Bol. Soc. Paran. Mat.
©SPM – E-ISSN-2175-1188
SPM: www.spm.uem.br/bspm

(3s.) **v. 2025 (43)** : 1–16.
ISSN-0037-8712
doi:10.5269/bspm.69633

Application of Algebraic lattices in image Encryption: Methods comparison and analysis

Latifa Bedda, Abdelkarim Boua* and Abdelhakim Chillali

ABSTRACT: In this paper, we have introduced a novel color image encryption technique that relies on repairing a secret encryption key using algebraic lattices represented as Hasse diagrams and cryptography based on the matrices. The color images are converted into its RGB components (Red, Green and Blue) and each color is converted into a matrix of integers between 0 and 255. In this encryption process we proposed tow color images Lena of type JPEG and Baboon of type BMP with similar size, and we have involved the mathematical operations: addition, multiplication, and binary calculations, also be carried out a comparative study between certain encryption algorithms on this proposed color images. The experimental results reveal that the presented methods of image encryption has the advantages of large key space, strong robustness and good encryption and decryption performance. In addition, the product method has the merits of excellent performance of encryption.

Key Words: Lattice, Hasse diagram, color image, encryption, decryption, image encryption, algorithm, comparative.

Contents

1 Introduction

With the rapid development of computer network and the increasing transmission of image files over various channels, security is an important issue in communication technology. To protect images from unethical treats, we need to use different methods. Encryption is one of the well-known technique for ensuring the security, veracity, and secrecy of image [4,5]. The primary goal of image encryption is to transform the original image into an encrypted form that is challenging to understand or decipher, it is necessary that no one can get know the content without a decryption key. This encryption process involves applying mathematical operations, algorithms, and keys to the pixel values.
Image encryption refers to the process of securing images or visual data using cryptographic techniques. It involves transforming the pixel values or the entire image data in such a way that it becomes unintelligible to unauthorized users, while ensuring that authorized users can reverse the encryption and recover the original image.

There are various approaches to image encryption, including symmetric key encryption and asymmetric key encryption. Cryptographers have designed several historical ciphers such as Data Encryption

[*] Corresponding author

Submitted September 15, 2023. Published May 20, 2025
2010 *Mathematics Subject Classification:* 35B40, 35L70.

Standard (DES), Advanced Encryption Standard (AES), and Rivest-Shamir-Adleman (RSA). DES and AES are the symmetric key algorithms used for data encryption. RSA is an asymmetric key method used for digital signature verification and encryption.

Image encryption differs from text encryption due to some essential features of images, which include large data capacity, high redundancy, strong correlations between pixel units, etc. [12,13]. These features make traditional encryption systems like DES, AES, and RSA [11] unsuitable for practical image encryption because image pixels are highly correlated. Various authors have combined AES with other mathematical concepts such as wavelet transformation [2] or chaotic system [3] for image encryption operations.

Generally, image encryption methods can be divided into the spatial domain and frequency domain. In spatial domain approaches, encryption process is obtained by scrambling the image pixels [8]. In the frequency-domain schemes, the encryption process is performed in the transform coefficients [9,10].

Inspired by a cryptosystem based on matrices [6], we propose an application of image encryption scheme that combines the algebraic lattice and the block matrix.

Cryptography based on matrices involves the utilization of matrices as essential components in encryption and decryption processes. These cryptographic techniques employ mathematical operations on matrices to ensure the confidentiality, integrity, and authentication of data. Matrix encryption is a notable example of cryptography based on matrices. In this technique, plaintext data is converted into matrices, and encryption is accomplished by performing mathematical operations on these matrices. Matrix multiplication, addition, and other operations based on modular arithmetic are commonly employed in the encryption process.

Lattice encryption has gained attention in the field of post-quantum cryptography due to its resistance against attacks from quantum computers. The hardness of lattice problems forms the basis of many lattice-based cryptographic constructions, such as fully homomorphic encryption, digital signatures, and key exchange protocols. Researches in lattice-based cryptography continues to explore new algorithms and protocols to ensure the security and efficiency of these encryption schemes in practical applications.

In this paper, we propose a novel encryption algorithm for color images. Color image can be represented using matrices. In digital image processing, color images are often represented as three-dimensional matrices, where each element in the matrix corresponds to a pixel's RGB (Red, Green, Blue) values. The three dimensions of the matrix represent the color channels, and the values in each element determine the color intensity for that specific pixel. By manipulating these matrices, various image processing techniques, including encryption and decryption, can be applied to color images. Therefore, we suggest a technique for image encryption, that relies on repairing a secret encryption key using algebraic lattices represented as Hasse diagrams and cryptography based on the matrices. In addition, for methods we have involved the mathematical operations: addition, multiplication, and binary calculations

In order to simulate the proposed methods, we made the calculations and comparison with data implemented on the same computer and our implementation uses MATLAB R2020a software.

2 algebraic lattice

Definition 2.1 [1, Definition, p: 6] *A lattice L is a partially ordered set (poset) in which every two element x and y in L, have both a unique least upper bound (l.u.b), denoted by $x \vee y$, and unique greatest lower bound (g.l.b) denoted by $x \wedge y$.*

The least upper bound is also called the join of x and y, and the greatest lower bound is also called the meet of x and y. We have g.l.b$\{x,y\} = x \wedge y$ and l.u.b$\{x,y\} = x \vee y$.

Lemma 2.1 [1, Lemma 1, p: 8] *In lattice $(L, \vee, \wedge)$, the binary operations join $\vee$ and meet $\wedge$ have important algebraic properties, given x, y, z in L,the following axioms are satisfied:*

1. $x \vee x = x$, $x \wedge x = x$;
2. $x \vee y = y \vee x$, $x \wedge y = y \wedge x$;
3. $x \vee (y \vee z) = (x \vee y) \vee z$, $x \wedge (y \wedge z) = (x \wedge y) \wedge z$;

4. $x \vee (x \wedge y) = x$, $x \wedge (x \vee y) = x$*.*

Moreover $x \leqslant y$ *is equivalent each of the conditions* $x \vee y = y$ *and* $x \wedge y = x$*.*

A lattice L is complete when each of its subset X has a l.u.b and a g.l.b in L. Setting $X = L$, we see that any non-void complete lattice contain a least element noted 0 and greatest element noted 1.

Any finite lattice or lattice of finite length is complete.

When L is complete, it is possible to represent L as a Hasse diagram.

In this encryption algorithm, we need represent a lattice by a square matrix of elements 0 and 1. To accomplish this, the lattice needs to be initially presented as a Hasse diagram. Then, it can be represented as a square matrix.

Hasse diagrams are named after the German mathematician H. Hasse, who lived from 1898 to 1979 and used them to illustrate algebraic structures [14]. These diagrams serve as visual representations of a mathematical concept, specifically the concept of partial order. One goes back to the end of the 19th century, when Dedekind and Vogt made important theoretical investigations into arrangement (as documented in Rival [15]). Together with H. Hasse, the American mathematician G. Birkhoff studied partial orders extensively and raised the importance of this mathematical structure through his famous work "Lattice Theory [16]"

A Hasse diagram of a finite poset is a drawing where each element is represented by a point, and if x covers y, x is drawn above y and joined to it by a line.

A Hasse diagram is the best embedding for a poset $(P, <)$, it is drawn according to the following rules:

- If $x < y$ then x is placed below y;
- No edge is implied by transitivity;
- All edges whose orientation is omitted go up words.

To represent a lattice using a Hasse diagram, follow these steps:

1. Identify the elements of the lattice: Start by listing all the elements of the lattice. These elements can be represented by nodes in the Hasse diagram.
2. Determine the partial order: Identify the partial order relationship between the elements. For each pair of elements, determine if there is an order relation between them (one element is less than or equal to the other).
3. Draw the diagram: Begin drawing the Hasse diagram by placing the nodes representing the elements in a vertical order. The topmost node represents the maximum element, and the bottommost node represents the minimum element.
4. Add edges: Connect the nodes with directed edges to represent the partial order relationship. An edge from node a to node b indicates that a is less than or equal to b. Ensure that the edges are drawn in a way that reflects the partial order correctly.

A Hasse diagram is a graphical representation of a partially ordered set (poset) and provides a visual depiction of the lattice structure, highlighting the order relationships between its elements.

To represent a Hasse diagram as a matrix, we can create a square matrix with dimensions equal to the number of elements in the Hasse diagram and given a following definition

Definition 2.2 *Let* L *be a finite lattice with* $|L| = n$*, we considered* H *a Hasse diagram of* L*. We define an* n*-dimensional array over the set* $\{0, 1\}$ *as a function :*

$A : L \times L \longrightarrow \{0, 1\}$ *such as* $A(a_i, a_j) = a_{i,j} = 1$ *if* a_i *and* a_j *have related by an edge in* H *and* 0 *otherwise.*

For a matrix A*, we usually write* $a_{i,j}$ *for the element in the position* (i, j)*.*

By representing a Hasse diagram as a matrix, we can analyze the order relationships more systematically and perform computations or algorithms based on the matrix representation.

Definition 2.3 *Two $n \times n$ matrices A and B are said to commute if $AB = BA$. Denoted by C_A a set of commuting matrices with A defined by*

$$C_A = \{X \in M_n(\mathbb{Z}) \mid AX = XA\}$$

Example 2.1 Let $L_1 = \{a, b, c, d\}$ be a lattice represented by the following Hasse diagram:

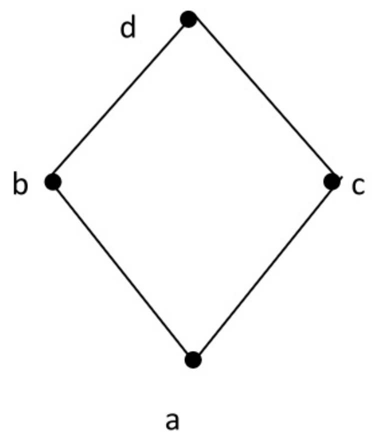


Figure 1: **Lattice** L_1

and the matrix associated is:

$$A = \begin{pmatrix} 1 & 1 & 1 & 0 \\ 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 \end{pmatrix}$$

Lemma 2.2 *The set C_A of matrices that commute with matrix A is as follows:*

$$C_A = \Big\{X \in M_4(\mathbb{Z}) \mid X = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 \\ a_5 & a_6 & a_1 + a_4 - a_6 & a_2 + a_3 - a_5 \\ a_2 + a_3 - a_5 & a_1 + a_4 - a_6 & a_6 & a_5 \\ a_4 & a_3 & a_2 & a_1 \end{pmatrix};$$
$$a_k \in \mathbb{Z}, k = 1, ..., 6\Big\}$$

Example 2.2 Let $L_2 = \{a, b, c, d\}$ a lattice represented by it's Hasse diagram:

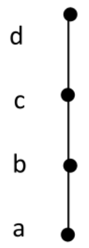


Figure 2: **Lattice L_2**

And the matrix associated is:

$$B = \begin{pmatrix} 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 \end{pmatrix}$$

Lemma 2.3 *The set C_B of matrices that commute with matrix B is as follows:*

$$C_B = \left\{ Y \in M_4(\mathbb{Z}) \mid Y = \begin{pmatrix} b_1 & b_2 & b_3 & b_4 \\ b_2 & b_1 + b_3 & b_2 + b_4 & b_3 \\ b_3 & b_2 + b_4 & b_1 + b_3 & b_2 \\ b_4 & b_3 & b_2 & b_1 \end{pmatrix}; b_k \in \mathbb{Z}, k = 1, ..., 4 \right\}$$

3 Cryptographic application

Definition 3.1 [7] *An encryption scheme consists of three sets: a key set K, a message set M, and a ciphertext set C together with the following three algorithms:*

1. *A key generation algorithm, which outputs a valid encryption key $k \in K$ and a valid decryption key $k^{-1} \in K$.*

2. *An encryption algorithm, which takes an element $m \in M$ and an encryption key $k \in K$ and outputs an element $c \in C$ defined as $c = E_k(m)$.*

3. *A decryption function, which takes an element $c \in C$ and a decryption key $k^{-1} \in K$ and outputs an element $m \in M$ defined as $m = D_{k^{-1}}(c)$. We require that $D_{k^{-1}}(E_k(m)) = m$.*

Lemma 3.1 *Let $m, n \in \mathbb{N}^*$ and A, B, C, X, Y be a square matrices of same order. If $AX = XA$ and $BY = YB$, then*

$$\textstyle\sum_{k=0}^{m-1} \sum_{l=0}^{n-1} X^{m-1-k} A^{n-1-l} C B^l Y^k = \sum_{l=0}^{n-1} \sum_{k=0}^{m-1} A^{n-1-l} X^{m-1-k} C Y^k B^l.$$

Proof: This equality is evident since $AX = XA$ and $BY = YB$.

3.1 Key exchange protocol

Alice and Bob agree on public an arbitrary square matrix $C \in M_n(\mathbb{N})$. Alice choose a private keys $l \in \mathbb{N}^*$ and lattice L_1 with a matrix associated is A of same order than C, and publish the set C_A of commuting matrices with A. In turn, Bob choose a private keys $t \in \mathbb{N}^*$ and lattice L_2 with a matrix associated is B of same order than C, and publish the set C_B of commuting matrices with B. Alice choose an other private key $Y \in C_B$ and calculate a matrix T such as $T = \sum_{i=0}^{l-1} A^{l-1-i} C Y^i$ and sends the result to Bob. In parallel, Bob choose an other private key $X \in C_A$ and calculate the matrix S such as $S = \sum_{j=0}^{t-1} X^{t-1-j} C B^j$ and send this result matrix to Alice. Both Alice and Bob calculate separately the matrices M and N such as

$$M = \sum_{i=0}^{l-1} A^{l-1-i} S Y^i$$

and

$$N = \sum_{j=0}^{t-1} X^{t-1-j} T B^j$$

returning to the Lemma 3.1 we conclude that $M = N$. Noted by K a secret key exchanged between Alice and Bob, we have $K = M$.

Application :
Alice and Bob agree on public the matrix

$$C = \begin{pmatrix} 3 & 13 & 7 & 19 \\ 1 & 32 & 9 & 27 \\ 11 & 5 & 12 & 33 \\ 29 & 7 & 53 & 211 \end{pmatrix}$$

Alice choose the private keys $l = 3$, lattice L_1 (**fig:1**) converted to the matrix $A = \begin{pmatrix} 1 & 1 & 1 & 0 \\ 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 \end{pmatrix}$ and publish the set C_A on the public.

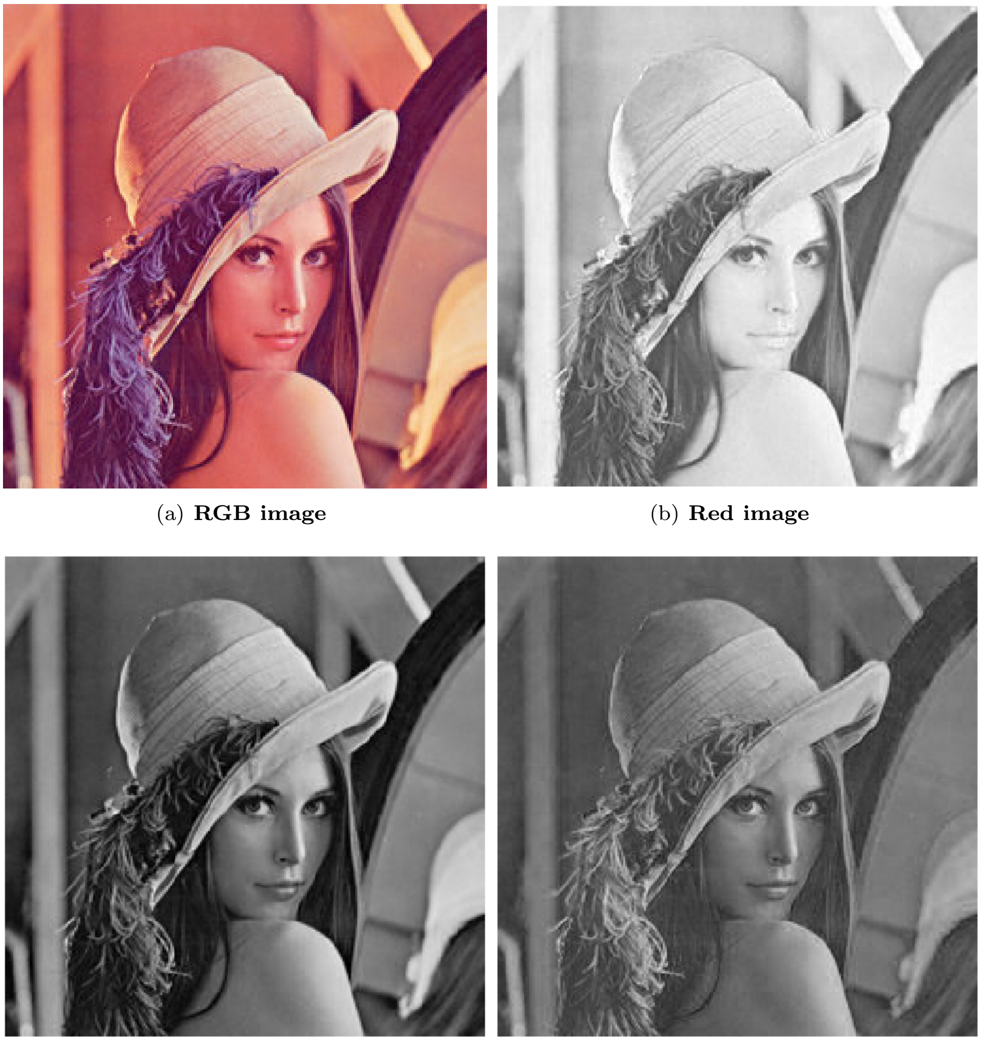
Bob chose the private keys $t = 5$, lattice L_2 (**fig:2**) converted to the matrix $B = \begin{pmatrix} 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 \end{pmatrix}$ and publish the set C_B on the public.

Alice choose the matrix $Y = \begin{pmatrix} 5 & 12 & 3 & 7 \\ 12 & 8 & 19 & 3 \\ 3 & 19 & 8 & 12 \\ 7 & 3 & 12 & 5 \end{pmatrix}$ that in C_B and calculates the matrix T to send it to Bob. Similarly, Bob choose the matrix $X = \begin{pmatrix} 21 & 5 & 37 & 103 \\ 13 & 20 & 104 & 29 \\ 29 & 104 & 20 & 13 \\ 103 & 37 & 5 & 21 \end{pmatrix}$ that in C_A and calculates the matrix S to send it to Alice.
With they private keys Alice and Bob calculate the secret key exchange $K = M = N$.
The secret key exchange is

$$K = (1.0e + 13) \times \begin{pmatrix} 1.8788 & 3.4170 & 3.0745 & 2.2424 \\ 1.8557 & 3.3725 & 3.0368 & 2.2154 \\ 2.0297 & 3.6444 & 3.3216 & 2.3964 \\ 2.1808 & 3.9160 & 3.5691 & 2.5714 \end{pmatrix}$$

3.2 Proposed color image encryption

The color image is a three-dimensional image, and is decomposed into three-channel images of red, green and blue (R, G, B) and spliced into a two-dimensional gray rectangle image. The suggested algorithm takes an input image of any size, $m \times n \times 3$, where the third dimension accounts for the RGB values, and uses m and n in the encryption/decryption processes.
Our proposed color image encryption process contains two Steps which are explained in de following: In first step, we select a color image proposed of Lena, of type jpeg with a pixel size $256 \times 256 \times 3$. As it's shown in **figure 3** with three-channel images of **(b)**, **(c)** and **(d)** (R, G, B):



(a) **RGB image**

(b) **Red image**

(c) **Green image**

(d) **Blue image**

Figure 3: **Lena color and the** (R, G, B) **components.**

The Lena image is saved in the matrix noted "Bim" of the pixel values of integers between 0 and 255 correspond for each point of the image. The matrix Bim is decomposed into three matrices of each color $B_1(256, 256, 1)$, $B_2(256, 256, 2)$ and $B_3(256, 256, 3)$ which represent the images (b), (c) and (d), respectively.
In second step: we will generate the secret key of encryption. For that we transfer the matrix K of size (4,4) into a column vector K' of size (16, 1) of values modulo (256) by using the following algorithm:

```
$V = reshape(K, 16, 1)$    ( K is the secret key that Alice and Bob calculated )
$K' = zeros(n, 1);$
   for $i = 1 : n$
     $K'(i) = mod(V(i), 256);$
   end
```

We obtain:

$$K' = \begin{pmatrix} 64 \\ 169 \\ 197 \\ 50 \\ 65 \\ 232 \\ 12 \\ 27 \\ 129 \\ 88 \\ 244 \\ 147 \\ 4 \\ 55 \\ 43 \\ 150 \end{pmatrix}$$

In order to perform matrix operations with the matrix B_1, B_2 and B_3 for encryption, it is necessary to resize the vector K' to a size of $(256, 1)$. it is a vector that we obtain with a repetition of vector K' until we obtain 256 rows in a column. For this transformation, we give this algorithm:

```
$Kcl = zeros(n, n);$
   for $i = 1 : n$
     for $j = 1 : n$
         $Kcl(i, j) = K'(i);$
     end
   end
$Kcl$
$Cle = reshape(Kcl, n \times n, 1)$
```

Cle is a column vector of size 256 × 1, this is the secret key that we will use for our encryption methods.

3.3 Proposed encryption methods

We present a novel encryption schemes proposed for color image. The encryption processes in this technique comprises three distinct methods which will are detailed in the following sections and we provide the algorithm of encryption and decryption.

3.3.1 The Sum encryption method

This encryption technique applies the sum of two vectors, the vector Cle and each column vector of each matrix B_1, B_2 and B_3 with results are the values $modulo(256)$ as follows:

$S_1 = mod(B_1(i, j) + Cle(i), 256)$ for $i = 1 : 256$ and $j = 1 : 256$,

$S_2 = mod(B_2(i, j) + Cle(i), 256)$ for $i = 1 : 256$ and $j = 1 : 256$,

$S_3 = mod(B_3(i,j) + Cle(i), 256)$ for $i = 1 : 256$ and $j = 1 : 256$,

S_1, S_2 and S_3 are the encrypted matrices images of B_1, B_2 and B_3, From this encrypted matrices, we deduce the encrypted image complete for image Lena gives in **figure 4**

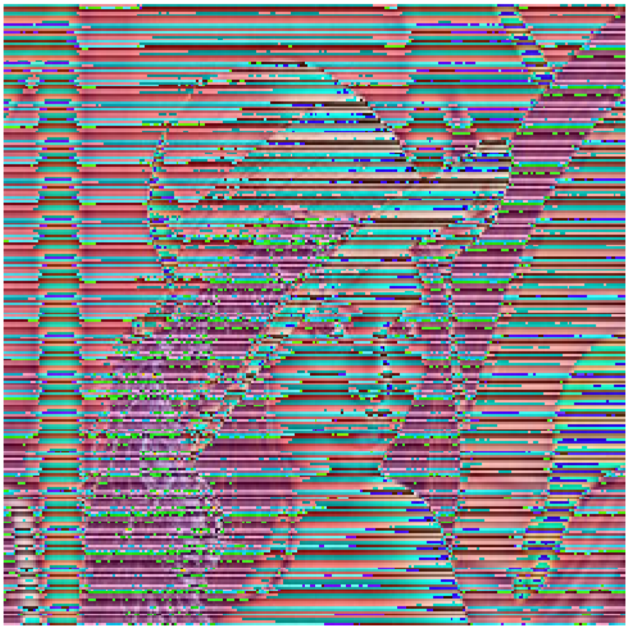


Figure 4: **Sum encryption image of Lena**

The ciphered image can be decrypted by the formula as follows:

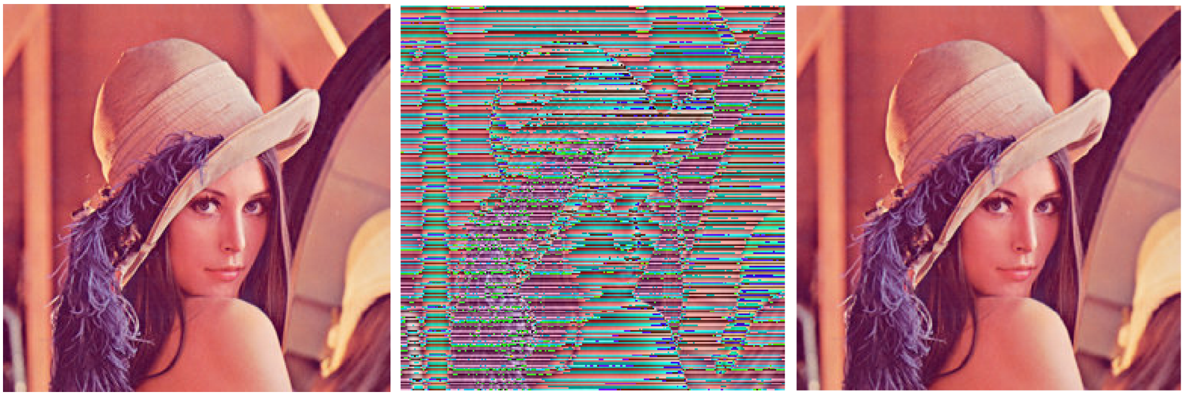
$inS_1 = mod(S_1(i,j) - Cle(i), 256)$ for $i = 1 : 256$ and $j = 1 : 256$

$inS_2 = mod(S_2(i,j) - Cle(i), 256)$ for $i = 1 : 256$ and $j = 1 : 256$

$inS_3 = mod(S_3(i,j) - Cle(i), 256)$ for $i = 1 : 256$ and $j = 1 : 256$

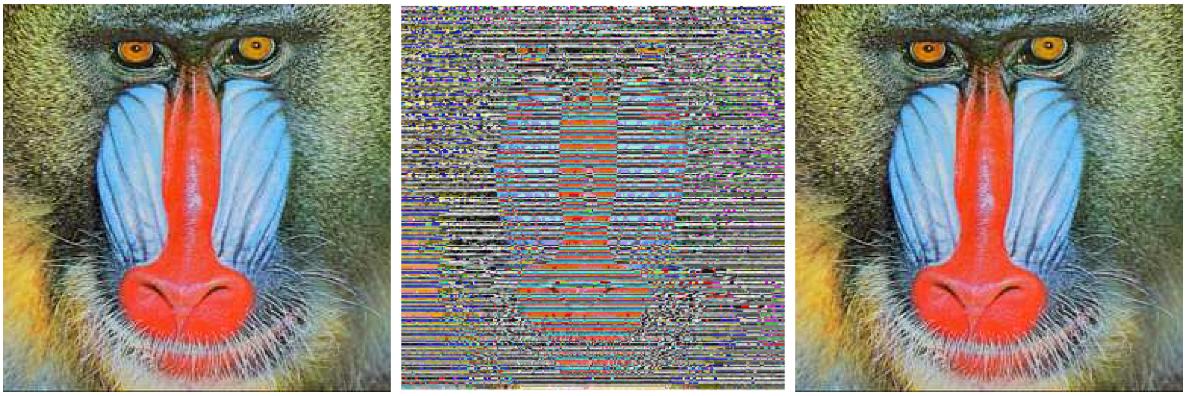
such as inS_1, inS_2 and inS_3 are the decrypted matrices images , respectively, of S_1, S_2 and S_3. From this decrypted matrices, we end up with the original image of Lena.

We apply the same method for the Baboon image of type bmp, the results of sum encryption and decryption of proposed method of Lena image and Baboon image are shown in Figures **5** and **6** respectively,



(a) **Original image of Lena** (b) **Encryption image of Lena** (c) **Decryption image of Lena**

Figure 5: **Encrypted and decrypted Lena image by sum.**



(a) **Original image of baboon** (b) **Encryption image of Baboon** (c) **Decryption image of Baboon**

Figure 6: **Encrypted and Decrypted Baboon image by Sum.**

3.3.2 The product encryption method

For this encryption algorithm we have performed a product of two column vectors by multiplying each column vector of matrix B_k by the secret key Cle and this makes component by component $modulo(257)$ such as :

$P_1 = mod(B_1(i,j) \times Cle(i), 257)$ for $i = 1:256$ and $j = 1:256$

$P_2 = mod(B_2(i,j) \times Cle(i), 257)$ for $i = 1:256$ and $j = 1:256$

$P_3 = mod(B_3(i,j) \times Cle(i), 257)$ for $i = 1:256$ and $j = 1:256$

such as P_1 , P_2 and P_3 is, respectively, the encrypted matrix image of B_1 , B_2 and B_3
This result encryption matrices generate the matrix Pr, which serves as the representation of the encrypted image of the original image.

Encryption process of proposed method is shown in **figure 7**

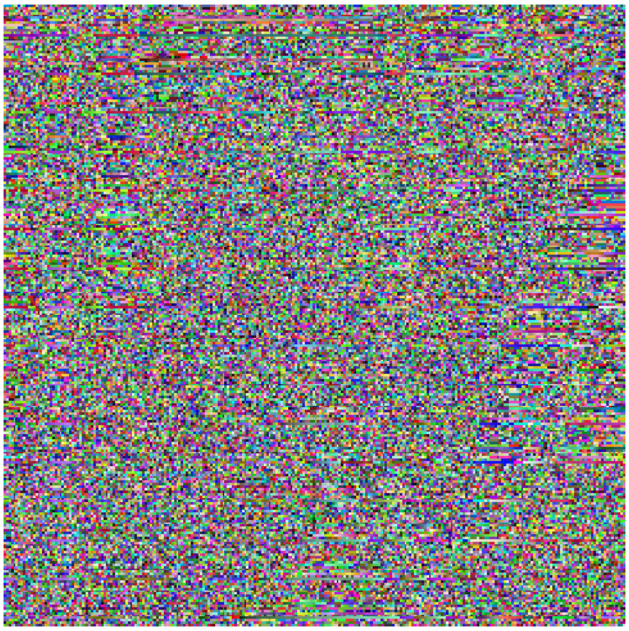


Figure 7: **Product. Encrypted image of Lena**

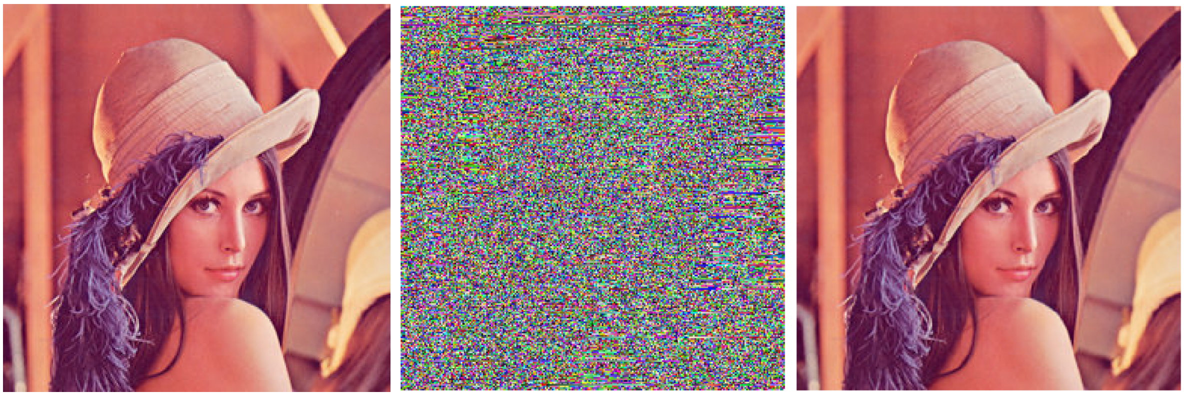
During the decryption process we will need the following inverse function for the secret key Cle noted by $inCle$ calculated by the following expression ,
if $(Cle(i) \times j) mod(257) = 1$, then $inCle(i) = j$ is the inverse value of $Cle(i)$ that for $i = 1 : 256$.
For this decryption we use the similarly process for encryption but with inverse vector $inCle$, the formula is as follows:

$inP_1(i,j) = mod(P_1(i,j) \times inCle(i), 257)$; for $i = 1 : n$ and $j = 1 : n$

$inP_2(i,j) = mod(P_2(i,j) \times inCle(i), 257)$; for $i = 1 : n$ and $j = 1 : n$

$inP_3(i,j) = mod(P_3(i,j) \times inCle(i), 257)$; for $i = 1 : n$ and $j = 1 : n$

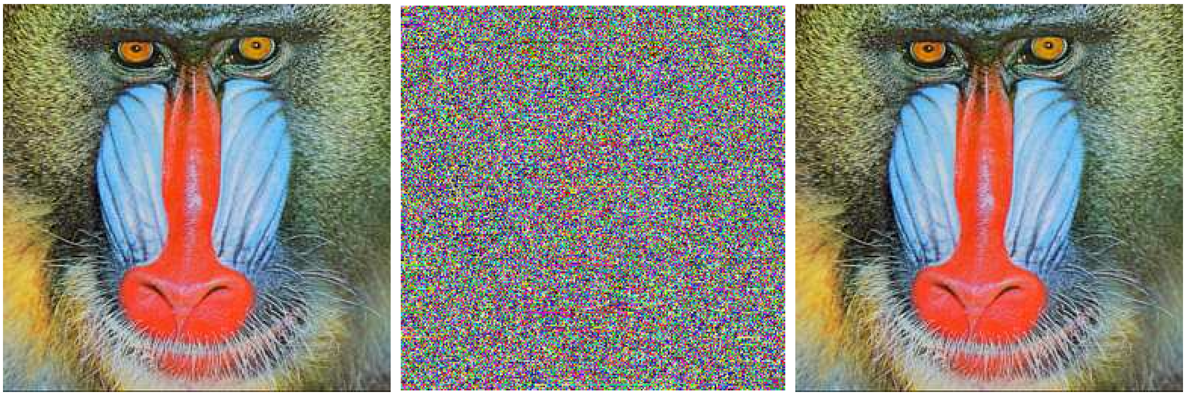
After that, we obtained the decrypted matrix image $inPr$.
The result of the product encryption and decryption proposed method is shown in **figure 8**



(a) **original image of Lena** (b) **Encryption image of Lena** (c) **Decryption image of Lena**

Figure 8: **Encrypted and decrypted Lena image by product.**

With the same algorithm for encryption and decryption of Baboon image, we obtained the result as follows in **figure 9**



(a) **Original image of Baboon** (b) **Ecryption image of Baboon** (c) **Decryption image of Baboon**

Figure 9: **Encrypted and decrypted Baboon image by product.**

3.3.3 The binary encryption method

This process for encryption involves the following stages: First, we converted the secret key, the vector Cle, on the binary unite 8 and we get the matrix of size 256×8 noted by $bnCle$. The same applies for the matrices B_1, B_2 and B_3, we obtained the binary matrices of size (65536×8) deneted, respectively, bnB_1, bnB_2 and bnB_3.

second, the encryption is performed by the following code applied on the matrices bnB_1, bnB_2 and bnB_3.

Binary matrix bnB_1 encryption:

```
for $k = 1 : 256$
  for $i = 1 : 256$
        $j = 256 \times (k-1) + i;$
        $bnE1(j, 1:8) = mod(bnB1(j, 1:8) + bnCle(i, 1:8), 2);$
  end
end
```

Binary matrix bnB_2 encryption:

```
for $k = 1 : 256$
    for $i = 1 : 256$
        $j = 256 \times (k-1) + i;$
        $bnE2(j, 1:8) = mod(bnB2(j, 1:8) + bnCle(i, 1:8), 2);$
    end
end
```

Binary matrix bnB_3 encryption:

```
for $k = 1 : 256$
   for $i = 1 : 256$
         $j = 256 \times (k-1) + i;$
         $bnE3(j, 1:8) = mod(bnB3(j, 1:8) + bnCle(i, 1:8), 2);$
   end
end
```

Third, we converted the encrypted matrix image bnE_k for $k = 1, 2, 3$, on to decimal matrix denoted by E_k of size (65536×8).

Finally, To finish this process for encryption, it is necessary to resize of each one of the matrices E_1, E_2 and E_3 on to matrices, respectively, M_1, M_2 and M_3 of size 256×256, that we get the encryption matrix image noted $MatM$ for the matrix image Bim. The result can be seen in **figure 10**

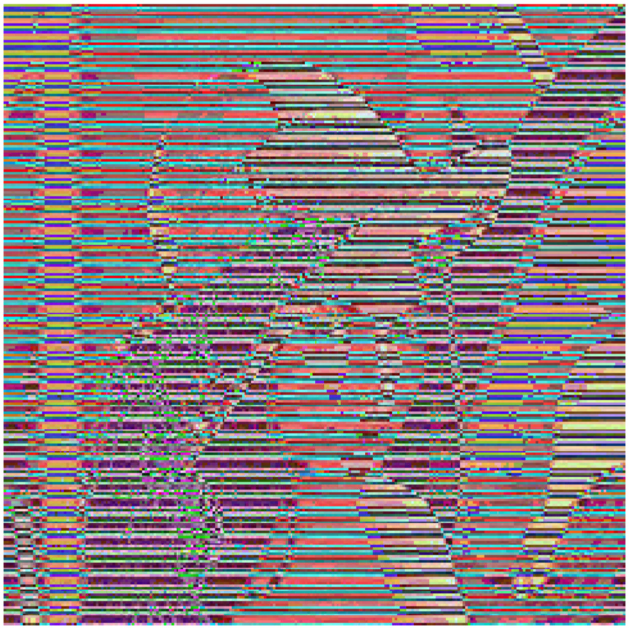


Figure 10: **Binary. Encrypted image of Lena**

The same approach can be applied to decrypt the encrypted image obtained. We can start directly with the encrypted binary matrices above and apply the same code to them.

The binary matrix bnE_1 decryption:

```
    for $k = 1 : 256$
      for $i = 1 : 256$
            $j = 256 \times (k - 1) + i;$
            $bnC1(j, 1 : 8) = mod(bnE1(j, 1 : 8) + bnCle(i, 1 : 8), 2);$
      end
    end
$bnC1;$
```

The binary matrix bnE_2 decryption:

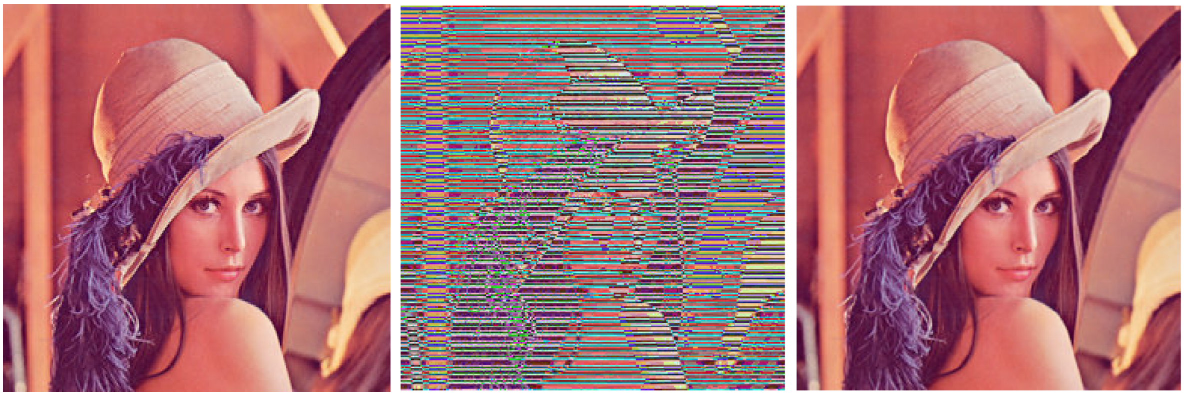
```
    for $k = 1 : 256$
      for $i = 1 : 256$
             $j = 256 \times (k - 1) + i;$
            $bnC2(j, 1 : 8) = mod(bnE2(j, 1 : 8) + bnCle(i, 1 : 8), 2);$
     end
   end
$bnC2;$
```

The binary matrix bnE_3 decryption:

```
   for $k = 1 : 256$
     for $i = 1 : 256$
           $j = 256 \times (k - 1) + i;$
```

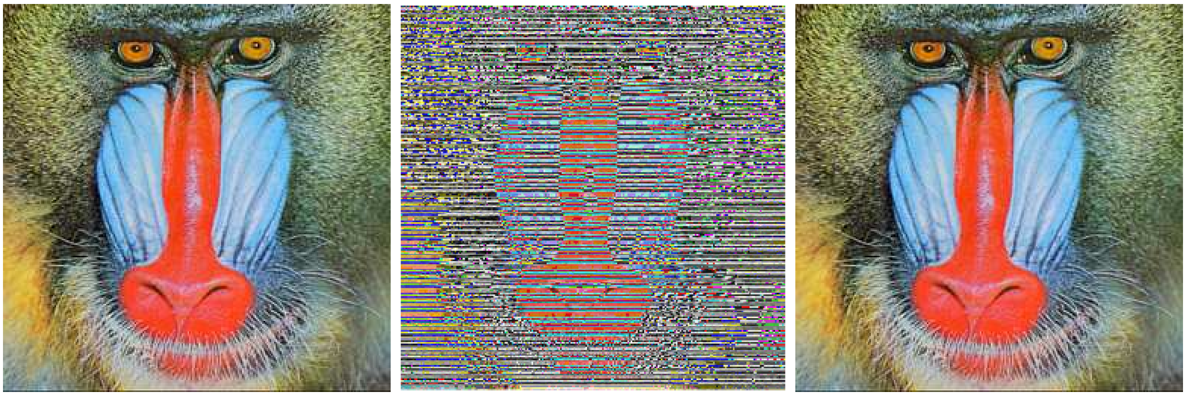
```
        $bnC3(j, 1:8) = mod(bnE3(j, 1:8) + bnCle(i, 1:8), 2);$
    end
  end
$bnC3;$
```

After to convert this above binary matrices decrypted $bnC1$, $bnC2$ and $bnC3$ in to decimal matrices, we get the image decrypted. The results of encryption and decryption of proposed method for Lena image and Baboon image are presented in **figures 11** and **12** respectively.



(a) **original image of Lena** (b) **Encryption image of Lena** (c) **Decryption image of Lena**

Figure 11: **Encrypted and decrypted Lena image by binary.**



(a) **Original image of Baboon** (b) **Ecryption image of Baboon** (c) **Decryption image of Baboon**

Figure 12: **Binary encryption and decryption image of Baboon.**

3.3.4 Comparing various encryption methods

This section provides the results of simulation, performance and robustness of the different encryption algorithms proposed applied to the tow color images, Lena of type JPEG and Baboon of type BMP with similar size. The results are presented in **table 1**:

Table 1: Performance of the encrypted and decrypted image.

Method	Performance of encrypted image	Performance of decrypted image	Time execution
Sum	Way	Excellent	Very good
Product	Excellent	Excellent	Good
Binary	Good	Excellent	Good

4 Conclusion

This paper provides a new method in encrypted image based on lattice and matrix, this proposed algorithm has been implemented color images of different types and the same size. The simulation, performance and experimental results indicate that has a good encryption results and larger key space.

References

1. G. Birkhoff, *Lattice Theory,* Amer. Math. Soc., New York, 1940.
2. H. R. Shakir, *An image encryption method based on selective AES cod- ing of wavelet transform and chaotic pixel shuffling, Multimedia Tools and Applications* 78(18) (2019) pp. 26073-26087.
3. S. Toughi, M.H. Fathi and Y.A. Sekhavat, *"An image encryption scheme based on elliptic curve pseudo random and Advanced Encryption System,"* Signal Processing 141 (2017) pp. 217-227, .
4. Nestor, T.; Belazi, A.; Abd-El-Atty, B.; Aslam, M.N.; Volos, C.; De Dieu, N.J.; Abd El-Latif, A.A. *A new 4D hyperchaotic system with dynamics analysis, synchronization, and application to image encryption.* Symmetry 2022, 14, 424.
5. Zhu, S.; Deng, X.; Zhang, W.; Zhu, C. *Image Encryption Scheme Based on Newly Designed Chaotic Map and Parallel DNA Coding.* Mathematics 2023, 11, 231.
6. Zeriouh, M., Chillali, A., and Boua, A. (2019). *Cryptography based on the matrices.* Bol. Soc. Paran. Mat, 3(3), 75-83.
7. C. Boyd and A. Mathuria, *Protocols for Authentication and Key Establishment, Information Security and Cryptography* Series; Springer-Verlag, Heidelberg, 2003.
8. Y. Qin, Z. Wang, Q. Pan, Q. Gong, *Optical color-image encryption in the diffractive-imaging scheme,* Opt. Lasers Eng. 77 (2016) 191–202.
9. S. Yuan, Y. Yang, X. Liu, X. Zhou, Z. Wei, *Optical image transformation and encryption by phase-retrieval-based double random-phase encoding and compressive ghost imaging*, Optics Lasers Eng. 100 (2018) 105–110.
10. X. Liao, M.A. Hahsmi, R. Haider, et al., *An efficient mixed inter-intra pixels substitution at 2bits-level for image encryption technique using Dna and Chaos*, Optik 153 (2018) 117–134.
11. Menezes A, Van Oorschot P, Vanstone S. *Handbook of applied cryptography.* Boca. Raton, FL: CRC Press; 1997
12. Jastrzebski K, Kotulski Z. *On improved image encryption scheme based on chaotic map lattices.* Eng Trans 2009;57(2):69–84.
13. Chung KL, Chang LC. *Large encryption binary images with higher security.* Pattern Recognit Lett 1998;19(56):461–8.
14. Hasse, H. Vorlesungen über Klassenkörpertheorie, Physica-Verlag: Würzburg, 1967.
15. Rival, I. *In: Graphs and order*; Rival, I., Ed.; D.Reidel Publishing Company: Dordrecht, 1985; pp. 103-133.
16. Birkhoff, G. *Lattice theory*, American Mathematical Society: Rhode Island; Vol: XXV, 1984.

Latifa Bedda,
University Sidi Mohammed Ben Abdellah,
Polydisciplinary Faculty,
Department of Mathematics,
Taza,
Morocco.
E-mail address: latifabedda@gmail.com or latifa.bedda@usmba.ac.ma

and

Abdelkarim Boua,
University Sidi Mohammed Ben Abdellah,

Polydisciplinary Faculty,
Department of Mathematics,
Taza,
Morocco.
E-mail address: abdelkarimboua@yahoo.fr or karimoun2006@yahoo.fr

and

Abdelhakim Chillali,
University Sidi Mohammed Ben Abdellah,
Polydisciplinary Faculty,
Department of Mathematics,
LSI, Taza,
Morocco.
E-mail address: abdelhakim.chillali@usmba.ac.ma