Encryption algorithms on BMP and JPEG images

SARA CHILLALI, LAHCEN OUGHDIR
Sidi Mohamed Ben Abdellah University
FP, LSI, TAZA, MOROCCO

Abstract: - In this article we carried out a comparative study between certain encryption algorithms on BMP and JPEG images, we established a comparison between certain types of encryption systems and our algorithm. We made the comparison with data implemented on the same computer and our implementation.

Key-Words: -Image, Algorithm, Encryption, Comparative.

Received: March 16, 2021. Revised: January 7, 2022. Accepted: January 25, 2022. Published: February 18, 2022.

1 Introduction

As you The need for disk space envisaged by the storage or the transmission of a digital image or any other graphic form comprising thousands of bytes and at a rate more than 500 images per day, we let think about the good encryption of this data produced for stokers in a confidential way, without someone being able to see or use them other than those who have the right of access. This problem is supposed to be solved by a few encryption algorithms. In order to prove the performance of our encryption algorithm, we made a comparison between some algorithms already implemented and our.
The comparison will be made on several points and according to certain criteria; (see [4, 5]):

• Type and size of keys.

• The visibility and performance of the encryption operation applied to the image.

• The encryption and decryption time.

• Type and size of images (BMP or JPEG).

• Comparison graph.

For symmetrical systems:

Simple algorithms use any keys.

Secret key algorithms:

- DES (64 bits)
- 3-WAY (96 bit)
- RC5 (128 bit)
- IDEA (128 bit)

On the other hand, asymmetric systems call on arithmetic operations based on finite fields, the factorization of large numbers into two prime numbers, elliptic curves ..., the size of an RSA key of 1024 bits corresponding to a size of 256 bits for elliptical curves.

2 Encryption and Decryption Algorithms

2.1 Problem Formulation

Find a method of encryption and decryption to keep encrypted images without anyone being able to see or use them other than those who have the rights of access to information, add more these methods must be effective and better than the already existing.

2.2 Problem Solution

In our article [1, 2], we established an encryption method based on matrices, in this part we present another method using elliptic curves.
Let $E_{a,b}(p)$ an elliptic curve on the field $\mathbb{F}_p$ where p is a large prime number, such that discrete logarithm problem in $E_{a,b}(p)$ is difficult. [2, 6]
Using a Diffie–Hellman key exchange, see [2, 3], on such a chosen curve we can build a secret key which allows us to generate a secret matrix to encrypt and decrypt our images. Suppose Ali has created such a secret key $K = (x, y)$ and shares it with the people who have the right to access the

encrypted database. Ali wants to stock an image confidentially « img », it follows the structure of the proposed algorithm which consists of five encryption steps, as described by:

- Setp1 :

Turn the image, img into a matrix $M(m_{i,j})$; $m_{i,j} \in \{0,1,2,\dots,255\}$. This matrix is obtained from the transformation of the original image into matrix.

- Setp2 :

For each i $\in \{1,2,\dots,256\}$ calculate : $iK = (x_i, y_i)$

- Setp3 :

Pixel 0 receives the value x_{256},
for i from 1 to 255 do,
pixel i receives the value x_i,
if $x_i = x_j$ is already taken by a pixel $j < i$ then pixel i receives the value y_i, so the pixels $0, 1, \dots, i, \dots, 255$ will be transformed to $z_0, z_1, \dots, z_i, \dots, z_{255}$
where $z_0 = x_{256}$ and for i from 1 to 255, $z_i = x_i$ or y_i

- Setp4 :

In class $z_0, z_1, \dots, z_i, \dots, z_{255}$ in ascending order, the smallest value receives the pixel 0, the next value receives the pixel 1 so on, the last value receives the pixel 255.

- Setp5 :

The bijective function f defined by: $f: \{0,1,2,\dots,255\} \to \{0,1,2,\dots,255\}$; f(i) is the value of the pixel establish in setp4, we transform the matrix $M(m_{i,j})$ by the function f to the matrix $M_f = M(f(m_{i,j}))$.
The matrix M_f, thus constructed represents ; "cryptimg" the encrypted image of "img".

Decryption Algorithm :

A person who wants to use a stored image; "cryptimg" encrypted by Ali, it has the private key which allows it to calculate the reciprocal function of f ; f^{-1} and find the matrix $M = M(f^{-1}(f(m_{i,j})))$, that we can transform it to the image "img".

3 Comparison of the Encryption Quality

To study the performance of the encrypted image, we divide the performance of the encrypted image into four categories, Excellent, Good, Average and Bad, then assign each category a statistical class in the interval form of our choice as follows:

Excellent:=]15,20]; Good:=]12,15]; Way:=]8,12]; and Bad:=]0,8].

3.1. Encryption Len Image

In this sub-section, we present the results of the encrypted images obtained from different types of standard Lena image, the results are presented as follows:

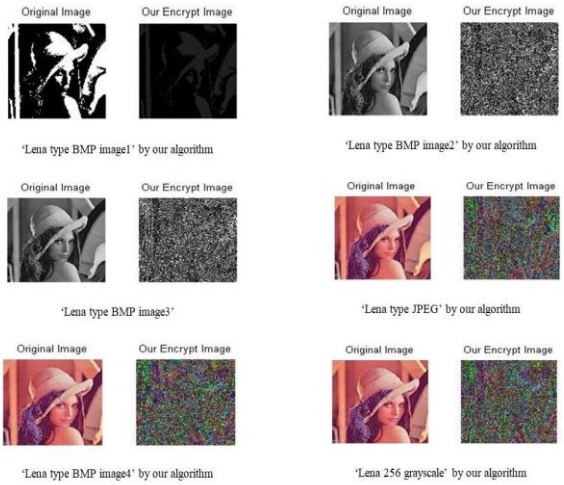

Fig.1: Encrypt Lena Image by our Algorithm

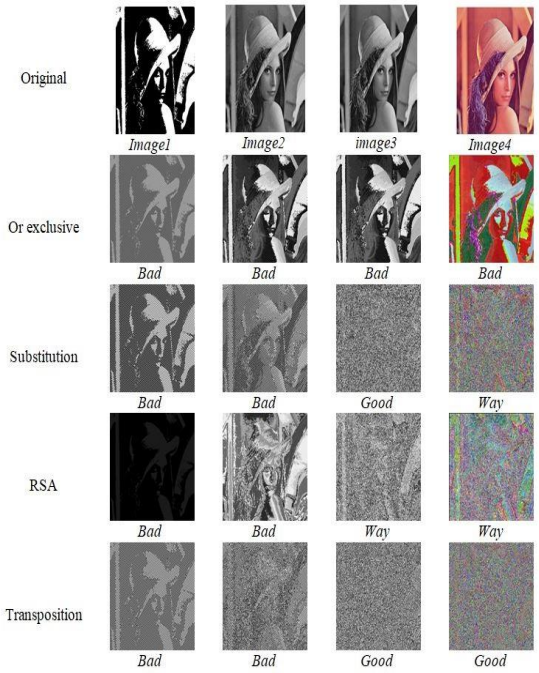

Fig. 2: Encrypt Lena Image by various Algorithms

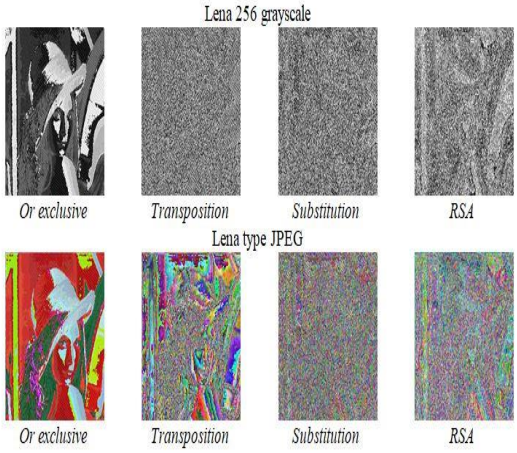

Fig. 3: Encrypt Lena (type) by various Algorithms

3.2 Results Interpretation

The results of the performance of the encrypted image are grouped in the following table:

Table 1. Performance of the encrypted image

Encryption method	Image 1 2 NG	Image 2 16N G	Image 3 256 NG	Image 4 Colo r	Lena JPE G	Lena 256 grays cale
our method	]15,20]	]15,20]	]15,20]	]15,20]	]15,20]	]15,20]
or exclusive	]0,8]	]0,8]	]0,8]	]0,8]	]0,8]	]0,8]
substitution	]0,8]	]8,12]	]15,20]	]15,20]	]0,8]	]8,12]
RSA	]0,8]	]0,8]	]8,12]	]8,12]	]8,12]	]12,15]
transposition	]0,8]	]0,8]	]8,12]	]12,15]	]8,12]	]0,8]

Let X be the mean of this performance, which we will calculate for each algorithm and then conclude the performance of each algorithm from the interval where X belongs, the results are gathered in this table which follows:

Table 2. Mean : X

Encryption method	X	Performance
our method	17,5 ∈]15,20]	Excellent
or exclusive	4 ∈]0,8]	Bad
substitution	10,5 ∈]8,12]	Way
RSA	8,58 ∈]8,12]	Way
transposition	7,58 ∈]0,8]	Bad

3.3 Interpretation

- The quality of the image encryption operation by our secret key encryption algorithm is better compared to conventional encryption algorithms such as transposition, substitution, or exclusive and RSA.
- The higher the gray level, the better the quality for encryption.
- The quality of the image encryption operation by our secret key encryption algorithm is better compared to conventional encryption algorithms such as transposition, substitution, or exclusive and RSA.

4 Comparison of Execution Times of Different Algorithms

We will do a calculation of the encryption and decryption time between these different encryption algorithms, then give an interpretation of the results obtained, also increasing the size of the image to be encrypted ; noted that 1 Ko = 8000 bit, which is what we get for this encryption time. The results are grouped in the following tables:

Table 3. The encryption time in seconds

Encryption method	Image 64×64 (12 Ko)	Image 128×128 (48Ko)	Image 256×256 (192 Ko)	Image 512×512 (768Ko)
Our method	0.010	0.085	0.125	0.677
or exclusive	0.028	0.176	0.625	1.641
substitution	0.028	0.185	0.625	1.656
RSA	0.052	0.453	0.877	2.937
transposition	0.028	0.185	0.625	1.677

Table 4. The decryption time in seconds

Decryption method	Image 64×64 (12Ko)	Image 128×128 (48 Ko)	Image 256×256 (192Ko)	Image 512×512 (768Ko)
Our method	0.010	0.085	0.125	0.677
or exclusive	0.060	0.192	0.625	1.641
substitution	0.062	0.203	0.630	1.676
RSA	0.092	0.520	0.911	3.256
transposition	0.062	0.203	0.630	1.677

Remark:

According to the results obtained in the calculation of encryption and decryption time between these different encryption algorithms, we remark that:

- The encryption algorithms like transposition, substitution and RSA are slower than our encryption algorithm.
- Note also that each time increases in the size of the image to be encrypted, obtains a greater encryption time.
- In the comparison between the two encryption and decryption tables, note that the encryption time and faster compared to the decryption time in these algorithms except in our algorithm where we have the equality of the two times.

Open Problem :
Find an encryption algorithm for images better than existing algorithms and rank existing algorithms according to their efficiency.

5 Conclusion

In this study, the ECC image encryption technique was proposed. Thus, the effectiveness of this type of encryption was studied and we established a comparison between certain types of encryption systems and our algorithm.

References:

[1] Chillali, S., Oughdir, L.," A diagram of confidentiality of information during a traffic offence", AIP Conference Proceedings, Volume 2074, Issue 1, id.020028, (2019).
[2] Chillali, S., Oughdir, L., "ECC Image Encryption Using Matlab Simulink Blockset", Lecture Notes in Networks and Systems, 2021, 211 LNNS, pp. 835–846, DOI: 10.1007/978-3-030-73882-2_76
[3] Diffie, W., Hellman, M.,"New directions in cryptography", IEEE Transactions on Information Theory, (1976).
[4] Keinert, J., Teich, J.,"Design of Image Processing Embedded Systems Using Multidimensional Data Flow", Springer New York, (2011).
[5] Haouzia, A., Noumei, R.,"Methods for image authentication: a survey", Multimed Tools Appl. 39(146), (2008).
[6] Silverman, J.,'The Arithmetic of Elliptic Curves', Graduate Texts in Mathematics, Springer, (2009).