Multimedia Tools and Applications
https://doi.org/10.1007/s11042-024-19472-6

A new image encryption approach that uses an improved Hill-Vigenère method and chaotic maps

S. El Kaddouhi[1] · Y. Qobbi[2] · A. Abid[2] · M. Jarjar[2] · H. Zaaraoui[3] · A. Jarjar[4]

Received: 23 May 2023 / Revised: 19 May 2024 / Accepted: 26 May 2024

Abstract
Image encryption is an interesting field of research that is an adequate solution to ensure the safety and security of private information from unauthorized access. It involves rearranging the original message into an incomprehensible presentation so that only the intended recipient can understand and use it. In this paper, a new approach for image encryption based on an improved Hill-Vigenère ciphers using three chaotic maps is proposed. Firstly, five pseudo-random vectors and two control vectors are determined using three chaotic maps (Logistic map, Tent map, and Henon map). Secondly, the color image of size (n, m) is concatenated and merged with chaotic vectors to generate a vector of size 3 nm. Thirdly, the chaotic vectors are used to develop a new dynamic matrix inspired by the static Hill matrix and a new dynamic substitution matrix inspired by the Vigenère matrix, and to combine these two matrices. Finally, each original pixel is XORed with the previous encrypted pixel, then it's encrypted. This chaining mechanism increases the impact of the avalanche effect and makes the method robust to differential attacks. The performance of our algorithm is evaluated against various differential and statistical attacks based on several factors, such as key sensitivity, histogram, entropy, correlation, avalanche effect, UACI, NPCR, and PSNR. The proposed method is compared with several recent methods in the field. The simulation results, security results and the comparison results with other algorithms demonstrate that the algorithm has excellent security, which has the ability to resist common attacks.

Keywords Image encryption · Confusion · Diffusion · Hill cipher · Vigenère cipher · Chaotic maps

1 Introduction

The rapid advancement of science and technology has fostered an environment where individuals readily exchange personal data across digital platforms. However, this increased reliance on digital infrastructure has concurrently exacerbated concerns regarding unauthorized access to sensitive information, posing a significant challenge to information security [1, 2]. Data protection strategies often employ cryptographic methods like encryption

Extended author information available on the last page of the article

and steganography to ensure information security and confidentiality [3, 4]. While encryption transforms data into an unreadable format, steganography conceals the very existence of sensitive information within innocuous cover media, offering complementary approaches to safeguarding data against unauthorized access and potential breaches [4].

In the field of cryptography, various classical and modern algorithms have been explored and can be divided into as either symmetric or asymmetric algorithms [1, 2]. Symmetric algorithms, also known as private-key cryptography, employ a single shared key for both encryption and decryption processes [1]. Popular examples include the Advanced Encryption Standard (AES), Data Encryption Standard (DES), and Blowfish [1]. Asymmetric algorithms, or public-key cryptography, utilize a pair of mathematically related keys: a public key for encryption and a private key for decryption [1]. Popular examples include the RSA, Elliptic Curve, and Diffie-Hellman [1].

Although traditional cryptographic algorithms such as DES, AES, and RSA have proven effective for text encryption, their direct application to image data presents significant challenges [3]. Inherent properties of images, including large data size, high redundancy, and strong inter-pixel correlations, make these algorithms inefficient and potentially vulnerable when applied to image encryption [3]. Several algorithms have been proposed over the past decade for use in image encryption to meet security needs and protect the privacy of image information. One of the main techniques is a chaotic image encryption [3].

Chaotic encryption exploits the inherent complexity and nonlinear dynamics of chaotic systems to improve data security, with the goal of generating highly unpredictable ciphertexts that are resistant to traditional cryptanalysis methods [1–3]. By incorporating chaotic maps into encryption algorithms, researchers exploit properties such as sensitivity to initial conditions and deterministic randomness to establish complex relationships between plaintext, ciphertext, and encryption keys [1–3]. Thus, many chaos-based image encryption techniques [5–46] have been presented in recent decades. these techniques use the chaos to introduce randomness, disrupt statistical models, obscure any perceptible connection between the original image, the encrypted image and the secret key and thus respect the principles of confusion and diffusion (recommendations of Shannon) [1].

Confusion is a fundamental principle in image encryption that aims to obscure the relationship between the plaintext image, the ciphertext image, and the encryption key, making it difficult for attackers to decipher the original content [1–3]. This is typically achieved through operations such as pixel permutation, substitution, or a combination of both, often utilizing chaotic systems or other sources of randomness [1–3]. Permutation focusing on disrupting the pixel positions within an image to obscure its visual content and break correlations between adjacent pixels. By rearranging the pixel locations according to a specific rule or key, permutation introduces confusion into the encryption process, making it difficult for attackers to analyze the image statistically or visually [11–15]. Substitution involves changing pixel values based on a predefined rule or key, thereby hiding the original content of the image and introducing confusion into the encryption process. Unlike permutation, which rearranges pixel positions, substitution directly modifies pixel values, often using substitution tables (S-Boxes) or mathematical functions derived from chaotic systems. Efficient substitution techniques aim to achieve high nonlinearity and an avalanche effect, where a minor change in the plaintext image results in a substantial change in the cipher image [16–24]. There are various substitution methods, including simple XOR operations [5], the S-Boxes inspired by the Vigenère cipher [25–28], the Hill's cipher improvements [29, 30], the Feistel improvements [31, 32], the genetic algorithms [33–39, 42, 46].

Diffusion is a critical process in image encryption that aims to propagate the effect of a single plaintext change throughout the entire ciphertext, thereby obscuring statistical

relationships and enhancing resistance against cryptanalysis. Unlike permutation and substitution, which focus on individual pixel positions or values, diffusion operates on a larger scale, spreading the impact of modifications across multiple pixels. This is typically achieved through iterative operations involving XOR, modular arithmetic, or other mathematical functions, often incorporating chaotic sequences for added randomness. Effective diffusion techniques strive for a high avalanche effect, ensuring that even a small change in the plaintext image results in a significantly different ciphertext, making it difficult for attackers to decipher the original content [3].

In this article, we introduce an effective method for image encryption. It is based on the Hill cipher, the Vigenère cipher and three chaotic maps. Our technique takes place in four steps: First, five chaotic vectors and two control vectors are created from three chaotic maps (chaotic map, skew tent map and Henon map). In the second step, the original image is vectorized using chaotic vectors. In the third step, we proposed two improvements, one on the classical method of Hill and the other on the classical method of Vigenère. The fourth step is to encrypt the images using a combination of improved Hill and Vigenère methods and a diffusion mechanism to chain the system.

The main innovations and contributions of this article are as follows: (1) The proposal of a new chaotic system composed of three chaotic maps. The system allows seven pseudo-random vectors to be generated. (2) the use of concatenation attached to confusion with chaotic vectors to vectorize the original image. (3) The construction of a new S-box inspired by the Vigenère matrix. (4) The construction of a new dynamic matrix of size 3×3 inspired by the static Hill matrix. (5) The proposal of a new method to combines improved Hill's method and improved Vigenère's method using a control vector. (6) The use of a chaining mechanism connecting each pixel to the previous encrypted pixel to increase the avalanche effect. (7) The design of a new image encryption algorithm based on the combination of improved S-Box and Hill matrix and using a chaining mechanism.

This article is structured as follows: the second part describes some previous works. The third part presents the theoretical basis used in our method. The steps of our approach as well as the results obtained and their interpretations are the subject of the fourth and fifth parts. The conclusion and perspectives of this work are presented in the last part.

2 Related work

Several approaches for image encryption have been developed in recent decades, including:

The paper [6] describes a color image encryption algorithm that determines the necessary parameters for pixel scrambling using a two-dimensional chaotic map (2D-LSCM). The first step involves transforming the pixels of each channel by switching the rows and columns of different channels in accordance with the random sequences produced by the 2D-LSCM. Next, the four most significant bits of each channel's pixels are concatenated and shifted in a circular manner, both horizontally and vertically. The second stage consists of diffusing the scrambled pixels of each channel using the diffusion sequences controlled by the control sequences. The proposed method achieves high security and efficiency for color image encryption. Its main strengths include plaintext sensitivity, large keyspace, and fast encryption speed suitable for real-time applications. However, it only scrambles the most significant bits of each pixel, potentially leaving the least significant bits vulnerable. Additionally, assessment of resistance to specific advanced attacks is limited.

Noura Khalil et al.,[7] develop an efficient image encryption scheme for both color and grayscale images, employing a hybrid approach with chaotic maps. A 2D sine–cosine cross-chaotic map is utilized in the confusion phase to scramble pixel positions and break correlations. A 1D combined Logistic-Tent map generates a chaotic sequence for diffusion, modifying pixel values through bitwise XOR operations. This combination leverages the strengths of both 1D and 2D chaotic maps, achieving a balance between security and efficiency. The technique's reliance on the combined Logistic-Tent map and 2D sine–cosine map without thorough analysis of their long-term unpredictability raises potential security concerns.

In the article [8], the authors introduce a novel image encryption algorithm combining chaotic systems with Latin squares. The algorithm utilizes a permutation-substitution network based on the two-dimensional logistic map and Latin square operations for confusion and diffusion. Key strengths include a large key space, resistance against various attacks (brute-force, differential, chosen/known plaintext, and statistical), and robustness to noise during decryption. The scheme also incorporates LSB noise embedding and cyclic shift operations for added security. The proposed technique relies on the 2D logistic map, which is known to have weaknesses when discretized and may be susceptible to initial value estimation.

The authors of the article [9] develop a novel 2D hyperchaotic map called 2D-CLSS and utilizes it for image encryption. The 2D-CLSS demonstrates promising chaotic properties and a wide hyperchaotic range, making it suitable for cryptographic applications. The proposed image encryption scheme employs a simultaneous permutation and diffusion strategy, modifying both pixel positions and values based on chaotic sequences generated by the 2D-CLSS. The scheme exhibits strong security performance against various attacks, including statistical, differential, noise, and data loss attacks.

A color image encryption technique based on permutation, substitution, Boolean operations, and chaotic maps was proposed by Tahir Sajjad Ali, et al. [12]. The scheme employs three steps involving permutation, substitution, and diffusion. Permutation is achieved using a permutation table generated by a piecewise linear chaotic map, while substitution utilizes a chaotic S-box for pixel replacement. Finally, diffusion is implemented using the XOR operation with a logistic map-based random sequence. Security analysis demonstrates that the proposed algorithm effectively resists various attacks, including brute-force, statistical, and differential attacks.

Rasul Enayatifar, et al. [14] provides a novel image encryption method employing a synchronous permutation-diffusion technique for gray-level images. The method utilizes a 3D chaotic logistic map and DNA sequences to achieve both permutation and diffusion simultaneously, resulting in a faster encryption process. By combining chaotic systems with DNA operations, the scheme offers enhanced security against common attacks. Extensive experimental results and security analyses demonstrate the effectiveness and robustness of the proposed method in protecting image data during transmission.

Majid Mollaeefar et al. [15] proposes a novel color image encryption scheme based on two newly designed chaotic maps: BCosinus-Arcsinus (CA) and BSinus-Power Logistic (SPL), offering improved chaotic behavior. The scheme includes a chaotic-diagonal permutation method that is highly dependent on the plain image, resulting in efficient pixel shuffling and low correlation between adjacent pixels. The diffusion phase utilizes a coupled map based on the SPL map and a random selection technique to modify pixel values in each color channel independently. The encryption process boasts a large key space, high key sensitivity, and resistance against various attacks.

The article [21] proposes a fast and secure image encryption algorithm utilizing novel 1D chaotic systems and a new plain image substitution technique (PIST). The PIST enhances sensitivity to the original image pixels by performing bit-wise XOR operations between adjacent pixels. The algorithm employs S-boxes generated from the chaotic systems to achieve confusion and diffusion through a scrambling-masking process. Security tests and evaluations demonstrate the efficiency and the reliability of the proposed cryptosystem.

Younes Qobbi, et al. [24] present an image encryption algorithm using two chaotic maps (map and tent), dynamic permutation and a large substitution table. The permutation is generated by three parameters calculated from the pixel values of three-color channels (Red, Green and Blue) of the plain image. The second phase consists of performing a substitution of the pixels of each channel using a large substitution table generated by three chaotic permutations. In order to increase the avalanche effect of the proposed system, an enhanced ECBC chaining mode is used. Experimental results and security analyzes demonstrate the robustness of the proposed algorithm against statistical, brute-force, and differential attacks.

Ritesh Bansal, et al. [28] present a new image encryption scheme based on chaotic maps and the Vigenère scheme. This scheme has a turn consisting of two stages: diffusion and confusion. The first stage consists of three steps: forward scattering, the matching process using the Vigenère scheme, and backward scattering. In a later part, position swapping using a chaotic map is used to swap pixel positions.

M. Essaid, et al. [29] propose a new image encryption algorithm based on a secure variant of Hill Cipher (HC) and three improved one-dimensional (1D) chaotic maps. The proposed scheme fully satisfies the two basic concepts of security, namely confusion and diffusion. The confusion is ensured by the product of a vector consisting of the key-pixel pair and a 2×2 Hill matrix on the one hand, and the addition of another pseudo-random translation vector on the other hand. And diffusion is ensured by a strong avalanche effect which connects each encrypted pixel to its neighbour.

The article [32] describes a new cryptosystem which integrates the most powerful genetic operators in the field of color image encryption. This technique begins with the application of an advanced Feistel scheme and ends with the implementation of deeply modified genetic operators. After vectorization of the original image, an application of the advanced Feistel scheme on blocks of random size will be launched. The output vector is transcribed into restricted ASCII code to carry out a genetic crossing suitable for the encryption of color images. The resulting output vector is transcribed into restricted ASCII code to significantly improve the effects of genetic crossing. Simulations on various images demonstrate the effectiveness and security of the proposed cryptosystem against known attacks.

The image encryption method proposed by Mahdieh Ghazvini, et al. [35] is based on genetic algorithm and chaos. The encryption process includes three main stages: the confusion phase, the diffusion phase and the improvement phase using a genetic algorithm. At first, Chen's chaotic map is used in the confusion stage to generate a scrambled image by shuffling the pixels of the simple image, and in the diffusion stage, the Logistic-Sine map changes the gray level values of these pixels. It produces some of the encrypted images which were considered as the initial population for the genetic algorithm. Then, using the genetic algorithm, the encrypted images are optimized to the maximum. Finally, the best encrypted image is the final encrypted image.

Jieyu Zheng, et al. [36] expose a new image encryption scheme combining dynamic DNA sequence encryption with an improved 2D logistic sine map (2D-LSMM) for

enhanced security. The 2D-LSMM exhibits better ergodicity and randomness compared to traditional chaotic maps, while dynamic DNA encoding rules, determined by chaotic sequences, add complexity to the encryption process. A logistic map generates a chaotic image for processing DNA operations with the plaintext image. Experimental results and security analysis demonstrate the effectiveness of the scheme in resisting various attacks, including statistical and differential attacks.

Bhaskar Mondal et al. [39] presents a secure image encryption scheme utilizing a novel hybrid pseudo-random number generator (HPRNG) and genetic operations. The HPRNG combines a linear feedback shift register (LFSR) with chaotic maps to generate a highly random bit sequence. The encryption process involves XOR operations and genetic operations like mutation and multipoint crossover, applied to image blocks for confusion and diffusion. The scheme boasts a large key space and produces cipher images with low correlation to the original images and high entropy values. The proposed method is efficient and demonstrates comparable or superior security performance compared to existing schemes.

3 Theoretical foundations

3.1 Chaotic maps

Chaotic maps are mathematical functions that exhibit complex, unpredictable behaviour even though they are deterministic. These maps are widely studied in various fields including physics, biology, and cryptography due to their ability to generate randomness and simulate chaotic systems. Examples of the most popular chaotic maps include the logistic map, the Henon map, and the Tent map.

3.1.1 The logistic map

The logistics map is a one-dimensional chaotic map. The following equation provides its definition:[7]

$$u_{n+1} = \mu_0 u_n \left(1 - u_n\right) \tag{1}$$

where u_0 is the initial condition and μ_0 is the control parameter.

The Fig. 1 presents the bifurcation plot of the logistic map with $u_0 = 0.79878796$ and $\mu_0 \in [24]$.

As shown in Fig. 1 the logistics map behaves chaotically when $\mu_0 \in [3{,}754]$, so in our experiment we chose $u_0 = 0.79878796$ and $\mu_0 = 3.755$.

3.1.2 The tent map

The Tent map is a one-dimensional chaotic map described by the following recurrence relation [7]:

$$v_{n+1} = \begin{cases} \mu_1 v_n if v_n < 0.5 \\ \mu_1 \left(1 - v_n\right) Otherwise \end{cases} \tag{2}$$

where v_0 is the initial condition and μ_1 is the control parameter.

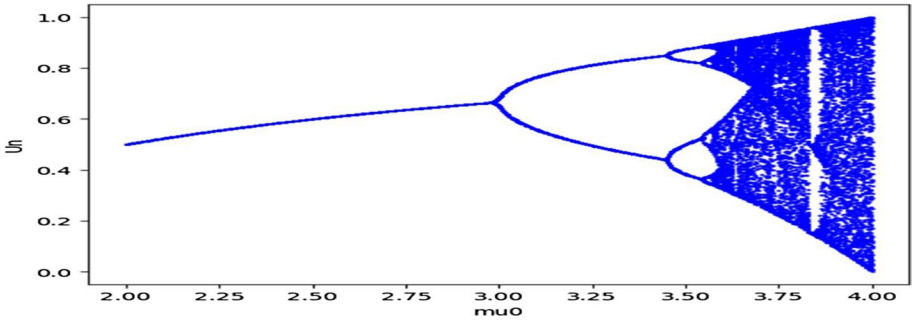


Fig. 1 Bifurcation plot of the logistic map [7]

The Fig. 2 presents the bifurcation plot of the tent map with $v_0 = 0.89878796$ and $\mu_1 \in [02]$.

As shown in Fig. 2 the logistics map behaves chaotically when $\mu_1 \in [12]$, so in our experiment we chose $v_0 = 0.89878796$ and $\mu_1 = 1.39$.

3.1.3 The Henon map

The Henon map is a two-dimensional discrete-time dynamical system known for its simple formulation and complex chaotic behaviour. It is defined by the following equation: [33]

$$x_{n+1} = 1 - \mu_2 x_n^2 + y_n y_{n+1} = \mu_3 x_n \tag{3}$$

The Henon map is governed by two control parameters μ_2 and μ_3.

The Henon map may also be deconstructed into a one-dimensional map, defined as follows:

$$w_{n+2} = 1 - \mu_2 w_{n+1}^2 + \mu_3 w_n \tag{4}$$

where w_0 and w_1 is the initial conditions and $\mu_2 and \mu_3$ is the control parameters.

The Fig. 3 presents the bifurcation plot of the Henon map with $w_0 = 0.47856$, $w_1 = 0.78796$, $\mu_2 \in [11.5]$ and $\mu_3 = 0.3$

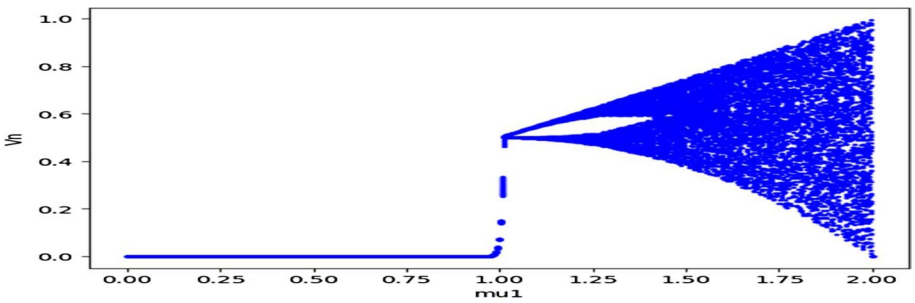


Fig. 2 Bifurcation plot of the tent map [7]

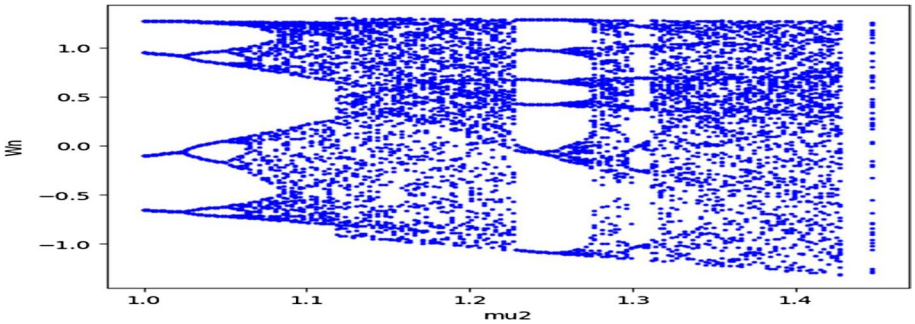


Fig. 3 Bifurcation plot of the Henon map [33]

As shown in Fig. 3 the Henon map behaves chaotically when $\mu_2 \in [1.31.45]$, so in our experiment we chose $w_0 = 0.47856$, $w_1 = 0.78796$, $\mu_3 = 1.4$ and $\mu_3 = 0.3$.

3.2 The HILL cipher

The Hill cipher [41] is a text encryption system, based on the segmentation of original text to blocks $\boldsymbol{X} = \{\boldsymbol{x}_1, \boldsymbol{x}_2, \ldots, \boldsymbol{x}_p\}$ of size $\boldsymbol{p}$, and on the construction of an invertible matrix $\boldsymbol{A}$ of size $\boldsymbol{p} \times \boldsymbol{p}$ whose elements are in $\boldsymbol{Z}/26\boldsymbol{Z}$. Encrypted blocks $\boldsymbol{Y} = \{\boldsymbol{y}_1, \boldsymbol{y}_2, \ldots, \boldsymbol{y}_p\}$ are obtained by the following encryption formula:

$$\mathrm{Y} = \mathrm{A} \times \mathrm{X} \ (\mathrm{mod} 26) \tag{5}$$

Decryption is determined by the equation below:

$$\mathrm{X} = \mathrm{A}^{-1} \times \mathrm{Y} \tag{6}$$

$\mathbf{A}^{-1}$ is the inverse matrix of $\mathbf{A}$

3.3 The Vigenère cipher

The Vigenère cipher [43] is a symmetric cipher using polyalphabetic substitution to encrypt and decrypt the secret message. To encrypt a text, we choose an encryption key, to each letter of the Plain-Text we match a letter of the key (the key being repeated as many times as necessary). The correspondence uses a substitution table of size 26×26 (Matrice de Vigenère). The letter of the Cipher Text will be taken from the column corresponding to the letter of the Plain-Text, and from the row corresponding to the letter of the key.

Let m, be a positive integer and $\mathrm{K} = (\mathrm{k}_1, \mathrm{k}_2, \ldots, \mathrm{k}_m)$ be a key where each $Ki \in Z_{26}$. If we set C the Ciphertext, P as the Plain-Text and K as the key, we can express this mechanism by the following formula:

Encryption:

$$C_i = (P_i + K_{imodm}) mod 26 \tag{7}$$

Decryption:

$$P_i = (C_i - K_{imodm}) mod 26 \tag{8}$$

4 Proposed method

Our method for image encryption contains four steps. In the first, we used the logistic map, the tent map and the Henon map to generate three chaotic sequences which are used to construct five pseudo-random vectors and two binary control vectors. In the second, the original image is vectorized utilizing the chaotic vectors. In the third stage, we introduce improvement to the Hill cipher and Vigenère cipher. Finally, the images are encrypted employing a combination of the improved Hill and Vigenère methods, along with a diffusion mechanism.

The various steps of our image encryption method are shown in Fig. 4 below.

4.1 Chaotic vector development

To build our algorithm, we use the logistic map, the tent map and the Henon map to generate three chaotic sequencesu_n, v_n and w_n. These three sequences are used to construct five pseudo-random vectors (V1, V2, V3, V4 and V5) and two control binary vectors (CV1 and CV2). The generation of these vectors is determined by the following algorithm 1:

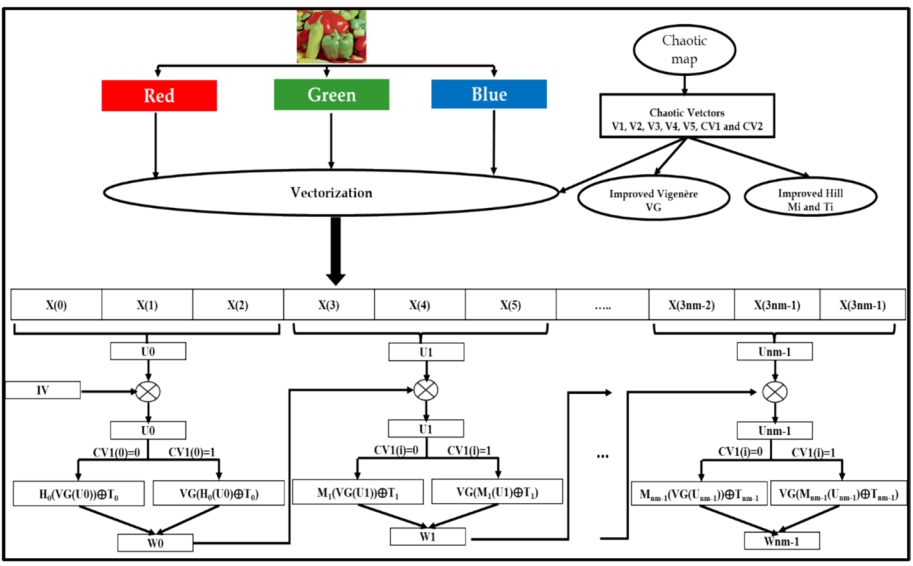


Fig. 4 Diagram of image encryption by our method

Algorithm 1 Control and chaotic vector creation

Input
Chaotic sequences: u_n, v_n and w_n
Output
Chaotic vectors: V1, V2, V3, V4, V5
Control vectors: CV1, CV2
Begin
For i=0 **To** 3nm-1

$$V1(i) = \mathrm{mod}\left(E\left(\frac{u(i)+2v(i)}{3} * 10^{10}\right), 255\right)$$

$$V2(i) = \mathrm{mod}\left(E\left(\frac{v(i)+w(i)}{2} * 10^{10}\right), 255\right)$$

$$V3(i) = \mathrm{mod}\left(E\left(\frac{u(i) * w(i) + \inf(u(i), w(i))}{2} * 10^{10}\right), 255\right)$$

$$V4(i) = E\left(\frac{V1(i) + 2 * V2(i)}{3}\right)$$

$$V5(i) = E\left(\frac{2 * V1(i) + V3(i)}{3}\right)$$

If $u(i) \geq v(i)$ **then**
$CV1(i) = 0$
Else
$CV1(i) = 1$
End if
If $u(i) \geq w(i)$ then
$CV2(i) = 0$
Else
$CV2(i) = 1$
End if
End for
End

4.2 Preparation of the original image

4.2.1 Vectorization of the original image

After the three color channels were extracted (RGB) and converted to vectors $(Vr), (Vg)$ and (Vb) of size $(1, nm)$, we apply a concatenation attached to a confusion with the chaotic vectors to generate the vector $\boldsymbol{X}(\boldsymbol{x}_0, \boldsymbol{x}_1, ..., \boldsymbol{x}_{3nm-1})$ of size $(1, 3nm)$. The algorithm 2 explains this operation.

Algorithm 2 Original image vectorization

Input
Original image vectors: (Vr), (Vg) and (Vb) of size (1, nm)
Chaotic vectors: V1, V2, V3, V4, V5 and CV2
Output
Vector image: X of size (1, 3nm)
Begin
For i=0 **To** nm-1
If $CV2(i) = 0$ **then**
$X(3i) = Vr(i) \oplus V1(3i)$
$X(3i+1) = Vg(i) \oplus V2(3i+1)$
$X(3i+2) = Vb(i) \oplus V3(3i+2)$
Else
$X(3i) = Vr(i) \oplus V3(3i)$
$X(3i+1) = Vg(i) \oplus V4(3i+1)$
$X(3i+2) = Vb(i) \oplus V5(3i+2)$
End if
End for
End

4.2.2 Block subdivision (U_i)

The image vector (X) will be converted into a matrix U of size (nm, 3). The matrix U is given by algorithm 3:

Algorithm 3 Block subdivision

Input
Vector image: X of size (1, 3nm)
Output
Matrix image: U of size (nm,3)
Begin
For i=0 **To** nm-1
U[i,0]= X(3i)
U[i,1]= X(3i+1)
U[i,2]= X(3i+2)
End for
End

4.3 Combined Hill-Vigenère method

4.3.1 Improved Vigenère method

This step consists of establishing a substitution matrix (SB), whose first row is generated from a permutation (P) obtained using the reference method [42], and the other rows are obtained by shifts from the first row. The algorithm 4 explains this operation.

Algorithm 4 Substitution matrix development

```
Input
        Chaotic vectors: V1 and CV2
Output
        Substitution matrix: SB of size (255, 255)
Begin
// First line construction
    int c=0
    For i=0 to 255
        For j 0 to 255
            if (V1(j)==i) then
                SB(0,j)=c
                c++
            End if
        End for
    End for
// Next lines construction
    for i=1 to 255
        for j=0 to 255
            if (CV2(j)==1) then
                SB(i,j)=SB(i-1, (mod(j+V1(i)),256))
            else
                SB(i,j)=SB(i-1,(mod(j+V2(i)),256))
            End if
        End for
    End for
End
```

The application of the improved Vigenère method on a Ui block is given by the following formula:

$$VG\left(U_i\right) = SB\left(V1(i), U_i \oplus \mathrm{V3(i)}\right) \tag{9}$$

4.3.2 The Improved Hill method

This step proposes a classic Hill cipher improvement using an affine transformation composed of an invertible matrix of size (3,3) and a translation vector.

The matrices (M_i) are invertible dynamic matrices of size (3, 3) constructed by the following formula:

$$M_i = \begin{pmatrix} 1 & V1(i) & V3(i) \\ V2(i) & 1 + V1(i) * V2(i) & V4(i) \\ 0 & 0 & 2V5(i) + 1 \end{pmatrix} \tag{10}$$

The translation vectors are invertible dynamic vectors of size (1,3) constructed by the following formula:

$$T_i = \begin{pmatrix} V5(i) \\ V4(i) \\ V3(i) \end{pmatrix} \tag{11}$$

4.3.3 Combined Hill-Vigenère method

Our proposed method combines improved Hill's method and improved Vigenère's method using the following formula:

$$W_i = \begin{cases} M_i\big(VG\big(U_i\big)\big) \oplus T_i if CV1(i) = 0 \\ VG\big(M_i\big(U_i\big) \oplus T_i\big) else \end{cases} \tag{12}$$

4.4 The encryption steps

The encryption process begins by calculating an initialization vector IV, then applying the combined Hill-Vigenère method on the (IV XOR U1) to obtain the vector W1. Then, to apply the combined Hill-Vigenère method on the (W1 XOR U2) to obtain the vector W2. The same steps will be repeated on the other vectors Ui to obtain the vectors Wi that form the encrypted image (see Fig. 4). The algorithm 5 illustrates this step.

Algorithm 5 Encryption algorithm

```
Input
        Chaotic vectors: V1, V2, V3
        Matrix image: U of size (nm,3)
        Substitution matrix: SB of size (255, 255)
Output
        Encrypted Matrix image: W of size (nm,3)
Begin
// Initialization vector
    IV(0)=0
    IV(1)=0
    IV(2)=0
    for i=1 to nm-1
        IV(0)=IV(0)⊕U[i,0]
        IV(1)=IV(1)⊕ U[i,1]
        IV(2)=IV(2)⊕ U[i,2]
    End for
// Block (U0)
    a=U[0,0]⊕IV(0)
    b= U[0,1]⊕IV(1)
    c= U[0,2]⊕IV(2)
    if (CV2(0) ==0) then
        a= SB(V1(0), a⊕V3(0))
        b= SB(V1(1), b⊕V3(1))
        c= SB(V1(2), c⊕V3(2))
        W[0,0]= mod(a+V1(0)*b+V3(0)*c,256)⊕V5(0)
        W[0,1]= mod(a*V2(0)+(1+V1(0)*V2(0))*b+V4(1)*c,256)⊕V4(0)
        W[0,2]= mod(a*(2V5(0)+1),256)⊕V3(0)
    else
        a= mod(a+V1(0)*b+V3(0)*c,256)⊕V5(0)
        b= mod(a*V2(0)+(1+V1(0)*V2(0))*b+V4(1)*c,256)⊕V4(0)
        c= mod(a*(2V5(0)+1),256)⊕V3(0)
        W[0,0]= SB(V1(0), a⊕V3(0))
        W[0,1]= SB(V1(1), b⊕V3(1))
        W[0,2]= SB(V1(2), c⊕V3(2))
    End if
// Blocks (U1, … Unm-1)
    for i=1 to nm-1
        a=U[i,0]⊕W[i-1,0]
        b=U[i,1]⊕ W[i-1,1]
        c=U[i,2]⊕ W[i-1,2]
        if (CV2(0) ==0) then
            a= SB(V1(3i), a⊕V3(3i))
            b= SB(V1(3i+1), b⊕V3(3i+1))
            c= SB(V1(3i+2), c⊕V3(3i+2))
            W[i,0]= mod(a+V1(3i)*b+V3(3i)*c,256)⊕V5(3i)
            W[i,1]= mod(a*V2(3i)+(1+V1(3i)*V2(3i))*b+V4(3i)*c,256)⊕V4(3i)
            W[i,2]= mod(a*(2V5(3i)+1),256)⊕V3(3i)
        else
            a= mod(a+V1(3i)*b+V3(3i)*c,256)⊕V5(3i)
            b= mod(a*V2(3i)+(1+V1(3i)*V2(3i))*b+V4(3i)*c,256)⊕V4(3i)
            c= mod(a*(2V5(3i)+1),256)⊕V3(3i)
            W[i,0]= SB(V1(3i), a⊕V3(3i))
            W[i,1]= SB(V1(3i+1), b⊕V3(3i+1))
            W[i,2]= SB(V1(3i+2), c⊕V3(3i+2))
        End if
    End for
End
```

4.5 The decryption step

The proposed approach is a symmetric technique with broadcast implementation. Therefore, in the decryption step, we apply the following decryption functions:

$$U_i = \begin{cases} M_i^{-1}\left(VG^{-1}\left(W_i\right)\right) \oplus T_i if CV1(i) = 0 \\ VG^{-1}\left(M_i^{-1}\left(W_i\right) \oplus T_i\right) else \end{cases} \tag{13}$$

–M^{-1} denotes the inverse matrix of the matrix (M). Its expression is given by:

$$M_i^{-1} = \begin{pmatrix} \alpha & \beta & \gamma \\ \delta & 1 & \theta \\ 0 & 0 & \rho \end{pmatrix}$$

With:$\alpha = 1 + V1(i) * V2(i), \beta = -V1(i), \quad \gamma = \frac{(2V5(i)+1)V3(i)-V4(i)}{2V5(i)+1}, \delta = -BL(i),$
$\theta = \frac{V4(i)-V2(i)*V3(i)}{2V5(i)+1}$ and $\rho = \frac{1}{2V5(i)+1}$

–The inverse Vigenère function VG^{-1} is given by the following formula:

$$VG^{-1}\left(W_i\right) = SB^{-1}\left(V1(i), W_i \oplus \mathrm{V3(i)}\right) \tag{14}$$

–The inverse substitution matrix SB^{-1} of size 255×255 is given by the following formula:

$$SB^{-1}(i, SB(i, j)) = j \tag{15}$$

5 Experimental results

To evaluate our encryption approach presented in this article, various tests are used, namely: visual evaluation, keyspace analysis, Keyspace Sensitivity, statistical attack analysis (entropy, histogram, correlation) and differential attack analysis (UACI, NPCR, avalanche effect). The tests are run on a set of standard images of various sizes, extracted from the USC-SIPI database [47]. For the performance analysis, we will present the simulation of ten images of different sizes (Female (256×256), Couple (256×256), House (256×256), baboon (512×512), Lena (512×512), Peppers (512×512), Splash (512×512), Airplane (512×512) Stockton (1024×1024) and Washington (2250×2250)) chosen from the images used to test our method. For comparison with recent publications, we will choose the three most commonly used images in the literature (Baboon, Lena and Peppers).

5.1 Visual evaluation

This test allows us to visualize if the encrypted images can provide information about the original image and if the decrypted images are identical to the original images. Table 1 presents the results obtained for ten images chosen from the test images.

Table 1 Simulation results

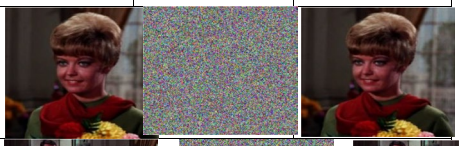
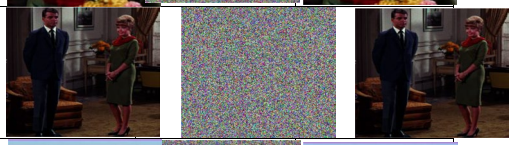
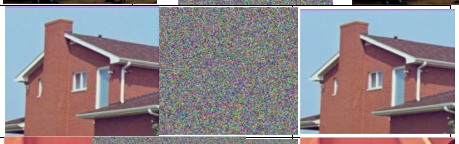
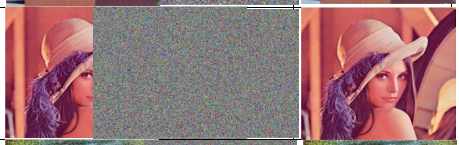
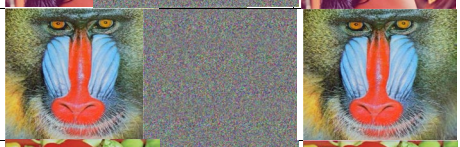
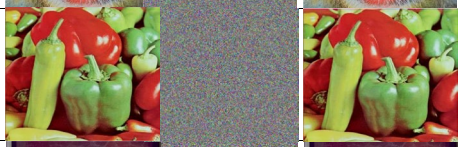
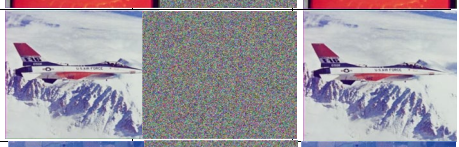
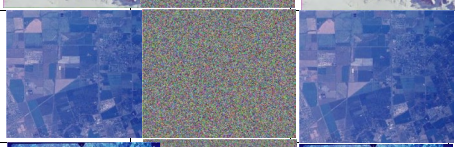
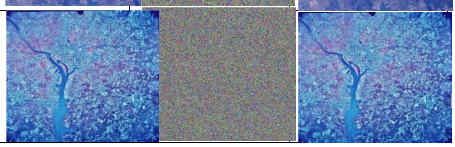
Name	Original Image	Encrypted images	Decrypted images
Female (256x256)			
Couple (256×256)			
House (256×256)			
Lena (512×512)			
Baboon (512×512)			
Peppers (512×512)			
Splash (512×512)			
Airplane (512x512)			
Stockton (1024×1024)			
Washington (2250x2250)			

Table 2 Keyspace comparison

Methods	Keyspace
Our Method	$\mathbf{2^{512}}$
Demirtaş, M [6]	2^{512}
Khalil, N., [7]	2^{262}
Machkour, M. et al. [8]	2^{256}
Huang, L. et al. [11]	2^{183}
Nkandeu, Y., P., K. et al. [21]	2^{475}
Qobbi Y et *al.*[24]	2^{128}
Bansal, R. [28]	2^{448}
Ghazvini, M. [35]	2^{224}
Jasra B et *al.*[37]	2^{512}

We notice no resemblance between the encrypted image and the original image. Therefore, an attacker cannot extract any information about the original image from the encrypted image. We also see that the decrypted images are the same as the encrypted images.

5.2 Brute Force attack

5.2.1 Keyspace analysis

Keyspace analysis tests the resistance of an encryption system against brute force attacks. To do this, the cipher must have a keyspace greater than 2^{100}. Our system has a total key space composed of four initial conditions u_0, v_0, w_0, w_1 and four control parameters μ_0, μ_1, μ_2, μ_3 (reals of 64 bits), which is $2^{8*64} = 2^{512}$. Thus, it is large enough, which makes brute force attacks impractical. Table 2 shows total key space comparison results with the current encryption algorithms. It is obvious that our key space has high precision, and it should defend the brute force attack.

5.2.2 Keyspace sensitivity

Our encryption key has high sensitivity, which means that a slight modification of a single parameter will automatically lead to a significant difference compared to the original image. Figure 5 illustrates this property, ensuring that in the absence of the correct encryption key, the original image cannot be restored. Without possession of the real secret encryption key, the attacker is unable to reconstruct the original image.

5.3 Statistical attack analysis

5.3.1 Histogram analysis

A histogram is a graphical representation of the distribution of pixels in an image. To avoid a statistical attack, the encrypted images must have a uniform histogram. Table 3 shows the histograms of the original images and their encrypted images generated by the proposed system.

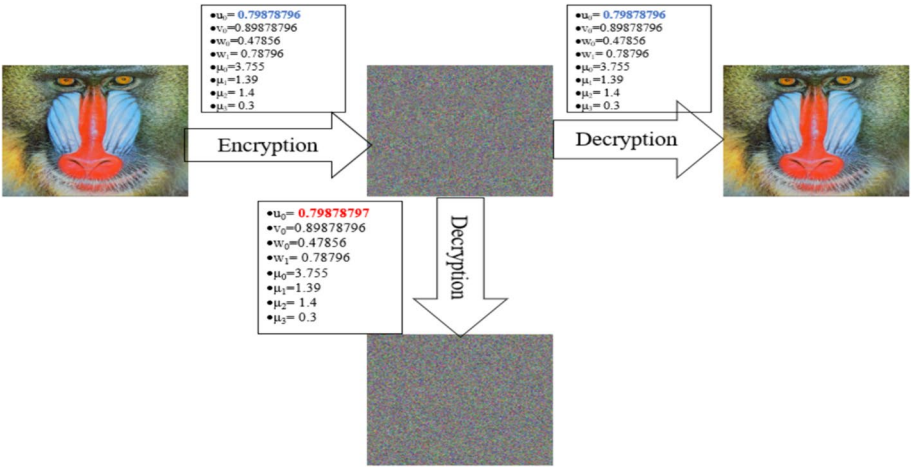


Fig. 5 Keyspace Sensitivity

The results in Table 3 illustrate that the histograms of the encrypted images are quite uniform and different from those of the original images. This shows that the encrypted image does not provide any information to use a statistical attack.

5.3.2 Correlation analysis

The correlation determines the independence of adjacent pixels. It is defined as follows:

$$C_{xy} = \frac{\sum_{i=1}^{N} \left(x_i - E(x)\right)\left(y_i - E(y)\right)}{\sqrt{\sum_{i=1}^{N} \left(x_i - E(x)\right)^2 \times \sum_{i=1}^{N} \left(y_i - E(y)\right)^2}} \tag{16}$$

where E(x) is the average of the pixel values of the image.

Table 4 illustrates the values of the vertical, horizontal and diagonal correlation of the clear and encrypted images by our system.

An encrypted image should show no correlation between adjacent pixels. Our method examined several measures of image correlation, all of which are very close to zero. This can protect our method against statistical attacks.

5.3.3 Entropy analysis

Entropy is a measure of randomness used to describe simple image texture. The entropy value is close to 8 for encrypted images. Mathematically, it is defined as:

$$H(X) = -\sum_{i=0}^{n-1} Pr(X_i) \times log_2\left(\frac{1}{Pr(X_i)}\right) \tag{17}$$

where X denotes the test image, Xi is the value of the pixel and Pr(Xi) represents the probability of Xi.

Table 3 Histograms of the original images and encrypted images

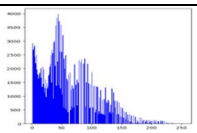
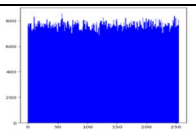
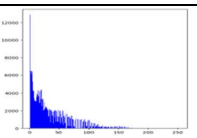
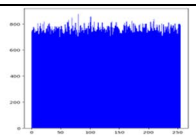
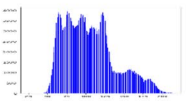
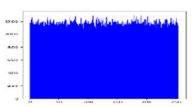
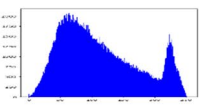
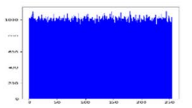
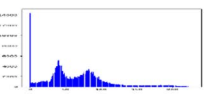
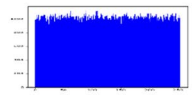
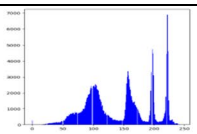
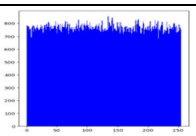
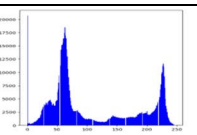
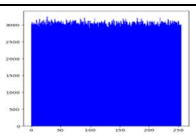
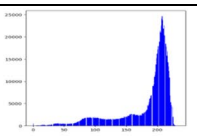
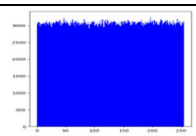
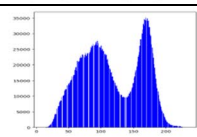
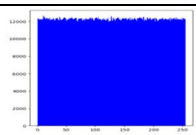
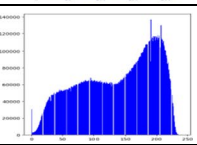
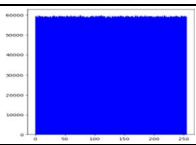
Image	Original image Histogram	Encrypted image Histogram
Female		
Couple		
Lena		
Baboon		
Peppers		
House		
Splash		
Airplane		
Stockton		
Washington		

Table 4 Correlation coefficients

Image	Original Image			Encrypted Image		
	Horizontal	Vertical	Diagonal	Horizontal	Vertical	Diagonal
Female	0.95	0.96	0.93	-0.0008	0.0007	-0.0002
Couple	0.94	0.95	0.90	0.0014	0.0015	-0.0061
Lena	0.98	0.97	0.97	-0.0002	0.0006	-0.0037
Baboon	0.86	0.92	0.85	0.0017	-0.0001	-0.0015
Peppers	0.96	0.96	0.95	0.0017	-0.0008	0.0007
House	0.94	0.97	0.92	0.0002	-0.0026	0.0009
Splash	0.98	0.98	0.96	-0.0005	0.0008	-0.0001
Airplane	0.96	0.97	0.93	0.0008	-0.0013	-0.001
Stockton	0.90	0.92	0.86	-0.0003	-0.0009	-0.0004
Washington	0.74	0.79	0.67	-0.0006	0.0003	0.0002

Table 5 Entropy analysis

Image	Entropy
Female	7.9991
Couple	7.9990
Lena	7.9993
Baboon	7.9992
Peppers	7.9994
House	7.9991
Splash	7.9997
AIRPLANE	7.9997
Stockton	7.9999
Washington	7.9999

The entropy values of the five images encrypted by our system are shown in Table 5 below.

The data in Table 5 indicate that all the entropy values of encrypted images are close to 8. Therefore, the proposed algorithm can withstand information entropy analysis attacks due to the high randomness of the l encrypted image.

5.4 Differential attack analysis

Differential attack analysis is a technique used to determine how an encrypted image changes when the original image's pixels or key value are slightly altered. Differential attacks are managed by **NPCR** (number of pixels changed Rate), **UACI** (Unified Averaged Changed Intensity) constants and **AE** (avalanche effect).

–**The NPCR** is given as follows:

$$NPCR = \frac{\sum_1^w \sum_1^h D_{ij}}{w * h} \times 100(\%) \tag{18}$$

where H and W are the height and width of the image.
D(i, j) is given as follows:

$$D_{ij} = \begin{cases} 1 si C1_{ij} \neq C2_{ij} \\ 0 sinon \end{cases}$$

–**The UACI** is given as follows:

$$UACI = \frac{1}{w \times h} \frac{\sum_{ij} \left| C1_{ij} - C2_{ij} \right|}{255} \times 100(\%) \tag{19}$$

With C1 the encrypted image of the original image and C2 the encrypted image of the modified original image.
–**The avalanche effect** corresponds to the number of bits that have been modified if a single bit of the original image is modified. The mathematical expression of this avalanche effect is given by Eq. 20.

$$\left(\frac{\sum_i bitchange}{\sum_i bittotal} \right) * 100 \tag{20}$$

To calculate the NPCR, UACI and AE values, a pixel is randomly chosen and its value is modified. Then the original image and the modified image are encrypted according to the proposed method. The NPCR, UACI and AE values obtained are presented in Table 6 below.

NPCR, UACI and avalanche effect values are higher than expected values (99.60% for NPCR, 33.40% for UACI and 50% for AE). These results demonstrate how sensitive our system is to small changes in an image; even if there is only a one-bit variation between two images, the decrypted image will be entirely different. This demonstrates that the suggested approach has good performance in defending against differential attacks.

Table 6 NPCR, UACI and avalanche effect values

Images	NPCR	UACI	AE
Female	99.75	33.44	52.1414%
Couple	99.73	33.52	52.0425%
Lena	99.73	33.45	52.0588%
Baboon	99.74	33.49	52.1196%
Peppers	99.74	33.46	52.0973%
House	99.76	33.47	52.0725%
Splash	99.73	33.48	52.1164%
AIRPLANE	99.73	33.44	52.0956%
Stockton	99.74	33.47	52.0582%
Washington	99.73	33.45	52.0890%

5.5 Peak signal-to-noise ratio (PSNR) analysis

Peak Signal-to-Noise Ratio (PSNR) is a commonly employed metric to quantify the fidelity of a reconstructed or processed image compared to its original version. In the context of image encryption, the plaintext image is considered the reference signal, while the encrypted image represents the degraded or noisy version. PSNR is typically expressed in decibels (dB) due to the logarithmic nature of the scale, allowing for a compact representation of a wide range of signal-to-noise ratios. It is mathematically given as:

$$PSNR = 20log_{10}\left(\frac{255}{\sqrt{MSE}}\right) \tag{21}$$

where MSE is given as follows:

$$MSE = \frac{1}{M \times N}\sum (IO(i,j) - IC(i,j))^2 \tag{22}$$

M×N is the image size, IO(i,j) is a pixel of the original image and IC(i,j) is a pixel of the encrypted image.

The PSNR of a good encryption algorithm should be as small as possible to ensure the high security of encryption algorithm. Table 7 lists the PSNR of ten images. It can be seen that the PSNR value of the encryption algorithm proposed in this article is small, indicating that the plain image and encrypted image are very different, so the encryption algorithm has higher security.

5.6 Encryption time and complexity

The encryption time of a crypto system is a parameter that can affect the effectiveness of an encryption algorithm. The paper simulates the proposed algorithm on an Intel Core I5 CPU 1.7 GHz and 8 GB of RAM. The encryption times of the seven simulation images are shown in the following Table 8. Using the proposed method, image encryption times change in the interval [0.05 2].

The execution time depends on the hardware used, the algorithm and the size of the image. On the other hand, the complexity depends solely on the algorithm. So, to show the

Table 7 PSNR values

Image	PSNR
Female	1.15
Couple	1.46
Lena	3.86
Baboon	4.01
Peppers	3.31
House	4.14
Splash	3.16
AIRPLANE	2.87
Stockton	2.96
Washington	3.74

Table 8 Encryption time

Images	Encryption time
Female	0.11
Couple	0.14
Lena	0.58
Baboon	0.50
Peppers	0.31
House	0.10
Splash	0.72
AIRPLANE	0.93
Stockton	1.64
Washington	1.74

effectiveness of our algorithm in terms of speed, we will calculate its complexity. Suppose the image size is 3 NM. The time consumed by the proposed algorithm can be divided into five parts. The first part concerns the generation of chaotic vectors (algorithm 1). The

Table 9 Performance comparisons with the existing approaches

Images	Methods	Entropy	NPCR	UACI	Correlation coefficients		
					Horizontal	Vertical	Diagonal
Lena	**Our method**	**7.9993**	**99.73**	**33.45**	**-0.0002**	**0.0006**	**-0.0037**
	Demirtaş, M [6]	7.9994	99.60	33.45	0.0010	-0.0014	0.0004
	Khalil, N., [7]	7.9993	99.61	33.51	0.0023	0.0011	0.0016
	Machkour, M. et al. [8]	7.9993	99.71	33.39	-0.0001	0.0011	-0.0009
	Niu, Y. et *al*.[33]	7.9976	99.61	33.51	0.0305	-0.0043	0.0042
	Belazi A et *al*.[23]	7.9991	99.62	33.67	−0.0026	-0.0175	-0.008
	Qobbi Y et *al*.[24]	7.9991	99.60	33.47	−0.0025	−0.0008	0.0029
	Jasra B et *al*.[37]	7.9924	99.61	33.78	-0.0045	0.0149	-0.0033
Baboon	**Our method**	**7.9992**	**99.74**	**33.49**	**0.0017**	**-0.0001**	**-0.0015**
	Machkour, M. et al. [8]	7.9993	99.70	33.37	0.0021	0.0019	0.0021
	Bansal, R. [28]	7.9997	99.60	33.46	0.0001	0.0102	0.0027
	Essaid, M. [29]	7.9997	99.63	33.45	0.0015	0.0061	- 0.0028
	Ghazvini, M. [35]	7.9986	99.57	33.17	-0.0023	-0.0002	-0.0008
	Belazi A et *al*.[23]	7.9988	99.61	33.64	-0.0143	-0,0151	-0.0085
	Qobbi Y et *al*.[24]	7.9997	99.61	33.43	0.0023	−0.0074	0.0154
	Jasra B et *al*.[37]	7.9998	99.61	33.76	-0.0024	0.0148	-0.0010
Pepper	**Our method**	**7.9997**	**99.73**	**33.43**	**0.0017**	**-0.0008**	**0.0007**
	Demirtaş, M [6]	7.9993	99.60	33.47	0.0012	-0.001	-0.0024
	Machkour, M. et al. [8]	7.9992	99.71	33.32	0.0017	0.0008	0.0023
	Bansal, R. [28]	7.9997	99.60	33.49	−0.00004	0.0006	0.0043
	Essaid, M. [29]	7.9998	99.63	33.42	−0.0033	0.0003	- 0.0009
	Belazi A et *al*.[23]	7.9990	99.62	33.66	-0.0263	-0.0147	-0.0065
	Qobbi Y et *al*.[24]	7.9998	99.61	33.46	0.0037	0.0004	−0.0003
	Jasra B et *al*.[37]	7.9997	99.61	33.77	-0.0012	0.0114	0.0001

complexity of the generation algorithm is O(3NM). The second part is the vectorization operation (algorithm 2) which has a complexity of order O(3NM). The time complexities of Algorithms 3 and 4 are O(3NM), respectively. The last part is the encryption process (algorithm 5). The implementation of the broadcast operation is based on the XOR operation between pixels, and the corresponding complexity is O(3NM). In general, the time complexity of the proposed algorithm is O(3NN).

5.7 Comparison

Table 9 shows the comparison of the proposed method with other recently published methods based on values of entropy, NPCR, UACI, and correlation coefficient and using three images.

It is shown in Table 9 that our technique gives satisfactory results compared to other data in the literature. The entropy of the three images gives values extremely close to the ideal value of 8 and higher than the values obtained by most other methods. For the values of the correlation coefficients according to the three directions, we realize that all the methods have values of the correlation coefficient very close to zero. For the NPCR and UACI, the values of the proposed scheme are very close to the values of NPCR (99.6%) and UACI (33.4%) expected, and they are the highest compared to the other techniques. Accordingly, from Table 8, we can conclude that the suggested method outperforms many recently published studies in terms of correlation entropy values of the NPCR and UACI.

6 Conclusion

In this article, we introduced a new method for image encryption. The method uses three chaotic maps to extract five pseudo-random vectors and two control vectors, which are used to vectorize the original image. Then it proposes two improvements, one on the classical method of Hill and the other on the classical method of Vigenère. Then it uses the combination of these two enhancements with a chaining mechanism to encrypt the images. The proposed method is found to be sensitively dependent on the single image, as shown by the key sensitivity analysis. The size of the key space is large enough to resist brute force attacks. The Histograms of encrypted images show a uniform distribution of pixels. The correlation coefficients of the encrypted images are very close to zero. An information entropy greater than 7.999 is an indication of randomness. The average NPCR (>99.6), UACI (<33.4) and AE (>40) values show that the proposed method can effectively resist differential attacks. From the security analysis, it seems that the perfect original image cannot be recovered by applying known cryptographic attacks. It is therefore secure and applicable in real-time image encryption transmission applications. In future work, we hope to generate very large S-boxes and large Hill matrices and minimize the encryption time in order to be able to encrypt images in real time.

Data Availability Authors declare that all the data being used in the design and production cum layout of the manuscript is declared in the manuscript.

Declarations

Conflicts of Interest The authors declare that they have no conflicts of interest.

References

1. Zia U, McCartney M, Scotney B, Martinez J, AbuTair M, Memon J, Sajjad A (2022) Survey on image encryption techniques using chaotic maps in spatial, transform and spatiotemporal domains. Int J Inf Secur 21:917–935. https://doi.org/10.1007/s10207-022-00588-5
2. Kumari M, Gupta S, Sardana P (2017) A Survey of Image Encryption Algorithms. 3D Res 8. https://doi.org/10.1007/s13319-017-0148-5
3. Fang P, Liu H, Wu C, Liu M (2022) A survey of image encryption algorithms based on chaotic system. Visual Comp 3. https://doi.org/10.1007/s00371-022-02459-5
4. Abdulla AA (2023) Digital image steganography: challenges, investigation, and recommendation for the future direction. Soft Comput. https://doi.org/10.1007/s00500-023-09130-8
5. Wang X, Guan N, Liu P (2022) A selective image encryption algorithm based on a chaotic model using modular sine arithmetic. Optik 258:168955. https://doi.org/10.1016/j.ijleo.2022.168955
6. Demirtaş M (2022) A new RGB color image encryption scheme based on cross-channel pixel and bit scrambling using chaos. Optik 265:169430. https://doi.org/10.1016/j.ijleo.2022.169430
7. Khalil N, Sarhan A, Alshewimy MAM (2021) An efficient color/grayscale image encryption scheme based on hybrid chaotic maps. Opt Laser Technol 143:107326. https://doi.org/10.1016/j.optlastec.2021.107326
8. Machkour M, Saaidi A, Benmaati ML (2015) A Novel Image Encryption Algorithm Based on the Two-Dimensional Logistic Map and the Latin Square Image Cipher. 3D Res 6:1–18. https://doi.org/10.1007/s13319-015-0068-1
9. Gao X (2021) Image encryption algorithm based on 2D hyperchaotic map. Opt Laser Technol 142:107252. https://doi.org/10.1016/j.optlastec.2021.107252
10. Essaid M, Akharraz I, Saaidi A, Mouhib A (2018) A new image encryption scheme based on confusion-diffusion using an enhanced skew tent map. Procedia Comput Sci 127:539–548. https://doi.org/10.1016/j.procs.2018.01.153
11. Huang L, Cai S, Xiao M, Xiong X (2018) A simple chaotic map-based image encryption system using both plaintext related permutation and diffusion. Entropy 20:1–20. https://doi.org/10.3390/e20070535
12. Sajjad T, Rashid A (2020) A new chaos-based color image encryption algorithm using permutation substitution and Boolean operation. Multimedia Tools Appl 79:19853–19873. https://doi.org/10.1007/s11042-020-08850-5
13. Patro K.A.K, Banerjee A, Acharya B (2018) A simple, secure and time efficient multi-way rotational permutation and diffusion based image encryption by using multiple 1-D chaotic maps. Springer Nature Singapore 396–418. https://doi.org/10.1007/978-981-10-8660-1_30
14. Enayatifar R, Abdullah AH, Isnin IF, Altameem A, Lee M (2017) Image encryption using a synchronous permutation-diffusion technique. Opt Lasers Eng 90:146–154. https://doi.org/10.1016/j.optlaseng.2016.10.006
15. Teng L, Wang X, Xian Y (2022) Image encryption algorithm based on a 2D-CLSS hyperchaotic map using simultaneous permutation and diffusion. Inf Sci 605:71–85. https://doi.org/10.1016/j.ins.2022.05.032
16. Çavuşoğlu Ü, Kaçar S, Pehlivan I, Zengin (2017) Secure image encryption algorithm design using a novel chaos based S-Box. Chaos, Solitons Fractals. 95:92–101. https://doi.org/10.1016/j.chaos.2016.12.018
17. Zhu S, Wang G, Zhu C (2019) A secure and fast image encryption scheme based on double chaotic s-boxes. Entropy 21:790. https://doi.org/10.3390/E21080790
18. Qobbi Y, Jarjar A, Essaid M, Benazzi A (2021) Development of Large Chaotic S-boxes for Image Encryption. Lecture Notes in Networks and Systems 211. LNNS, 847–858. https://doi.org/10.1007/978-3-030-73882-2_77
19. Zhang Y (2018) The unified image encryption algorithm based on chaos and cubic S-Box. Inf Sci 450:361–377. https://doi.org/10.1016/j.ins.2018.03.055
20. Ullah A, Jamal SS, Shah T (2017) A novel construction of substitution box using a combination of chaotic maps with improved chaotic range. Nonlinear Dyn 88:2757–2769. https://doi.org/10.1007/s11071-017-3409-1

21. Nkandeu YPK, Tiedeu A (2019) An image encryption algorithm based on substitution technique and chaos mixing. Multimedia Tools Appl 78:10013–10034. https://doi.org/10.1007/s11042-018-6612-2
22. Zahid AH, Al-Solami E, Ahmad M (2020) A Novel Modular Approach Based Substitution-Box Design for Image Encryption. IEEE Access 8:150326–150340. https://doi.org/10.1109/ACCESS.2020.3016401
23. Belazi A, Khan M, El-Latif AAA, Belghith S (2017) Efficient cryptosystem approaches: S-boxes and permutation–substitution-based encryption. Nonlinear Dyn 87:337–361. https://doi.org/10.1007/s11071-016-3046-0
24. Qobbi Y, Jarjar A, Essaid M, Benazzi A (2022) Image encryption algorithm using dynamic permutation and large chaotic S-box. Multimedia Tools Appl. https://doi.org/10.1007/s11042-022-14175-2
25. Zhang Y, Xiao D, Wen W, Nan H (2014) Cryptanalysis of image scrambling based on chaotic sequences and Vigenère cipher. Nonlinear Dyn 78:235–240. https://doi.org/10.1007/s11071-014-1435-9
26. Bhateja AK, Bhateja A, Chaudhury S, Saxena PK (2015) Cryptanalysis of Vigenere cipher using Cuckoo Search. Appl Soft Comput 26:315–324. https://doi.org/10.1016/j.asoc.2014.10.004
27. Li S, Zhao Y, Qu B, Wang J (2013) Image scrambling based on chaotic sequences and Vigenère cipher. Multimed Tools Appl 66:573–588. https://doi.org/10.1007/s11042-012-1281-z
28. Bansal R, Gupta S, Sharma G (2017) An innovative image encryption scheme based on chaotic map and Vigenère scheme. Multimedia Tools Appl 76:16529–16562. https://doi.org/10.1007/s11042-016-3926-9
29. Essaid M, Akharraz I, Saaidi A, Mouhib A (2019) Image encryption scheme based on a new secure variant of Hill cipher and 1D chaotic maps. J Inform Secur Appl 47:173–187. https://doi.org/10.1016/j.jisa.2019.05.006
30. Hraoui S, Gmira F, Abbou MF, Oulidi AJ, Jarjar A (2019) A New Cryptosystem of Color Image Using a Dynamic-Chaos Hill Cipher Algorithm. Procedia Comp Sci 148:399–408. https://doi.org/10.1016/j.procs.2019.01.048
31. Yao W, Zhang X, Zheng Z, Qiu W (2015) A color image encryption algorithm using 4-pixel Feistel structure and multiple chaotic systems. Nonlinear Dyn 81:151–168. https://doi.org/10.1007/s11071-015-1979-3
32. Hraoui S, JarJar A (2022) Single Feistel lapse acting on reduced ASCII codes followed by a genetic crossover. SN Appl Sci 4:113. https://doi.org/10.1007/s42452-022-04972-7
33. Niu Y, Zhou Z, Zhang X (2020) An image encryption approach based on chaotic maps and genetic operations. Multimedia Tools Appl. https://doi.org/10.1007/s11042-020-09237-2
34. Qobbi Y, Jarjar A, Essaid M, Benazzi A (2022) Image encryption algorithm based on genetic operations and chaotic DNA encoding. Soft Comput 26:5823–5832. https://doi.org/10.1007/s00500-021-06567-7
35. Ghazvini M, Mirzadi M, Parvar N (2020) A modified method for image encryption based on chaotic map and genetic algorithm. Multimedia Tools Appl 79:26927–26950. https://doi.org/10.1007/s11042-020-09058-3
36. Zheng J, Liu LF (2020) Novel image encryption by combining dynamic DNA sequence encryption and the improved 2D logistic sine map. IET Image Proc 14:2310–2320. https://doi.org/10.1049/iet-ipr.2019.1340
37. Bhat J, Moon AH (2022) Color image encryption and authentication using dynamic DNA encoding and Hyper Chaotic System. Expert Syst Appl 206:117861. https://doi.org/10.1016/j.eswa.2022.117861
38. Wang X, Zhao M (2021) An image encryption algorithm based on hyperchaotic system and DNA coding. Opt Laser Technol 143:107316. https://doi.org/10.1016/j.optlastec.2021.107316
39. Mondal B, Mandal T (2020) A secure image encryption scheme based on genetic operations and a new hybrid pseudo random number generator. Multimedia Tools Appl 79:17497–17520. https://doi.org/10.1007/s11042-019-08352-z
40. Kanso A (2011) Self-shrinking chaotic stream ciphers. Commun Nonlinear Sci Numer Simulat 16:822–836. https://doi.org/10.1016/j.cnsns.2010.04.039
41. Dubins LE, Freedman DA (1981) The american mathematical. Am. Math. Mon. 88:485–494
42. Qobbi Y, Abid A, Jarjar M, EL Kaddouhi S, Jarjar A, Benazzi A (2023) Adaptation of a genetic operator and a dynamic S-box for chaotic encryption of medical and color images. Scientific African 19:e01551. https://doi.org/10.1016/j.sciaf.2023.e01551
43. Qowi Z, Hudallah N (2021) Combining Cesar cipher and hill cipher in the generating encryption key on the vigenere cipher algorithm. J Phys: Conf Ser 1918:042009. https://doi.org/10.1088/1742-6596/1918/4/042009
44. Srinivasu PN, Md Norwawi N, Amiripalli SS, Deepalakshmi P (2022) secured compression for 2D medical images through the manifold and fuzzy trapezoidal correlation function. GU J Sci 35(4):1372–1391

45. Kaur M, Kumar V (2018) Fourier Mellin moment-based intertwining map for image encryption. Modern Phys Lett B. 32(9):1850115. https://doi.org/10.1142/S0217984918501154
46. Kaur M, Kumar V (2018) Parallel non-dominated sorting genetic algorithm II-based image encryption technique. Imaging Sci J 66(8):453–462. https://doi.org/10.1080/13682199.2018.1505327
47. The USC-SIPI database: http://sipi.usc.edu/database

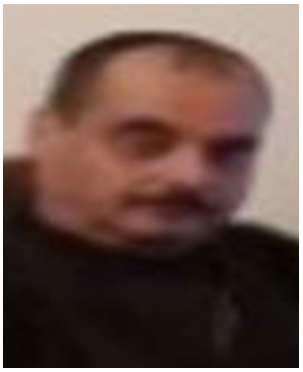
S. El Kaddouhi he received the PhD degree from SMBA-Fez University in 2017. He is currently a professor of computer science at ENS-Meknes Moulay Ismail university. His current research interests include computer vision, artificial intelligence, optimization, image encryption, face recognition, face detection.

Y. Qobbi he received the PhD degree from UMP-Oujda University in 2022. He is currently a professor of computer science. Rresearcher in computer security at MATSI laboratory of the Mohammed Premier University of Oujda, Morocco.

A. Abid Doctoral student enrolled in the MATSI laboratory at ESTO of Mohamed Premier University, Oujda, Morocco and an associate professor of computer science at the CPGE. In 2014, he obtained his computer engineering degree from ENSIAS Interested in cryptography, image processing, deep learning.

M. Jarjar PhD in Electrical Engineering from Mohamed Ben Abdellah University FST Fez. Chief Engineer in Multinational automotive wiring company. Researcher in applied mathematics in computer security.

H. Zaaraoui he received the PhD degree from SMBA-Fez University in 2021. His current research interests include computer vision, artificial intelligence, machine learning, deep learning, optimization, face recognition.



A. Jarjar high school math teacher for over 30 years. image encryption researcher. Authors of several articles. Researcher in applied mathematics in computer security.

Authors and Affiliations

S. El Kaddouhi[1] · Y. Qobbi[2] · A. Abid[2] · M. Jarjar[2] · H. Zaaraoui[3] · A. Jarjar[4]

✉ S. El Kaddouhi
s.elkaddouhi@umi.ac.ma

Y. Qobbi
qobbi.younes@ump.ac.ma

A. Abid
abdellahab90@gmail.com

M. Jarjar
jarjarmariem@gmail.com

H. Zaaraoui
hicham.zaaraoui@usmba.ac.ma

A. Jarjar
abdoujjar@gmail.com

[1] SAIP Laboratory, Ecole Normale Supérieure, Moulay Ismail University of Meknès, Meknes, Morocco

[2] MATSI Laboratory Mohamed First University Oujda, Oujda, Morocco

[3] LSI, Polydisciplinary Faculty of Taza, Sidi Mohamed Ben Abdellah University of Fès, Fès, Morocco

[4] High School Moulay Rachid Taza, Taza, Morocco