# Image Encryption Algorithm based on Elliptic Curves

SARA CHILLALI*, LAHCEN OUGHDIR
Engineering Sciences Laboratory – LSI,
Higher Normal School of Fez (ENSF),
Sidi Mohamed Ben Abdellah University,
Fez,
MOROCCO

**Corresponding Author*

*Abstract:* - Several cryptography schemes on the images use chaos theory, these schemes are very effective but have weaknesses such as the distribution of keys between the two entities that want to exchange an image confidentially. In this work, we propose an efficient encryption scheme using elliptic curves, we show that the proposed scheme is tamper-proof against any attack. It also proves security because of the problem of discrete logarithm on this elliptic curve whose calculation is difficult. This scheme achieves the required objectives such as non-repudiation, confidentiality, and integrity. During the security analysis of the proposed scheme, we verified that many security attributes have been satisfied.

*Key-Words:* - Cryptography, Elliptic curve, Image processing, Analysis of data, Embedded systems, Matlab.

Received: July 16, 2022. Revised: October 22, 2023. Accepted: November 24, 2023. Published: December 31, 2023.

## 1 Introduction

The embedded systems are open and free domains. That is to say, when you send information from one point to another, it is redirected via several stations where you can read this data.

The analysis of this data via these systems is in fact as open as sending a postcard.

The protection of transmitted data is an open domain which can only be ensured by effective encryption.

This work consists of implementing an encryption algorithm applied to standard image files (BMP, JPEG, TIFF), based on simulated attacks.

Cryptology is a mathematical science that has two branches; cryptography and cryptanalysis.

On the one hand, traditional cryptography is the study of methods of transmitting data in a confidential way.

Cryptanalysis, on the other hand, is the study of cryptographic processes in order to find weaknesses and particularly to be able to decrypt encrypted messages.

Image processing is certainly the most innovative process that man has known, motivated by his needs in various fields, including imaging, the later, generates sensitive problems solved by the various image processing techniques.

The digital image is represented by a matrix of points called pixels (Picture Element), each one has a characteristic of a gray level or a color coming from the corresponding location in the real image or calculated from an internal description of the scene to represent.

We can represent an image by a matrix$M(m_{i,j})$ ; $m_{i,j} \in \{0,1,2,\dots,255\}$.

The real-time image processing system is a visualization and interpretation system. The functions performed by each module of the system are as follows:

1- The video camera transforms the optical image into an analog signal.

2- The conversion of the signal into a set of digital data by performing coordinated sampling operations, and the quantification of the amplitudes of the light intensity measured by the digitization module.

3- The storage and visualization of digital data is ensured by the visualization module and the result will be saved in a file.

In [1], the authors invented a key distribution method based on a very difficult mathematical problem to solve; this problem is the discrete logarithm on a cyclic group of finite order.

In [2], the authors gave an encryption method using matrices built in [3], as points out in his article of image cryptography based on chaos and cubic. In other cryptography problems we find discrete logarithm problem on a Montgomery Curves in [4]

and the closest vector problem in, [5]. In this work, we expose a new method of image encryption, based on the last problem, using a Diffie-Hellman key exchange on an elliptic curve. The security of this type of encryption is proven because the resolution of the problem of discrete logarithm is almost impossible on these curves.

In the following, $\mathbb{F}_P$ denotes a finite field where p is a prime number greater than or equal to 5, [6].

In this context, an elliptic curve over $\mathbb{F}_P$ is a plane curve defined by an equation of the form :$y^2 = x^3 + ax + b$ ; where a and b are in $\mathbb{F}_P$ and $\Delta = -16(4a^3 + 27b^2)$ is not equal to zero.
We denote this curve by : $E_{a,b}(p)$, we can write :

$$E_{a,b}(p) = \{(x,y) \in \mathbb{F}_p^2 / y^2 = x^3 + ax + b\} \cup \{[0:1:0]\} \quad (1)$$

The law '+' defined on $E_{a,b}(p)$ by :
For each three points $P(x_1, y_1), Q(x_2, y_2)$ and $R(x_3, y_3)$ of the elliptic curve defined by (1) such that $R = P + Q$. Then R is given by:

- $R = [0:1:0]$, for $x_1 = x_2, y_2 = -y_1$;
- $R(x_3, y_3)$ ; $x_3 = t^2 - x_1 - x_2$ and $y_3 = -tx_3 - s$, with:

$$t = \begin{cases} \frac{y_2 - y_1}{x_2 - x_1}, & \text{if } P \neq Q \\ \frac{3x_1^2 + a}{2y_1}, & \text{if } P = Q \end{cases} \quad \text{and}$$

$$s = \begin{cases} \frac{x_2 y_1 - x_1 y_2}{x_2 - x_1}, & \text{if } P \neq Q \\ y_1 - \frac{a x_1 + x_1^3}{2y_1}, & \text{if } P = Q \end{cases}$$

A point multiplication can be considered as a series of consecutive point additions: $kP = \underbrace{P + P + \cdots + P}_{k \text{times}}$
$(E_{a,b}(p), +)$ is an abelian group of neutral element [0 :1 :0], called the point at infinity.

The principle of public key cryptography is based on two keys, one is public and the other is private. Finding the private key from the public key is equivalent to solving a difficult problem.

On elliptic curves, it is the problem of the discrete logarithm that must be solved to find the secret key. That is to say, find k knowing $kP = Q$ with P and Q are known and $Q \in < P >$.

# 2 Proposed Encryption Scheme

Let $E_{a,b}(p)$ be an elliptic curve on the field $\mathbb{F}_P$ defined by (1), where p is a large prime number such as the discrete logarithm problem in $E_{a,b}(p)$ is difficult.

## 2.1 Key Exchange between Entities A and B

1) The two entities A and B agree on a prime number p, a generator P of a cyclic subgroup of known order of the elliptic curve $E_{a,b}(p)$.
2) A chooses a random integer secret $t < ord(P)$, and sends tP to B.
3) B also chooses a random integer secret $l < ord(P)$, and sends lP to A.
4) A computes tlP.
5) B computes ltP.
The secret key between A and B is : $K_{lt} = ltP = tlP$.

## 2.2 Secret Key Calculation Algorithm

Each for himself, A and B build the secret encryption key ; K by the following steps:

- Step1 :

Construction of matrix A of size [T,3,3] :
Let $iK = (x_i, y_i), i \in \{1,2,\dots,T\}$, the matrix $A(A(i,j,p))$ ; $A(i,j,p) \in \{0,1,2,\dots,T-1\}$ is constructed as following :
For $i \in \{1,2,\dots,T\}$ and $p \in \{1,2,3\}$ ;

$$A(i,1,p) = x_i \ [T]$$
$$A(i,2,p) = y_i \ [T]$$
$$A(i,3,p) = i$$

- Step2 :

Build an encryption matrix B, whose size is the size of the image:
Let $[m,n,p]$ the size of the image to be encrypted, then

$$B(i,j,1) = A(k,1,1), k \in \{1,2,\dots,(i+j\ [T])\}$$
$$B(i,j,2) = A(k,2,2), k \in \{1,2,\dots,(i*j\ [T])\}$$
$$B(i,j,3) = A(k,3,3), k \in \{1,2,\dots,(i-j\ [T])\}$$

- Step3 :

Convert matrix B to a column matrix C of size $[mn,1,3]$, this matrix is constructed as following :

$$C((j-1)n + i, 1, p) = B(i,j,p), \quad i = 1,\dots,n; j = 1,\dots,m; p = 1,2,3$$

Finally convert the decimal numbers of the matrix C into binaries of size t=size(T) , so the obtained matrix $\tilde{C} = (c_i)_{i=1,\dots,nm}$ is the secret key built between the two entities A and B.
Each $c_i$ can be written as $c_i = c_{i1}c_{i2}\dots c_{it}$, where $c_{ik}$ equals to 0 or 1.

## 2.3 Encryption Algorithm

The need to encrypt, store and transmit a digital image or any other graphic form comprising thousands of bytes and at the rate of more than 5000

images per day, for a traffic for example, we question the amount of data produced for this last.
This problem had to be solved by cryptography and coding in order to guarantee confidentiality, integrity, authentication and non-repudiation while maintaining a faithful replica of the original data.
If we look at the image on the physical plane, we find that the image signal is very redundant in nature. Neigh boring pixels generally have similar gray levels, which shows a significant spatial correlation. By exploiting dissociation, it is possible to reduce the disturbance of this redundancy.
Let $\tilde{C}$ a secret key between A and B.
B wants to send an image confidentially « img » to A, it follows the structure of the proposed algorithm which consists of five encryption steps, as described by:

- Step1 :

Turn the image, « img » in to a matrix M. The public size of M is $[n, m, p]$.

- Step2 :

Convert matrix M to a column matrix S of size mn, such that :

$$S\big((j-1)n+i,1,p\big) = M(i,j,p),$$
$$i = 1,\dots,n; j = 1,\dots,m; p = 1,2,3$$

- Step3 :

Convert the decimal numbers of the matrix S into binaries of size t ; $\tilde{S} = (s_i)_{i=1,\dots,nm}$.

- Step4 :

Calculate, $\tilde{D} = \tilde{C} \oplus \tilde{S}$ where $\tilde{D}(d_i)_{i=1,\dots,nm}$ and $d_{ik} = c_{ik} + s_{ik}$

- Step5 :

Convert the binary numbers from matrix $\tilde{D}$ to decimals modulo 256 to get a matrix column D, then the matrix of the decrypted image is the matrix N such that:

$$N(i,j,p) = D(i+(j-1)n,1,p),\ i = 1,\dots,n; j = 1,\dots,m; p = 1,2,3$$

The transformation of N into image, "encryption(img)" is the encryption of the image origin "img".

### 2.4 Decryption Algorithm

A receives "encryption(img)" sent by B, he has the private key which allows him to reciprocally calculate the matrix M, which we can transform to the image "img". Figure 1 illustrates such a situation:

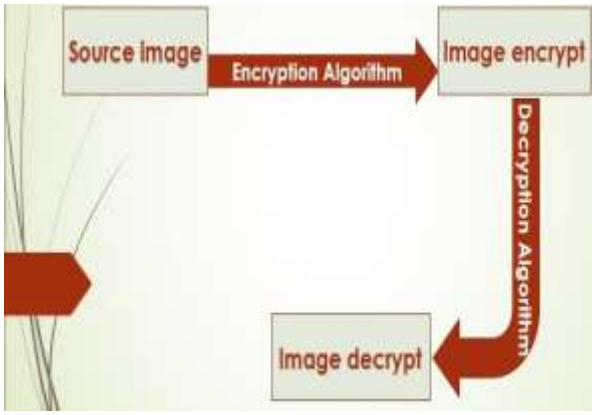

Fig. 1: Encrypt and decrypt Algorithm

### 2.5 Security

Cryptography on elliptic curves (ECC) is a public key encryption technique based on the theory of elliptic curves that can be used to create faster cryptographic keys, smaller and more efficient.

According to some researchers, ECC can achieve a level of security with a 164-bit key than other systems require a 1024-bit key. ECC was developed by a mobile e-commerce security provider. The security of our contribution is based on the problem of the discrete logarithm on an elliptic curve, until now, there is no specific algorithm which solves such a problem on special elliptic curves.

## 3 Example and Illustration

To check the performance of the proposed scheme, the results of simulation experiments were evaluated by several criteria in this section. Our experimental environment was a desktop PC with 64-bitWindows 10 OS, Intel i7-2600 CPU, and 8GB RAM.

The programming language was Matlab, the test images were chosen from image database.

In this part all illustrations are done by MATLAB, we assume that ;
$p = 2543, a = 1758$ and $b = 254$.
Let the elliptical curve defined on $\mathbb{F}_{2543}$ by an equation: $y^2 = x^3 + 1758x + 254$
We have :

$$E_{1758,254}(2543) = \{(x,y) \in \mathbb{F}_{2543}^2 / y^2 = x^3 + 1758x + 254\} \cup \{[0:1:0]\} \quad (2)$$

Let $K = (146, 2377) \in E_{1758,254}(2543)$, the secret key between A and B, we count $iK = (x_i, y_i)$, $i \in \{1,2,\dots,256\}$ ; $T = 256, t = size(256) = 8$.

### 3.1 Encryption and Decryption Simulation

The images where we have chosen for the encryption and decryption test are downloaded from

a standard image processing library, we have selected 20 black and white images and 15 colors with different extensions (bmp, jpg, tif) and different sizes, [7].

The intrinsic features of bit distribution in digital images were revealed. Higher bits of pixels hold higher weight of an image's information, and there are strong correlations among the higher bit planes.

In the instance of Figures, the 8th bit plane and the 7th bit plane tend to have opposite values.

These features shall not be neglected in a secure cryptosystem.

To build our way through bit maps, the strategy has been extended to color, grayscale and black and white images with different extensions in this article.

By these means, an ordinary image of size [m, n, p] is extended to a matrix M of the same size. All the p bit planes of the pixels of the ordinary image have been placed in the p th matrix M (:,:, p) ; p=1,2,3.

After generating a key matrix of size [n, m, p], the p bit planes were restored by XOR operations which were performed on pixels. As illustrated in the following figures, the entire cryptosystem is managed by Matlab. The inputs to the algorithm are the ordinary image "img" of size [n, m, p] and the parameters (Bmp, Jpg, Tif). The output is the encrypted image.

We will include five examples of figures, one in black and white and the other in color, the set is detailed in Figure 2, Figure 3, Figure 4, Figure 5 and Figure 6.


Fig. 2: Image encryption and decryption experimental result using Mandrill

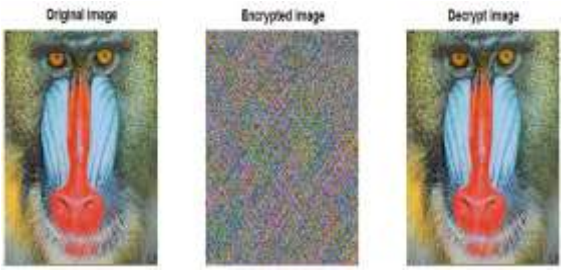


Fig. 3: Image encryption and decryption experimental result using Mandrill


Fig. 4: Image encryption and decryption experimental result using Lena


Fig. 5: Image encryption and decryption experimental result using Peppers

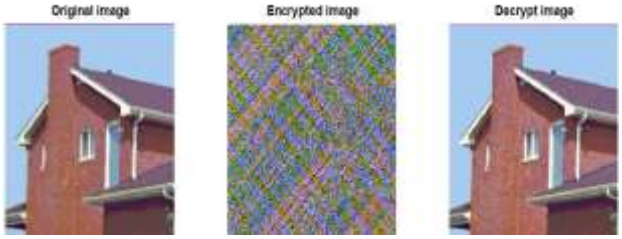


Fig. 6: Image encryption and decryption experimental result using House

## 3.2 Analysis by Histogram

The histogram is the foundation of various spatial image processing techniques, e.g., image enhancement. Moreover, the inherent information of histograms is useful in image compression and segmentation.

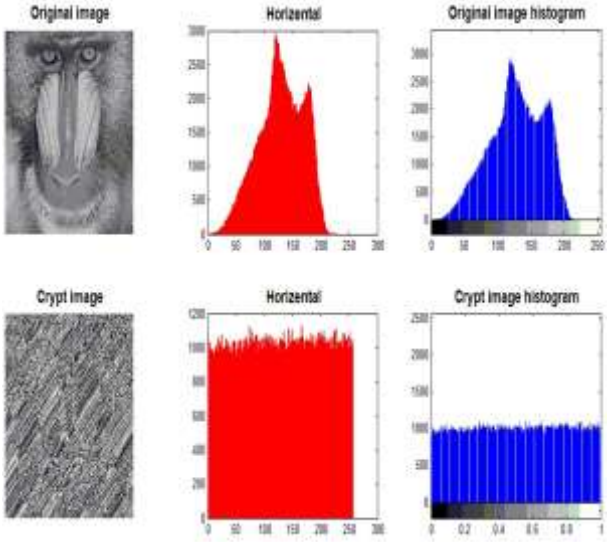


Fig. 7: Histogram of Mandrill image Red and Blue color component

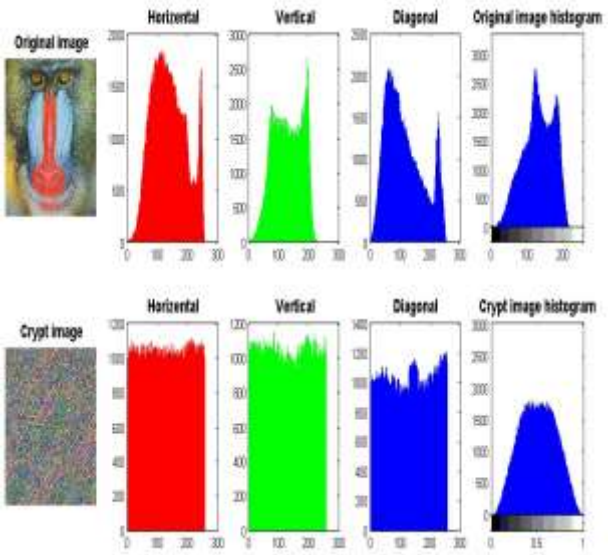


Fig. 8: Histogram of Mandrill image Red, Green and Blue color component

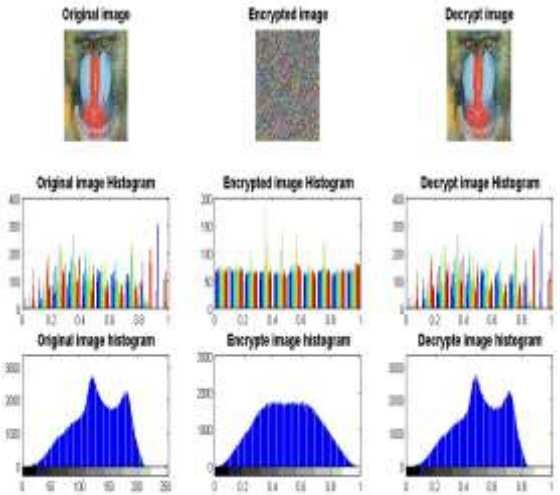


Fig. 9: Histogram of Mandrill image Blue color component

In Figure 8, the histograms of the three channels R, G and B of the encrypted image are uniformly disturbed compared to the other channels of the original image, Thus the encryption algorithm used shows the dependence of the statistical properties of the images encrypted and original images is almost random, hence cryptanalysis is very difficult.

This is also checked for white and black images in Figure 7.

According to Figure 9, it should be noted that the original image and the decrypted image have the same histogram, which can be explained by the performance of our approach.

### 3.3 Analysis by Correlation

Plain images usually are redundant in the spatial domain, which means that adjacent pixels are highly correlated. Whereas, in cipher images, such a correlation should be broken. To measure the correlation between adjacent pixels, we calculated correlation coefficients as below:

$$\rho_{x,y} = \frac{E((x-E(x))(y-E(y))}{\sigma_x \sigma_y} \quad (3)$$

The x and y are pixel vectors of the same length. The $E(x)$ and $E(y)$ are their arithmetic mean values, and the $\sigma_x$ and $\sigma_y$ are their standard deviations. The range of correlation coefficients is [-1, 1]. If x and y are not correlated, $\rho_{x,y}$ shall be close to 0. See the next table, Table 1, of correlation coefficients:

Table 1. Correlation coefficients

| ID | Size (ko) | Original Image Correlation | | | Encryption Image Correlation | | | Decryption Image Correlation | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | | H-V | H-D | V-D | H-V | H-D | V-D | H-V | H-D | V-D |
| 1 | 769 | 0.8786 | 0.6764 | 0.9106 | -0.0013 | 0.0007 | 0.0009 | 0.8786 | 0.6764 | 0.9106 |
| 2 | 768 | 0.3565 | 0.1237 | 0.8074 | -0.0026 | 0.0012 | 0.0019 | 0.3565 | 0.1237 | 0.8074 |
| 3 | 768 | 0.2752 | 0.3952 | 0.8379 | 0.0002 | 0.0018 | 0.0046 | 0.2752 | 0.3952 | 0.8379 |
| 4 | 15.2 | 0.8830 | 0.7013 | 0.9189 | 0.0067 | -0.0002 | -0.0005 | 0.8830 | 0.7013 | 0.9189 |
| 5 | 36.9 | 0.8863 | 0.7028 | 0.9180 | -0.0007 | 0.0018 | 0.0015 | 0.8863 | 0.7028 | 0.9180 |
| 6 | 32.1 | 0.8843 | 0.6952 | 0.9173 | -0.0002 | -0.0018 | 0.0013 | 0.8843 | 0.6952 | 0.9173 |
| 7 | 192 | 0.6378 | 0.4823 | 0.9418 | -0.0053 | 0.0012 | 0.0045 | 0.6378 | 0.4823 | 0.9418 |
| 8 | 768 | 0.4753 | 0.2939 | 0.4201 | 0.0009 | 0.0032 | 0.0001 | 0.4753 | 0.2939 | 0.4201 |
| 9 | 191 | 0.8775 | 0.6791 | 0.9169 | 0.0041 | -0.0001 | -0.0014 | 0.8775 | 0.6791 | 0.9169 |
| 10 | 610 | 0.5759 | 0.3751 | 0.5282 | -0.0023 | 0.0013 | 0.0022 | 0.5759 | 0.3751 | 0.5282 |
| 11 | 768 | 0.8788 | 0.6755 | 0.9119 | -0.0016 | 0.0002 | 0.0011 | 0.8788 | 0.6755 | 0.9119 |
| 12 | 121 | 0.5387 | 0.3421 | 0.9242 | -0.0094 | 0.0044 | 0.0035 | 0.5387 | 0.3421 | 0.9242 |
| 13 | 768 | 0.3565 | 0.1237 | 0.8074 | -0.0026 | 0.0012 | 0.0019 | 0.3565 | 0.1237 | 0.8074 |
| 14 | 389 | 0.1661 | 0.2121 | 0.5228 | -0.0027 | -0.0011 | -0.0005 | 0.1661 | 0.2121 | 0.5228 |
| 15 | 768 | 0.2752 | 0.3952 | 0.8379 | 0.0002 | 0.0018 | 0.0046 | 0.2752 | 0.3952 | 0.8379 |

According to the Table 1, the pixels of the original image and those of the decrypted image are strongly correlated, while the pixels of the encrypted image are uncorrelated because their correlation

coefficients are almost zero. We can say that the proposed encryption algorithm makes plus cryptanalysis more difficult.

### 3.4 Information Entropy

Information entropy was proposed by C. E. Shannon, which is a measure of the randomness of information. For a digital image, it is difficult to predict the content if its information entropy is high. The formula for calculating the entropy of information is given in equation (4). The ideal value of a cipher image's information entropy is its bit-depth d. In Table 2, the information entropy of plain images cipher images and decrypt images are listed:

$$H(m) = -\sum_{i=1}^{L} p(m_i)\log_2(p(m_i)) \quad (4)$$

Table 2. Entopy

| ID | Size (ko) | Original Image Entropy | Encryption Image Entropy | Decryption Image Entropy |
|---|---|---|---|---|
| 1 | 121 | 7.0907 | 7.9958 | 7.0907 |
| 2 | 768 | 6.8657 | 7.9974 | 6.8657 |
| 3 | 691 | 7.5459 | 7.9993 | 7.5459 |
| 4 | 1009 | 7.2176 | 7.9993 | 7.2176 |
| 5 | 432 | 7.5148 | 7.9994 | 7.5148 |
| 6 | 429 | 7.6336 | 7.9991 | 7.6336 |
| 7 | 8.02 | 0.8829 | 7.9859 | 0.8829 |
| 8 | 64.8 | 7.5785 | 7.9955 | 7.5785 |
| 9 | 192 | 7.4444 | 7.9985 | 7.4444 |
| 10 | 192 | 6.9047 | 7.9970 | 6.9047 |
| 11 | 192 | 7.4444 | 7.9985 | 7.4444 |
| 12 | 13.1 | 3.5335 | 7.9791 | 3.5335 |
| 13 | 64.8 | 7.5902 | 7.9956 | 7.5902 |
| 14 | 132 | 7.3946 | 7.9996 | 7.3946 |
| 15 | 256 | 7.0480 | 7.9983 | 7.0480 |
| 16 | 512 | 3.8764 | 7.7954 | 3.8764 |
| 17 | 64.2 | 7.4429 | 7.9953 | 7.4429 |
| 18 | 256 | 7.4451 | 7.9988 | 7.4451 |
| 19 | 256 | 7.2925 | 7.9991 | 7.2925 |
| 20 | 512 | 4.3812 | 7.7949 | 4.3812 |

The values of the entropy of the encrypted images are almost equal to 8, it is indeed the theoretical value, which proves the uniformity of the histograms of the encrypted images, hence the resistance of our approach to attacks by entropy.
In addition the entropy of the original image is equal to that of the decrypted image so we do not lose information on the original image.

### 3.5 Analysis of Embedded Capacity and PSNR

In this subsection, we will select 19 8-bit grayscale images with different sizes to display the experimental results under a table. At the same time, an objective assessment is carried out through: analysis of the on-board capacity; the peak signal noise ratio (PSNR) and safety analysis.

In order to measure the processed image quality, we usually refer to PSNR value for objective evaluation, MSE is the expected value of the square of the difference between the original image and the processed image, as is shown in the Eq. (5) and Eq. (6).

$$MSE = \frac{1}{nm}\sum_{i,j}(m(i,j) - img(i,j))^2 \quad (5)$$

$$PSNR = 10log_{10}\left(\frac{65025}{MSE}\right) \quad (6)$$

Where $nm$ the size of the image, m(i, j) pixel value of the original image and img(i, j) pixel value of the crypt image. The results obtained are collated in Table 3:

Table 3. Crypt image MSE and PSNR

| ID | Size (ko) | MSE | PSNR |
|---|---|---|---|
| 1 | 121 | 1.7835e+004 | 5.6521 |
| 2 | 768 | 1.2360e+004 | 7.2446 |
| 3 | 691 | 1.7683e+004 | 5.6892 |
| 4 | 1009 | 1.5032e+004 | 6.3947 |
| 5 | 432 | 9.7515e+003 | 8.2741 |
| 6 | 429 | 1.8634e+004 | 5.4619 |
| 7 | 64.8 | 1.2367e+004 | 7.2421 |
| 8 | 192 | 1.7170e+004 | 5.8171 |
| 9 | 192 | 3.2404e+004 | 3.0588 |
| 10 | 192 | 1.7170e+004 | 5.8170 |
| 11 | 13.1 | 1.2368e+004 | 7.2419 |
| 12 | 64.8 | 1.4267e+004 | 6.6214 |
| 13 | 132 | 1.1206e+004 | 7.6704 |
| 14 | 256 | 1.7725e+004 | 5.6790 |
| 15 | 512 | 4.3299e+004 | 1.8000 |
| 16 | 64.2 | 1.7542e+004 | 5.7239 |
| 17 | 256 | 1.7555e+004 | 5.7208 |
| 18 | 256 | 1.7972e+004 | 5.6189 |
| 19 | 512 | 4.0593e+004 | 2.0803 |

According to the results obtained for the values in dB of the PSNR, these values are lower than 13dB, which shows that one obtained a high quality of encryption and that one cannot make a cryptanalysis by a small change in the clear image.

### 3.6 Efficiency

In the proposed scheme, the bit level permutation is performed in a linear time complexity. During this time, the diffusion phase is also linear. If the encrypted image is of size [n, m, p], the time complexity of the algorithm is O(nm). The time complexity of the algorithm in, [8] is also O(mn). However, our bit-level pattern is slower than the pixel-level pattern of, [8]. We can accompany the permutation by a sorting operation. Thus, the efficiency of the scheme was linked to the sorting algorithm adopted.

The efficiency is represented in Figure 10 and the comparison between the encryption time and the decryption time is in Figure 12, this efficiency depends on the size of the image in ko.

To know the histogram of time, we can see the representation Figure 11.


Fig. 10: The polygon of time

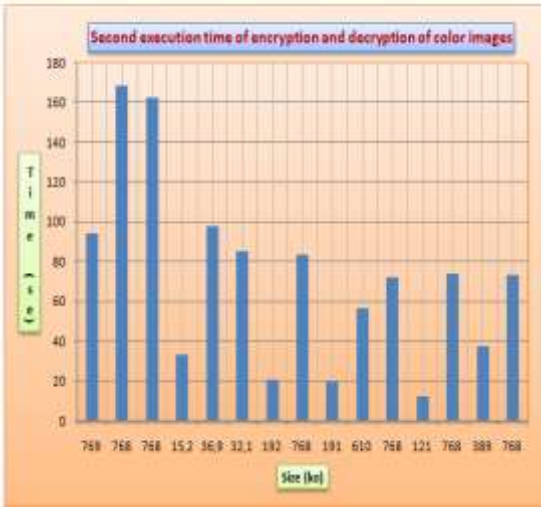


Fig. 11: The histogram of time

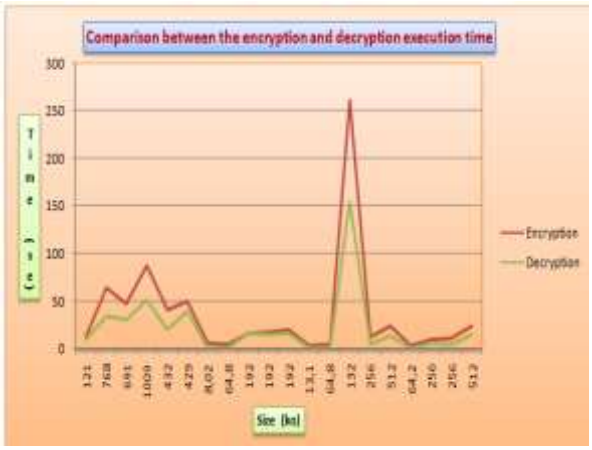


Fig. 12: Comparison of time

Experience in an elliptic curve cryptographic environment, we use an 80-bit security level, processing on an Intel i7 3.07 GHz machine. The time required for a task is as follows: 3.21ms.

In the chaotic environment, the time spent by the same task is as follows: 4.5ms.

We prove that the proposed scheme is much more profitable than the other existing schemes in, [9], [10], [11] and [12], while these schemes are also signature schemes.

The execution time of the encryption is equal to that of the decryption by adding the construction time of the secret encryption matrix to it.

## 4 Conclusion

In this article, the secret data is integrated into the encrypted image by building a secret encryption matrix. This scheme not only makes it possible to realize that the secret data can be extracted in clear text and in encrypted text, but also that the capacity of integration is increased on the basis of the guarantee that the original image is completely restored. At the same time, the algorithm is used for self-integration, which improves the PSNR value. The main contributions of this document are summarized as follows:

1. Improved integration capacity.
2. By homomorphic property, secret data can be extracted in the field of plain text and encrypted text.
3. At the same time, the diagram uses a block strategy and the correlation within the block.

*Acknowledgement:*
The authors gratefully acknowledge the helpful comments and suggestions of the reviewers.

*References:*

[1] Diffie, W., Hellman, M., "New directions in cryptography", *IEEE Transactions on Information Theory*, 1976.

[2] Zeriouh, M., Chillali, A., Boua, A., "Cryptography Based on the Matrices", *Bol. Soc. Paran. Mat.,* 37(3), pp.75–83, 2019.

[3] Hua, Z.Y., Zhou, Y.C., Pun, C.M., Chen, C.L.P, "2D sine logistic modulation map for image encryption", *Inf. Sci.*, 297, 80–94, 2015.

[4] Moha Ben Taleb, E., Grini, A., Chillali, A., El FadilE, "El Gamal Cryptosystem on a Montgomery Curves Over Non Local Ring", WSEAS Transactions on Mathematics, Vol. 21, 2022, pp. 85-89, https://doi.org/10.37394/23206.2022.21.13.

[5] ELHASSANI, M,. CHILLALI, A,. MOUHIB, A,. "A heuristic method to approximate the closest vector problem", WSEAS Transactions on Mathematics, Vol. 20, 2021, pp. 745-755, https://doi.org/10.37394/23206.2021.20.79.

[6] Cheddour, Z., Chillali, A., Mouhib, A.,"Elliptic curves over a finite ring", Annals of the University of Craiova, *Mathematics and Computer Science Series*, Vol. 50(2), 2023, Pages 313–324.

[7] Chillali, S., Oughdir, L., ―ECC Image Encryption using System Generator, *Journal of Theoretical and Applied Information Technology*, Vol. 100, No. 15, 5419- 5425, 2022.

[8] Zhang, Y, "The unified image encryption algorithm based on chaos and cubic", *S-Box. Inf. Sci.*, 450, 361–377, 2018.

[9] L. Zhang, F. Zhang, "A New Certificateless Aggregate Signature Scheme", *Comput. Commun.*, Vol 32 (6), 1079-1085, 2009.

[10] H. Xiong, Z. Guan, Z. Chen, F Li, "An Efficient Certificateless Aggregate Signature with Constant Pairing Computation", *Inform. Sci.*, vol 219, pp 225–235, 2014.

[11] D. He, J. Chen, R. Zhang, "An efficient and provably-secure certificateless signature scheme without bilinear pairings", *Int. J. Commun. Syst.*, vol 25, pp 1432–1442, 2012.

[12] A. Karati, SK H Islam, G.P. Biswas "A Pairing-free and Provably Secure Certificateless Signature Scheme", *Information Sciences*, vol. 450, pp 378-391, 2018.

**Contribution of Individual Authors to the Creation of a Scientific Article (Ghostwriting Policy)**

- Sara Chillali carried out the simulation and the cosimulation and has implemented the Algorithm in Matlab Simulink.
- Lahcen Oughdir was also responsible for this Recherch.

The authors equally contributed in the present research, at all stages from the formulation of the problem to the final findings and solution.

**Sources of Funding for Research Presented in a Scientific Article or Scientific Article Itself**

No funding was received for conducting this study.

**Conflict of Interest**

The authors have no conflicts of interest to declare.