International Journal of Advanced Science and Computer Applications (2025); 4(1):
DOI: 10.47679/ijasca.v4i1.57
https://ijasca.org/index.php/ijasca

RESEARCH ARTICLE

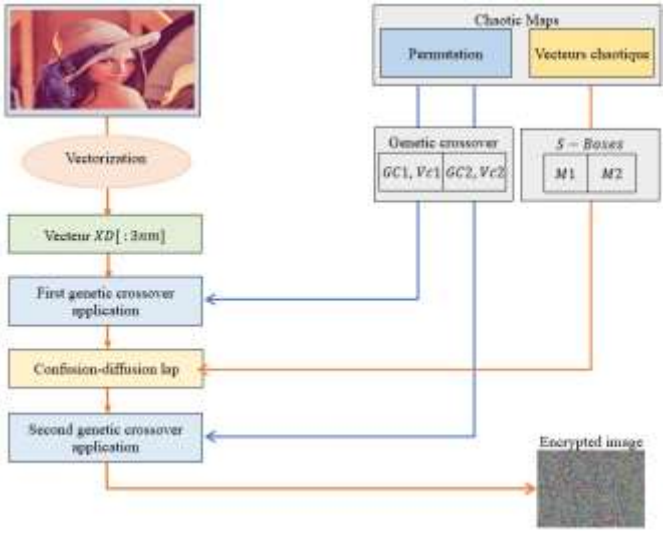
Enhanced Vigenere And Affine Ciphers Surrounded By Dual Genetic Crossover Mechanisms For Encrypting Color Images

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

Published online: 14 March 2025

Abstract

This paper introduces an enhanced technique for encrypting color images, surpassing the effectiveness of genetic crossover and substitution methods. The approach integrates dynamic random functions to bolster the integrity of the resulting vector, elevating temporal complexity to deter potential attacks. The enhancement entails amalgamating genetic crossover using two extensive pseudorandom replacement tables derived from established chaotic maps in cryptography. Following the controlled vectorization of the original image, our method commences with an initial genetic crossover inspired by DNA behavior at the pixel level. This process is followed by a confusion-diffusion lap, strengthening the relationship between encrypted pixels and their neighboring counterparts. The confusion-diffusion mechanism employs dynamic pseudorandom affine functions at the pixel level. Subsequently, a second genetic crossover operator is applied. Simulations conducted on various images with varying sizes and formats demonstrate the resilience of our approach against statistical and differential attacks. **Graphical abstract**



Keyword: Genetic crossover; pseudorandom functions; S-Box; chaotic map

Introduction

The exploration of securing information during network transmission has gained significant attention in research. Encryption technology, specifically symmetric and asymmetric encryption algorithms in cryptography [1], plays a pivotal role in this context. Symmetric encryption is known for its efficiency, strong security, and quick encryption speed using a large key, where the security heavily relies on safeguarding the encryption key. This method involves minimal computation, ensuring high protection and fast encryption with a lengthy key. The security of data transmission hinges on protecting the encryption key. Conversely, asymmetric encryption, offering high security, entails longer encryption and decryption times, making it suitable for limited data encryption like passwords. Here, the security of data transmission depends on both the key and the algorithm. According to the principle of Kirchhoff, the protection of the key system is closely linked to the ciphering key rather than the algorithm. To tackle these

MATSI Laboratory, Mohammed First University, Oujda, Morocco

*) corresponding author

Email: abdoujjar@gmail.com

Received 21 November 2024 | Received in revised form 17 Januari 2025 | Accepted 06 February 2025
Available online 14 March 2025

challenges, various image encryption methods leverage symmetry theory principles, and this paper adopts a similar approach centered on such algorithms.

Despite the diligent efforts of researchers to enhance ciphering methods' security, numerous image encryption techniques have been compromised successfully [2, 3]. In the quest for increased security, many scholars have turned to multi-round encryption approaches [4, 5], albeit at the cost of significant time investment. Some authors have advocated for encryption methods tailored specifically to an image's relevant characteristics [6, 7]. Zhou et al. introduced a ciphering architecture for medical images employing an optimized game theory method [6], showcasing flexibility and reliability in safeguarding medical images from attacks. Çelik et al. proposed an encryption image architecture utilizing data hiding and logistic maps [8], demonstrating satisfactory security performance in experiments. Inspired by these studies, we suggest leveraging existing technology to identify the facial contour area when encrypting human images, allowing for individual encryption of these regions. Following the encryption of the facial part, the entire image undergoes an additional layer of encryption. This approach, compared to traditional single-round encryption, exhibits superior encryption effectiveness. Even in the face of algorithmic attacks, private aspects such as the face remain indistinguishable and irretrievable. In contrast to multi-round encryption schemes, these techniques offer shorter processing times and higher speeds for data encryption and decryption.

As chaos theory continues to evolve, researchers have systematically explored the attributes of pseudorandomness, and sensitivity to initial values [9, 10]. Additionally, various chaotic image encryption algorithms have emerged, integrating principles from diverse disciplines such as genetic algorithms rules such as quantum maps [11] and perceptron-like networks [12]. In [13], Chatterjee et al designed an encryption architecture that involves replacement-diffusion operation using standard and logistic maps, addressing the issue of dynamic degradation. Li et al. [14] demonstrate that the use of chaotic sequences as keys can compromise the algorithm's security. Efficiently, chaotic methods have various variations, with some, such as the PWLCM, logistic, Henon, and skew tent maps [15, 16, 17, and 18], being renowned for image encryption. Focusing on the logistic and PWLCM maps, they offer several advantages, including enhanced sensitivity and randomness, resulting in more secure, chaotic, and unique sequences.

Most existing research relies on independent block encryption, making it vulnerable to statistical attacks. Additionally, the small size of the private key exposes it to brute-force attacks. With the weakness of diffusion and chaining functions between the encrypted and plaintext blocks, this technique remains susceptible to differential attacks.

Our objective is to develop a novel image encryption crypto-system that reintroduces diffusion and confusion, placing our new technique beyond the reach of known differential attacks.

Our contribution to addressing the identified anomalies in previous research is the development of a new image encryption crypto-system using two large substitution matrices of sizes (256,256) incorporating pseudo-random affine functions for diffusion restoration to counteract statistical and differential attacks. This process is surrounded by two genetic crossover operations. Additionally, our method is simple and robust because each pixel is encrypted with a specified random affine function after and before genetic crossover operations. Furthermore, the size of the private key in our crypto-system exceeds 100 bits by a significant margin, which is sufficient to counteract any brute-force attack. The algorithm exhibits robust security, proven through simulation, security assessments, and result comparisons with other algorithms. It demonstrates a high level of robustness and makes our new technique impervious to differential and statistical attacks.

This research paper is divided into various sections, including a section on previous related work that details assumptions and related research; a section describing the theoretical framework, explaining the basis of chaotic sequences, and the genetic mutation, as well as classical Vigenere and affine techniques; a section detailing the proposed approach, revealing the nuances of the encryption and decryption process; a section devoted to results and discussions, presenting research findings, discussions, and comparisons with other similar techniques; and a section summarizing the findings and proposing research directions.

Previous related works

The preceding sections delved into the potential significance of confusion-diffusion features within image ciphering, particularly across substitution and permutation procedures. Another critical perspective to underscore pertains to the quality of the encryption key. Previous research on methods exploiting permutation and substitution patterns and enhancing key qualities has been a motivating factor for this study. Initially, substitution and permutation encryption methods were confined to pixel-level applications. Recent studies, such as [19], emphasize the growing popularity of pixel-level substitutions and permutations as image processing techniques. In reference [20], the authors introduced a multiple-image encryption approach using 3D bit planes and a genetic central dogma for permutation between bit planes. Similarly, reference [21] proposed an enhanced logistic map incorporating diffusion, key stream generation, and permutation to enhance resistance against assaults. Study [22] presented a method based on the permutation operation of DNA genomic sequences, coupling one-way mapping networks with an XOR operation. Study [23] introduced a novel image encryption method utilizing binary bit plane scrambling and the SPD bit plane diffusion technique for an ordinary image, incorporating elements of the card game technique. Reference [24] examined the resilience of HCIE when faced with known-plaintext-only and known-plaintext/chosen-plaintext attacks. Article [25] suggested a DNA-based method capable of simultaneously performing bit plane searching and pixel diffusion in a single step. Reference [26] proposed an improved algorithm aimed at addressing potential security issues in Liu's algorithm. However, article [27] presented a unique approach to color image encryption, combining heterogeneous bit permutation and correlated chaos techniques. A new bit-level image encryption method, outlined in [28], utilized PWLCM map, introducing a new diffusion procedure to mutually diffuse two sequences. Reference [29] proposed an image encryption method based on a self-organized structure with units updated according to rules dependent on the number of limited neighboring units. Article [30] provided a solution for secure and efficient image encryption using adaptive permutation-diffusion and random DNA coding. However, [31] proposed an efficient symmetric image ciphering technique to address the low sensitivity issue of the plain image. Recently, Chen et al. [32] developed an enhanced digital image encryption method using a collage model and a one-dimensional quadratic chaotic system, expanding the key space for robust resilience against exhaustive attacks. Wang Yiming et al. [33] proposed an improved 3D chaotic system characterized by various dynamic behaviors. In [34], a color image encryption method based on a

hypercomplex chaotic system and skew tent map was introduced. Wu et al. [35] proposed a new color image encryption method based on DNA, one-time keys, spatiotemporal chaos, and sequence operations. In [36], the authors proposed a quantum image encryption scheme based on permutation using an improved quantum representation model, achieving consecutive intraputation through sorting an interpermutation and chaotic sequence operations involving the qubit XOR process between chosen bit planes. However, [37] suggested a combination of intertwined patterns, including zigzag, Hilbert, and Morton patterns, to aggregate confusion-diffusion and enhance complexity and randomness. Consequently, in [38], the authors put forth a poly-alphabetic cipher as a novel system for encrypting and decrypting data.

The mentioned systems generally use small-size substitution tables, namely 16x16, 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.

Theoretical background

In this section, we present used chaotic maps, the genetic crossover, the classical Vigenere, and affine ciphering techniques employed in this study.

Chaotic maps

The chaotic maps in question are used to create two chaotic sequences, (h) and (l), each of size $(1;\ 3\ nm)$ used to construct different subkeys for encryption and decryption processes.

PWLCM map

The first chaotic sequence will be generated by the PLWCM map [18]. It is a sequence of real numbers defined by equation (1).

$$h_{n+1} = f(h_n) = \begin{cases} h_0 \in\ ]0\,;1[\ ,\ \ k \in\ ]0{,}5;4[& \\ k^{-1}\ h_n & if\ \ 0 < h_n\ < k \\ (0{,}5-k)^{-1}(h_n - k) & \mathrm{k} < h_n\ < 0{,}5 \\ f(1-h_n) & \text{otherwise} \end{cases} \qquad (1)$$

The parameters (h_0) and (k) represent the initial state and its control parameter, respectively.

Logistic map

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

$$l_{n+1} = \delta.\, l_n(1 - l_n) \ \text{ Where } \ l_0 \in]0{,}5;1[\ and\ \delta \in [3{,}75;4] \qquad \mathbf{(2)}$$

Genetic crossover

Genetic crossover is a confusion between the heritage gene and another pseudo-random gene generated from the chaotic maps used in our cryptosystem.

Classical Vigenere method

The classical Vigenere cipher system is based on a matrix (M) 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 // first line
   M(1, i) = i
end for
for i = 1 to 26 // other lines
   for i = 1 to 26
      M(i, j) = M(i − 1, mod(j + 1,26))
   end for
end for
```

Let (Pk) be the plain message, (Ck) be the cipher message, (Ke) be the encryption key, (M) 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

//Encryption	//Decryption
$for\ i = 1\ to\ n$	$for\ i = 1\ to\ n$
$Ck_i = M(Ck_i, Ke_i) = Pk_i + Ke_i\ \ mod\ 26$	$Pk_i = M^{-1}(Pk_i, Ke_i) = Ck_i - Ke_i\ \ mod\ 26$
$end\ for$	$end\ for$

Affine functions in $(\mathbf{Z}/n\mathbf{Z})$

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

$$\begin{cases} f: Z/nZ \ \rightarrow \ \ Z/nZ \\ \quad x \ \longmapsto \ \ mod(ax + b; n) \end{cases} \qquad a, b \in\ Z/nZ \qquad (3)$$

The function (f) is a bijective function in (Z/nZ) if and only if (a) is invertible and (b) is any.
Indeed, we have $y = mod(ax + b; n)$
Then, $ax = mod(y - b; n)$ and $x = mod(a^{-1}.(y - b); n)$
Where (a^{-1}) is the inverse of (a) in ring (Z/nZ).
Or, we know that (a) is invertible in (Z/nZ) if and only if aΛn = 1.
Particular case:
$n = 2^k, k \in N$Particular case, (a) is invertible in ring $(Z/2^kZ)$ if and only if (a) is odd.
Example in a ring (Z/8Z):

Table 1. Affine function example in a ring $(Z/8Z)$

x	0	1	2	3	4	5	6	7
$f(x) = mod(7x + 6; 8)$	6	5	4	3	2	1	0	7

(f) is an invertible function of the ring $(Z/8Z)$.

Our approach

This new technique uses the two most widely deployed chaotic maps in the field of cryptography [18, 19] by integrating large S-boxes incorporating strong pseudorandom affine functions for the confusion-diffusion process. The confusion-diffusion process is encapsulated by two genetic crossover. This technique is structured around the subsections described below.

Pseudorandom vectors generation

(1). Used chaotic sequences

Two chaotic sequences (h) and (l) were generated based on PWLCM and Skew tent chaotic maps described in section (3.1). These sequences, used in our approach, are extremely sensitive to the initial conditions and easy to implement in any cryptosystem.

(2). Sub keys 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 vectors generation

$for\ i\ =\ 1\ to\ 3nm$
// Confusion vectors
Vc1(i)= [E(max(h(i);l(i)),10^{11}) mod 253]+2
$Vc2(i) = [E(((h(i) + 2 * l(i))/3).10^{11})\ mod\ 254] + 1$
$Vc3(i) = [E(|h(i) - l(i)|.10^{10})\ mod\ 254] + 1$
// Translation vectors
$Vr(i) = \left[E\left((h(i) + l(i)).10^{12}\right) mod\ 253\right] + 2$
$Ve(i) = \left[E\left(\left(\frac{2*h(i)+3*l(i)}{5}\right).10^{12}\right) mod\ 253\right] + 2$
// Multiplication vectors
$Va(i) = \left[2 * E\left((h(i) + l(i)).10^{12}\right) + 1\right] mod\ 256 + 1$
$Vb(i) = \left[2 * E\left((h(i) * l(i)).10^{12}\right) + 1\right] mod\ 254 + 3$
$end\ for$

The two vectors (Va) and (Vb) contain only the invertible elements in the ring $(Z/256Z)$. In addition, our 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. $(\boldsymbol{Ba_i})$ Binary random vectors generation, $\boldsymbol{i} \in \{1, 2, 3\}$

//Binary vectors construction
$for\ i \leftarrow 1\ to\ 3nm$
$if\ h(i) > l(i)\ then$
$Ba1(i) \leftarrow 0$
$else:\ \ Ba1(i) \leftarrow 1$
$end\ if$
$if\ h(i) > 0{,}5\ then$
$Ba2(i) \leftarrow 0$
$else:\ \ Ba2(i) \leftarrow 1$
$end\ if$
$if\ h(i) \leq l(i)\ then$
$Ba3(i) \leftarrow 0$
$else:\ Ba3(i) \leftarrow 1$
$end\ if: end\ for$

Generation of genetic crossover table (GC)

This operation is a genetic crossover adapted to the encryption of color images that will be accompanied by a table (GC) of size (3nm,2). The construction of this table is given by the steps below:

- The 1st column is the arrangement (P) obtained by a decreasing sort on the first (3nm) values of the sequence (h).
- The second column is the permutation (P') obtained by an increasing sort on the first (3nm) values of the sequence (l).

Substitution tables generation

Our algorithm requires the development of two new replacement tables $(M1)$ and $(M2)$, each of size $(256;\ 256)$ and with coefficients in the ring $(Z/256Z)$.

(1). (M1) S-BOX generation

The main mission of this section is to construct the new Vigenere substitution matrix, called ($M1$), with a size of ($256; 256$), following the instructions provided below.

- The first row of the table ($M1$) 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 control vector $Ba1(i)$. This table was generated by Algorithm 5.

Algorithm 5. (M1) Substitution box generation

$for\ i \leftarrow\ 1\ to\ 256\ //First\ line$
$M1(1,i)\ \leftarrow\ Pt1(i)$
$end\ for$
$for\ i \leftarrow\ 2\ to\ 256\ //Next\ lines$
$for\ j \leftarrow\ 1\ to\ 256$
$if\ Ba1(i) = 0\ then$
$M1(i,j)\ \leftarrow\ M1(i-1, mod(j + Vc2(i),256))$
$else$
$M1(i,j)\ \leftarrow\ M1(i-1, mod(j + Vc3(i),256))$
$end\ if$
$end\ for: end\ for$

(2). (M2) S-BOX generation

The construction of the new substitution matrix ($M2$) of size ($256; 256$) is described by the following steps:

- The 1st line is the rearrangement ($Pr1$) obtained by a broad ascending order on the first 256 values of the vector ($Vc3$);
- The 2nd line is the rearrangement ($Pr2$) obtained by a broad ascending order on the first 256 values of the vector ($Vc2$);
- The 3rd line is the rearrangement ($Pr3$) obtained by a broad ascending order on the first 256 values of the vector ($Vc1$);
- The ith line ($i > 3$) is the composition of the functions of row ($i-2$) and ($i-3$) or ($i-3$) and ($i-1$), depending on the value of the control vector $Ba2(i)$.

These steps are illustrated in Algorithm 6 below.

Algorithm 6. (M2) Substitution box generation

$for\ i\ \leftarrow\ 1\ to\ 256$ //3 first lines
$M2(1,i)\ \leftarrow\ Pr1(i)$
$M2(2,i)\ \leftarrow\ Pr2(i)$
$M2(3,i)\ \leftarrow\ Pr3(i)$
$end\ for$
$for\ i\ \leftarrow\ 4\ to\ 256$ //Next lines
$for\ j \leftarrow\ 1\ to\ 256$
$if\ \ Ba2(i) = 0\ \ then$
$M2(i,j)\ \leftarrow\ M2(i-2, Tv2(i-3,j))$
$else$
$M2(i,j)\ \leftarrow\ M2(i-3, Tv2(i-1,j))$
$end\ if$
$end\ for$
$end\ for$

Encryption phase

The encryption phase unfolds through the subsequent stages:

(1). Original image vectorization

This phase involves uploading the original image of dimensions (n, m) and then extracting the (RGB) channel vectors (R), (G), and (B), which are concatenated under the control of the binary vector (Ba1) into a single vector (XD) of dimensions ($1, 3nm$). The mathematical formulation of this phase is described in Algorithm 8.

Algorithm 7. Original image vectorization algorithm

$for\ j \leftarrow\ 1\ to\ \ nm$
$if\ Ba1(j) = 0\ then$
$XD(3j-2)\ \leftarrow\ R(j) \oplus Vc1(j)$
$XD(3j-1)\ \leftarrow\ G(j) \oplus Vc2(j)$
$XD(3j)\ \leftarrow \mathrm{B}(j) \oplus Vc3(j)$
$else$
$XD(3j-2)\ \leftarrow\ R(j) \oplus Vc3(j)$
$XD(3j-1)\ \leftarrow\ G(j) \oplus Vc1(j)$
$XD(3j)\ \leftarrow\ B(j) \oplus Vc2(j)$
$end\ if: end\ for$

(2). First genetic crossover operation

After image preparation above, the genetic crossover will be applied to the integrity of the output vector (XD). This operation will be subject to the control of the table ($GC1$) and given by the expression (4) below.

$$X(i) = XD(GC1(i,1)) \oplus Vc1(GC1(i,2)) \ , \quad i \in [1\,, 3nm] \qquad (4)$$

The first column of the table ($GC1$) indicates the rank of the pixel to be modified, while its second column indicates the rank of the chaotic value chosen for the confusion. This algorithm is illustrated by the following figure (2).

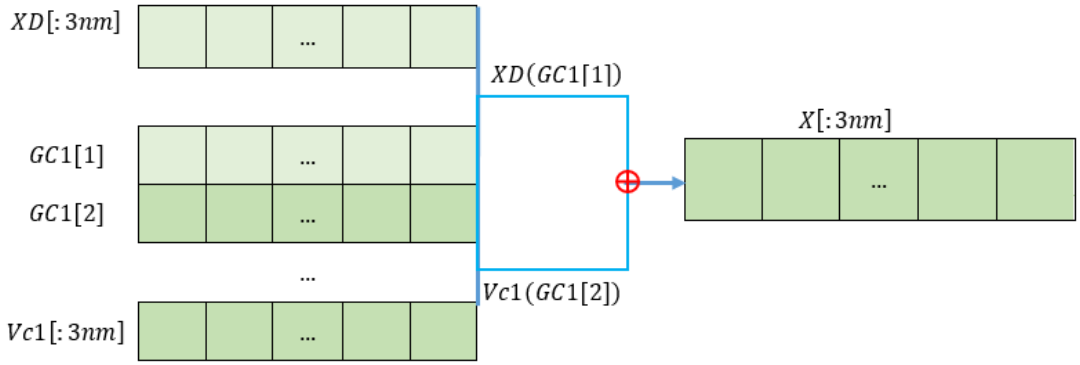


Fig 1. First genetic crossover operation

The first column of the table ($\boldsymbol{GC1}$) indicates the rank of the pixel to be modified, while its second column indicates the rank of the chaotic value chosen for the confusion.

Confusion and diffusion process

(1). Expression of the pseudorandom functions

Let (f_i) be the family of affine functions acting on the pixels. These functions are defined by equation (5).

$$\begin{cases} f_i : Z/256Z \ \rightarrow \ Z/256Z \\ x \ \longmapsto \ \begin{cases} mod(Va(i) * X(i) + Ve(i); 256) \ si \ Ba2(i) = 0 \\ mod(Vb(i) * X(i) + Vr(i); 256) \ si \ Ba2(i) = 1 \end{cases} \end{cases} \qquad (5)$$

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

(2). Confusion and diffusion function expression

The new substitution function involving matrices ($M1$) and ($M2$) is given by Algorithm7.

Algorithm 8. ($\boldsymbol{Fv}$) confusion and diffusion function expression

$Z(i) = Fv(X(i))$
if $Ba2(i) = 0$ *then*
  $Z(i) \leftarrow M1(Vc1(i), M2(Vc2(i); mod(Va(i) * X(i) + Ve(i); 256)))$
else
  $Z(i) \leftarrow M2(Vc3(i), M1(Vc1(i);\ mod(Vb(i) * X(i) + Vr(i); 256)))$
end if

(3). Initialization value calculation

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

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

This algorithm is illustrated in Figure 2 below.

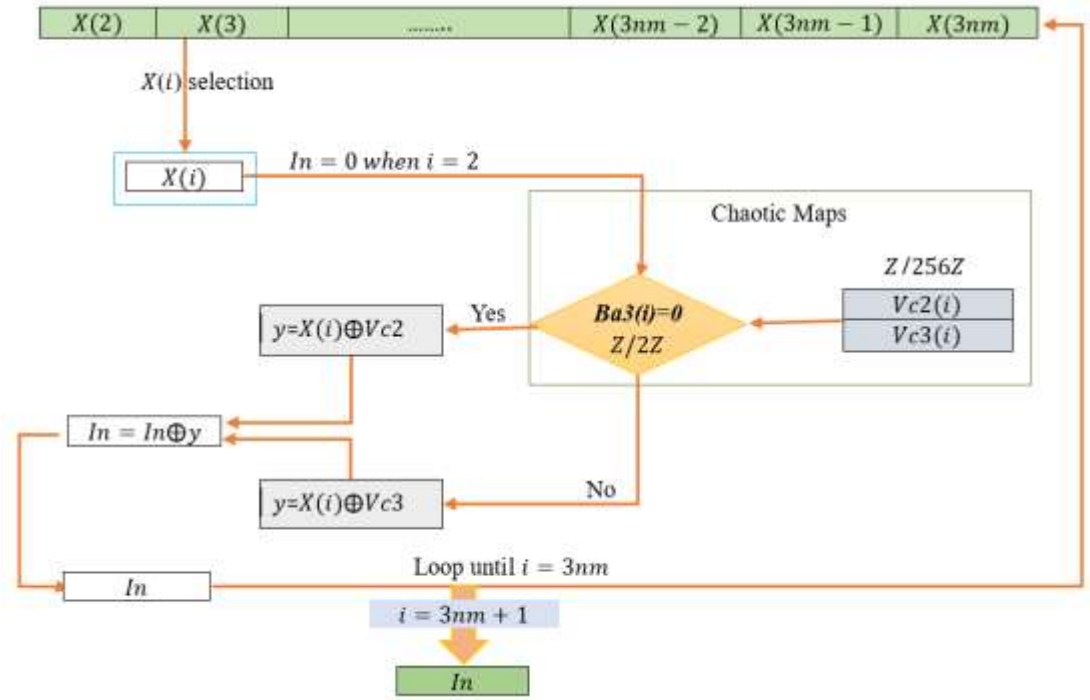


Fig 2. Initialization value calculation diagram

(4). Confusion and diffusion circuit

To overcome any differential attack, we first perform a diffusion round 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. Confusion and diffusion circuit

```
//First pixel encryption
Z(1) = Fv( X(1)⊕In⊕Vc1(1))
//Next pixels encryption
for i = 2 to 3nm
    α = f_i(X(i))⊕Z(i − 1)
    if Ba3(i) = 0 then
    Z(i) = Fv(α⊕Vc2(i))
    else
    Z(i) = Fv(α⊕Vc3(i))
    end if
end for
```

This algorithm can be interpreted in Figure 3.

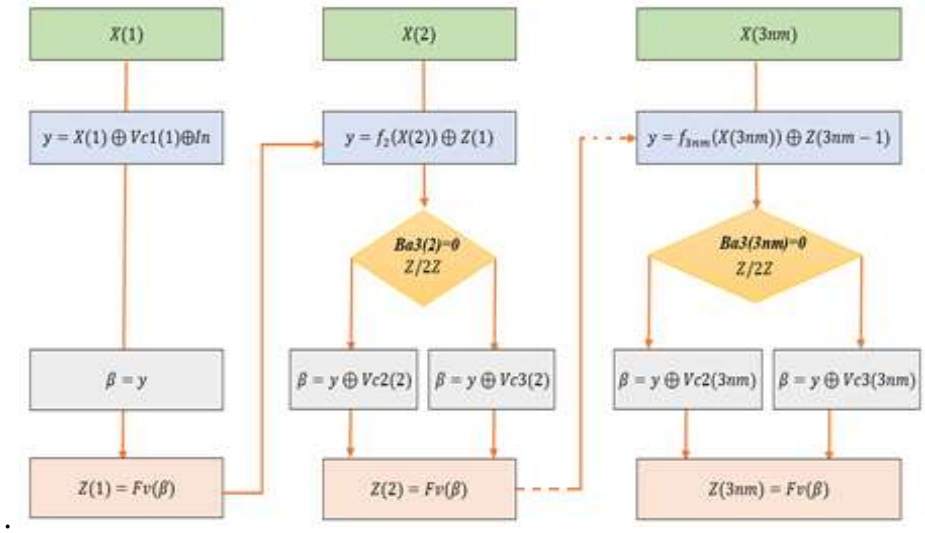


Fig 3. New circuit using dynamic pseudorandom affine functions

Second genetic crossover operation

After image preparation above, the genetic crossover will be applied to the integrity of the output vector (Z). This operation will be subject to the control of the table ($GC2$) and given by the expression (6) below.

$$T(i) = Z(GC2(i,1)) \oplus Vc2(GC2(i,2)) \ , \quad i \in [1, 3nm] \qquad (6)$$

The first column of the table ($GC2$) indicates the rank of the pixel to be modified, while its second column indicates the rank of the chaotic value chosen for the confusion. This algorithm is illustrated by the following figure (4).

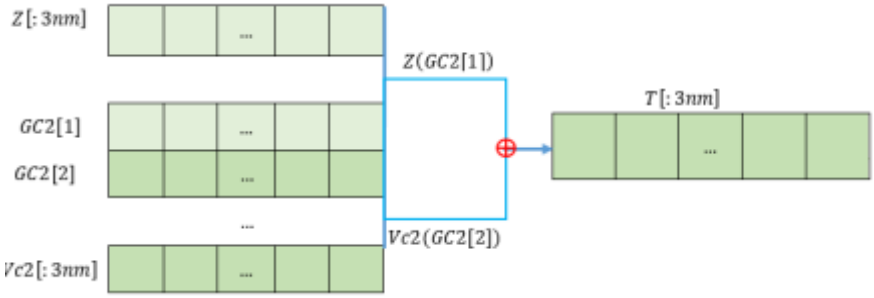


Fig 4. Second genetic crossover operation

The first column of the table ($\boldsymbol{GC2}$) indicates the rank of the pixel to be modified, while its second column indicates the rank of the chaotic value chosen for the confusion. The result vector (T) represents the cipher image.

Phase of decryption

The suggested encryption system is symmetric and employs two diffusion functions, necessitating that the decryption process commence by applying the inverse functions to the last operation. The encrypted image undergoes a transformation into a vector (Z) with dimensions (1; 3nm), upon which the subsequent steps are carried out:

- Application of the reverse for the second genetic crossover operation.
- Inverse of the pseudorandom functions and inverse of the confusion and diffusion circuit;
- Application of the reverse for the first crossover operation.

Result and Discussion

Experimental results

All the simulations were implemented in Python on the Windows 10 operating system with a hardware environment consisting of an i7 processor laptop, a 1 TB hard drive, and 32 GB of RAM. The main test image "Lena", as well as its encrypted and decrypted images, as well as all the plain images we used, are shown in Figure 5. These image samples were taken from the SIPI database (https://sipi.usc.edu/database/). The keys and other experimental parameters are generated from the chaotic maps described above. Prior to initiating the decryption process, the secret key needs to be securely transmitted to the recipient through a protected channel.

Statistical attacks

Several reference images chosen at random were tested by our new algorithm, and we recorded the following simulations:

(1). Analysis of possible keys space

Our algorithm uses two chaotic maps generated by four real parameters represented by 32 bits each, which encompasses a key of 120 bits. This ensures that our system is resistant to any brute-force attack.

(2). Key strength analysis

Our system uses two of the most widely utilized chaotic maps in the field of cryptography. Because they are highly sensitive to initial conditions, this guarantees significant responsiveness to our encryption key. This can be seen in the diagram in Figure 6.


Lena 256x256


Baboon 512x512


Panda 169x179


Vegetables 173x181


Apricot 165x177

Nike 158x182


Peper 512x512


House 512x512

Fig 5. Tested images

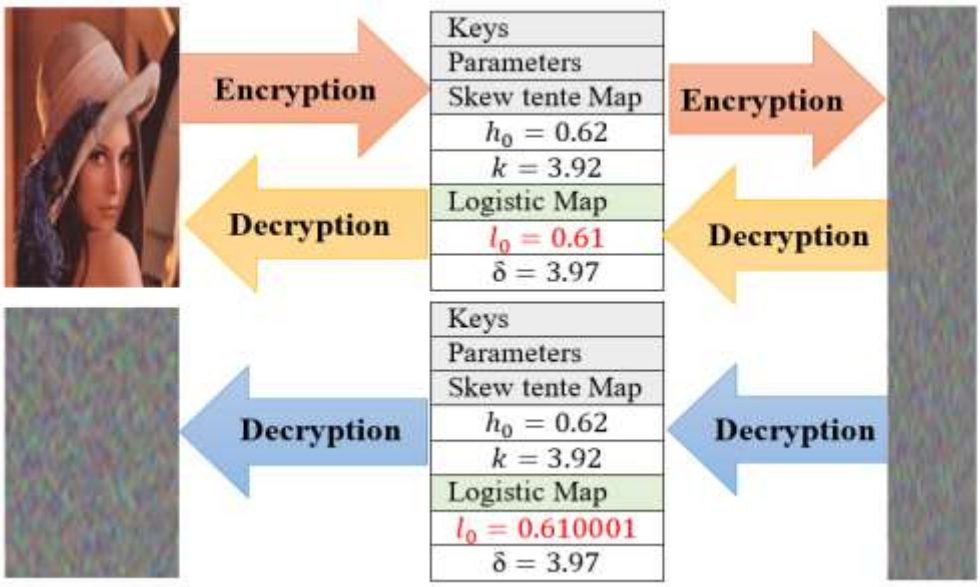


Fig 6. Key strength analysis

As illustrated in Figure 6, any modification of the encryption key will lead to two different ciphered images being obtained during the encryption stage. In addition, two decrypted images across the decryption stage will have completely different shapes. This demonstrates that the proposed algorithm exhibits high sensitivity to any small change in the encryption key.

(3). Visual aspect analysis

It is clear that the ciphered image is visually not similar to the plain image, as shown in Figure 7. In addition, all frequency distributions of images ciphered by our architecture are uniformly distributed, which confirms good security in opposition to any statistical attack.

(4). Analysis of histograms

Histograms of images showing the distribution of pixel values. Generally, an unauthorized party can derive crucial details about the encrypted image based on its disorganized histogram. Hence, to prevent the retrieval of useful information by an impostor, it is imperative that the histograms of cipher images are numerically not similar with those of plain ones. Additionally, they must exhibit a constant pixels distribution. Figures (8.a to h) illustrate the histograms of a sample of images tested by our algorithm, while Figures (9.a' to h') shows cipher images histograms. A histogram of the main tested image "Lena" is shown in Figure 8.a'. Figures (8.a to h) show three RGB channel histograms of the clear images, and Figures (9.a' to h') show the RGB channel histograms of ciphered images generated by the suggested method. It is observable that the histograms of the images generated by the encryption stage are almost uniform and flat.

Similarly, through the computation of histogram variances expressed in (7), we investigated the coherence of the encrypted images. A smaller variance in a ciphered image indicates greater uniformity and a higher protection level for the proposed image encryption method [21, 22].

$$H_{Var}(X) = \frac{1}{n^2}\sum_{p=1}^{n}\sum_{c=1}^{n}\frac{1}{2}(x_p - x_c) \qquad (7)$$

Where $X = x1, x2, \ldots, x256$ represents the histogram value vectors; and xp and xc denote pixels with p and c gray levels, respectively.

Table 4 lists the observed variances in the selected test images. Analysis of the data in the table reveals notably high variances in the plaintext images, contrasting with significantly lower variances in the encrypted counterparts. Specifically, the average variance for the encrypted "Lena" image was 223.666333, compared to 81232.023 for its plain image counterpart. A comparative assessment further suggested that for most of the tested images, the histogram variances in encrypted images obtained using the proposed method were consistently lower than those obtained in [23, 24, and 25]. This comparative evidence supports the assertion that our proposed algorithm has an enhanced capacity to bolster the security of the encryption process.

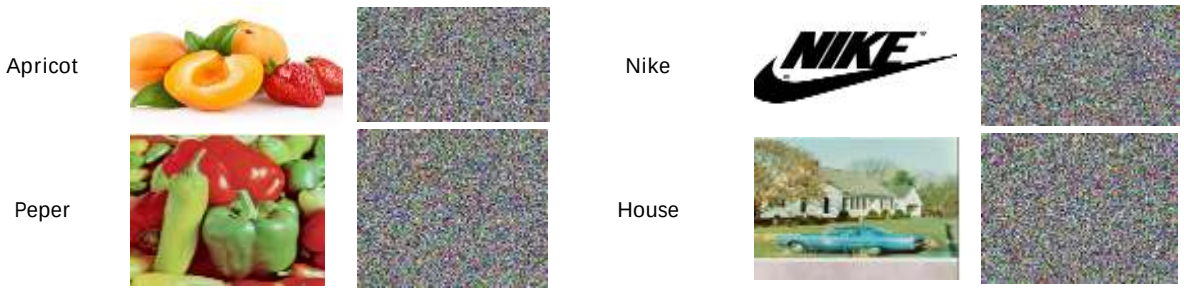


Fig 7. Visual aspect analysis

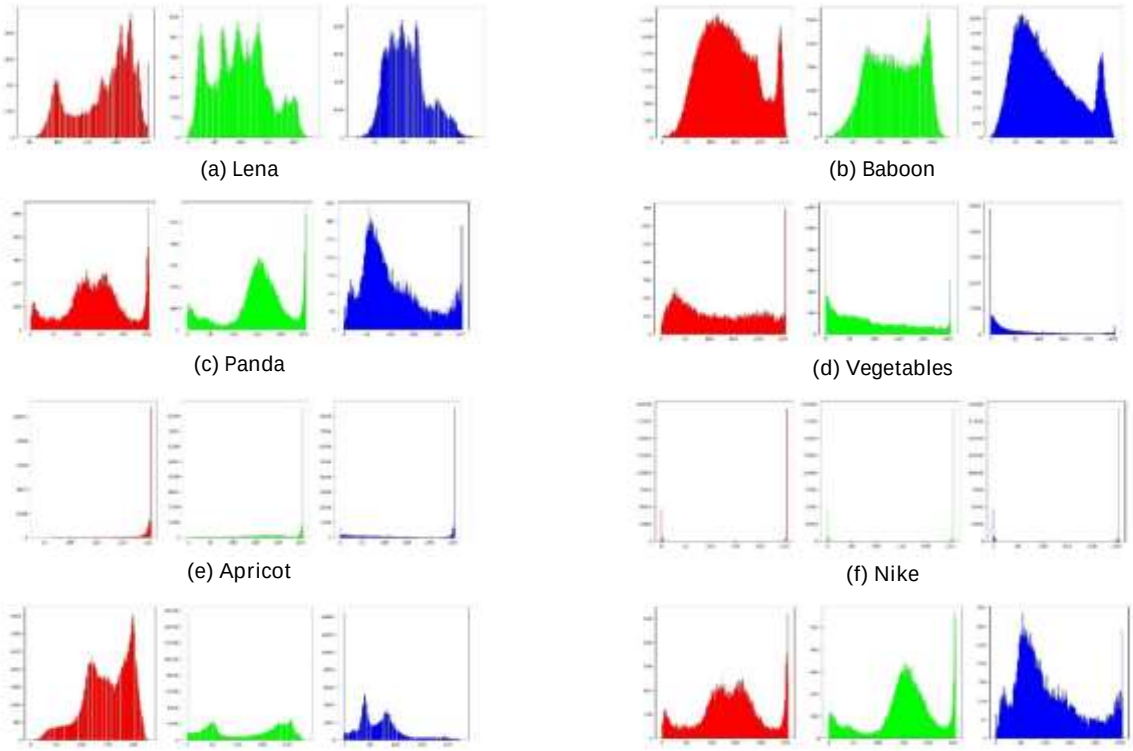


Fig 8. Histograms of the original images (RGB)

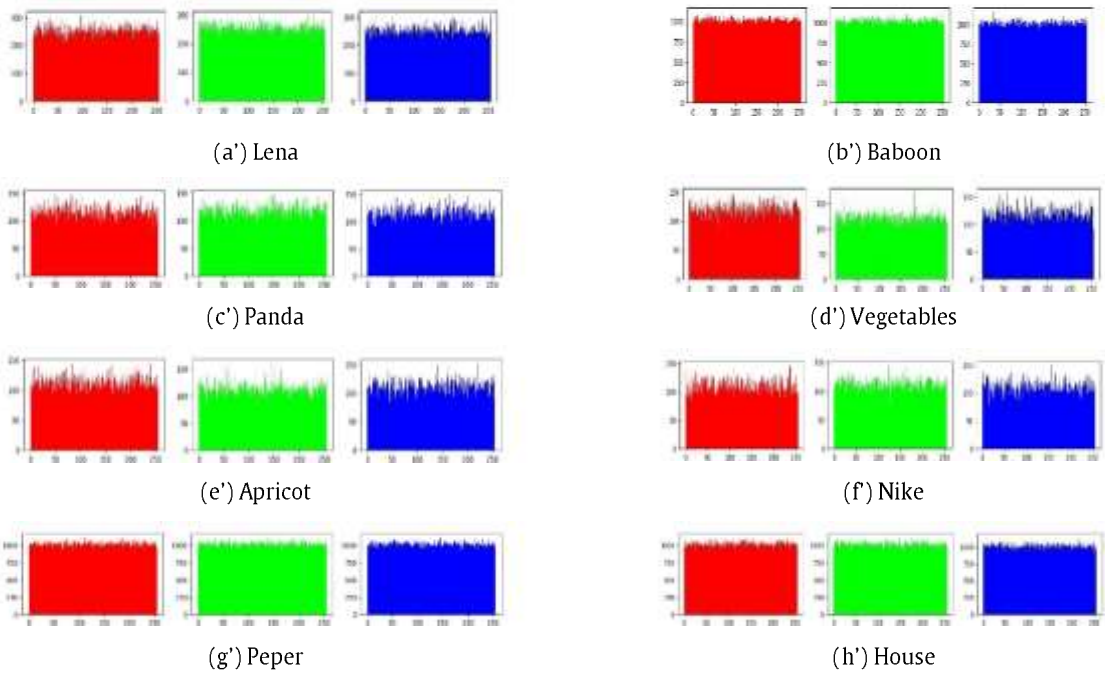


Fig 9. Histograms of the original images (RGB)

Table 2. Comparison of histogram variance for encrypted images between references

Images		Lena	House	Tree
Original	Red	123072,50	992034,12	129825,53
	Green	87100,835	1330180,12	57011,60
	Blue	33522,73	768126,75	81373,71
Proposed encrypted	Red	218,98	1136,54	250,86
	Green	231,03	1109,79	214,998
	Blue	220,99	1059,99	257,96
Encrypted [23]	Red	219,51	1136,56	250,87
	Green	231,05	1119,74	215,09
	Blue	221,11	1060,54	258,75
Encrypted [24]	Red	247,78	1070,20	282,81
	Green	279,62	1231,20	254,87
	Blue	265,71	941,65	225,79
Encrypted [25]	Red	264,27	1057,13	209,92
	Green	240,26	939,83	215,60
	Blue	251,12	1037,40	254,69

(5). Analysis of entropy

This constant serves for an image of size (n, m) as a metric to assess the security of that image encryption algorithm, indicating the level of unpredictability and randomness within a system. It is given by equation (8) below.

$$S(MC) = \frac{-1}{3nm}\sum_{i=1}^{3nm} p(i).log_2(p(i)) \quad (8)$$

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

Hence, as the entropy approaches 8, pixels are highly disordered in the image. A higher entropy ensures reduced information leakage from the specific ciphered image.

Table 5 presents the entropy values for the tested images, juxtaposed with those of several existing ciphering methods. The obtained results reveal that the values of entropy are greater than or equal to 7.996, comparable to [25] and surpassing values from [23, 33, 34, and 35].

(6). Correlation analysis

Equation (9) provides the correlation of an image with dimensions (n, m).

$$corr = \frac{cov(x,y)}{\sqrt{var(x)}.\sqrt{var(y)}} \quad (9)$$

Table 6 presents the pixel correlation values for images sourced from the SIPI database and other test images. Analysis of the data in the table reveals that the correlation in the plain image is notably high, nearly equal to a value of 1 for each channel. Conversely, in images encrypted using our proposed algorithm, the correlation is significantly low. This finding substantiates the effective security level achieved by our algorithm. Furthermore, these findings illustrate a substantial reduction in correlation within the encrypted image, signifying that information cannot be gleaned from the encrypted image by attackers through this method.

Table 3. Comparison of encrypted image entropy with other methods: (L) Lena, (Pe) Pepper, (H) House, (B) Baboon, (Pa) Panda, and (V) Vegetables

Algorithm	images	Encrypted		
		Red	Green	Blue
Proposed	(L)	7,9975	7,9975	7,9974
	(Pe)	7,9995	7,9995	7,9996
	(H)	7,9986	7,9984	7,9985
	(B)	7,9994	7,9993	7,9996
	(Pa)	7,9979	7,9973	7,9977
	(V)	7,9996	7,9995	7,9996
[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
[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
[34]	(L)	7,9870	7,9870	7,9860
[35]	(L)	7,9730	7,9750	7,9710

Table 4. Correlations between pixels in images taken from the SIPI database

Images		Original image			Encrypted image		
		Horizontal	Vertical	Diagonal	Horizontal	Vertical	Diagonal
Lena	Red	0,95580	0,96480	0,93220	-0,00376	0,00815	-0,00131
	Green	0,93556	0,95756	0,91902	-0,00298	0,00912	-0,00673
	Blue	0,90773	0,93930	0,89130	-0,00145	-0,00672	0,00064
Apricot	Red	0,98385	0,96944	0,98629	-0,00137	-0,00188	-0,00541
	Green	0,97883	0,98511	0,96537	-0,00107	0,00150	0,00234
	Blue	0,99153	0,98348	0,98724	0,00489	-0,00571	-0,00118
Panda	Red	0,95175	0,96552	0,93161	0,00513	-0,00077	-0,00495
	Green	0,95215	0,96436	0,93066	0,00788	-0,00080	0,00027
	Blue	0,95542	0,97086	0,94265	0,00007	0,01097	-0,00106
Nike	Red	0,98681	0,99219	0,97287	-0,00438	-0,01651	0,00668
	Green	0,98851	0,99103	0,97352	0,00239	0,00179	-0,00345
	Blue	0,98675	0,99049	0,97189	0,00875	0,00579	-0,00303
Vegetables	Red	0,97886	0,98012	0,96108	0,00124	-0,00326	0,00075
	Green	0,97749	0,97952	0,95947	-0,00076	-0,00245	0,00447
	Blue	0,97224	0,97091	0,94729	-0,00103	-0,00500	0,00152

Table 7 presents the pixel correlations observed in the 'Lena' image. A comparison with prior methods demonstrates that adjacent pixel mutual correlation in our encrypted image is inferior to that in references [25, 26], albeit comparable to that in reference [23]. All image correlation metrics tested by the proposed encryption system are very close to 0. This approach safeguards us from statistical attacks.

Table 5. Correlation between ciphered "Lena" pixels

Method	Horizontal	Vertical	Diagonal
Proposed	-0,0027336	0,0035	-0,0024696
[23]	-0,0042707	-0,0032498	-0,0020192
[25]	-0,0029883	0,0091357	-0,0067375
[26]	-0,0098	-0,0050	-0,0013

Differential attacks

To test the algorithm's efficacy in opposition to differential attacks, metrics such as the number of unified average change intensity (UACI), pixel change rate (NPCR), and avalanche effect are employed.

(1). NPCR and UACI metrics analysis

These metrics can be given by equations (10) and (11) below.

$$NPCR = \left(\frac{1}{3nm}\sum_{i,j=1}^{nm} Df(i,j)\right).100 \qquad (10)$$

$$UACI = \left(\frac{1}{3nm}\sum_{i,j=1}^{3nm} \frac{|Im_1(i,j) - Im_2(i,j)|}{255}\right).100 \qquad (11)$$

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

The data from Table 8 present UACI and NPCR values for two images, "Lena" and "Pepper", demonstrating that the UACI is greater than or equal to 33.53 and that the NPCR is greater than or equal to 99.69. These values clearly indicate that the NPCR efficacy of the proposed encryption architecture was comparable to that of [23] and superior to that of [25, 29, 30, 31, 32], while the UACI value was similar to that found in the same references. This finding suggests that the proposed approach exhibits high encryption performance, especially in halting differential attacks.

Table 6. Comparison of the NPCR and UACI

Method	Lena		Pepper	
	NPCR	UACI	NPCR	UACI
Proposed	99,73%	33,56	99,69	33,53
[23]	99,68%	33,46	99,67	33,48
[25]	99,60%	33,49	99,61	33,46
[29]	99,66%	33,44	99,63	33,47
[30]	99,60%	33,44	-	-
[31]	99,62%	33,65	-	-
[32]	99,6092%	33,4685	-	-

(2). PSNR metric analysis

In the domain of image processing, the mean squared error (MSE) and peak signal-to-noise ratio (PSNR) are commonly employed for evaluating the quality of encryption. These metrics are the most commonly employed criteria for evaluating the quality of two images within a cryptographic system. The PSNR measures the similarity between two images and is a

complement to the MSE. The mean squared error (MSE) for the original, decrypted, and encrypted images can be computed using the formula (12).

$$MSE = \frac{1}{(3nm)^2} \sum_{i,j=1}^{3nm} |Im_1(i,j) - Im_2(i,j)|^2 \qquad (12)$$

Where ($Im1$) and ($Im2$) are the plain and the cipher images, respectively. (n) denotes the number of rows in the original image, and (m) represents the number of columns in the image, and MSE stands for mean squared error.

The PSNR is evaluated in decibels and is inversely proportional to the mean squared error. It is determined by equation (13).

$$PSNR = 10 * log_{10}\left(\frac{(2^L - 1)^2}{MSE}\right) (dB) \qquad (13)$$

Where L=8 denotes the bit depth of the particular image.

A greater maximum signal-to-noise ratio (PSNR) signifies a reduced discrepancy between the plain and cipher images. In the event of identical plain and cipher images, the PSNR will be infinite. A comparison of the PSNR values between our approach and those of other references is illustrated in the table below.

The lower PSNR values observed in Table 9 for the original-to-encrypted images suggest that the proposed architecture provides better ciphering than those in [23, 36, and 37]. The value of this metric is comparable to that in [38]. These findings demonstrated that the proposed method is capable of retrieving images without significant information loss.

Table 7. The PSNR (dB) between the original, the encrypted, and the decrypted image

Method	Type of PSNR	Lena	Baboon	Panda	Vegetables
Our	Original to Encrypted	∞	∞	∞	∞
	Original to Encrypted	7,0211	7,1721	7,1727	6,8799
[23]	Original to decrypted	∞	∞	∞	∞
	Original to Encrypted	8,1102	8,7776	8,1648	6,8760
[36]	Original to Encrypted	8,3655	8,8532	-	-
[37]	Original to Encrypted	8,2522	8,8223	-	-
[38]	Original to decrypted	∞	∞	-	-
	Original to Encrypted	7,0257	7,1515	-	-

Conclusion

A fresh encryption method was devised by integrating a confusion-diffusion process alongside two genetic crossover operations tailored for image encryption. Following this, dynamic pseudorandom affine functions, utilizing coefficients generated through chaotic maps, were merged to create replacement operators. The process also involved integrating two comprehensive substitution matrices to aid in altering pixel values by employing novel Vigenere replacement functions. Simulations conducted on a diverse set of randomly selected images from different databases, featuring various formats and sizes, demonstrated the resilience of our algorithm against both differential and statistical attacks.

Declarations

Competing Interests

All authors of this article confirming the absence of any conflict between them, and there are no private or public organizations or laboratories to fund this research, thus avoiding any expected conflicts. This document does not contain any research or experiments conducted on animals or humans.

Funding

No government or private agency has financial work. This article is a great effort of the authors.

Acknowledgment:

Nothing to report. We publish this article to help the scientific community only

Compliance with Ethical Standards

Our article is in line with the ethics of the news paper

Research Data Policy and Data Availability Statements

In this article no scientific material or animal is used, except personal computers which remain at our disposal.

REFERENCES

[1] Alnajim, Abdullah M., et al. "Hybrid chaotic-based PRNG for secure cryptography applications." Applied Sciences 13.13 (2023): 7768.

[2] Es-Sabry, Mohammed, et al. "Securing Images Using High Dimensional Chaotic Maps and DNA Encoding Techniques." IEEE Access (2023).

[3] Rehman, Mujeeb Ur, et al. "Efficient and Secure Image Encryption Using Key Substitution Process with Discrete Wavelet Transform." Journal of King Saud University-Computer and Information Sciences (2023): 101613.

[4] Maiti, Chinmay, et al. "An Efficient and Secure Method of Plaintext-based Image Encryption Using Fibonacci and Tribonacci Transformations." IEEE Access (2023).

[5] Toktas, Abdurrahim, et al. "A robust bit-level image encryption based on Bessel map." Applied Mathematics and Computation 462 (2024): 128340.

[6] J. Zhou, J. Li, X. Di, A novel lossless medical image encryption scheme based on game theory with optimized ROI parameters and hidden ROI position, IEEE Access 8 (2020) 122210–122228.

[7] P. Murali, V. Sankaradass, An efficient ROI-based copyright protection scheme for digital images with SVD and orthogonal polynomials transformation, Optik 170 (2018) 242–264.

[8] Çelik, Hidayet, and Nurettin Doğan. "A hybrid color image encryption method based on extended logistic map." Multimedia Tools and Applications (2023): 1-24.

[9] X. Wang, S. Gao, Image encryption algorithm for synchronously updating Boolean networks based on matrix semi-tensor product theory, Inf. Sci. 507 (2020) 16–36.

[10] Huang, Penghe, et al. "A Novel Color Image Encryption Algorithm Using Coupled Map Lattice with Polymorphic Mapping." Electronics 11.21 (2022): 3436.

[11] G. Ye, K. Jiao, X. Huang, Quantum logistic image encryption algorithm based on SHA-3 and RSA, Nonlinear Dyn. 104 (2021) 2807–2827.

[12] Y. Zhang, A. Chen, Y. Tang, et al., Plaintext-related image encryption algorithm based on perceptron-like network, Inf. Sci. 526 (2020) 180–202.

[13] Chatterjee, Debanjan, Barnali Gupta Banik, and Abhinandan Banik. "Attack resistant chaos-based cryptosystem by modified baker map and logistic map." International Journal of Information and Computer Security 20.1-2 (2023): 48-83.

[14] C. Li, K. Tan, B. Feng, et al., The graph structure of the generalized discrete Arnold's cat map, IEEE Trans. Comput. 71 (2) (2022) 364–377.

[15] X. Wang, P. Liu, A new full chaos coupled mapping lattice and its application in privacy image encryption, IEEE Trans. Circuits Syst. I: Regul. Pap. 69 (3) (2022) 1291–1301.

[16] Chen, Y., Xie, S., & Zhang, J. (2022). A hybrid domain image encryption algorithm based on improved henon map. Entropy, 24(2), 287.

[17] Qumsieh, R., Farajallah, M., & Hamamreh, R. (2019). Joint block and stream cipher based on a modified skew tent map. Multimedia Tools and Applications, 78, 33527-33547.

[18] Zhang, Xiaoqiang, and Jingxi Tian. "Multiple-image encryption algorithm based on genetic central dogma." Physica Scripta 97.5 (2022): 055213.

[19] Sabir, S., & Guleria, V. (2023). Multilayer permutation-substitution operations based novel lossless multiple color image encryption. Multimedia Tools and Applications, 1-42.

[20] Zhang, X., & Tian, J. (2022). Multiple-image encryption algorithm based on genetic central dogma. Physica Scripta, 97(5), 055213.

[21] Ramasamy, P., Ranganathan, V., Kadry, S., Damaševičius, R., & Blažauskas, T. (2019). An image encryption scheme based on block scrambling, modified zigzag transformation and key generation using enhanced logistic—Tent map. Entropy, 21(7), 656.

[22] Wu, X., Kurths, J., & Kan, H. (2018). A robust and lossless DNA encryption scheme for color images. Multimedia Tools and Applications, 77, 12349-12376.

[23] Butt, K. K., Li, G., Khan, S., & Manzoor, S. (2020). Fast and efficient image encryption algorithm based on modular addition and SPD. Entropy, 22(1), 112.

[24] Li, C. (2016). Cracking a hierarchical chaotic image encryption algorithm based on permutation. Signal Processing, 118, 203-210.

[25] Khan, S., Lansheng, H., Qian, Y., Lu, H., & Meng Jiao, S. (2021). Security of multimedia communication with game trick based fast, efficient, and robust color-/gray-scale image encryption algorithm. Transactions on Emerging Telecommunications Technologies, 32(2), e4034.

[26] Zhang, X., Nie, W., Ma, Y., & Tian, Q. (2017). Cryptanalysis and improvement of an image encryption algorithm based on hyperchaotic system and dynamic S-box. Multimedia Tools and Applications, 76, 15641-15659.

[27] Wang, X., & Zhang, H. L. (2015). A color image encryption with heterogeneous bit-permutation and correlated chaos. Optics Communications, 342, 51-60.

[28] Xu, L., Li, Z., Li, J., & Hua, W. (2016). A novel bit-level image encryption algorithm based on chaotic maps. Optics and Lasers in Engineering, 78, 17-25.

[29] Niyat, A. Y., Moattar, M. H., & Torshiz, M. N. (2017). Color image encryption based on hybrid hyperchaotic system and cellular automata. Optics and Lasers in Engineering, 90, 225-237.

[30] Chen, J., Zhu, Z. L., Zhang, L. B., Zhang, Y., & Yang, B. Q. (2018). Exploiting self-adaptive permutation–diffusion and DNA random encoding for secure and efficient image encryption. Signal Processing, 142, 340-353.

[31] Ye, G., & Huang, X. (2017). An efficient symmetric image encryption algorithm based on an intertwining logistic map. Neurocomputing, 251, 45-53.

[32] Chen, C., Zhu, D., Wang, X., & Zeng, L. (2023). One-dimensional quadratic chaotic system and splicing model for image encryption. Electronics, 12(6), 1325.

[33] Wang, Y., Leng, X., Zhang, C., & Du, B. (2023). Adaptive fast image encryption algorithm based on three-dimensional chaotic system. Entropy, 25(10), 1399.

[34] Kadir, A., Hamdulla, A., & Guo, W. Q. (2014). Color image encryption using skew tent map and hyper chaotic system of 6th-order CNN. Optik, 125(5), 1671-1675.

[35] Wu, X., Wang, K., Wang, X., Kan, H., & Kurths, J. (2018). Color image DNA encryption using NCA map-based CML and one-time keys. Signal Processing, 148, 272-287.

[36] Liu, X., Xiao, D., & Xiang, Y. (2018). Quantum image encryption using intra and inter bit permutation based on logistic map. IEEE Access, 7, 6937-6946.

[37] Winarno, E., Nugroho, K., & Adi, P. W. (2023). Combined Interleaved Pattern to Improve Confusion-Diffusion Image Encryption based on Hyperchaotic System. IEEE Access.

[38] Aung, T. M., Naing, H. H., & Hla, N. N. (2019). A complex transformation of monoalphabetic cipher to polyalphabetic cipher:(Vigenère-Affine cipher). International Journal of Machine Learning and Computing, 9(3), 296-303