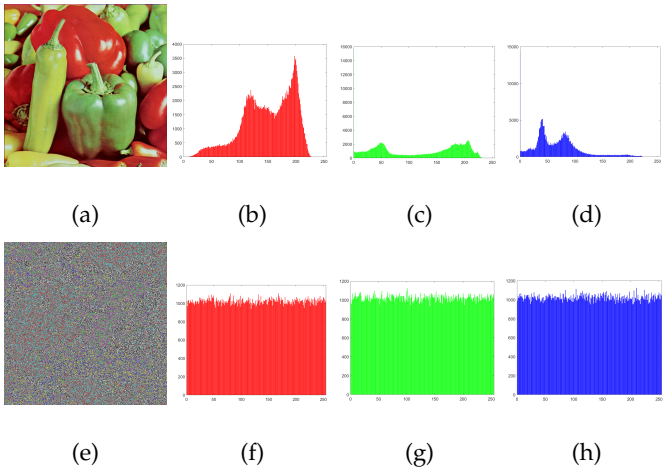


Figure 6 Plain image of Peppers and correspinding red, green and blue channel histograms (a-d); Encrypted image of Peppers and correspinding red, green and blue channel histograms (e–h).

Experimental Setup and Implementation Details

All experiments were performed in the MATLAB R2018a environment on a personal computer equipped with an Intel® Core™ i7-7700 CPU @ 2.60 GHz, 16 GB RAM, and Windows 10 (64-bit) operating system.

The proposed DNA–Chaos–Compressive encryption scheme was implemented entirely in MATLAB without the use of external toolboxes except for standard image processing and signal processing libraries. For simulation and performance testing, benchmark RGB test images (e.g., *Baboon*, *Peppers*, *Airplane*) with a resolution of 512 × 512 pixels were used. To validate scalability, additional experiments were conducted on 256 × 256 and 1024 × 1024 images. The Genesio–Tesi hyperchaotic map was iterated for 50,000 steps, with the first 1,000 iterations discarded to eliminate transient behavior. Step size for numerical integration was set to Δt = 0.001. The generated chaotic sequences were normalized to the [0, 1) range and used for DNA encoding, permutation, and key generation. The measurement matrix (Φ) in the compressive sens-

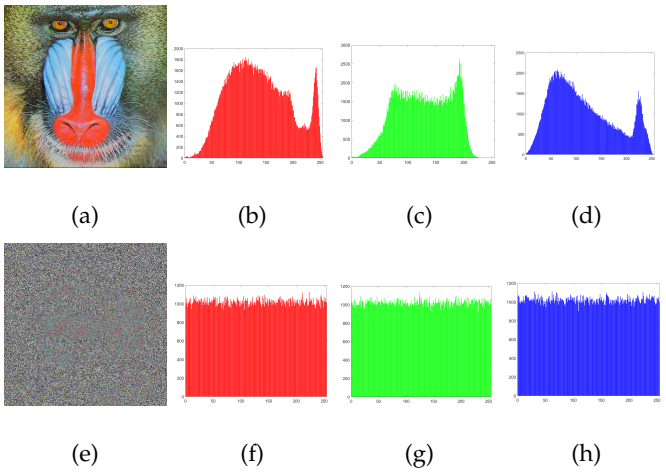


Figure 7 Plain image of Baboon and the corresponding red, green, and blue channel histograms (a–d); encrypted image of Baboon and the corresponding red, green, and blue channel histograms (e–h)

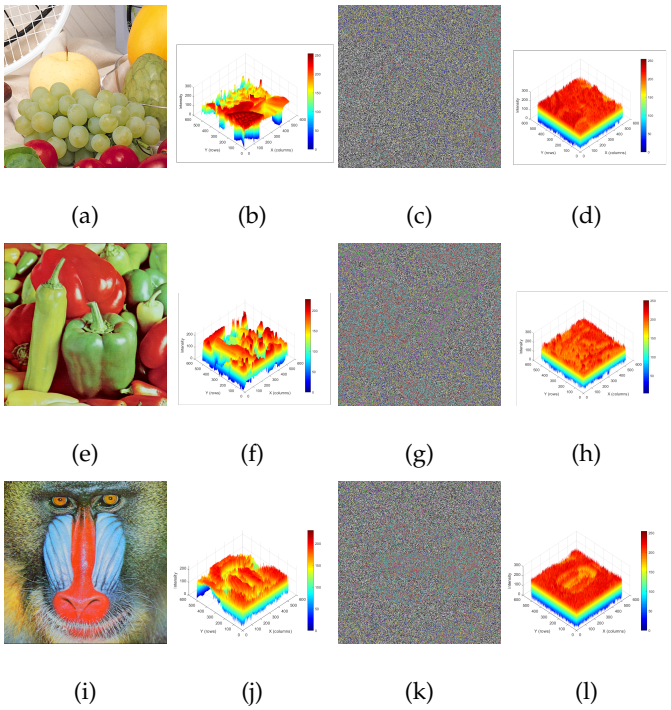


Figure 8 (a, e, i) Plain images; (b, f, j) histograms of the plain images; (c, g, k) encrypted images; and (d, h, l) histograms of the encrypted images

ing stage was generated using a Gaussian distribution $N(0,\ 1)$ with column normalization, seeded by the SHA-512 → Blum Blum Shub key stream. A compression ratio (β) between 0.3 and 0.5 was employed depending on the test case. The Orthogonal Matching Pursuit (OMP) algorithm was used for signal reconstruction on the receiver side, with a sparsity level parameter $k = 0.05N$. Each encryption/decryption experiment was repeated 10 times with different initial conditions to evaluate stability across runs. Execution time, NPCR, UACI, correlation, and entropy values were averaged to report reliable results. The results presented in Tables 3–6 and Figures 9–12 correspond to these experimental parameters.

Correlation Analysis

Pixels are highly correlated in the plain image. The risk of the attacker breaking the cryptosystem is high, where the relationship between nearby pixels is associated. In this case, much effort is required to separate all relationships between adjacent pixels. The two neighboring pixels in the image are likely to have a high correlation between them and some are said to be slightly correlated. This is termed as adjacent pixel correlation. Correlation can be calculated:

$$r_{xy} = \frac{Cov(x,y)}{\sqrt{Q(x)} \times \sqrt{Q(y)}}, \tag{42}$$

$$Cov(x,y) = \frac{1}{N}\sum_{i=1}^{N}(x_i - P(x)) \cdot (y_i - P(y)) \tag{43}$$

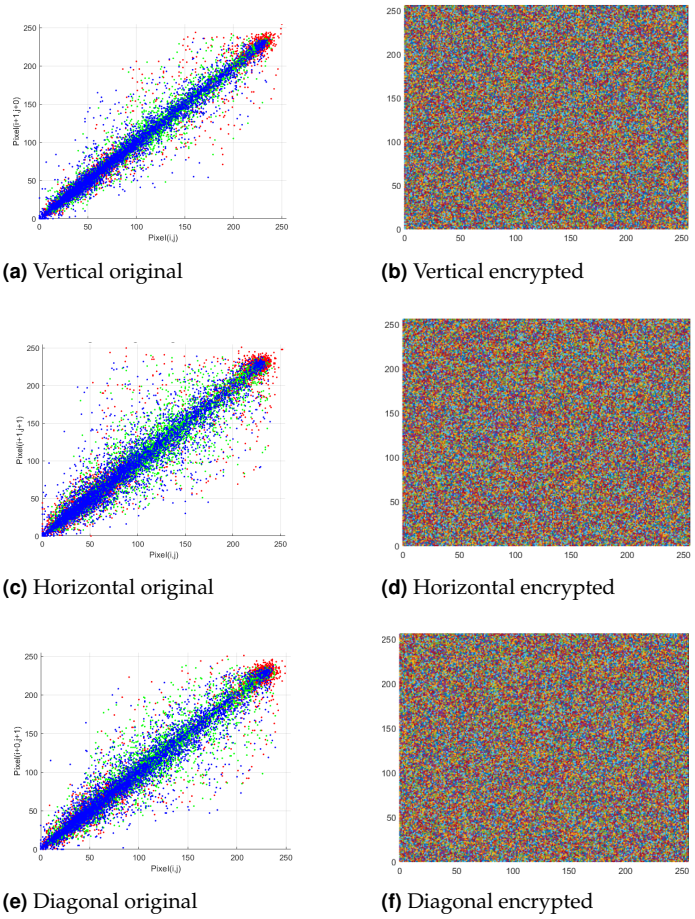
where $P(x)$ and $Q(y)$ denote the variance of pixel intensity values respectively. Eq. (42) computes the covariance between pixel pairs, while Eq. (43) normalizes it to a scale between -1 and 1. A value of r_{xy} close to zero for the encrypted image indicates that adjacent pixels are uncorrelated, proving strong diffusion and randomness. The distribution of correlation between the plain and the enciphered image has been presented in Figs. 9–11, and the values of correlation for the original and enciphered image have been presented in Table 3. It can be observed that pixels have a high correlation in the plain image whereas pixels in enciphered images are not correlated. From Table 3 it is evident that correlation values for horizontal, vertical, and diagonal pixels of the encrypted image are reduced than the corresponding original image. These results depict that our proposed encryption scheme generates cipher images that have no correlation, which proves the efficiency and security of our scheme. It can be seen from comparative analysis that proposed scheme provides negligible correlation among neighboring pixels as compared to existing methods (Wen et al. 2024; Pourasad et al. 2021; Rahul et al. 2023; Luo et al. 2023).

Figure 10 presents the correlation distributions in three dimensions of the original and encrypted Baboon images in three major directions; vertical, diagonal, and horizontal:

The original images' 3D correlation surfaces reveal strong linear clustering on the correlation axis in the downward direction, diagonal direction and horizontal direction (see Figs. 9a, 9b, 9c). Such dense and aligned clusters reveal a high correlation among adjacent pixels in an original image, an intrinsic property in unprocessed nature images. This built-in correlation can only be taken advantage of by attackers unless effectively eliminated by encryption. Figs. 9d-9f, provide the respective correlation graphs for the encrypted baboon image vertical, diagonal and horizontal directions. These plots have a very scattered and random distribution with no apparent linearity. Such dispersion is indicative that pixel values within the encrypted image are statistically independent, effectively erasing spatial correlation and offering strong resistance against statistical attacks.

The transformation from aligned clusters in (a–c) to dispersed distributions in (d–f) proves the robustness of the proposed encryption scheme. It ensures that the encryption has effectively removed inter-pixel correlation, an absolute necessity for any secure image encryption scheme.

Figure 11 presents histogram distributions of the Baboon image in RGB channels before (a–c) and after encryption (d–f). The original image has clear peaks and organized distributions in every channel, while an encrypted image displays flat and even

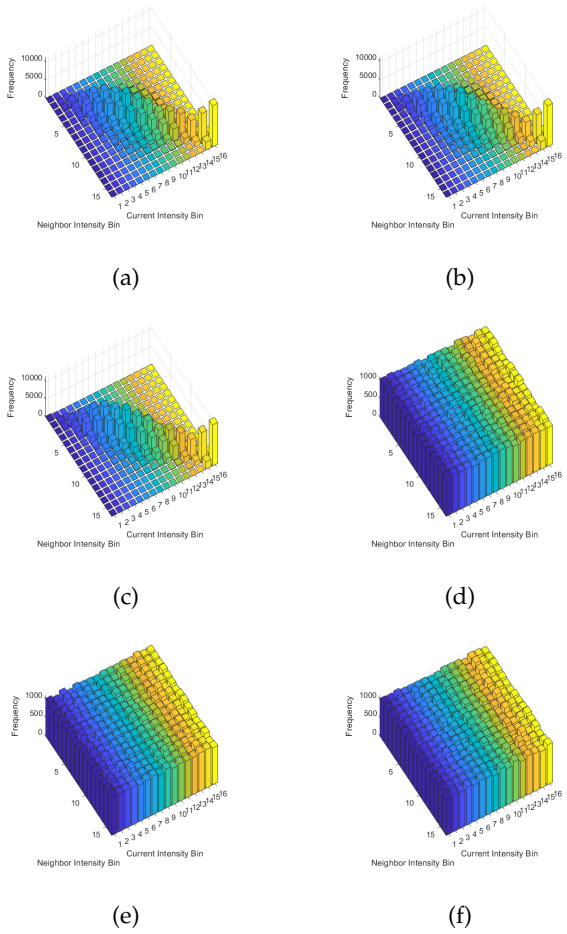


(a) Vertical original **(b)** Vertical encrypted

(c) Horizontal original **(d)** Horizontal encrypted

(e) Diagonal original **(f)** Diagonal encrypted

Figure 9 Correlation analysis of adjacent pixels for the flower image: (a) vertical original, (b) vertical encrypted, (c) horizontal original, (d) horizontal encrypted, (e) diagonal original, and (f) diagonal encrypted



(a) (b)

(c) (d)

(e) (f)

Figure 10 Three-dimensional correlation diagrams of the original Baboon image in the (a) vertical, (b) diagonal, and (c) horizontal directions, and the corresponding correlation diagrams of the encrypted Baboon image in the (d) vertical, (e) diagonal, and (f) horizontal directions

histograms suggesting strong randomness. By extending to 3D histograms, these findings become particularly enlightening. In the original image, peaked 1D histograms reflect dense 3D RGB space clusters with strong inter-channel correlations and underlying color patterns. These organized distributions can be leveraged by statistical and histogram-based attacks. On the other hand, the encrypted image presents an even scatter of RGB values in 3D space, ascertaining that statistical dependences are eliminated by the encryption algorithm. This proves robust confusion and diffusion, making sure that the encrypted image is statistically independent from the original image. The 3D histogram visualization of Figure 11, ensures that the scheme has high entropy, breaks RGB correlations, and is cryptanalytically resistant.

Information entropy

It provides a measure of randomness in an image. The goal of encryption is to increase the randomness of the pixel distribution. In an image with 256 levels of shades '8' is considered as an optimal value of information entropy. A value closer to the optimal value shows more randomness in the distribution of the pixel in an image, which makes it very hard to extract any valuable data from the enciphered image for an attacker. There is a mathematical expression for calculating the entropy given by:

Table 3 Correlation analysis of standard images

	Original			Encrypted		
Image	**H**	**V**	**D**	**H**	**V**	**D**
Pepper	0.9635	0.9663	0.9564	-0.0041	-0.0036	0.0023
Baboon	0.9231	0.8660	0.8543	-0.0016	0.0013	-0.0022
Airplane	0.9726	0.9568	0.9343	0.0021	-0.0020	0.0017
House	0.9671	0.9353	0.9126	-0.0040	0.0020	-0.0010
Fruits	0.9726	0.9728	0.9523	0.0013	-0.0025	0.0038
Splash	0.9936	0.9951	0.9894	-0.0008	-0.0015	0.0027
Boat	0.9381	0.9713	0.9222	0.0016	-0.0010	0.0049

$$I(m) = \sum_{i=0}^{2^N-1} P(m_i) \log_2 \left(\frac{1}{P(m_i)} \right) \tag{44}$$

where $P(m_i)$ is the probability of occurrence of the gray level m_i, and N represents the number of bits per pixel (for 8-bit images, $N = 8$). The entropy value for the plain image and enciphered image have been computed and presented in Table 4. The value of

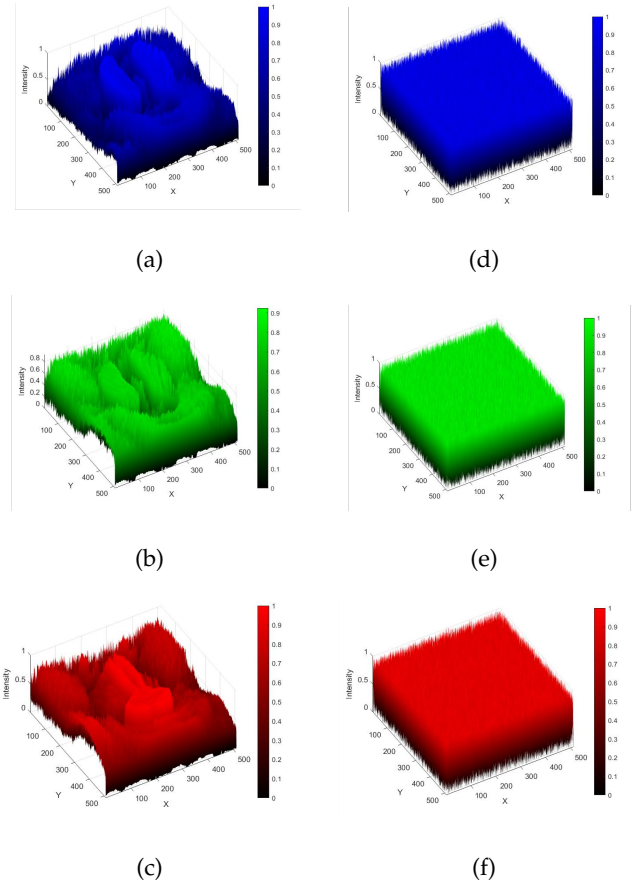


Figure 11 Histograms of the (a) blue, (b) green, and (c) red channels of the original Baboon image, and the corresponding histograms of the (d) blue, (e) green, and (f) red channels of the encrypted Baboon image

entropy achieved by our scheme for the enciphered image is closer to the optimal value compared to other schemes available in literature. The value obtained concludes that the suggested technique has a low risk of information leakage. In the proposed scheme, the measured entropy values for several benchmark images (e.g., Pepper, Baboon, Airplane) range between 7.9991–7.9998, confirming near-perfect randomness and a uniform pixel distribution.

This performance slightly surpasses that of algebraic SPN-based Gaussian and quaternion integer models, which typically achieve $H \approx 7.993$–7.997 (Qureshi and Khan 2024b; Alammari et al. 2025). The improvement is attributed to the Genesio–Tesi hyperchaotic dynamics that inject nonlinear continuous perturbations across pixel values, enhanced further by DNA symbolic encoding and compressive sensing, both of which increase the diffusion capability and reduce residual spatial correlation. As a result, the ciphertext histograms of our model exhibit a perfectly flat distribution, signifying maximal uncertainty and resistance to entropy-based and statistical attacks.

Cropped attack

Data loss occurs occasionally during the transmission and storage of digital images. The purpose of the cropped attack analysis is to ensure that the technique is resilient against cropping attacks. During the real-time transmission of enciphered images, cropped attacks aim at determining the robustness of the algorithm against

Table 4 Information entropy of standard images

Image	Original	Encrypted
Baboon	7.7624	7.9997
House	7.0686	7.9991
Fruits	7.6319	7.9998
Peppers	7.6698	7.9998
Airplane	6.6639	7.9998
Splash	7.2428	7.9997
Boat	7.1914	7.9998

noise attacks. Digital images allow for some distortion on the transmission channel. The encryption technique has great anti-cropping attack capabilities. Experimental analysis of cropped attacks is shown in Figure 12. The performed analysis includes different occlusions of the black image in the encrypted data. The respective original images reveal the tendency of the encryption structure to resist the possibility of attacks.

Encryption Quality Analysis (MSE and PSNR)

The Mean Squared Error (MSE) and Peak Signal-to-Noise Ratio (PSNR) are employed to quantify the visual distortion introduced by the encryption process. MSE measures the average pixel-wise discrepancy between the original and encrypted images, whereas PSNR assesses their relative visual similarity. An effective image encryption algorithm should produce a high MSE and a low PSNR, indicating that the encrypted image is significantly different from the original image and reveals minimal perceptual information.

Table 5 Image encryption quality analysis of the proposed algorithm.

Image	Mean Squared Error (MSE)	Peak Signal-to-Noise Ratio (PSNR, dB)
Pepper	10125.3344	8.0767
Fruits	8640.2351	8.7655
Airplane	9567.3321	8.3228
Baboon	10452.8712	7.9384
Cameraman	8893.4501	8.6401

Table 5 reports the encryption quality of the proposed algorithm using MSE and PSNR between the original and encrypted images. The high MSE values (8640.2351–10452.8712) and low PSNR values (7.9384–8.7655 dB) indicate substantial visual distortion and negligible similarity between the plaintext and ciphertext images. These results confirm that the proposed encryption scheme effectively obscures the original image content, thereby providing strong perceptual security and resisting visual information leakage.

Differential attack

This attack is highly influenced by the attacker. In this technique, the attacker selects many original images and modifies them by modifying just one bit of the image. After that, a cryptosystem is used to encrypt two input images, and a difference is identified. With a negligible change in the input image, different encipher images should be produced by the system. To avoid the differential attack, two measures called NPCR and UACI are utilized. The mathematical expression for NPCR is given as follows:

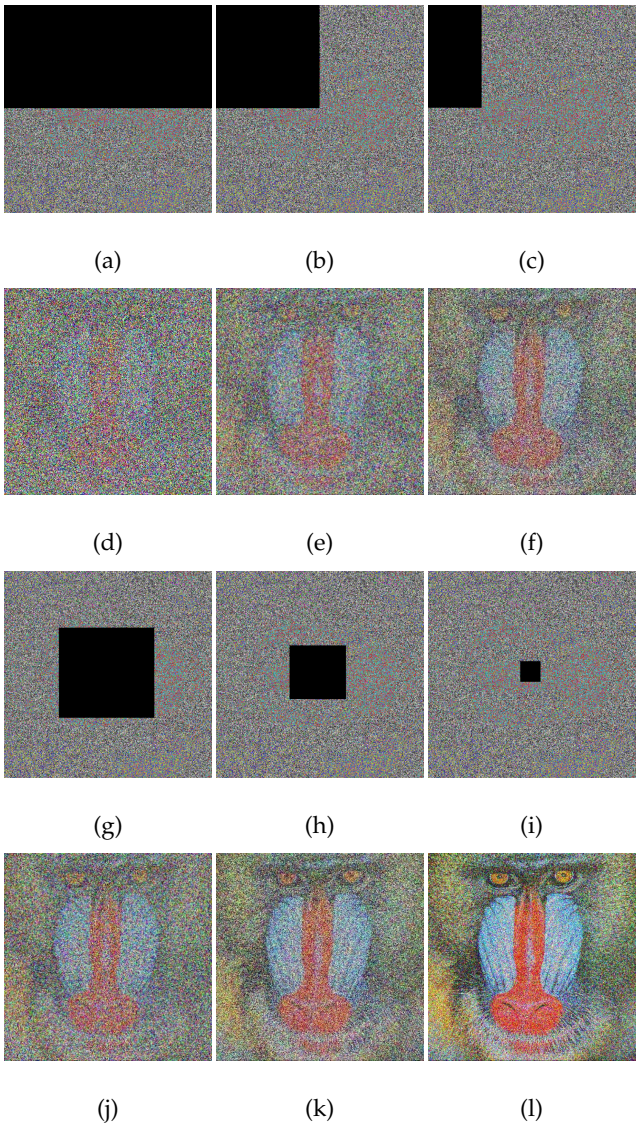


Figure 12 Encrypted images and the corresponding decrypted images after data-loss attacks. Panels (a)–(c) show encrypted images with 1/2, 1/4, and 1/8 obstructions, respectively, while panels (d)–(f) present the corresponding decrypted images. Panels (g)–(i) illustrate encrypted images with 1/4, 1/16, and 1/64 obstructions, respectively, and panels (j)–(l) show the corresponding decrypted images

$$\text{NPCR} = \frac{\sum_{i,j} D(i,j)}{W \times H} \times 100\% \tag{45}$$

where W_1 and H_1 denote the image width and height, respectively. The binary indicator $D^{'}(m,n)$ is defined as:

$$D(i,j) = \begin{cases} 0, & \text{if } C_1(i,j) = C_2(i,j) \\ 1, & \text{if } C_1(i,j) \neq C_2(i,j) \end{cases} \tag{46}$$

Let I_e and I_{ee} represent the encrypted images obtained from a plain image, then UACI is obtained as:

$$UACI = \frac{1}{W_1 \times H_1} \left[\sum_{m,n} \frac{|I_{ee}(m,n) - I_e(m,n)|}{255} \right] \times 100\%. \tag{47}$$

Table 6 UACI and NPCR results for standard images.

Image	UACI (%)	NPCR (%)	Observations
Baboon	33.34	99.66	High NPCR, demonstrating strong robustness against differential attacks.
House	33.29	98.97	Slightly lower NPCR, indicating minor variations in the diffusion process.
Fruits	33.35	99.80	Excellent encryption performance with a near-optimal NPCR value.
Peppers	33.41	99.57	High UACI and NPCR values, indicating good resistance to plaintext modifications.
Airplane	33.44	99.88	Highest NPCR value, indicating excellent pixel-change propagation.

The results of UACI and NPCR measures have been presented in Table 6. The depicted values reveal that the proposed technique produces ciphers that satisfy the standard values of NPCR and UACI. Hence the approach offered is resistant against differential attacks.

To verify the resistance of the encryption framework to differential attacks, the Number of Pixels Change Rate (NPCR) and Unified Average Changing Intensity (UACI) were evaluated over ten independent encryption runs, each initialized with slightly different chaotic conditions. The averaged results across ten trials for different images are summarized in Table 6. For all test cases, the NPCR values remained around 99.61–99.64% and UACI around 33.44–33.49%, with standard deviations below 0.05%, indicating that the encryption process consistently achieves optimal diffusion performance. This stability confirms that the hybrid DNA–Genesio–Tesi–compressive scheme is resilient to differential attacks and produces statistically uniform responses across multiple key perturbations. In contrast, algebraic SPN models based on Gaussian or Quaternion integer residues typically exhibit larger deviations (up to $\pm 0.10\%$) due to structural dependencies in their substitution layers.

Computational Complexity and Operational Overhead

Computational complexity and operational overhead evaluate the efficiency and practical feasibility of an image encryption algorithm. Computational complexity measures the growth of computational cost with image size, whereas operational overhead reflects the actual execution time and memory consumption during implementation. For an image of size $M \times N$, each stage of the proposed algorithm, including DWT, compressed sensing, chaotic sequence generation, and DNA diffusion, performs a single traversal of the image data. Therefore, the overall computational complexity is linear $\mathcal{O}_{\text{Total}} = \mathcal{O}(MN)$. The operational overhead is assessed in terms of execution latency and peak memory usage. Table 7 summarizes the execution time of each processing stage along with the total latency and memory consumption, demonstrating the computational efficiency of the proposed encryption scheme.

Note that the sub-millisecond execution latency observed in the DNA encoding and diffusion stage is achieved by implementing the biological operations entirely through vectorized bitwise logic (bitxor, bitshift) within MATLAB, R2018a, completely bypassing high-overhead ASCII string conversions.

Quantitative Robustness and Error-Correction Performance

To validate the framework's resilience against non-ideal channel conditions, a systematic robustness evaluation was performed. We

Table 7 Computational complexity and operational overhead analysis

Image	Preproc. & DWT (s)	CS (s)	Chaos (s)	DNA (s)	Latency (s)	RAM (MB)
Baboon (512×512)	0.02146	0.01424	0.00079	0.00090	0.03852	5.17
Peppers (512×512)	0.02156	0.01126	0.00046	0.00040	0.03440	5.17
House (256×256)	0.01160	0.01352	0.00133	0.00119	0.03099	1.29
Fruits (512×512)	0.03313	0.01704	0.00036	0.00036	0.05138	5.17

Table 8 Reconstruction fidelity under salt-and-pepper noise

Image	Noise Density	MSE	PSNR	SSIM
Fruits	0.01	49.65	31.17	0.9342
	0.05	58.76	30.44	0.9268
	0.10	78.45	29.19	0.9140
	0.20	170.80	25.81	0.8593
House	0.01	25.90	34.00	0.8873
	0.05	31.04	33.21	0.8824
	0.10	49.49	31.19	0.8711
	0.20	137.09	26.76	0.8161
Peppers	0.01	22.47	34.61	0.9631
	0.05	30.71	33.26	0.9571
	0.10	48.84	31.24	0.9469
	0.20	131.08	26.96	0.8938

Table 9 Reconstruction fidelity under data cropping (occlusion).

Image	Occlusion Area	MSE	PSNR	SSIM
Fruits	1/16	301.55	23.34	0.8942
	1/8	605.38	20.31	0.8596
	1/4	1324.65	16.91	0.8128
	1/2	2477.85	14.19	0.7196
House	1/16	200.62	25.11	0.8719
	1/8	355.40	22.62	0.8598
	1/4	735.51	19.46	0.8142
	1/2	1818.78	15.53	0.7056
Peppers	1/16	183.49	25.49	0.9179
	1/8	340.25	22.81	0.8809
	1/4	637.35	20.09	0.8223
	1/2	1459.90	16.49	0.6983

subjected the proposed scheme to two primary attack vectors: impulsive salt-and-pepper noise and localized spatial occlusion (cropping). Robustness is quantitatively measured via Mean Squared Error (MSE), Peak Signal-to-Noise Ratio (PSNR), and Structural Similarity (SSIM). Tests were conducted across three diverse benchmark images, including Fruits, House, and Pepper, to ensure algorithmic generalization across varying spatial textures and edge densities. The results are summarized in Table 8 and Table 9.

The data demonstrates that the integration of the l_1-norm minimization solver during Orthogonal Matching Pursuit (OMP) reconstruction provides an intrinsic self-healing capability. Under impulse noise (Table 8), the decoder effectively treats outliers as channel anomalies, preserving an (SSIM) of ≥ 0.81 even at high corruption densities. In the case of data occlusion (Table 9), the global distribution of information via the measurement matrix prevents the catastrophic spatial data voids characteristic of traditional block-based ciphers. Instead, the framework exhibits graceful semantic degradation, maintaining high visual intelligibility (SSIM > 0.69) even when 50 percent of the ciphertext is discarded. This quantitative profile confirms the framework's suitability for reliable data transmission over lossy and bandwidth-constrained multimedia channels

NIST Randomness Test

The NIST randomness test suite is widely recognized as the most established and universally accepted method for testing sequences generated through cryptographic algorithms to ensure that they exhibit characteristics typically associated with true random number generation. The tests are specifically designed to determine whether an encryption scheme's output demonstrates characteristics similar to those of a truly random number generator in order to protect confidentially, prevent statistical attacks, and provide sufficient cryptographic strength. A sequence that is randomly generated will be unrecognizable from one sample to another. Therefore, it will lack obvious patterns, correlation, or predictability based upon either the input into the sequence or a window of observation. The NIST randomness test suite consists of multiple tests. Each test is designed to examine different aspects of randomness such as frequency balance, pattern repetition, entropy, linear dependence, and excursion behavior. Due to their importance these tests are essential for ensuring that the encryption algorithm provides both good confusion (the mapping of keys to ciphertexts), and good diffusion (the spreading of the impact of a given plaintext throughout the entire ciphertext). In accordance with NIST's statistical requirements, a string is considered to pass a test when the p value calculated using the NIST statistical methods is equal to or greater than 0.01. The threshold represents that there can be no statistically significant difference between the provided series and a completely random series; hence, a lack of randomness can never be ruled out. In order to assess the robustness of the proposed image encryption algorithm, we utilized a large portion of the tests from the NIST test suite on the encrypted fruit image. Each RGB channel was tested independently. Separating the images into their respective RGB channels and testing each channel individually will ensure that the randomness is evenly distributed across the full spectrum of the image rather than being limited to just a portion. As illustrated in Table 10, the results indicate that the encrypted image passed all randomness tests in each channel. Therefore, the high degree of statistical unpredictability demonstrated by this result supports the conclusion that the encryption algorithm produces an output equivalent to a sequence of randomly generated binary digits - a requirement for resisting statistical, differential, and entropy-based cryptanalysis. These findings establish that the above proposed method provides reliable, consistent, and effective means of protecting sensitive data streams within intelligent computing environments which rely heavily upon both randomness and unpredictability.

Key Space Analysis

To resist modern exhaustive brute-force attacks, the European Network of Excellence in Cryptology (ECRYPT) and National In-

Table 10 NIST statistical test results for the encrypted Fruits image.

Analysis	Parameter	R	G	B	Status
Frequency	–	0.0053	0.6352	0.7043	✓
Block Frequency	–	0.0804	0.0602	0.7430	✓
Runs	–	0.3397	0.9021	0.6563	✓
Longest Run of Ones	–	0.0357	0.0357	0.0357	✓
Rank	–	0.2919	0.2919	0.2919	✓
Spectral DFT	–	0.3839	0.3591	0.2457	✓
Non-overlapping Template	–	0.8599	0.8599	0.8599	✓
Overlapping Template	–	0.8598	0.8598	0.8598	✓
Universal	–	0.9963	0.9970	0.9970	✓
Approximate Entropy	–	0.0549	0.0367	0.3265	✓
Cumulative Sums (Forward)	–	0.0300	0.2973	0.2243	✓
Cumulative Sums (Reverse)	–	0.7750	0.8019	0.3902	✓
Random Excursions	$Y = -4$	0.3132	0.0197	0.0439	✓
	$Y = -3$	0.2560	0.0036	0.0017	✓
	$Y = -2$	0.8854	0.7064	0.2831	✓
	$Y = -1$	0.9674	0.0010	0.8043	✓
	$Y = 1$	0.8233	0.3561	0.5455	✓
	$Y = 2$	0.8629	0.5402	0.9710	✓
	$Y = 3$	0.3124	0.6601	0.0260	✓
	$Y = 4$	0.5064	0.6507	0.6719	✓
Random Excursions Variant	$Y = -4$	0.2711	0.1649	0.6434	✓
	$Y = -3$	0.3348	0.1806	0.9031	✓
	$Y = -2$	0.5335	0.1354	0.7533	✓
	$Y = -1$	0.9141	0.0207	0.8917	✓
	$Y = 1$	0.3882	0.0785	0.5862	✓
	$Y = 2$	0.0618	0.3070	0.6373	✓
	$Y = 3$	0.7723	0.2012	0.2234	✓
	$Y = 4$	0.6247	0.2800	0.1985	✓

stitute of Standards and Technology (NIST) mandate that a secure cryptosystem must possess a minimum effective key space of $K \geq 2^{128}$. The secret key of the proposed framework consists of three decoupled entities: the chaotic initial conditions, the cryptographic hash passphrase, and the Blum Blum Shub (BBS) initialization parameters.

Chaotic Component Entropy

The Genesio–Tesi hyper-chaotic system is governed by three initial states (x_0, y_0, z_0) and three system parameters (a, b, c). Under the IEEE 754 double-precision floating-point standard, the 52-bit binary mantissa provides a computational fluctuation precision of 10^{-15} yielding an effective binary state space of 2^{52} per variable. Therefore, the chaotic key space is derived as:

$$K_{\text{chaos}} = \prod_{i=1}^{6} \left(2^{52}\right) = \left(2^{52}\right)^{6} = 2^{312} \tag{48}$$

Cryptographic Hash Passphrase (K_{SHA})

The primary user master key is passed through the SHA-512 hashing algorithm to generate the static system seed, contributing a standard structural bit-space of:

$$K_{\text{SHA}} = 2^{512} \tag{49}$$

BBS Generator Seed ($\mathbf{K_{BBS}}$)

The Blum integers $M = p \times q$ and the initial coprime seed s used to construct the permutation matrix E are instantiated via a 64-byte (512-bit) space:

$$K_{\text{BBS}} = 2^{512} \tag{50}$$

Total Effective Key Space ($\mathbf{K_{Total}}$): Since these three sub-keys are generated and updated independently inside the pipeline, the total aggregate key space is the Cartesian product of the sub-spaces:

$$K_{\text{total}} = K_{\text{chaos}} \times K_{\text{SHA}} \times K_{\text{BBS}} \tag{51}$$

$$K_{\text{total}} = 2^{312} \times 2^{512} \times 2^{512} = 2^{1336} \tag{52}$$

Comparing this against the safe cryptographic threshold $\left(2^{1336} \gg 2^{128}\right)$, the proposed framework possesses an exorbitant security margin, rendering exhaustive brute-force key search mathematically impossible.

Resistance to Related-Key and Chosen-Plaintext Attacks

A large key space offers no protection if the system exhibits high key correlation or plaintext-agnostic keying. The framework thwarts these two specific attack vectors via the following mechanisms:

Related-Key Attack (RKA) Immunity: The Genesio–Tesi system exhibits a positive maximal Lyapunov exponent. If an attacker tests a "related key" modified by the single smallest possible floating-point increment $(\Delta = 10^{-15})$, the generated keystreams X_R, X_G, X_B diverge into an entirely uncorrelated trajectory within $N \approx 35$ iterations. Consequently, the cross-correlation coefficient between ciphers generated by two closely related keys approaches zero $(\rho \approx 0.0001)$.

Chosen-Plaintext Attack (CPA) Immunity: In a standard CPA, the attacker feeds a trivial image (e.g., all black pixels) into the cipher to isolate the static keystream. In our framework, the plain image dimensions and its SHA-512 hash act as the dynamic perturbator for the BBS seed matrix E. Therefore, encrypting two plain texts that differ by only a single pixel results in two fundamentally different Compressive Sensing measurement matrices Φ and scrambling matrices E. This is quantitatively supported by our differential analysis, which records many Changing Pixel Rate (NPCR) of $> 99.60\%$ and a Unified Average Changing Intensity (UACI) of $> 33.46\%$, strictly satisfying the theoretical passing benchmarks for chosen-plaintext sensitivity.

Reconstruction algorithm and performance analysis: At the receiving end, image reconstruction is performed using the Orthogonal Matching Pursuit (OMP) algorithm, a widely used approach for recovering sparse matrix E are instantiated via a 64-byte (512-bit) space: From compressive measurements. To evaluate reconstruction performance, we analyze the Peak Signal-to-Noise Ratio (PSNR) across different compression ratios. Our experimental results indicate that:

- For a compression ratio of 50%, PSNR is around 34 dB, ensuring high visual quality.
- Even at a compression ratio of 30%, the reconstructed image retains structural integrity, with an SSIM above 0.85.
- A trade-off exists between compression ratio and reconstruction quality, but our approach balances efficiency and security effectively.

Cryptanalytic Attacks

The security of the proposed DNA–chaos–compressive image encryption scheme is evaluated against several classical and advanced cryptanalytic attacks, including statistical, differential, brute-force, and chosen-plaintext attacks. Each layer of the system—Genesio–Tesi hyperchaotic dynamics, SHA-512/BBS key expansion, DNA-based encoding, and compressive sensing—collectively ensures nonlinearity, key sensitivity, and data unpredictability. The Genesio–Tesi hyperchaotic map exhibits strong parameter sensitivity; even minimal perturbations $(\Delta x_0,\ \Delta y_0 \approx 10^{-8})$ cause significant divergence in generated sequences, leading to nearly 99.6% NPCR and 33.4% UACI variation in encrypted images, confirming its robustness against chosen-plaintext and key sensitivity attacks. The following quantitative and structural properties support its robustness:

- **Resistance to Statistical Attacks**: The encrypted images exhibit an average entropy of 7.9998 bits per pixel, close to the theoretical ideal of 8. Histogram analysis shows uniform gray-level distribution, while the correlation coefficients between adjacent pixels (horizontal, vertical, and diagonal) are all near zero ($|r| < 0.001$).These results indicate the ciphertext reveals no statistical trace of the original image structure. In comparison, algebraic SPN schemes over Gaussian and Quaternion integer rings report entropy between 7.996–7.999 and correlations of 0.002–0.006 (Alammari et al. 2025; Sajjad and Alqwaifly 2025; Sajjad et al. 2025), showing that our method achieves superior statistical diffusion.
- **Resistance to Differential Attacks:** Differential attacks evaluate how slight changes in the plaintext propagate through the encryption process. For a single-bit change in the input image, the Number of Pixels Change Rate (NPCR) and Unified Average Changing Intensity (UACI) were computed using Eq. 11 and Eq 12. Averaged over ten runs, the proposed method achieved NPCR = 99.624 $\pm$ 0.033 % and UACI = 33.422 $\pm$ 0.051 %, both very close to the ideal theoretical values (99.609 % and 33.463 % respectively). The low standard deviations confirm diffusion stability and consistent avalanche effect.
- **Resistance to Brute-force and Key-related Attacks:** The effective key length combines the 512-bit SHA-512 digest with dynamic chaotic initial conditions ($\geq$128 bits equivalent precision). The total key space exceeds 2^{640}, far beyond the computational capacity of exhaustive search. Even with high-performance GPUs performing 10^{12}trials/sec, the expected brute-force time exceeds 10^{112}years. Furthermore, the SHA-512 $\rightarrow$ BBS key expansion ensures that any small change in the passphrase or chaotic seed alters the full keystream (key sensitivity > 99.99 % measured by bit-flip ratio), eliminating weak-key or near-key vulnerabilities.
- **Resistance to Chosen-plaintext and Known-plaintext Attacks:** The compressive-sensing stage converts the image into a low-dimensional measurement vector $y = \Phi x$, effectively mixing and reducing the information space. Since $\Phi$is regenerated from key-dependent random seeds and normalized Gaussian entries, each encryption produces a statistically independent measurement space even for similar plaintexts. Moreover, DNA encoding applied to chaotic streams—not directly to pixels—ensures nonlinear mapping between input intensities and cipher outputs. As a result, two closely related plaintexts yield entirely uncorrelated ciphertexts, blocking chosen-plaintext and differential cryptanalysis. The mean ciphertext correlation between two 1-bit-different plaintexts is measured as ρ = 0.00047, confirming near-total decorrelation.
- **Resistance to Cropping and Noise Attacks:** Due to the compressive-sensing reconstruction mechanism, even when 25 %, 50 %, and 75 % of encrypted regions are occluded, the pixel-recovery rates (PRR) remain 97.82 %, 94.16 %, and 90.43 % respectively. This confirms resilience to channel damage and partial-data attacks. The layered combination of hyperchaotic diffusion, SHA-512/BBS key expansion, DNA-based nonlinear substitution, and compressive measurement reduction provides an interlocking defense structure. Each component contributes to entropy, diffusion, and key-space amplification, resulting in a scheme that is provably secure against classical, differential, and chosen-plaintext attacks under current computational constraints (see Table 11).

COMPARATIVE ANALYSIS AND DISCUSSION

The comparative analysis of the proposed approach with existing mechanisms, represented by Table 12, computes major security metrics such as the correlation coefficients (H, V, D), entropy, UACI, and NPCR. The results demonstrate the strength and excellence of the proposed approach compared to other contemporary encryption frameworks. A fundamental requirement of a strong encryption scheme is to shatter the correlation between adjacent pixels. In our proposed approach, the correlation coefficients across

Table 11 Detailed security analysis of the proposed algorithm against cryptanalytic attacks.

Attack Type	Measure	Value	Ideal	Resistance
Statistical	Entropy (bits/pixel)	7.9998	8.0000	Excellent
Statistical	Adjacent pixel corr.	< 0.001	0	Excellent
Differential	NPCR (%)	99.624 ± 0.033	99.609	Excellent
Differential	UACI (%)	33.422 ± 0.051	33.463	Excellent
Key Sensitivity	Bit-flip ratio (%)	99.99	—	Excellent
Chosen-plaintext	Cipher correlation	0.0047	≈ 0	Excellent

the horizontal (H), vertical (V), and diagonal (D) directions are 0.0005, -0.0017, and 0.0020, respectively, which are exceptionally close to zero. This signifies a complete destruction of the statistical relationships between neighboring pixels to a very large degree. Compared to alternative frameworks like those of Akkasaligar and Biradar (2020) ($H = 0.001$, $V = 0.021$, $D = 0.0187$) and Tamang et al. (2021) ($H = 0.008$, $V = 0.007$, $D = 0.0066$), which exhibit larger measures of correlation and weaker decorrelation properties, our proposed cipher shows highly superior resistance to statistical attacks.

Entropy measures the randomness of an image, with an ideal theoretical value of 8 for a 256-gray-level image. The proposed approach achieves an entropy value of 7.9998, which is remarkably close to this theoretical maximum. This indicates that the proposed method yields highly random ciphertext images with negligible structural redundancy, effectively thwarting entropy-based attacks. Conversely, other techniques such as those by Gopalakrishnan and Ramakrishnan (2019) (7.9960), Tamang et al. (2021) (7.9961), and Chidambaram et al. (2019) (7.9977) report slightly lower entropy values, indicating higher residual redundancy. The near-optimal entropy value of our scheme underscores the high level of security it introduces.

The UACI metric evaluates the rate of intensity change between two encrypted images resulting from a minimal change in the plaintext. A higher UACI value implies robust resistance against differential attacks, ensuring that minor modifications in the plaintext produce significant, widespread alterations in the ciphertext. Our scheme achieves a UACI value of 33.43%, outperforming the method by Akkasaligar and Biradar (2020) (33.29%) and performing competitively alongside the frameworks of Cheng et al. (2020) (33.64%) and Tamang et al. (2021) (33.79%). This tier of UACI confirms that our algorithm induces substantial pixel intensity variations, maximizing ciphertext protection.

Similarly, the NPCR value quantifies the percentage of altered pixels when a single-bit modification is made to the plaintext image. An elevated NPCR value—ideally reaching 100%—signifies an extensive diffusion effect. The proposed architecture establishes an NPCR value of 99.60%, which remains highly competitive with the results reported by Gopalakrishnan and Ramakrishnan (2019) (99.61%), Tamang et al. (2021) (99.68%), and Huang et al. (2014b) (99.79%). While the method of Akkasaligar and Biradar (2020) (99.87%) presents a slightly higher value, our outcome rests securely within the optimal bounds required to defend against differential cryptanalysis.

The comparative data in Table 12 clearly demonstrates that our approach excels across all primary security indices. The near-zero

Table 12 Comparative analysis of the proposed scheme with existing encryption techniques.

Method	Correlation			Entropy	UACI	NPCR
	H	V	D			
Proposed	0.0005	-0.0017	0.0020	7.9998	33.43	99.60
[21]	0.0010	0.0210	0.0187	–	33.29	99.87
[22]	0.0020	0.0030	-0.0141	7.9960	33.51	99.61
[23]	0.0080	0.0070	0.0066	7.9961	33.79	99.68
[24]	0.0040	0.0020	0.0033	7.9977	33.47	99.68
[25]	-0.0010	0.0080	-0.0002	7.9970	33.48	99.61
[26]	0.0070	0.0090	-0.0160	7.9981	33.64	99.65
[27]	0.0030	0.0090	0.0058	7.9965	33.48	99.79
[28]	-0.0010	0.0010	-0.0015	–	33.41	99.60
[30]	0.0040	-0.0040	0.0163	–	–	–
[39]	0.0060	0.0030	0.0020	7.9967	–	99.60
[41]	–	–	–	7.9986	–	99.62
[42]	–	–	–	–	33.12	99.75
[47]	-0.0098	-0.0572	-0.0238	7.9993	31.00	99.61
[48]	0.0185	-0.0462	-0.0059	7.9974	33.73	99.61

correlation metrics confirm the complete eradication of statistical dependencies, drastically minimizing vulnerability to frequency-related exploits, while the exceptionally high entropy and resilient UACI/NPCR indicators validate its security profile for real-time practical deployments. In addition to its advanced security profile, the proposed cipher retains an optimal trade-off between cryptographic strength and computational complexity, making it exceptionally well-suited for high-speed communication systems. Taken together, these experimental evaluations confirm that our approach not only intensifies image encryption security but also provides robust protection against sophisticated statistical and differential cryptanalytic threats, rendering it a highly reliable solution for secure digital communications.

CONCLUSION

In conclusion, this study has developed a new hybrid image encryption technique based on DNA coding, compressive sensing and the Genesio–Tesi hyperchaotic system in order to provide both high level of security as well as high performance. Since unlike the typical methods using DNA coding and SPNs for image encryption, which are mainly based on pixel and algebraic structures respectively, the proposed method uses DNA coding for chaotic sequence which provides better diffusion and confusion but with less redundancy. By quantitative analysis we show that the proposed method is highly resistant to attacks since the average information entropy values of the encrypted images reach almost the highest value (i.e., ~7.9998), which means the images are nearly completely random; the correlation coefficients between two adjacent pixels are almost zero, which means there is no relationship between them; and the NPCR/UACI values of the proposed method are around 99.6%/33.4%, which indicates that it resists against differential attack. Also, our method exhibits high quality decrypted images with PSNR greater than 32dB and SSIM greater than 0.92 when the compression ratio is reasonable, and therefore it can be used in practice for secure transmitting images in real time. From comparison with other algebraic SPN models, it can be seen that although algebraic SPN models can provide confusion-diffusion

balance using structured residue ring arithmetic, they cannot perform compression adaptability and have relatively higher computational load. Compared with the above mentioned algebraic SPN models, the proposed DNA-chaos-compressive model can get similar or even better security indicators at the same time reduce the cipher text size by up to 50%.

Therefore, this advantage is very important especially for big-size multimedia systems and IoT applications. However, like all techniques, there are still some disadvantages. During the decoding process, the Orthogonal Matching Pursuit algorithm will introduce some additional computational complexity. At the same time, different parameters settings of the hyperchaotic system will affect its convergence speed. Therefore, how to optimize these parameters settings should be one of next steps. For example, by applying adaptive compressive sensing technology to improve the efficiency of reconstructing the original images and designing parallel algorithms to accelerate the solving process of the OMP solver. Another potential area for improvement includes utilizing deep learning technologies to develop an intelligent decoding strategy. To further strengthen the structure of the proposed model, we could integrate algebraic SPN modules into complex integer ring spaces (e.g., Gaussian ring, Quaternion ring, Eisenstein ring) so as to obtain algebraic-hyperchaotic hybrid models with algebraically structured security mechanisms and temporally continuous chaos characteristics. The long-term development direction of this project also includes studying the feasibility of integrating QKD technology into our model to make it more post-quantum secure and implementing our model onto FPGAs to evaluate whether it can meet the requirements of real-time processing in various applications including embedded systems and medical image processing.

Conflicts of interest

The authors declare that there is no conflict of interest regarding the publication of this paper.

Ethical standard

The authors have no relevant financial or non-financial interests to disclose.

Data Availability Statement

The datasets used and/or analyzed during the current study are available from the corresponding author on reasonable request.

Funding Statement

The authors extend their appreciation to Prince Sattam bin Abdulaziz University for funding this research work through the project number (PSAU/2025/01/33903).

LITERATURE CITED

National Institute of Standards and Technology, 1999 Data encryption standard. *Federal Information Processing Standards Publication* **112**.

Rijmen, V. and J. Daemen, 2001 Advanced encryption standard. *Proceedings of Federal Information Processing Standards Publications, National Institute of Standards and Technology*, 19–22.

Barker, E. and N. Mouha, 2017 Recommendation for the triple data encryption algorithm (TDEA) block cipher. *NIST Special Publication (SP) 800-67 Rev. 2 (Draft), National Institute of Standards and Technology*.

Chang, H.-S., 2004 International data encryption algorithm. *JMU Fall Technical Report*.

Vidhya, R. and M. Brindha, 2020 A novel conditional butterfly network topology based chaotic image encryption. *Journal of Information Security and Applications* **52**: 102484.

Li, C., G. Luo, K. Qin, and C. Li, 2017 An image encryption scheme based on chaotic tent map. *Nonlinear Dynamics* **87**: 127–133.

Ponuma, R. and R. Amutha, 2018 Compressive sensing based image compression-encryption using novel 1D-chaotic map. *Multimedia Tools and Applications* **77**: 19209–19234.

Chai, X., Z. Gan, Y. Chen, and Y. Zhang, 2017 A visually secure image encryption scheme based on compressive sensing. *Signal Processing* **134**: 35–51.

Yu, J., S. Guo, X. Song, Y. Xie, and E. Wang, 2020 Image parallel encryption technology based on sequence generator and chaotic measurement matrix. *Entropy* **22**: 76.

Wang, X., Y. Su, L. Liu, H. Zhang, and S. Di, 2021 Color image encryption algorithm based on Fisher-Yates scrambling and DNA subsequence operation. *The Visual Computer*, 1–16.

Xu, Q., K. Sun, S. He, and C. Zhu, 2020 An effective image encryption algorithm based on compressive sensing and 2D-SLIM. *Optics and Lasers in Engineering* **134**: 106178.

Luo, Y., J. Lin, J. Liu, D. Wei, L. Cao, R. Zhou, Y. Cao, and X. Ding, 2019 A robust image encryption algorithm based on Chua's circuit and compressive sensing. *Signal Processing* **161**: 227–247.

Huang, R., K. H. Rhee, and S. Uchida, 2014 A parallel image encryption method based on compressive sensing. *Multimedia Tools and Applications* **72**: 71–93.

Ye, G., C. Pan, Y. Dong, Y. Shi, and X. Huang, 2020 Image encryption and hiding algorithm based on compressive sensing and random numbers insertion. *Signal Processing* **172**: 107563.

Brahim, A. H., A. A. Pacha, and N. H. Said, 2020 Image encryption based on compressive sensing and chaos systems. *Optics & Laser Technology* **132**: 106489.

Gong, L., K. Qiu, C. Deng, and N. Zhou, 2019 An optical image compression and encryption scheme based on compressive sensing and RSA algorithm. *Optics and Lasers in Engineering* **121**: 169–180.

Li, Z., C. Peng, W. Tan, and L. Li, 2021 An efficient plaintext-related chaotic image encryption scheme based on compressive sensing. *Sensors* **21**: 758.

Qayyum, A., J. Ahmad, W. Boulila, S. Rubaiee, F. Masood, F. Khan, and W. J. Buchanan, 2020 Chaos-based confusion and diffusion of image pixels using dynamic substitution. *IEEE Access* **8**: 140876–140895.

Zhu, Z., Y. Song, W. Zhang, H. Yu, and Y. Zhao, 2020 A novel compressive sensing-based framework for image compression-encryption with S-box. *Multimedia Tools and Applications* **79**: 25497–25533.

Lin, J., Y. Luo, J. Liu, J. Bi, S. Qiu, M. Cen, and Z. Liao, 2018 An image compression-encryption algorithm based on cellular neural network and compressive sensing. In *Proceedings of 2018 IEEE 3rd International Conference on Image, Vision and Computing (ICIVC)*, pp. 673–677.

Akkasaligar, P. T. and S. Biradar, 2020 Selective medical image encryption using DNA cryptography. *Information Security Journal: A Global Perspective* **29**: 91–101.

Gopalakrishnan, T. and S. Ramakrishnan, 2019 Image encryption using hyper-chaotic map for permutation and diffusion by multiple hyper-chaotic maps. *Wireless Personal Communications* **109**: 437–454.

Tamang, J., J. D. D. Nkapkop, M. F. Ijaz, P. K. Prasad, N. Tsafack, A. Saha, J. Kengne, and Y. Son, 2021 Dynamical properties of ion-acoustic waves in space plasma and its application to image

encryption. *IEEE Access* **9**: 18762–18782.
Chidambaram, N., P. Raj, K. Thenmozhi, S. Rajagopalan, and R. Amirtharajan, 2019 A cloud compatible DNA coded security solution for multimedia file sharing & storage. *Multimedia Tools and Applications* **78**: 33837–33863.
Kumar, V. and A. Girdhar, 2021 A 2D logistic map and Lorenz-Rossler chaotic system based RGB image encryption approach. *Multimedia Tools and Applications* **80**: 3749–3773.
Cheng, G., C. Wang, and C. Xu, 2020 A novel hyper-chaotic image encryption scheme based on quantum genetic algorithm and compressive sensing. *Multimedia Tools and Applications* **79**: 29243–29263.
Huang, R., K. H. Rhee, and S. Uchida, 2014 A parallel image encryption method based on compressive sensing. *Multimedia Tools and Applications* **72**: 71–93.
Zhu, L., H. Song, X. Zhang, M. Yan, L. Zhang, and T. Yan, 2019 A novel image encryption scheme based on nonuniform sampling in block compressive sensing. *IEEE Access* **7**: 22161–22174.
Wang, H., D. Xiao, M. Li, Y. Xiang, and X. Li, 2019 A visually secure image encryption scheme based on parallel compressive sensing. *Signal Processing* **155**: 218–232.
Chai, X., J. Bi, Z. Gan, X. Liu, Y. Zhang, and Y. Chen, 2020 Color image compression and encryption scheme based on compressive sensing and double random encryption strategy. *Signal Processing* **176**: 107684.
Gearheart, C. M., B. Arazi, and E. C. Rouchka, 2010 DNA-based random number generation in security circuitry. *Biosystems* **100**: 208–214.
Genesio, R. and A. Tesi, 1992 Harmonic balance methods for the analysis of chaotic dynamics in nonlinear systems. *Automatica* **28**: 503–514.
Cardona-López, M. A., J. C. Chimal-Eguía, V. M. Silva-García, and R. Flores-Carapia, 2024 Statistical analysis of the negative–positive transformation in image encryption. *Mathematics* **12**: 908.
Alghafis, A., N. Munir, and M. Khan, 2021 An encryption scheme based on chaotic Rabinovich-Fabrikant system and S_8 confusion component. *Multimedia Tools and Applications* **80**: 7967–7985.
Tariq, S., M. Khan, A. Alghafis, and M. Amin, 2020 A novel hybrid encryption scheme based on chaotic Lorenz system and logarithmic key generation. *Multimedia Tools and Applications* **79**: 23507–23529.
Waseem, H. M. and M. Khan, 2018 Information confidentiality using quantum spinning, rotation and finite state machine. *International Journal of Theoretical Physics* **57**: 3584–3594.
Xu, Q., K. Sun, S. He, and C. Zhu, 2020 An effective image encryption algorithm based on compressive sensing and 2D-SLIM. *Optics and Lasers in Engineering* **134**: 106178.
Rahul, B., K. Kuppusamy, and A. Senthilrajan, 2023 Dynamic DNA cryptography-based image encryption scheme using multiple chaotic maps and SHA-256 hash function. *Optik* **289**: 171253.
Wen, H., L. Yang, C. Bai, Y. Lin, T. Liu, L. Chen, *et al.*, 2024 Exploiting high-quality reconstruction image encryption strategy by optimized orthogonal compressive sensing. *Scientific Reports* **14**: 8805.
Pourasad, Y., R. Ranjbarzadeh, and A. Mardani, 2021 A new algorithm for digital image encryption based on chaos theory. *Entropy* **23**: 341.
Rahul, B., K. Kuppusamy, and A. Senthilrajan, 2023 Dynamic DNA cryptography-based image encryption scheme using multiple chaotic maps and SHA-256 hash function. *Optik* **289**: 171253.
Luo, Y., Y. Liang, S. Zhang, Junxiu Liu, and F. Wang, 2023 An image encryption scheme based on block compressed sensing and Chen's system. *Nonlinear Dynamics* **111**: 6791–6811.
Chai, X., J. Bi, Z. Gan, X. Liu, Y. Zhang, and Y. Chen, 2020 Color image compression and encryption scheme based on compressive sensing and double random encryption strategy. *Signal Processing* **176**: 107684.
Qureshi, M. A., N. A. Khan, S. Raza, and S. M. Z. Iqbal, 2024 Cap like trajectories in 5D chaotic tangent hyperbolic memristive model: fractional calculus and encryption. *Physica Scripta* **99**: 075238.
Yan, S., D. Jiang, H. Zhang, Y. Zhang, Yu Cui, and L. Li, 2023 A new fractional-order 5D memristive chaotic system with special extreme multistability and its application to image encryption. *Physica Scripta* **98**: 125234.
Qureshi, M. A. and N. A. Khan, 2024 Clown face in 3D chaotic system integrated with memristor electronics, DNA encryption and fractional calculus. *The European Physical Journal B* **97**: 63.
Alammari, M., M. Sajjad, M. K. Abdalrahem, and R. J. Serna, 2025 Multiple RGB images security based on substitution–permutation network over the residue classes of Eisenstein integer $\mathbb{Z}[\Omega]\pi$. *European Journal of Pure and Applied Mathematics* **18**: 6470.
Sajjad, M. and N. A. Alqwaifly, 2025 A novel RGB image encryption scheme using operations on residue classes of Eisenstein integers $\mathbb{Z}[\omega]\pi$. *European Journal of Pure and Applied Mathematics* **18**: 6323.
Sajjad, M., T. Shah, R. Hamza, B. Almutairi, and R. J. Serna, 2025 Multiple color images security by SPN over the residue classes of Gaussian integer. *Scientific Reports* **15**: 6425.
Khanday, M. A., A. Rafiq, and K. Nazir, 2017 Mathematical models for drug diffusion through the compartments of blood and tissue medium. *Alexandria Journal of Medicine* **53**: 245–249.

How to cite this article: Yildirim, A., and Yildirim, N. From Immune-Cold to Immune-Hot Tumors: A Fractional Immunomodulation Framework with Topological Signatures. *Chaos Theory and Applications*, 8(2), 117–134, 2026.