Symmetric Image Encryption using Scrambling Technique Based on Matrix Reodering Coding

Mamy Alain Rakotomalala[1*], Falimanana Randimbindrainibe[2], Sitraka R. Rakotondramanana[3]
Department of Telecommunication, High School Polytechnic of Antananarivo, University of Antananarivo, Madagascar
Department of Telecommunication, High School Polytechnic of Antananarivo, University of Antananarivo, Madagascar
Department of Telecommunication, High School Polytechnic of Antananarivo, University of Antananarivo, Madagascar

Abstract

For having performance of image security, the good option is using combination between the ciphering and steganography. The ciphering protect the information to the person with bad intention and the steganography facilitate the transmission of the secret key. The scrambling technique could a candidate of the ciphering algorithm. The zigzag pattern has 8 variant and could be used for it. For that, we invent a new algorithm based on key coding the scrambling technique based on matrix reordering. For the first approach, we use scrambling methods separately with all component RGB and 15bits of key repartitioning like this : 3bits for the repetitively order t of scrambling color, 3bits for the colors scrambling, 3bits for the pixel scrambling techniques of Red, 3bits for the pixel scramblingtechniques of Green, 3bits for the pixel scrambling techniques of Blue. After the simulation on Matlab, the result confirm that it has a good performance on correlation, PSNR, UACI, NPCR and histogram but one bit error doesn't modify so much the deciphering image comparing the original image. To avoid this, we prefer to use scrambling methods at all the component of the image and use 9bits of key like : repartitioning like this: 3bits of repetitively order of scrambling, 3bits of scrambling color for all component of image, 3bits of scrambling pixels techniques. The two approaches for the ciphering, steganography and deciphering are simulated, evaluated, and interpreted in this article.

Keywords: *Ciphering, scrambling, Steganography, Zigzag, Key.*

I. INTRODUCTION

The ciphering is technique used to protect the information for person with bad intention and steganography is technique used to hide discreetly information in other information. On image, it is possible to use symmetric key for ciphering combining with steganography for the transmission of the key. For the ciphering, it is possible use scrambling methods with more variant and code it following a generated secret key. The good option of that is the zigzag , it has 8 variants of patterns.

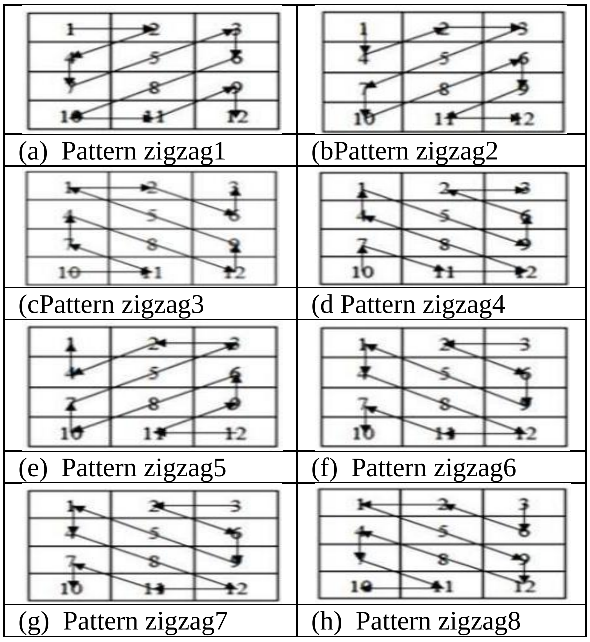
II. GENERALITY OF IMAGE SCRAMBLING

The scrambling is a technique used to make an image unknown, unidentified and confused. Some research and works [1-4]try to define and talk about scrambling and the different scrambling technique.

The scrambling of image uses two blocks: the scrambling of pixels position (pixels scrambling) and the scrambling of the value of the pixels (color scrambling).

A. Pixels scrambling

It is a matrix reorganization transforming the image position in the 2 dimensional spaces with defined pattern. The image is represented in 2 dimensions m*n and has 3 fundamental colors: Red Green Blue which are coded 8 bits each.



(a) Pattern zigzag1 (bPattern zigzag2 (cPattern zigzag3 (d Pattern zigzag4 (e) Pattern zigzag5 (f) Pattern zigzag6 (g) Pattern zigzag7 (h) Pattern zigzag8

Figure 1:*Different patterns of zigzag*

Using this method, abscissa indices and ordinate indices of original image are improved by the selects indices of the pattern and formed a confused image comparing to the original image. In this article, we only use eight zigzag patterns represented in figure 1 [4-12].

If we take the pattern zigzag_1:
By using linearization, the calculation of this linearized position will be derived from the original image M having size m*n.

$$C(p,q) = \frac{1+(-1)^{p+q}}{2}\left[\frac{(p-1+q)(p-2+q)}{2}+q\right]+\frac{1-(-1)^{p+q}}{2}\left[\frac{(p-1+q)(p-2+q)}{2}+p\right] \quad (1)$$

C(p,q) is the position of the linear index of abscissa and ordinate of the original image.
p, q is the index of abscissa between 1 and m; of ordinate between 1 à and n of the original image
So the index of abscissa and ordinate issued from the linear position if the scrambled image with the zigzag is noted V has its formula like this:

$$c(p,q) = V(p_{permute}, q_{permute}) \rightarrow C(p,q) =$$
$$= m * p\_permute + q\_permute \quad (2)$$

C(p,q) is the position of the linear index of abscissa and ordinate of the original image.
p, q is the index of abscissa between 1 and m; of ordinate between 1 à and n of the original image

V is the scrambled image by zigzag path.

p_permute, q_permute is the position of the linear index of abscissa and ordinate of the scrambled image

The index of the scrambled image is calculated by the formula (3) after using the formula (2):

$$\begin{cases} \forall p \in [1;m]; \forall q \in [1;n]; q\_permute = \mathrm{mod}(C(p,q),n) \\ \forall p \in [1;m]; \forall q \in [1;n]; p\_permute = \dfrac{C(p,q) - q\_permute}{m} \end{cases} \quad (3)$$

C(p,q) is the position of the linear index of abscissa and ordinate of the original image.

p, q is the index of abscissa between 1 and m; of ordinate between 1 à and n of the original image

p_permute, q_permute is the position of the linear index of abscissa and ordinate of the scrambled image

The Formula 1 could be simplified by putting *A=p+q and B=p-q* :

$$C(p,q) = \frac{1}{2}\left[(p+q)^2 + (-1)^{p+q-1}(p-q)+1\right] = \frac{1}{2}\left[(A)^2 + (-1)^{A-1}B+1\right] \quad (4)$$

C(p,q) is the position of the linear index of abscissa and ordinate of the original image.
p, q is the index of abscissa between 1 and m; of ordinate between 1 à and n of the original image.
A is *p+q;*

B is *p-q.*

For the classical zigzag, the transformation could be done in affecting the new position to the original position in the scrambled image and the original image:

$$\begin{cases} \forall p\_permute \in [1;m]; \\ \forall q\_permute \in [1;n]; \\ \forall k \in [1;3]; \\ V(p\_permute, q\_permute, k) = V(p,q,k) \\ \forall p \in [1;m]; \forall q \in [1;n]; q\_permute = mod(C(p,q),n) \\ \forall p \in [1;m]; \forall q \in [1;n]; p\_permute = \dfrac{C(p,q)-q\_permute}{m} \\ \forall p \in [1;m]; \forall q \in [1;n]; C(p,q) = \\ \frac{1}{2}[(p+q)^2+(-1)^{p+q-1}(p-q)+1] \end{cases} \quad (5)$$

M is the original image with the size m*n
C(p,q) is the position of the linear index of abscissa and ordinate of the original image.
p, q is the index of abscissa between 1 and m; of ordinate between 1 à and n of the original image
V is the scrambled image
p_permute, q_permute is the position of the linear index of abscissa varying between 1 and m and the index of ordinate varying between 1 and n in the scrambled image
k is the fundamental color image : 1 for Red, 2 for Green et 3 for Blue.
With the same approach, we can determine the mathematic model for other pattern zigzag.
The appellation of the pixel scrambling function for the pattern zigzag1 is "pattern_zigzag_1". The appellations for other zigzag path are done with the same process.

B. The color scrambling

To improve the classic zigzag, the fundamental colors Red Green Blue should be changed [4, 13-19]. In order to change only the position of the pixels at the same time, the value of these pixels is also changed by using a xor operator following this formula:

$$\begin{cases} \forall p\_permute \in [1;m]; \\ \forall q\_permute \in [1;n]; \\ V(p\_permute, q\_permute, 1) = \\ bitxor\left(M(p,q,1), p * \frac{256}{n}\right) \\ V(p\_permute, q\_permute, 2) = \\ bitxor\left(M(p,q,2), p * \frac{256}{m}\right) \\ V(p\_permute, q\_permute, 3) = \\ bitxor\left(M(p,q,3), (p+q) * \frac{256}{m+n}\right) \\ \forall p \in [1;m]; \forall q \in [1;n]; q\_permute = mod(C(p,q),n) \\ \forall p \in [1;m]; \forall q \in [1;n]; p\_permute = \dfrac{C(p,q)-q\_permute}{m} \\ \forall p \in [1;m]; \forall q \in [1;n]; C(p,q) = \\ \frac{1}{2}[(p+q)^2+(-1)^{p+q-1}(p-q)+1] \end{cases} \quad (6)$$

M is the original image with the size m*n
C(p,q) is the position of the linear index of abscissa and ordinate of the original image.
p, q is the index of abscissa between 1 and m; of ordinate between 1 à and n of the original image
V is the scrambled image.
p_permute, q_permute is the position of the linear index of abscissa varying between 1 and m and and the index of ordinate between 1 and n of the scrambled image.
The fundamental colors Red Green Blue are scrambled by using bitxor with $p*256/n$; $q*256/m$ et $(p+q)*256/(m+n)$.
With the same approach than the color scrambling for the pattern_zigzag_1, we can determine the color scrambling for other pattern zigzag.
The appellation of the color scrambling of pattern_zigzag_1 is "zigzag_color1". The appellations for other zigzag path are done with the same process.

C. Repetitively order t

To ameliorate the result of scrambling technique, and to resolve the prediction problem, the process is not limited for only one transformation that for many composition of transformation. With (t-1)composition of transformation, we will get the repetitively order value t.

$$\Gamma_t = \underbrace{\sigma_t \circ \sigma_{t-1} \circ \ldots \circ \sigma_1}_{(t-1)-répétition} \qquad (7)$$

« o » : the composition operator of 2 transformations.

During the scrambling process inverse, we can recuperate the original image.

$$\Gamma_t^{-1} = \underbrace{\sigma_t^{-1} \circ \sigma_{t-1}^{-1} \circ \ldots \circ \sigma_1^{-1}}_{(t-1)-répétition} = \underbrace{\sigma_1^{-1} \circ \sigma_2^{-1} \circ \ldots \circ \sigma_t^{-1}}_{(t-1)-répétition} \qquad (8)$$

III. PROPOSED SYMMETRIC ENCRYPTION ALGORITHM BASED ON SCRAMBLING TECHNIQUE

The proposed algorithm is based oncoding the scrambling technique using zigzag path with the repetitively order "t" for all image and scrambling of pixels for all component of the image and finally the steganography for inserting the key of ciphering in the ciphered image. In this article, we use symmetric ciphering. So the key of ciphering is the same as the key of deciphering.

A. Proposed Steganography algorithm

The steganography [20-22]: is the art of dissimulation for passing the secret message discreetly on the other message. The secret message is the ciphering key and the key insertion could be done in the ciphered image with size M*N.

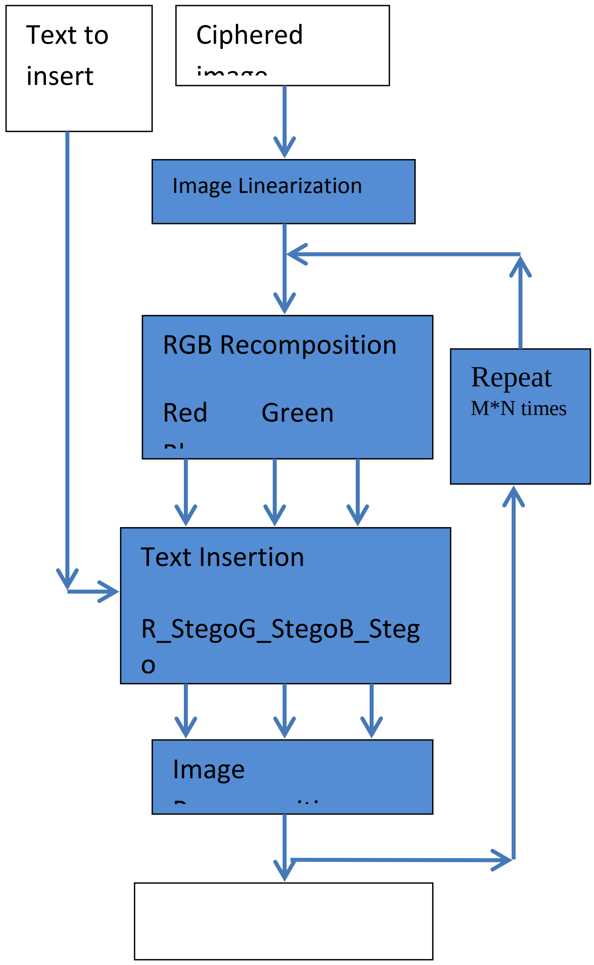


Figure 2:Proposed Steganography algorithm

The inverse operation consists to recuperate the ciphering key for doing the deciphering algorithm.

The goal of steganography in this algorithm is to insert the file text element contains the key in the file image by not so modifying the appearance of the image and also by recuperating the key at the reception. The steganography is described at the schema bloc on the Figure 2.The linearization of the image consists to transform the image 2D with size [M, N] to be a linearized matrix with size M*N.

- The RGB Decomposition consists to separate the fundamentals colors: Red Green and Blue.
- The text insertion has like goal to insert the text by not so modifying the image RGB by considering the following conditions :

$$\begin{cases} R\_stego = bitand(redc, 248); \\ G\_stego = bitand(greenc, 248); \\ B\_stego = bitand(bluec, 252); \end{cases}$$

$$\begin{cases} if(\text{bitand}(\text{text},128) == 128) alors\ R\_stego = \text{bitor}(R\_stego,4) \\ if(\text{bitand}(\text{text},64) == 64) alors\ R\_stego = \text{bitor}(R\_stego,2) \\ if(\text{bitand}(\text{text},32) == 32) alors\ R\_stego = \text{bitor}(R\_stego,1) \\ if(\text{bitand}(\text{text},16) == 16) alors\ G\_stego = \text{bitor}(G\_stego,4) \\ if(\text{bitand}(\text{text},8) == 8) alors\ G\_stego = \text{bitor}(G\_stego,2) \\ if(\text{bitand}(\text{text},4) == 4) alors\ G\_stego = \text{bitor}(G\_stego,1) \\ if(\text{bitand}(\text{text},2) == 2) alors\ B\_stego = \text{bitor}(B\_stego,2) \\ if(\text{bitand}(\text{text},1) == 1) alors\ B\_stego = \text{bitor}(B\_stego,1) \end{cases}$$

For recuperating the text in the stego_ciphered_image, the formula should respect the following conditions:

$$\begin{cases} \text{if}(\text{bitand}(R\_stego,4) == 4) alors\ (\text{txt} = \text{bitor}(\text{txt},128)) \\ \text{if}(\text{bitand}(R\_stego,2) == 2) alors\ (\text{txt} = \text{bitor}(\text{txt},64)) \\ \text{if}(\text{bitand}(R\_stego,1) == 1) alors\ (\text{txt} = \text{bitor}(\text{txt},32)) \\ \text{if}(\text{bitand}(G\_stego,4) == 4) alors\ (\text{txt} = \text{bitor}(\text{txt},16)) \\ \text{if}(\text{bitand}(G\_stego,2) == 2) alors\ (\text{txt} = \text{bitor}(\text{txt},8)) \\ \text{if}(\text{bitand}(G\_stego,1) == 1) alors\ (\text{txt} = \text{bitor}(\text{txt},4)) \\ \text{if}(\text{bitand}(B\_stego,2) == 2) alors\ (\text{txt} = \text{bitor}(\text{txt},2)) \\ \text{if}(\text{bitand}(B\_stego,1) == 1) alors\ (\text{txt} = \text{bitor}(\text{txt},1)) \end{cases}$$

B. *Criteria of evaluation*

The image to be treated is lena.jpg with size 256x256x3.

The following results are obtained by the Matlab simulation. The criteria used for this article are: PSNR (Peak Signal to Noise Ratio), SSIM (Structural SIMilarity), NPCR (Number of Pixel change rate), UACI (Unified Average Changing Intensity), rxy (correlation coefficient).

Le PSNR [4, 24] is used to measure the distortion of the numeric image. Le PSNR is defined by the following Formula :

$$PSNR = 10.\log_{10}\left(\frac{d^2}{RMSE}\right) \quad (9)$$

d is the maximum value of the pixel. In general case, d=255

RMSE or the Root Mean-Square Error for 2 images I_0 and I_r with size m×n is defined by:

$$EQM = \frac{1}{mn}\sum_{i=0}^{m-1}\sum_{j=0}^{n-1}(I_0(i,j) - I_r(i,j))^2 \quad (10)$$

$I_0(i, j)$ is the value of the coordinates (i, j) of the image I_0 ; $I_r(i, j)$ is the value of the coordinates (i, j) of the image I_r .

❖ The Structural Similarity or SSIM [4, 24] is a reliable measure of the similarity between two numeric images.

$$SSIM(X,Y) = \frac{(2\mu_X\mu_Y + c_1)(2\sigma_X\sigma_Y + c_2)(2COV(X,Y) + c_3)}{(\mu_X^2 + \mu_Y^2 + c_1)(\sigma_X^2 + \sigma_Y^2 + c_2)(\sigma_X\sigma_Y + c_3)} \quad (11)$$

μ_X , μ_Y is the average value of the random variable X, Y; σ_X^2 , σ_Y^2 is the variance of X, Y; $COV(X,Y)$ is the covariance of X and Y; c_1 , c_2 , c_3 are 3 values to stabilize the division when the value is too small.

❖ The NPCR [4, 25]measure the difference rate between two images. The NPCR formula is given by :

$$NPCR^{R/G/B} = \frac{\sum_{i=1}^{H}\sum_{j=1}^{W} D^{R/G/B}_{i,j}}{W \times H} 100\% \quad (12)$$

With

$$D^{R/G/B}_{i,j} = \begin{cases} 0 & si \quad C^{R,G,B}_{i,j} = \overline{C}^{R,G,B}_{i,j} \\ 1 & si \quad C^{R,G,B}_{i,j} \neq \overline{C}^{R,G,B}_{i,j} \end{cases} \quad (13)$$

$C^{R,G,B}_{i,j}$ and $\overline{C}^{R,G,B}_{i,j}$ represent the components RGB with the two images

$$L^{R/G/B} = 8$$

W and *H* represent the Width and Height of image.

❖ L'UACI [4, 25] is the Unified Average Changing Intensity between two images.

$$UACI^{R/G/B} = \frac{1}{W \times H}\sum_{i=1}^{H}\sum_{j=1}^{W}\frac{C^{R/G/B}_{i,j} - \overline{C}^{R/G/B}_{i,j}}{2^{L^{R/G/B}} - 1} \times 100\% \quad (14)$$

❖ The coefficient of correlation [4,23] is defined by :

$$r_{X,Y} = \frac{COV(X,Y)}{\sqrt{V(X).V(Y)}} = \frac{COV(X,Y)}{\sigma_X\sigma_Y} \quad (15)$$

COV(X,Y) is the covariance between two random variables X andY; $V(X), V(Y)$ is the variance between de X and Y; σ_X, σ_Y is the standard deviation between X and Y.

The covariance is equal to the expectation between the products of the standardised random variable. It is defined by the following formula:

$$COV(X,Y) = E[(X - E[X])(Y - E[Y])] \quad (16)$$

E is the mathematical expectation; X, Y is a random variable.

The variance is defined by the following formula:

$$V(X) = E[(X - E[X])^2] = COV(X,X) \quad (17)$$

E is the mathematical expectation; COV the covariance.

The goal of the covariance is to quantify the liaison between two random variablesX, Y, for theliaison sense and intensity. The coefficient of simple linear correlation, says Bravais-Pearson is a normalized covariance by the product between the two standard deviations. The correlation is between -1 and 1.Near the extreme value -1 and 1, the similarity between the two variables is important. The expression « intensive correlation » means that two variables are very similar and the correlation is near the value 1.The expression « linear independent » or « no correlation » means that the correlation between two variables is nil and there is no similarity between them. The expression « perfect correlation » means that the value $r_{xy}$is equal to ± 1 .

C. Approach 1

This approach is described on the Figure 3 andthe key structure is described on the Table 1.

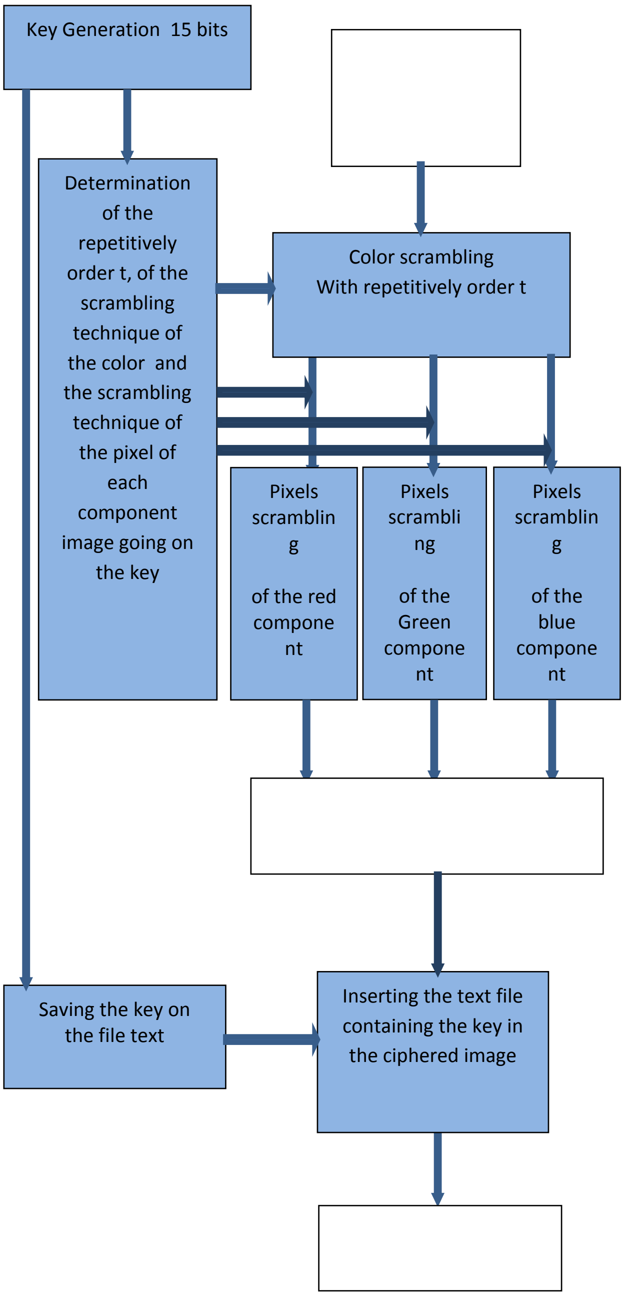


Figure 3:Approach 1 algorithm

We use 15bits of key like 3bits is the choice of the repetitively order of the scrambling technique, 3bits is the choice of the scrambling technique used of the color, 3bits for describing the scrambling technique with the pixel emplacement with different path on the image component. The following code is described on the Table 1.

Table1:(a) Key structure using the approach 1 (b) key signification

(a)

3 bits	3 bits	3 bits	3 bits	3 bits

(b)

3 bits	Repetitively order **t**of scrambling color
3 bits	Color scrambling Techniques
3 bits	Pixels scrambling Techniques to Red component
3 bits	Pixels scrambling Techniques to Green component
3 bits	Pixels scrambling Techniques to Blue component

Tableau 2:Code used (a) Repetitively order t of the scrambling,(b) scrambling color technique, (c) Scrambling technique based on the confusion of the pixel emplacement and different paths

(a)

Code	Repetitively order**t**of the scrambling
000	1
001	2
010	3
011	4
100	5
101	6
110	7
111	8

(b)

Code	Color scrambling Techniques
000	zigzagcolor_1
001	zigzagcolor_2
010	zigzagcolor_3
011	zigzagcolor_4
100	zigzagcolor_5
101	zigzagcolor_6
110	zigzagcolor_7
111	zigzagcolor_8

(c)

Code	Pixels scrambling Techniques to different component
000	Pattern_zigzag_1
001	Pattern_zigzag_2
010	Pattern_zigzag_3
011	Pattern_zigzag_4
100	Pattern_zigzag_5
101	Pattern_zigzag_6
110	Pattern_zigzag_7
111	Pattern_zigzag_8

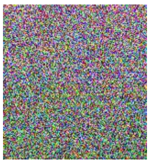
These tables 2 (a),(b),(c) show us the code corresponding to the Repetitively order t, Color scrambling Techniques and the Pixels scrambling techniques to different component used in this article.

1. Result and discussion

The obtained results are shown in the figure 3, 4 and table 3, 4,5,6,7.

Key: 100 001 110 101 100
We could generate automatically or manually the Key used for ciphering and deciphering.
We use the same key the ciphering process and deciphering process.

t=5
zigzagcolor_2
Pattern_zigzag_7 Red component
Pattern_zigzag_6 Green component
Pattern_zigzag_5 Blue component



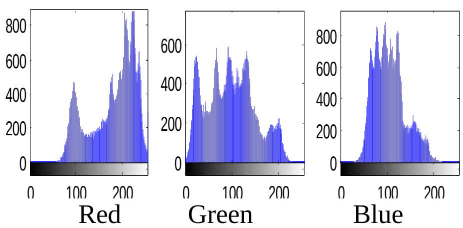
OriginalImage CipherImage
.

The original image to be ciphered is the image Lena.jpg, with size 256x256x3. The image ciphered is so different of the original images. The correlation rxyis less than 0.02. So, there are no correlation between the ciphered image and original image.

StegoCiphered Image Deciphered Image

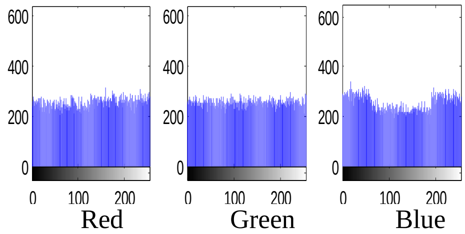
We have deciphering like perfect algorithm. The deciphered image is very similar with the original image. The evaluation parameters results confirm this: rxy andSSIMmore than 0.99, PSNRmore than 54, NPCR less than 0.04 and UACI less than 0.0005.

Figure 3:Key used and image obtained after different steps on the approach 1



Histograms of each original image component

The histogram of each original image component is different each other



Histograms of each ciphered image component

The histogram of each ciphered image component has tendency to be flat and so different of the original image

Figure 4: Histograms of original and ciphered component by using approach 1

Table 3: Correlation coefficient obtained by using the approach 1

Rxy	Between the original image and the cipher image	Between the original image and the Stegocipher image
Red component	0.028993785	0.028982803
Green component	-0.001315694	-0.00132380
Blue component	0.014350866	0.014349423
Rxy	Between the ciphered image and the Stegociphered image	Between the original image and the deciphered image
Red component	0.999996354	0.999992300
Green component	0.999979350	0.999959477
Blue component	0.999999895	0.9999996282

Table 4:SSIM obtained using approach 1

SSIM	Between the original image and the cipher image	Between the original image and the Stegocipher image
Red component	0.0067791488	0.00677893996
Green component	0.0064798139	0.00648000295
Blue component	0.0089701314	0.00897007471
SSIM	Between the cipher image and the Stegocipher image	Between the original image and the decipher image
Red	0.9999999183	0.9997425719

component		
Green component	0.9999995645	0.9999651399
Blue component	0.9999999865	0.9999940580

Table 5:PSNR obtained using approach 1

PSNR	Between the original image and the cipher image	Between the original image and the Stegocipher image
Red component	8.0099915727	8.0098597228
Green component	8.5690718609	8.5688662024
Blue component	9.4289113415	9.4289209829
PSNR	Between the cipher image and the Stegocipher image	Between the original image and the decipher image
Red component	62.105964607	62.421704651
Green component	54.58712087	54.68911717
Blue component	77.21075272	78.736854358

Table 6:NPCR obtained using approach 1

NPCR en %	Between the original image and the cipher image	Between the original image and the Stegocipher image
Red component	99.6337890625	99.6322631835
Green component	99.5956420898	99.595642089
Blue component	99.630737304	99.630737304
NPCR en %	Between the cipher image and the Stegocipher image	Between the original image and the decipher image
Red component	0.041198730	0.0411987304
Green component	0.041198730	0.0411987304
Blue component	0.0320434570	0.03204345703

Table 7:UACI obtained using approach 1

UACI en %	Between the original image and the cipher image	Between the original image and the Stegocipher image
Red component	26.08539057	26.085953057
Green component	9.646875718	9.6468158796
Blue component	10.18855076	10.188634535
UACI en %	Between the cipher image and the Stegocipher image	Between the original image and the decipher image
Red component	0.0006642061	0.0005624808
Green component	0.0001376282	0.00026328890
Blue component	0.0001974666	0.00007778990

After all results, we could say that the original image is so different between the ciphered image and the ciphered image and indeed with stego_ciphered_image. The ciphered image and stego_ciphered _image are so similar and even for the deciphered image and original image. We could say that we have performed deciphering algorithm.

2. Impact of 1 bit changing with the recuperated key

If it has one bit changing in the key. The impacts of this error could be interpreted by:

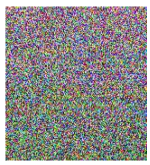
- If the error is located on the choice of scrambling technique in the different component, the results are presented in the figure 5 and the table 8.

Original Key
100 001 110 101 100

t=5, zigzagcolor_2
Pattern_zigzag_7 Red component
Pattern_zigzag_6 Green component
Pattern_zigzag_5 Blue component

Recuperated Key
100 001 110 101 101
t=5, zigzagcolor_2
Pattern_zigzag_7 Red component
Pattern_zigzag_6 Green component
Pattern_zigzag_6 Blue component


Original Image


Ciphered Image

The ciphered image and Stego_ciphered image are different between the original image

StegoCiphered Image Deciphered Image.

Between the original image and deciphered image, only the component blue change. The Table 8confirms this result and it could be explain by the high similarity of the deciphered and original image. Result not so good.

Figure 5:Original Key, Recuperated Key and Obtained image if the error is located in the scramblingtechnique of the different components.

Table 8:Value of the different parameter if the error is locating in the scrambling technique of the different components

Between the original image and the decipher image			
	Red component	Green component	Blue Component
rxy	0.99999230	0.99995947	0.00467422
NPCR	0.041198%	0.041198%	99.20959%
UACI	0.000562%	0.000263%	9.849051%
PSNR	62.4217046	54.689117	9.82206732
SSIM	0.999742	0.999965	0.00956815

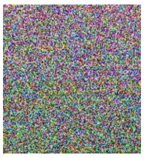
- If the error is located in the choice of color scrambling confusion, we obtain result in figure 6 :

Original Key
100 001 110 101 100

t=5, zigzagcolor_2
Pattern_zigzag_7 Red component
Pattern_zigzag_6 Green component
Pattern_zigzag_5 Blue component

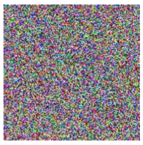
Recuperated Key
100 011 110 101 100

t=5, zigzagcolor_4
Pattern_zigzag_7 Red component
Pattern_zigzag_6 Green component
Pattern_zigzag_5 Blue component

Original Image Ciphered Image

The ciphered image and Stego_ciphered image are different between the original image

StegoCiphered Image Deciphered Image.

Image deciphered is not recognized comparing to the original image. Good Result

Figure 6:Original Key, Recuperate Key, Obtained image if the error is located in the choice of the scrambling technique

Tableau 9:Value of the different parameter if the error is locating in choice of the scrambling technique of the different components

Between the original image and the decipher image			
	Red component	Green component	Blue component
rxy	-0.005418	0.0011373	0.0063393
NPCR	99.58801%	99.629211%	99.620056%
UACI	25.34561%	9.964204%	9.534008%
PSNR	8.074912	8.652108	9.6260251
SSIM	0.011446	0.01037	0.010896

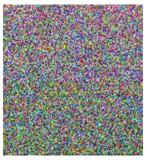
- If the error is located in the repetitively order of the scrambling technique, we could have :

Original Key
100 001 110 101 100

t=5, zigzagcolor_2
Pattern_zigzag_7 Red component
Pattern_zigzag_6 Green component
Pattern_zigzag_5 Blue component

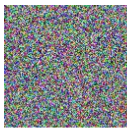
Recuperated Key
110 001 110 101 100

t=7, zigzagcolor_2
Pattern_zigzag_7 Red component
Pattern_zigzag_6 Green component
Pattern_zigzag_5 Blue component

Original Image Ciphered Image

The original image and Ciphered image are different.

StegoCipher Image Decipher Image

Image deciphered is not recognized comparing the original image. Good Result

Figure 7:Original Key, Recuperate Key, Obtained image if the error is located in the repetitively order of the scrambling

Table 10:Value of the different parameter if the error is locating in the repetitively order of the scrambling

Between the original image and the decipher image			
	Red component	Green Component	Blue component
rxy	0.08926296	0.00847798	0.01274287
NPCR	99.52697%	99.60021%	99.45068%
UACI	20.20588%	9.389301%	10.93727%
PSNR	9.0681990	8.5336335	11.2772705
SSIM	0.00990409	0.00872481	0.0151120

The approach 1 algorithm has a principal inconvenient that it is not sensible with the one bit changing of the recuperated key in the last 9bits on the scrambling technique of each component of the image. For avoiding this, we introduce the approach 2.

D. Approach 2

The approach 2 is described on the Figure 8and the structure of the key used is defined on the Table 11.

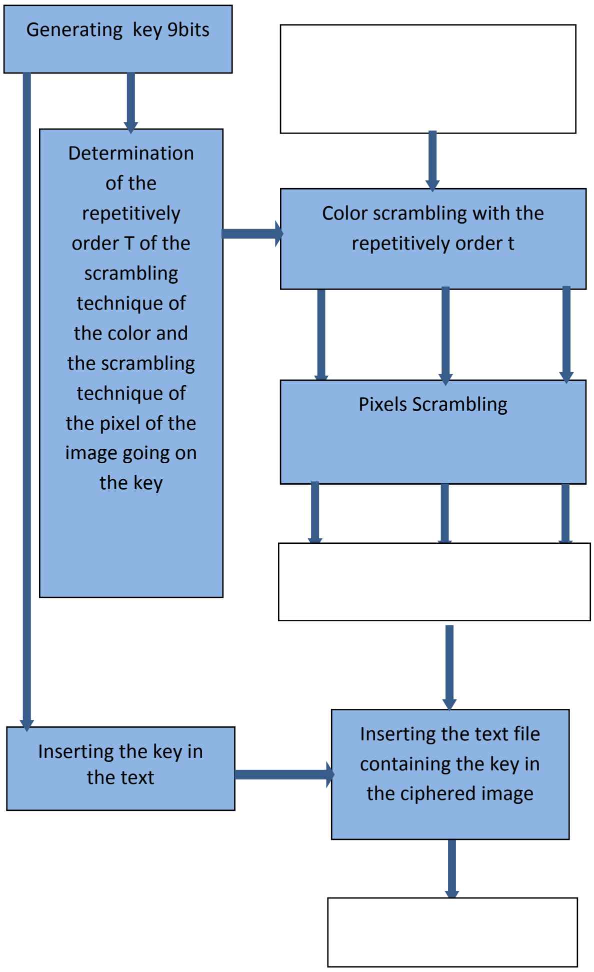


Figure 8:*Approach 2 algorithm*

We use 9bits of key like 3bits for the choice of the repetitively order, given in table 2 (a), 3bits for the choice scrambling technique for all componentsRGBgiven in table 2 (b), and 3bits for the scrambling technique based on the pixel emplacement of different path for the image entiregiven in table 2 (c).

Table 11:Key structure for the approach 2

Repetitively order of the scrambling color	Scrambling color for all component of image	Scrambling pixels techniques
3 bits	3 bits	3 bits

1. Result and Discussion

The results are represented in the figure 9 and table 12, 13, 14, 15, 16.

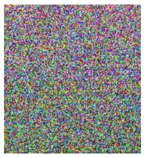
Key: 100 001 000 Key used for the ciphering and deciphering. We could generate it automatically or manually.
t=5 zigzagcolor_2 Pattern_zigzag_1
  Original Image Ciphered Image
The original image to be ciphered isLena.jpg,with size 256x256x3.The ciphered image is so different between the original images.rxyless than 0.03, so no correlation between ciphered image and original image.
  StegoCiphered Image Deciphered Image.
We have like perfect algorithm of deciphering. The deciphered image and original image is so similar. The parameter result of evaluation confirm this by : rxy andSSIMmore than 0.99, PSNRmore than 55, NPCR less than 0.045 et UACI less than0.0007

Figure 9:Key used and obtained image for the approach 2

Table 12: Correlation coefficient for the approach2

rxy	Between the original image and the cipher image	Between the original image and the Stegocipher image
Red component	0.0290922511	0.02907791
Green component	-0.00794350	-0.00795089
Blue component	-0.00690471	-0.00690617
rxy	Between the cipher image and the Stegocipher image	Between the original image and the decipher image
Red component	0.9999961	0.9999826633
Green component	0.99999151	0.99999947178
Blue component	0.99999162	99.592590332

Table 13:SSIM obtained for the approach 2

SSIM	Between the original image and the cipher image	Between the original image and the Stegocipher image
Red component	0.01139402	0.011393756
Green component	0.006571788	0.0065719490
Blue component	0.009014385	0.0090143540
SSIM	Between the cipher image and the Stegocipher image	Between the original image and the decipher image
Red component	0.99999986	0.999982163
Green component	0.999999826	0.999974130
Blue component	0.99999998	0.999991550

Table 14:PSNR obtained for the approach 2

PSNR	Between the original image and the cipher image	Between the original image and the Stegocipher image
Red component	8.010294666	8.010166706
Green component	8.544542178	8.544397497
Blue component	9.364007988	9.364017997
PSNR	Between the cipher image and the Stegocipher image	Between the original image and the decipher image
Red component	61.90069701	62.05495766
Green component	58.45014317	58.37659211
Blue component	78.16646934	77.21075272

Table 15:NPCR obtained for the approach 2

NPCR en %	Between the original image and the cipher image	Between the original image and the Stegocipher image
Red component	99.592590332	99.589538574
Green component	99.612426757	99.612426757
Blue component	99.6795654	99.678039550
NPCR en %	Between the cipher image and the Stegocipher image	Between the original image and the decipher image
Red component	0.0427246093	0.0427246093
Green component	0.0396728515	0.0396728515
Blue component	0.0366210937	0.03662109375

Table 16:UACI obtained for the approach 2

UACI en %	Between the original image and the cipher image	Between the original image and the Stegocipher image
Red component	26.0969932406	26.0976694144
Green component	9.69412410960	9.69409419041
Blue component	10.2812643612	10.2813541187
UACI en %	Between the cipher image and the Stegocipher image	Between the original image and the decipher image
Red component	0.00077191521	0.00021541819
Green component	0.00018549900	0.00065822227
Blue component	0.0001974666	0.00013762829

By the result in figure 9 and table 12,13,14,15 and 16, we could confirm that this approach 2 hasapproximately the same performance like the approach 1.

2. Impactof 1bit changing in the key

With the same approach like precedent, if the error of one bit changing is seen for the recuperating of the key, the impact of the error is like this:

- If the error is located on the choice of pixels scrambling technique. We could have as result in figure 10 and table 17.

In this case, we obtain an unknown and unidentified deciphered image. It’s the result that we search.
In cryptography, the goal is to obtain a deciphered image similar of the original image by using true key. But with wrong key, we must get an unknown and unidentified deciphered image.

Tableau 17:Value of the parameter if the error is locating in the choice of the pixel scrambling techniques

Between the original image and the decipher image			
	Red component	Green component	Blue component
rxy	-0.0125592	-0.0039589	0.00213328
NPCR	99.67956%	99.55749%	99.61242%
UACI	28.49454%	9.696679%	8.763128%
PSNR	7.5992769	8.5992379	9.5354537
SSIM	0.0082060	0.00857349	0.00763133

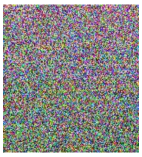
Original Key
100 001 000

t=5
zigzagcolor_2
Pattern_zigzag_1

Recuperated Key
100 001 010

t=5
zigzagcolor_2
Pattern_zigzag_3


Original Image


Ciphered Image

The original image and ciphered image is so different


Stego Ciphered Image


Deciphered Image

The Stego_ciphered_image and deciphered image are different of the original image. Good result.

Figure 10:Original Key, Recuperated Key and image obtained if the error is locating in the choice of the pixel scrambling techniques

- If the error is located in the choice of the scrambling technique of all component color, the figure 11 and the table 18 show us the result.

Tableau 18:Value of different parameter if the error is locating in the choice of scrambling technique of all component of image

Between the original image and the deciphered image			
	Red component	Green component	Blue component
rxy	-0.0101968	0.000665	-0.0017245
NPCR	99.62615%	99.63226%	99.59106%
UACI	28.23138%	9.744382%	9.416462%
PSNR	7.6392106	8.5929703	9.548651
SSIM	0.00874866	0.0085374	0.00831378

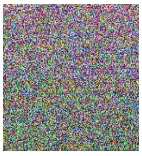
Original Key
100 001 000

t=5
zigzagcolor_2
Pattern_zigzag_1

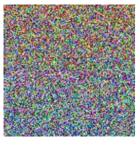
Recuperated Key
100 100 000

t=5
zigzagcolor_5
Pattern_zigzag_1


Original Image


Ciphered Image

Original image and Ciphered image is so different


StegoCiphered Image


Deciphered Image

Stego_ciphered _image and deciphered image are different of original image: Good Result.

Figure 11:Original Key, Recuperated Key, Image obtained if the error is locating in the choice of scrambling technique of all component of image

- If the Key error is located in the repetitively order of the scrambling, we could have result in figure 12 and table 19:
These results confirm us that with bad key recuperation in repetitively order of the scrambling, we can’t recognize or identify the ciphered image.

Tableau 19:Value of different parameter if the error is locating in repetitively order of the scrambling

Between the original image and the deciphered image			
	Red component	Green component	Blue component
Rxy	0.08926300	0.00846014	0.01274474
NPC	99.530029%	99.60021%	99.45373%

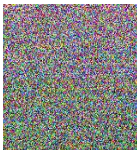
R			
UACI	20.206286%	9.389756%	10.93729%
PSNR	9.06806364 8	8.53369070	11.277289
SSIM	0.00989765 5	0.00872496	0.0151139

Original Key
100 001 000

t=5
zigzagcolor_2
Pattern_zigzag_1

Recuperated Key
110 001 000

t=7
zigzagcolor_2
Pattern_zigzag_1

Original Image Ciphered Image.

Original image and Ciphered image are so different


StegoCiphered Image Deciphered Image

Deciphered image is so different comparing to the original image: Good Result.

Figure 12:Original Key, Recuperated Key, Image obtained if the error is locating in repetitively order of the scrambling

IV. CONCLUSION

In this article we create ciphering algorithm using all forms of zigzag with pixel scrambling and for transmitting the key we use steganography. For that, the approach is divided with two methods. The first, use 15bits of key repartitioning like this : 3bits for the repetitively order t of scrambling color, 3bits for the colors scrambling, 3bits for the pixel scrambling techniques of Red, 3bits for the pixel scrambling techniques of Green,3bits for the pixel scrambling techniques of Blue. The scrambling technique is separate of all components Red Green Blue. For the performance, the original image and ciphered image has correlation less than 0.02 and histogram with flat tendency. Deciphered image and original image has correlation more than 0.99, PSNR more than 54, NPCR less than 0.041 and UACI less than 0.05. For the performance of the steganography, the ciphered image and stego_ciphered image has correlation more than 0.99, SSIM more than 0.999, NPCR more than 99.5% and UACI between 10%-20%. Like conclusion, this approach 1 has a good performance for the criteria correlation, SSIM, UACI, and NPCR. The original image and ciphered image is so different, the ciphered image and stego_ciphered image is so similar, and the deciphered image and original is also so similar. Unlikely, this approach one has inconvenient. The error of one bit only of the key not has an impact the deciphered image if this error is locating in the last 9bits of the key. So, the good option is not using the scrambling separately with the component RGB. The approach 2 use 9bits of ciphering repartitioning like this: 3bits of repetitively order of scrambling, 3bits of scrambling color for all component of image, 3bits of scrambling pixels techniques. With this approach, the result is similar as the first approach for all criteria: Correlation, SSIM, PSNR, NPCR, UACI and Histogram and it has advantage like with one bit error of the key the deciphering image is very different of the original in all partition of the key.

REFERENCES

[1] BhaskarMondal, Neel Biswas, TarniMandal, "A Comparative study on Cryptographic Image Scrambling", Proceedings of the Second International Conference on Research in Intelligent and Computing in Engineering pp. 261–268, Conference Paper June 2017.

[2] QI Dongxu, ZOU Jiancheng, HAN Xiaoyou. "A new class of scrambling transformation and its application in the image information covering ", Journal of Science in China (Series E), 2000, 43(3)… 304 - 312.

[3] J.C.Zou and R.K.Ward, "Introducing Two New Image Scrambling Methods", Proc. Of IEEE Pac. Rim Conf. on Comm., Comp. and Sig. Proc., pp. 708-711, 2003.

[4] Mamy Alain Rakotomalala, Tahina E. Rakotondraina and Sitraka R. Rakotondramanana, "Contribution for Improvement of Image Scrambling Technique Based on Zigzag Matrix Reodering";International Journal of Computer Trends and Technology (IJCTT) – Volume 61 Number 1 - July 2018

[5] PunitaKumari and Kalpana Jain, "Digital Image Encryption Technique Using Block Based Scrambling and Substitution", Global Journal of Computer Science and Technology, Vol.1, USA (2017)

[6] KokSheik Wong, Kiyoshi Tanaka, "SCALABLE IMAGE SCRAMBLING METHOD USING UNIFIED CONSTRUCTIVE PERMUTATION FUNCTION ON DIAGONAL BLOCKS", 28th Picture Coding Symposium, Japan 8-10 (12) (2012)

[7] Ahmet C¸ agrıBagbaba, BernaOrs, "Hardware Implementation of Novel Image Compression-Encryption System on a FPGA", Istanbul Technical University, Turkey (2013)

[8] CHADY EL MOUCARY, "A Novel Blind Digital Watermarking Technique for Stegano-Encrypting Information Using Nine-AC-Coefficient Prediction Algorithm with an Innovative Security Strategy", WSEAS Transactions on Signal Processing, Vol.5, Issue.11, Libanese (06) (2009)

[9] J.M.Rodriguesa, W. Puecha and A.G. Borsb, "A Selective Encryption for Heterogenous Color JPEG Images Based on VLC and AES Stream Cipher", University of Montpellier, France (2002)

[10] S.S.Maniccama, N.G. Bourbakis, "Image and video encryption using SCAN patterns", The Journal of the Pattern Recognition Society, Greece 18 (8) (2003)

[11] Shalin J Patel, "Image Encryption and Compression using Scan Patterns", International Journal for Scientific Research & Development (IJSRD), Vol. 3, Issue 03,Kalol (2015)

[12] FaramarzSadeghi, FatemehZarisfiKermani, and MarjanKuchaki Rafsanjani, “Optimizing Image Steganography by Combining the GA and ICA”, the ISC International Journal of Information Security, Vol.7, No.1, Iran (1) (2015) 47-58
[13] ReemaDhiman, Butta Singh, “IMAGE ENCRYPTION TECHNIQUES: A LITERATURE REVIEW”, International Journal of Advanced Research in Computer Science (IJARCS), Vol.8, No.7, India (7-8) (2017)
[14] ChengqingLia, DongdongLina, JinhuLub, “Cryptanalyzing an Image Scrambling Encryption Algorithm of Pixel Bits”, IEEE Multimedia, China 6 (8) (2017)
[15] Sabah Fadhel, MohdShafry, Omar Farook, “Chaos Image Encryption Methods: A Survey Study”, Bulletin of Electrical Engineering and Informatics, Vol.6, No.1, Malaysia (3) 2017 99-104
[16] FarzanaKabir, JasmeetKaur, “Color Image Encryption for Secure Transfer over Internet: A survey”, International Research Journal of Engineering and Technology (IRJET), Vol.4, India (10) 2017
[17] S.El Assad, M. Farajallah and C. Vladeanu, “Fast and Secure Chaos-based Cryptosystem for Images”, International Journal of Bifurcation and Chaos (IJBC), (2) (2016)
[18] SangitaVishwakarma, Mrs. ShahanaQureshi, “TECHNIQUES OF VISUAL CRYPTOGRAPHY SCHEMES: A REVIEW”, Journal of Emerging Technologies and Innovative Research (JETIR), Vol. 4, (4) (2017)
[19] C.Muramatsu, S. Higuchi, T. Morita and H. Fujita, “Similarity estimation for reference image retrieval in mammograms using convolutional neural network”, Texas 27 (2) (2018)
[20] A.Cheddad, J. Condell, K. Curran et P. McKevitt, “Digital image steganography: Survey and analysis of current methods”, Signal Processing 90, pages 727–752. (2010).
[21] S.Kouider,.« Insertion adaptative en stéganographie application aux images numériques dans le domaine spatial », Université de Montpellier, 2013.
[22] J.A.Mazumde, et K. Hemachandran, « Study of Image steganography using LSB,DFT and DWT», International Journal of Computers & Technology, 2013.
[23] R.Rakotomalala, “Analyse de corrélation, Étude des dépendances - Variables quantitatives Version 1.1”, Support Université Lumière Lyon 2, 27 (12) (2017)
[24] Z.Wang, A.C. Bovik , H.R. Seikh, et E.P. Simon celli, «Image quality assessment: from visibility to structural similarity», IEEE Transaciations on Image Processing, volume 13, 2004.
[25] Junqin Zhao, WeichuangGuo, Ruisong Ye, “A Chaos-based Image Encryption Scheme”, International Journal of Computer Trends and Technology (IJCTT) – volume 15 number 4 – Sep 2014 Using Permutation-Substitution Architecture