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 43-54
www.iosrjournals.org

Performances Ofimage Encryption Based on Chaotic Artificial Neuronal Networks Combined With The Fibonacci Transform

Mamy Alain Rakotomalala[1*], Falimanana Randimbindrainibe[2],Sitraka R. Rakotondramanana[3], Roméo T. Rajaonarison[4]
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
Department of Telecommunication, High School Polytechnic of Antananarivo, University of Antananarivo, Madagascar
Correspondions Author:Mamy Alain Rakotomalala

Abstract: *This research work is a presentation on the algorithm's performance about a chaotic ciphering based on the Artificial Neuronal Network or ANN with the Fibonacci Transform. All criteria of performance used hereinare: PSNR, SSIM, NPC, UACI, entropy, correlation coefficient, and resistance to noise and to JPEG compression with loss. The image ciphered on ANNyields indicators to cryptanalysts. To improve this result, it is combined with the Fibonacci Transform. As expected, the result gives a ciphered image completely unrecognizable with a lowvalue of PSNR and SSIM and a NPCR value superior to 99.5%, a UACI value likely to even go beyond 28%, a correlation coefficient between -0.004 and 0.0004, an entropy of 7.99 nearing the maximum possible value 8, resistance tosound or noise with a variance of 0.4 and resistance to JPEG compression with loss.*

Keywords: *ANN, Fibonacci Transform, NPCR, UACI, JPEG*

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

I. Introduction

Information security represents one of the major concerns of modern researchers. To that end, what is supposed to be « encryption techniques » have been devised to turn the information into something difficult to comprehend for thosepeople who have no access to it. These techniques could arouse the interest of a great many varieties of entities such as armies, trading businesses, or plain individuals. Illustrations relating to the information and the relevant techniques have already been developed, namely the algorithm AES and the algorithm DES [1 -4]. This articleproposes an algorithm of image encryption basedon a chaotic neuronal network combined with theFibonacci transform [5-11]. The purpose is to study the performance of the given algorithm in terms of PNSR (Peak Signal to Noise Radio), SSIM (Structural SIMilarity), NPCR Number of Pixel Change Rate), UACI (Unified Average Changing Intensity), rxy (correlation coefficient), entropy and resistance to sound or noise and JPEG compression with loss. This article is describing first of all things, the general principle of the neuronal network and the chaotic encryption, followed by the presentation of the algorithm of image encryption based on the neuronal network combined with the Fibonacci transform,and eventually, the presentation and interpretation of the resulting factsby means ofMatlab simulation.

II. Neuronal Artificial Networks And Cryptography

2.1.Mathematical sample of the artificial neuronal network (ANN)

An artificial neuronal network consists of an array of units of simplified processes communicating with each other by means of signals over a large number of weighted connexions. The main aspects of ANN are[12-14]:

- An array of unit processes (« neurons », « cells »);
- An activation time $Y_k$for each unit, corresponding to the output of the given unit ;
- Connexionsbetween units. In general, each connexion is defined by a weight W_{jk}which determines the effect of the signal of unit j a on unit k;
- A rule of propagation fixing the actual entry $S_k$of a unit from its externalcontribution;

- A function of activation F_k, fixing the new level of activation based on the effective entry S_k (t) et the real activation Y_k (t) (that is to say the updating);
- An external entry$\Theta_k$for each unit;
- A method forcollecting data (the initiation rule for it);
- An adequate surrounding allowing the system to work thoroughly, with entry signals as well as error signals requested to carry out the task.

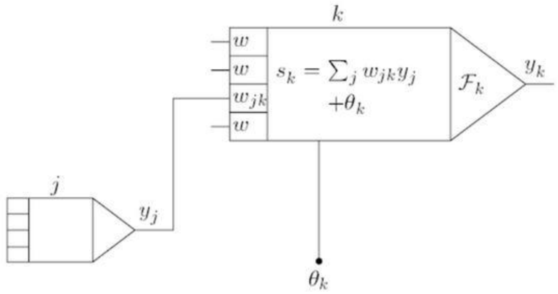


Figure 1:*The basic components of an artificial neuronal network*

2.1.1.Units of processes

Each unit works in a relatively plain manner: reception of the neighboring entries or frommany other external sources and use of these to calculate an output signal propagated to other units. In plus of this process, the second task is the adjustment of the weights.In neuronal networks there are three types of units: the entry units (inputs), receiving data from outside the neuronal network, the outputs sending data out of the neuronal network, and hidden units with inputs and outputs remaining inside the neuronal network.

2.1.2. The connexions between units

In most cases, each unit is supposed to provide a positive contribution as soon as its connexion entry. The total unit k is simplythe weighted sumtotal of all the independent connected outputs plus a variance θk:

$$s_k(t) = \sum_j \omega_{jk}(t)\, y_j(t) + \theta_k(t) \tag{1}$$

If ω_{jk} is positivethe contribution is referred to as an excitation forω_{jk} negative, it is an inhibition.In some cases more complex rules are combined for inputs and there, the excitation inputs have to be differentiated from inhibition outputs. We mean by units, the ones used in propagation referring to the above, which are sigma units. A new rule of propagation, introduced by Feldman and Ballard, has been named the rule of propagation for sigma-pi unit:

$$s_k(t) = \sum_j \omega_{jk}(t) \prod_m y_{jm}(t) + \theta_k(t) \tag{2}$$

2.1.3. Activation and output rules

A rule on the application of a total entry to activate the unit is also seriouslyrequested; thus, a function$F_k$taking up the total entry S_k (t) as well as the actual activation Y_k (t) and producing a new valueof the unit kactivation:

$$y_k(t+1) = \mathcal{F}_k(y_k(t).\, s_k(t)) \tag{3}$$

Most of the time, the function of activation is a non- decreasing one of the unit total entry

$$y_k(t+1) = \mathcal{F}_k(s_k(t)) = \mathcal{F}_k\left(\sum_j \omega_{jk}(t)\, y_j(t) + \theta_k(t)\right) \tag{4}$$

although activation functions are not limited to being non-decreasing ones. As a general rule, some types of threshold functions are used:a plain threshold function (a sgn function), a linear or a semi-linear one, or even one complying with aregular limitation threshold.In that prospect, thesigmoid function has been used.

$$y_k = \mathcal{F}(s_k) = \frac{1}{1 + e^{s_k}} \tag{5}$$

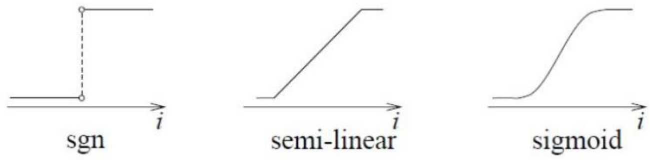


Figure 2:*Varied unit activation signals*

2.2 Ciphering based on chaos

2.2.1 Introduction

Chaotic oscillations are deterministic but strongly influenced by initial conditions and likely to take up a « pseudo-random » aspect. In 1990, Pecora and Carroll published an article in which they had theoretically and experimentally demonstrated about the possibility to synchronize two chaotic systems [15 – 19].

2.2.2 Use of dynamic systems in ciphering

The ciphering system presented herein stands on the consideration of chaotic signals generated by discontinuous regular non-linear movements, discrete systems represented by the equation[15-19]:

$$x_{k+1} = f(x_k);\ x_0 \epsilon I \tag{6}$$

or /and in which the unit interval or the square unit is$f: I \to I$; the purpose being to bring out the mathematical properties of these chaotic systems likely to increase the security of the ciphering systems based on dynamic systems.

A dynamic system of the type (6) is said to be chaotic if the following requirements are met:

- Sensitivity to initial conditions :

$$\exists \delta > 0\ \forall x_0 \in I, \varepsilon > 0\ \exists n \in \mathbb{N}, y_0 \in I:\ |x_0 - y_0| < \delta \Rightarrow |f^n(x_0) - f^n(y_0)| > \delta \tag{7}$$

- Topologicaltransitivity:

$$\forall I_1, I_2 \subset I \exists x_0 \in I_1, n \in \mathbb{N}:\ f^n(x_0) \in I_2 \tag{8}$$

- Density of the recurrence point:

For

$$P = \{p \in I / \exists n \in \mathbb{N}:\ f^n(p) = p\} \tag{9}$$

The set of recurrence points in f. $P$is dense in$I$:

$$\bar{P} = I \tag{10}$$

III. Presentation Of The Image Chaotic Ciphering Algorithm Based On The Neuronal Network Combined With The Fibonacci Transform

The algorithm proposed in figure 3 stands on the use of RNA (ANN) and with the technique of scrambling or the Fibonacci transform.

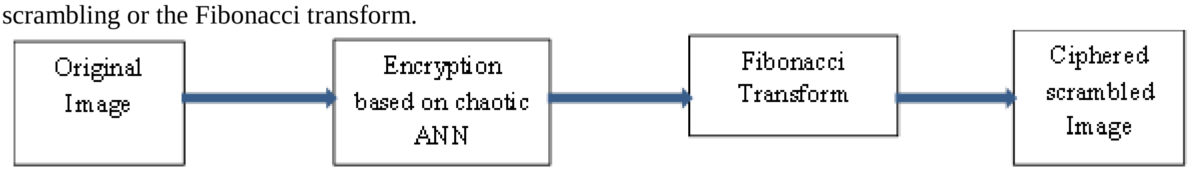


Figure 3:*Algorithm of proposed ciphering*

3.1. Image ciphering based on Artificial Neuronal Network

Neuronal chaotic networks offer a great capacity of memory. Each memory is encoded by an instable chaotic recurrent orbit. Our purpose consists in using a neuronal chaotic network to cipher an image. A neuronal network is said to be chaotic when its weights and variancesare determined by a chaotic sequence.Let's take g digital signal of M long and g (n) the unit value of one byte of the signal g in the position n [12-14].

Stage1: Charging an image and measuring its size

Stage2: Fixing the parameter μ and the initial point x (0) of the network so as to get the equation (1) to assume a chaotic behavior.

Stage 3: Developing the chaotic sequence x (l), x (2)... x (M) making use of the one-dimensional simple logistic card defined within an interval E by:

$$x(n+1) = \mu x(n)(1 - x(n)) \tag{11}$$

Stage 4: For n moving from 0to M-1, all the parameters of the chosen neuronal network are calculated.For the calculationof the weights and the parameter theta, the following formulas are used:

$$w_{ji} = \begin{Bmatrix} 1\ sii = jetb(8n+i) = 0 \\ -1\ sii = jetb(8n+i) = 1 \\ 0\ sii \neq j \end{Bmatrix} \quad (12)$$

$$\theta_i = \begin{Bmatrix} -\frac{1}{2} sib(8n+i) = 0 \\ \frac{1}{2} sib(8n+i) = 1 \end{Bmatrix} \quad (13)$$

And for thecalculation of the error the following is obtained:

$$d_i' = f(\sum_{i=0}^{7} w_{ji} . d_i + \theta_i) \quad (14)$$

And the ciphered signal is given by:

$$g(n) = \sum_{i=0}^{7} d_i 2^i \quad (15)$$

Stage5: Theciphered ‘g’ is obtained so the algorithm is over.

The process of deciphering is exactly the same as the above process, except that the input signal of deciphering to the chaotic neuronal network (CNN) has to be ‘g’ (n) and its output has to be ‘g’ (n).

For the case of an image,the pixels are processed by neurons. The expected result of the ciphering is a disordered image. During the stage of deciphering CNN, inthe same chaotic system and its initial state, that is to say the same binary chaotic system, the original image can be properly restored making use of CNN deciphering.

Supposingthat theciphering is known without the binary chaotic sequence : when the ANN is applied to a signal of M long, 8M bytes are required. The number of possible ciphered items is 8 × M. Considering the raw data of 65536 bytes, 8M is equal to 524288 and all the results likely to be got are 252428 (≈ 10157810). In chaotic systems, it is common happening that:

- There is a clear dependence on initial conditions.
- Dense, limited but non- recurrent or almost-recurrent courses develop in the space of states.

This will result in the unpredictability of the binary chaotic sequence. Actually it is a pretty difficult task to properly decipher a ciphered image through exhaustiveresearch without knowing x (0) andμ. Therefore CNNis among the most reliable in matter of security.

3.2 The Fibonacci transform

The Fibonacci transformis one among the many techniques of image scrambling. Scrambling is a technique usedto turn an image into something incomprehensible and scrambled. Several publications [3-4, 7, 20] have tried to give an appropriate definition of this word. In this article, the emphasiswill be laid on the scrambling based on permutation.Leonard de Pise known as Fibonacci took interest in the sequence called Fibonacci series as follows:

$$F_n = \begin{cases} 0 & si \quad n=1 \\ 1 & si \quad n=2 \\ F_{n-1} + F_{n-2} & \end{cases} \quad (16)$$

The Fibonacci series obtained are: 0, 1, 1, 2, 3, 5, 8, 13, 21, 34… In 2012, Minati Mishra, Priyadarsini Mishra, M.C. Adhikary**,** and Sunit Kumar proposedthe use of theFibonnacciseries as a matrix of transformation [7-8]:

$$T_i = \begin{pmatrix} F_i & F_{i+1} \\ F_{i+2} & F_{i+3} \end{pmatrix} \quad (17)$$

The Fibonacci transform is defined by:

$$\begin{pmatrix} x' \\ y' \end{pmatrix} = T_i \begin{pmatrix} x \\ y \end{pmatrix} (modN) \quad (18)$$

x’ and y’ being a new position of the pixel ; x et y as the original position of this pixel, N asthe size of the image matrix; T_i as the Fibonaccitransform matrix ;and$F_i$asthe ranking word for the Fibonacci series, the figure 4shows the image obtained through the Fibonacci transform, which is a scrambled image.

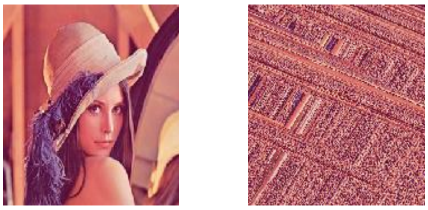


Figure 4: *Illustration about Fibonacci transform*

IV. Results And Comments

The following results have been obtained through Matlab simulation.The parameters used for the evaluation of the selected algorithm are: the PSNR (Peak Signal to Noise Ratio),theSSIM(Structural SIMilarity), the NPCR(Number of Pixel change rate), the UACI (Unified Average Changing Intensity), therxy (coefficient of correlation), the entropy and the response time of the algorithm.

- ThePSNR isa unit of distortion used for measuring in matter of digital images. The PSNR is defined by the following formula[10] :

$$PSNR = 10.\log_{10}\left(\frac{d^2}{EQM}\right) \tag{19}$$

dbeing the possible maximum value for a pixel. In general d=255 and EQM is the average quadratic error definedby:

$$EQM = \frac{1}{mn}\sum_{i=0}^{m-1}\sum_{j=0}^{n-1}(I_0(i,j) - I_r(i,j))^2 \tag{20}$$

- The Structural Similarity or SSIM is a reliable unit measurement for the similarity between two digital images[17].

$$SSIM(X,Y) = \frac{(2\mu_X\mu_Y + c_1)(2\sigma_X\sigma_Y + c_2)(2COV(X,Y) + c_3)}{(\mu_X^2 + \mu_Y^2 + c_1)(\sigma_X^2 + \sigma_Y^2 + c_2)(\sigma_X\sigma_Y + c_3)} \tag{21}$$

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

- The NPCR isusedto measure the percentage of pixel differentiating two given images. The NPCR isdefined by [11] :

$$NPCR^{R/G/B} = \frac{\sum_{i=1}^{H}\sum_{j=1}^{W} D^{R/G/B}{}_{i,j}}{W \times H} 100\% \tag{22}$$

with

$$D_{i,j}^{R/G/B} = \begin{cases} 0 & si \quad C_{i,j}^{R,G,B} = \overline{C}_{i,j}^{R,G,B} \\ 1 & si \quad C_{i,j}^{R,G,B} \neq \overline{C}_{i,j}^{R,G,B} \end{cases} \tag{23}$$

$C_{i,j}^{R,G,B}$ et $\overline{C}_{i,j}^{R,G,B}$ representthe Red, Green and Blue channel colors of both images

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

W et$H$ represent thewidth and the length of the image.

- The UACI is the average value of two image light intensities [11].

$$UACI^{R/G/B} = \frac{1}{W \times H} \sum_{i=1}^{H} \sum_{j=1}^{W} \frac{C_{i,j}^{R/G/B} - \overline{C}_{i,j}^{R/G/B}}{2^{L^{R/G/B}} - 1} \times 100\% \qquad (24)$$

- The coefficient of correlation [21] is definedby :

$$r_{X,Y} = \frac{COV(X,Y)}{\sqrt{V(X).V(Y)}} = \frac{COV(X,Y)}{\sigma_X \sigma_Y} \qquad (25)$$

*COV(X, Y)*being the covariance between the random variables X et Y ; $V(X), V(Y)$ being the variance of X and Y ; σ_X, σ_Y the classical gaps between X and Y.

- The covariance is equal to the expectation of the product of the targeted variables.The covariance isdefinedby the following formula :

$$COV(X,Y) = E[(X - E[X])(Y - E[Y])] \qquad (26)$$

E being the mathematical expectation; X, Y being any random variables.

- The variance is definedbythe following formula :

$$V(X) = E[(X - E[X])^2] = COV(X,X) \qquad (27)$$

E being the mathematical expectation; COV being the covariance.

The purpose of the covariance isto quantizethe liaison between two random variables X et Y, so as to emphasize the aim of the liaisonand its intensity. The coefficient of simple linear correlation ofBravais-Pearson (or of Pearson), as it is called, is a standardizationof the covarianceby the product of the classical variable gaps. The correlation varies between -1 and +1. The nearer the extreme values they are, the more likely and the stronger the similarity between the variables is. The expression « strongly correlated »means that both variables are quite similar and that their correlation move towards 1. The expression « linearly independent » or « total absence of correlation » means that there is no correlation at all, thus no similarity between the two random variables. The expression « thorough correlation » means that the value of r is ± 1.

- The entropyis definedby the following formula [10]:

$$H(X) = -\sum_{x \in X} p(x) \log_2 p(x) \qquad (28)$$

X being a random variable; the entropy measuresthe uncertaintyrelating to the resultof the random variable X. This uncertainty is maximum when the value is nearing 8.

4.1 Results obtained after chaotic ciphering based on ANN

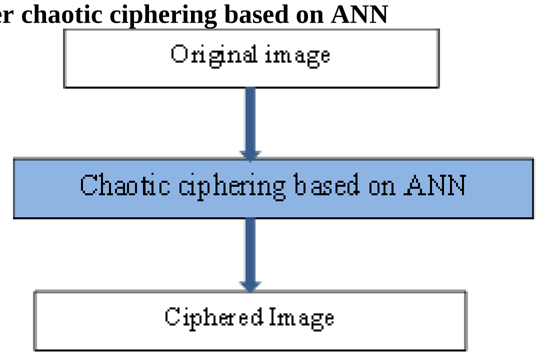
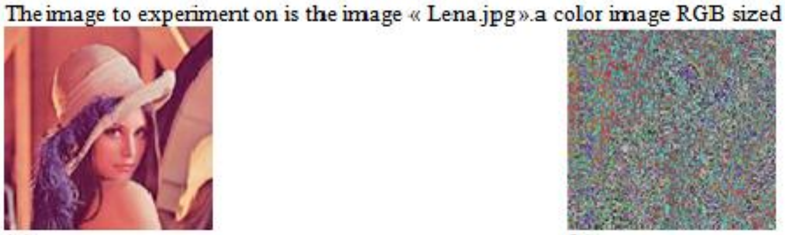


Figure 5: *Chaotic ciphering based on ANN*

The image to experiment on is the image « Lena.jpg ».a color image RGB sized 256x25.



(a) (b)

Figure 6 : **(a)** *Original Image* *(b) chaotically ciphered image based on ANN*

Table 1: *PSNR, SSIM, NPCR, UACI and rxy between the original image and the ciphered image*

	PSNR	SSIM	NPCR en %	UACI en %	Rxy
Red components	7.58498206801303	0.00668035819594577	98.272705078125	27.8137446384804	-0.0257198550382347
Green components	8.57882442669835	0.00288029499037004	98.272705078125	9.23680922564338	-0.0322423269697677
Blue components	10.1488325109972	0.0142573181289539	98.272705078125	8.86174819048713	0.0310892525267459

These results prove that the ciphered image is already a quite different image compared with the original image: with a PSNR nearing 10, an SSIM nearing 0.01, a NPCR nearing 98%,amaximumUACI of 27.8%and with a correlation coefficient rxybetween-0.03 and 0.03. Yet, for cryptanalysts, the ciphered image can yield any indicator of the original image.In order to improve these results, this ciphering technique is combined with the Fibonacci transform.

4.2 Results obtained after using the Fibonacci transform

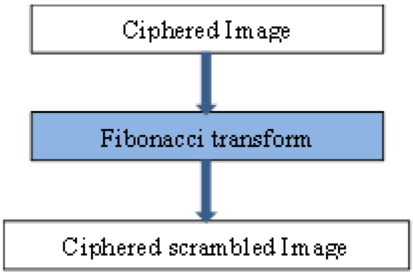


Figure 7: *The Fibonacci Transform process*

(a) (b)

Figure 8 : *(a)CipheredImage resulting from chaotic ciphering based on ANN (b) ciphered scrambled Image from the Fibonacci transform*

Table 2: *PSNR, SSIM, NPCR, UACI and rxy between the original image and the ciphered scrambled image*

	PSNR	SSIM	NPCR en %	UACI en %	rxy
Red components	7.65477802328489	0.0119789286915041	99.57275390625	28.0444575291054	-0.000998185711316714
Green components	8.699098249713	0.00882008760771249	99.6475219726563	9.34170592064951	0.000444496411413061
Blue components	10.0347914076817	0.00931943399134347	99.54833984375	9.07589183134191	-0.00400393766166028

The image resulting from the application of the Fibonacci transform or the ciphered scrambled image - Figure 8 – is a scrambled image with no indicator of any kind of the original image.

The fact of combining the chaotic ciphering based on ANN with the Fibonacci Transform results in a blatant improvement of expected results as shown in table2. If the PSNR andthe SSIM stay more or less the same, there is clear evidence of actual improvements relating to the NPCR, the UACI and especially the rxy. Here therxy variesbetween -0.004 and 0.004, which means there is no correlation of any kind between the original image and the ciphered scrambled one.A NPCR nearing 99% means that only 1% of the pixels have remained unchanged.

The entropy of the ciphered scrambled image is 7.99338439532115which isquite near 8. This result proves that the uncertainty is maximum as for the recognition of the image.

4.3 Reconstruction

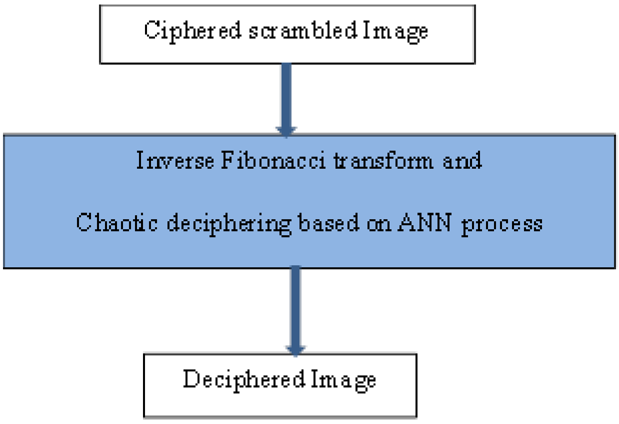


Figure 9: *The decipheringprocess*

Table3 :*PSNR, SSIM, NPCR, UACI and rxy between the original image and the deciphered image*

	PSNR	SSIM	NPCR	UACI	rxy
For red components	Infinite	1	0	0	1
For green components	Infinite	1	0	0	1
For blue components	Infinite	1	0	0	1

The results in Table 3 and Figure 9 show that after deciphering, a complete restoration of the original image is obtained.

(a) (b)

Figure 10: *(a)Ciphered scrambled image (b) Deciphered image*

4.3 Performance against noise attack

The objective is to know the noiseeffecton the algorithm. Isit possible to recognize the deciphered image compared with theoriginaloneafter noise attack? The Figure 11develops the action of a noise attack on the algorithm.

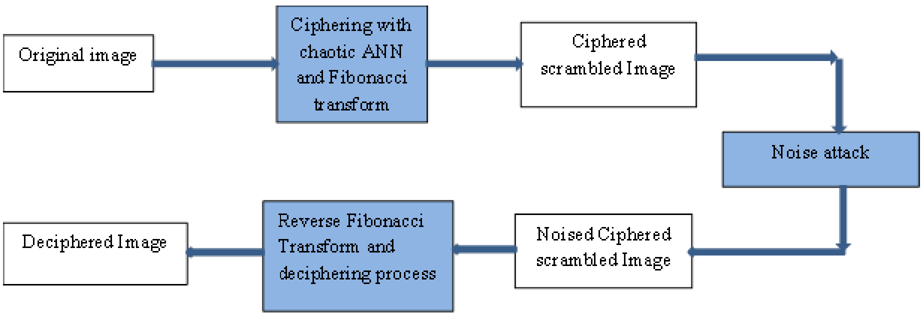


Figure 11: *Noiseattackprocess*

The noise is considered as an impulse noise type “salt & pepper”.

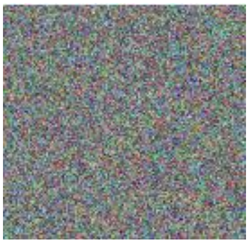
- Case 1: noise with variance 0.2, we obtain the results in table 4 and 5 and the figure 12.

Table 4: *PSNR, SSIM, NPCR, UACI and rxybetween the original image and the deciphered scrambled imageafternoiseattack(noise with variance 0.2)*

	PSNR	*SSIM*	*NPCR en %*	*UACI en %*	*rxy*
For red components	7.5849820680 1303	0.00668035819594 577	98.272705078125	27.813744638 4804	- 0.02571985503823 47
For green components	8.5788244266 9835	0.00288029499037 004	98.272705078125	9.2368092256 4338	- 0.03224232696976 77
For blue components	10.148832510 9972	0.01425731812895 39	98.272705078125	8.8617481904 8713	0.03108925252674 59

Table 5: *PSNR, SSIM, NPCR, UACI and rxy between the original image and the deciphered image after noise attack (noise with variance 0.2)*

	PSNR	SSIM	NPCR en %	UACI en %	rxy
For red components	14.55133600309 14	0.23309685594561 5	20.0302124023 438	5.51489138135 723	0.653707975278 915
For green components	15.28963052128 31	0.25788781990504 1	19.7326660156 25	2.08151424632 353	0.703341525802 391
For blue components	16.31187314466 1	0.22901535625315 5	19.8547363281 25	2.05272001378 676	0.588863731390 527



(a)

(b)

Figure 12 : *(a)Ciphered scrambledimage submitted to noise with variance 0.2 and (b) the corresponding deciphered image*

- Case 2: noise with variance 0.4, we obtain the results in table 6 and 7 and the figure 13.

Table 6: *PSNR, SSIM, NPCR, UACI and rxybetween the original image and the ciphered image after noise attack (noise with variance 0.4)*

	PSNR	SSIM	NPCR en %	UACI en %	rxy
For red components	7.584982068013 03	0.0066803581959457 7	98.272705078 125	27.8137446384 804	- 0.02571985503823 47
For green components	8.578824426698 35	0.0028802949903700 4	98.272705078 125	9.23680922564 338	- 0.03224232696976 77
For blue components	10.14883251099 72	0.0142573181289539	98.272705078 125	8.86174819048 713	0.03108925252674 59

Table 7:*PSNR, SSIM, NPCR, UACI and rxy between the original image and the deciphered one after noise attack (noise with variance 0.4)*

	PSNR	SSIM	NPCR en %	UACI en %	rxy
For red components	11.55976244468 79	0.129052363949444	39.755249023437 5	10.96771240234 38	0.4388523412995 88
For green components	12.18901769127 42	0.140177385354227	40.167236328125	4.240130256204 04	0.4709105985888 15
For blue components	13.16751121775 06	0.115447616258301	40.029907226562 5	4.256334491804 53	0.3525804838533 41

(a)

(b)

Figure 13 : *(a)Ciphered scrambledimage submitted to noise with variance0.4 and (b) the corresponding deciphered image*

The resultsin the table 5,7 and Figures 12, 13show us that after submission to impulse noise with variance 0.2 and 0.4, the deciphered image is likely to be recognized but with a slightly sounding aspect.With relatively low PSNR, SSIM, NPCR and UACI values compared with the original image, the deciphered image can still be recognized. This is also due to the high values of the correlation coefficients.The table4,6giveus the results between the original image and the ciphered scrambled image under noise submission, which is a totally unrecognizable image.

4.4 Performance against compression

The purpose is to know whether after submission to compression the deciphered image can be recognized compared to the original image.The Figure 14 represents the processof submission to the compression JPEGeffect with loss of the algorithm.

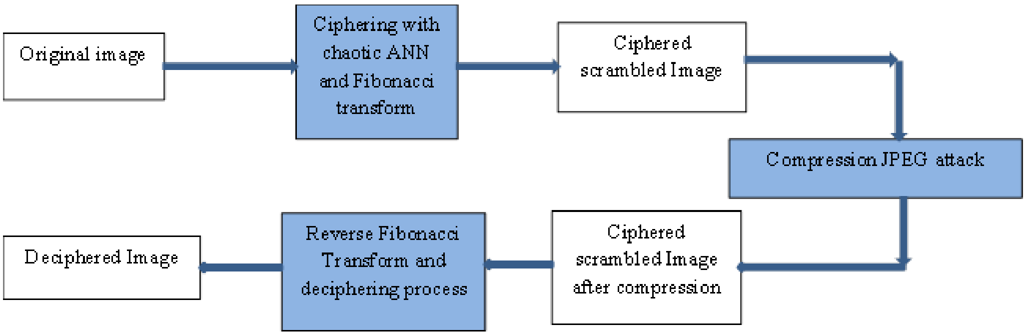


Figure 14:*The process of compression JPEG attack*

(a)

(b)

Figure 15 : *(a) Original image(b)ciphered scrambled image*

(a)

(b)

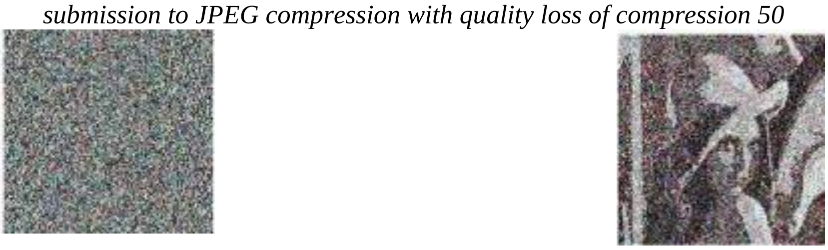
Figure 16 : *(a)Ciphered scrambled image submitted to JPEG compression with quality loss of compression100 and (b) the corresponding deciphered image*

Table 8: *PSNR, SSIM, NPCR, UACI and rxy between the original image and the deciphered one after submission to JPEG with loss in compression quality100*

	PSNR	SSIM	NPCR en %	UACI en %	rxy
For red components	9.69086634673453	0.153780703920413	99.578857421875	24.1105562097886	0.528519635595804
For green components	14.0455117476798	0.222608546027231	99.1317749023438	5.45793720320159	0.695818043451142
For blue components	13.5921228084825	0.18914381299824	99.237060546875	6.86221852022059	0.62902902273541

Table 9: *PSNR, SSIM, NPCR, UACI and rxy between the original image and the deciphered one after submission to JPEG compression with quality loss of compression 50*

	PSNR	SSIM	NPCR en %	UACI en %	rxy
For red components	9.58736931577285	0.147349545472652	99.5269775390625	24.7352510340074	0.521451924317748
For green components	13.4054853586169	0.147349545472652	99.0325927734375	5.13680850758272	0.65654182918824
For blue components	12.9891557142416	0.166109040686109	99.3133544921875	6.98987175436581	0.587492020669813



(a) (b)

Figure 17 : *Ciphered scrambled image after submission to JPEG compression with quality loss of compression 50 and the corresponding deciphered image*

According to the results in table8 and table9:

- The PSNR and SSIM values are relatively low, which means the original image is completely different from the deciphered one.
- The NPCR values are quite high, which shows that a great amount of the pixels in the original image and the deciphered one are actually different.
- The UACI values are relatively medium, which means that even if the pixels in both images are different, the difference is fairly good to allow the recognition of the image.
- The rxy values are high, that is to say, over 0.5, which shows that there is a good correlation or similarity between the originalimage and the deciphered one.

  Consequently, the deciphered image is recognizable but of alower quality compared with the original image:Figures 15, 16, 17. It can be deduced that this algorithm has a good performance when submitted to JPEG compression with loss.

V. Conclusion

One research relating to secure important information has been presented throughout this article. The chosen algorithm, that is to say, the algorithm of chaotic image ciphering based on artificial neuronal network combined with the Fibonacci Transform makes a thorough reconstitution of the original image possible after deciphering. The ciphered scrambled image is totally unrecognizable after the ciphering operation.The results obtained right after give PSNR values under 10 for red and green components and equal to 10 for blue ones, SSIM values nearing 0.01 and quite high NPCR values over 99.5%. Moreover, the correlation coefficient between the original image and the ciphered scrambled one is 0.004 for the blue components and about 0.0009 for the other components, which is evidence of the non-existence of correlation between the original image and the ciphered scrambled one. Once more, the results obtained have shown that the selected algorithm keeps a quite good performance when submitted to sound or noise effects and JPEG compression with loss.With a noise attack with0.4 variance, a correlation coefficientaround 0.4 between the ciphered scrambled image and the deciphered one, can be obtained. And as for theJPEG compression with a loss in the quality of compression 50, correlation coefficients over 0.5 between the ciphered scrambled image and the deciphered one can be obtained.

As a conclusion, this algorithm is quite useful to secure imagetransmission in surroundings or areas strongly submitted bynoise and compression attack.

References

[1]. Manoj, .B,Manjula and N.Harihar, *"Image Encryption and Decryption using AES"*, International Journal of Engineering and Advance Technology (IJEAT), vol.1, issue.5, (6) (2012),290-294.

[2]. KundankumarRameshwarSaraf, Vishal PrakashJagtap and Amit Kumar Mishra, *"Text and Image Encryption Decryption Using Advance Encryption Standard"*, International Journal of Emerging Trends and Technology in computer science (IJETTCS),vol.3, issue.3, (5-6) (2014), 118-126.

[3]. AshawakMahmood and Alabaichi, *"Color image encryption using 3d chaotic map with AES key depend S-Box"*, International Journal of Computer Science and Network security (IJCSNS), vol.16, No.10,Iraq (10) (2016).

[4]. Vinita SHadangi, Shiddharth Kumar Choudhary, K. Abhymanyu Kumar Patro and BidhudendraAcharya, *"Novel Arnold Scrambling Based CBC-AES Image Encryption"*, International Journal Of Theory an Applications (IJCTA), Vol.10, 15 (11) (2017).

[5]. Lini Abraham and Neenu Daniel, *"Secure Image Encryption Algorithms: A Review"*, International Journal of Scientific& Technology Research (IJSTR), Vol.2, issue.4, (4) 2013.

[6]. Romi Singh, Shipra Sharma andShikha Singh, *"Image Encryption using Block Scrambling technique"*, International Journal Computer Technology Applications (IJCTA) , Vol.5 , India 3 (5) (2014) 963-855.

[7]. Minati Mishra, Priyadarsini Mishra, M.C. Adhikary and Sunit Kumar, *"Image Encryption using Fibonacci-Lucas Transformation"*, International Journal Of Cryptography and Information Security (IJCIS), Vol.2, No.3, Kolhan University, (8) (2012).

[8]. JianchengZou, Rabab K. Ward and DongxuQi,*"The Generalized Fibonacci Transformations and application to image scrambling"*,Conference Paper in Acoustic Speec and Signal Processing, University of British Columbia, (01) (2015).

[9]. MinalChauhan and RashminPrajapati, *"Image Encryption Using Chaotic Based Artificial Neural Network"*, International Journal of Scientific & Engineering Research (IJSER), Vol.5, Issue.6, (6) (2014).

[10]. Amber ShaukatNasim M.Sc., Junqin Zhao, WeichuangGuo and Ruisong Ye, *"Chaos based cryptography and image encryption"*, University of Applied Sciences, Luebeck, Germany (2012)

[11]. Junquin Zhao, WeichungGuo, Ruisong Ye, *"A Chaos-based Image Encryption Scheme Using Permutation-Substitution Architecture"*, International Journal of Computer Trends and Technology (IJCTT), Vol.15, No.4, Shantou University, China (9) (2014)

[12]. AreedAbdallah, MokhatarBeram and Ahmed Salah Al-DeenAbdallah, *"Hybrid Image Encryption based on Genetic algorithm and Neural Network"*, International Journal of Engineer Research and Technology (IJERT), Vol.6; Issue.6;University of Sudan (7) (2017).

[13]. Qurban Ali Memon, "Neural network based double encryption for JPEG2000 image", Journal of ICT, Vol.16, No. 1, United Arab Emirates University, Arab (6) (2017) 137-155

[14]. S. Nythia, S. Priyaa, R. Priyanka and S. Saranya, *"Face image recognition and scrambling for privacy using neural networks"*, International Journal of Scientific & Engineering Research (IJE) , India (2017)

[15]. DhanalaxmiBanavath and SrinivasuluTadisetty, *"A Novel Image Self--Adaptive Encryption Algorithm Based On Composite Chaotic System"*, Vol.9, No.1, India (1-6) (2017) 160-164.

[16]. PunitaKumari andKalpana Jain, *"Digital Image Encryption Technique Using Block BasedScrambling and Substitution"*, Global Journal of Computer Science and Technology, Vol.17, USA (2017)

[17]. Seesa Paul, *"A Study on various Image Scrambling Techniques"*, International Journal for Scientific Research & Development| (IJSRD), Vol.4, Issue.12, India (2017).

[18]. V.V.M Sireesha and Y.

[19]. V.D. PushpaLatha, *"Implementation of Image Encryption and Compression using Chinese Reminder Theorem and Chaotic Logistic Maps"*, International Journal of Advanced Research in Computer and Communication Engineering (IJARCCE)CertifiedISO 3297:2007 , Vol.6, Issue.5,(5) (2017)

[20]. Brasher J. Hamza, *"HD remote sensing image protection approach based on modified AES Algorithm"*, International Journal of Video Image Processing and Network Security (IJIVPNS-IJENS), Vol.17, Iraq (2017)

[21]. Yicong Zhou, SosAgaian, Valencia M. Joyner and Karen Panetta, *"Two Fibonacci P-code Based Image Scrambling Algorithms"*,http://proceedings.spiedigitallibrary.org/, 1 (20) (2017)

[22]. R. Rakotomalala, *"Analyse de corrélation, Étude des dépendances - Variables quantitatives Version 1.1"*, Support Université Lumière Lyon 2, 27 (12) (2017)

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

Mamy Alain Rakotomalala. «Performances Ofimage Encryption Based on Chaotic Artificial Neuronal Networks Combined With The Fibonacci Transform." IOSR Journal of Computer Engineering (IOSR-JCE) 20.4 (2018): 43-54.