New image encryption approach using a dynamic-chaotic variant of Hill cipher in Z/4096Z

Hicham Rrghout[1], Mourad Kattass[1], Younes Qobbi[1], Naima Benazzi[2], Abdellatif JarJar[1], Abdelhamid Benazzi[1]
[1]MATSI Laboratory, High School of Technology, Mohammed First University, Oujda, Morocco
[2]LEEM Laboratory, High School of Technology, Mohammed First University, Oujda, Morocco

Article Info

Article history:

Received Mar 4, 2024
Revised May 24, 2024
Accepted Jun 4, 2024

Keywords:

Hill cipher
Chaotic map
Ring $Z/2^{12}Z$
Affine transformation
Encryption

ABSTRACT

Currently, digital communication generates a considerable amount of data from digital images. Preserving the confidentiality of these images during transmission through network channels is of crucial importance. To ensure the security of this data, this article proposes an image encryption approach based on enhancing the Hill cipher by constructing pseudo-random matrices operating in the ring $Z/2^{12}Z$ injected into a controlled affine transformation. This approach relies on the use of chaotic maps for generating matrices used in the encryption process. The use of the ring $Z/2^{12}Z$ aims to expand the key space of our cryptosystem, thus providing increased protection against brute-force attacks. Moreover, to enhance security against differential attacks, a matrix of size (4×4), not necessarily invertible, is also integrated into a diffusion phase. The effectiveness of our technique is evaluated through specific tests, such as key space analysis, histogram analysis, entropy calculation, negative pixel count rate (NPCR) and unified average changing intensity (UACI) values, correlation analysis, as well as avalanche effect assessment.

Corresponding Author:

Hicham Rrghout
MATSI Laboratory, High School of Technology, Mohammed First University
Oujda, Morocco
Email: h.rrghout@ump.ac.ma

1. INTRODUCTION

With the increasing connectivity and interoperability of devices and online platforms, data has become increasingly exposed to external threats such as hacking, data interception, and malware attacks. Therefore, it has become essential to implement robust security measures to ensure that data, including digital images, remains confidential and secure throughout its transfer over networks. To address this problem, several security measures have been established, among which cryptography [1]–[4] holds a prominent place. Image encryption finds its utility in various domains, including Internet communications, medical imaging, and military communications.

Encryption can be categorized into two main types: symmetric and asymmetric [5], [6]. In symmetric encryption, the sender and the receiver share the same key, just like in the Hill cipher and the Vigenère cipher [7], [8], while in asymmetric encryption, two distinct keys are used. The first key called the public key, is used by the sender to encrypt the message, while the second key, called the private key, is used by the receiver to decrypt the message, as in the Rivest–Shamir–Adleman (RSA) encryption [9], [10]. Recently, several techniques have shown their effectiveness in information transfer, among which are chaos-based techniques [11]–[14]. Chaos, as a complex and unpredictable phenomenon inherent in nonlinear dynamical systems, has generated increasing interest in the field of encryption.

The application of chaos in encryption provides fertile ground for exploring new secure approaches in the field of cryptography. On the other hand, several encryption techniques have been developed, among which is the Hill cipher [15], [16], which is a classical technique generally applied to text. It is based on two steps: the first is the decomposition of the plaintext into blocks of size n, where (n, n) represents the size of the fixed invertible matrix in a carefully selected ring. This matrix is considered the encryption key. Then, each block is transformed using the key matrix to obtain the encrypted image.

Although the Hill cipher offers advantages, like other classical cryptographic techniques, it has certain limitations that require special attention. Therefore, many researchers have relied on combining the Hill cipher and chaos to enhance data security. Qobbi *et al.* [17] proposed a novel method for encrypting color images. They employed an affine transformation with an invertible matrix and a dynamic translation vector to process image blocks. A substitution matrix controlled by chaotic maps was used for preliminary confusion. In their article, Jarjar *et al.* [18] proposed a new encryption system for arbitrary-sized color images. This approach enhances the classical Hill method by using a (3×3) invertible matrix in the ring Z/256Z. Simulations conducted on a wide range of images demonstrate that this approach can withstand various known attacks. Almaiah *et al.* [19] proposed a new hybrid encryption approach between the elliptic curve cryptosystem and Hill cipher (ECCHC) to convert Hill cipher from a symmetric technique to an asymmetric one, thereby enhancing its security and efficiency and resisting attacks. Santoso [20] utilized hybrid encryption by combining Hill cipher with a 3×3 matrix key and RSA cryptography with a 512-bit key. The demonstration indicates that this approach overcomes security issues during data exchange, ensuring that sent messages cannot be read by unauthorized individuals. Verma and Agarwal [21] proposed an advanced and hybrid cryptosystem in which a 62×62 table is employed instead of 26, and the Hill cipher is combined with it to bolster security.

In this article, we propose the use of an invertible matrix of dimension (4×4) operating within the ring $Z/2^{12}Z$. This combination adds extra complexity, making the task of potential attackers more challenging. This manuscript is structured as follows: section 1 provides the introduction, where we address the issue of image transfer security and various techniques to tackle this problem. In section 2, we present some previous research. Then, in the third section, we describe our proposed method. Section 4 focuses on presenting the results obtained and their comparison with previous works. Finally, we conclude our study.

2. PROPOSED METHOD

In this work, we propose a combination of chaos and the Hill cipher, where the elements of an invertible matrix of size (4×4) operate within the ring $Z/2^{12}Z$. This innovative approach aims to leverage chaotic characteristics to enhance resistance against various cryptographic attacks. The integration of chaos and the Hill cipher paves the way for significant advancements in designing robust encryption systems tailored to current information security challenges. Our study is structured as follows:

Step 1: Generation of chaotic sequences
Step 2: Preparation of the original image of size 1×3NM.

- Vectorization of the original image
- Transition from the ring $Z/2^8Z$ to the ring $Z/2^{12}Z$

Step 3: Creation of the confusion matrix
Step 4: Creation of the diffusion matrix
Step 5: Encryption process on the ring $Z/2^{12}Z$
Step 6: Transition from the ring $Z/2^{12}Z$ to $Z/2^8Z$

2.1. Generation of chaotic sequences

Based on the concept of chaos, this study employs two of the most renowned chaotic maps in the field of cryptography. These maps are selected for their effectiveness and widespread recognition. Their utilization aims to enhance the security and complexity of our cryptographic methods.

2.1.1. The sine map

In this study, we focus on the one-dimensional chaotic sine map [22]. It is a well-known chaotic map used in cryptography. The expression for this map is given by (1).

$$x_{n+1} = \mu sin(x_n) \quad (1)$$

With $\mu \in [0, 1]$ as the control parameter exhibiting chaotic behavior for $\mu \in [0.87, 1]$.

2.1.2. The PWLCM map

Piecewise linear chaotic map (PWLCM) [23] are utilized to generate pseudo-random sequences for cryptographic applications. These maps are effective in enhancing security. The mathematical definition is provided in (2).

$$\mathrm{y_n} = \mathrm{F}(\mathrm{y_{n-1}}, \mathrm{d}) = \begin{cases} \frac{y_{n-1}}{d} & ,0 \leq y_{n-1} \leq d \\ \frac{y_{n-1} - d}{0.5 - d} & , d \leq y_{n-1} \leq 0.5 \\ F\,(1 - y_{n-1}, d) & ,d \leq y_{n-1} \leq 1 \end{cases} \qquad 2)$$

The PWLCM is known to exhibit chaotic behavior when its chosen initial condition lies within the interval: y_0 ∈ [0; 1] and its parameter d ∈ [0; 0.5].

2.2. Preparing the original image of size N×M

After loading the original image of size N×M and extracting three color channels, the image undergoes the following transformations:

- The 2-dimensional array representing the image is transformed into a one-dimensional array U of size (1×3NM).
- The elements of array U are converted to the ring 2^{12}Z.

2.2.1. Generating pseudo-random vectors L and C

To introduce a pseudo-random aspect to the image preparation phase, we will use a pseudo-random vector L of size 1×3NM generated from chaotic maps using Algorithm 1:

Algorithm 1. Generation of a pseudo-random vector

```
For i=0 to 3NM-1
L[i] = int((x[i])*$10^9$)%50
```

The pseudo-random vector L will be used to generate another pseudo-random vector C in the ring Z/3Z of size 1×3NM, subdivided into blocks of three elements, with each block containing distinct values of 0, 1, and 2. The use of vector C allows for the creation of a random distribution of elements from the three vectors representing the three channels (R, G, B), as well as the creation of controlled pseudo-random sequences. This is accomplished according to Algorithm 2 as:

Algorithm 2. Pseudo-random vector C

```
For i=0 to NM-1
d=0
  For j=0 to 3NM-1
      For k=0 to 2
       If L[3i+k]==j
           C[3i+k]=d
            d=d+1
```

2.2.2. Vectorization of the original image

The three channels (R, G, B) are converted into three vectors VR, VG, and VB, each of size 1×NM. These three vectors are concatenated to generate the one-dimensional vector U of size 1×3NM, using the pseudo-random vector C. The assignment of elements to the vector U of rank i is as follows:

- If $C(i) = 0$, the element comes from vector VR
- If $C(i) = 1$, the element comes from vector VG
- If $C(i) = 2$, the element comes from vector VB

This is achieved using Algorithm 3:

Algorithm 3. Vectorization of the original image

```
For i =0 to NM-1
For k=0 to 2:
if C[3i+k]==0 then
          U[3i+k]=VR[i]
else if C[3i+k]==1 then
          U[3i+k]=VG[i]
     else:
          U[3i+k]=VB[i]
```

Figure 1 provides a detailed breakdown of the various stages of the vectorization process. This process effectively reduces the intense correlation between adjacent pixels. We can think of this first step as a moderate form of encryption of the original image. A second cycle is necessary to increase the complexity of our method, thus making differential attacks more difficult to perform.

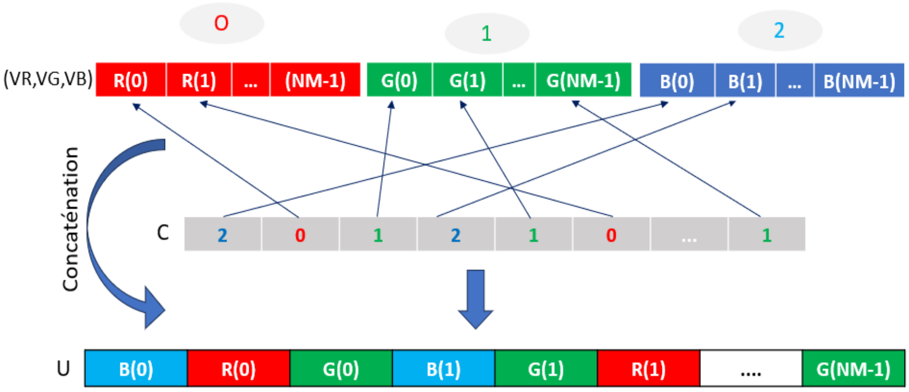


Figure 1. Pseudo-random vectorization process of the image

2.2.3. Transition from the ring $Z/2^8Z$ to the ring $Z/2^{12}Z$

The transition from the ring $Z/2^8Z$ to the ring $Z/2^{12}Z$ aims to enhance the robustness and security of the encryption process. After vectorizing the original image, all elements of U are converted into an 8-bit binary form, and after concatenating all the bits, each block of 12 bits of the resulting vector is converted into a decimal value (V_i) in the ring $Z/2^{12}Z$. Figure 2 illustrates the various steps necessary to obtain the vector V of size 1×2NM in the ring $Z/2^{12}Z$.

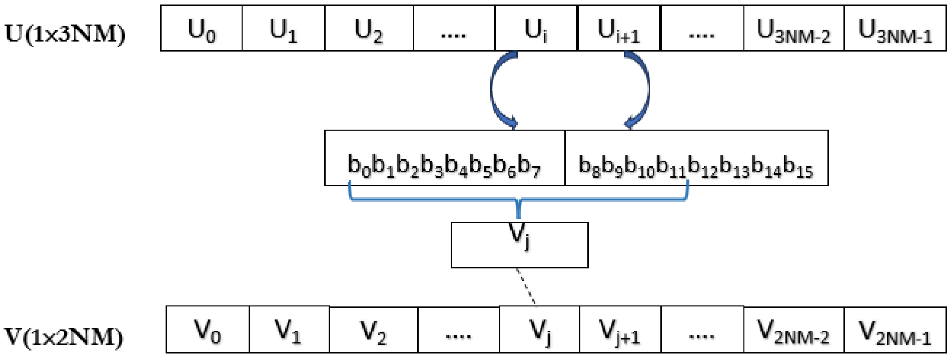


Figure 2. Adapting the image to a vector of size (1×2NM)

2.2.4. Adaptation of the vector V size

As we will be using Hill matrices of order (4×4), we divide the vector V into two sub-vectors:

- Vector W of size (1×4t), where t is the number of blocks of size 4.
- Vector Z of size (1×r), where r represents the size of the vector to be truncated.

The sizes of W and Z are determined based on the following expressions:

$$2 \times N \times M \equiv r\ [4]$$
$$0 \leq r \leq 3$$
$$t = \frac{2 \times N \times M \text{ - } r}{4}$$

With: r is the size of Z if $r \neq 0$; t is the number of blocks of size 4. This division is illustrated by Algorithm 4:

Algorithm 4. Adjustment of the image size

```
//Construction de W
For i=0 to 4t-1
W(i)=V(i)
                 Next i
//Construction de Z
For i=4t to 2×N×M-1
Z(i)=V(i)
Next i
```

This adaptation is illustrated by Figure 3.

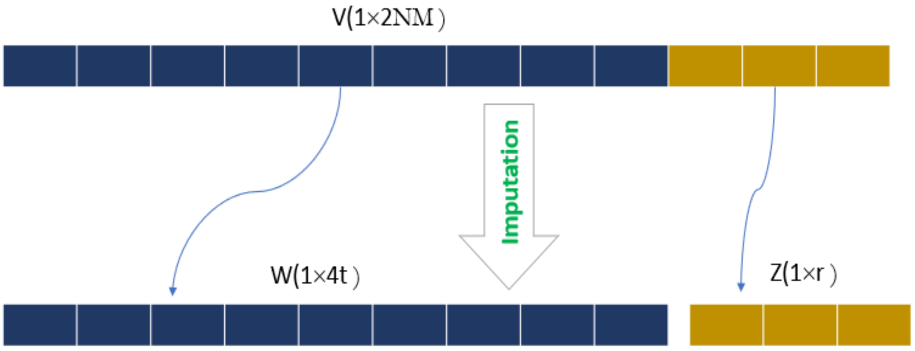


Figure 3. Adaptation of the image vector dimension

2.3. Improvement of Hill cipher

Hill cipher is an encryption technique that relies on matrix manipulation and matrix calculations to encrypt data. In our system, we have incorporated two matrices:

- The first matrix CH_1, is of size 4×4, which is invertible and used for the confusion process.
- The second matrix CH_2, also of size 4×4, which is not necessarily invertible and used for diffusion.

To overcome the linearity issue associated with Hill cipher, we incorporate two pseudo-random vectors, denoted by K and T, of size 1×2NM, defined by Algorithm 5 as follows:

Algorithm 5. Generation of two chaotic vectors

```
For i =0 to 2NM-1
  $K[i]=int((max(x[i],y[i])*10^9))\%2^{12}$
  $T[i]=int((min(x[i],y[i])*10^9))\%2^{12}$
```

2.3.1. Construction of the confusion matrix

In our approach, the improvement of the Hill cipher involves generating an invertible matrix of order (4×4) by using the product of two matrices A and B, one upper triangular and the other lower triangular, where all elements of these matrices are of pseudo-random nature, injected into the ring $Z/2^{12}Z$.

$$A = \begin{pmatrix} a1 & a2 & a3 & a4 \\ 0 & a5 & a6 & a7 \\ 0 & 0 & a8 & a9 \\ 0 & 0 & 0 & a10 \end{pmatrix} \quad \text{and} \quad B = \begin{pmatrix} b1 & 0 & 0 & 0 \\ b2 & b5 & 0 & 0 \\ b3 & b6 & b8 & 0 \\ b4 & b7 & b9 & b10 \end{pmatrix}$$

The two matrices A and B are invertible if and only if all diagonal elements of A and B are odd. Then, the inverse of CH_1 is denoted by CH_1^{-1} and is obtained by calculating the product of the inverses of B and A.

- $CH_1 = A * B$
- $\mathrm{CH}_1^{-1} = B^{-1} * A^{-1}$

2.3.2. Construction of the diffusion matrix

To enhance security against brute force attacks and implement the diffusion process, we use a matrix CH2 of order (4×4). This matrix is not necessarily invertible and its elements belong to the ring $Z/2^{12}Z$. The components of CH2 are derived from chaotic maps, utilizing Algorithm 6 as follows:

Algorithm 6. The elements of matrix CH_2

```
For K=0 to 3:
   For j=0 to 3:
       $CH_2$[k,j]=K[2*N+3*k+j]
```

2.4. Encryption process of vector W over the ring $Z/2^{12}Z$

2.4.1. Installing the diffusion phase

To set up this phase, an initialization vector IS of size (1×4) is introduced. The element of vector IS are obtained through Algorithm 7. In this context, t represents the number of blocks of size 4 in vector W.

Algorithm 7. Initialization vector generation

```
IS[0]=0
For i=1 to 4t-1
     IS[0]=IS[0] ⊕ W[i]
Next i
IS[1]=IS[0] ⊕ W[1]
IS[2]=IS[0] ⊕ W[2]
IS[3]=IS[0] ⊕ W[3]
```

2.4.2. Modification of the first block V_0

The elements of the initialization vector are used to initiate a diffusion step. This step is essential for enhancing security. The operation is executed using the subsequent expressions.

$$W[0]=W[0]\oplus IS[0]$$
$$W[1]=W[1]\oplus IS[1]$$
$$W[2]=W[2]\oplus IS[2]$$
$$W[3]=W[3]\oplus IS[3]$$

2.4.3. Confusion phase

Confusion is the initial step of our encryption system. In this step, we use the matrix CH_1 in a specified affine transformation. Vector Y represents the encrypted image.

$$\begin{pmatrix} Y[4i] \\ Y[4i+1] \\ Y[4i+2] \\ Y[4i+3] \end{pmatrix} = CH_1 \times \begin{pmatrix} W[4i] \\ W[4i+1] \\ W[4i+2] \\ W[4i+3] \end{pmatrix} (\text{mod } 2^{12}) \oplus \begin{pmatrix} K[4i] \\ K[4i+1] \\ K[4i+2] \\ K[4i+3] \end{pmatrix}$$

2.4.4. Diffusion phase

To bolster security against potential differential attacks, we adopt cipher block chaining (CBC) mode. This mode enhances encryption by incorporating the previous ciphertext block into the encryption of the current block. Its implementation helps fortify our encryption method.

$$\begin{pmatrix} W[4(i+1)] \\ W[4(i+1)+1] \\ W[4(i+1)+2] \\ W[4(i+1)+3] \end{pmatrix} = CH_2 \times \begin{pmatrix} Y[4i] \\ Y[4i+1] \\ Y[4i+2] \\ Y[4i+3] \end{pmatrix} (\text{mod } 2^{12}) \oplus \begin{pmatrix} T[4i] \\ T[4i+1] \\ T[4i+2] \\ T[4i+3] \end{pmatrix}$$

2.5. Encryption process of vector Z over the ring $Z/2^{12}Z$

Let X(1×r) be the encrypted vector of vector Z(1×r). The encryption process of Z varies depending on the value of r, allowing the determination of the elements of Z to be encrypted as:

If r = 1	If r = 2	If r = 3
$X[0]=Z[0]\oplus K[N]$	$X[0] = Z[1] \oplus K[N]$	$X[0] = Z[0] \oplus K[N]$
	$X[1] = Z[2] \oplus K[N + 1]$	$X[1] = Z[1] \oplus K[N + 1]$
		$X[2] = Z[2] \oplus K[N + 2]$

Let Y_c be the final output vector of size (1×2NM) representing the encrypted image, obtained by concatenating vector Y with vector X, according to Algorithm 8. Figure 4 provides a detailed illustration of the proposed encryption process.

Algorithm 8. Encrypted image

```
For i=0 to 4t-1
Yc[i]=Y[i]
Next i
For i= 0 to r-1
Yc[i+4t]=X[i]
Next i
```

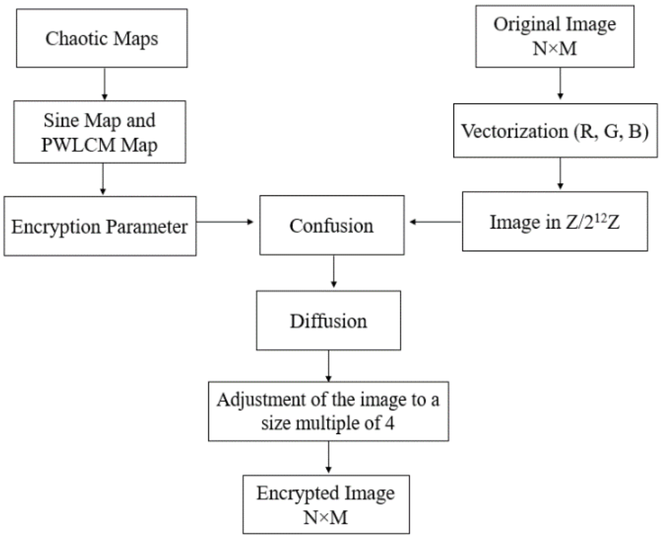


Figure 4. Encryption process

2.6. Decryption

The decryption process is the reverse operation of the initial mechanism, using the same encryption keys. Our method relies on a symmetric encryption system with diffusion implementation. This process is carried out by following the steps below:

Axis 1: Transformation of the encrypted image into a one-dimensional array.
Axis 2: Convert each 12-bit block into a decimal value.
Axis 3: Generation of chaotic sequences.
Axis 4: Creation of the invertible matrix CH^{-1} using the following mathematical form: $CH_1^{-1} = B^{-1}*A^{-1}$
Axis 5: Adaptation of the encrypted image vector.

The vector Y_c of the encrypted image is subdivided into two sub-vectors: i) The vector Y of size (1×4t), where t represents the number of blocks of size 4; ii) The vector X of size (1×r), where r represents the size of vector X to be truncated, with $1 < r \leq 3$.

Axis 6: Decryption of vector $X(1\times r)$.

Let Z of size (1×r) be the decrypted vector of vector X of size (1×r). The decryption process of vector X is determined by the following expression, which varies according to the value of r, thereby deducing the elements of X to decrypt:

$$\begin{array}{lll} \text{If } r = 1 & \text{If } r = 2 & \text{If } r = 3 \\ Z[0] = X[0] \oplus K[N] & Z[0] = X[0] \oplus K[N] & Z[0] = X[0] \oplus K[N] \\ & Z[1] = X[1] \oplus K[N+1] & Z[1] = X[1] \oplus K[N+1] \\ & & Z[2] = X[2] \oplus K[N+2] \end{array}$$

Axis 7: Inverse confusion phase and inverse diffusion of vector Y(1×4t).

Let Y_i represents the encrypted block i of the image and W_i represent the decrypted block i of the image, we have:

$$Y_i = CH_1(W_i) \oplus K(i) \text{ and } W_i = W_i \oplus\left(CH_2(Y_{i-1}) \oplus T(i-1)\right)$$
$$\text{So } Y_i = CH_1\left(W_i \oplus\left(CH_2(Y_{i-1}) \oplus T(i-1)\right)\right) \oplus K(i)$$
$$W_i = CH_1^{-1}[Y_i \oplus K(i)] \oplus[CH_2(Y_{i-1}) \oplus T(i-1)]$$

The vector V of size (1×3NM) representing the original image is obtained by concatenating the vector W with the vector Z, as described in Algorithm 9. The various encryption steps are illustrated in Figure 5.

Algorithm 9. Original image

```
For i=0 to 4t-1
V[i]=W(i)
Next i
For i=0 to r-1
V[i+4t]=Z(i)
Next i
```

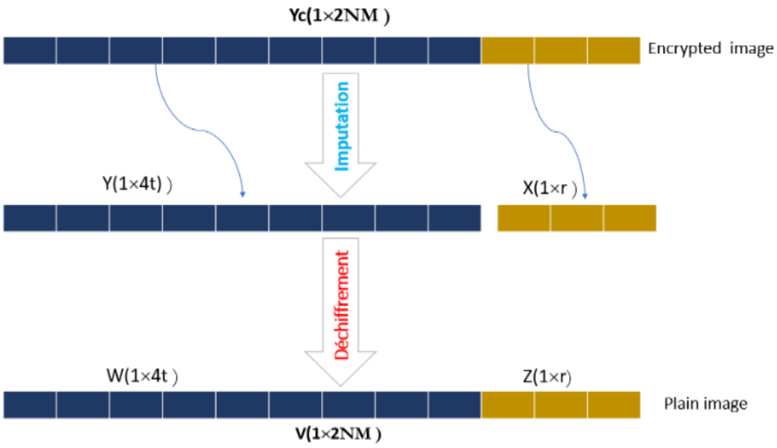


Figure 5. Decryption process

3. RESULTS AND DISCUSSION

To assess the security of a cryptosystem, it must undergo various efficiency tests against all known attacks, including exhaustive, statistical, and differential attacks. Our approach is thus tested on a diverse set of color and medical images using Python on a Windows 10 operating system. The hardware setup includes an Intel(R) Core (TM) i5-6300U CPU @ 2.40 GHz processor with a speed of 2.50 GHz and 8 GB of RAM.

3.1. Visual testing

The encryption scheme we proposed was evaluated using various standard images commonly used for image processing tests. We particularly highlighted the results obtained for three specific images: Baboon (512×512), House (256×256) and Peppers (512×512). Figure 6 presents the original images along with their encrypted versions. The results confirm that the encrypted image contains no information from the original image.

3.2. Analysis of brute force attacks

3.2.1. Key space

For a robust encryption algorithm, it is crucial that the key space is extensive, ideally surpassing 2^{100}. In our algorithm, we leverage two chaotic maps derived from four real parameters, with each parameter encoded in 32 bits. This configuration results in an overall key space of 2^{128}, significantly exceeding the desired threshold of 2^{100}.

3.2.2. Number of possible matrices

The elements a2, a3, a4, a6, a7, and a9 of matrix A can take values from 0 to 4095, thus offering 4096 possibilities for each element. Therefore, the total number of possibilities to choose the values of a2, a3, a4, a6, a7, and a9 is $(4096)^6 = (2^{12})^6=2^{72}$. By imposing the condition that the diagonal elements must be odd, each element of a1, a5, a8, and a10 has 2^{11} possibilities, or $(2^{11})^4 =2^{44}$. Thus, the total number of choices for the elements of A is $2^{72}\times2^{44}=2^{116}$. Similarly, for B, we get 2^{116} possibilities. Therefore, the number of possibilities for matrix CH_1 is $(2^{116})^2=2^{232}$. On the other hand, each element of matrix CH_2 can take 2^{12} values. Thus, the total number of possibilities to choose matrix CH_2 is $(2^{12})^{16}=2^{192}$. Consequently, the total number of possible matrices is $2^{232}\times2^{192}=2^{424}$, which is significantly very large. It is deduced that our approach is immune to brute force attacks.

3.2.3. Key sensitivity

Our system utilizes two well-established chaotic maps commonly used in cryptography due to their exceptional sensitivity to initial conditions. This sensitivity guarantees a high degree of responsiveness to our encryption key. This is demonstrated in Figure 7.

This ensures that the original image cannot be recovered without knowing the genuine encryption secret key. In other words, the security of the encryption process relies on the confidentiality of this key. Without it, retrieving the original image from the encrypted one is impossible.

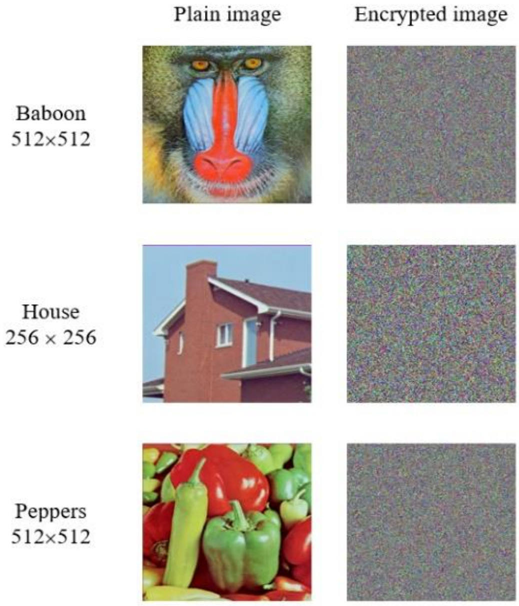
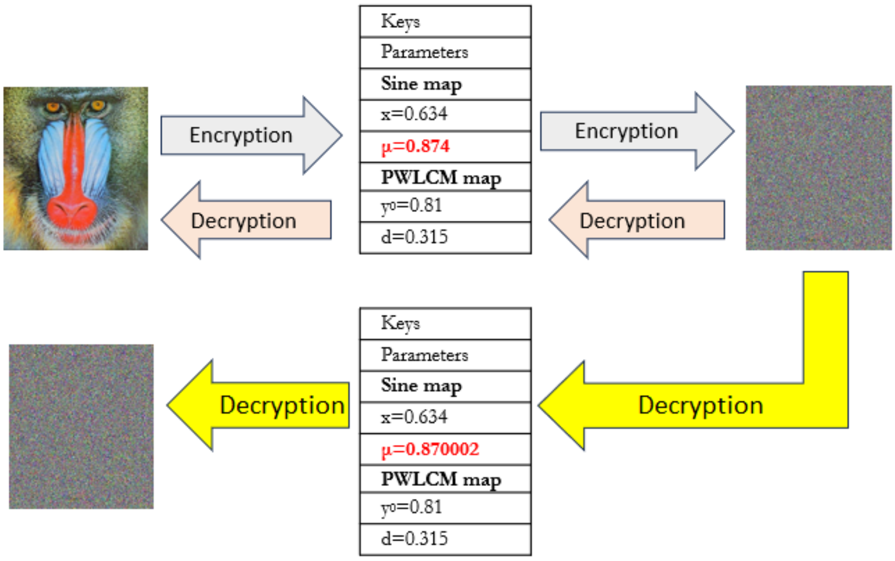


Figure 6. Visual test of selected images



Keys
Parameters
Sine map
x=0.634
μ=0.874
PWLCM map
y0=0.81
d=0.315

Keys
Parameters
Sine map
x=0.634
μ=0.870002
PWLCM map
y0=0.81
d=0.315

Figure 7. Key sensitivity

3.3. Robustness to statistical attacks

3.3.1. Correlation analysis

The encryption operation aims to reduce the correlation between adjacent pixels to almost zero in order to counter statistical attacks. The correlation coefficient [24] is calculated using (3), (4), and (5).

$$\mathrm{corr}_{x\,y} = \frac{\mathrm{cov}(x,y)}{\sqrt{D(x)\ x\ D(y)}} \quad (3)$$

$$\mathrm{corr}_{x\,y} = \frac{\mathrm{cov}(x,y)}{\sqrt{D(x)\ x\ D(y)}} \quad (4)$$

$$D(x) = \frac{1}{N}\sum_{1}^{N}(x_i - E(x))^2 \ and \ D(y) = \frac{1}{N}\sum_{1}^{N}(y_i - E(y))^2 \quad (5)$$

where x and y represent the color component values of adjacent pixels in the image, N is the total number of selected adjacent pixels in the image, and r_{xy} is the correlation coefficient. The correlation coefficient is presented in Table 1. Our method has demonstrated that all evaluated image metrics exhibited values extremely close to zero. This confirms the robustness of our algorithm against any statistical attack.

Table 1. Correlation coefficients

Images		V			H			D	
	R	G	B	R	G	B	R	G	B
Baboon	0.0020	0.0013	0.0017	-0.0038	0.0010	-0.0019	0.0022	-0.0020	0.0009
House	0.0044	0.0070	0.0059	-0.0024	0.0015	-0.0051	0.0043	-0.0036	-0.0006
Peppers	-0.00005	0.0003	-0.0033	0.0024	-0.0012	-0.0036	-0.0015	-0.0003	-0.0047

3.3.2. Histogram analysis

Ideally, a robust encryption algorithm [24] should distribute values in a random or pseudo-random manner. Figure 8 provides an illustration of the histograms of the encrypted image. The histogram outcomes of images encrypted by our algorithm reveals a uniform distribution.

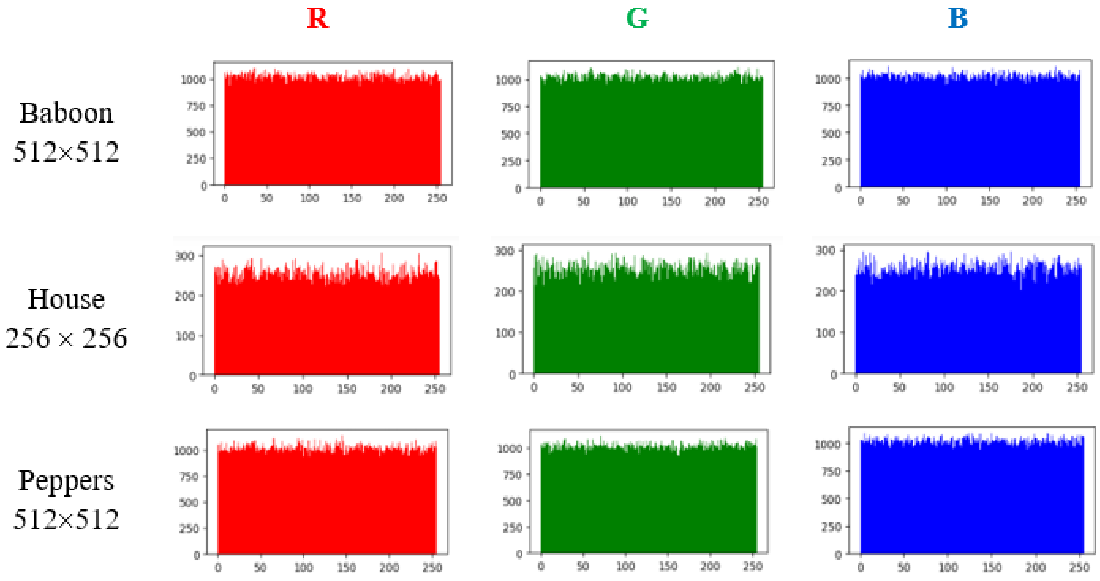


Figure 8. Histograms of encrypted images

3.3.3. Entropy analysis

Entropy measures the amount of random information present in the encryption. It is expressed [25] by (6):

$$H(m) = -\sum_{i=0}^{255} p(m_i)\, log_2\, (p(m_i)) \quad (6)$$

The theoretical entropy is equal to 8. Table 2 illustrates the entropy values of the three images encrypted by our system. Each of the images evaluated by our method exhibits entropy close to 8. This ensures the resilience of our system against entropy-based attacks.

Table 2. Entropy analysis

Image	Entropy	
	Original image	Encrypted image
Baboon	7.6444	7.9993
House	7.2718	7.9969
Peppers	7.2978	7.9993

3.4. Differential attacks

3.4.1. NPCR and UACI

The negative pixel count rate (NPCR) and the unified average changing intensity (UACI) [26] are commonly used measures in the field of steganography and cryptography to assess the sensitivity to changes in pixels in encrypted images. These two parameters are calculated as (7)-(9):

$$\mathrm{NPCR} = (\frac{1}{\mathrm{NM}} \sum_{\mathrm{i,j=1}}^{\mathrm{NM}} \mathrm{D(i,j)} * 100 \tag{7}$$

$$\mathrm{D(i,j)} = \begin{cases} 1 \text{if } \mathrm{C_1\ (i,j)} \neq \mathrm{C_2\ (i,j)} \\ 0 \text{ if } \mathrm{C_1\ (i,j)} = \mathrm{C_2\ (i,j)} \end{cases} \tag{8}$$

$$\mathrm{UACI} = (\frac{1}{\mathrm{NM}} \sum_{\mathrm{i,j=1}}^{\mathrm{NM}} \frac{\mathrm{ABS((C_1\ (i,j) - C_2\ (i,j))}}{255} * 100 \tag{9}$$

Table 3 provides the NPCR and UACI values for several pairs of slightly different values. The NPCR and UACI values obtained with our proposed scheme are remarkably close to the expected values, set at 99.6% and 33.4%, respectively. This suggests that our algorithm is highly resistant to any form of differential attack.

Table 3. NPCR and UACI values

Images	NPCR (%)	UACI (%)
Baboon	99.7381	33.4895
House	99.8672	33.8410
Peppers	99.6136	33.5024

3.4.2. Avalanche effect

The avalanche effect, the study [27] is a property whereby a small, minimal variation in input data should result in substantial differences in the encrypted results. The avalanche effect (AE) is calculated by expression (10):

$$\mathrm{AE} = \frac{\text{Number of changed bits}}{\text{Total number of bits in encrypted image}} \tag{10}$$

Table 4 illustrates the avalanche effect values.

Table 4. Avalanche analysis

Images	Avalanche effect (%)
Baboon	52.0683
House	53.3358
Peppers	50.0215

All the obtained values exceed 50%. This observation ensures that a change of a single bit in the clear image results in significant modifications of the bits in the encrypted image. Thus, our system is robust against any known attack.

3.5. Comparison

In Table 5, we will conduct a thorough performance analysis, comparing our technique to various other approaches. The comparison will primarily emphasize entropy, NPCR, UACI, and correlation coefficient values. This detailed review aims to offer a comprehensive understanding of the encryption strengths and capabilities of our technique.

Table 5. Comparison with other approaches

Parameter	Image	Our approach	Ref [28]	Ref [29]	Ref [30]	Ref [31]
Entropy	Baboon (512×512)	7.9993	7.9987	7.9998	7.9997	7.9998
	House (256×256)	7.9969	--	--	7.9992	--
	Peppers (512×512)	7.9993	7.9992	7.9998	7.9998	7.9997
NPCR	Baboon (512×512)	99.7381	99.63	99.654	99.6372	99.61
	House (256×256)	99.8672	--	--	99.6196	--
	Peppers (512×512)	99.6136	99.60	99.745	99.6316	99.62
UACI	Baboon (512×512)	33.4895	33.40	33.454	33.4542	33.45
	House (256×256)	33.8410	--	--	33.5703	--
	Peppers (512×512)	33.5024	33.17	33.784	33.4214	33.43
Vertical correlation	Baboon (512×512)	0,0017	--	0.0031	0.0061	−0.0012
	House (256×256)	0,0058	--	--	−0.0057	--
	Peppers (512×512)	-0,0010	-0.0002	-0.0012	0.0003	--

By closely examining the results obtained from various metrics and comparing our method to other encryption techniques, we were able to identify the strengths of our approach and its ability to meet security requirements. Our study demonstrates that our method provides a reliable and effective solution for image encryption, thus offering adequate protection against potential threats.

4. CONCLUSION

In this study, we presented an encryption system that combines a chaotic system with the Hill cipher. To achieve this, we used a reversible matrix of dimension (4×4) within the ring $Z/2^{12}Z$ for the confusion process, while a non-invertible matrix of the same dimension was used in an affine transformation for the diffusion process. The results of our security analysis confirm the strength and reliability of our method against exhaustive, statistical, and differential attacks. In summary, our work represents a significant advancement in the search for robust solutions to secure data in the field of modern cryptography. In our future research, our goal is to evaluate the impact of using larger Hill matrices on the performance and security of our image encryption system. These future research endeavors aim to further enhance the robustness and effectiveness of our encryption approach.

REFERENCES

[1] W. Alexan, M. Elkandoz, M. Mashaly, E. Azab, and A. Aboshousha, “Color image encryption through chaos and KAA map,” *IEEE Access*, vol. 11, pp. 11541–11554, 2023, doi: 10.1109/ACCESS.2023.3242311.

[2] X. Chai, J. Fu, Z. Gan, Y. Lu, and Y. Zhang, “An image encryption scheme based on multi-objective optimization and block compressed sensing,” *Nonlinear Dynamics*, vol. 108, no. 3, pp. 2671–2704, Mar. 2022, doi: 10.1007/s11071-022-07328-3.

[3] L. Teng, X. Wang, and Y. Xian, “Image encryption algorithm based on a 2D-CLSS hyperchaotic map using simultaneous permutation and diffusion,” *Information Sciences*, vol. 605, pp. 71–85, Aug. 2022, doi: 10.1016/j.ins.2022.05.032.

[4] H. Rrghout, M. Kattass, Y. Qobbi, N. Benazzi, A. Jarjar, and A. Benazzi, “Robust image encryption algorithm using a new variant of Hill cipher,” in *ACM International Conference Proceeding Series*, May 2023, pp. 1–6, doi: 10.1145/3607720.3607750.

[5] V. N. Jaya Shruthy and V. Maheswari, “A hybrid combination of symmetric and asymmetric encryption technique with graph labeling,” in *AIP Conference Proceedings*, 2022, vol. 2516, doi: 10.1063/5.0108506.

[6] J. G. Sekar, E. Periyathambi, and A. Chokkalingam, “Hybrid chaos-based image encryption algorithm using Chebyshev chaotic map with deoxyribonucleic acid sequence and its performance evaluation,” *International Journal of Electrical and Computer Engineering*, vol. 13, no. 6, pp. 6952–6963, Dec. 2023, doi: 10.11591/ijece.v13i6.pp6952-6963.

[7] U. I. Erondu, E. O. Asani, M. O. Arowolo, A. K. Tyagi, and N. Adebayo, “An encryption and decryption model for data security using vigenere with advanced encryption standard,” in *Using Multimedia Systems, Tools, and Technologies for Smart Healthcare Services*, IGI Global, 2022, pp. 141–159.

[8] A. K. Jaithunbi, S. Sabena, and L. Sairamesh, “Preservation of data integrity in public cloud using enhanced vigenere cipher based obfuscation,” *Wireless Personal Communications*, vol. 129, no. 1, pp. 271–284, Oct. 2023, doi: 10.1007/s11277-022-10097-2.

[9] A. Gadad and D. Anbusezhiyan, “Cloud security: literature survey,” *International Journal of Electrical and Computer Engineering*, vol. 13, no. 4, pp. 4734–4742, Aug. 2023, doi: 10.11591/ijece.v13i4.pp4734-4742.

[10] J. K. M. S. U. Zaman and S. A. Laskar, “RSA cryptosystem: block cipher or stream cipher,” *2023 4th International Conference on Computing and Communication Systems (I3CS)*, Shillong, India, 2023, pp. 1-7, doi: 10.1109/I3CS58314.2023.10127232.

[11] V. Rudnytskyi, O. Korchenko, N. Lada, R. Ziubina, L. Wieclaw, and L. Hamera, “Cryptographic encoding in modern symmetric and asymmetric encryption,” *Procedia Computer Science*, vol. 207, pp. 54–63, 2022, doi: 10.1016/j.procs.2022.09.037.

[12] H. Rrghout *et al.*, “Combination of an improved feistel scheme and genetic operators for chaotic image encryption,” in *Studies in Computational Intelligence*, vol. 1145, Springer Nature Switzerland, 2024, pp. 79–91.

[13] Q. Lai, H. Zhang, P. D. K. Kuate, G. Xu, and X. W. Zhao, “Analysis and implementation of no-equilibrium chaotic system with application in image encryption,” *Applied Intelligence*, vol. 52, no. 10, pp. 11448–11471, Aug. 2022, doi: 10.1007/s10489-021-03071-1.

[14] M. Kattass, H. Rrghout, A. Jarjar, A. Abid, M. Jarjar, and A. Benazzi, “An efficient image encryption algorithm using chaotic S-boxes of pseudo-random size,” *in Proceedings of the 6th International Conference on Networking, Intelligent Systems & Security (NISS '23)*. Association for Computing Machinery, New York, NY, USA, Art. no. 32, pp. 1–6, doi: 10.1145/3607720.3607754.

[15] L. S. Mezher and A. M. Abbass, “Mixed Hill cipher methods with triple pass protocol methods,” *International Journal of*

Electrical and Computer Engineering, vol. 11, no. 5, pp. 4449–4457, Oct. 2021, doi: 10.11591/ijece.v11i5.pp4449-4457.

[16] D. E. Mfungo, X. Fu, X. Wang, and Y. Xian, “Enhancing image encryption with the kronecker xor product, the Hill cipher, and the sigmoid logistic map,” *Applied Sciences*, vol. 13, no. 6, p. 4034. 2023, doi: 10.3390/app13064034.

[17] Y. Qobbi, A. Jarjar, M. Essaid, and A. Benazzi, “New image encryption scheme based on dynamic substitution and Hill cipher,” in *Lecture Notes in Electrical Engineering*, vol. 745, Springer Singapore, 2022, pp. 797–808.

[18] M. Jarjar, S. Najah, K. Zenkouar, and S. Hraoui, “Further improvement of the HILL method applied in image encryption,” in *2020 1st International Conference on Innovative Research in Applied Science, Engineering and Technology*, Apr. 2020, pp. 1–6, doi: 10.1109/IRASET48871.2020.9092046.

[19] M. A. Almaiah, Z. Dawahdeh, O. Almomani, A. Alsaaidah, Ahmad Al-Khasawneh, and S. Khawatreh, “A new hybrid text encryption approach over mobile ad hoc network,” *International Journal of Electrical and Computer Engineering*, vol. 10, no. 6, pp. 6461–6471, Dec. 2020, doi: 10.11591/IJECE.V10I6.PP6461-6471.

[20] Y. S. Santoso, “Message security using a combination of Hill cipher and RSA algorithms,” *Jurnal Matematika Dan Ilmu Pengetahuan Alam LLDikti Wilayah 1 (JUMPA)*, vol. 1, no. 1, pp. 20–28, Mar. 2021, doi: 10.54076/jumpa.v1i1.38.

[21] N. Verma and R. Agarwal, “A hybrid cryptosystem of vigenère and Hill cipher using enhanced vigenère table,” in *Cognitive Science and Technology*, Springer Nature Singapore, 2023, pp. 509–520.

[22] S. Shao, J. Li, P. Shao, and G. Xu, “Chaotic image encryption using piecewise-logistic-sine map,” *IEEE Access*, vol. 11, pp. 27477–27488, 2023, doi: 10.1109/ACCESS.2023.3257349.

[23] N. R. Manihira and A. K. Dauda,“Image encryption using chaotic maps and DNA encoding,” *Journal of Xidian University*, vol. 14, no. 4, Apr. 2020, doi: 10.37896/jxu14.4/206.

[24] A. Kumar, P. Singh, K. A. K. Patro, and B. Acharya, “High-throughput and area-efficient architectures for image encryption using PRINCE cipher,” *Integration*, vol. 90, pp. 224–235, May 2023, doi: 10.1016/j.vlsi.2023.01.011.

[25] M. Hasan, “Image encryption based on multiplicative ciphers,” *Journal of Humanitarian and Applied Sciences*, vol. 7, no. 14, pp. 288–297, 2022.

[26] K. A. Santoso, S. Hidayatulloh, and A. Kamsyakawuni, “Image security system using Playfair cipher and modification of electronic code book (ECB) algorithm,” *REFILKOM: Journal of Technology and Information Systems*, vol. 1, no. 1, pp. 12–20, 2023.

[27] Y. Alemami, M. A. Mohamed, and S. Atiewi, “Advanced approach for encryption using advanced encryption standard with chaotic map,” *International Journal of Electrical and Computer Engineering*, vol. 13, no. 2, pp. 1708–1723, Apr. 2023, doi: 10.11591/ijece.v13i2.pp1708-1723.

[28] M. Ghazvini, M. Mirzadi, and N. Parvar, “A modified method for image encryption based on chaotic map and genetic algorithm,” *Multimedia Tools and Applications*, vol. 79, no. 37–38, pp. 26927–26950, Jun. 2020, doi: 10.1007/s11042-020-09058-3.

[29] Y. Qobbi, A. Jarjar, M. Essaid, and A. Benazzi, “Image encryption algorithm based on genetic operations and chaotic DNA encoding,” *Soft Computing*, vol. 26, no. 12, pp. 5823–5832, Jun. 2022, doi: 10.1007/s00500-021-06567-7.

[30] M. Essaid, I. Akharraz, A. Saaidi, and et A. Mouhib, “Image encryption scheme based on a new secure variant of Hill cipher and 1D chaotic maps,” *Journal of Information Security and Applications*, vol. 47, pp. 173–187, Aug. 2019, doi: 10.1016/j.jisa.2019.05.006.

[31] Y. Qobbi, A. Abid, M. Jarjar, S. El Kaddouhi, A. Jarjar, and A. Benazzi, “Adaptation of a genetic operator and a dynamic S-box for chaotic encryption of medical and color images,” *Scientific African*, vol. 19, Mar. 2023, doi: 10.1016/j.sciaf.2023.e01551.

BIOGRAPHIES OF AUTHORS

Hicham Rrghout received a master's degree in electronics and telecommunications from Abdelmalek Essaadi University, Morocco in 2012. Currently, a Ph.D. student registered in the MATSI laboratory at ESTO of Mohamed University, Oujda, Morocco, and a professor of computer science in the qualifying secondary cycle. Interested in cryptography and image processing. He can be contacted at email: h.rrghout@ump.ac.ma.

Mourad Kattass received a master's degree in embedded systems and robotics from the Faculty of Science and Technology at Abdelmalek Essaadi University, Morocco, in 2020, and a bachelor’s degree in computer science, electronics, electrotechnics, and automation from the Faculty of Science at Sidi Mohammed Ben Abdellah University, Morocco, in 2006, respectively. Currently, he is pursuing a Ph.D. in mathematics and computer science at Mohammed First University, Oujda, Morocco. His research interests include computer science. He can be contacted at email: mourad.kattass@ump.ac.ma.

Younes Qobbi received the Ph.D. degree from UMP-Oujda University in 2022. He is currently a professor of computer science. Researcher in computer security at MATSI laboratory of the Mohammed Premier University of Oujda, Morocco. He can be contacted at email: qobbi.younes@ump.ac.ma.

Naima Benazzi member of the Laboratory of Electrical Engineering and Maintenance (LEEM) and serves as a professor and researcher at Mohammed First University in Oujda, Morocco. Passionate about new technologies and innovation, she is always open to new opportunities in her field. She can be contacted via email: benazzin@gmail.com.

Abdellatif Jarjar received the master’s degree in fundamental mathematics from Franche Compté Besonçon University, French, in 1987 and Laureate in mathematics from High Normal School, Morocco, in 1988, respectively. Currently, Searcher in mathematics and computer science in Mohammed First University, Oujda, Morocco. His research interests include computer science. He can be contacted at email: abdoujjar@gmail.com.

Abdelhamid Benazzi received a master's degree in fundamental mathematics from Franche Compté Besonçon University, France, in 1987. Professor of mathematics and searcher in computer science from Mohammed First University, Oujda, Morocco. His research interests include computer science. He can be contacted at email: a.benazzi@ump.ac.ma.