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

Enhanced Color Image Encryption Utilizing a Novel Vigenere Method with Pseudorandom Affine Functions

Hamid El Bourakkadi[1*], Abdelhakim Chemlal[1], Hassan Tabti[2], Mourad Kattass[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: Hamid El Bourakkadi (hamid.elbourakkadi.d23@ump.ac.ma)

Received: 01-03-2024 **Revised:** 02-28-2024 **Accepted:** 03-05-2024

Citation: 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.

Abstract: In the realm of digital image security, this study presents an innovative encryption methodology for color images, significantly advancing the traditional Vigenere cipher through the integration of two extensive pseudorandom substitution matrices. These matrices are derived from chaotic maps widely recognized for their cryptographic utility, specifically the logistic map and the skew tent map, chosen for their straightforward implementation capabilities in encryption systems and their high sensitivity to initial conditions. The process commences with the vectorization of the original image and the computation of initial values to alter the starting pixel's value, thereby initiating the encryption sequence. A novel aspect of this method is the introduction of a Vigenere mechanism that employs dynamic pseudorandom affine functions at the pixel level, enhancing the cipher's robustness. Subsequently, a comprehensive permutation strategy is applied to bolster the vector's integrity and elevate the temporal complexity against potential cryptographic attacks. Through simulations conducted on a varied collection of images, encompassing different sizes and formats, the proposed encryption technique demonstrates formidable resilience against both brute-force and differential statistical attacks, thereby affirming its efficacy and security in safeguarding digital imagery.

Keywords: Reversible affine function; Hybrid chaining; Chaotic map; Global permutation; Substitution box

1 Introduction

Ciphering images is the process of protecting them by altering their pixels in a way that makes them indecipherable. It protects image confidentiality and integrity, particularly when the images are sensitive and confidential, as in the military case [1] and medical images [2, 3]. Perturbations in ciphering steps complicate the statistical relationships between original and ciphered images and make predicting them difficult. Diffusion, on the other hand, distributes data in its initial form efficiently and uniformly throughout the entire ciphered image. Encryption methods achieve diffusion and confusion [4, 5] through dense substitution and permutation of each pixel. Substitution is performed by changing the image pixel values to other values. Permutation randomly arranges image pixels [6] to conceal the statistical relationships between the image pixels. Various methods can be used for replacement, such as the substitution box (S-box) operation [7–9]. As the patterns of replacement and permutations become more difficult, the situation becomes more unpredictable and complex. Therefore, a combination of replacement, which integrates dynamic affine functions, and permutations must be applied at the smallest unit of images, which is the pixel.

The most important component of the ciphering process is the key, which plays a vital role in protection and ciphering data confidentiality. Hence, the key must satisfy various criteria, encompassing considerations such as length, space, and complexity [10, 11]. This implies that the user-inputted key for image encryption needs preprocessing to generate a more intricate form, such as a pseudorandom sequence [12]. However, these keys can also be changed by simply performing standard operations, such as rearranging the image stream [13]. In the current context of modern image encryption, the use of keys can produce real sequences of chaotic behavior that are sensitive to initial conditions, thus providing a high level of security [14]. Chaotic methods have various variations, some of which are renowned for image ciphering, such as piecewise linear chaotic maps (PWLCMs), logistic, Henon,

and skew tent maps [15–18]. Focusing on the logistic and skew tent maps, they present several advantages, such as improving randomness and sensitivity, leading to more chaotic, unique, and secure sequences.

Most of the algorithms mentioned above use independent block encryption. Consequently, all these techniques remain vulnerable to statistical attacks. Moreover, the small size of their private keys exposes them to brute-force attacks. Additionally, in the absence of any diffusion or chaining function between the encrypted blocks and plaintext blocks, these techniques remain susceptible to differential attacks.

This study aims to develop a new image encryption cryptosystem using a large private key to guard against brute-force attacks. Additionally, diffusion and confusion functions are employed to ensure that the cryptosystem remains beyond the reach of differential attacks, placing the new technique out of the scope of any such attacks. Similarly, the integration of multiple pseudo-random vectors in the confusion process ensures strong protection against statistical attacks.

The rest of this study is divided into various sections, namely, a section on previous related work, detailing the assumptions and related research; a section describing the theoretical framework, explaining the basis of chaotic sequences, as well as classical Vigenere and affine techniques; a section detailing the proposed approach, revealing the nuances of the encryption and decryption processes; a section devoted to results and discussions, presenting the research findings, discussions, and comparisons with other similar techniques; and a section summarizing the findings and proposing research directions.

2 Related Works

The prior sections explored the potential significance of confusion and diffusion features in image ciphering, applied across substitution and permutation procedures. Another aspect to highlight concerns the ciphering key quality. Research in the prior research on the design of methods that exploit permutation and substitution patterns, as well as on improving key qualities, has been a source of motivation for this study. Initially, substitution and permutation ciphering methods were applied exclusively to pixels. Recent research, such as the study of Sabir and Guleria [19], highlights the increasing popularity of pixel-level substitutions and permutations as image processing techniques. Zhang and Tian [20] presented a multiple image ciphering approach relying on 3D bit planes and a genetic central dogma to perform a permutation between bit planes. Similarly, Ramasamy et al. [21] proposed an improved logistic map that included diffusion, key stream generation, and permutation to resist assaults. Wu et al. [22] presented a method based on the deoxyribonucleic acid (DNA) genomic sequence permutation operation that coupled one-way mapping networks with an XOR operation. Butt et al. [23] introduced a new image ciphering method using binary bit plane scrambling and the SPD bit plane diffusion technique for an ordinary image, incorporating elements of the card game technique. Li [24] investigated the resilience of HCIE when faced with a known-plaintext-only attack and a known-plaintext/chosen-plaintext attack. Khan et al. [25] proposed a new DNA-based method capable of performing the simultaneous functions of bit plane searching and pixel diffusion in a single step. Zhang et al. [26] proposed an improved algorithm aimed at eliminating potential security issues in Liu's algorithm. However, Wang and Zhang [27] proposed a novel approach to color image encryption that utilizes a combination of heterogeneous bit permutation and correlated chaos techniques. A new bit-level image ciphering method proposed by Xu et al. [28] is based on PWLCMs. First, the ordinary image is transformed into two binary sequences of the same size. Second, a new diffusion strategy is introduced to mutually diffuse the two sequences. Niyat et al. [29] proposed an image ciphering method based on a self-organized structure with a set of units updated according to rules that depend on the number of limited neighboring units. Chen et al. [30] presented a solution for protected and efficient image ciphering using adaptive permutation-diffusion and random DNA coding, where the permutation and diffusion procedures are perturbed by the intrinsic characteristics of the plaintext. However, Ye and Huang [31] proposed an efficient symmetric image ciphering technique to resolve the low-sensitivity issue of an ordinary image. Recently, Chen et al. [32] developed an enhanced digital image ciphering method using a collage model and a one-dimensional quadratic chaotic system, thus expanding the key space that offers robust resilience against exhaustive attacks. Wang et al. [33] proposed an improved 3D chaotic system characterized by various dynamic behaviors, such as phase shifts and expansion and contraction phenomena that vary with parameter changes. The proposed model covers a wide chaotic range and demonstrates its applicability in image encryption processes. Hence, a color image ciphering method based on a hypercomplex chaotic system and a skew tent map was proposed by Kadir et al. [34]. Wu et al. [35] proposed a new color image ciphering method based on DNA, one-time keys, spatiotemporal chaos and sequence operations. Liu et al. [36] proposed a quantum image ciphering scheme based on permutation using an improved quantum representation model and realized consecutive intraputation by sorting an interpermutation and chaotic sequence operations involving the qubit XOR process between chosen bit planes. However, Winarno et al. [37] proposed a combination of several intertwined patterns, incorporating zigzag, Hilbert, and Morton patterns, to aggregate confusion-diffusion and improve complexity and randomness. Thus, Aung et al. [38] proposed a poly-alphabetic cipher that constitutes a new system for encrypting and decrypting data.

The mentioned systems generally use small-size substitution tables, namely 16×16, which constitute a simple

permutation that does not influence the statistical distribution of pixels. This leads to vulnerability to statistical attacks. Additionally, the replacement functions are defined by simple analytical expressions. Similarly, techniques using genetic algorithms operating at the DNA level typically exhibit a static notation, such as the conversion from Z/4Z to DNA.

The new trends in the field of symmetric cryptography involve the use of genetic algorithms through the application of specific genetic operators adapted to the encryption of voluminous data, typically acting at the level of DNA and ribonucleic acid (RNA). On the other hand, researchers are attempting to utilize Euclidean networks for symmetric encryption of textual data.

The contribution of this study lies in overcoming all anomalies indicated in prior research and developing a new image encryption cryptosystem using two large substitution tables of sizes (256; 256), accompanied by dynamic affine functions for diffusion restoration. Furthermore, the size of the private key in the cryptosystem far exceeds 100 bits, placing the new technique beyond the reach of any differential attacks.

3 Theoretical Background

This section introduces the chaotic maps, classical Vigenere, and affine ciphering methods used in this work.

3.1 Skew Tent Map

This map [28] is a one-dimensional map expressed by Eq. (1).

$$\begin{cases} h_0 \in [0.5, 1], \quad k \in [3.75, 4] \\ h_{n+1} = \begin{cases} \frac{h_n}{k} \; si \; 0 < h_n < k \\ \frac{1-h_n}{1-k} \; sinon \end{cases} \end{cases} \tag{1}$$

where, h_0 and k represent the initial state and its control parameter, respectively.

3.2 Logistic Map

The second chaotic sequence is generated by the logistic map [19]. It is a simple polynomial-degree recurrent sequence defined by Eq. (2).

$$\begin{cases} l_0 \in [0.5, 1] \text{ and } \delta \in [3.75, 4] \\ l_{n+1} = \delta \cdot l_n \left(1 - l_n\right) \end{cases} \tag{2}$$

3.3 Classical Vigenere Method

The classical Vigenere cipher system is based on a matrix (Vt) of fixed dimensions (26, 26) reserved for text encryption only. It is defined by Algorithm 1.

Algorithm 1. Classical Vigenere S-box

for $i = 1$ to 26 // 1ère ligne
    $Vt(1, i) = i$
end for
for $i = 1$ to 26 // lignes suivantes
    for $j = 1$ to 26
        $Vt(i, j) = Vt(i - 1, \bmod(j + 1, 26))$
    end for
end for

Let Pk be the plain message, Ck be the cipher message, Ke be the encryption key, Vt be the Vigenere matrix, and n be the length of the plain message. The encryption and decryption algorithms associated with the classical Vigenere method are given in Algorithm 2.

Algorithm 2. Classical Vigenere encryption and decryption algorithms

//Chiffrement
for $i = 1$ to n
  $Ck_i = Vt\left(Pk_i, Ke_i\right) = Pk_i + Ke_i \bmod 26$
end for
//Déchiffrement
for $i = 1$ to n
  $Pk_i = Vt\left(Ck_i, Ke_i\right) = Ck_i - Ke_i \bmod 26$
end for

The classical Vigenere method uses a small 26×26 substitution table, whose static and public default makes the method easier to attack. Similarly, the simple analytical expression of the classical Vigenere substitution function is easily reconstructed.

3.4 Classical Affine Method

Let f be an affine function defined in the ring Z/nZ by Eq. (3).

$$\begin{cases} f : Z/nZ & \to Z/nZ \\ x & \mapsto \mathrm{mod}(ax+b;n) \end{cases} \quad a,b \in Z/nZ \tag{3}$$

The function f is bijective in (Z/nZ) if and only if (a) is invertible and (b) is any.

Indeed, $y = \mathrm{mod}(ax+b;n)$ is obtained.

Then, $ax = \mathrm{mod}(y-b;n)$ and $x = \mathrm{mod}\left(a^{-1}\cdot(y-b);n\right)$, where, a^{-1} is the inverse of a in ring Z/nZ. Or, a is invertible in (Z/nZ) if and only if $\mathrm{a} \wedge \mathrm{n} = 1$.

Particular case:

$n = 2^k, k \in N$ Particular case, then a is invertible in ring $Z/2^kZ$ if and only if a is odd.

Example in a ring Z/16Z: Table 1 represents an example of affine functions in ring Z/16Z.

Table 1. Affine function example in a ring Z/16Z

x	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
f(x)=mod(5x+12; 16)	12	1	6	11	0	5	10	15	4	9	14	1	8	13	2	7

Note: f is an invertible function of the ring Z/16Z.

The classical affine transformation is static and thus remains vulnerable to any brute-force attack. The shortcomings of traditional Vigenère and affine systems have been previously outlined in this study. To overcome all these flaws, substitution tables of large size are used, specifically 256×256, generated from pseudorandom vectors employing new replacement and diffusion functions involving more than one S-box. Similarly, the affine functions used are dynamic and pseudorandom.

4 The Proposed Method

This new technique uses the two most widely deployed chaotic maps in the field of cryptography [18, 19] by integrating large S-boxes and strong affine diffusion functions [20, 39]. This technique is structured around the axes described below.

4.1 Used Chaotic Sequences

Two chaotic sequences h and l that are extremely sensitive to the initial conditions and easy to implement in any cryptosystem are used in this approach, as described above.

4.2 Subkey Construction

Seven pseudorandom vectors $Vc1, Vc2, Vc3, Vr, Ve, Va$, and Vb with coefficients in the ring $Z/256Z$ are generated by Algorithm 3 below.

Algorithm 3. Pseudorandom vector generation

for $i = 1$ to 3 nm

// Confusion vectors

$\mathrm{Vc\,1(i)} = \left[\mathrm{E}\left(\mathrm{sup(h(i);1(i))}\cdot 10^{11}\right) \bmod 253\right] + 2$

$Vc2(i) = \left[E\left(((h(i)+2*l(i))/3)\cdot 10^{11}\right) \bmod 254\right] + 1$

$Vc3(i) = \left[E\left(|h(i)-l(i)|\cdot 10^{10}\right) \bmod 254\right] + 1$

// Translation vectors

$Vr(i) = \left[E\left((h(i)+l(i))\cdot 10^{12}\right) \bmod 253\right] + 2$

$Ve(i) = \left[E\left(\left(\frac{2*h(i)+3*l(i)}{5}\right)\cdot 10^{12}\right) \bmod 253\right] + 2$

// Multiplication vectors

$Va(i) = \left[2*E\left((h(i)+l(i))\cdot 10^{12}\right)+1\right] \bmod 253 + 4$

$Vb(i) = \left[2*E\left((h(i)*l(i))\cdot 10^{12}\right)+1\right] \bmod 253 + 4$

end for

The two vectors Va and Vb contain only the invertible elements in the ring $Z/256Z$. In addition, the system requires the generation of three binary vectors, $Ba1, Ba2$ and $Ba3$, to control the encryption process. These two vectors are generated by Algorithm 4.

Algorithm 4. (Ba_i) Binary random vector generation, $i \in \{1, 2, 3\}$

// Binary vectors construction
for $i \leftarrow 1$ to 3 nm
if $h(i) > l(i)$ then
  $\text{Ba}_1(i) \leftarrow 0$
else
  $\text{Ba}_1(i) \leftarrow 1$
end if
if $h(i) > 0.5$ then
  $\text{Ba}_2(i) \leftarrow 0$
else
  $\text{Ba}_2(i) \leftarrow 1$
end if
if $h(i) \leq l(i)$ then
  $\text{Ba}_3(i) \leftarrow 0$
else
  $\text{Ba}_3(i) \leftarrow 1$
end if; end for

4.3 Substitution Table Construction

The algorithm requires the development of two new replacement tables Tv1 and Tv2, each of size (256; 256) and with coefficients in the ring Z/256Z.

4.3.1 Tv1 S-box construct

The main mission of this section is to construct the new Vigenere substitution matrix, called Tv1, with a size of (256; 256), following the instructions provided below.

• The first row of the table $Tv1$ is the permutation $Pt1$ of the first 256 values of the vector $Vc1$, obtained by sorting them in decreasing order.

• For ranks higher than 1, the rank line is a rank shift $Vc2(i)$ or $Vc3(i)$, depending on the value of the control vector $Ba1(i)$. This table was generated by Algorithm 5.

Algorithm 5. Tv1 S-box construction

for $i \leftarrow 1$ to 256
  $Tv1(1, i) \leftarrow \text{Pt1}(i)$
end for
for $i \leftarrow 2$ to 256
  if $Ba1(i) = 0$ then
    for $j \leftarrow 1$ to 256
      $Tv1(i, j) \leftarrow Tv1(i - 1, \text{mod}(j + Vc2(i), 256))$
    end for
  else
    for $j \leftarrow 1$ to 256
      $Tv1(i, j) \leftarrow Tv1(i - 1, \text{mod}(j + Vc3(i), 256))$
    end for
end for

Example:
Creation of the first line

Range	1	2	3	4	5	6	7	8
$(Vc1)$ Values	6	6	3	7	8	8	2	4
Sort	4	5	7	3	2	1	8	6

Permutation $Pt1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 4 & 5 & 7 & 3 & 2 & 1 & 8 & 6 \end{pmatrix}$

Table 2 represents an example of generation of s-box Tv1 of size (8, 8) controlled by Ba1.

Table 2. Tv1 creation example

Tv1	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**Vc2**	**Vc3**	**Bal**
1	4	5	7	3	2	1	8	6	*2*	*5*	*1*
2	1	8	6	4	5	7	3	2	**4**	6	0
3	3	2	1	8	6	4	5	7	1	**3**	1
4	7	3	2	1	8	6	4	5	**2**	3	0
5	1	8	6	4	5	7	3	2	4	**6**	1
6	7	3	2	1	8	6	4	5	**4**	1	0
7	6	4	5	7	3	2	1	8	3	**4**	1
8	7	3	2	1	8	6	4	5	**6**	6	0

4.3.2 Tv2 S-box construct

The construction of the new substitution matrix Tv2 of size (256; 256) is described by the following steps:

• The first line is the rearrangement $\mathrm{Pr}\,1$ obtained by a broad ascending sort on the first 256 values of the vector $Vc3$;

• The second line is the rearrangement $\mathrm{Pr}\,2$ obtained by a broad ascending sort on the first 256 values of the vector $Vc2$;

• The third line is the rearrangement $\mathrm{Pr}\,3$ obtained by a broad ascending sort on the first 256 values of the vector $Vc1$;

• The i-th line $(i > 3)$ is the composition of the functions of line $(i-2)$ and $(i-3)$ or $(i-3)$ and $(i-1)$, depending on the value of the control vector $\mathrm{Ba2}(i)$.

These steps are illustrated in Algorithm 6 below.

Algorithm 6. Tv2 S-box construction

for $i \leftarrow 1$ to 256
$\mathrm{Tv2}(1,i) \leftarrow \mathrm{Pr1}(i)$
$\mathrm{Tv2}(2,i) \leftarrow \mathrm{Pr2}(i)$
$\mathrm{Tv2}(3,i) \leftarrow \mathrm{Pr3}(i)$
end for
for $i \leftarrow 4$ to 256
  for $j \leftarrow 1$ to 256
    if $\mathrm{Ba2}(i) = 0$ then
      $Tv2(i,j) \leftarrow Tv2(i-2, Tv2(i-3,j))$
    else
      $Tv2(i,j) \leftarrow Tv2(i-3, Tv2(i-1,j))$
    end if
  end for
end for

Example: Tv2 creation of size (8; 8) controlled by Ba2 as shown in Table 3.

Table 3. Tv2 creation example

T v 2		1	2	3	4	5	6	7	8	Ba2
Pr 1	1	7	6	3	4	2	5	8	1	1
Pr 2	2	4	1	6	8	7	2	5	3	0
Pr 3	3	2	1	3	6	4	5	7	8	0
Pr 4 = Pr 1 o Pr 3	4	6	7	3	5	4	2	8	1	**1**
Pr 5 = Pr 2 o Pr 4	5	2	5	6	7	8	1	3	4	**1**
Pr 6 = Pr 4 o Pr 5	6	7	4	2	8	1	6	3	5	**0**
Pr 7 = Pr 4 o Pr 6	7	8	5	7	1	6	2	3	4	**1**
Pr 8 = Pr 6 o Pr 5	8	5	1	3	7	6	4	2	8	**0**

4.3.3 Expression of the improved affine function

Let f_i be the family of affine functions acting on the pixels. These functions are defined by Eq. (4).

$$\begin{cases} f_i : Z/256Z \to Z/256Z \\ x \mapsto \begin{cases} \mathrm{mod}(Va(i) * X(i) + Ve(i); 256) \; si \; Ba2 \; (i) = 0 \\ \mathrm{mod}(Vb(i) * X(i) + Vr(i); 256) \; si \; Ba2 \; (i) = 1 \end{cases} \end{cases} \tag{4}$$

Since the elements $Va(i)$ and $Vb(i)$ are invertible in ring $Z/256Z$, the functions f_i are reversible for all $i \in [1; 3\,\mathrm{nm}]$.

4.3.4 Hybrid chaining function expression

The new substitution function involving tables Tv1 and Tv2 is given by Algorithm 7.

Algorithm 7. *Fv* hybrid chaining function expression

$Z(i) = Fv(X(i))$
  if $Ba2(i) = 0$ then
    $Z(i) \leftarrow Tv1(Vc1(i), Tv2(Vc2(i), \mathrm{mod}(Va(i) \cdot X(i) + Ve(i), 256)))$
  else
    $Z(i) \leftarrow Tv2(Vc3(i), Tv1(Vc1(i), \mathrm{mod}(Vb(i) \cdot X(i) + Vr(i), 256)))$
  end if

4.4 Encryption Phase

The encryption phase unfolds through the subsequent stages:

4.4.1 Original image vectorization

This phase involves uploading the original image of dimensions (n,m) and then extracting the Red, Green and Blue (RGB) channel vectors Cr, Cg and Cb, which are concatenated under the control of the binary vector Ba1 into a single vector X of dimensions (1,3nm), as illustrated in Figure 1 below.

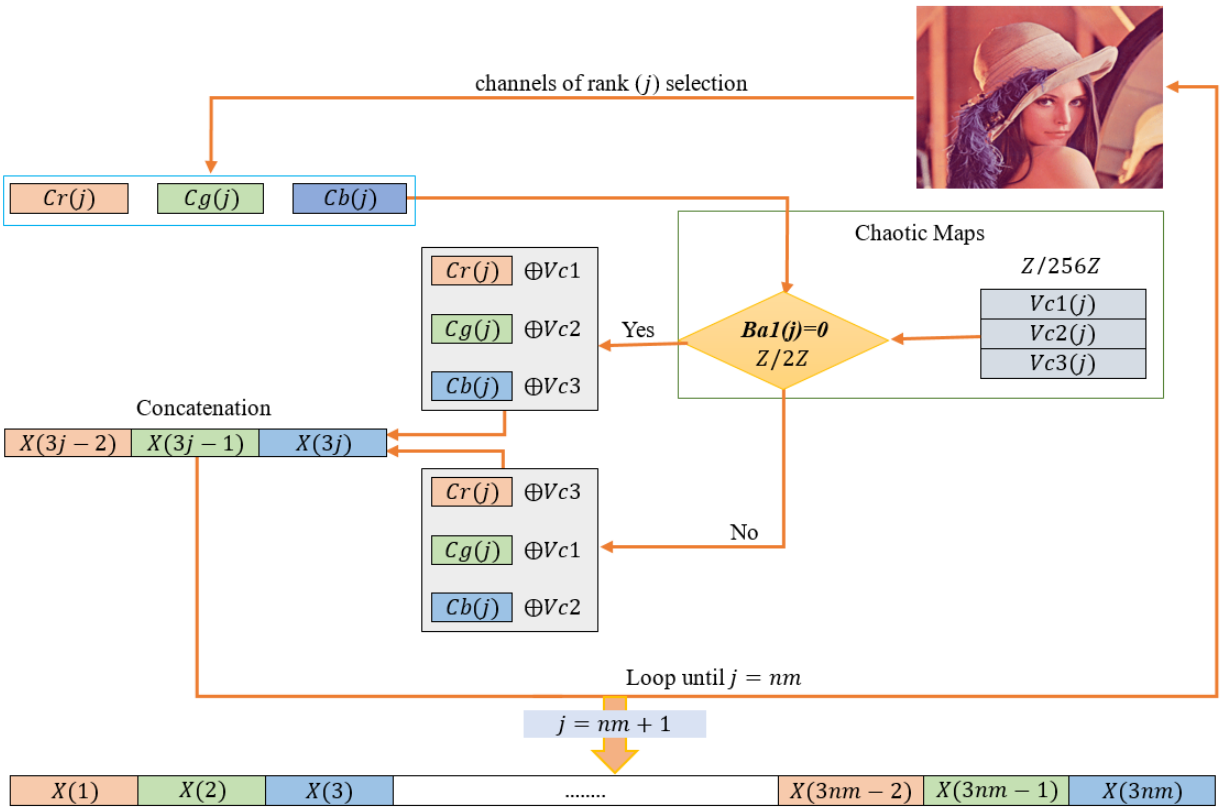

Figure 1. Original image vectorization diagram

The mathematical formulation of this phase is described in Algorithm 8.

Algorithm 8. Original image vectorization algorithm

for $j \leftarrow 1$ to nm
  if $Ba1(j) = 0$ then
    $X(3j-2) \leftarrow Cr(j) \oplus Vc1(j)$
    $X(3j-1) \leftarrow Cg(j) \oplus Vc2(j)$
    $X(3j) \leftarrow Cb(j) \oplus Vc3(j)$
  else
    $X(3j-2) \leftarrow Cr(j) \oplus Vc3(j)$
    $X(3j-1) \leftarrow Cg(j) \oplus Vc1(j)$
    $X(3j) \leftarrow Cb(j) \oplus Vc2(j)$
end if; end for

4.4.2 Improved Vigenere circuit by the affine method

This improved Vigenere lap starts by calculating the initialization value In, which is closely linked to the plain image and is intended to change the value of the starting pixel and launch the encryption phase. This value is calculated by Algorithm 9 below.

Algorithm 9. Initialization value calculation

$\text{In} = 0$
for $i = 2$ to $3nm$
  if $Ba3(i) = 0$ then
    $\text{In} = \text{In} \oplus X(i) \oplus Vc2(i)$
  else
    $\text{In} = \text{In} \oplus X(i) \oplus Vc3(i)$
  end if
end for

This algorithm is illustrated in Figure 2 below.

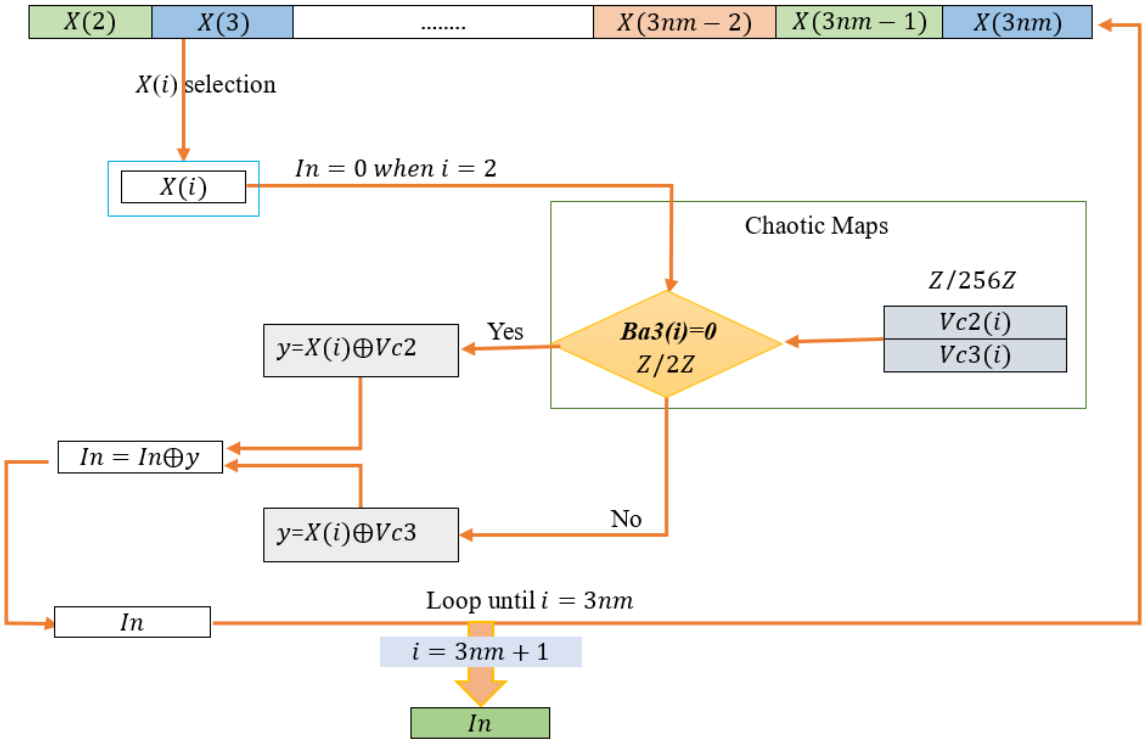

Figure 2. Initialization value calculation diagram

To overcome any differential attack, a diffusion round is first performed using the chaotic confusion vectors and a chaining between the ciphered pixels and the following plain pixels using the bijective affine functions. The diffusion process is illustrated by Algorithm 10.

Algorithm 10. Hybrid chaining function expression

//First pixel encryption
$Z(1) = Fv(X(1) \oplus In \oplus Vc1(1))$
//Next pixels encryption
for $i = 2$ to $3nm$
  $\alpha = fi(X(i)) \oplus Z(i-1)$
  if $Ba3(i) = 0$ then
    $Z(i) = Fv(\alpha \oplus Vc2(i))$
  else
    $Z(i) = Fv(\alpha \oplus Vc3(i))$
  end if
end for

This algorithm can be interpreted in Figure 3.

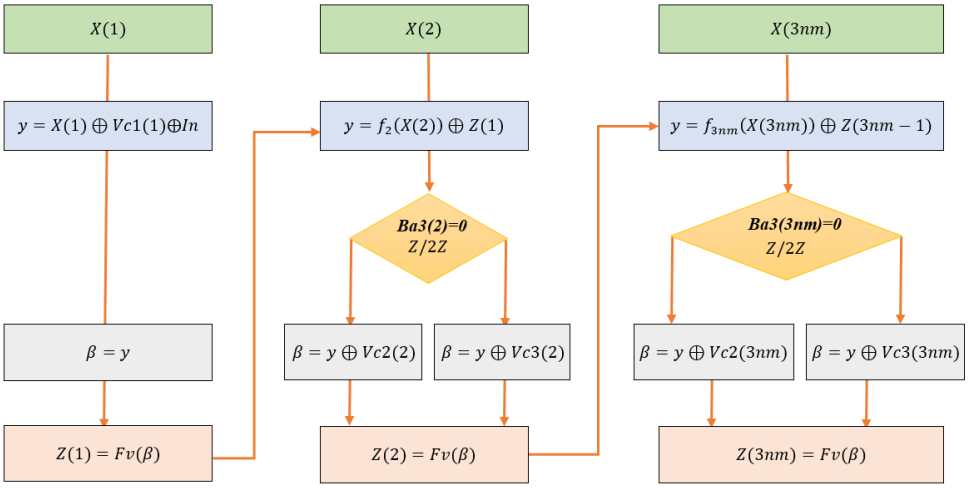

Figure 3. New circuit using dynamic pseudorandom affine functions

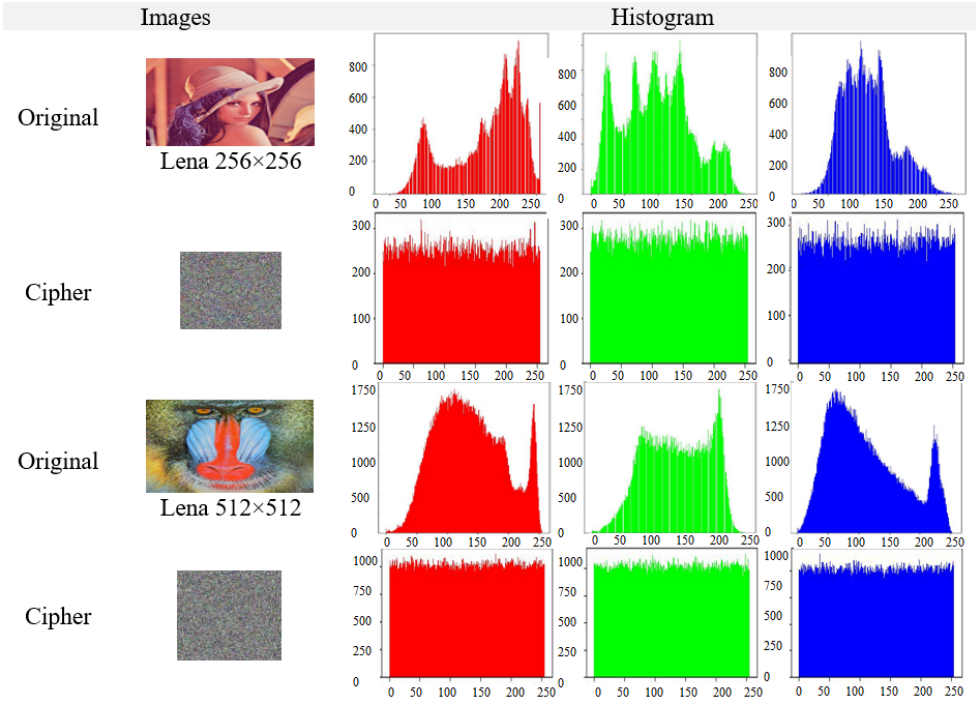

Figure 4. Ciphered image samples of different sizes and formats

4.4.3 Global permutation

To augment the attack complexity of the proposed system, the vector Z is subjected to a global rearrangement Pg process involving the first (3nm) values of the chaotic sequence l. This permutation phase is determined by the following Algorithm 11:

Algorithm 11. Global permutation

for $i = 1$ to $3nm$

$Zs(i) = Z(Pg(i))$

end for

The image generated by this new Vigenere-affine hybrid method is represented by the vector Zs.
Histograms of cipher images represented by the vector Zs is given by the Figure 4.

4.5 Phase of Decryption

The suggested encryption system is symmetric and uses two diffusion functions, which require the decryption process to start with the last intervention using the inverse functions. The encrypted image is transformed into a vector Zs with dimensions (1; 3nm) on which the following steps are executed:

- Application of the inverse permutation;
- Inverse of the affine function;
- Inverse of the improved Vigenere-affine function;
- Inverse of the diffusion function.

The decryption process is illustrated in Figure 5.

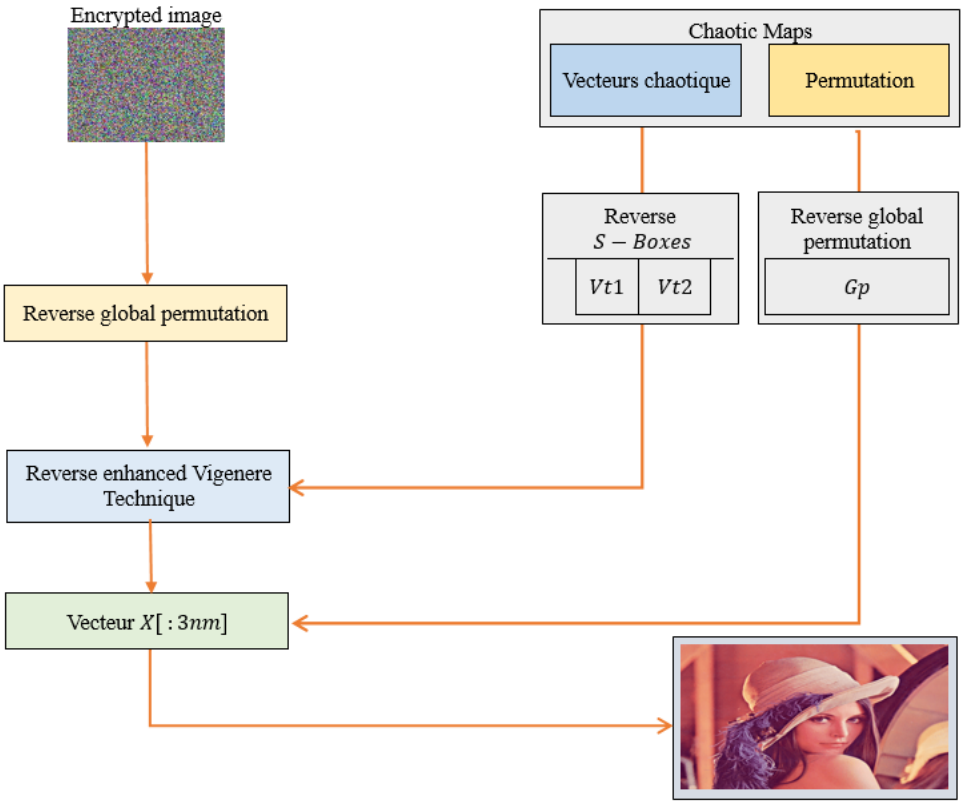

Figure 5. Decryption process

5 Results and Discussion

All simulations were executed using Python on the Windows 10 operating system, employing a hardware setup comprising an i7 processor laptop with a 1 TB hard drive and 32 GB of RAM. Figure 6 displays the main test image, "Lena," along with its encrypted and decrypted versions, as well as all plain images utilized. These image samples were sourced from the SIPI database (https://sipi.usc.edu/database/). The keys and various experimental

parameters are generated using the previously described chaotic maps. Before commencing the decryption process, it is imperative to securely transmit the secret key to the recipient through a protected channel.

Figure 6. Tested images

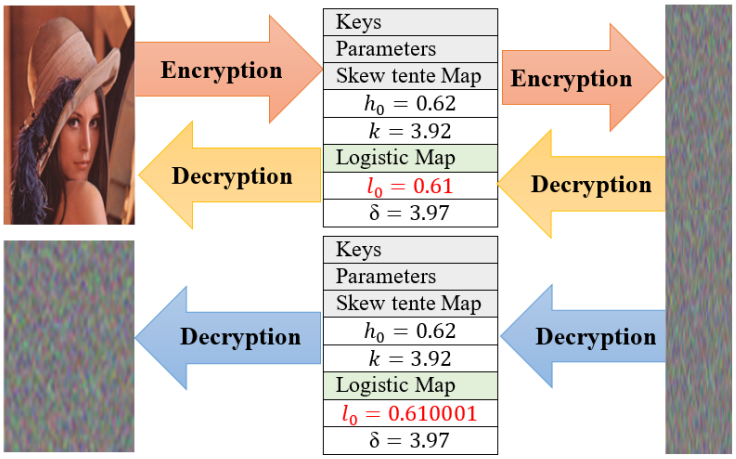

Figure 7. Key strength analysis

5.1 Statistical Attacks

The new algorithm was applied to a random selection of reference images, and the resulting simulations were documented as follows:

5.1.1 Analysis of possible key space

The system employs two chaotic maps generated using four real parameters, each represented by 32 bits, resulting in a key comprising 120 bits. This design guarantees resistance against brute-force attacks.

5.1.2 Key strength analysis

The system employs two extensively employed chaotic maps within the realm of cryptography. Their heightened sensitivity to initial conditions ensures a pronounced responsiveness to the encryption key, as illustrated in Figure 7.

As depicted in Figure 7, altering the encryption key results in the generation of two distinct encrypted images during the encryption process. Furthermore, the decryption stage produces two decrypted images with entirely distinct shapes, highlighting the proposed algorithm's heightened sensitivity to even minor changes in the encryption key.

5.1.3 Visual aspect analysis

The encrypted image, as depicted in Figure 8, exhibits a distinct visual dissimilarity from the original image. Furthermore, the algorithm ensures uniform distribution in the histograms of encrypted images, affirming robust protection against statistical attacks.

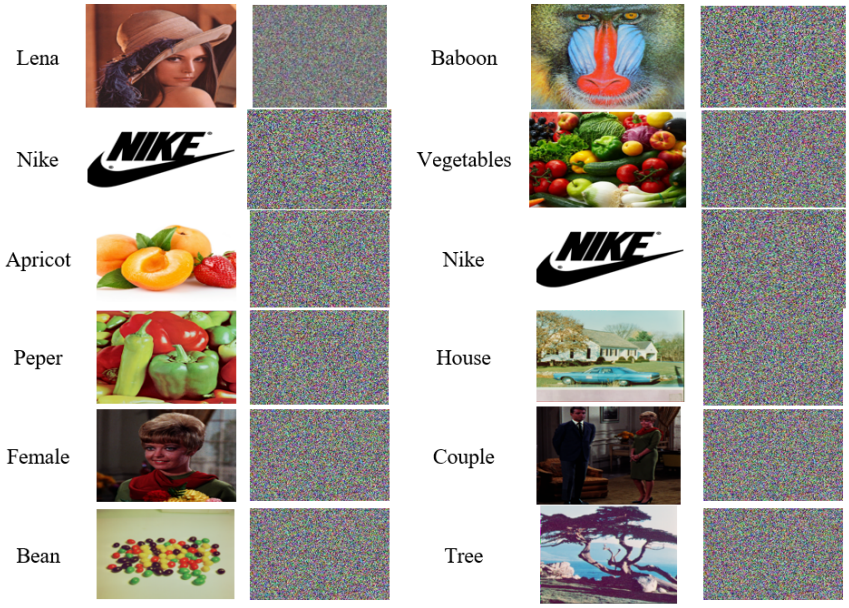

Figure 8. Visual aspect analysis

5.1.4 Analysis of histograms

Histograms depict the distribution of pixel values in images. Unauthorized individuals could extract crucial details about an encrypted image by analyzing its irregular histogram. Therefore, it is crucial to ensure that encrypted image histograms exhibit no numerical similarity with the original image, and maintain a consistent pixel distribution. Figures 9 - 13 showcase histograms of all test images, while Figure 14 displays histograms of images generated through encryption for each corresponding test image. Figure 9 specifically illustrates the histogram of the main test image "Lena." Figures 9 - 12 represent RGB channel histograms of clear images, whereas Subgraphs (a)-(j) of Figure 14 portray RGB channel histograms of encrypted images using the proposed method. Notably, the histograms of images produced during the encryption stage are characterized by a nearly uniform and flat distribution.

Likewise, by calculating the variances of histograms using Eq. (5), the consistency of encrypted images was examined. A reduced variance in an encrypted image signifies increased uniformity and a heightened level of protection for the suggested image encryption method [21, 22].

$$H_{Var}(X) = \frac{1}{n^2} \sum_{p=1}^{n} \sum_{c=1}^{n} \frac{1}{2} (x_p - x_c) \tag{5}$$

where, $X = x1, x2, \ldots, x256$ represents the histogram value vectors, and x_R and x_c denote pixels with p and c representing gray levels, respectively.

Table 4 presents the observed variations in the chosen test images. Examination of the data in the table reveals markedly elevated variances in the unencrypted images, in contrast to significantly lower variances in the encrypted versions. Specifically, the mean variance for the encrypted "Lena" image was 223.667, in comparison to 81232.023 for its plaintext counterpart. A comparative analysis further indicates that, for most of the tested images, the histogram variances in encrypted images generated using the proposed method consistently surpassed those obtained by several researchers [23–25]. This comparative evidence supports the claim that the proposed algorithm has an improved capability to enhance the security of the encryption process.

5.1.5 Analysis of entropy

The entropy of an image with dimensions (n, m) functions as a measure to evaluate the security of the image encryption algorithm. It signifies the degree of unpredictability and randomness inherent in the system, as expressed by the Eq. (6) provided.

$$S(MC) = \frac{-1}{3nm} \sum_{i=1}^{3nm} p(i) \cdot \log_2(p(i)) \tag{6}$$

where, $p(i)$ represents the probability of the occurrence of level i in the plain image.

Table 4. Comparison of histogram variance for encrypted images among references

Images		Lena	Female	Couple	House	Tree	Bean
Original images	Red	123072.500	620306.750	289630.656	992034.125	129825.531	129765.984
	Green	87100.835	860899.312	337863.062	1330180.12	57011.605	349251.718
	Blue	33522.734	790776.56	210359.812	768126.75	81373.710	537500.062
Encrypted images							
Ours	Red	218.99	262.241	275.069	1136.544	250.867	214.759
	Green	231.02	233.21	242.961	1109.793	214.998	258.798
	Blue	220.991	254.804	238.089	1059.993	257.959	237.997
Ref. [23]	Red	219.513	262.265	275.095	1136.569	250.877	214.782
	Green	231.052	233.211	243.858	1119.742	215.093	259.715
	Blue	221.119	255.813	238.196	1060.540	258.754	238.384
Ref. [24]	Red	247.78	280.64	284.35	1070.2	282.81	232.98
	Green	279.62	280.46	247.37	1231.2	254.87	279.61
	Blue	265.71	230.42	260.76	941.65	225.79	245.61
Ref. [25]	Red	264.27	252.67	274.74	1057.13	209.92	281.18
	Green	240.26	261.44	256.74	939.83	215.60	269.64
	Blue	251.12	267.49	234.56	1037.40	254.69	225.77

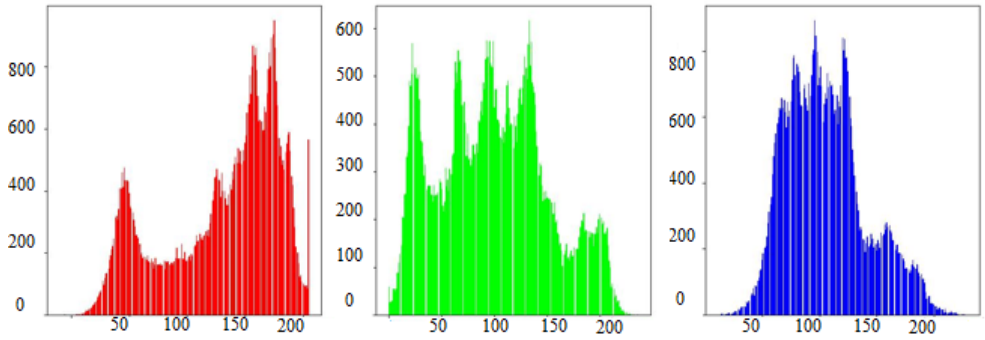

Figure 9. Histograms of the original images (RGB) for Lena

Table 5. Comparison of encrypted image entropy with other methods

Algorithm	Images	Encrypted		
		Red	Green	Blue
Ours	L	7.9973	7.9974	7.9971
	Pe	7.9994	7.9994	7.9995
	H	7.9983	7.9982	7.9983
	B	7.9994	7.9992	7.9994
	Pa	7.9975	7.9971	7.9974
	V	7.9994	7.9995	7.9993
Ref. [23]	L	7.9974	7.9974	7.9971
	Pe	7.9993	7.9994	7.9992
	H	7.9993	7.9992	7.9993
	B	7.9972	7.9971	7.9966
	Pa	7.9992	7.9994	7.9994
Ref. [25]	L	7.9972	7.9973	7.9970
	Pe	7.9993	7.9994	7.9994
	H	7.9993	7.9992	7.9993
	B	7.9974	7.9970	7.9974
	Pa	7.9993	7.9994	7.9993
Ref. [34]	L	7.987	7.987	7.986
Ref. [35]	L	7.973	7.975	7.971

Note: L, Pe, H, B, Pa and V represent Lena, Pepper, House, Baboon, Panda, and Vegetables, respectively.

Therefore, as the entropy approaches Eq. (8), the random arrangement of pixels in the image becomes more refined. Increased entropy contributes to minimizing information leakage from the encrypted image.

Table 5 displays entropy values for the examined images, compared to those of various existing encryption methods. The results indicate that the entropy values are consistently equal to or greater than 7.996, similar to the

study of Khan et al. [25], and outperforming values reported by several researchers [23, 33–35].

Table 6. Correlations between pixels in images taken from the SIP database

Images		Original Image			Encrypted Image		
		Horizontal	Vertical	Diagonal	Horizontal	Vertical	Diagonal
Lena	Red	0.9558	0.9648	0.9325	-0.003771	0.008149	-0.00132
	Green	0.93556	0.95756	0.91902	-0.002981	0.009127	-0.006732
	Blue	0.90773	0.9393	0.8913	-0.001449	-0.006716	0.000643
Apricot	Red	0.98385	0.96944	0.98629	-0.00136621	-0.0018756	-0.0054082
	Green	0.97883	0.98511	0.96537	-0.00106622	0.0015054	0.0023428
	Blue	0.99153	0.98348	0.98724	0.0048931	-0.0057105	-0.0011768
Panda	Red	0.95175	0.96552	0.93161	0.0051302	-0.0007677	-0.0049534
	Green	0.95215	0.96436	0.93066	0.0078786	-0.0007949	0.0002736
	Blue	0.95542	0.97086	0.94265	0.000070	0.0109689	-0.0010586
Nike	Red	0.98681	0.99219	0.97287	-0.0043816	-0.0165139	0.0066847
	Green	0.98851	0.99103	0.97352	0.0023923	0.0017955	-0.0034511
	Blue	0.98675	0.99049	0.97189	0.0087519	0.0057946	-0.0030269
Vegetables	Red	0.97886	0.98012	0.96108	0.0012429	-0.0032612	0.0007536
	Green	0.97749	0.97952	0.95947	-0.0007566	-0.0024509	0.0044757
	Blue	0.97224	0.97091	0.94729	-0.0010254	-0.0049974	0.0015236

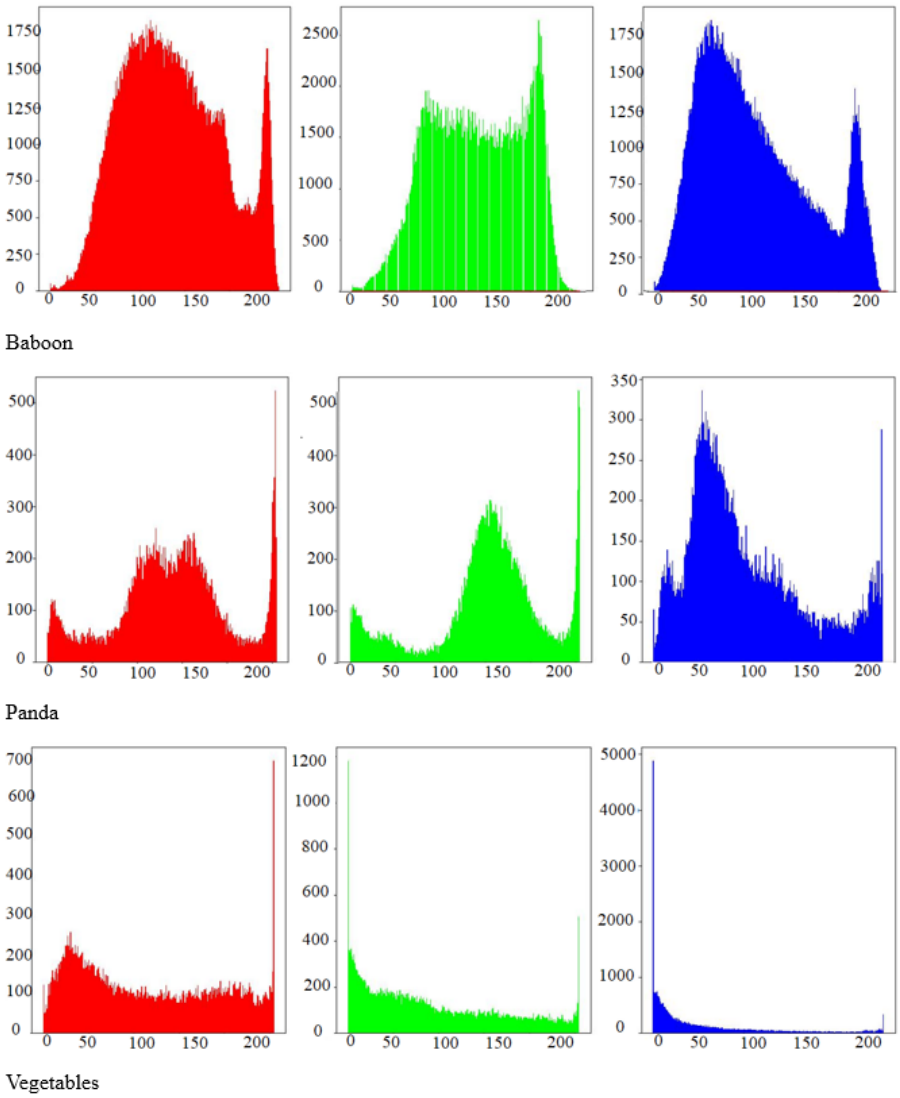

Figure 10. Histograms of the original images (RGB) for Baboon; Panda; Vegetables

5.1.6 Correlation analysis

Eq. (7) provides the correlation of an image with dimensions (n, m).

$$\text{corr} = \frac{\text{cov}(x, y)}{\sqrt{\text{var}(x)} \cdot \sqrt{\text{var}(y)}} \tag{7}$$

Table 6 displays the pixel correlation values of images obtained from the SIPI database and additional test images. Examination of the table data indicates a remarkably high correlation in the original image, approaching a value of 1 for each channel. In contrast, images encrypted with the proposed algorithm exhibit a significantly lower correlation. This observation supports the robust security achieved by the algorithm. Moreover, these results highlight a considerable decrease in correlation within the encrypted image, indicating that attackers cannot extract information from the encrypted image using this method.

Table 7. Correlation between ciphered "Lena" pixels

Method	Horizontal	Vertical	Diagonal
Proposed method	-0.002733667	0.00352	-0.002469667
Ref. [23]	-0.0042707	-0.0032498	-0.0020192
Ref. [25]	-0.0029883	0.0091357	-0.0067375
Ref. [26]	-0.0098	-0.0050	-0.0013

Table 7 displays the pixel correlations detected within the 'Lena' image. A juxtaposition with previous techniques reveals that the mutual correlation of adjacent pixels in the encrypted image is lower than that in several studies [25, 26], although it is similar to that in the study of Butt et al. [23]. The correlation metrics for all tested image correlations by the proposed encryption system are nearly zero, providing protection against statistical attacks.

Table 8. Comparison of the NPCR and UACI

Method	Lena		Pepper	
	NPCR	UACI	NPCR	UACI
Proposed method	99.68 %	33.49	99.67	33.48
Ref. [23]	99.68 %	33.46	99.67	33.48
Ref. [25]	99.60 %	33.49	99.61	33.46
Ref. [29]	99.66 %	33.44	99.63	33.47
Ref. [30]	99.60 %	33.44	-	-
Ref. [31]	99.62 %	33.65	-	-
Ref. [32]	99.6092 %	33.4685	-	-

Table 9. The PSNR (dB) between the original image, the encrypted image, and the decrypted image

Method	Type of PSNR	Lena	Baboon	Panda	Vegetables
Proposed method	Original to Encrypted	∞	∞	∞	∞
	Original to Encrypted	7.0312	7.1811	7.1748	6.8800
Ref. [23]	Original to Decrypted	∞	∞	∞	∞
	Original to Encrypted	8.1102	8.7776	8.1648	6.8760
Ref. [36]	Original to Encrypted	8.3655	8.8532	-	-
Ref. [37]	Original to Encrypted	8.2522	8.8223	-	-
Ref. [38]	Original to Decrypted	∞	∞	-	-
	Original to Encrypted	7.0257	7.1515	-	-

5.2 Differential Attacks

To evaluate the effectiveness of the algorithm against differential attacks, metrics like the number of pixel change rate (NPCR), the unified average change intensity (UACI), and the avalanche effect are utilized.

5.2.1 NPCR and UACI analysis

These metrics can be given by Eqs. (8) and (9) below.

$$NPCR = \left(\frac{1}{3nm} \sum_{i,j=1}^{nm} Df(i,j) \right) \cdot 100 \tag{8}$$

$$UACI = \left(\frac{1}{3nm} \sum_{i,j=1}^{3nm} \frac{|Im_1(i,j) - Im_2(i,j)|}{255} \right) \cdot 100 \tag{9}$$

where, $Df(i,j) = \begin{cases} 1 & \text{if} \quad Im_1(i,j) \neq Im_2(i,j) \\ 0 & \text{if} \quad Im_1(i,j) = Im_2(i,j) \end{cases}$, $Im_1(i,j)$ is the first image pixel of rank (i,j) and $Im_2(i,j)$ is the second image pixel of rank (i,j).

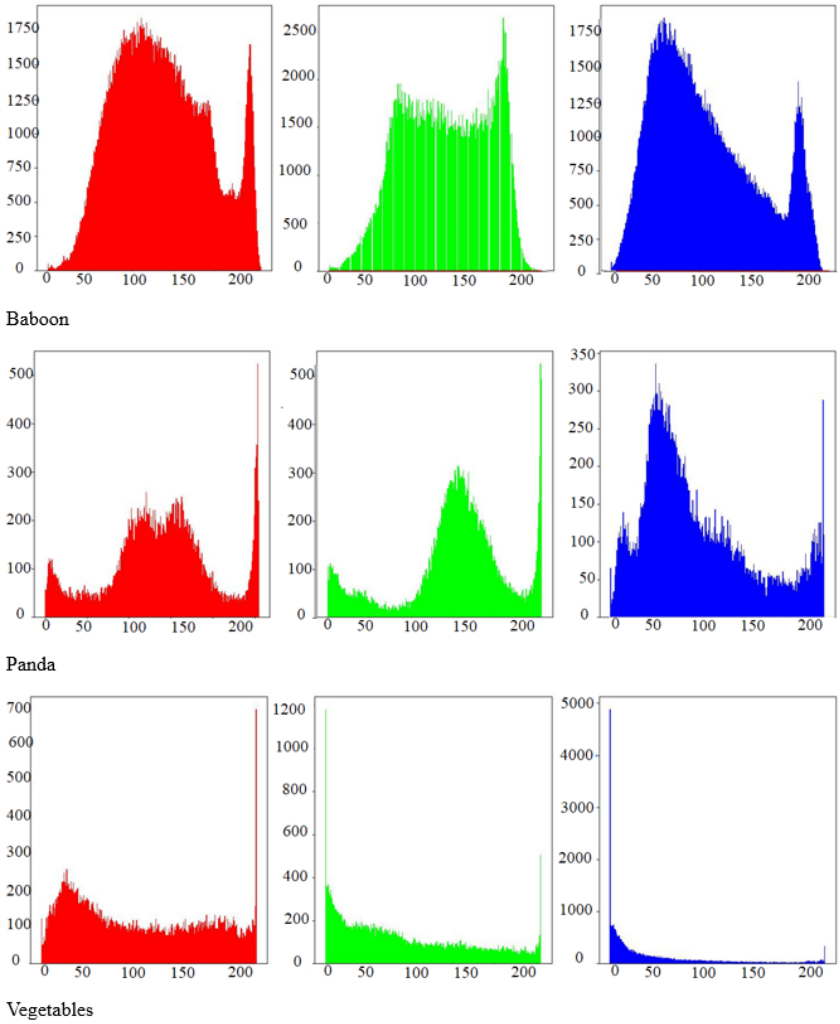

Figure 11. Histograms of the original images (RGB) for Apricot; Nike; Pepper

The information in Table 8 reveals UACI and NPCR values for two images, "Lena" and "Pepper". It illustrates that the UACI is equal to or exceeds 33.4, and the NPCR is equal to or exceeds 99.6. These results unequivocally demonstrate that the NPCR performance of the suggested encryption algorithm is on par with that of the algorithm proposed by Butt et al. [23] and surpasses that of several other algorithms [25, 29–32]. Meanwhile, the UACI value aligns closely with that of several algorithms [23, 25, 29–32]. This indicates that the proposed approach showcases robust encryption performance, particularly in thwarting differential attacks.

5.2.2 Analysis of the peak signal-to-noise ratio (PSNR) metric

In the field of image processing, the mean squared error (MSE) and PSNR are widely used to assess the effectiveness of encryption. These metrics serve as common criteria for evaluating the quality of two images in a cryptographic system. The PSNR gauges the similarity between images and complements the MSE. Eq. (10) can be applied to calculate the MSE for the original, decrypted, and encrypted images.

$$MSE = \frac{1}{(3nm)^2} \sum_{i,j=1}^{3nm} |Im_1(i,j) - Im_2(i,j)|^2 \tag{10}$$

where, Im_1 and Im_2 represent the original and encrypted images, respectively. The symbol n indicates the number of rows in the original image, while m signifies the number of columns in the image. The evaluation of $PSNR$ is conducted in decibels and exhibits an inverse relationship with the mean squared error, as determined by Eq. (11).

$$PSNR = 10 * \log_{10}\left(\frac{\left(2^L - 1\right)^2}{MSE}\right)(dB) \tag{11}$$

where, L=8 denotes the bit depth of the particular image.

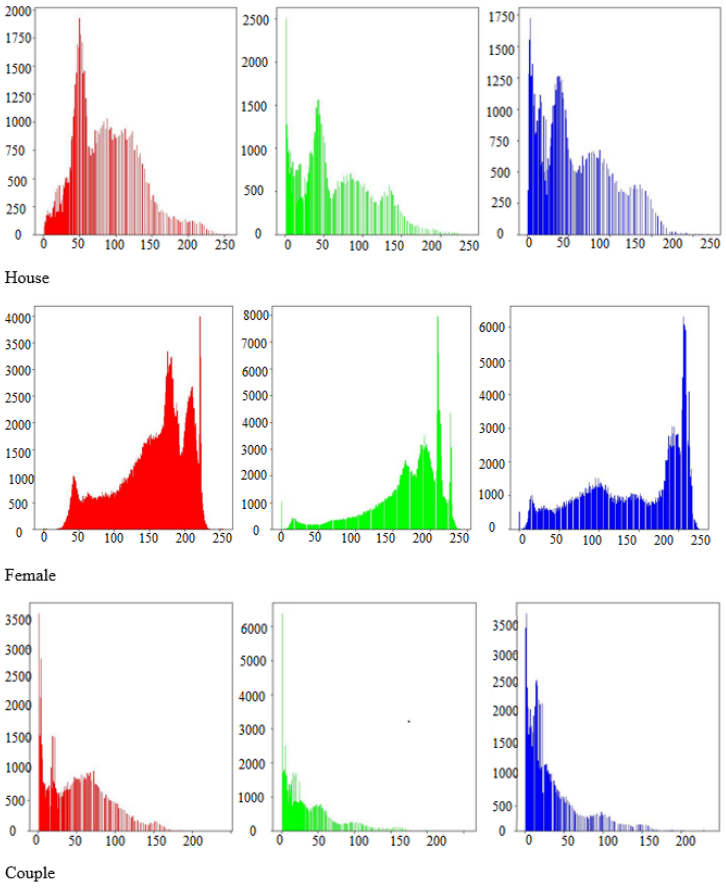

Figure 12. Histograms of the original images (RGB) for House; Female; Couple

A higher PSNR indicates a smaller difference between the original and decrypted images. When the original and encrypted images are identical, the PSNR becomes infinite. The table below presents a comparison of PSNR values between the proposed approach and other references.

The lower PSNR values observed in Table 9 for the original-to-encrypted images suggest that the proposed algorithm offers superior encryption compared to the methods in several studies [23, 36, 37]. The metric's value is comparable to that in the study of Aung et al. [38], indicating that the proposed method can recover images without substantial information loss.

6 Advantages and Limitations of the Proposed Method

6.1 Advantages

The method has several benefits, namely:

• Difficulty to recover encryption keys due to the extreme sensitivity of the used chaotic maps to the initial conditions.

• Robustness of the method due to non-commutative algebraic operations.

• The system can be applied to any image of arbitrary format and size.

• Use of pseudo-random and bijective affine functions.

• High attack complexity of the method due to the replacement S-box design under a chaotic decision control vector.

• Difficulty of S-box reconstruction due to their pseudorandom vector-based construction.

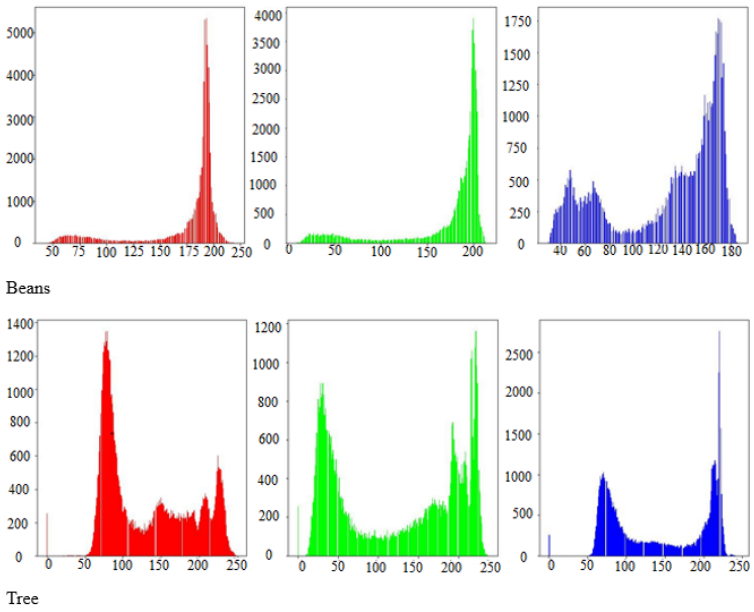

Figure 13. Histograms of the original images (RGB) for Beans; Tree

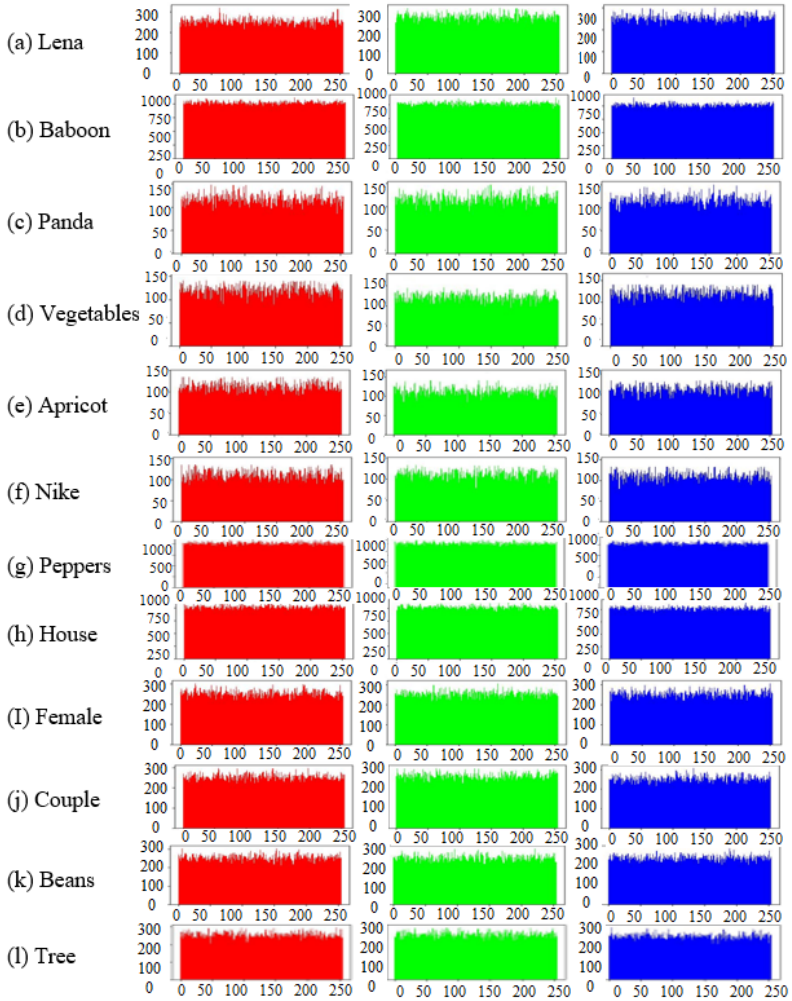

Figure 14. Histograms of the cipher images (RGB)

6.2 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.

7 Conclusions

A hybrid circuit combining the affine and Vigenere techniques was applied, employing two novel substitution tables and a robust diffusion and confusion function, followed by a global permutation tailored for image encryption. Additionally, the incorporation of highly sensitive chaotic maps into the initial conditions allowed us to suggest an improved method for ciphering color images. Simulations conducted on a randomly selected sample of images from the SIPI database, featuring various formats and sizes, demonstrated the algorithm's ability to withstand any known attacks.

As a perspective, some algorithms will be integrated with 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] A. M. Alnajim, E. Abou-Bakr, S. S. Alruwisan, S. Khan, and R. A. Elmanfaloty, "Hybrid chaotic-based PRNG for secure cryptography applications," *Appl. Sci.*, vol. 13, no. 13, p. 7768, 2023. https://doi.org/10.3390/app13137768

[2] E. H. Rachmawanto and R. Zulfiningrum, "Medical image cryptosystem using dynamic josephus sequence and chaotic-hash scrambling," *J. King Saud Univ.-Comput. Inf. Sci.*, vol. 34, no. 9, pp. 6818–6828, 2022. https://doi.org/10.1016/j.jksuci.2022.04.002

[3] D. F. Santos and H. E. Espitia, "Secure medical image transmission scheme using lorenz's attractor applied in computer-aided diagnosis for the detection of eye melanoma," *Computation*, vol. 10, no. 9, p. 158, 2022. https://doi.org/10.3390/computation10090158

[4] P. N. Andono, "Improved pixel and bit confusion-diffusion based on mixed chaos and hash operation for image encryption," *IEEE Access*, vol. 10, pp. 115 143–115 156, 2022. https://doi.org/10.1109/ACCESS.2022.3218886

[5] E. Winarno, K. Nugroho, and P. W. Adi, "Combined interleaved pattern to improve confusion-diffusion image encryption based on hyperchaotic system," *IEEE Access*, vol. 11, pp. 69 005–69 021, 2023. https://doi.org/10.1109/ACCESS.2023.3285481

[6] M. Kaur, D. Singh, K. Sun, and U. Rawat, "Color image encryption using nondominated sorting genetic algorithm with local chaotic search based 5D chaotic map," *Future Gener. Comput. Syst.*, vol. 107, pp. 333–350, 2020. https://doi.org/10.1016/j.future.2020.02.029

[7] W. Alexan, Y. L. Chen, L. Y. Por, and M. Gabr, "Hyperchaotic maps and the single neuron model: A novel framework for chaos-based image encryption," *Symmetry*, vol. 15, no. 5, p. 1081, 2023. https://doi.org/10.3390/sym15051081

[8] W. J. Jun and T. S. Fun, "A new image encryption algorithm based on single S-box and dynamic encryption step," *IEEE Access*, vol. 9, pp. 120 596–120 612, 2021. https://doi.org/10.1109/ACCESS.2021.3108789

[9] M. Ramzan, T. Shah, M. M. Hazzazi, A. Aljaedi, and A. R. Alharbi, "Construction of S-boxes using different maps over elliptic curves for image encryption," *IEEE Access*, vol. 9, pp. 157 106–157 123, 2021. https://doi.org/10.1109/ACCESS.2021.3128177

[10] J. Zhao, S. Wang, and L. Zhang, "Block image encryption algorithm based on novel chaos and DNA encoding," *Information*, vol. 14, no. 3, p. 150, 2023. https://doi.org/10.3390/info14030150

[11] M. Abu-Faraj, A. Al-Hyari, C. Obimbo, K. Aldebei, I. Altaharwa, Z. Alqadi, and O. Almanaseer, "Protecting digital images using keys enhanced by 2D chaotic logistic maps," *Cryptography*, vol. 2023, no. 2, p. 20, 2023. https://doi.org/10.3390/cryptography7020020

[12] S. Vaidyanathan, A. S. Tewa Kammogne, E. Tlelo-Cuautle, C. N. Talonang, B. Abd-El-Atty, A. A. Abd El-Latif, E. M. Kengne, V. F. Mawamba, A. Sambas, P. Darwin, and B. Ovilla-Martinez, "A novel 3-D jerk system, its bifurcation analysis, electronic circuit design and a cryptographic application," *Electronics*, vol. 12, no. 13, p. 2818, 2023. https://doi.org/10.3390/electronics12132818

[13] Y. L. Ma, C. Q. Li, and B. Ou, "Cryptanalysis of an image block encryption algorithm based on chaotic maps," *J. Inf. Secur. Appl.*, vol. 54, p. 102566, 2020. https://doi.org/10.1016/j.jisa.2020.102566

[14] E. Moya-Albor, A. Romero-Arellano, J. Brieva, and S. L. Gomez-Coronel, "Color image encryption algorithm based on a chaotic model using the modular discrete derivative and langton's ant," *Mathematics*, vol. 11, no. 10, p. 2396, 2023. https://doi.org/10.3390/math11102396

[15] A. Hasheminejad and M. J. Rostami, "A novel bit level multiphase algorithm for image encryption based on PWLCM chaotic map," *Optik*, vol. 184, pp. 205–213, 2019. https://doi.org/10.1016/j.ijleo.2019.03.065

[16] Y. Chen, S. C. Xie, and J. Z. Zhang, "A hybrid domain image encryption algorithm based on improved henon map," *Entropy*, vol. 24, no. 2, p. 287, 2022. https://doi.org/10.3390/e24020287

[17] R. Qumsieh, M. Farajallah, and R. Hamamreh, "Joint block and stream cipher based on a modified skew tent map," *Multimed. Tools Appl.*, vol. 78, pp. 33 527–33 547, 2019. https://doi.org/10.1007/s11042-019-08112-z

[18] Y. Q. Luo, J. Yu, W. R. Lai, and L. F. Liu, "A novel chaotic image encryption algorithm based on improved baker mapand logistic map," *Multimed. Tools Appl.*, vol. 78, pp. 22 023–22 043, 2019. https://doi.org/10.1007/s11042-019-7453-3

[19] S. Sabir and V. Guleria, "Multilayer permutation-substitution operations based novel lossless multiple color image encryption," *Multimed. Tools Appl.*, vol. 83, p. 16563–16604, 2023. https://doi.org/10.1007/s11042-023-15992-9

[20] X. Q. Zhang and J. X. Tian, "Multiple-image encryption algorithm based on genetic central dogma," *Phys. Scripta*, vol. 97, no. 5, p. 055213, 2022. https://doi.org/10.1088/1402-4896/ac66a1

[21] P. Ramasamy, V. Ranganathan, S. Kadry, R. Damaševičius, and T. Blažauskas, "An image encryption scheme based on block scrambling, modified zigzag transformation and key generation using enhanced logistic—Tent map," *Entropy*, vol. 21, no. 7, p. 656, 2019. https://doi.org/10.3390/e21070656

[22] X. J. Wu, J. Kurths, and H. Kan, "A robust and lossless DNA encryption scheme for color images," *Multimed. Tools Appl.*, vol. 77, pp. 12 349–12 376, 2018. https://doi.org/10.1007/s11042-017-4885-5

[23] K. K. Butt, G. H. Li, S. Khan, and S. Manzoor, "Fast and efficient image encryption algorithm based on modular addition and SPD," *Entropy*, vol. 22, no. 1, p. 112, 2020. https://doi.org/10.3390/e22010112

[24] C. Q. Li, "Cracking a hierarchical chaotic image encryption algorithm based on permutation," *Signal Process.*, vol. 118, pp. 203–210, 2016. https://doi.org/10.1016/j.sigpro.2015.07.008

[25] S. Khan, L. S. Han, Y. K. Qian, H. W. Lu, and M. J. Shi, "Security of multimedia communication with game trick based fast, efficient, and robust color-/gray-scale image encryption algorithm," *Trans. Emerg. Telecommun. Technol.*, vol. 32, no. 2, p. e4034, 2021. https://doi.org/10.1002/ett.4034

[26] X. P. Zhang, W. G. Nie, Y. L. Ma, and Q. Q. Tian, "Cryptanalysis and improvement of an image encryption algorithm based on hyperchaotic system and dynamic s-box," *Multimed. Tools Appl.*, vol. 76, pp. 15 641–15 659, 2017. https://doi.org/10.1007/s11042-016-3861-9

[27] X. Y. Wang and H. L. Zhang, "A color image encryption with heterogeneous bit-permutation and correlated chaos," *Opt. Commun.*, vol. 342, pp. 51–60, 2015. https://doi.org/10.1016/j.optcom.2014.12.043

[28] L. Xu, Z. Li, J. J. Li, and W. Hua, "A novel bit-level image encryption algorithm based on chaotic maps," *Opt. Lasers Eng.*, vol. 78, pp. 17–25, 2016. https://doi.org/10.1016/j.optlaseng.2015.09.007

[29] A. Y. Niyat, M. H. Moattar, and M. N. Torshiz, "Color image encryption based on hybrid hyperchaotic system and cellular automata," *Opt. Lasers Eng.*, vol. 90, pp. 225–237, 2017. https://doi.org/10.1016/j.optlaseng.2016.10.019

[30] J. X. Chen, Z. L. Zhu, L. M. Zhang, Y. S. Zhang, and B. Q. Yang, "Exploiting self-adaptive permutation–diffusion and DNA random encoding for secure and efficient image encryption," *Signal Process.*, vol. 142, pp. 340–353, 2018. https://doi.org/10.1016/j.sigpro.2017.07.034

[31] G. D. Ye and X. L. Huang, "An efficient symmetric image encryption algorithm based on an intertwining logistic map," *Neurocomputing*, vol. 251, pp. 45–53, 2017. https://doi.org/10.1016/j.neucom.2017.04.016

[32] C. Chen, D. L. Zhu, X. Wang, and L. J. Zeng, "One-dimensional quadratic chaotic system and splicing model for image encryption," *Electronics*, vol. 12, no. 6, p. 1325, 2023. https://doi.org/10.3390/electronics12061325

[33] Y. M. M. Wang, X. L. Leng, C. K. Zhang, and B. X. Du, "Adaptive fast image encryption algorithm based on three-dimensional chaotic system," *Entropy*, vol. 25, no. 10, p. 1399, 2023. https://doi.org/10.3390/e25101399

[34] A. Kadir, A. Hamdulla, and W. Q. Guo, "Color image encryption using skew tent map and hyper chaotic system of 6th-order CNN," *Optik*, vol. 125, no. 5, pp. 1671–1675, 2014. https://doi.org/10.1016/j.ijleo.2013.09.040

[35] X. J. Wu, K. S. Wang, X. Y. Wang, H. B. Kan, and J. Kurths, "Color image DNA encryption using NCA map-based CML and one-time keys," *Signal Process.*, vol. 148, pp. 272–287, 2018. https://doi.org/10.1016/j.sigpro.2018.02.028

[36] X. B. Liu, D. Xiao, and Y. P. Xiang, "Quantum image encryption using intra and inter bit permutation based on logistic map," *IEEE Access*, vol. 7, pp. 6937–6946, 2018. https://doi.org/10.1109/ACCESS.2018.2889896

[37] E. Winarno, K. Nugroho, P. W. Adi, and D. R. I. M. Setiadi, "Combined interleaved pattern to improve confusion-diffusion image encryption based on hyperchaotic system," *IEEE Access*, vol. 11, pp. 69 005–69 021, 2023. https://doi.org/10.1109/ACCESS.2023.3285481

[38] T. M. Aung, H. H. Naing, and N. N. Hla, "A complex transformation of monoalphabetic cipher to polyalphabetic cipher: (Vigenère-Affine cipher)," *Int. J. Mach. Learn. Comput.*, vol. 9, no. 3, pp. 296–303, 2019. http://dx.doi.org/10.18178/ijmlc.2019.9.3.801

[39] T. S. Ali and R. Ali, "A novel color image encryption scheme based on a new dynamic compound chaotic map and S-box," *Multimed. Tools Appl.*, vol. 81, no. 15, pp. 20 585–20 609, 2022. https://doi.org/10.1007/s11042-022-12268-6