Acadlore Transactions on AI and Machine Learning
https://www.acadlore.com/journals/ATAIML

# DNA-Level Enhanced Vigenère Encryption for Securing Color Images

Abdelhakim Chemlal[1], Hassan Tabti[2*], Hamid El Bourakkadi[1], Rrghout Hicham[1], Abdellatif Jarjar[1], Abdellhamid Benazzi[1]

[1] MATSI Laboratory, Mohammed First University, 60000 Oujda, Morocco
[2] LSIA Laboratory, Sidi Mohamed Ben Abdellah University, 30000 Fez, Morocco

* Correspondence: Hassan Tabti (hassan.tabti1@usmba.ac.ma)

**Received:** 03-28-2024 **Revised:** 06-07-2024 **Accepted:** 06-18-2024

**Citation:** A. Chemlal, H. Tabti, H. El Bourakkadi, R. Hicham, A. Jarjar, and A. Benazzi, "DNA-level enhanced Vigenère encryption for securing color images," *Acadlore Trans. Mach. Learn.*, vol. 3, no. 2, pp. 119–136, 2024. https://doi.org/10.56578/ataiml030205.



**Abstract:** This study presents the development of a novel method for color image encryption, leveraging an enhanced Vigenère algorithm. The conventional Vigenère cipher is augmented with substantial substitution tables derived from widely used chaotic maps in the cryptography domain, including the logistic map and the A.J. map. These enhancements incorporate new confusion and diffusion functions integrated into the substitution tables. Following the Vigenère encryption process, a transition to deoxyribonucleic acid (DNA) notation is implemented, controlled by a pseudo-random crossover matrix. This matrix facilitates a genetic crossover specifically adapted for image encryption. Simulations conducted on a variety of images of diverse formats and sizes demonstrate the robustness of this approach against differential and frequency-based attacks. The substantial size of the encryption key significantly enhances the system's security, providing strong protection against brute-force attacks.

**Keywords:** Substitution box; Enhanced Vigenère; Broadcast function; Chaotic map

## 1 Introduction

The secure transmission of confidential information is sensitive and has become a significant challenge with the rapid advancement of hardware and software technologies [1–3]. One method to overcome this paradox is to encrypt the data before sending it through public, unsecured channels that remain vulnerable to malicious attacks. With the power of current computers, it is easy for an attacker to extract and detect the secret message [4] by attempting brute-force, statistical, and, in some cases, differential attacks. The use and implementation of conventional systems for encrypting large volumes of data remain limited and vulnerable to statistical attacks [5, 6]. Due to a lack of chaining, these algorithms continue to face differential attacks. It is in this context that these systems have been significantly improved and adapted for encrypting data with high redundancy and correlation, such as Vigenère [7–11] and Feistel [12–15]. The unpredictability and high sensitivity to initial conditions, which are desirable for encoding and decoding sensitive data, have led to the development of multiple encryption algorithms. These algorithms integrate dynamic and quantum systems [16, 17] into genetic algorithms adapted for image encryption through actions at the DNA level [18–21].

One-dimensional chaotic maps are simple, less time-consuming, and easy to implement within an encryption algorithm [22–24]. Some of the most widely applied chaotic maps in image encryption include the logistic map, tent map, Henon map, piecewise linear chaotic (PWLCM) map and sinusoidal map.

Motivated by the fact that the new chaotic A.J. map exhibits highly chaotic behavior over a wide range of intervals and has high sensitivity to initial conditions [25, 26], it was integrated with the logistic map into the new encryption system proposed in this study.

The contribution of this study lies in the development of a procedure aimed at creating fresh substitution tables of various sizes, carried out using multiple linear congruential generators (LCGs). Furthermore, a genetic crossover method was introduced, which is suitable for encrypting large sets of data. An enhanced version of the Vigenère technique was employed, wherein newly developed substitution tables were integrated, aiming to strengthen the preservation of plaintext image integrity. The recommended encryption architecture significantly reduced encryption

time compared to those suggested by other researchers. The addition of genetic crossover applied at the DNA level significantly increased the complexity of attacks on the new system proposed in this study.

The rest of this study is divided into several different parts. The first part describes previous work and the conditions of their applications in the field of color image encryption. The second part explains the theoretical framework for the use of chaotic sequences as well as the procedures of genetic operators. The third part illustrates the proposed technology. A final section is dedicated to experimental results, presenting simulations, discussions, and comparisons with similar techniques, followed by a conclusion.

## 2 Related Works

Recently, Jarjar et al. [27] introduced a pioneering 5D chaotic system and its applications. Similarly, El Bourakkadi et al. [28] put forth an algorithm employing transcoding and scrambling of DNA between genes to augment the scrambling effect. Additionally, Zhang and Liu [29] outlined a technique using parallel DNA to overcome the shortcomings of popular DNA-based image encryption algorithms. Yao et al. [30] proposed an architecture centered on DNA storage for image encryption, leveraging molecular biology mechanisms to process information for pixel replacement through genetic hybridization. This method accomplishes double diffusion using pixel diffusion and genetic crossover. Moreover, Gao et al. [31] outlined a novel image encryption architecture incorporating genetic and obfuscation operations. Elmanfaloty et al. [32] proposed a new algorithm, which integrates one-dimensional chaotic logic tent maps to generate pseudorandom series for DNA encoding. Further, Khan et al. [33] outlined an algorithm that combines finite state machines and DNA computation to construct private keys with great simplicity to ensure confusion and diffusion.

Liu and Liu [34] proposed a dual-arrangement DNA transcoding-based image ciphering scheme at the bit-level and pixel-level to address the complete disorder of adjacent pixels. Al_Mola [35] proposed an algorithm, which combines DNA encoding and discrete 4D chaotic graphs to enhance encryption performance and distribution. Zhang et al. [36] suggested a novel ciphering architecture joining rearrangement and replacement based on the ribonucleic acid (RNA) level to counter all known attacks. Additionally, Soltani et al. [37] outlined a system, which combines RNA and DNA-based transcoding system to enhance biometric data security. Sun et al. [38] proposed a new chaotic system for image encryption using RNA operations and the cardioid method. Tahbaz et al. [39] introduced a hybrid image encryption approach involving RNA codons and magical chaos. Finally, Zhao et al. [40] suggested a novel 7D complex encryption architecture by integrating the RNA calculation process.

## 3 Theoretical Basics

Drawing upon chaos theory as its foundation, the proposed methodology in this study relies on several pivotal axes, including harnessing the inherent unpredictability of chaotic systems, utilizing nonlinear dynamics to bolster security measures, and exploiting sensitive dependence on initial conditions for robust encryption. Furthermore, the proposed approach capitalizes on the complex behavior of chaotic systems to craft intricate cryptographic schemes, thereby ensuring resilience against various attack vectors. By integrating chaos-based principles across multiple dimensions, the proposed method offers a versatile framework capable of adapting to evolving security challenges, thus reinforcing data protection in dynamic environments.

### 3.1 Selected Chaotic Sequences

The proposed technology in this study recommends the use of the two popularly studied chaotic maps in the cryptographic field, namely, A.J. and logistic maps.

#### 3.1.1 Logistic map

This map $(U_n)$ [41, 42] is a sequence expressed by a simple second-degree polynomial defined recurrently by formula (1). It has a strong sensibility to initial states, as confirmed by its Lyapunov exponent value. It is easy to configure this map in any cryptosystem.

$$\begin{cases} u_0 \in [0.5-1], \mu \in [3.75-4] \\ u_{n+1} = \mu u_n \left(1-u_n\right) \end{cases} \tag{1}$$

#### 3.1.2 A.J. map

The expression of this map [39] is given in formula (2).

$$\begin{cases} w_0 \in \left[1/(1+p) \quad p/(1+p)\right] \quad p \in [1, 47\ \ \varphi] \\ f\left(w_n\right) = w_{n+1} = \begin{cases} p^2 w_n & \text{if } 0 \le w_n \le 1/(1+p) \\ p - p w_n & \text{if } 1/(1+p) \le w_n \le 1 \end{cases} \end{cases} \tag{2}$$

The choice of these three chaotic maps is justified by their ease of implementation in the encryption system, but above all by their extreme sensibility to initial states. At the same time, the significant size of the private key ensures protection against any brute-force attack.

## 4 The Proposed Method

Based on the construction of multiple substitution tables using pseudorandom LCGs and a genetic crossover acting at the bit level under the control of a crossover table constructed from the chaotic maps used, the proposed method is described in the next sub-sections.

### 4.1 Design of Subkeys

To ensure the smooth execution of the encryption and decryption processes, this technique requires the creation of several pseudo-random vectors aimed at establishing an algorithm capable of countering any known attack. These vectors come in various forms.

#### 4.1.1 Constructing ciphering parameters

This stage takes effect at the pixel layer by implementing a novel modified Vigenère method using the parameters below.

i. XT tables for confusion and diffusion processes.
ii. BT binary tables for control and decision processes.
iii. Two big substitution tables of WS1 and WS2.

#### 4.1.2 Building of TG array

The array TG, with a size of (3nm;5) and elements in $G_2 56$, is composed of several pseudo-random arrays generated by chaotic cards, aiming to establish diffusion and confusion at the pixel level. This development is described as follows:

**Algorithm 1.** XT design

l. $\rightarrow$ For $i = 1$ to $3\,\mathrm{nm}$
2. $\rightarrow TG(i;1) = mod\left(E\left(|u(i) - w(i)| * 10^{12}\right), 252\right)\Big) + 3$
3. $\rightarrow TG(i;2) = mod\left(E\left((u(i) + w(i)) * 10^{10}\right), 254\right)\Big) + 1$
4. $\rightarrow TG(i;3) = mod\left(E\left(Sup(u(i); w(i)) * 10^{11}\right), 254\right) + 1$
5. $\rightarrow TG(i;4) = mod\left(E\left(\left(\frac{u(i)+w(i)}{2} * 10^{11}\right), 253\right)\right) + 2$
   $TG(i;5) = mod\left(E\left(\left(u(i) * 10^6 + w(i) * 10^7\right), \quad 253\right)\right) + 2$ : Next $i$

Every individual column within the table XT signifies an independent pseudo-random vector distinct from the remaining vectors.

#### 4.1.3 Calculus of binary arrays TQ

The binary table TQ, with a size of (3nm;2), is used to control all image encryption operations in the proposed new system. It is implemented as follows:

**Algorithm 2. TQ design**

1. $\rightarrow$ For $i = 1$ to $3\,\mathrm{nm}$
2. $\rightarrow$ if $u(i) > w(i)$ Then
3. $\rightarrow$ TQ $(i;1) = 0$ Else $TQ(i;1) = 1$
4. $\rightarrow$ End if
5. $\rightarrow$ if $TG(i;1) \geq TG(i;5)$ Then
6. $\rightarrow TQ(i;2) = 0$ Else TQ $(i;2) = 1$
7. $\rightarrow$ end if
8. $\rightarrow$ Next $i$

Every column within this algorithm depicts a binary vector that functions as a control for one or multiple encryption procedures.

#### 4.1.4 Development of the substitution table

The substitution box (S-box) computation by the proposed novel architecture is described in different sections below.

(1) S-box construct (WS1)

This section aims to create the new Vigenère substitution matrix WS1, with dimensions of (256;256), by following the detailed instructions provided below.

• The first row of the table (WS1) is the permutation (Pt1) of the first 256 values of the vector TG(:2), obtained by sorting them in decreasing order.

• For ranks higher than 1, the rank line is a rank shift TG(:1) or TS(:3) depending on the value of the control vector TQ(i;1). This table was generated by Algorithm 3.

**Algorithm 3.** (S1) S-box construction

for $i \leftarrow 1$ to 256
  $\mathrm{WS1}(1, i) \leftarrow \mathrm{Pt1}(i)$;
end for
for $i \leftarrow 2$ to 256
  if $TQ(i;1) = 0$ then
    for $j \leftarrow 1$ to 256
      $\mathrm{WS1}(i, j) \leftarrow \mathrm{WS1}(i-1, \mathrm{mod}(j + \mathrm{TG}(i;1), 256))$;
    end for
  else
    for $j \leftarrow 1$ to 256
      $\mathrm{WS1}(i, j) \leftarrow \mathrm{WS1}(i-1, \mathrm{mod}(j + \mathrm{TG}(i;3), 256))$;
    end for
end for

An example is shown as follows:
• Establishment of the initial row.

| Rank | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
|---|---|---|---|---|---|---|---|---|
| $TG(i;2)$ | 1 | 6 | 3 | 7 | 8 | 8 | 4 | 6 |
| Sorting | 8 | 4 | 7 | 3 | 1 | 2 | 6 | 5 |
| Permutation $P1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 8 & 4 & 7 & 3 & 1 & 2 & 6 & 5 \end{pmatrix}$ | | | | | | | | |

• Generation of WS1.
Table 1 shows an example of WS1.

**Table 1.** WS1 example

| **WS1** | **1** | **2** | **3** | **4** | **5** | **6** | **7** | **8** | **TG(i;1)** | **TG(i;3)** | **TQ(i;1)** |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | 8 | 4 | 7 | 3 | 1 | 2 | 6 | 5 | 3 | 7 | 1 |
| 2 | 4 | 7 | 3 | 1 | 2 | 6 | 5 | 8 | 1 | 5 | 0 |
| 3 | 1 | 2 | 6 | 5 | 8 | 4 | 7 | 3 | 5 | 3 | 1 |
| 4 | 8 | 4 | 7 | 3 | 1 | 2 | 6 | 5 | 4 | 3 | 0 |
| 5 | 7 | 3 | 1 | 2 | 6 | 5 | 8 | 4 | 4 | 2 | 1 |
| 6 | 5 | 8 | 4 | 7 | 3 | 1 | 2 | 6 | 5 | 1 | 0 |
| 7 | 3 | 1 | 2 | 6 | 5 | 8 | 4 | 7 | 3 | 4 | 1 |
| 8 | 4 | 7 | 3 | 1 | 2 | 6 | 5 | 8 | 6 | 1 | 0 |

**Table 2.** WS2 example

| **WS2** | **1** | **2** | **3** | **4** | **5** | **6** | **7** | **8** | **TQ(i;2)** |
|---|---|---|---|---|---|---|---|---|---|
| $P1$ | 1 | 8 | 4 | 7 | 3 | 1 | 2 | 6 | 5 | 1 |
| $P2$ | 2 | 4 | 5 | 6 | 3 | 8 | 2 | 1 | 7 | 0 |
| $P3$ | 3 | 7 | 5 | 8 | 6 | 4 | 1 | 2 | 3 | 0 |
| $P4 = P1oP3$ | 4 | 6 | 1 | 5 | 2 | 3 | 8 | 4 | 7 | 1 |
| $P5 = P2oP4$ | 5 | 2 | 4 | 8 | 5 | 6 | 7 | 3 | 1 | 1 |
| $P6 = P4oP5$ | 6 | 1 | 2 | 7 | 3 | 8 | 4 | 5 | 6 | 0 |
| $P7 = P4oP6$ | 7 | 6 | 1 | 4 | 5 | 7 | 2 | 3 | 8 | 1 |
| $P8 = P6oP5$ | 8 | 2 | 3 | 6 | 8 | 4 | 5 | 7 | 1 | 0 |

(2) S-box construct (WS2)

The construction of the new substitution matrix (WS2), with a size of (256;256), is described by the following steps:

• The 1st line is the rearrangement (P1) obtained by a broad ascending sort on the first 256 values of the vector TG(:3);

• The 2nd line is the rearrangement (P2) obtained by a broad ascending sort on the first 256 values of the vector TG(:4);

• The 3rd line is the rearrangement (P3) obtained by a broad ascending sort on the first 256 values of the vector TG(:5);

• The i-th line (i>3) is the composition of the functions of lines (i-2) and (i-3) or (i-3) and (i-1), depending on the value of the control vector TQ(:2).

These steps are illustrated in Algorithm 4.

**Algorithm 4.** (WS2) S-box construction

for $i \leftarrow 1$ to 256
  $\mathrm{WS2}(1,i) \leftarrow \mathrm{Pr1}(i)$;
  $\mathrm{WS2}(2,i) \leftarrow \mathrm{Pr2}(i)$;
  $\mathrm{WS2}(3,i) \leftarrow \mathrm{Pr3}(i)$;
end for
for $i \leftarrow 4$ to 256
  for $j \leftarrow 1$ to 256
    if $TQ(i;2) = 0$ then
      $\mathrm{WS2}(i,j) \leftarrow \mathrm{WS2}(i-2, \mathrm{WS2}(i-3,j))$;
    else
      $\mathrm{WS2}(i,j) \leftarrow \mathrm{WS2}(i-3, \mathrm{WS2}(i-1,j))$;
    end if
  end for
end for

Table 2 shows an example of WS2.

#### 4.1.5 Pixel transcription based on S-boxes

To transform the i-th pixel X(i) into Y(i), the VW expression given in Algorithm 5 was used.

**Algorithm 5.** X(i) pixel encryption

$\mathrm{VW}(X(i)) = Y(i)$;
  if $TQ(i;2) = 0$ then
    $Y(i) \leftarrow \mathrm{WS1}(TG(i;2), \mathrm{WS2}(TG(i;3), X(i) \oplus TG(i;4))) \oplus TG(i;1)$;
  else
    $Y(i) \leftarrow \mathrm{WS2}(TG(i;3), \mathrm{WS1}(TG(i;1), X(i) \oplus TG(i;5))) \oplus TG(i;2)$;
end if

The encryption process in this stage relies on the decision vector TQ(:2) and incorporates two nested S-boxes, adding complexity to the confusion and substitution functions. Any slight alteration to a parameter of the secret keys can result in a distinct ciphering expression, leading to a different cipher image.

### 4.2 Preparing the Image for Encryption

Before proceeding with encryption, it is imperative to prepare the initial image by following these steps, laying the groundwork for this technique.

#### 4.2.1 Vectorization of the plain image

After the extraction of red, green, and blue (RGB)-channels and their transformation into $((Xr),(Xg),(Xb))$ vectors, each with a dimension of (1,nm). This process generates the vector $X(x_1, x_2, ....., x_3nm)$, as outlined in Algorithm 6.

**Algorithm 6.** Transitioning to vector X

1. → for $i = 2$ to nm
2. → If $TQ(i;1) = 0$ Then
3. → $X(3i-2) = VW(Xb(i) \oplus TG((3i-2);2)$
4. → $X(3i-1) = VW(Xr(i) \oplus TG((3i-1);1)$
5. → $X(3i) = VW(Xg(i) \oplus TG((3i);3)$
6. → Else
7. → $X(3i-2) = VW(Xb(i) \oplus TG((3i-2);3)$
8. → $X(3i-1) = VW(Xr(i) \oplus TG((3i-1);4)$
9. → $X(3i) = VW(Xg(i) \oplus TG((3i);5)$
10. → End if: Next $i$

This initial process generated a slightly encrypted new image whose statistical parameters ensure strong security against any statistical and frequency attacks, as shown in Figure 1.

This transition is governed by the CR vector. This can effectively break the pixel's correlation relationship, resulting in a robust system that can withstand statistical and brute-force attacks. This approach's effectiveness is depicted in Figure 2 below. This initial encryption round ensures that the proposed cryptographic system is immune to any statistical or brute-force attacks.

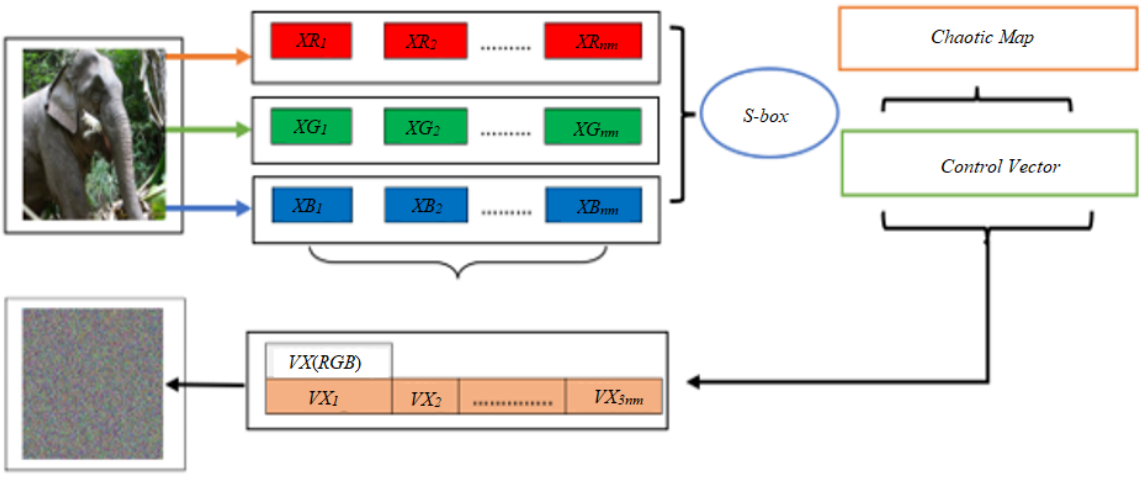



**Figure 1.** Original image vectorization

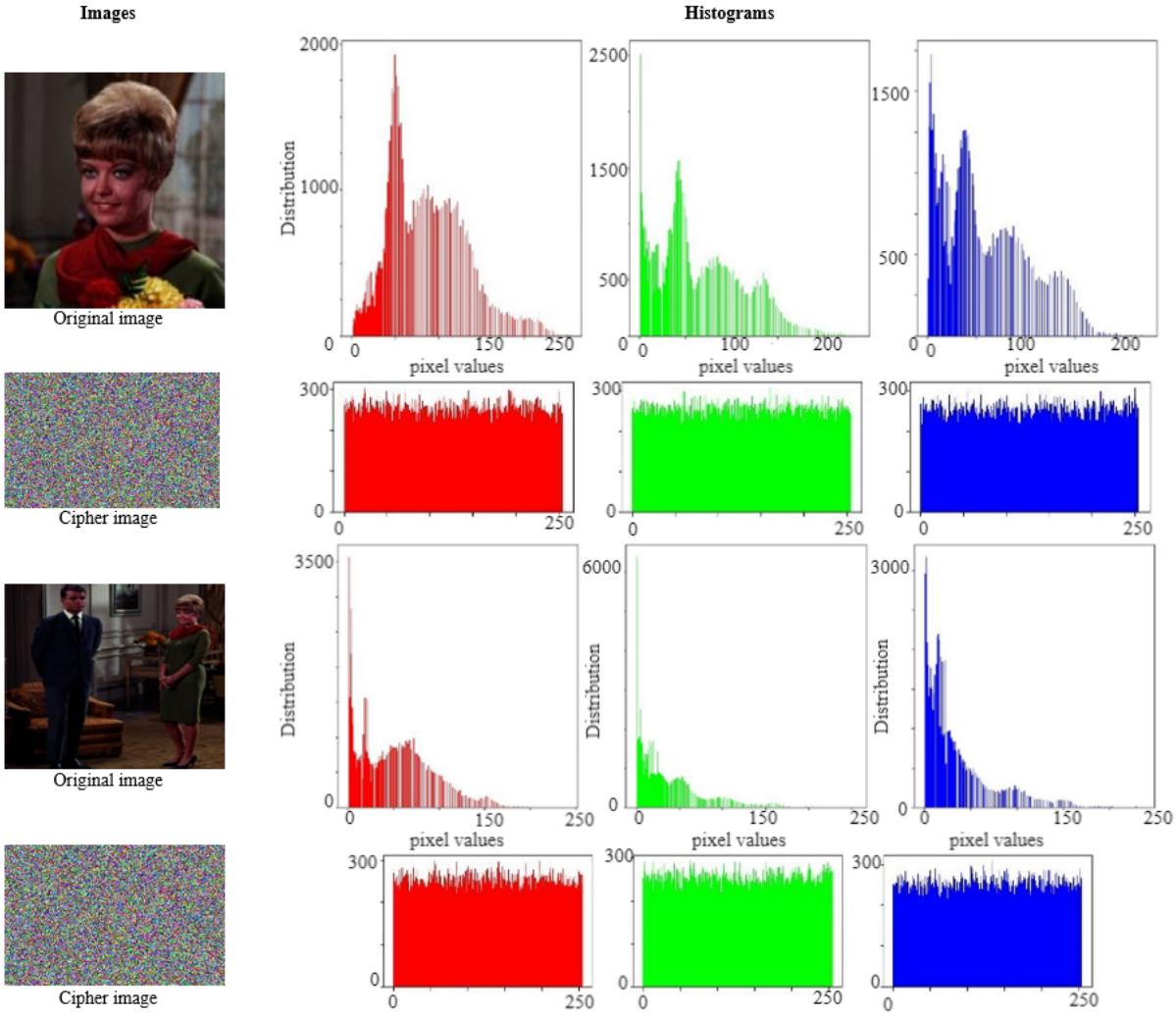



**Figure 2.** Histogram and entropy for original and encrypted sample of images

Two S-boxes, encryption, and broadcast expressions were used in order, aiming to prevent the proposed system from differential attacks.

4.2.2 Initialization value computation

To modify the value of the starting pixel and begin the encryption process, a constant IC was calculated from the plain image in conjunction with the pseudo-random vector and under the control of a binary vector. This process is determined by Algorithm 7.

| **Algorithm 7.** First initialization value calculation | |
|---|---|
| 1. $\rightarrow IC = 0$ | 5. $\rightarrow$ Else |
| 2. $\rightarrow$ For $i = 2$ to 3 nm | 6. $\rightarrow IC = WV(X(i)) \oplus IV \oplus \mathrm{TG(i;1)}$ |
| 3. $\rightarrow$ If TQ $(i;2) = 0$ Then | 7. $\rightarrow$ Next $i$ |
| 4. $\rightarrow IC = X(i) \oplus IV \oplus \mathrm{TG(i;5)}$ | |

4.2.3 Encryption system process

The computed constant serves solely to alter the pixel's value and initiate the ciphering operation. Figure 3 depicts the improved ciphering procedure involving S-boxes.

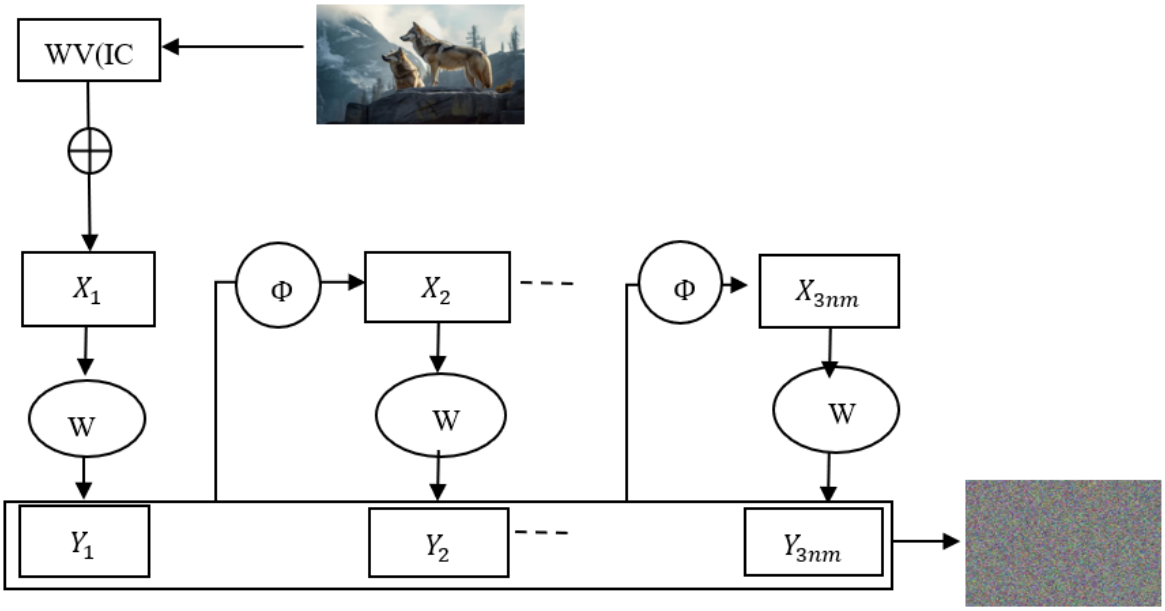



**Figure 3.** First stage of the image ciphering process

This encryption stage using an advanced broadcasting function $\Phi(Y(i))$ based on nested S-boxes (WS1) and (WS2) is given by formula (3).

$$\Phi(Y(i)) = WS1(\mathrm{TG(i;2)}, WS2(\mathrm{TG(i;4)}; WV(Y(i)) \oplus X(i+1))) \tag{3}$$

This operation can be given by Algorithm 8.

| **Algorithm 8.** First stage of the image ciphering algorithm | |
|---|---|
| First pixel encryption | 4. $\rightarrow$ If TQ $(i;1) = 0$ Then |
| 1. $\rightarrow Y(1) = WV(XT(1;1) \oplus X(1)) \oplus WV(IV)$ | 5. $\rightarrow Y(i) = WV(\Phi(X(i))) \oplus TG(i;5)$ |
| Next Pixel Encryption | 6. $\rightarrow$ else |
| 2. $\rightarrow$ For $i = 2$ to $3nm$ | 7. $\rightarrow Y(i) = WV(\Phi(X(i))) \oplus TG(i;4)$ |
| 3. $\rightarrow \Phi(X(i)) = WV(TG(i;3) \oplus Y(i-1)) \oplus X(i)$ | 8. $\rightarrow$ Next $i$ |

The obtained array Y that signifies the cipher picture is a set of components corresponding each to a nucleotide.

4.2.4 First-stage analysis

The first-round encryption time is given in Figure 4 below.

The initial phase yielded highly satisfactory outcomes, and these would be further enhanced in the subsequent stage. To elevate the time complexity of the attack, the resulting vector was subjected to a second lap employing bit-wise crossover.

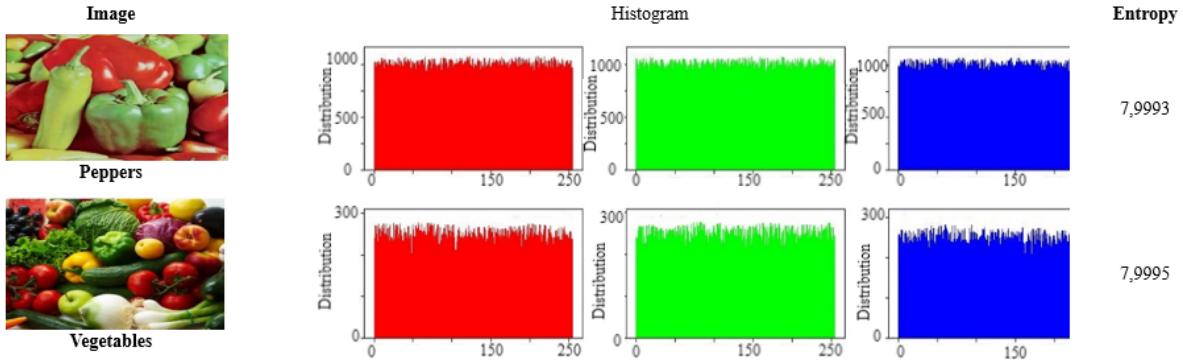



**Figure 4.** First round encryption time

4.2.5 Pseudorandom transition into binary notation

The vector Y underwent a transformation where each pixel was converted into a nucleotide represented by the notation XS. The details of this process are outlined in Figure 5.

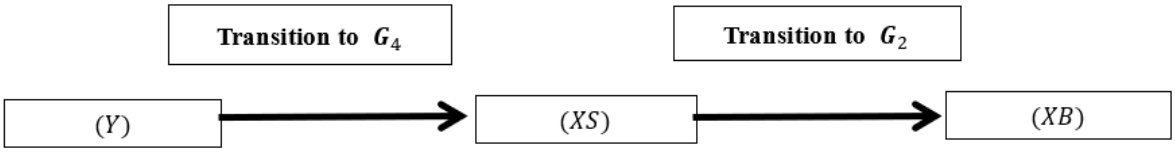



**Figure 5.** Binary transition

Let TV be the table transition from $(Z/4Z)$ to $(Z/2Z)$, as shown in Table 3.

**Table 3.** Table transition example from $(Z/4Z)$ to $(Z/2Z)$

| **(TV)** | 1 | 2 | |
|---|---|---|---|
| 0 | 0 | 0 | **(TR)** |
| 1 | 0 | 1 | |
| 2 | 1 | 0 | |
| 3 | 1 | 1 | |

The subsequent method illustrates the trajectory of vector Y with dimensions of (1; 3nm) as it moves from the pixel to the group $G_4$, aligning with array Y of 12nm components, as outlined in Algorithm 9. This transition is depicted in Figure 6.

**Algorithm 9.** Transition to $G_4$ and $G_2$

| | |
|---|---|
| // transmission into $(\boldsymbol{G_4})$ | $\boldsymbol{\beta(4) = \mathbf{mod}(y, 4)}$ |
| For $\boldsymbol{i} = 1$ to 3 nm | // transition to $(\boldsymbol{G_2})$ |
| $\boldsymbol{x = E\left(\frac{Y(i)}{16}\right)}$ | If $\boldsymbol{TQ(i, 2) = 0}$ |
| $\boldsymbol{y = mod(Y(i), 16)}$ | For j = 0 to 7 |
| $\boldsymbol{\beta(1) = E\left(\frac{x}{4}\right)}$ | $\mathrm{XB(8i - (3 * j + 7)\%8) = TR(,j\%\mathbf{4}); (j\%\mathbf{2}) + \mathbf{1})}$ |
| $\boldsymbol{\beta(2) = mod(x, 4)}$ : | Else |
| $\boldsymbol{\beta(3) = E\left(\frac{y}{4}\right)}$ | $\mathrm{XB\left((8i - (5^{*}j + 1)\,\%8)\right) = TR(\boldsymbol{\beta}(j\%\mathbf{4}); (j\%\mathbf{2}) + \mathbf{1})}$ |
| | Next $j$: Next $i$ |

4.2.6 Genetic crossbreeding

The conversion of the vector XB resulted in the generation of a matrix MB with dimensions of (4nm; 8). Simultaneously, the vector BT(:2) underwent transformation into a matrix MT with a size of (4nm; 8), serving as input for a genetic crossover tailored for color image encryption. This process is regulated by the matrix NB and guided by the crossover table MC with dimensions of (4nm; 9). The construction of the table MC involves the implementation of the steps below:

The $1^{st}$ line is the rearrangement computed through a strict ascending sort of the 1st 4nm values of the sequence u. It indicates the index of the $1^{st}$ column of the table MB to be multiplied by$2^0$.

The $2^{nd}$ line is the rearrangement computed through strict sorting in ascending order on the $1^{st}$ 4nm elements of the sequence v. It indicates the index of the $2^{nd}$ column in the table MB to be multiplied by $2^1$.

The $3^{rd}$ row is the rearrangement computed through a broad sense sorting in descending order on the $1^{st}$ 4nm elements of the sequence XT(:1). It indicates the index of the $3^{rd}$ column in the table MB to be multiplied by$2^2$.

The $4^{th}$ line is the rearrangement computed through a broad sense sorting in ascending order on the $1^{st}$ 4nm elements of the sequence XT(:2). It indicates the index of the $4^{th}$ column in the table MB to be multiplied by $2^3$.

The $5^{th}$ line is the rearrangement computed through strict sorting in descending order of the $1^{st}$ 4nm elements in the sequence XT(:3). It indicates the index of the $5^{th}$ column in the table MB to be multiplied by$2^4$.

The $6^{th}$ line is the rearrangement computed through a broad sense sorting in ascending order on the $1^{st}$ 4nm elements of the sequence XT(:4). It indicates the index of the $6^{th}$ column in the table MB to be multiplied by $2^5$.

The $7^{th}$ row is the rearrangement computed by a broad sense sorting in descending order on the first 4nm elements of the sequence XT(:5). It indicates the index of the $7^{th}$ column in the table MB to be multiplied by $2^6$.

The $8^{th}$ line is the rearrangement computed through strict sorting in ascending order on the first 4nm elements of the sequence BT(:1). It indicates the index of the $8^{th}$ column in the table MB to be multiplied by $2^7$.

The $9^{th}$ row is the rearrangement computed through a broad sense sorting in ascending order on the $1^{st}$ 4nm elements of the sequence BT(:2). It indicates the index of the $9^{th}$ column in the table MB to be multiplied by $2^8$.

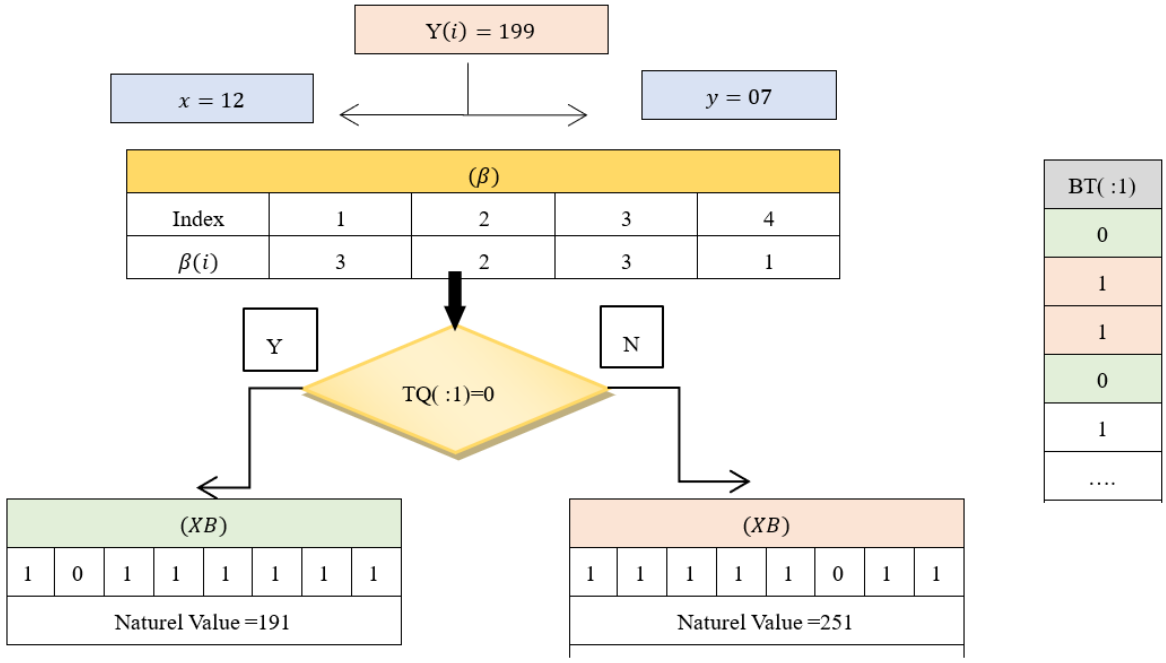



**Figure 6.** Transition to $G_4$ and $G_2$

Algorithm 10 clarifies this operation.

| **Algorithm 10.** Confusion of binary terms | |
|---|---|
| 1. → For $i = 1$ to 4 nm | 5. → $Z(MC(i;9)) = x \oplus XT(i;1)$ |
| 2. → for $j = 0$ to 7 | 6. → Else |
| 3. → $x = MB\left(MC(i;j) * 2^j\right)$ | 7. → $Z(MC(i;9)) = x \oplus XT(i;3)$ |
| 4. → next $j$ | 8. → End if |
| → if $BT(i;1) = 0$ then | → Next $i$ |

An example of a confusing operation is depicted in Figure 7.

### 4.2.7 Decryption procedure

A symmetric encryption system featuring a broadcast implementation was employed in the proposed approach. Consequently, during the decryption procedure, the reverse ciphering formula was employed, commencing with the final step. Any formula utilized within the proposed cryptosystem is reversible, ensuring the existence of a reverse of the ciphering formula. This process was structured around the subsequent operations:

(a) Reciprocal of the conversion to binary
(b) Reciprocal of the crossover operation
(c) 2nd lap reciprocal encryption process
(d) Transformation to RGB

Reciprocal of Vigenère matrix generation-decryption first-round process, including reverse of Vigenère lap and rearrangement step

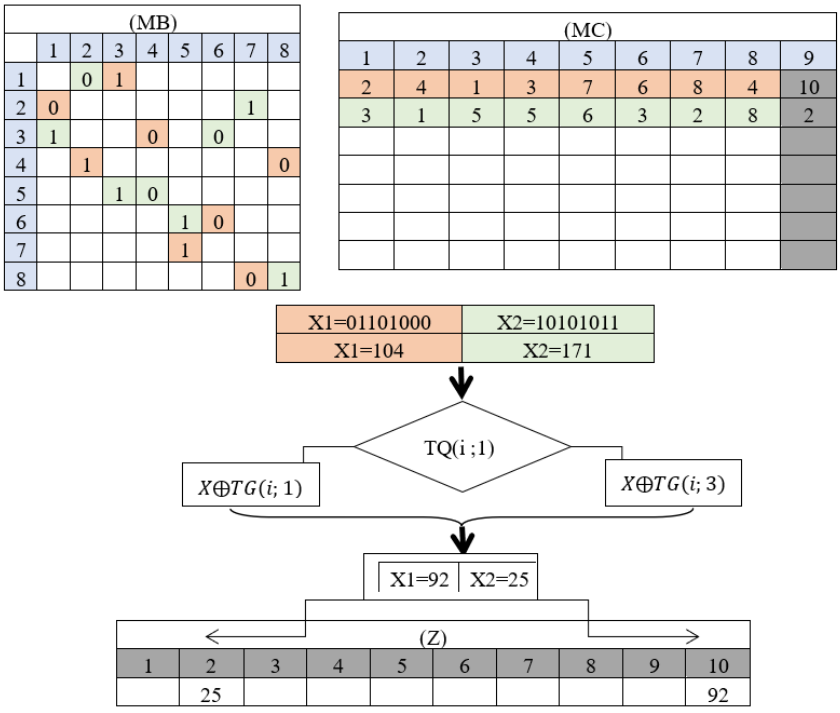



**Figure 7.** Example of confusing operation

4.2.8 Reciprocal of Vigenère matrix

To apply the inverse Vigenère transformation, Algorithm 11 was used.

**Algorithm 11.** Vigenère reciprocal

for $j = 1$ to 256
  for $i = 1$ to 256
    $GV(j, VG(j, i)) = i$
    $DV(j, VD(j, i)) = i$
  Next $i, j$

Table 4 shows an example of the construction of the matrix used in the inverse Vigenère transformation.

**Table 4.** Example of GV reverse S-box transformation

| VG | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | CR | KL | C L | | GV | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | 3 | 5 | 8 | 6 | 2 | 7 | 1 | 4 | | | | | 1 | 7 | 5 | 1 | 8 | 2 | 7 | 6 | 3 |
| 2 | 2 | 7 | 1 | 4 | 3 | 5 | 8 | 6 | 1 | 5 | 4 | ↔ | 2 | 3 | 1 | 5 | 4 | 6 | 8 | 2 | 7 |
| 3 | 5 | 8 | 6 | 2 | 7 | 1 | 4 | 3 | 1 | 3 | 5 | | 3 | 6 | 4 | 8 | 7 | 1 | 3 | 5 | 2 |
| 4 | 2 | 7 | 1 | 4 | 3 | 5 | 8 | 6 | 0 | 3 | 4 | | 4 | 3 | 1 | 5 | 4 | 6 | 8 | 2 | 7 |
| 5 | 1 | 4 | 3 | 5 | 8 | 6 | 2 | 7 | 1 | 4 | 2 | | 5 | 1 | 7 | 3 | 2 | 4 | 6 | 8 | 5 |

By following the same logic of Vigenère's traditional technique, the traditional substitution function reciprocal depicted in formula (4) was obtained.

$$\text{if } z = VG(y, x) \text{ Then } x = GV(y, z) \tag{4}$$

4.2.9 Vigenère's inverse expression

The inverse expression of Vigenère transformation given by Algorithm 8 is provided by Algorithm 12.

**Algorithm 12.** Vigenère reciprocal

$WV(Y(i)) \leftarrow X(i)$;
if $TQ(i;2) = 0$ then
  $X(i) \leftarrow \mathrm{SW2}(TG(i;3), \mathrm{SW1}(TG(i;2), Y(i) \oplus TG(i;1))) \oplus TG(i;4)$;
else
  $X(i) \leftarrow \mathrm{SW1}(TG(i;1), \mathrm{SW2}(TG(i;3), TG(i;2) \oplus Y(i))) \oplus TG(i;5)$;
end if

4.2.10 Reverse diffusion

The inverse expression of the diffusion function used in the scheme of this study is given by formula (5).

$$\Pi^{-1}\left(X'(k)\right) = GV\left(CL(k), DV\left(KR(k), X'(k)\right) \oplus X(k-1)\right) \tag{5}$$

### 4.3 Results and Discussions

In this section, a considerable quantity of images randomly chosen from an extensive database underwent evaluation using the proposed novel algorithm. The performance outcomes were presented and juxtaposed with those of other algorithms. It is understood that an effective algorithm can withstand any documented attack. Figure 8 illustrates a selection of reference images subjected to testing with the newly developed algorithm.

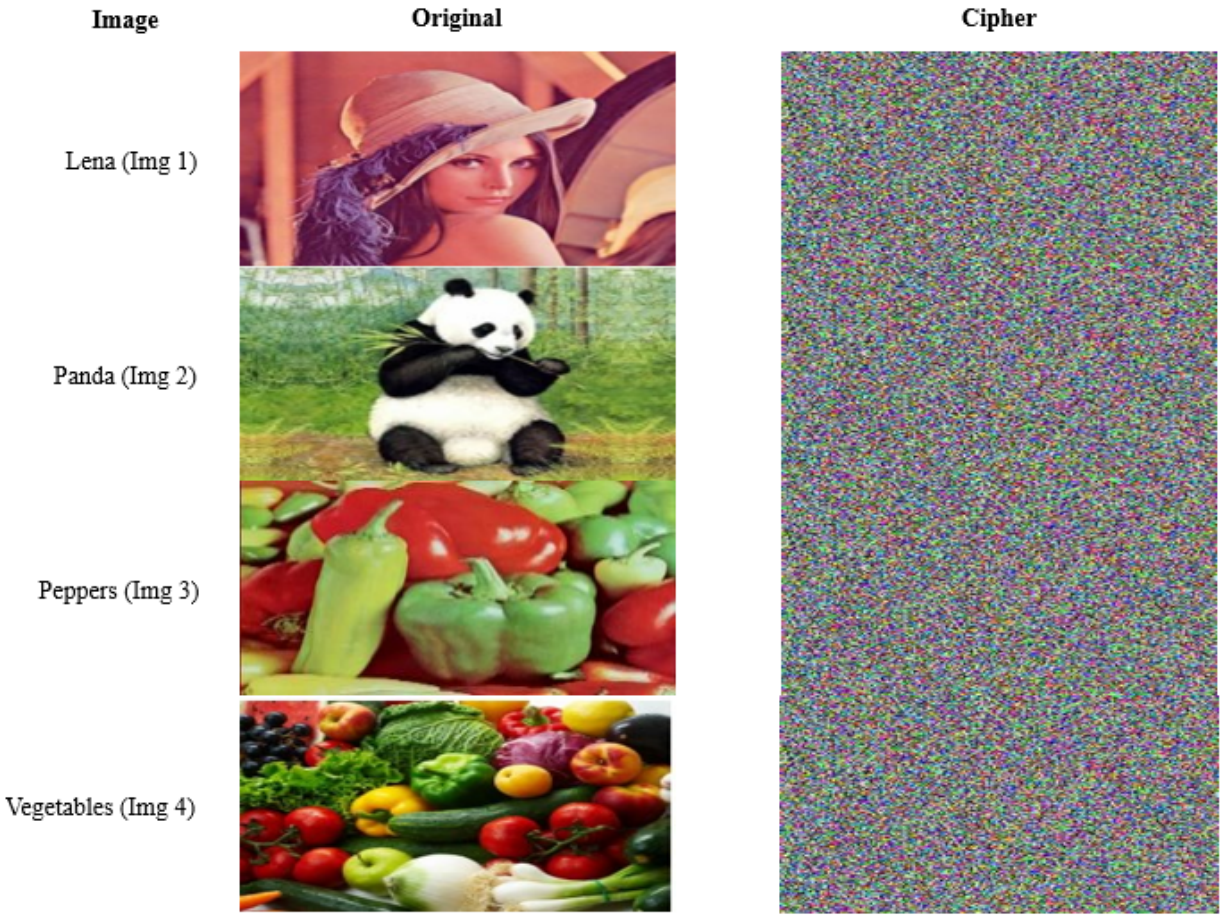



**Figure 8.** Sample of image visual test

They involve the reconstruction of encryption keys in a stochastic manner.

4.3.1 Key-space analysis

A brute force attack, employed in cryptanalysis, is a method aimed at discovering the encryption key by systematically testing all possible combinations. Consequently, the feasibility of brute-force attacks is rendered

implausible when dealing with a substantial encryption key. In the algorithm of this study, the secret key possesses a size significantly exceeding $(2^{128})$ [42, 43], which ensures enhanced resistance to brute force attacks. The cryptographic simulation relies on the generation of a secret key derived from the popularly employed chaotic maps. Consequently, the key comprises six parameters, each encoded in 32 bits, resulting in a total global size of $(2^{6*32})=(2^{192})\geq(2^{100})$.

4.3.2 Sensitivity analysis of a secret key

Within the algorithm of this study, each of the chaotic maps exhibits significant sensitivity to starting states. Consequently, any change on a parameter during the secret key building process leads to the generation of a distinct private key. This results in the generation of divergent chaotic vectors, giving rise to a random encrypted image, as illustrated in Figure 9.

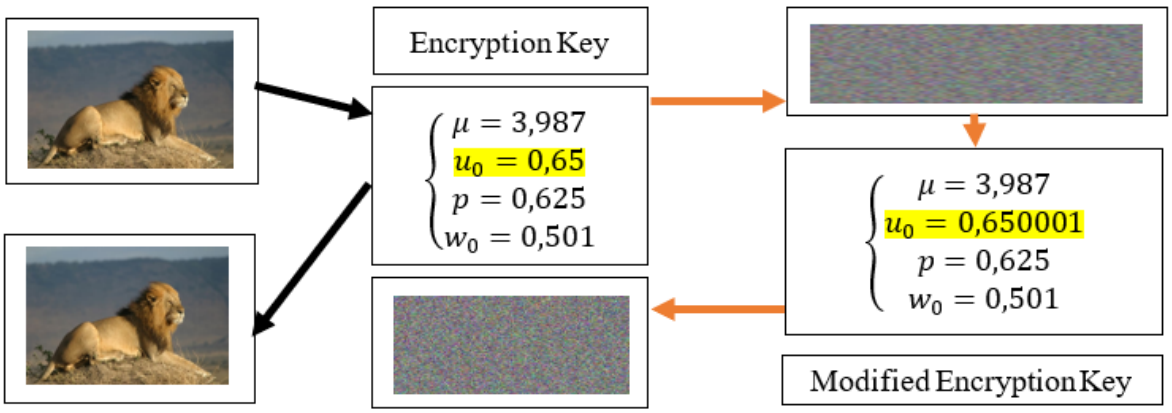



**Figure 9.** Sensitivity of the ciphering key

It can be observed that a perturbation on a single parameter in the order of $10^{-7}$ is insufficient to accurately reconstruct the original image.

4.3.3 Security against statistical attacks

To demonstrate that the proposed novel encryption method is robust against any statistical attack, numerous tests were applied to many pictures taken from diverse databases. This highlights noteworthy results.

(1) Analysis of histograms

A graphical representation of pixel distribution is based on RGB levels. An image histogram illustrates the frequency of pixels that share the same RGB level. The abscissa axis corresponds to RGB levels ranging from zero to 255, with each vertical bar denoting the occurrences of a specific RGB level in the picture. Cryptographically, analyzing the color distribution in an encrypted image is crucial, as it can potentially reveal details about the original image. Conversely, a flat and uniformly distributed histogram in the encrypted image may indicate a lack of data about the plain picture or its relation to the cipher counterpart. Figure 10 presents simulation results for the proposed system.

The algorithm of this study consistently generated encrypted images with flattened histograms when applied to various reference images. The uniformity exhibited in the histograms serves as robust protection against potential attacks targeting the histogram.

(2) Entropy studies

Eq. (6) expresses an image pixel-associated entropy.

$$H(MC) = \frac{1}{t}\sum_{i=1}^{t} -\pi(i)\log_2(\pi(i)) \tag{6}$$

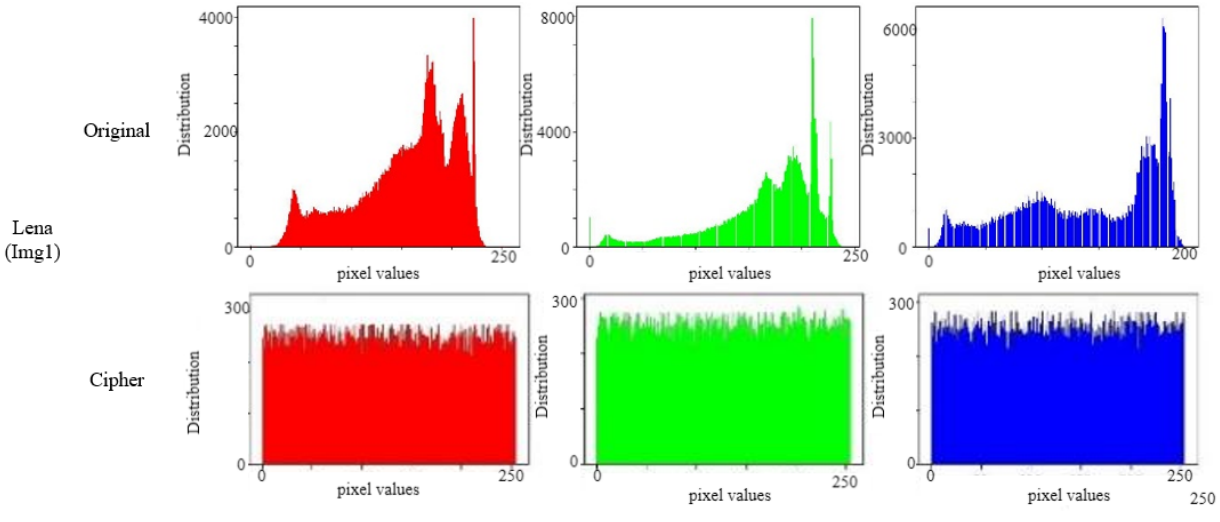
where, $\pi(i)$ represents the probability of the occurrence of level $i$ in the original image.

Table 5 presents the entropy values for the images subjected to the proposed technique.

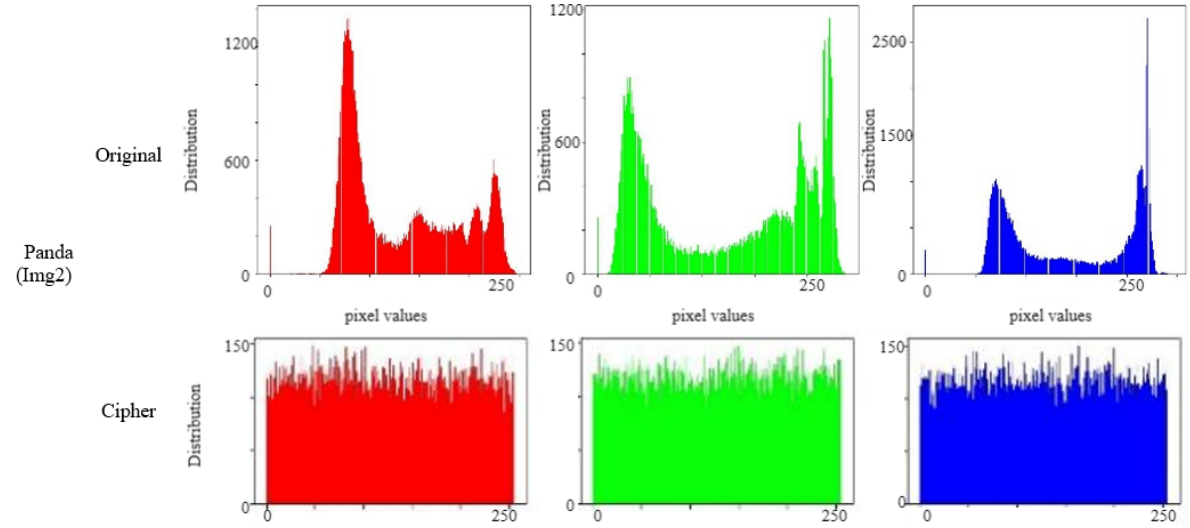
(3) Analysis of correlation

Correlation is a method utilized in scientific contexts to assess the migration of pixels in one image concerning a citation image by comparing the two images. The pertinent expression is specified by Eq. (7).

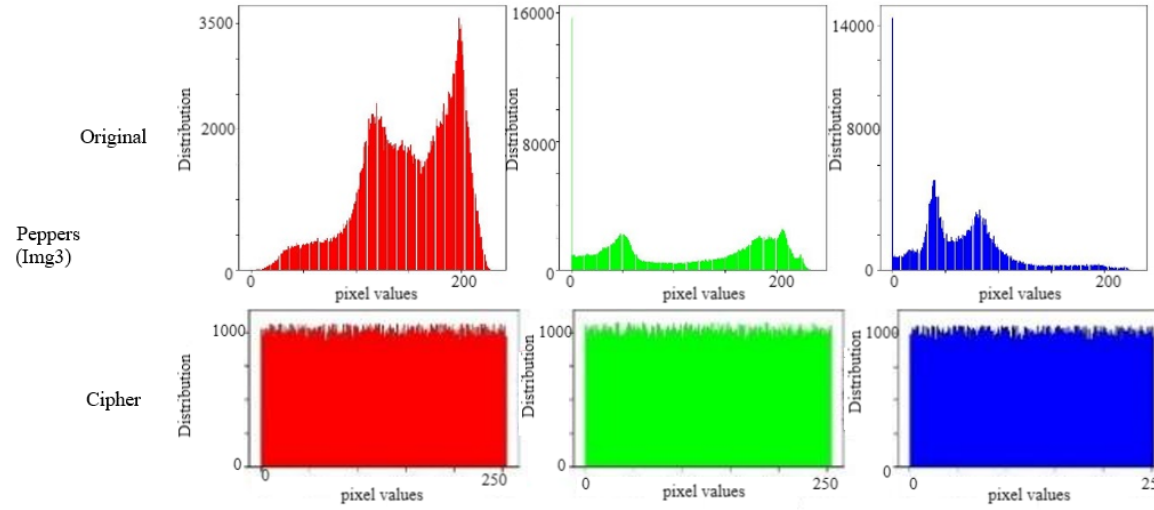
$$r = \frac{\mathrm{cov}(x,y)}{\sqrt{V(x)}\sqrt{V(y)}} \tag{7}$$




(a)




(b)




(c)

**Figure 10.** Histogram analysis

**Table 5.** Entropy analysis

| Image No. | Entropy |
|---|---|
| Img1 | 7.9997 |
| Img2 | 7.9996 |
| Img3 | 7.9992 |
| Img4 | 7.9993 |

Table 6 represents the correlation between pixels in a sample of ciphered images in three directions. It can be observed that the correlation value approaches zero, thereby ensuring enhanced resilience and counteracting correlation-based attacks. Each pixel in the original image exhibits a high correlation with its neighboring pixels in the vertical, horizontal, or diagonal directions. This correlation encapsulates information exploitable by an attacker for reproducing the original image. A robust encryption system should minimize this correlation to its lowest feasible extent, ideally approaching zero. This correlation value serves as a crucial metric for evaluating the system's efficacy.

**Table 6.** Cipher image correlation

| Image No. | Horizontal | Vertical | Diagonal |
|---|---|---|---|
| Img1 | 0.0087 | -0.0068 | 7.7766e-04 |
| Img2 | -0.0034 | -1.0498e-06 | 0.0026 |
| Img3 | 0.0059 | 0.0064 | -0.0033 |
| Img4 | -0.0100 | 0.0021 | -0.0087 |

4.3.4 Analysis of differential constants

Two encrypted images, derived from $Ci_1$ and $Ci_2$, respectively, were considered, with their corresponding plaintext images differing by only one pixel. The mathematical expression for the Normalized Pixel Change Rate (NPCR) analysis of an image is provided by formula (8). Two encrypted images $C_1$ and $C_2$ were considered, with their corresponding clear images exhibiting a variation in only one pixel. The mathematical analysis of NPCR for an image is expressed by formula (8).

$$\begin{aligned} NPCR &= \left( \frac{1}{nm} \sum_{i,j=1}^{nm} Di(i,j) \right) * 100 \\ Di(i,j) &= \begin{cases} 1 & \text{if} \quad Ci_1(i,j) \neq Ci_2(i,j) \\ 0 & \text{if} \quad Ci_1(i,j) = Ci_2(i,j) \end{cases} \end{aligned} \tag{8}$$

The Unified Adaptive Classification for Image Denoising (UACI) mathematical analysis of an image is given by formula (9).

$$\left( \frac{1}{nm} \sum_{i,j=1}^{nm} Abs\left(Ci_1(i,j) - Ci_2(i,j)\right) \right) * 100 \tag{9}$$

The computed differential values for the reference images assessed using the proposed novel technology align with universal standards, as illustrated in Table 7. Specifically, the NPCR value approaches 99.99%, and the UACI value surpasses 34.65%. These results affirm the security of the proposed encryption system against differential attacks, a safeguard attributed to the implementation of the initial round.

**Table 7.** NPCR and UACI for different images

| Image No. | NPCR | UACI |
|---|---|---|
| Img1 | 99.61 | 33.42 |
| Img2 | 99.60 | 33.43 |
| Img3 | 99.62 | 33.42 |
| Img4 | 99.63 | 33.45 |

Table 8 provides a comparative analysis of alternative methodologies, affirming the straightness of the proposed system.

**Table 8.** Examination of correlation and differential constants

| Image No. | Correlation | NPCR | UACI |
|---|---|---|---|
| Lena | 0.00032 | 99.97 | 34.68 |
| 42 | -0.0016 | 99.6017 | 28.137 |
| 43 | 0.0036 | 99.617 | 29.932 |
| Peppers | -0.0025 | 99.87 | 34.96 |
| 42 | -0.0125 | 99.618 | 29.168 |
| 43 | 0.0040 | 99.61 | 29.049 |

#### 4.3.5 Analysis of avalanche effect

The avalanche effect represents an essential characteristic present in nearly all cryptographic hash functions and block-coding algorithms. It induces increasingly significant alterations as data propagates through the algorithmic structure. This constant determines the avalanche impact within the cryptographic framework. Its approximation is expressed by formula (10).

$$\left( \frac{\sum_i \text{ bit change}}{\sum_i \text{ bit total}} \right) * 100 \tag{10}$$

Table 9 displays the avalanche effect values obtained from the images tested using the proposed method.

**Table 9.** Avalanche effect values

| Image | Cyphered Image |
|---|---|
| Img 1 | 51.03 |
| Img 2 3 | 50.24 |
| Img 3 4 | 50.11 |
| Img 4 | 50.05 |

The avalanche effect values derived from the images analyzed by the proposed technology offer robust defense against differential attacks.

#### 4.3.6 Math security

The chaotic sequences employed in this study demonstrate a remarkable sensitivity to initial conditions. Simultaneously, the considerable length of the proposed encryption key provides the system with robust defense against brute force attacks. The introduction of randomness via permutation additionally amplifies the intricacy of potential attacks. Finally, the incorporation of robust chaining mechanisms in both towers guarantees the resilience of the novel encryption system against any recognized form of attack.

#### 4.3.7 Benefits of this procedure

This approach has various advantages, some of which are highlighted as follows:

• Encryption keys generated from chaotic cards exhibit high sensitivity to first conditions, posing a challenge in accurately reconstructing the actual key employed.

• The utilization of an S-box structure, regulated by a chaotic decision vector, enhances the attack complexity of the proposed methodology.

• The pseudorandom sizing of the substitution table poses challenges in reconstructing the utilized S-boxes.

• Non-commutative algebraic operations contribute to the robustness of the system.

• The proposed approach is applicable to images of varying sizes and formats.

#### 4.3.8 Limitations

The effectiveness of the approach is predominantly influenced by the constraints imposed by the selection of chaotic maps, the design of S-boxes, and the pseudo-random characteristics of the generated S-boxes.

## 5 Conclusion

Satisfactory results have been achieved using two recently constructed substitution tables derived from pseudo-random linear congruence generators in conjunction with new Vigenère functions. Additionally, combining pixel-level operations followed by DNA-level genetic crossover has yielded promising results in the domain of encrypting voluminous data with high redundancy and correlation. Implementing chaining functions protects the system against any differential attacks. The minimal encryption time encourages all researchers to implement the proposed approach

in a video sequence encryption system. The efficiency of the encryption process underscores the viability of further enhancements to increase the method's effectiveness.

Future perspectives include the integration of additional algorithms into the proposed method, such as wavelet transformations, reinforcement learning, supervised learning, and fuzzy methods.

### Data Availability

The data used to support the research findings are available from the corresponding author upon request.

### Conflicts of Interest

The authors declare no conflict of interest.

### References


[1] H. P. Wen and Y. T. Lin, "Cryptanalysis of an image encryption algorithm using quantum chaotic map and DNA coding," *Expert Syst. Appl.*, vol. 237, p. 121514, 2024. https://doi.org/10.1016/j.eswa.2023.121514

[2] T. Shah and T. Ul Haq, "Construction of 24-by-24 nonlinear layer for symmetric algorithm and its application to data encryption in parallel with DNA transform," *J. Supercomput.*, vol. 80, no. 1, pp. 1037–1058, 2024. http://doi.org/10.1007/s11227-023-05512-9

[3] C. F. Hu, Z. H. Li, Y. H. Xu, C. Zhang, X. M. Liu, D. J. He, and L. H. Zhu, "Multi-round efficient and secure truth discovery in mobile crowdsensing systems," *IEEE Internet Things J.*, vol. 11, no. 10, pp. 17 210–17 222, 2024. http://doi.org/10.1109/JIOT.2024.3359757

[4] H. El Bourakkadi, A. Chemlal, H. Tabti, M. Kattass, A. Jarjar, and A. Benazzi, "Improved Vigenère using affine functions surrounded by two genetic crossovers for image encryption," *Indones. J. Electr. Eng. Comput. Sci.*, vol. 34, no. 3, p. 1787, 2024. http://doi.org/10.11591/ijeecs.v34.i3.pp1787-1799

[5] Q. M. Jiang, S. M. Yu, and Q. X. Wang, "Cryptanalysis of an image encryption algorithm based on two-dimensional hyperchaotic map," *Entropy*, vol. 25, no. 3, p. 395, 2023. https://doi.org/10.3390/e25030395

[6] K. Shreya Narasimhan and R. Bala Krishnan, "Text steganography: Enhanced character-level embedding algorithm using font attribute with increased resilience to statistical attacks," *Multimed. Tools Appl.*, 2024. https://doi.org/10.1007/s11042-024-19272-y

[7] H. El Bourakkadi, A. Chemlal, H. Tabti, M. Kattass, A. Jarjar, and A. Benazzi, "Improved Vigenère approach incorporating pseudorandom affine functions for encrypting color images," *Int. J. Electr. Comput. Eng.*, vol. 14, no. 3, p. 2684, 2024. https://doi.org/10.11591/ijece.v14i3.pp2684-2694

[8] N. R. Zhou, L. L. Hu, Z. W. Huang, M. M. Wang, and G. S. Luo, "Novel multiple color images encryption and decryption scheme based on a bit-level extension algorithm," *Expert Syst. Appl.*, vol. 238, p. 122052, 2024. https://doi.org/10.1016/j.eswa.2023.122052

[9] I. A. Zalukhu, Z. Sitorus, S. Suhardiansyah, and N. Septiani, "Enhancing text messages with a combination of Vigenère cipher and one time pad using random key LFSR," *Jurnal Sains Dan Teknol.*, vol. 6, no. 1, pp. 52–57, 2024. https://doi.org/10.55338/saintek.v6i1.3190

[10] A. AlSideiri, S. AlShamsi, H. AlBreiki, M. AlMoqbali, M. AlMaamari, and S. AlSaadi, "Cybersecurity enhancement through hybrid encryption: Combining RSA and Vigenère algorithms in the cypher-X system," *Baghdad Sci. J.*, vol. 21, no. 5SI, pp. 1765–1765, 2024. https://doi.org/10.21123/bsj.2024.10539

[11] D. Gautam, C. Agrawal, P. Sharma, M. Mehta, and P. Saini, "An enhanced cipher technique using Vigenère and modified Caesar Cipher," in *2018 2nd International Conference on Trends in Electronics and Informatics (ICOEI)*, Tirunelveli, India, 2018, pp. 1–9.

[12] M. Kattass, H. Rrghout, M. Jarjar, A. Jarjar, F. Gmira, and A. Benazzi, "Chaotic image encryption using an improved Vigenère cipher and a crossover operator," in *Computing, Internet of Things and Data Analytics. ICCIDA 2023. Studies in Computational Intelligence*, 2023.

[13] L. M. Rodriguez-R, R. E. Conrad, T. Viver, D. J. Feistel, B. G. Lindner, S. N. Venter, L. H. Orellana, R. Amann, R. Rossello-Mora, and K. T. Konstantinidis, "An ANI gap within bacterial species that advances the definitions of intra-species units," *Microb. Genet.*, vol. 15, pp. e02 696–23, 2024.

[14] Y. F. Wang, L. Teng, and X. Y. Wang, "An image encryption algorithm based on circular rotation and generalized Feistel structure," *Soft Comput.*, vol. 28, pp. 4335–4358, 2024.

[15] A. Bhattacharjee, R. Bhaumik, A. Dutta, M. Nandi, and A. Raychaudhuri, "BBB security for 5-round even-mansour-based key-alternating Feistel ciphers," *Des. Codes Cryptogr.*, vol. 92, pp. 13–49, 2024.

[16] D. Zakharov and M. Pudovkina, "Full round impossible differentials for Feistel ciphers," *J. Comput. Virol. Hack. Tech.*, vol. 20, pp. 295–300, 2024.

[17] S. Kumar and D. Sharma, "A chaotic based image encryption scheme using elliptic curve cryptography and genetic algorithm," *Artif. Intell. Rev.*, vol. 57, p. 87, 2024.

[18] N. A. El Salam Mohamed, H. El-Sayed, and A. Youssif, "Mixed multi-chaos quantum image encryption scheme based on Quantum Cellular Automata (QCA)," *Fractal Fract.*, vol. 7, no. 10, p. 734, 2023.

[19] A. Abid, Y. Qobbi, A. Benazzi, M. Jarjar, and A. Jarjar, "Two enhanced feistel steps for medical image encryption," in *2022 IEEE 3rd International Conference on Electronics, Control, Optimization and Computer Science (ICECOCS)*, Fez, Morocco, 2022, pp. 1–4.

[20] P. K. Behera and S. Gangopadhyay, "Evolving bijective S-Boxes using hybrid adaptive genetic algorithm with optimal cryptographic properties," *J. Ambient Intell. Humaniz. Comput.*, vol. 14, pp. 1713–1730, 2023.

[21] A. Abid, M. Jarjar, M. Kattass, H. Rrghout, A. Jarjar, and A. Benazzi, "Genetic algorithm using feistel and genetic operator acting at the bit level for images encryption," *Int. J. Saf. Secur. Eng.*, vol. 14, no. 1, pp. 15–27, 2024. https://doi.org/10.18280/ijsse.140102

[22] H. Tabti, H. EL Bourakkadi, A. Chemlal, A. Jarjar, K. Zenkouar, and S. Najah, "Genetic crossover at the RNA level for secure medical image encryption," *Int. J. Saf. Secur. Eng.*, vol. 14, no. 1, pp. 201–216, 2024. https://doi.org/10.18280/ijsse.140120

[23] J. M. Zheng and Y. B. Tian, "An image encryption algorithm using cascade chaotic map and S-box," *Entropy*, vol. 24, no. 12, p. 1827, 2022. https://doi.org/10.3390/e24121827

[24] A. Latoui and M. E. H. Daachi, "A two-parameter extended logistic chaotic map for modern image cryptosystems," *Digit. Signal Process.*, vol. 148, p. 104463, 2024. https://doi.org/10.1016/j.dsp.2024.104463

[25] Z. Q. Zhang, Y. Wang, L. Y. Zhang, and H. Zhu, "A novel chaotic map constructed by geometric operations and its application," *Nonlinear Dyn.*, vol. 102, pp. 2843–2858, 2020. https://doi.org/10.1007/s11071-020-06060-0

[26] A. Jarjar, M. Jarjar, A. Abid, M. Jarjar, S. El Kaddouhi, and A. Benazzi, "A single Vigenère circuit and two genetic operators interacting at the DNA level are combined to encrypt a color image," *Preprint, Research Square*, 2023. https://doi.org/10.21203/rs.3.rs-2462868/v1

[27] A. Jarjar, A. Abid, S. El Kaddouhi, M. Kattass, and A. Benazzi, "An altered Vigenère circuit used in a genetic cross again for encryption of medical images," *Preprint, Research Square*, 2023. https://doi.org/10.21203/rs.3.rs-2766159/v1

[28] H. El Bourakkadi, A. Chemlal, H. Tabti, M. Kattass, A. Jarjar, and A. Benazzi, "Enhanced color image encryption utilizing a novel vigenere method with pseudorandom Affine functions," *Acadlore Trans. Mach. Learn.*, vol. 3, no. 1, pp. 36–56, 2024. https://doi.org/10.56578/ataiml030104

[29] B. W. Zhang and L. F. Liu, "Chaos-based image encryption: Review, application, and challenges," *Mathematics*, vol. 11, no. 1, p. 2585, 2023. https://doi.org/10.3390/math11112585

[30] X. Y. Yao, R. Z. Xie, X. Z. Zan, Y. Q. Su, P. Xu, and W. B. Liu, "A novel image encryption scheme for dna storage systems based on DNA hybridization and gene mutation," *Interdiscip. Sci. Comput. Life Sci.*, vol. 15, pp. 419–432, 2023. https://doi.org/10.1007/s12539-023-00565-z

[31] X. Y. Gao, B. Sun, Y. H. Cao, S. Banerjee, and J. Mou, "A color image encryption algorithm based on hyperchaotic map and DNA mutation," *Chinese Phys. B*, vol. 32, p. 030501, 2023. https://doi.org/10.1088/1674-1056/ac8cdf

[32] R. A. Elmanfaloty, A. M. Alnajim, and E. Abou-Bakr, "A finite precision implementation of an image encryption scheme based on DNA encoding and binarized chaotic cores," *IEEE Access*, vol. 9, pp. 136 905–136 916, 2021. https://doi.org/10.1109/ACCESS.2021.3118050

[33] S. Khan, L. Han, H. Lu, K. K. Butt, G. Bachira, and N. U. Khan, "A new hybrid image encryption algorithm based on 2D-CA, FSM-DNA rule generator, and FSBI," *IEEE Access*, vol. 7, pp. 81 333–81 350, 2019. https://doi.org/10.1109/ACCESS.2019.2920383

[34] Q. Liu and L. F. Liu, "Color image encryption algorithm based on DNA coding and double chaos system," *IEEE Access*, vol. 8, pp. 83 596–83 610, 2020. https://doi.org/10.1109/ACCESS.2020.2991420

[35] S. Al_Mola, "A review in use of 4D hyper chaotic systems and DNA for image encryption," *Al-Salam J. Eng. Tech.*, vol. 2, no. 1, pp. 94–102, 2023. https://doi.org/10.55145/ajest.2023.01.01.0011

[36] D. Z. Zhang, X. C. Wen, C. Yan, and T. Y. Li, "An image encryption algorithm based on joint RNA-level permutation and substitution," *Multimed. Tools Appl.*, vol. 82, pp. 23 401–23 426, 2023. https://doi.org/10.1007/s11042-022-14255-3

[37] M. Soltani, H. Shakeri, and M. Houshmand, "A robust hybrid algorithm for medical image cryptography using patient biometrics based on DNA and RNA computing," *Preprint, Research Square*, vol. 2023. http://doi.org/10.21203/rs.3.rs-3314772/v1

[38] M. Y. Sun, W. H. Cui, Y. Tao, and T. W. Shi, "Chaotic color image encryption algorithm based on RNA operations and heart shape chunking," *IAENG Int. J. Comput. Sci.*, vol. 50, no. 1, p. 121, 2023.

[39] M. Tahbaz, H. Shirgahi, and M. Yamaghani, "Evolutionary-based image encryption using Magic Square Chaotic algorithm and RNA codons truth table," *Multimed. Tools Appl.*, vol. 83, pp. 503–526, 2024. https://doi.org/10.1007/s11042-023-15677-3

[40] L. J. Zhao, L. L. Zhao, F. P. Cui, and T. T. Sun, "Satellite image encryption based on RNA and 7D complex chaotic system," *Vis. Comput.*, vol. 2023, pp. 1–21, 2023. https://doi.org/10.1007/s00371-023-03128-x

[41] M. Talhaoui, X. Wang, and M. Midoun, "A new one-dimensional cosine polynomial chaotic map and its use in image encryption," *Vis. Comput.*, vol. 37, pp. 541–551, 2021. https://doi.org/10.1007/s00371-020-01822-8

[42] S. Y. Wang, L. Hong, and J. Jiang, "An image encryption scheme using a chaotic neural network and a network with multistable hyperchaos," *Optik*, vol. 268, p. 169758, 2022. https://doi.org/10.1016/j.ijleo.2022.169758

[43] K. A. Telem, H. Fotsin, and J. Kengne, "Image encryption algorithm based on dynamic DNA coding operations and 3D chaotic systems," *Multimed. Tools Appl.*, vol. 80, pp. 19 011–19 041, 2021. https://doi.org/10.1007/s11042-021-10549-0