International Journal of Computational Intelligence in Engineering (IJCIE)
Vol. 01, No. 03, May 2026, pp. 1-13
ISSN: XXXX-XXXX, DOI: 10.5281/zenodo.19977269

Hybrid Chaotic-DNA Cryptosystem With Galois Field Diffusion For Secure Color Image Encryption

M Krishna Prasad[1*], Aadishesh Gopal Padasalgi[2], Chandrappa S[3], Manjunath Sargur Krishnamurthy[4], Sagar Basavaraju[5]

[1]Dept. of AIML, BMS Institute of Technology and Management, Bengaluru, India. Email: krishnamuralimk08@gmail.com
[2]Dept. of AIML, BMS Institute of Technology and Management, Bengaluru, India. Email: aadishesh05@gmail.com
[3]Dept. of CSE (Data Science), Nagarjuna College of Engineering and Technology, Bengaluru, India. Email: chandrucs21@gmail.com
[4]JP Morgan & Chase Co., Houston, USA. Email: manjunath.skmurthy@yahoo.com
[5]Department of ECE, Amrita School of Engineering, Amrita Vishwa Vidyapeetham, India. Email: b_sagar@blr.amrita.edu

Article Info

Article history:

Received Feb 26, 2026
Revised Apr 25, 2026
Accepted Apr 30, 2026

Keywords:

Chaotic Maps
DNA Cryptography
Color Image Encryption
Galois Field
Pixel Scrambling
Information Entropy
Image Security

ABSTRACT

Security issues in digital image transmission have become an important concern in multimedia communication. Because of their large image data volume, high redundancy and strong correlation among the neighboring pixels, the conventional encryption algorithms are not suitable for practical image encryption. In this paper, a chaotic color image encryption scheme based on Deoxyribonucleic Acid (DNA) coding calculation, multiplication arithmetic over the Galois field GF(17) and improved one-dimensional (1D) chaotic maps is presented. To address the limitations of classical 1D maps, including a narrow chaotic range and non-uniformity, three modified 1D chaotic maps, namely, Sine-Logistic Map (SLM), Chebyshev-Logistic Map (CLM) and Sine-Chebyshev Map (SCM) have been proposed. Furthermore, the chaotic initial values are modified using the plain image (the input color image is decomposed into Red, Green and Blue (R, G and B) planes, and bit-plane recombination is carried out), which makes it possible to defend against chosen-plaintext and known-plaintext attacks. In this scheme, the image pixels are first scrambled using chaotic sequences, and then DNA coding is applied. After DNA coding, DNA arithmetic operations are performed, and then DNA decoding is applied. In order to further diffuse the pixels, multiplication over GF(17) is applied. Security analysis, including histogram uniformity, information entropy, and inter-pixel correlation coefficients, demonstrates that the proposed scheme is secure.

This is an open access article under the CC BY-SA license.

Corresponding Author:

M Krishna Prasad
Dept. of AIML, BMS Institute of Technology and Management, Bengaluru, India.
Email: krishnamuralimk08@gmail.com

1. INTRODUCTION

Among all the types of data transited within current computer networks, digital images are considered one of the most frequently transported data types that find indispensable applications in modern scenarios, for instance in remote medical diagnosis, defense intelligence, e-commerce, and social networking. The increased flow of image data across open, unsecure channels requires efficient, effective image protection mechanisms as a critical research subject. Unlike text data, images have certain unique features, such as large data volume, high redundancy, and strong spatial correlation between adjacent pixels that make traditional cryptography techniques, for instance, DES and RSA, inappropriate for encrypting image data directly [1].

Image encryption aims to produce a meaningless cipher-text of visually meaningful images such that when presented to unauthorized parties, it looks like noise and can be decrypted to recover the original image perfectly

using the secret key only by authorized users [2]. Amongst all the techniques proposed in the literature for image encryption, chaotic methods gained widespread interest due to the chaotic properties such as sensitive dependence on initial condition, pseudo randomness, deterministic non-periodic behaviour and ergodicity [3].

While the chaotic maps of lower dimension such as logistic, Sine, Chebyshev variants are not complicated and are easier to implement in software or hardware environments, their security is still somewhat problematic because they have a limited range for their chaotic parameters and the distribution of outputs is not uniform, which leads to exploitable security flaws [2]. Higher dimensional chaotic maps could circumvent the limitation in terms of some security concerns by increasing their complexity and therefore consuming more computational cost [1].

DNA-based cryptography adds more dimension of security through using inherent enormous parallelism and information density of nucleic acid codes [4]. By encoding pixel values as DNA base sequences and performing the algebraic operations on DNA sequence level, we can achieve efficient diffusion and confusion. The Galois field arithmetic offers an exact algebraic method for pixel diffusion which is computationally unfeasible to be reversed without the possession of The secret key [5].

The present paper provides a chaotic color image encryption scheme which integrates three improved 1D chaotic maps, DNA computation and Galois field multiplication. The main technical contributions are as follows:

- A bit-plane recombination strategy links chaotic map initial values to the plaintext so that the proposed algorithm can prevent the chosen-plaintext and known-plaintext attack.
- The chaotic maps SLM, CLM and SCM are designed by transforming the traditional Logistic map, Sine map and Chebyshev map so that they own broader chaotic range and higher ergodicity.
- The DNA encoding and arithmetic combined with the Galois field multiplication based on GF(17) provide better confusion and diffusion performance together.
- Rigorous security analyses including histogram uniformity, pixel correlation and information entropy of the proposed encryption scheme are given to demonstrate its robustness.

The rest of the paper is organized as follows. The related works are reviewed in Section 2. Relevant theories are introduced in Section 3. The proposed method is described in Section 4. The experimental results and security analysis are demonstrated in Section 5. The conclusion is drawn in Section 6.

2. LITERATURE REVIEW

From the research published by Fridrich [6], the work of chaos in image encryption has been extensively studied. In recent 10 years, some authors have already used hybrid chaotic map, DNA and algebraic structure to improve the strength of image encryption scheme. Representative literatures and the problem solved by the proposed scheme are introduced as follows.

Bahri-Laleh et al. [7] proposed a stream cipher for RGB image encryption, where a Keystream generated by Particle Swarm Optimisation (PSO) algorithm is applied. The scheme has an acceptable encrypting speed but the histogram of the cipher image is not quite flat; hence the randomness is relatively poor. Fu et al. [8] designed a scheme based on hyperchaotic Lu system and logistic map with joint permutation and substitution. It reduces the number of iterations to one third by employing an efficient keystream extraction method, but shows a weakness to differential attack. Hua et al. [9] propose a 2D Sine Logistic Modulation Map (2D-SLMM) with excellent ergodicity and wider chaos interval, in combination with a Chaotic Magic Transform (CMT). However, it shows vulnerability to chosen-plaintext attack. Wu et al. [1] have successfully used two-dimensional logistic chaotic map for permutation-substitution, it offers both confusion and diffusion, but at much more cost of computing speed.

Chai et al. [4] merged a 2D logistic chaotic map and DNA sequence operations to give pixel-level diffusion in which the eight kinds of DNA coding rules were used. However, using only one logistic map has a limitation for randomness. Huang et al. [5] suggested a scheme quite similar to that proposed here, using an enhanced 1D chaotic map and combined with DNA coding and arithmetic in Galois field. The paper has good statistical analysis, but using multiplication in Galois field caused a problem on decryption because the original image information was lost when zero-pixels were formed, this problem is discussed in this paper. A summary comparison of representative methods is presented in Table 1.

Table 1. Comparison of representative image encryption methods

Ref.	Year	Method	Dataset	Key Contribution	Limitation
[2]	2024	FL Survey	Multi-modal	Comprehensive FL review	No implementation
[3]	2024	FL + CNN	MRI	High accuracy brain tumor classification	Not communication-efficient
[4]	2024	Adaptive FL	Wireless networks	Bandwidth-aware training	Limited validation
[9]	2026	FeTTL	Multi-institution	Handles domain shift	High model complexity
[6]	2023	Blockchain FL	Medical IoMT	Secure data sharing	Increased latency
[10]	2023	Personalized FL	Medical imaging	Handles heterogeneity	Limited CT focus
[11]	2024	Edge FL	Healthcare IoT	Low latency processing	Resource constraints
[12]	2025	Teacher-Student FL	CT	Semi-supervised tumor detection	High computation cost
[13]	2024	FL + Transfer Learning	CT/MRI	Improved accuracy using pretrained models	High communication cost
[14]	2025	KD-based FL	CT	Reduced communication rounds	Complex architecture
[15]	2025	Benchmark FL	Multi-dataset	Comparative eval. of FL methods	No unified solution
[16]	2025	One-shot FL	Medical images	Single-round communication	Limited scalability
[17]	2025	FedGIN	CT/MRI	Multimodal generalization	Focus on segmentation
[18]	2022	FedAvg baseline	General	Standard FL method	High comm. cost
[19]	2023	FedProx	Non-IID data	Improved convergence	Still comm.-heavy

3. THEORETICAL BACKGROUND

3.1 Cryptography Fundamentals

Cryptography is the study of secret writing that deals with methods to protect information from unauthorized parties by using an encryption algorithm and a secret key that can restore an encrypted ciphertext back into plaintext [10]. There are 3 fundamental properties which modern cryptosystems use, these are, confidentiality where sensitive information is prevented from being accessed, integrity where information cannot be modified and authenticity where the identity of those sending and receiving information can be validated.

Cryptosystems are typically split into 2 main categories of cryptosystem, which are, symmetric (single-key) and asymmetric (public-key). A symmetric cryptosystem has an identical key used to encrypt and decrypt a message. Common symmetric algorithms include DES, Triple-DES, and AES. A public key cryptosystem uses a mathematically associated pair of keys that are, unfortunately too computationally expensive for bulk image encryption and are known as RSA and Elliptic Curve Cryptography.

3.1.1 Multiplication over the Galois Field $GF(17)$

A Galois field $GF(p)$ (for a prime p) consists of additions, subtractions, multiplications and divisions and can thus be used to build diffusion layers for cryptosystems [5]. The presented design uses $GF(17)$. Given an 8-bit pixel value, the upper and lower four bits are divided and transformed from[0, 15] to [1, 16] before applying the lookup table, so:

$$T = (0:16)^{\mathrm{T}} \times (0:16) \ mod \ 17$$

where $(\cdot)^{\mathrm{T}}$ denotes sequence transposition. The diffusion effect of GF(17) multiplication on pixel values is more prominent than that of simple XOR or addition operations.

3.2 Chaotic Cryptography

Chaotic systems are deterministically designed but they are extremely sensitive to initial conditions and the generated sequences of outputs are computationally indistinguishable from random noise [8]. The characteristics above are similar to the confusion and diffusion properties that a secure cipher requires [6]. One-dimensional chaotic maps are desirable for image encryption due to low implementation complexity. However, a major drawback of classic 1D maps is that the range over which chaos is generated is too small and its output distribution is non-uniform.

3.2.1 Classical 1D Chaotic Maps

Logistic Map: The logistic map is defined as:

$$X_{\{k+1\}} = F_{L(\mu,X_k)} = \mu X_{k(1-X_k)}$$

where $\mu \in [0, 4]$. The map enters a fully chaotic regime only as $\mu \to 4$, leaving a narrow and non-uniform chaotic range.

Sine Map: The sine map is expressed as:

$$X_{\{k+1\}} = F_{S(r,X_k)} = r \sin(\pi X_k)$$

where $r \in [0, 1]$. Chaos emerges only when r approaches 1, and the distribution is similarly non-uniform.

Chebyshev Map: The Chebyshev map is defined as:

$$X_{\{k+1\}} = F_{C(u,X_k)} = \cos(u \arccos X_k)$$

where u ∈ ℕ. A chaotic state is reached only when $u > 2$, and prominent blank areas exist within $[1, 2]$.

3.2.2 Modified 1D Chaotic Maps

To overcome the deficiencies of classical 1D maps, three modified maps are proposed using a modulation coupling framework with $f(n) = 2^n$, $10 \leq n \leq 20$.

Sine-Logistic Map (SLM):

$$X_{\{k+1\}} = f(n)\left[F_{S(r^1,X_k)} + F_{L(2r^1,X_k)}\right] - \left\lfloor f(n)\left[F_{S(r^1,X_k)} + F_{L(2r^1,X_k)}\right]\right\rfloor$$

Chebyshev-Logistic Map (CLM):

$$X_{\{k+1\}} = f(n)\left[F_{C(r^2,X_k)} + F_{L(2r^2,X_k)}\right] - \left\lfloor f(n)\left[F_{C(r^2,X_k)} + F_{L(2r^2,X_k)}\right]\right\rfloor$$

Sine-Chebyshev Map (SCM):

$$X_{\{k+1\}} = f(n)\left[F_{S(r^3,X_k)} + F_{C(2r^3,X_k)}\right] - \left\lfloor f(n)\left[F_{S(r^3,X_k)} + F_{C(2r^3,X_k)}\right]\right\rfloor$$

In Equations (5)-(7), the floor operation $\lfloor \cdot \rfloor$ confines the output to [0, 1). Bifurcation parameters r_1, $r_2 \in [0, 15]$ and $r_3 \in (0, 15]$ provide an expanded parameter space relative to the classical maps.

3.3 DNA Cryptography

DNA cryptography uses the four bases of DNA - Adenine(A), Guanine(G), Cytosine(C) and Thymine(T) for representing binary data and performing algebraic operations. The 2-bit values are mapped to bases according to a scheme based on the Watson-Crick complementary pairing rule (A-T and C-G) of DNA bases. There are 8 possible rules of coding between the two bit values and the 4 DNA bases [11]. An 8 bit pixel value can be split in to four 2-bit values and each is then represented as a DNA base. A binary value, such as 10 (decimal 2), represented in two bits, can then be translated in to two different bases using two possible rules depending on if the bit pair has an odd number of 1's or even number of 1's etc. Operations of addition, subtraction, XOR, is also performed using the DNA base alphabet and is compatible with the binary values.

Table 2. DNA coding and decoding rules (partial)

	1	2	3	4	5	6	7	8
A	00	00	11	11	01	10	01	10
T	11	11	00	00	10	01	10	01
C	10	01	10	01	00	00	11	11
G	01	10	01	10	11	11	00	00

4. METHODOLOGY

4.1 System Overview

The suggested scheme encrypts a colored plain image of m x n, using a set of security keys comprising bifurcation parameters (r1, r2, r3) and the initial states (X10, X20, X30) for SLM, CLM and SCM respectively. A cipher image with same spatial dimension m x n is generated. The flow of the whole encryption process is shown in Fig.1

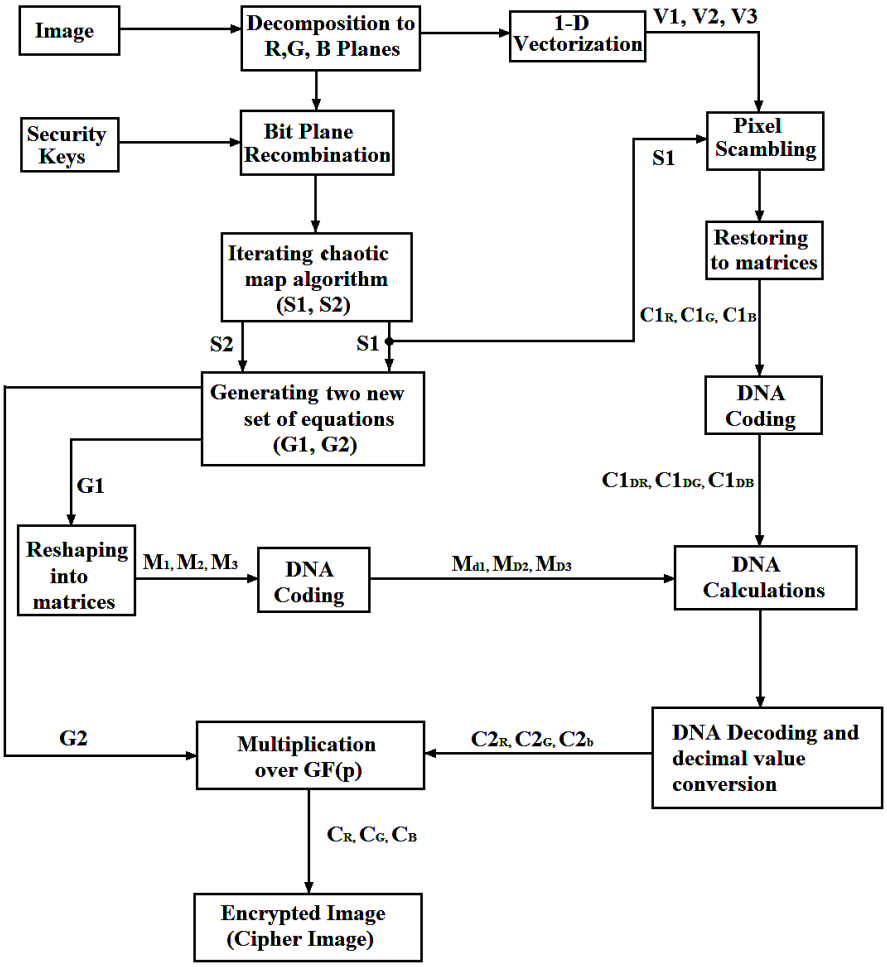


Fig. 1. Block diagram of the proposed encryption algorithm

4.2 Encryption Scheme

4.2.1 Image Decomposition and Bit-Plane Recombination

Initially the color input image is segregated into the three component matrices that define the Red (R), Green (G) and Blue (B) channels respectively. This is then decomposed into bit planes, but only those at odd positions are retained. Each of the three chaotic map initial conditions are then altered using statistics gathered from the odd bit planes:

$$X'^{10} = X^{10} + \frac{\Sigma R_{odd(x,y)}}{(255 \cdot n^2)}$$

$$X'^{20} = X^{20} + \frac{\Sigma G_{odd(x,y)}}{(5 \cdot n^2 \cdot n^2)}$$

$$X'^{30} = X^{30} + \frac{\Sigma B_{odd(x,y)}}{(5 \cdot n^2 \cdot n^2)}$$

This dependency between the plain image and the chaotic starting conditions guarantees that each distinct image generates a unique keystream, thereby providing built-in resistance against both chosen-plaintext and known-plaintext attack scenarios.

4.2.2 Generation of Chaotic Sequences

Two independent chaotic sequence sets, S_1 and S_2, are produced by running SLM, CLM, and SCM forward from their updated initial values. Each map is iterated for 2mn + 500 steps; the initial 500 output values are discarded

to eliminate transient initialization effects. Integer-valued sequences G_1 and G_2 are subsequently derived as follows:

$$\hat{X}^1_{c(i)} = fix\left(X^1_{c(i)} \times 10^4\right) mod\ 256, \qquad c \in \{R, G, B\}$$
$$\hat{X}^2_{c(i)} = fix\left(X^2_{c(i)} \times 2^{16}\right) mod\ 256, \qquad c \in \{R, G, B\}$$

4.2.3 Pixel Scrambling

Each channel matrix is vectorised into a 1D array and pixel positions are permuted using S_1:

$$\tilde{X}^1_{c(i)} = \left(\left\lfloor X^1_{c(i)} + 50 \right\rfloor \times 10^{12}\right) mod\ (mn) + 1$$
$$V_{c(i)} = V_{c\left(\tilde{X}^1_{c(i)}\right)}, \quad c \in \{R, G, B\}$$

The scrambled vectors are restored to m × n matrices C_1R, C_1G, C_1B.

4.2.4 DNA Computations

Both $\{C^1R, C^1G, C^1B\}$ and $\{M_1, M_2, M_3\}$ (reshaped from G_1) are encoded using DNA Rule 1. The resulting coded matrices undergo a mode-selected DNA arithmetic operation determined by:

$$\bar{X}^{11}(i) = \lceil X^{11}(i) \times 10^4 \rceil mod\ 3$$
$$E_D = C_D + M_D\ if\ \bar{X}^{11}(i) = 0;\ C_D - M_D\ if\ = 1;\ C_D \oplus M_D\ if\ = 2$$

DNA decoding uses a rule determined by:

$$\bar{X}^{12}(i) = \lceil X^{12}(i) \times 10^4 \rceil mod\ 8 + 1$$

The decoded binary values are converted to decimal matrices C_2R, C_2G, C_2B.

4.2.5 Multiplication over GF(17)

To further strengthen the encryption, $GF(17)$ multiplication is applied sequentially using sequences derived from G_2. Let $\otimes$ denote $GF(17)$ multiplication via the lookup table (Table 3):

$$CE_{c(i)} = CE_{c(i-1)} \otimes \hat{X}^1_{c(i)} \otimes C^2c(i)$$
$$C_{c(i)} = CE_{c(i-1)} \otimes \hat{X}^2_{c(i)} \otimes CE_{c(i)}, \qquad c \in \{R, G, B\}$$

The three resulting channel components C_R, C_G, and C_B are merged to form the final cipher image.

Table 3. GF(17) multiplication lookup table

×	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
2	0	2	4	6	8	10	12	14	16	1	3	5	7	9	11	13	15
3	0	3	6	9	12	15	1	4	7	10	13	16	2	5	8	11	14
4	0	4	8	12	16	3	7	11	15	2	6	10	14	1	5	9	13
5	0	5	10	15	3	8	13	1	6	11	16	4	9	14	2	7	12
6	0	6	12	1	7	13	2	8	14	3	9	15	4	10	16	5	11
7	0	7	14	4	11	1	8	15	5	12	2	9	16	6	13	3	10
8	0	8	16	7	15	6	14	5	13	4	12	3	11	2	10	1	9
9	0	9	1	10	2	11	3	12	4	13	5	14	6	15	7	16	8
10	0	10	3	13	6	16	9	2	12	5	15	8	1	11	4	14	7
11	0	11	5	16	10	4	15	9	3	14	8	2	13	7	1	12	6
12	0	12	7	2	14	9	4	16	11	6	1	13	8	3	15	10	5
13	0	13	9	5	1	14	10	6	2	15	11	7	3	16	12	8	4
14	0	14	11	8	5	2	16	13	10	7	4	1	15	12	9	6	3
15	0	15	13	11	9	7	4	2	1	16	14	12	10	8	6	4	2
16	0	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1

4.3 Proposed Encryption Algorithm

Algorithm 1: Chaotic Color Image Encryption

Input:

- Color plain image I $(m \times n)$;
- keys $(r_1, r_2, r_3, X_{10}, X_{20}, X_{30})$

Output:

- Cipher image $I_c(m \times n)$

Step 1: Decompose I into R, G, B matrices
Step 2: Bit-plane slice each channel; retain odd planes
Step 3: Update initial values via Eqs. (8)–(10)
Step 4: Iterate SLM, CLM, SCM for 2mn+500 steps; discard first 500
Step 5: Extract S_1, S_2; compute G_1 (Eq. 11), G_2 (Eq. 12)
Step 6: Reshape $G_1 \rightarrow M_1, M_2, M_3$
Step 7: Vectorise $R, G, B \rightarrow V_1, V_2, V_3$
Step 8: Scramble positions via Eqs. (13)-(14)
Step 9: $Restore \rightarrow C_1R, C_1G, C_1B$
Step 10: DNA Rule-1 encode $\{C_1R, C_1G, C_1B\}$ and $\{M_1, M_2, M_3\}$
Step 11: Mode-selected DNA arithmetic (Eqs. 15–16)
Step 12: Decode via Eq. (17); $convert \rightarrow C_2R, C_2G, C_2B$
Step 13: $GF(17)$ multiplication via Eqs. (18)-(19) $\rightarrow C_R, C_G, C_B$
Step 14: Merge $C_R, C_G, C_B \rightarrow I_c$
Step 15: Return I_c

4.4 Decryption Scheme

The decryption follows the reverse process of the encryption as well, and used the same key values. The calculation of multiplicative inverses in GF(17) is done first, and then DNA encoded and inverse arithmetic using reverse operation mode as

$$E_D = C_D - M_D \; if \; \bar{X}^{11}(i) = 0; \;\; C_D + M_D \; if \; = 1; \;\; C_D \oplus M_D \; if \; = 2$$

Pixel unscrambling then recovers the original RGB planes. The decryption block diagram is shown in Fig. 2.

4.5 Software Implementation

The proposed scheme was implemented in Python 3.7 using NumPy (v1.14.5) for matrix operations and chaotic sequence generation, Matplotlib (v3.0.3) for visualisation, and OpenCV-Python for image I/O. The GF(17) multiplication was realised via a pre-computed 17×17 lookup table to reduce runtime overhead.

5. RESULTS AND DISCUSSION

Three widely known color benchmark images, which were Lena, Mandrill and Nature with the spatial dimension of 256×256, were empirically evaluated. There were two cases of experiments performed; (i) encrypt with the operation of multiplication of GF(17) enabled and (ii) encrypt with the operation of multiplication of GF(17) disabled, to see the impact of the GF stage only.

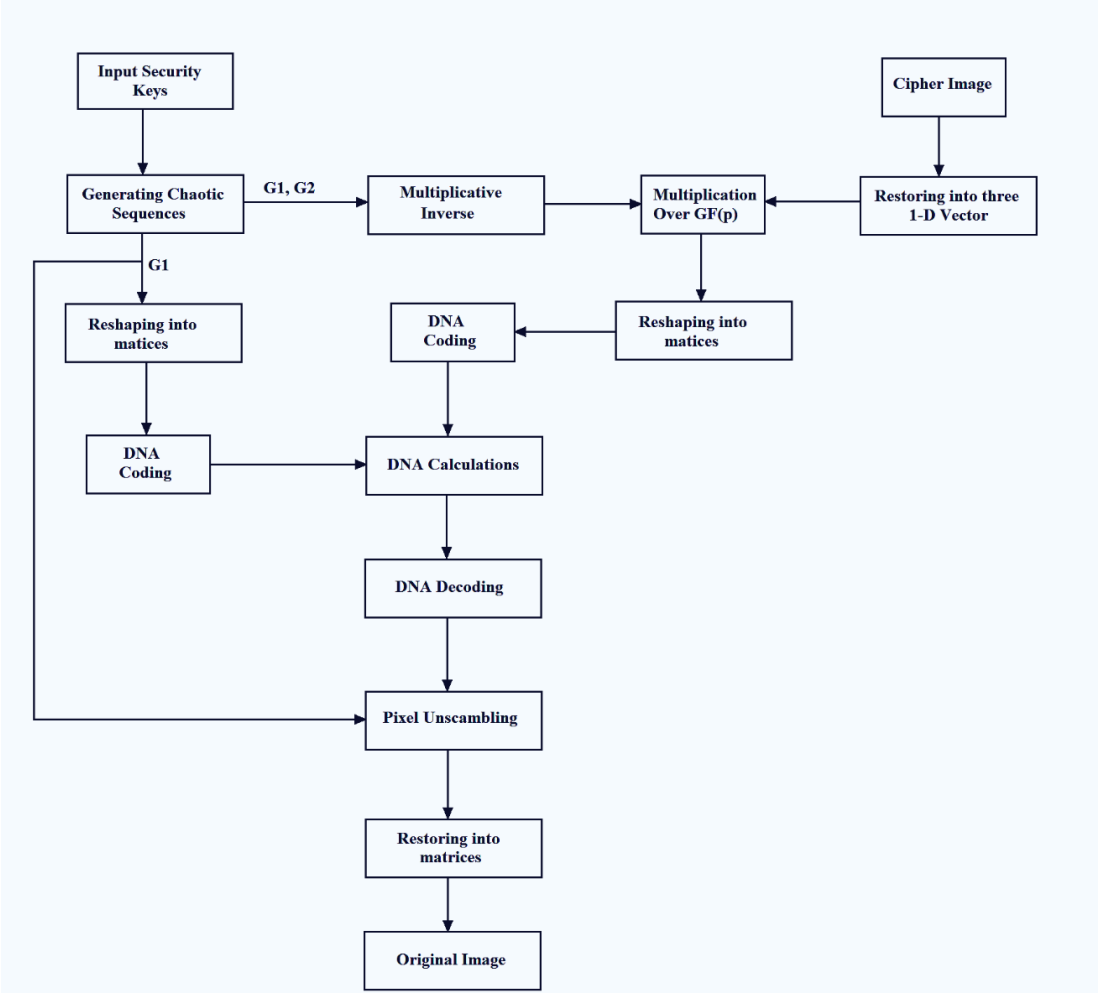
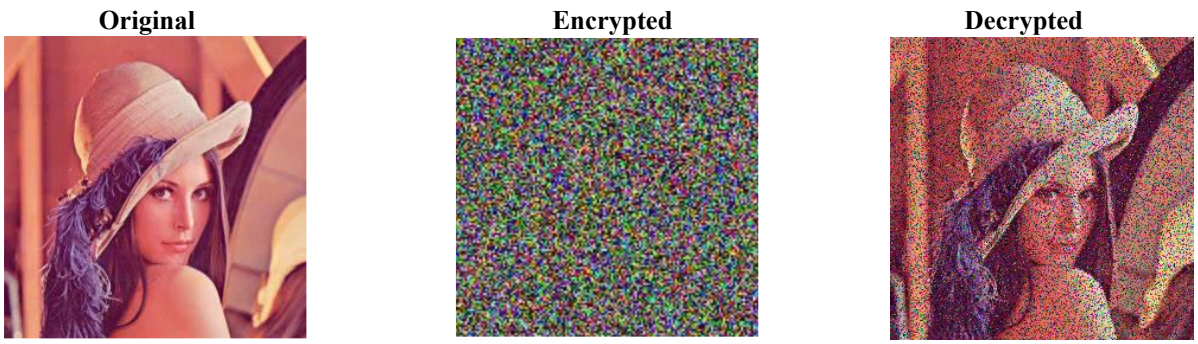


Fig. 2. Block diagram of the proposed decryption algorithm.

5.1 Visual Encryption Results

Figure 3 depicts the original, encrypted, and decrypted images produced with the GF(17) phase. As can be clearly seen, there is no recognizable visual information embedded within the cipher images-successful visual confusion has occurred. A slight distortion has appeared in the recovered images; this is due to loss of data at the pixel level caused by the fact that the GF(17) multiplication causes a zero-pixel to be generated. Figure 4 displays outcomes with the GF(17) step removed; here, the recovered images are indistinguishable from the original images-there is indeed lossless recovery in the absence of the Galois field stage.



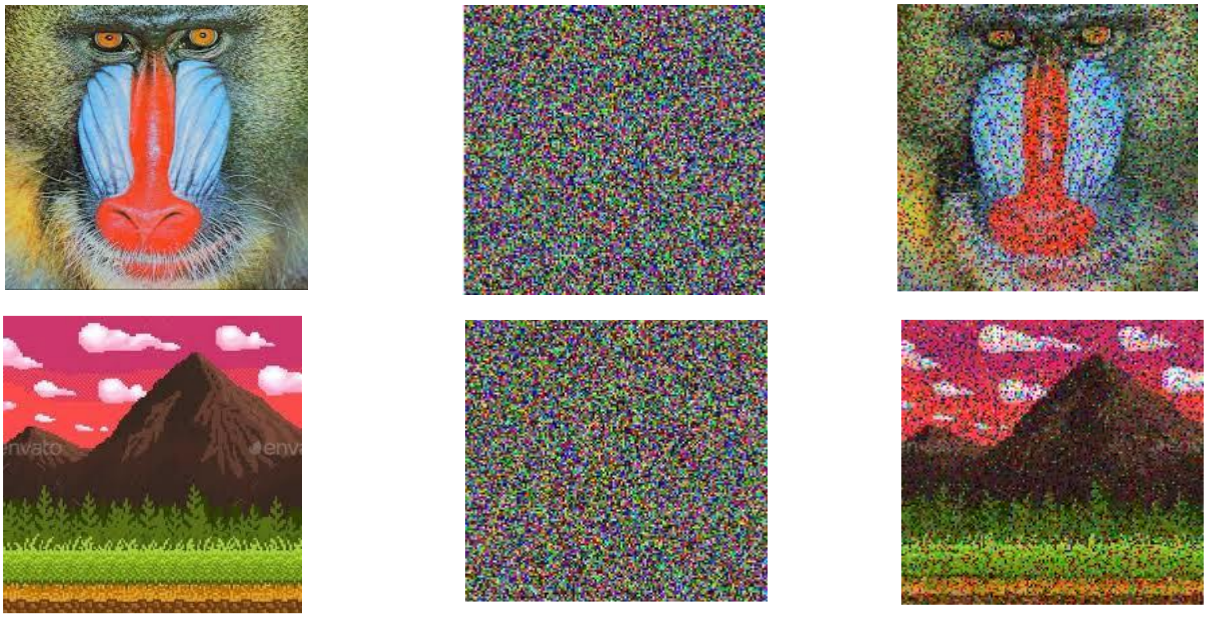


Fig. 3. Encryption/decryption results with GF(17) multiplication enabled

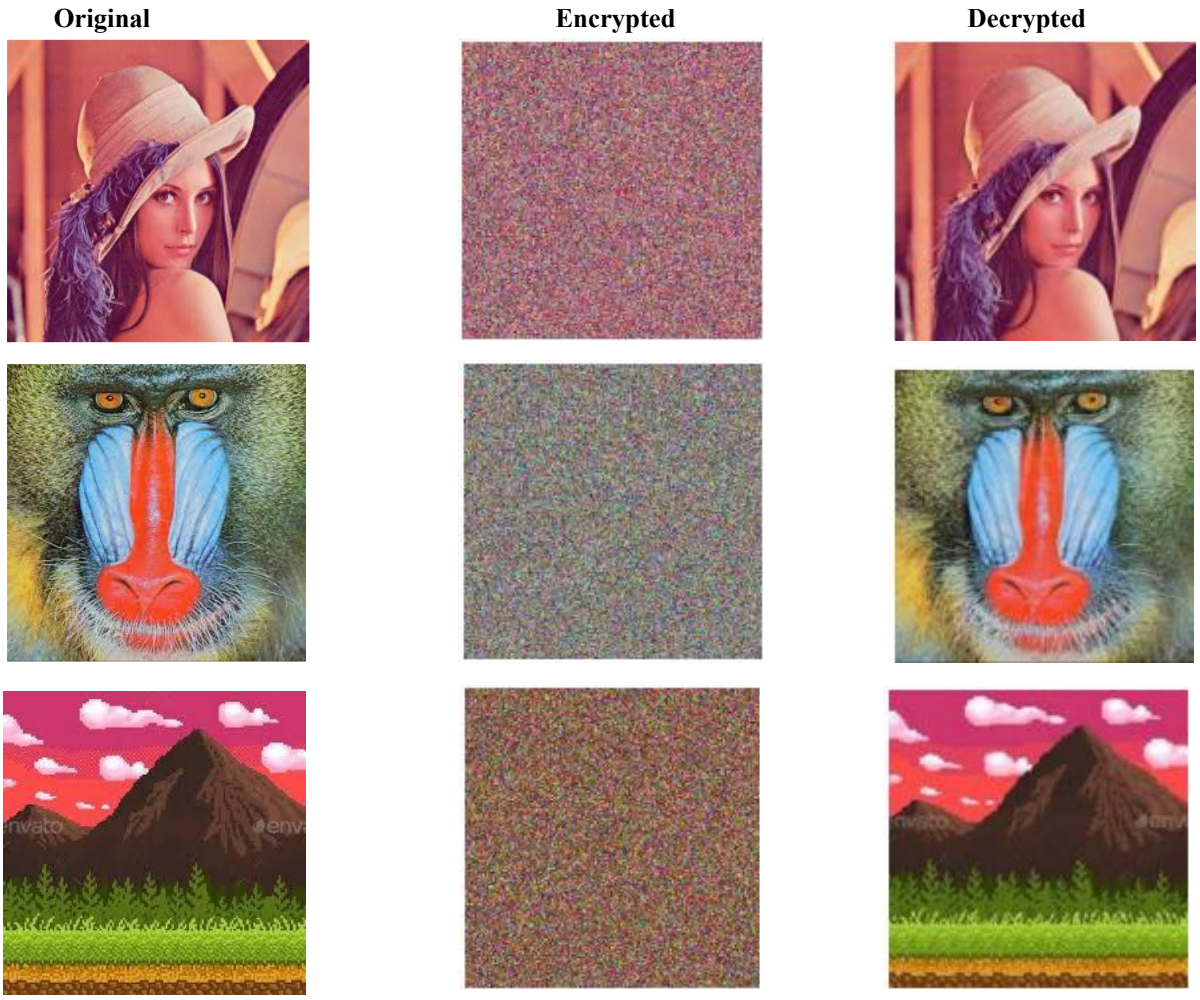


Fig. 4. Encryption/decryption results without GF(17) multiplication.

5.2 Histogram Analysis

The characteristic of good encryption technique will be producing cipher image histogram very smooth throughout the dynamic range. This would lead to an adversary be unable to attack statistically and gain information on plain image. Using GF(17), histogram of each cipher image obtained with it is nearly uniform on the full dynamic range [0, 255] compared to non-uniform histograms of the original images, which is obviously seen by eyes. Without using GF(17), the cipher images histogram is relatively non-flat and easier to attack statistically by using histogram.

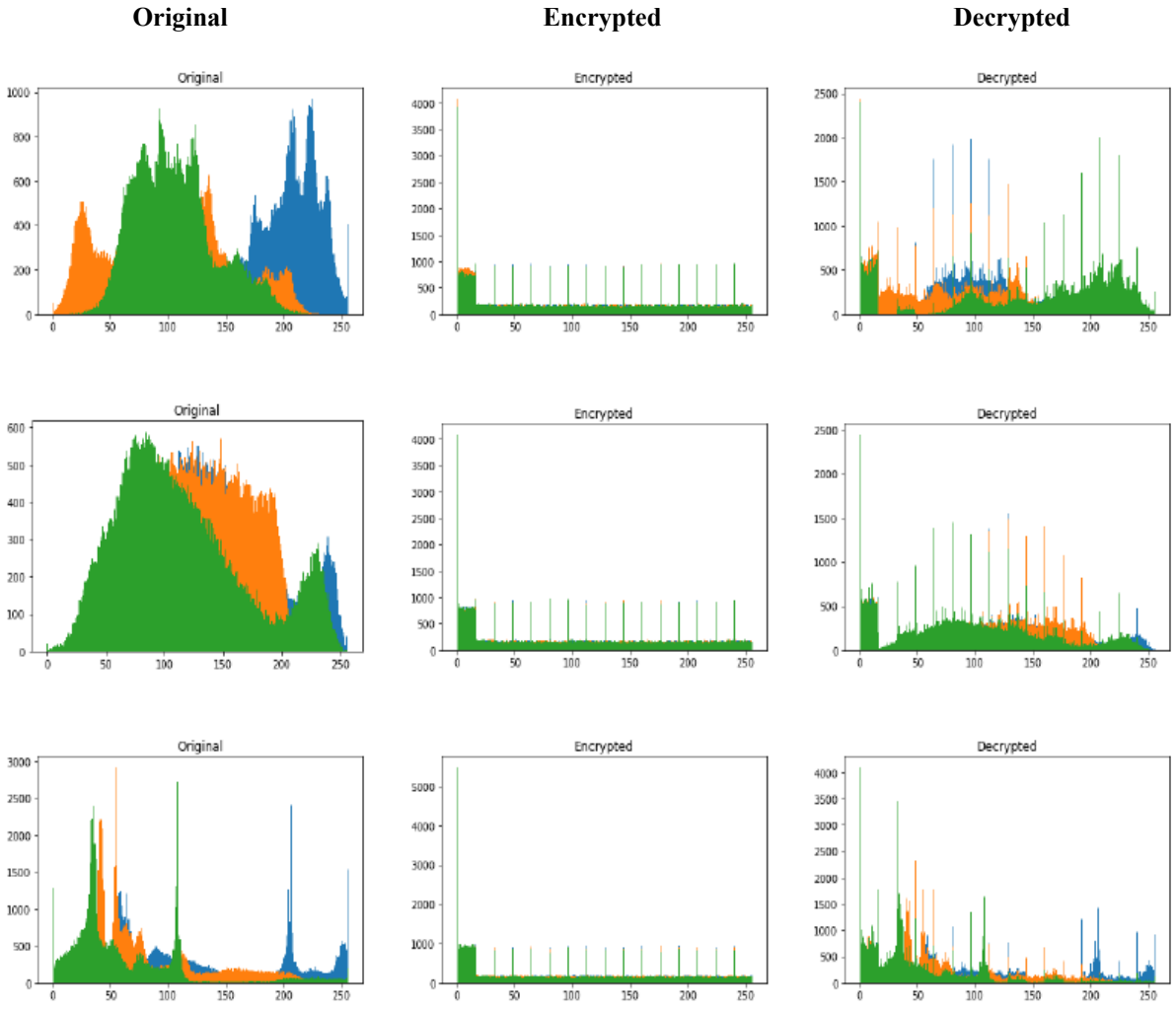
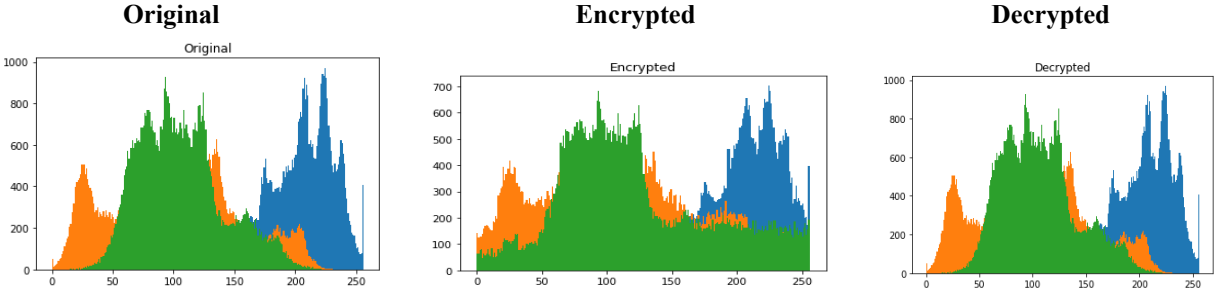


Fig. 5. Histogram analysis with GF(17) multiplication enabled.



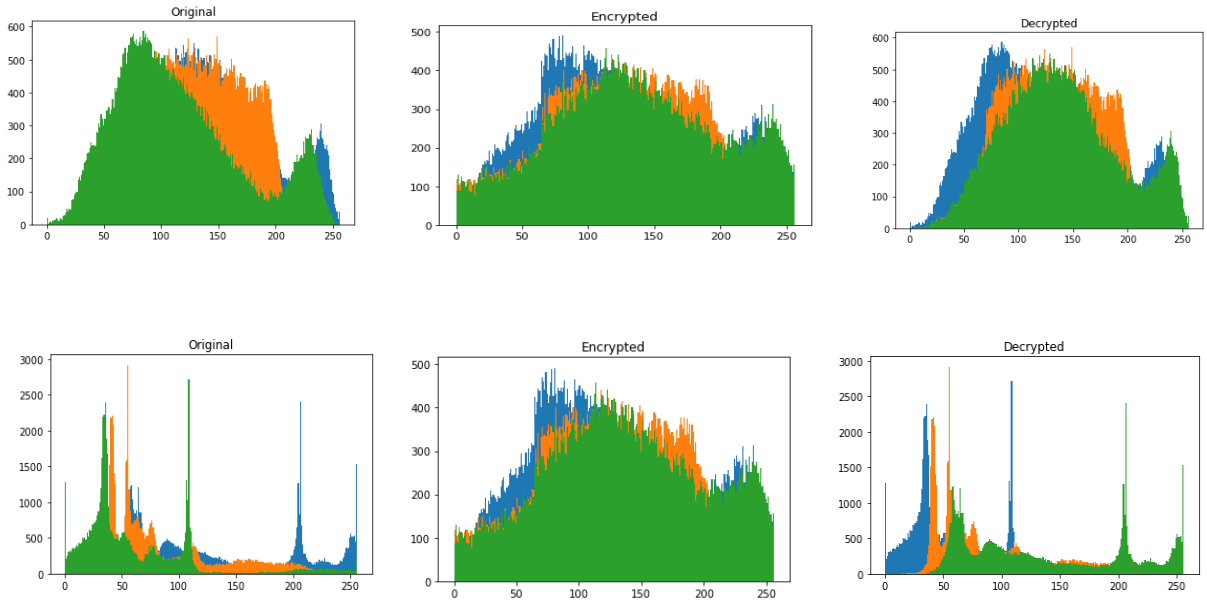


Fig. 6. Histogram analysis without GF(17) multiplication.

5.3 Correlation of Adjacent Pixels

The correlation coefficient r_{xy} is defined as:

$$r_{xy} = \frac{cov(x,y)}{\left(\sqrt{D(x)} \cdot \sqrt{D(y)}\right)}$$

We calculated the coefficients for 1000 random adjacent pixel-pair in horizontal, vertical and diagonal directions. Results are given in Tables 4 and 5. Coefficients for original images are all over 0.9, which show the strong correlation between pixel values. All cipher image coefficients become less than 0.08 in absolute value under GF(17), which means GF(17) provide a large extra effect of diffusion.

Table 4. Correlation coefficients with GF(17) multiplication (Lena, 256×256)

Image	Channel	Horizontal	Vertical	Diagonal
Original	R	0.952	0.970	0.932
	G	0.939	0.974	0.924
	B	0.935	0.973	0.916
Encrypted	R	0.076	0.076	0.005
	G	0.076	0.076	0.005
	B	−0.011	0.023	0.017

Table 5. Correlation coefficients without GF(17) multiplication (Lena, 256×256)

Image	Channel	Horizontal	Vertical	Diagonal
Original	R	0.952	0.970	0.932
	G	0.939	0.974	0.924
	B	0.935	0.973	0.916
Encrypted	R	−0.017	0.071	−0.024
	G	−0.174	0.071	−0.024
	B	0.014	0.123	−0.091

5.4 Information Entropy Analysis

Information entropy provides a measure of the randomness contained within a data source. For an 8-bit image channel, the theoretical upper bound on entropy is 8 bits. Entropy is evaluated using the formula:

$$H(m) = -\Sigma\, p(m_i) log^2 p$$

¡e calculated entropy for source image, encrypted images (for both experimental environments) are listed in Table 6 and Table 7. From these tables, it is obvious that all of the cipher channel entropy are greater than 7.4 bits when GF (17) is activated, and are greater than 7.891bits when GF(17) is disabled. These values are approaching the theoretically maximum 8 bits, therefore we conclude that the suggested algorithm produces the most random cipher images to prevent cryptanalysis based on entropy.

Table 6. Information entropy with GF(17) multiplication

Image	Red	Green	Blue
Original	7.297	7.585	7.585
Encrypted	7.466	7.424	7.456

Table 7. Information entropy without GF(17) multiplication

Image	Red	Green	Blue
Original	7.297	7.585	7.585
Encrypted	7.701	7.891	7.692

The entropy results indicate that, while GF(17) multiplication strengthens histogram uniformity and diffusion, its introduction of zero-pixel artifacts marginally reduces entropy in the cipher images relative to the no-GF condition. This represents an inherent trade-off between diffusion strength and lossless reconstruction. Future work should investigate constrained Galois field operations that avoid zero-pixel generation.

6. CONCLUSION

In this paper, a new color image encryption method is proposed which is based on combined three advanced 1D chaotic maps (SLM, CLM and SCM), DNA-level encoding, DNA arithmetic and modular multiplication over Galois field GF(17). The improved 1D chaotic maps has a bigger range of running parameter to (0,15] and a value of Mean Largest Lyapunov Exponent is close to 10 which is much bigger than 1D classic chaotic maps. Initial states of chaotic system is linked with plain image's bits planes directly provides perfect security of the encryption algorithm against chosen-plaintext attack and known-plaintext attack. DNA arithmetic at the bottom layer and pixel diffusion based on GF(17) arithmetic gives the ciphertext a flat histogram and a very close value of Information Entropy to maximum theoretical value 8 bits.

Experimental results over typical 256256 gray scale color test image show that the inter-pixel correlation coefficient of cipher images becomes under 0.08 (from over 0.9) in all spatial direction after encryption. Furthermore, comparison under condition with and without GF multiplication shows that GF multiplication has very high capability of histogram flattening and diffusion, while causes some information loss in decryption because of zero-pixel generation. The proposed direction of future work can be concluded as following: (i) Construct restricted GF multiplication module and avoid producing zero-pixel product. (ii) Extend the encryption technique to the area of color video encryption. (iii) Do NPCR, UACI analysis together with the implementation on FPGA.

CONFLICT OF INTEREST STATEMENT

The authors declare no conflict of interest.

DATA AVAILABILITY

The benchmark images employed in this study are freely accessible from the USC-SIPI Image Database (https://sipi.usc.edu/database/). The Python implementation code is available from the corresponding author upon reasonable request.

REFERENCES

[1] Y. Wu, J. P. Noonan, G. Yang, and H. Jin, "Image encryption using the two-dimensional logistic chaotic map," J. Electron. Imag., vol. 21, no. 1, p. 013014, 2012.

[2] Z. Hua, Y. Zhou, C.-M. Pun, and C. L. P. Chen, "2D Sine Logistic modulation map for image encryption," Inf. Sci., vol. 297, pp. 80–94, Mar. 2015.

[3] C. Fu, G.-Y. Zhang, M. Zhu, Z. Chen, and W.-M. Lei, "A new chaos-based color image encryption scheme with an efficient substitution keystream generation strategy," Secur. Commun. Netw., vol. 2018, p. 2708532, 2018.

[4] X. Chai, Y. Chen, and L. Broyde, "A novel chaos-based image encryption algorithm using DNA sequence operations," Opt. Lasers Eng., vol. 88, pp. 197–213, Jan. 2017.

[5] L. Huang, S. Wang, J. Xiang, and Y. Sun, "Chaotic color image encryption scheme using DNA coding calculations and arithmetic over the Galois field," Math. Probl. Eng., vol. 2020, p. 3965281, 2020.

[6] J. Fridrich, "Symmetric ciphers based on two-dimensional chaotic maps," Int. J. Bifurc. Chaos, vol. 8, no. 6, pp. 1259–1284, 1998.

[7] S. Bahri-Laleh, M. A. Balafar, and M.-R. Feizi-Derakhshi, "A stream cipher method for RGB image encryption using PSO base key generation," Int. J. Secur. Its Appl., vol. 11, no. 9, pp. 73–94, 2017.

[8] C. Fu et al., "A new chaos-based color image encryption scheme," Secur. Commun. Netw., 2018.

[9] Z. Hua et al., "2D Sine Logistic modulation map," Inf. Sci., 2015.

[10] W. Stallings, Cryptography and Network Security, 4th ed. Pearson Education India, 2006.

[11] H. Liu, X. Wang et al., "Image encryption using DNA complementary rule and chaotic maps," Appl. Soft Comput., vol. 12, no. 5, pp. 1457–1466, 2012.

[12] R. Zhang et al., "A novel plaintext-related color image encryption scheme based on cellular neural network and Chen's chaotic system," Symmetry, vol. 13, no. 3, p. 393, 2021.

[13] Y. Liu and J. Zhang, "A multidimensional chaotic image encryption algorithm based on DNA coding," Multimed. Tools Appl., vol. 79, pp. 21579–21601, 2020.

[14] X. Yan, X. Wang, and Y. Xian, "Chaotic image encryption algorithm based on arithmetic sequence scrambling model and DNA encoding operation," Multimed. Tools Appl., vol. 80, pp. 10949–10983, 2021.

[15] Q. Li and L. Chen, "An image encryption algorithm based on 6-dimensional hyper chaotic system and DNA encoding," Multimed. Tools Appl., vol. 83, pp. 5351–5368, 2024.

[16] Q. Wang, X. Zhang, and X. Zhao, "Color image encryption algorithm based on bidirectional spiral transformation and DNA coding," Phys. Scr., vol. 98, p. 025211, 2023.

[17] L. M. Adleman, "Molecular computation of solutions to combinatorial problems," Science, vol. 266, no. 5187, pp. 1021–1024, 1994.

[18] M. Babaei, "A novel text and image encryption method based on chaos theory and DNA computing," Nat. Comput., vol. 12, no. 1, pp. 101–107, 2013.

[19] S. Al-Maadeed, A. Al-Ali, and T. Abdalla, "A new chaos-based image-encryption and compression algorithm," J. Electr. Comput. Eng., vol. 2012, p. 179693, 2012.