IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 20, Issue 4, Ver. III (Jul - Aug 2018), PP 55-70
www.iosrjournals.org

Performances of Image Scrambling Techniques Based on The Permutation Transform

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
Corresponding Author:Mamy Alain Rakotomalala

Abstract: *This article gives us some comparison between the performances of techniquesrelating to image scrambling. The scrambling is a technique used for information and especially for any kind of image to transform them into totally incomprehensible and unrecognizable things. The scramblingtechniques that we talk about in this article are: the Arnold transform, the Fibonacci transform, the Luca transform and the Fibonacci-Luca transform. Performance criteria used for the purpose are mainly: the PSNR (Peak Signal to Noise Ratio), the SSIM (Structural SIMilarity), the NPCR (Number of Pixel Change Rate), the UACI (Unified Average Changing Intensity), the correlation coefficient and the response time. All techniques have their specific characteristics,each in relation to these parameters depending on the repetitively order "t". The principal interest is to enable the researcher to make a good choice of the scrambling techniques on account of their advantages. The results are obtained throughMatlab simulation and presented like a graph. All criteria considered as for the results obtained, with repetitively order 3, the Fibonacci transform has the best performance compared withall techniques.*

Keywords: *Permutation, Scrambling, Arnold, Fibonacci, Luca, Fibonacci-Lucas*

Date of Submission: 20-08-2018 Date of acceptance: 03-09-2018

I. Introduction

Withinthe course of these few years, information and communication technologies have evolved tremendously. Exchanging, storing, securing information in all its aspects have become the mainstays of the modern society. Ensuring data security, mainly confidential data, at the stage of storing or during their transmission within the network has turned into a real challenge to take up for researchers. In the batch of securing techniques, ciphering techniques and scrambling techniques deserve a special attention. The purpose of this article entitled « Performances of image scrambling techniques based on the permutation transform »is to make a comparison between the different techniques of scrambling namely the Arnold transform, the Fibonacci transform, the Luca Transform andthe Fibonacci-Luca Transform by means of the following criteria : the PNSR (Peak Signal to Noise Radio), the SSIM (Structural Similarity), the NPCR (Number of Pixel Change Rate), the UACI (Unified Average Changing Intensity), the correlation coefficient, and the response time. This article is divided into threeparts : firstly an overall presentation of image scrambling ; secondly, a description of the different scrambling techniques ; and lastly : commentary on the various results obtained.

II. Overall Presentation Of Image Scrambling

Scrambling is a technique used to turn an image into something incomprehensible and unrecognizable. Many publications[1-5] have tried to give an accurate definition of the word « scrambling » together with a presentation of the different techniques relating to it. In the present article, the talk will mainly be dealing with the scrambling based on permutation.

2.1 Definition of a permutation [2, 6]

A permutationof two variables: a and b marked by $\leftrightarrow$ is defined by an exchange of contents between both variables. This operation requires a third variable temp which will act as a timer.

$$(a \leftrightarrow b) = \begin{cases} temp \leftarrow a \\ a \leftarrow b \\ b \leftarrow temp \end{cases} \quad ou \quad (a \leftrightarrow b) = \begin{cases} temp \leftarrow b \\ b \leftarrow a \\ a \leftarrow temp \end{cases} \tag{1}$$

Taking $i \in N; i = \{1,2,3,\ldots,t\}$with *t*repetitively and Na two-dimensioned image of *W* x *H* (*W* is the length and *H* the height) ; the values of the colors R,G,B are associated with each pair $(x, y) \in \{1,2,...W\} \times \{1,2,...H\}$

The scrambling technique based on permutation will result into a series of pixel exchanges on the co-ordinates $(x, y) \in \{1,2,...W\} \times \{1,2,...H\}$ with $(x', y') \in \{1,2,...W\} \times \{1,2,...H\}$ proved by the following transformation:

$$\sigma_i : \begin{pmatrix} x'-1 \\ y'-1 \end{pmatrix} = \left\{ \begin{pmatrix} a_i & b_i \\ c_i & d_i \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} \right\} \begin{Bmatrix} \bmod W \\ \bmod H \end{Bmatrix} \forall (x, y) \in \{1,2,...W\} \times \{1,2,...H\}$$
$$\begin{cases} x'-1 = (a_i x + b_i y) \bmod W \\ y'-1 = (c_i x + d_i y) \bmod H \end{cases} \tag{2}$$

To be noted the transformation matrix T_i by:

$$T_i = \begin{pmatrix} a_i & b_i \\ c_i & d_i \end{pmatrix} \tag{3}$$

Thus, the transformation is actually the exchange of the levels of R, G, B between (x, y) et (x', y') as follows:

$$\forall (x, y) \in \{1,2,...W\} \times \{1,2,...H\}; calculer : \begin{cases} x'-1 = (a_i x + b_i y) \bmod W \\ y'-1 = (c_i x + d_i y) \bmod H \end{cases}; (x, y) \leftrightarrow (x', y') \tag{4}$$

To recover the original image, the reverse operation is defined by :

$$\sigma_i^{-1} : \begin{pmatrix} x'-1 \\ y'-1 \end{pmatrix} = \left\{ \begin{pmatrix} a_i & b_i \\ c_i & d_i \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} \right\} \begin{Bmatrix} \bmod W \\ \bmod H \end{Bmatrix} \forall (x, y) \in \{W, W-1,...,1\} \times \{H, H-1,...,1\} \tag{5}$$

$$\forall (x, y) \in \{W, W-1,...,1\} \times \{H, H-1,...,1\}; calculer : \begin{cases} x'-1 = (a_i x + b_i y) \bmod W \\ y'-1 = (c_i x + d_i y) \bmod H \end{cases}; (x, y) \leftrightarrow (x', y') \tag{6}$$

2.2 Order of repetitively t:

To improve the result of the scrambling and avoid mistakes in predictions, the calculation is not limited to only one permutation: more than one is requested. If the composition done for the permutation is (t-1),the value of the order of repetitively t will be:

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

« o » stands as the composition operator of two permutations.

In the case of a scrambling based on permutation, the reverse process makes it possible to recover the original image:

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

III. Presentation Of Different Image Scrambling Techniques

3.1The Arnoldtransform[2, 7-11]

As cryptography keeps evolving, in order to respect confidentiality and to preserve the image security, for the very first time, Vladimir Arnold experimented a technique of scrambling in 1960. The transformation matrix T is defined as follows :

:

$$T_i = \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix} \tag{9}$$

3.2The modified version of the Arnold transform

Even if several compositions of the order t are used, the transformation matrix *T* will remain the same.

$$T_1 = T_2 = ... = T_i = ... = T_t = \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix}$$

Thus, in 2004, Kong and Dan developed an Anti-Arnold algorithm which was innovation in this domain. The stipulated norm for the modified version of Arnold transformation is as follows :

$$T_1 \neq T_2 \neq ... \neq T_i \neq ... \neq T_t;$$

$$T_i = \begin{pmatrix} i+1 & i \\ 1 & 1 \end{pmatrix} \text{ ou } T_i = \begin{pmatrix} i & i+1 \\ 1 & 1 \end{pmatrix} \tag{11}$$

3.3The Fibonaccitransform[12-13]

Leonard de Pise,under the pseudonym of Fibonacci showed serious interest in the following sequence called the series ofFibonacci:

$$F_n = \begin{cases} 0 & si \quad n = 1 \\ 1 & si \quad n = 2 \\ F_{n-1} + F_{n-2} \end{cases} \tag{12}$$

The series of Fibonacci obtained are: 0, 1, 1, 2, 3, 5, 8, 13, 21, 34…

In 2012, MinatiMishra, PriyadarsiniMishra, M.C. Adhikary**,** and SunitKumar proposed the use of the series of Fibonnacias a transformation matrix:

$$T_i = \begin{pmatrix} F_i & F_{i+1} \\ F_{i+2} & F_{i+3} \end{pmatrix} \tag{13}$$

3.4The Lucatransform[12-13]

In addition to the series of Fibonacci, François Édouard Anatole Lucas, a mathematician by trade, invented his own series called the series of Lucas defined by the relation of recurrence here after:

$$L_n = \begin{cases} 2 & si \quad n = 1 \\ 1 & si \quad n = 2 \\ L_{n-1} + L_{n-2} \end{cases} \tag{14}$$

The series of Lucas are: 2, 1, 3, 4, 7, 11, 18, 29…

By analogywithFibonacci, the Lucas matrix of transformationwillbe defined by:

$$T_i = \begin{pmatrix} L_i & L_{i+1} \\ L_{i+2} & L_{i+3} \end{pmatrix} \tag{15}$$

3.5The Fibonacci-Lucatransform andthe Luca-Fibonacci transform [12-13]

It is also possible to use the Fibonacci series and Luca series at the same time, with the transformation matrix defined by:

$$T_i = \begin{pmatrix} F_i & F_{i+1} \\ L_i & L_{i+1} \end{pmatrix} \tag{16}$$

By analogy with the transform**Fibonacci-Luca,** the reverse **Luca-Fibonacci** is also possible :
The transformation matrix Lucas-Fibonacci is then defined by:

$$T_i = \begin{pmatrix} L_i & L_{i+1} \\ F_i & F_{i+1} \end{pmatrix} \tag{17}$$

IV. Results And Comments

4.1 Performance criteria

a. Coefficients of correlation with the pixels [1, 14]

The coefficient of correlation is defined by:

$$r_{xy} = \frac{COV(X,Y)}{\sqrt{Var(X)Var(Y)}} = \frac{COV(X,Y)}{\sigma_x \sigma_y} \tag{18}$$

With :

σ_x : as the gap unit of the variable X.
$E(X)$: as the expectation of X
$Var(X)$: as the variance of X.
COV(X,Y) : as the covariance between the variables X and Y.

$$COV(X,Y) = E\{[X - E(X)][Y - E(Y)]\} \tag{19}$$

The covariance is equal to the product of the targeted variables.

Its assignment is to quantize the liaison of the two variables X and Y, so as to emphasize the full significance of the liaison and its intensity. The coefficient of simple linear correlation of Bravais-Pearson (or simply Pearson) is a standardizationof the covariance by the product of all the gaps of the variables. The coefficient of correlation varies from – 1 and + 1. The nearer to the extreme values – 1 and + 1 the coefficient, the stronger the correlation between the variables.

The phrase « strongly correlated » is used for the purpose. If the coefficient is 0, it means that the two variables have not the same value of linearity.

Which gives: r = +1 absolute positive correlation, r = -1 absolute negative correlation and r = 0 absolute absence of correlation.

In this article, the coefficient of correlation is used so as to state the fact that there is actually a correlation between the original image and the scrambled ciphered image.

b. The time for response

What is meant here is the time taken by the scrambling operation and the one taken for the reverse operation. As a general rule, an algorithm with the shortest possible response time is preferred.

c. PSNR (Peak Signal to Noise Ratio) and SSIM (Structural SIMilarity) [1]

- The PSNR is a unit to measure the distortion when dealing with a digital image. The PSNR is definedby the following formula :

$$PSNR = 10.\log_{10}\left(\frac{d^2}{EQM}\right) \tag{20}$$

dis the highest possible value of a pixel.In general d=255 and EQM makethe average quadratic error defined by:

$$EQM = \frac{1}{mn}\sum_{i=0}^{m-1}\sum_{j=0}^{n-1}(I_0(i,j) - I_r(i,j))^2 \tag{21}$$

- The Structural Similarity or SSIM is a reliable measurement unit for the similarities between two digital images.

$$SSIM(X,Y) = \frac{(2\mu_X\mu_Y + c_1)(2\sigma_X\sigma_Y + c_2)(2COV(X,Y) + c_3)}{(\mu_X^2 + \mu_Y^2 + c_1)(\sigma_X^2 + \sigma_Y^2 + c_2)(\sigma_X\sigma_Y + c_3)} \tag{22}$$

μ_X , μ_Y being the average of X, Y; σ_X^2 , σ_Y^2 being the variance of X, Y ; $COV(X,Y)$ being the covariance between X and Y ; c_1 , c_2 , c_3 being three values to balance the division in case the value is too low.

d. The NPCR(Number of Pixel change rate) and the UACI (Unified Average Changing Intensity) [6]

❖ The NPCR is used to measure the percentage of pixels differentiating two givenimages.. It is defined by:

$$\mathrm{NPCR}^{R/G/B} = \frac{\sum_{i=1}^{H}\sum_{j=1}^{W} D_{i,j}^{R/G/B}}{W \times H} \times 100\%, \tag{23}$$

With

$$D_{i,j}^{R/G/B} = \begin{cases} 0\,, \; if \;\; C_{i,j}^{R/G/B} = \bar{C}_{i,j}^{R/G/B}, \\ 1, \;\; if \;\; C_{i,j}^{R/G/B} \neq \bar{C}_{i,j}^{R/G/B}. \end{cases}$$

$C^{R/G/B}$ and $\bar{C}^{R/G/B}$ representing the channels RGB of two images.

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

W and*H*are the width and the length of one image.

❖ The UACI is the average of the difference of light intensity between two given images.

$$\mathrm{UACI}^{R/G/B} = \frac{1}{W \times H}\sum_{i=1}^{H}\sum_{j=1}^{W} \frac{C_{i,j}^{R/G/B} - \bar{C}_{i,j}^{R/G/B}}{2^{L^{R/G/B}} - 1} \times 100\%. \tag{24}$$

4.2 Results

The following results have been obtained throughMatlabsimulation. The concerned image is a color image RGB lena.jpg, sized 256*256*3.

a. Coefficients of correlation of pixels

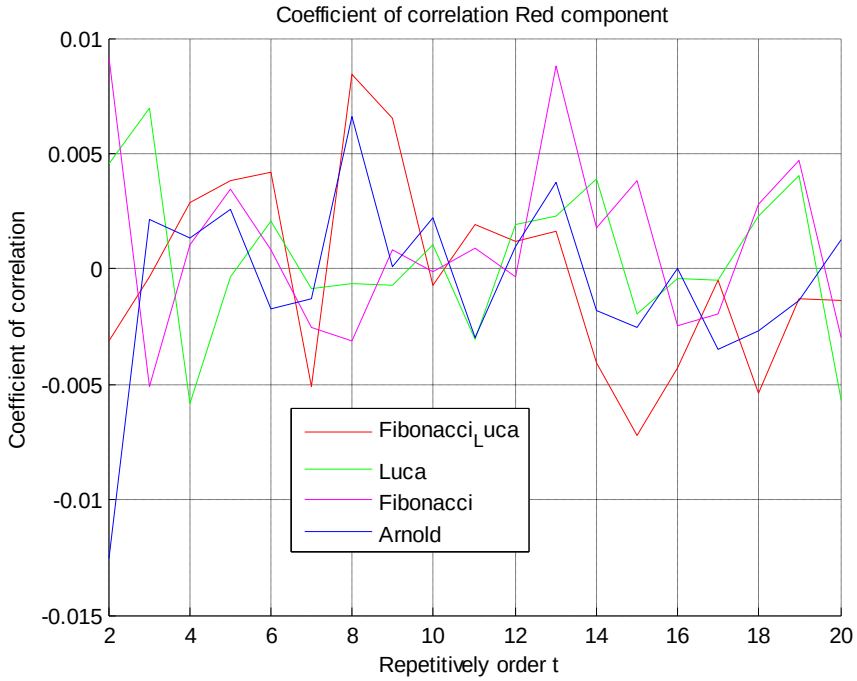

Figure 01: Graphs of correlation coefficients between the red components of the original image and the scrambled image

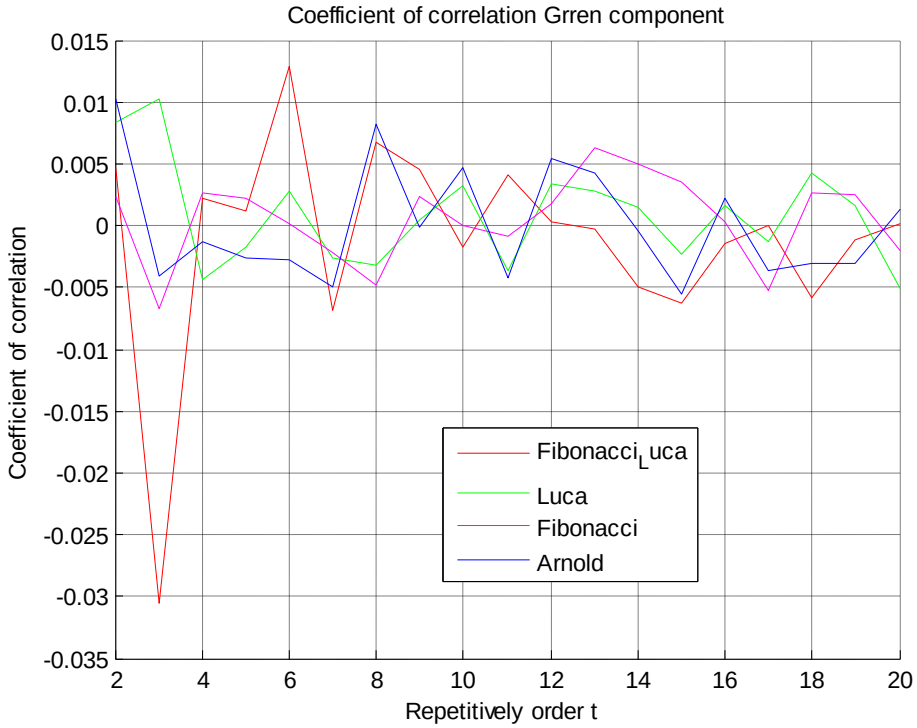

Figure 02: Graphs of correlation coefficients between the green components of the original image and the scrambled image

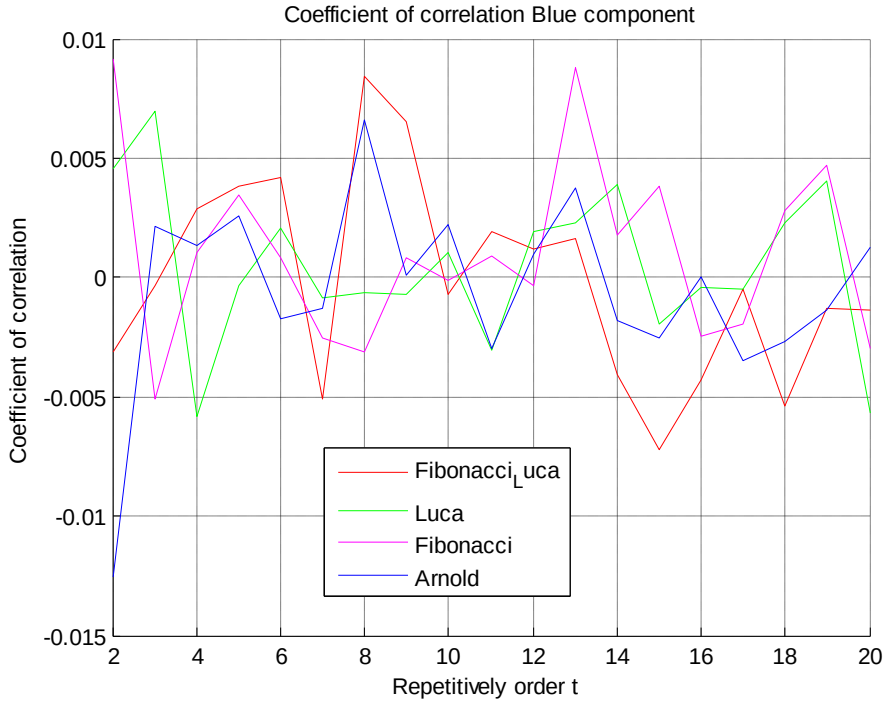

Figure 03: Graphs of correlation coefficients between the blue components of the original image and the scrambled image.

The results shown in figures 01, 02, 03clearly tell that the used scrambling techniques have more or less the same performances relating to correlation coefficients between the different colors of the original image and the scrambled one making use of these techniques: correlation coefficientsgoing from - 0.03 to 0.015. These results are confirmed in figures 17, 18, 19, 20, which mean that after scrambling, the obtained images have turned into incomprehensible images totally unrecognizable.For the repetitively order 2, the Arnold transform has the farthest correlation coefficients from 0, meaning a higher number of indicators in comparison with the

original image. But if instead, the nearest correlation coefficients to 0 are preferred asa choice criterion, the appropriate technique constituted by the correlation coefficients nearing 0 will be chosen so that there is no correlation at all between the original image and the scrambled one. For a specific order of repetitively, for an order of repetitively 3 for example, there is a choice between the Fibonccitransform and the Arnold transform.

b. The response time

As shown in Figure 04, the response times ofFibonacci transform, Luca transformand Arnold transformisapproximately proportional to the order of repetitively t. To obtain the shortest possible response time,t has to be chosen in its lowest possible value which is t=2 or 3. For Fibonacci-Luca transform, the response time is too enormous.

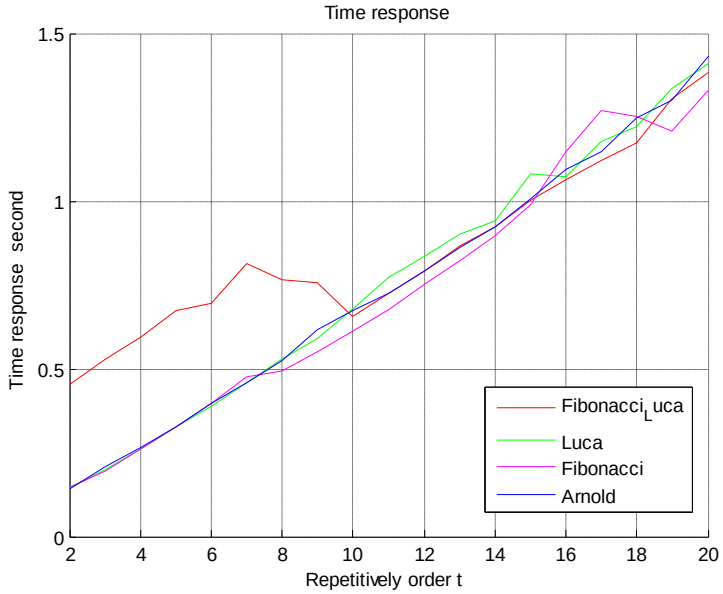

Figure 04: Response times in seconds of the different scrambling techniques

c. The PSNR (Peak Signal to Noise Ratio) andthe SSIM (Structural SIMilarity)

Relating to the PSNR results between the different colors of the original image and the scrambled one, they are represented in figures 05, 06, 07. A PSNR of the lowest possible value will be chosen so that the scrambled image totally differs from the original one. As an example: for an order of repetitively 3, one has the choice between the Fibonacci and Fibonacci-Luca transforms which have the lowest range of PNSR.

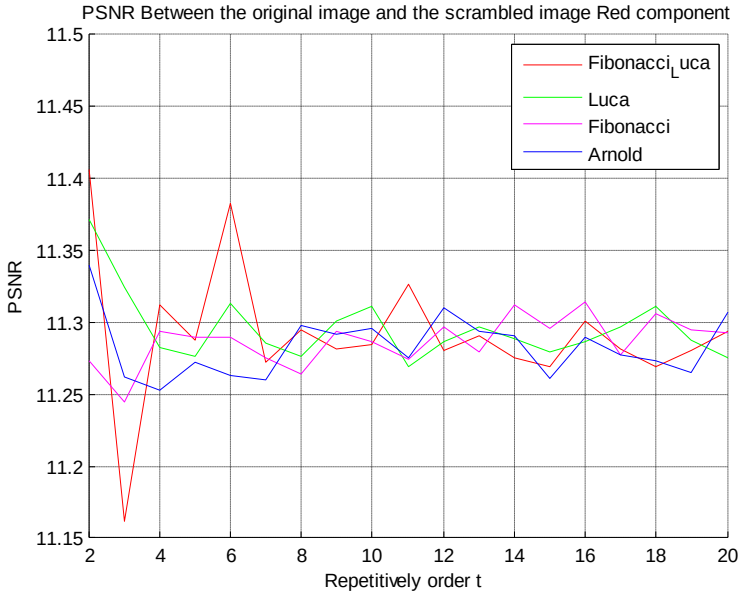

Figure 05: Graphs of PSNR between the red components of the original image and the scrambled one

Figure 06: Graphs of the PNSR between the green components of the original image and the scrambled one

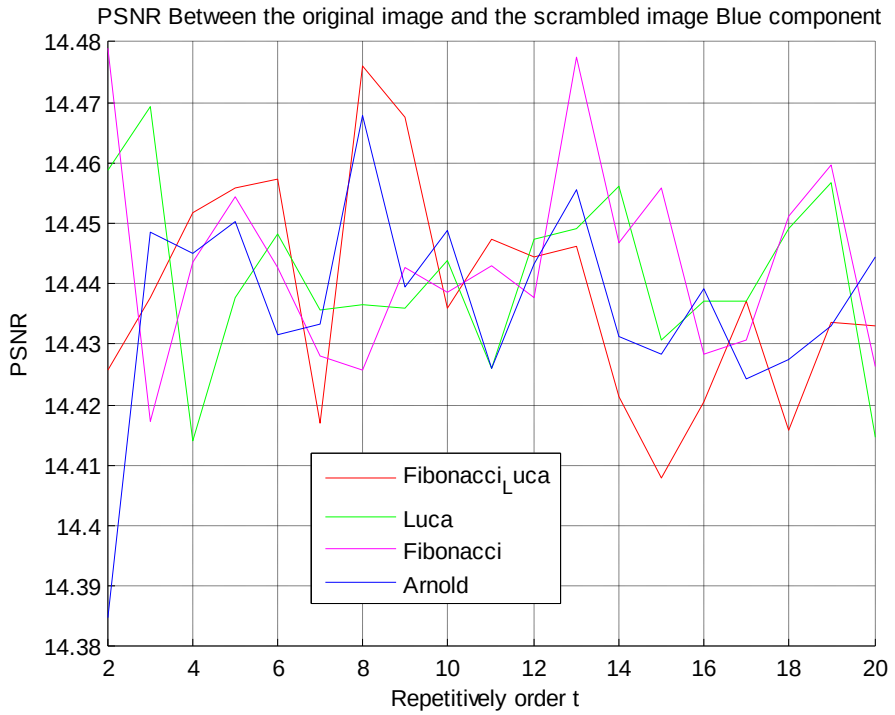

Figure 07: Graphs of thePSNRbetween the blue components of theoriginal image and the scrambled one

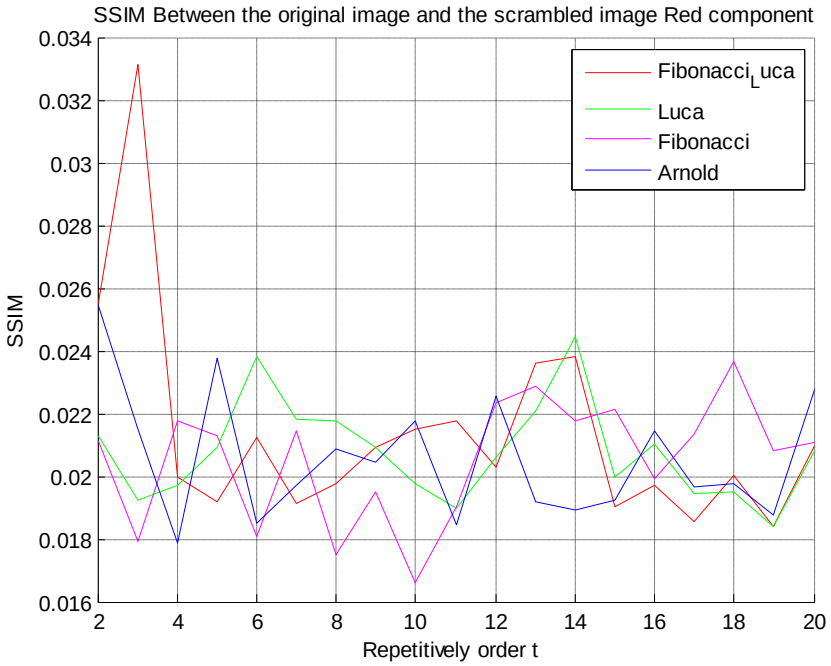

Figure 08: Graphs of the SSIM between the red components of the original image and the scrambled one.

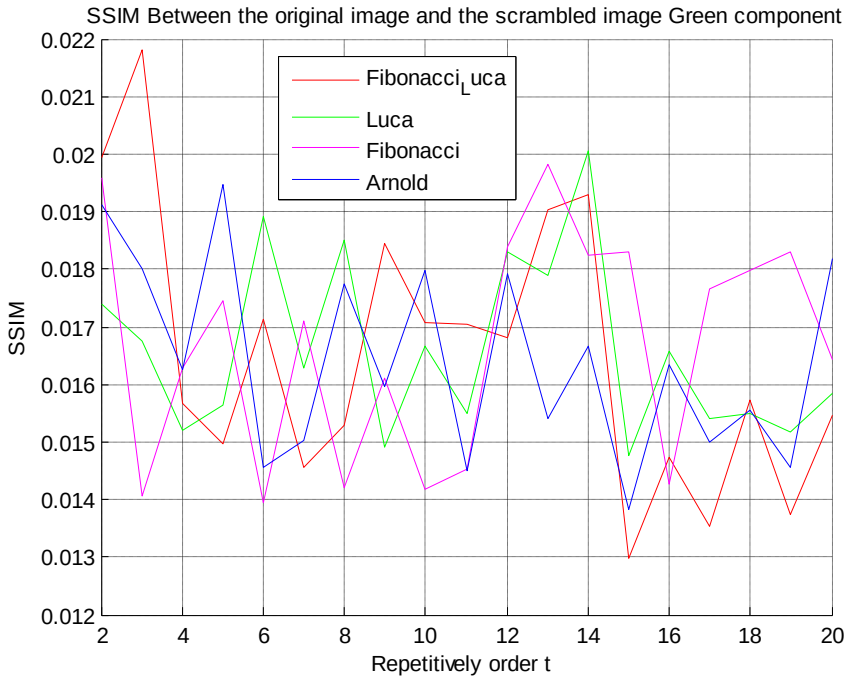

Figure 09: Graphs of SSIM between the green components of the original image and the scrambled one

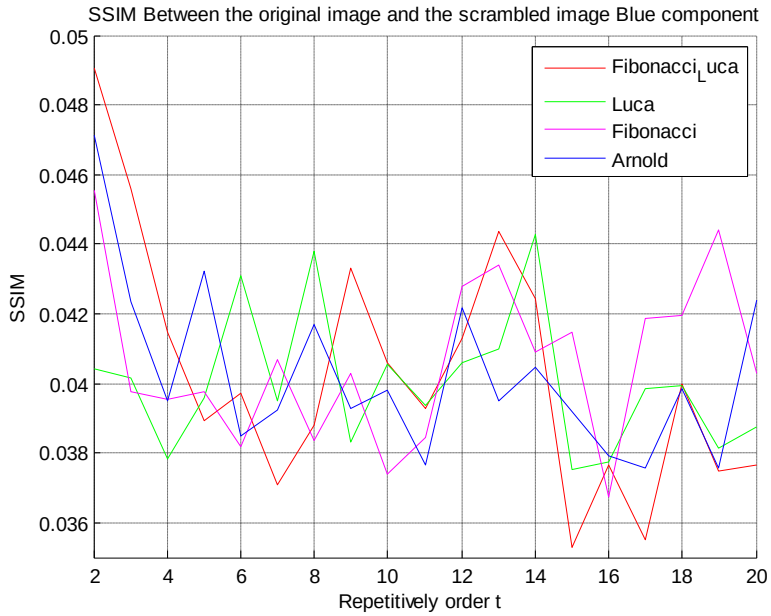

Figure 10: Graphs of the SSIM between the blue components of the original image and the scrambled one.

As for the SSIM, the technique with the lowest values of the different colors of the original image and the scrambled one are chosen. The results can be viewed in figures 08, 09, 10. For the order of repetitively 3, there is a choice between the Fibonacci transform and the Luca transform.

d. The NPCR (Number of Pixel change rate) andthe UACI (Unified Average Changing Intensity)

The results relating to the NPCR are shown in figures 11, 12, 13. Here, the technique with the highest value of NPCR will be chosen. For an order of repetitively 3, the Arnold transform has the lowest values of NPCR. Yet, these values are always higher than 99%.

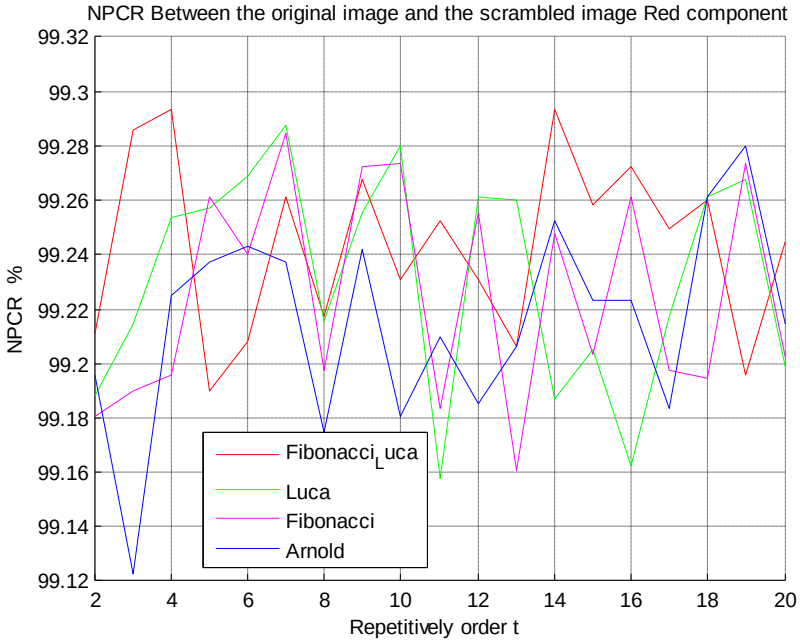

Figure 11: Graphs of the NPCR between the red components of the original image and the scrambled one

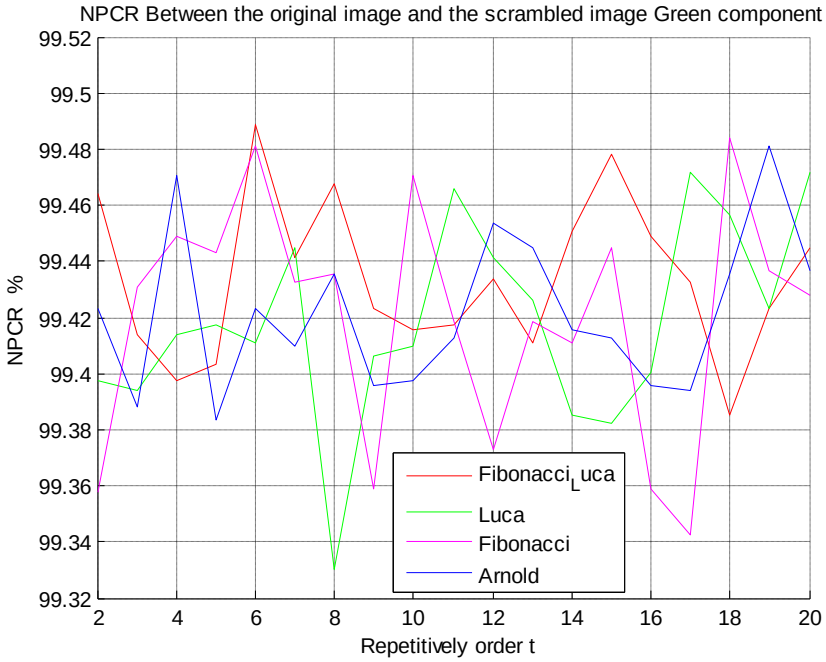

Figure 12: Graphs of the NPCR between the green components of the original image and the scrambled one

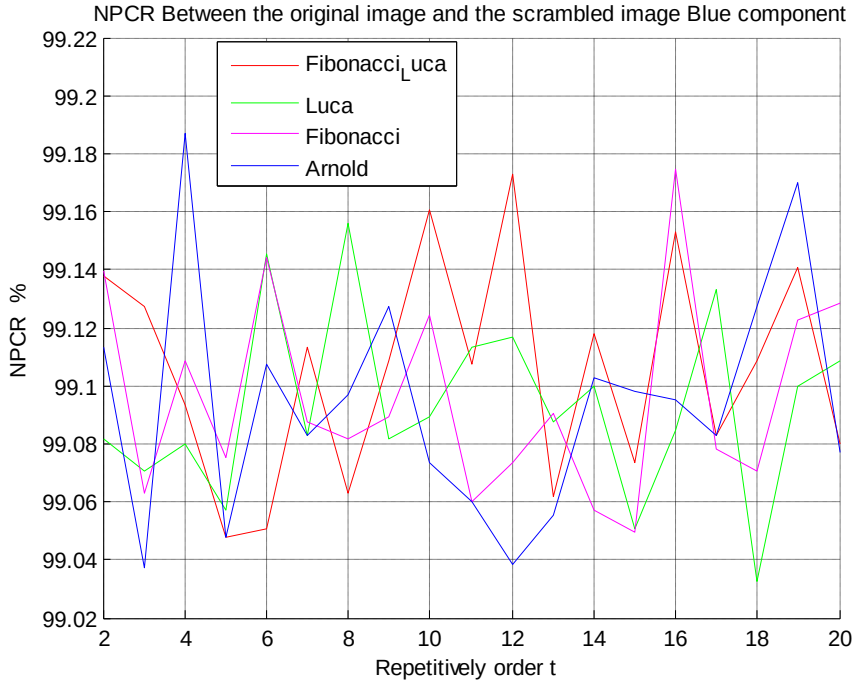

Figure 13: Graphs of the NPCR between the blue components of the original image and the scrambled one

As for the UACI, the technique with the highest values of UACI is chosen. The results relating to the UACI are shown in figures 14, 15, 16. For the order of repetitively 3, there is a choice between the Fibonacci transform and the Fibonacci-Luca transform.

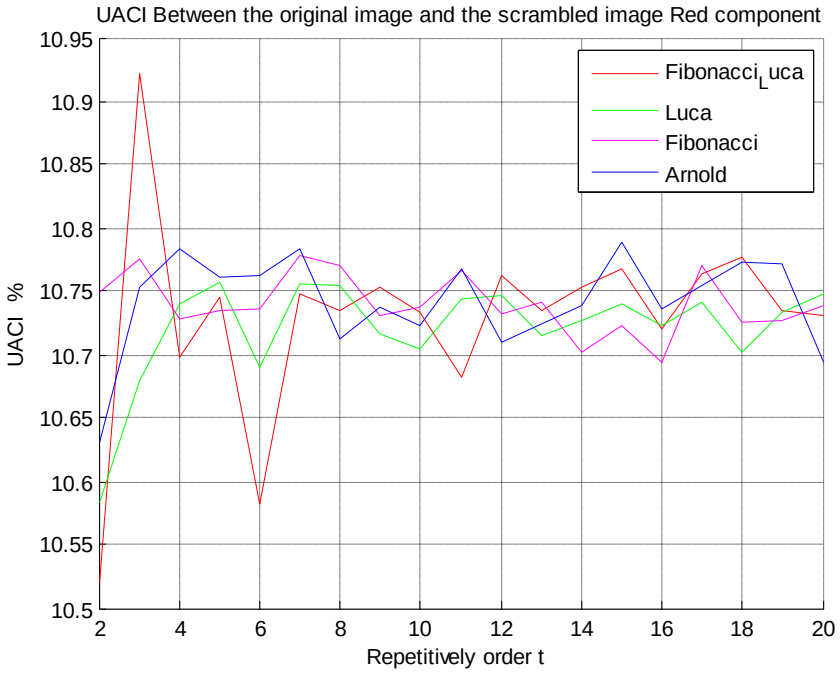

Figure 14: Graphsof theUACIbetween the red components of the original image and the scrambled one

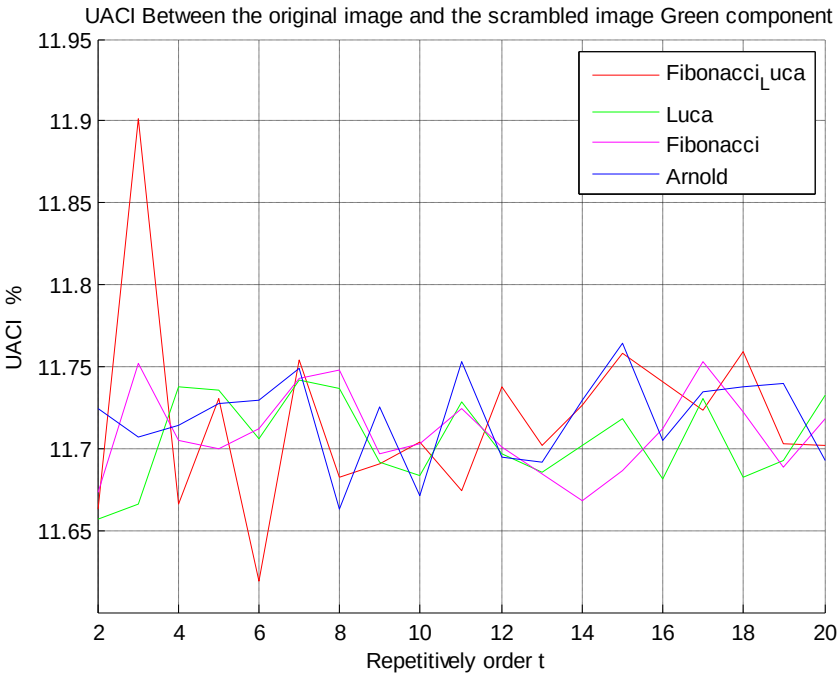

Figure 15: Graphs of the UACIbetween the green components of the original image and the scrambled one

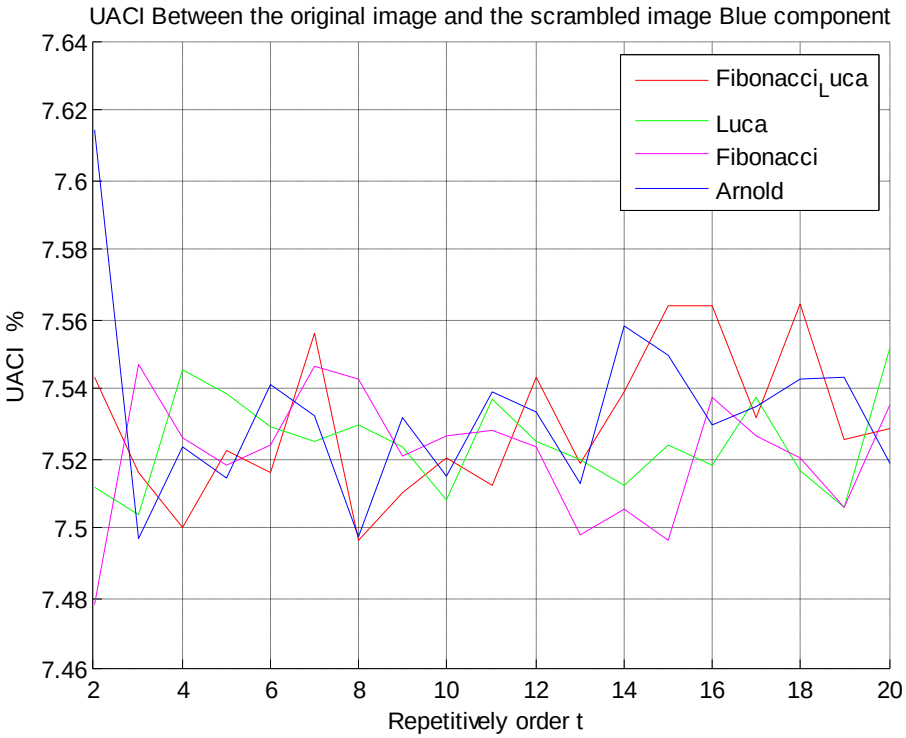

Figure 16: Graphs ofthe UACIbetween the blue components of the original image and the scrambled one

e. Images results after diverse transformation

The figures 17, 18, 19, 20 show a few images obtained after applying varied techniques of scrambling with a different order of repetitively each time and the reconstituted images with the reverse scrambling transforms. The images obtained after scrambling are all actually scrambled, impossible to recognize and incomprehensible.

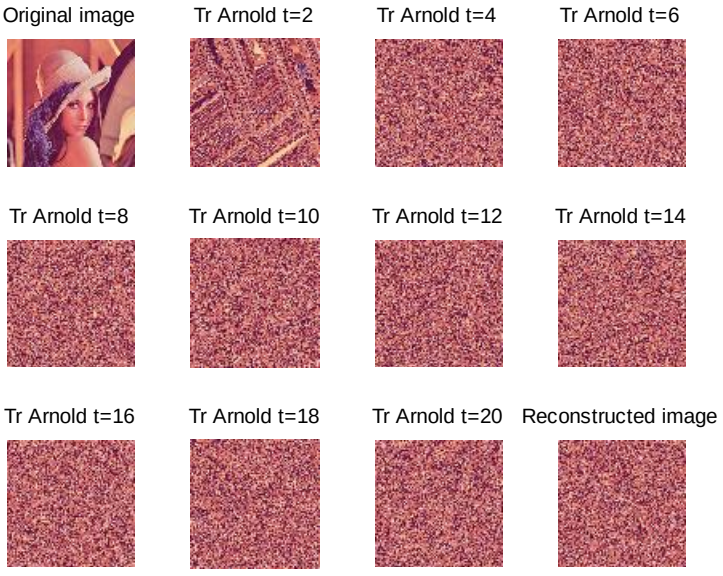

Figure 17: Images obtained through the Arnold transform with differentvalues of the order of repetitivelytandthe reconstituted image after the reverse transform technique

Figure 18: Images obtained through theFibonacci transform with different values of the order of repetitively t and the reconstituted image with the reverse technique

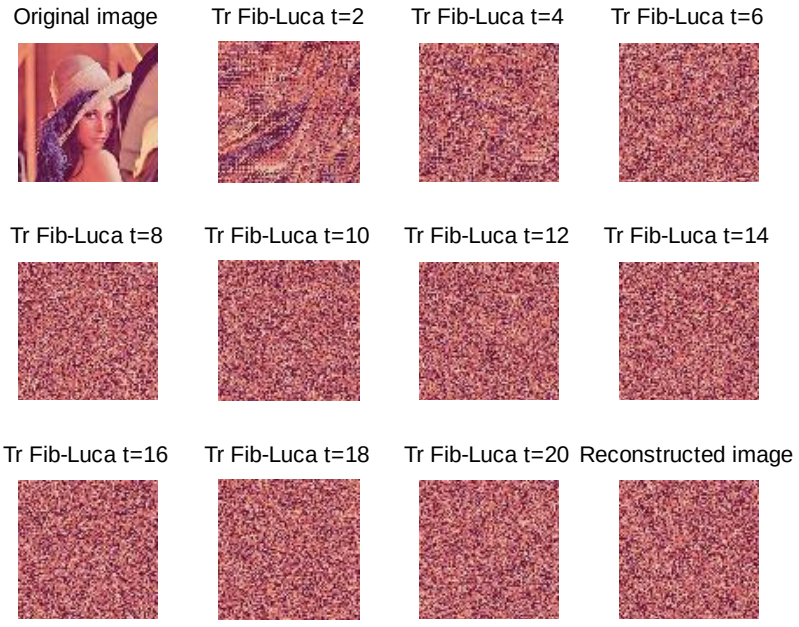

Figure 19: Images obtained through Fibonacci –Luca transform with varied values of the order of repetitively t and the reconstituted image with the reverse technique

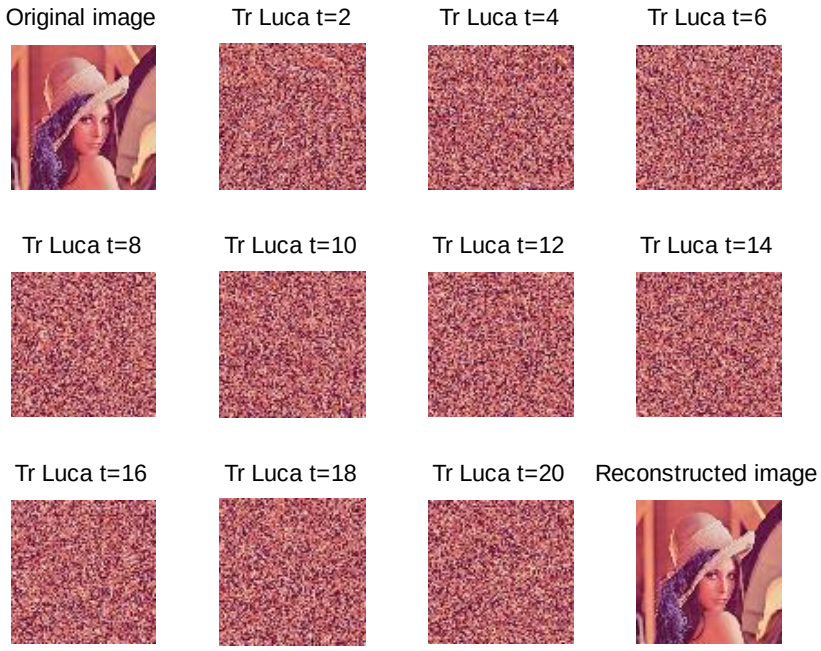

Figure 20: Images obtained through Luca transform with different values of the order of repetitively t and the reconstituted image with the reverse technique

V. Conclusions

This article gives a description of the differences of performances in the application of the varied techniques of image scrambling through a well-set comparison with each other namely: the Arnold transform, the Fibonacci transform, the Fibonacci-Luca transform and the Luca transform. The comparison is made according to the following criteria:the PSNR,the SSIM, the NPCR, and the UACI, thecorrelation coefficient and the response time. The resulting facts tell that when using all the above-said criteria, for an order of repetitively 3, the Fibonacci transform gives the best performance compared with the other techniques.Yet,all of them have this one same characteristic: their rapidity in matter of response time close to 0. 2 second for an order of repetitively t = 2 or t = 3.

These techniques of scrambling could become a full algorithm of encryption if ever combined with an alteration of the range of colors to hide the general aspect of the image for example.

References

[1]. Seesa Paul, "*A Study on various Image Scrambling Techniques*",IJSRD - International Journal for Scientific Research & Development| Vol. 4, Issue 12, 2017 | ISSN (online): 2321-0613

[2]. BhaskarMondal, Neel Biswas, TarniMandal, *"A Comparative study on Cryptographic ImageScrambling",* Proceedings of the Second International Conference on Research in Intelligent and Computing in Engineering pp. 261–268, Conference Paper June2017.

[3]. QIDongxu, ZOUJiancheng, HANXiaoyou. *"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.

[4]. 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.

[5]. W. Ding W.Q.Yan and D.X.Qi, *"Digital Image Scrambling Technology Based on Gray Code",* the 6th International Conference on Computer Aided Design & Computer Graphics, Wen Hui Publishers, Vol.3, pp.900-904. Dec., 1999.

[6]. 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

[7]. W.Ding and al., *"Digital image scrambling technology based on Arnold transformation"*, J.Comput. Aided Des.Comput.Graph. 2001, 13, (4) (China), pp. 338341.

[8]. Wang Lulu, Zhang Chong.: *"Arnold Scrambling Based On Digital ImageEncryptionTechnique"*. J. National Defense Technology Base. 10, (2010).

[9]. HuangFangyuan.: *"Arnold Scrambling Based On Image Scrambling Algorithm And Implementation",* J. Gui Zhou University (Natural Science). 25(3), (2008).

[10]. Wu Lingling, Zhang Jianwei, Geqi.*"Arnold Transformation And Its Inverse Transformation",* J. Micro Computer. 14, (2010).

[11]. Huang Liangyong, XiaoDegui.: *"The Best Scrambling Degree of Arnold Transformation On Binary Images"*. J. Computer Applications. 2 (2009)

[12]. JianchengZou, Rabak K. Ward, Dongxu Qi, *"The generalized Fibonacci transformations and application to image scrambling"*, Conference Paper in Acoustics, Speech, and Signal Processing, 1988. ICASSP-88., 1988 International Conference on June 2004.
[13]. Minati Mishra, Priyadarsini Mishra, M.C. Adhikary and Sunit Kumar, *"Image encryption using Fibonacci-lucas transformation"*, International Journal on Cryptography and Information Security (IJCIS),Vol.2, No.3, September 2012
[14]. R. Rakotomalala, *« Analyse de corrélation, Étude des dépendances - Variables quantitatives Version 1.1 »*, Support, Université Lumière Lyon 2, 27-Dec-2017

IOSR Journal of Computer Engineering (IOSR-JCE) is UGC approved Journal with Sl. No. 5019, Journal no. 49102.

* Mamy Alain Rakotomalala1. "Performances of Image Scrambling Techniques Based on The Permutation Transform." IOSR Journal of Computer Engineering (IOSR-JCE) 20.4 (2018): 55-70