TELKOMNIKA, Vol 16, No 1: February 2018, pp. 402~414
ISSN: 1693-6930, accredited **A** by DIKTI, Decree No: 58/DIKTI/Kep/2013
DOI: 10.12928/TELKOMNIKA.v16i1.6583

The Quality of the New Generator Sequence Improvent to Spread the Color System's Image Transmission

Mohamed Krim, Adda Ali-Pacha*, Naima Hadj Said
Laboratory of Coding and Security of Information, Faculty of Electrical Engineering, University of Science and Technology of Oran (USTO),BP 1505 El M'Naouer Oran 31000, Algeria,
Ph/Fax: +213-41 56 03 43/41 56 03 01
*Corresponding author, e-mail: a.alipacha@gmail.com

Abstract

This paper shows a new technic applicable for the digital devices that are the result of the finite's effect precision in the chaotic dynamics used in the coupled technic and the chaotic map's perturbation technics used for the generation of a Pseudo-Random Number Generator (PRNGs).The use of the pseudo- chaotic sequences coupled to the orbit perturbation method in the chaotic logistic map and the NewPiece-Wise Linear Chaotic Map (NPWLCM). The pseudo random number generator's originality proposed from the perturbation of the chaotic recurrence. Furthermore the outputs of the binary sequences with NPWLCM are reconstructed conventionally with the Bernoulli's sequences shifts map to change the shapes with the bitwise permetation then the results in simulation are shown in progress.After being perturbed, the chaotic system can generate the chaotic binary sequences in uniform distribution and the statistical properties invulnerable analysis. This generator also has many advantages in the possible useful applications of spread spectrum digitalimages, such as sensitive secret keys, random uniform distribution of pixels in Crypto system in secure and synchronize communication.

Keywords*: perturbation, PRNGs, Logistic map, NPWLCM, bernoulli's shift map, bitwise permeation*

1. Introduction

The chaotic secure communication is one important application of chaos theories .So how can we secure and synchronize a communication system in using the chaotic system with the direct spread spectrum sequence (DS-SS)? Initially in the field of the chaotic secure communication we've two types of the chaotic encryption systems: one is the analogue chaotic secure system based on the chaotic synchronization.The other is the digital encryption system based on the chaotic pseudo-random sequence [1] with many uses as in the military communication[2].The pseudo chaotic generations sequences of the random numbers based on a chaotic map are important in every aspect of the hiding information whith the cryptography [3] and the spread spectrum [4]. A random number generator (RNG) is a deterministic algorithm that seed outputs a longer sequence on in put that are computationally distinguishable from an uniform chosen random sequence. Different methods exist for generating chaotic sequences of the chaotic map's type.It is the logistic map which is the most studied discrete nonlinear map has been used in many scientific fields.Also this discrete map has a known mathematic distribution. Here also the logistic map makes a good parameter for using in the designs of the random bits generators. In the Chaotic spread spectrum communication systems a different user can be assigned to different generated sequences.

A number of the spreding technics images have been proposed- including the chaos-based image spreding- to provide a better solution for the security problem of the digital image. These technics give a good combination of speed and security. The use of the chaotic sequence as the spreading sequences has been proposed as it must seem absolutely random. These generator's (CPRNG) chaotic pseudo-random number has been analyzed in [5]. So we need a digital chaotic generator with important cryptographic properties such as balance on {0, 1} long-cycle length, high linear complexity, like function of the auto-correlation and the function cross-correlation near to zero [6].According to these properties, chaos sequence can be used as the random numbers generator. One of the simple systems are used to generate chaotic sequence is in the logistic map [7].The digital new system implementation gave more problems

Received Jun 6, 2017; Revised January 4, 2018; Accepted January 14, 2018

because of the finite precision of the digital representation.The methods have been proposed to find out the problems of the finite representation [8]. In this study we followed this condition: The cascading of several chaotic systems: the improvement is not significant because it gets another chaotic function that will in turn have the specific problems in the finite representation. The application of a perturbation presents an efficient solution to avoid redundancy in the cycles of the chaotic sequences. Several sources of disturbance are used for this purpose, such as the linears feedback shifts registers (LFSRs) .The number of the sequence generated by (LFSR) may be insufficient to wideband the direct spread spectrum sequence (DS-SS) in a very large number of users [7].Also the LFSR technics provide particular flexibility in incorporating security into multiple user systems [9]. The study in the non-linear dynamical system has developed the chaotic theories. This last is caracterized by: a well done function of the auto-correlation by spreadingas uniformal as, bya cycle of the maximal lenght which is the Hardwar implementation orthe easy device [9].Practicly ananalysis of the periodicity of chaotic requires full search over all possible initial values [10]. With these proprities; we propose chaos function can be used as a random number generator [11]-[12].Indeed the chaos’s properties functions ensure the properties of the chaotic sequence such as the sensitivity determined in the initial values and the control parameters.They are used for the different applications such as: pseudo-random sources, communications and securities.

These generators gave the pseudo-chaotics sequences and have a uniform distributed with long orbites. The proposed generator is done with structures that integrate a random technic and the copling technics between the perturbed chaotics maps in ordering the newpiece-wise linear chaotic map (NPWLCM), Bernoulli map.This technic improves randomness of the generated sequence but causes a down value speed performance. We established a chaotic pseudo number generator based on three weakly-coupled discrete chaotic maps perturbed in ordering the new (NPWLCM), Bernoulli map combined with permutation Bitwise (XOR) technic. Testing of algorithm was done based on the spreding and despreding average time, size of the key space, and the key sensitivity analysis. Beside that, we conducted a randomness analysis of the key stream which generated by these algorithm, and uniform distribution analysis of pixel values in the color images that has been spreding.Our algorithm provides very important tests stastics the peak of the signal-to-noise ratio (PSNR) and the Mean in the similarity structure (MSSIM).The best solution of the system of the finite precision of the digital chaotic.

The proposed name for the technic is the direct spread spectrum’s sequence based on the cryptography.The second is descuted according to the method of the synchronization of the chaotic systems for the information’s transmission applications.This synchronization approach is then used in a new pattern of the chaotic secure communication, which aims to increase the number and the amplitude of the transmitted messages and to improve the level of the security and robustness in the communication channel existed noise.

2. The Spread Spectrum Direct Sequence (DS-SS)

The spread spectrum’s direct sequence is one of the spread spectrum technics. Eventually a pseudo random sequence code symbols called (Chips) isused for the direct sequence code division multiple access (DS-CDMA) systems, but it lacks in the security due to the fact that there are a limited number of an available pseudo random sequence generator and they show the periodic correlation properties. A DS-ss system is the most common version usede today due to the simplicity implementation.In actual practice the base band informations digitized and Modulo-2 added to the code sequence and then modulated by Binary Phase-Shift Keying (BPSK)[7],[13]-[14].System as illustrated in Figure1.

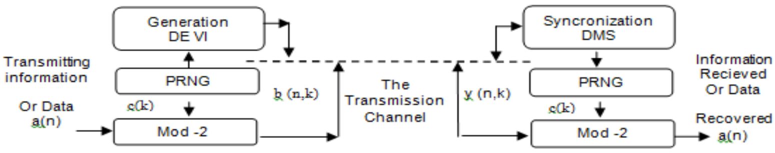

Figure1. Subclass model of the spread spectrum direct sequence system’s

2.1. The principle in the spread spectrum direct sequence system’s (DS-SS)

The symbols $a_0^{Nb}(n)$ with bit-rate (*br*). The every bit of $a_0^{Nb}(n)$ which will be assumed by a binary sequence code $c_0^{Kc}(k)$ in length K_c, which is defined by (*Mod 2*). The spread signal $b_0^l(n,k)$ is writen by equation (1):

$$b_0^l(n.T_b + k.T_c) = a_0^{Nb}(nT_b) \oplus c_0^{Kc}(k.T_c) \qquad k = 0,1,...,K_{c-1} \quad ; n = 0,1,...,N_{b-1} \qquad (1)$$

They are in these processes:

a. The pseudo-random sequence generator to spread the input signal.

b. The spreading is given the signal-spread for a Larger Band.
The despeeding processes are similar to the speeding processes but inreverse order. This dispread signal $a_0^{Nb}(n)$ is writen by equation (2) :

$$a_0^{N_b}(nT_b) = \begin{cases} 1 & \sum_{k=0}^{K_{C-1}} y_0^l(n.T_b + k.T_c) \oplus c_0^{Kc}(k.T_c) \geq \quad K_c / 2 \\ 0 & \sum_{k=0}^{K_{C-1}} y_0^l(n.T_b + k.T_c) \oplus c_0^{Kc}(k.T_c) < \quad K_c / 2 \end{cases} \qquad (2)$$

2.2. The Dynamic Modeling System (DMS)

The Dynamic Modeling System (DMS) has been used as a method of synchronization and generating sequence in this section .At the beginning the main idea of the based method dynamic system is given then a menu method for the initial condition perturbation for the chaotic is proposed and its performance is also shown in he Dynamic Modeling System (DMS).

3. The Chaotic Dynamic Secret Keys Generator

The finite precision’s effect of the of the chaotic dynamics aim to use two technics: the coupling and the perturbation chaotic orbit’s technic. The first technic effectively allows an expansion of the cycle length but without any control. The second technic allows not only a long cycle, but also imposing a minimum cycle length directly dependenty on the disturbance signal. This section is a new algorithm to generate random binary sequence (RBSG), using the- New Piece Wise Linear Chaotic Map- (NPWLCM) coupling with the logistic maps. Figure .2 shows the structure of the dynamic Secret Keys generator proposed [14].

3.1. The Perturbation Principles

This section is a new algorithm to generate random binary sequence (RBSG), using the - New Piece Wise Linear Chaotic Map- (NPWLCM) combined with the block perturbation and is introduced. The structure the Figure 2 is composed by a new algorithm to generate pseudo chaotic the - New Piece Wise Linear Chaotic Map- (NPWLCM) - a generator bloc about perturbation which role is to disrupt the orbit of the chaotic generator allowing it to access a new orbit and to establish synchronization based symbolic dynamics between transmitter and receiver and an effective solution to avoid redundancy and expand the cycles in the chaotic sequences.

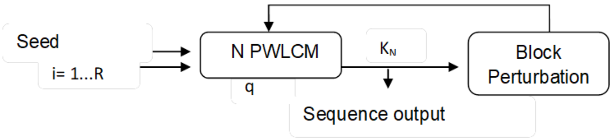

Figure 2. The first structure of the chaotic generator proposed (1st generator)

The generated matrix secret key use in spread spectrum steps as given:

Step 1: Initialization to set a logistic map.

$$x(n+1)=M\left[x(n)\right] \quad ,x_n \in\left[0,1\right] \quad n=0,1,2....,L \tag{3}$$

The input parameter for generating the matrix secret key is considered with the one seed input secret as a key *K₀*. So based on the value of *K₀* a set of secret keys are generated using a combination of the logistic map and - New Piece Wise Linear Chaotic Map- (NPWLCM) In this value of *K₀*, the initial condition $\mathrm{x}_0 \in\left[0...1\right],\ 0 <\lambda' \leq\ 4$.

Step 2: Generator chaotic the New pice-wise linear chaotic map (PWLCM), *x(n)* is used to :

$$x_0(n+1)=\sum_{i=1}^{R}2^{-i}x_i(n+i) \tag{4}$$

Step 3: Generate the key stream

$$k(n)=x_k(n)=M^k\left[x_0(n),q\right] \tag{5}$$

Step 4: The output sequence function the $\mathrm{M}_o^k=\left\{\mathrm{M}_o^1\ \mathrm{M}_o^2\ldots\ \mathrm{M}_o^L\right\}$ in length (L) are automatically generated and will be transformed into the binary sequences {0,1}.

3.2. Generate of the Binary Sequence

The proposed method consists of the following steps: First, the sequence $\{X_n\}$ is generated by the chaotic map method which must be amplified by a scale factor (*n')* and to integer part subsequence $\lfloor . \rfloor$method, we can use floor (f(x)) in matlab software [5, 6].The resulting sequence B_n has a finite level equal to (*m')* defined over (mod *m'*) and is transformed to the binary sequence as it is shown in Figure 3.

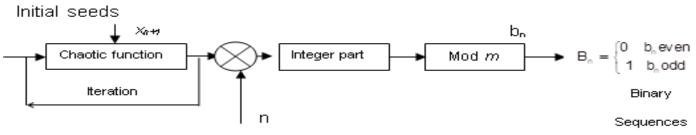

Figure 3. Subclass generation of the binary sequence.

The equation of the scheme is:

$$\mathrm{b}_n=\left\lfloor \mathrm{x}_{n+1}\,.\mathrm{n}' \right\rfloor.\mathrm{mod\ m'} \qquad \mathrm{m'}\ \leq\ \mathrm{n'} \tag{6}$$

We generate another $\left\{\mathrm{x}_n\right\}$ pseudo-random sequence B_n of natural numbers *n* bit sequence given by the binary chaotic sequence encoding (LSB: Least Signification Bit).

$$B_n=\begin{cases}0 & b_n even\\ 1 & b_n odd\end{cases} \qquad \text{And } n\in\left[0 \quad N\right], N\text{: Iterations} \tag{7}$$

4. The Chaotic Functions

The chaos has been successfully implemented in the analog communication systems following the work of Pecora and Carroll 1990 [8].The digital implementation gave more problems because of the finite precision of the digital representation. When the chaotic systems are represented with a finite precision, they become inevitably cyclic functions and their distribution and correlation deteriorate.

4.1. The Finite Precision of the Digital Chaotic:

The methods have been proposed to address the problems of the finite representation [8]:

a. Cascading of several chaotic systems.
b. Use of higher accuracy: brings significant improvements but the high cost of implementation.
c. Disruption of the chaotic orbit.

4.2. The Chaotic Sequence Generator Bits

Various nonlinear of the dynamical systems are used to generate the chaotic sequence.All the chaotic systems must have following properties [15]: Sensitivity to the initial conditions, the topological mixing , the topological Ergodicity and the density periodic orbits.

The discrete-time of the dynamical systems is the particular type of the non-linear dynamical systems generally described as an iterative the map $M : R^k \to R^k$ by the equation (8):

$$x_{n+1} = M\left(x_n\right); \qquad n = 0,1,2\ldots L \tag{8}$$

Where *n* is the discrete-time, $x_n \in R^k$ x is the time's state system at *n*, while x_{n+1} shows the next state and *k* is the dimension of the state-space.

4.3. The Used Chaotic Map

The applications of the logistic map all of them are about the image incryption [16].The properties of a logistic map can be quantitatively analyzed by methods of the statistical probability and the Lyponov exponent. Practically an analysis of the probability density of Logistic map sequences is not uniform [17]. Prac Piece Wise Linear Chaotic Map- (PWLCM) is called also a tent map and Piece Wise Linear Chaotic Map- (PWLCM) can produce the pseudo random sequences with the good statistical properties even under the condition of finite word length computing [18]. Piece Wise Linear Chaotic Map- (PWLCM) system has an uniform invariant distribution and good ergodicity so it can provide excellent random sequence, which is suitable for our cryptosystem, then to produce the pseudorandom sequences with good stastical prooprites [19]. The characteristics of Piece Wise Linear Chaotic Map- (PWLCM) are suitable for the design system of encryption. It is reported that some findings on the new series of dynamical indicators that can quantitatively reflected in the degradation effects on a digital the Piece Wise Linear Chaotic Map- (PWLCM) realized with a fixed-point finite precision.The Bernouli shift is an algorithm that gives a complex chaotic behaviour .It is characterized by the exponential growth and disorder [20]. Table 1 shows the formulat of the Piece Wise Linear Chaotic Map- (PWLCM), New Piece Wise Linear Chaotic Map- (NPWLCM) and Bernoulli's Shift Map.

Table 1. The Formulat of the Logistics Map, Piece Wise Linear Chaotic Map-(PWLCM), Piece Wise Linear Chaotic Map-(NPWLCM) and Bernoulli's Shift Map

Chaotic recurrences	Mathematical formulas	Parameters Critical
Logistics map. [21]	$x_{n+1} = M_{\lambda'}(x_n) = \lambda.' x_n (1 - x_n)$	$0 \le x_n \le 1, \quad \lambda' \le 4$
Tent map	$x_{n+1} = M_p\left(x_n\right) = \begin{cases} \frac{x_n}{p} & 0 \le x_n < p \\ \frac{1-x_n}{1-p} & p \le x_n < 1 \end{cases}$	$0 \le x_n \le 1, p \in \left(0, 0\,.\,5\right)$
Piece Wise Linear Chaotic Map (PWLCM). [22]	$x_{n+1} = M_q\left(x_n\right) = \begin{cases} \frac{x_n}{q} & 0 \le x_n < q \\ \frac{x_n - q}{0.5 - q} & q \le x_n < 1/2 \\ M\left(1 - x_n, q\right) & 1/2 \le x_n < 1 \end{cases}$	$0 \le x_n \le 1, \quad q \in \left(0, 0\,.\,5\right)$
New Piece Wise Linear Chaotic Map (NPWLCM)	$\mathrm{x}_{n+1} = \lambda x_n - \lfloor \lambda x_n \rfloor$	$\lambda = \left(1/q_0\right), q_0 \in (0 \quad 0.5)$

Table 1. The Formulat of the Logistics Map, Piece Wise Linear Chaotic Map-(PWLCM), Piece Wise Linear Chaotic Map-(NPWLCM) and Bernoulli's Shift Map

Chaotic recurrences	Mathematical formulas	Parameters Critical
Bernoulli's shift map	$x_{n+1} = M\left(x_n\right) = \mathrm{mod}(\lambda.x_n,1) = \begin{cases} \lambda x_n & \le x_n \le 1/2 \\ \lambda x_n - 1 & 1/2 \le x_n \le 1 \end{cases}$	$x_n \in \left[0 \quad 1\right]$, $\lambda \ge 1$

A-New Piece Wise Linear Chaotic Map- (NPWLCM) is 1D chaotic map. The basic Equation of the above map can be described as:

$$M\left(x\right) = frac\left(\lambda x\right) \tag{9}$$

Or *frac*: fractional part or $\left\{x\right\}$,λ>1 :*frac(x)* for $x \in R$ is defined a:

$$\left\{x\right\} = frac\left(x\right) = x - \lfloor x \rfloor, x \in R \tag{10}$$

Where $\lfloor x \rfloor$ is the floor function (i.e. the integer nearest to $-\infty$).The new piecewise linear chaotic map (NPWLCM maps) is given by:

$$x_{n+1} = \lambda.x_n - \lfloor \lambda.x_n \rfloor \quad , \quad and \quad \lambda = 1/q_o, (q_{\hat{o}} \in (0 \quad 0.5)) \tag{11}$$

Figure 4 shows cobweb diagram (left) and time domain waveform (right) for the (NPWLCM).

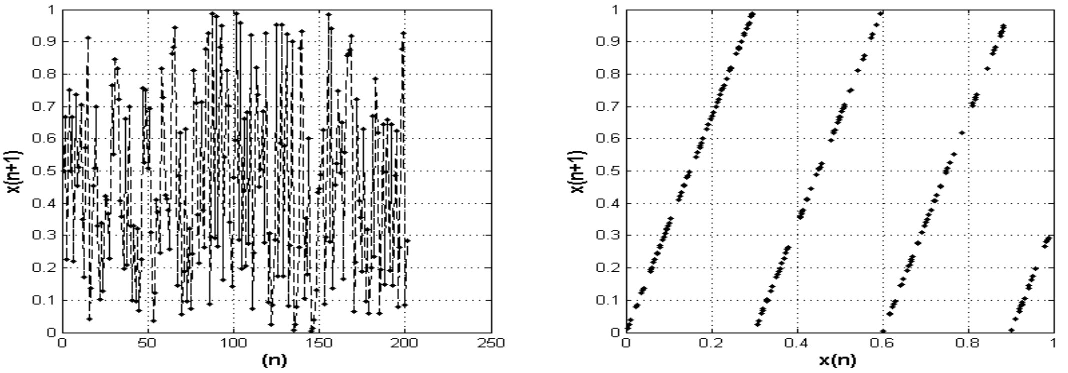

Figure 4. Diagram's Cobweb (Left) and time domain waveform (Right) for The (NPWLCM)

Figure 5 showssample results (NPWLCM) sensitivity for two initial conditions a 200 iterations.The sensitivity of the initial value of chaotic specifically, for *f (x)* application begins with two initial values that are close, say (*x*) and (*y*) such that (a large amount), and generate the orbits of the first two points is given by:

$$\varepsilon\left(n\right) = \left| f_1^n\left(x\right) - f_2^n\left(y\right) \right| \quad ; n = 0,1,2\ldots L \tag{12}$$

In this study the generation of the chaotic sequences is studied by analyzing the bifurcation diagram and in analyzing the Lyapunov Exponent (LE) also the Probability Density.

a. The Lyapunov Exponent: The Lyapunov exponent (λ_L) [23],of a 1D map $x_{n+1}=f(x_n)$ is:

$$\lambda_L(x) = \lim_{n\to\infty} \frac{1}{n} \sum_{i=1}^{n} \ln\left(\frac{df(x_{i-1})}{dx_{i-1}}\right) \in R \qquad (13)$$

As shown in Figure 6, Figure 7 and Figure 8 the sensitivity of the chaotic maps towards its initial value x_0 also indicates that: Depending on the value of (*λ)*, the dynamic in the system can change attractively giving periodicity or chaos. A diagram of bifurcation is a visual summary in the succession of the doubling time shown: as (*λ)* increases.

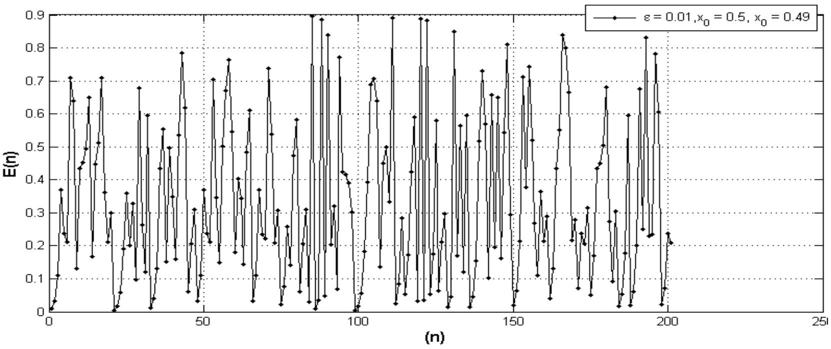

Figure 5. Sample results (NPWLCM) sensitivity for two initial conditions a 200 iterations

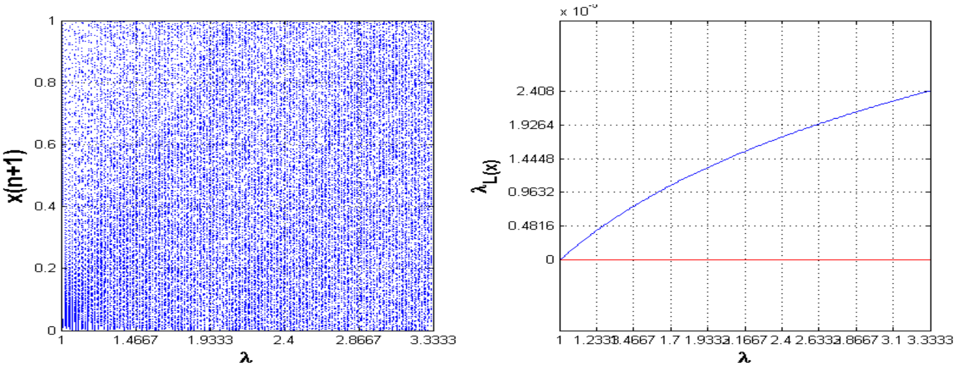

Figure 6. (Left) Diagram’s Bifurcation for 1≤λ≤3.33, (Right) Lyapunov Exponent for 1≤λ≤3.33 for the New PWCLM

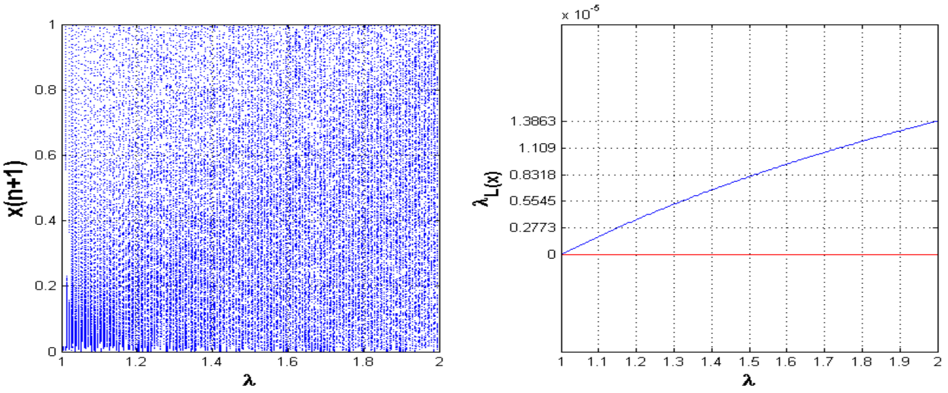

Figure 7. (*Left*) Diagram’s Bifurcation for 1≤λ≤2 ,*(*Right*)* Lyapunov Exponent 1≤λ≤2 for Bernoulli map

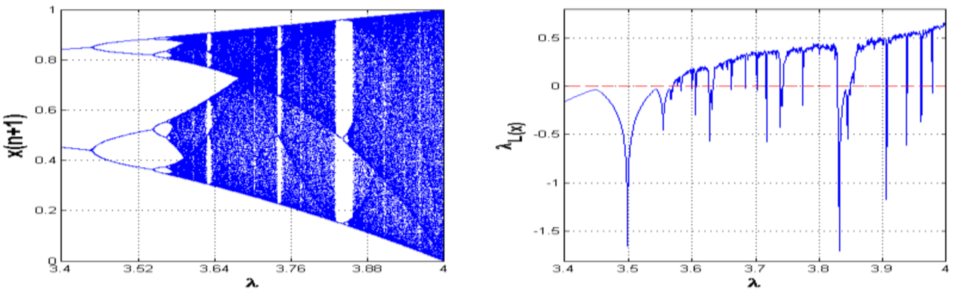

Figure 8. (Left) Diagram’s Bifurcation for 3.4 ≤λ’≤4 ,(Right) Lyapunov Exponent for 3.4 ≤λ’≤4 for logistic map

b. The Density Probability:The probability density permits a determination of the spreading function F_X [24]:

$$P(X\grave{o}[a,b]) = F_x\left(b\right) - F_x\left(a\right) = \int_a^b f\left(x\right)dx \qquad (14)$$

The histograms of Figure 9 and Figure 10 denote that the distribution of the Bernoulli map and New PWCLM density function have the better uniform distribution and have the better qualitative & quantitative properties.The Figure 11 has a bad distributed probability function which is required for random number generation.

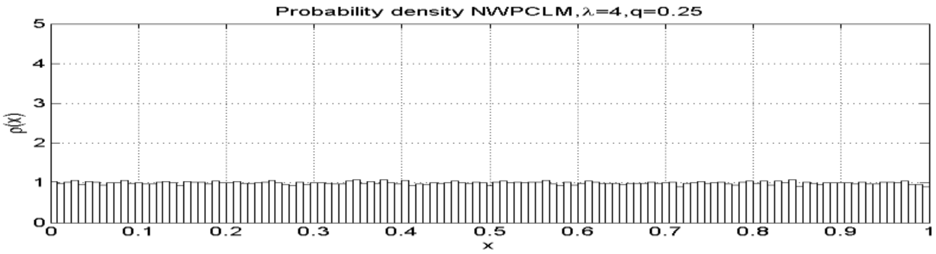

Figure 9. Simulation of the probability density for the New PWCLM

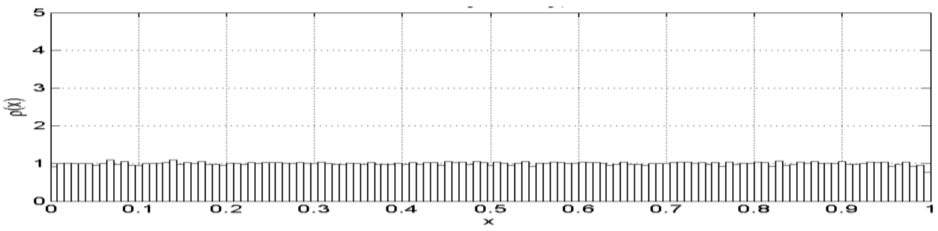

Figure10. Simulation of the probability density for the Bernoulli map

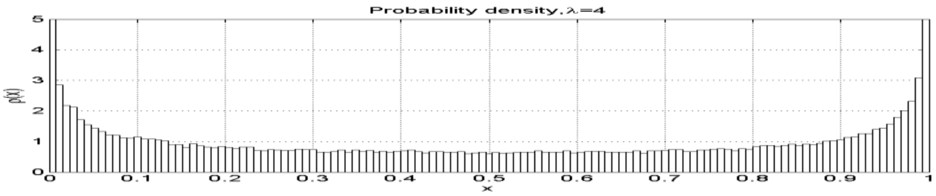

Figure 11.Simulation of the probability density for the logistic map

4.4. A New Pseudo's Random Bit generator Design

The structure of the proposed generator is shown in the Figure 12. The output are third of key K_1,K_2,K_3.The first one the input data for generating matrix secret key K_1 is done with the one seed input secret key K_0. Then based on the value of K_0 which is a set of secret keys is generated by using a combination of the logistic and the -New Piece Wise Linear Chaotic Map-(NPWLCM) methods. The second generating matrix secret key K_2 is done with the one seed input secret key K_0. Then based on the value of K_0 a set of secret keys is generated by using a combination of the logistic and the first Bernoulli map (Bernoulli map (1)) chaotic map methods. The third generating matrix secret key K_3 is done with the one seed input secret key K_0. After that based on the value of K_0 a set of secret keys which is generated by using a combination of logistic and second Bernoulli map (Bernoulli map (2)) methods of the chaotic map.

Finally, the output of the chaotic sequence is given in ascending order and forms combined with the Following standard based with block non-linear Boolean functions with permutation *Bitwise XOR* block.

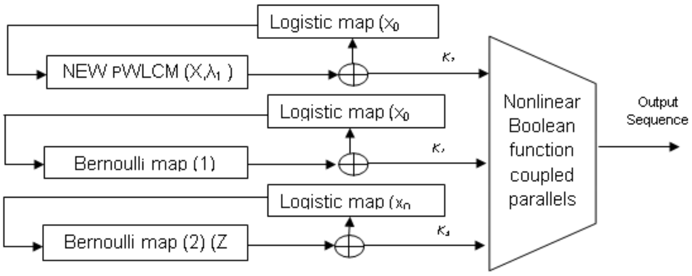

Figure 12. The structure of the chaotic proposed generator (3rd generator)

Generating permutation key sequence is described in the step 1 to step 3:

Setup 1: Input : (seed x_0, λ_0) ,(seed x_1 ,λ_1),(seed x_2, , λ_2),(seed x_3 , λ_3).
X→f^i(seed x_1,λ_1) , Y→f^i(seed x_2, , λ_2) , Z→f^i(seed x_3 , λ_3).

Setup 2:Permutation *bitwise xor*.The initial state is initialized with input with tow chaotic perturbed .We apply "*X*" stapes, where "*X*" is the bit size of the input of the input parameter "*X*"For each step *i*: Extract bit "*i*" form "*X*", If *X[i]=0*, apply the bitwise permeation With*Y*, $S_1 = X \oplus Y$; Els if WithZ, $S_2 = X \oplus Z$.

Setup 3: Output sequence is: $S = C\left(X,Y,Z\right) = S_1 \oplus S_2$.

The structure of our pseudo random number generator has been designed to be used as to the disturbance technic .Notice that the output of the proposed pseudo-random number generator depends on several chaotic recurrences.Also all the chaotic sequences intervening in the generation of the encoding sequences are transformed into the dynamic symbolic sequences which provide a partial description of the corresponding chaotic orbites.The dynamic symbolic sequences are difficult to locate their values.So that the observation of the used encrypting sequences does not provide any useful information.

5. The Spread Spectrum Color Image Resarch Method

An image spreading experiment is designed by using the proposed the algorithms system, where the generated chaotic sequence is employed to spread the image. Suppose that the size of RGB image is (M × N),or (M, N): The numbers of rows and column of pixels.

The spreading processes as shown in Figure13 are described in the step 1 to step 5:

Step 1: Firstly, we choose M=N=256.The color images are represented by three distincts color's of [25]: The red R; the green G and the blue B colors.

Step 2: The spreading of each color apart a color mixing step is used to mix data from different colors and to provide further confusion aspect in the resulting speeded image.

Step 3: This resulting data is show into the near 256 bit blocks(8 byte per block).Every pixel is represented in a given color by1 byte so we collect them one by one from one color to another using the following mechanism. The first byte is the blue and is spread by multiplying it with a long sequence of PN (Pseudo Noise) code, each information bit contains a number ofchips (First spread of The 8 chips) to obtain the spreader image S_R and first byte is the green which is spread by multiplying it with a long sequence of PN (Pseudo Noise) code. Each information of bit contains anumber ofchips (Second spread of The 8 chips S_G) that obtain the spreader image S_G and the first bytes is thered spread by multiplying it with a long sequence of PN (Pseudo Noise) code .Each information of bit contains number of chips (Third spread of The 8 chips) and obtain the spreader image S_B and then we'll take the second blue byte spread by multiplying it with first spread of The 8 chips S_R .The green byte spreads by multiplying it with Second spread of The 8 chips and red byte spread by multiplying it with Third spread of The 8 chips.

Step 4: The signal spreding additive with the channel of the Additive White Gaussian Noise (AWGN).

Step 5: The synchronously received sgnal (Ciperd-image). The despeeding processes are similar to the speeding processes but in reverse order.

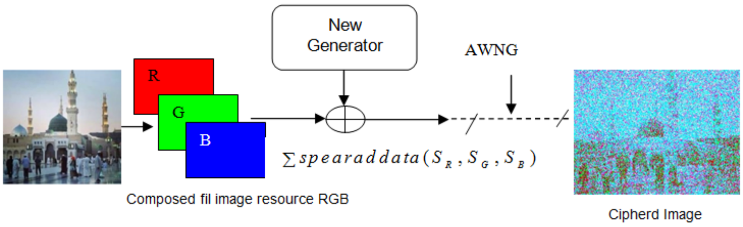
New Generator
AWNG
R
G
B
∑spearaddata(S_R , S_G , S_B)
Composed fil image resource RGB
Cipherd Image

Figure 13. Complete steps image spreading technic

5.1. Evaluation's Criteria and Basic Experiment Simulation

The signal-to-noise ratio peak (PSNR) and the structural similarity (SSIM) are the evaluation of the qualities of the spreading image.Till here we have to know how to evaluate the image quality of the Pseudo Noise (PN) code. Let $H(i_1,j_1)$ or $H(i_1=1,2,\dots,N\ ;\ j_1=1,2,\dots,M)$ be the ideal image, $S(i_1,j_1)$ or $S(i_1=1,2,\dots,N\ ;\ j_1=1,2,\dots,M)$ be image in the Pseudo noise .The total difference is can be written as:

$$D=\sum_{i_1=1}^{N}\sum_{j_1=1}^{M}H(i_1,j_1)-S(i_1,j_1) \qquad (15)$$

The formula for the Mean Square Error (MSE) [26] is:

$$MSE(H,S)=\frac{1}{M.N}\sum_{i_1=1}^{N}\sum_{j_1=1}^{M}\left(H\left(i_1,j_1\right)-S\left(i_1,j_1\right)\right)^2 \qquad (16)$$

The formula for the signal-to-noise ratio peak (PSNR) [27], [28] is:

$$PSNR(H,S)=10\log_{10}\left(\frac{\left(L^{th}\right)^2}{MSE}\right);and \quad L^{th}:Length=2^8-1\Big|_{pixel\ iof\ mage} \qquad (17)$$

The Structural Similarity Index (SSIM): The similarity compared the brightness, the contrast and the structure between every pair of vectors when the structural similarity (SSIM) between two Iimages (H) and (S) is given by the Equation (18) [27]-[28]:

$$SSIM\left(H,S\right)=I_1\left(H,S\right).I_2\left(H,S\right).I_3(H,S) \qquad (18)$$

The formula for the Mean structural similarity (MSSIM) is expressed as:

$$\mathrm{MSSIM}(H,S) = \frac{1}{M}\sum_{j=1}^{M}\mathrm{SSIM}(H_j,S_j) \tag{19}$$

5.2. The Experimental Results on Color Noisy Image Based on RGB Color Model

The applied proposed algorithms were : 1st generator (New Piece-Wise Linear Chaotic Map (NPWLCM) combined with the block perturbation the logistic map). 2nd generator(Bernoulli map combined with the block perturbation the logistic map). 3rd generator (Describded in section 4.4) .In the test color image (JPEG)of size (256*256 x 3) encoded into 8 bpp of colors.The analysis shows the possibility of reducing the speeding chips so that the image quality remains acceptable. The result images are shown in Figure 14.The below results exist in MATLAB 7.2.

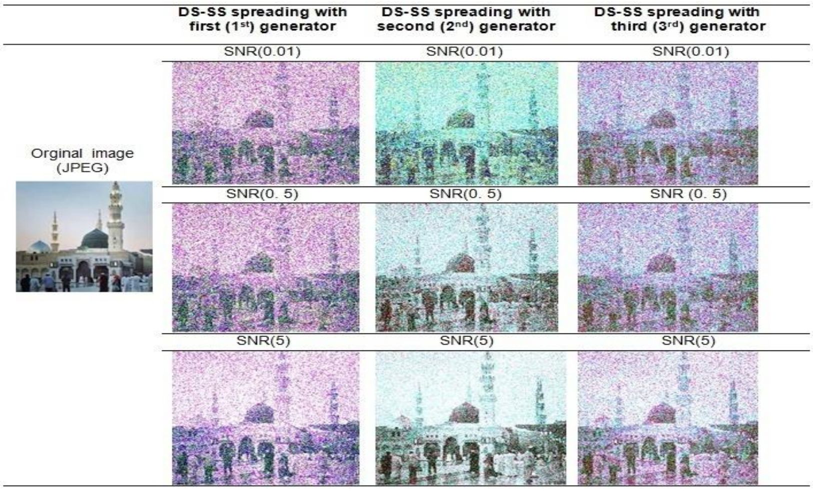
DS-SS spreading with first (1st) generator
DS-SS spreading with second (2nd) generator
DS-SS spreading with third (3rd) generator
SNR(0.01)
SNR(0.01)
SNR(0.01)
Orginal image (JPEG)
SNR(0. 5)
SNR(0. 5)
SNR (0. 5)
SNR(5)
SNR(5)
SNR(5)

Figure 14.Original image andthe speeding image with different the signal-to-noise ratio (SNR). Three qualities and similarities measures (1st generator, 2nd generator and 3rd generator)

The Figure 15, Figure 16 and Figure 17 show the performance compared with execution: MSE, PSNR and MSSIM of the orginal and spreading image for the thres generated typs. These results are obtained with a noise SNR=0.01 to 25 bite-rates.

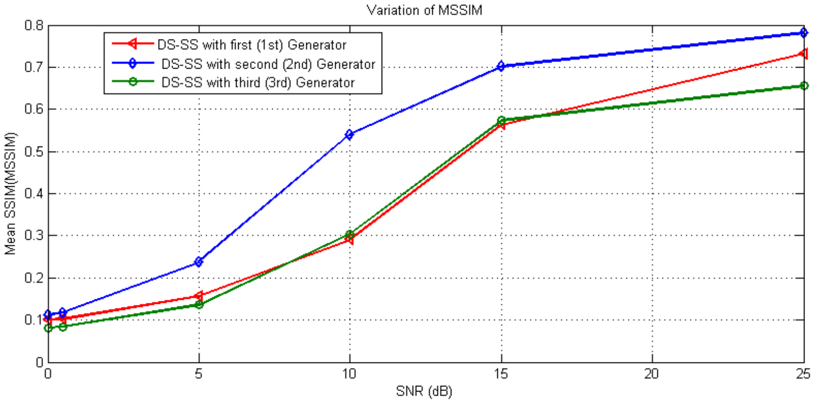

Figure 15. Mean SSIM to SNR and different spreading sequence (DS-SS)

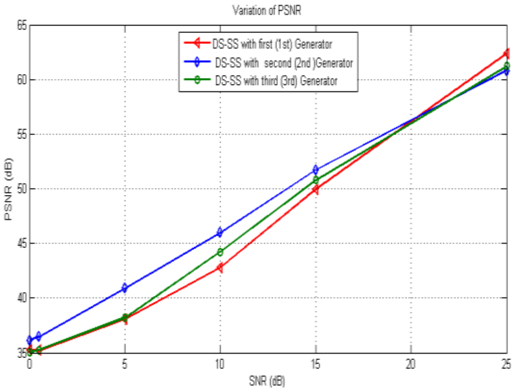

Figure 16. PSNR to SNR and different spreading sequence (DS-SS)

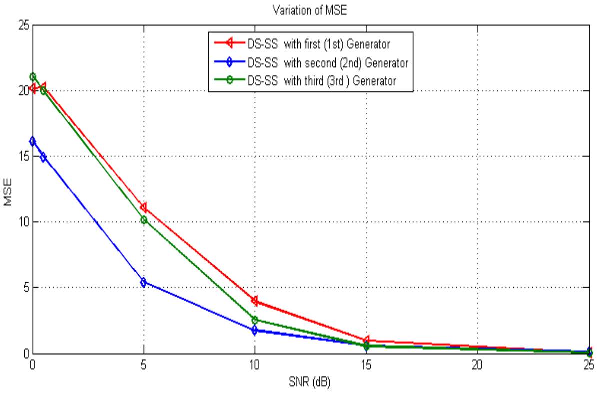

Figure 17. MSE to SNR and different spreading sequence (DS-SS)

An exponential decrease in Mean Square Error (MSE) is observed in Figure17 as the power increases in the first step. The*15 db* refers to a decrease in power; MSE is approaching oppositly nearly zero with 1st generator, 2nd generator and 3rdgenerator.In the absence of noise the two images are identical, and thuse the MSE is Zero.In this case the PSNR is infinite(See Figure 16).The results obtained are also ploted in Figure 16 and 17 it is observed from the resulted images and data, the 3rd generator is better than the other generators with the increase of the noise intensity.However the SSIM is better for the orginal one at some SNR .Then we are showing the comparaison forthe 1st generator ,the 2nd generator and the 3rd generator algorithms .The experiments are performed with the 3rd generator.The image spreading quality with the help PSNR is very simple as compared to SSIM.The efficiency of the proposed algorithm about the speeded image quality of the low bit-rate. It is shown that the difference in (PSNR, MSSIM) is greater and lower for the first algorithm, the second and the third algoritm.Hence the chaotic performance and the key size of the third (3rd) generator .These properties are suitable for different applications such as security.

6. Conclusion

Finally the obtained results are satisfactory in terms of the spreading quality's image. The digital communication system pseudo generator chaos is based in the (DS-SS) and is very important. They have different strong point and are equally important. They are based on a unique combination of the coupled technics and NPWLCM sequence of the perturbed logistic map which has been used the proposed system and must be protected from droppers in the case of the use of the different methods. All these features make the system robust and feasible to provide the required security in the synchronize communication system based for the digital sense of DS-SS system.

References

[1] Zhang Y .Plaintext Related Image Encryption Scheme Using Chaotic Map. *TELKOMNIKA (Telecommunication Computing Electronics and Control)*. 2014; 12 (1): 635-643.

[2] Adedeji Kazeem B, Ponnle Akinlolu A. Improved Image Encryption for Application over Wireless Communication Networks using Hybrid Cryptography Technique. *Indonesian Journal of Electrical Engineering and Informatics (IJEEI)*. 2016; 4(4):307-318.

[3] Michael GL, Michael H, Michael L. Pseudo Randomness and Cryptographic Applications.Princeton University Press. 1996: 134 Pages.

[4] Don T. Principles of Spread-Spectrum Communication Systems.SpringerScience+ Business Media, Boston. 2005.

[5] Stephen JC. Essentials of MATLAB® Programming.Second Edition. Australia. 2009.

[6] Math Works.Symbolic Math Toolbox™ 5 MuPAD® Tutorial. U.S. 2008.

[7] Krim M, Ali Pacha A, Hadj Said N. New Binary Code Combined with New Chaotic Map and Gold Code to Ameliorate the Quality of the Transmission. *Indonesian Journal of Electrical Engineering and Computer Science (IJEECS)* .2017; 5(1): 166-180.

[8] Noura H. Design and Simulation of Generators Crypto-systems and Functions hash bases performing chaos. Thesis. France: University Of Nantes (STIM).2012.

[9] Amit T, Abhishek Z, Rohit H. *Pseudo Chaotic Sequence Generator based DS-SS Communication System using FPGA*. International Conference on Industrial Automation and Computing (ICIAC). 2014; 13-18.

[10] Dąbal P. Pipelined pseudo-random number generator with the efficient post-processing method*.International Journal of Microelectronics and Computer Science*. 2015; 6(2): 43-48.

[11] MTS, Nurpeti E, Widya D. Performance of Chaos-Based Encryption Algorithm for Digital Image. *TELKOMNIKA (Telecommunication Computing Electronics and Control)*. 2014; 12(3): 675-682.

[12] Abdmouleh MK, Khalfallah A, Bouhlel MS. *Dynamic Chaotic Look-Up Table for MRI Medical Image Encryption*. Proceedings of the 2013 International Conference on Systems, Control, Signal Processing and Informatics. Research Unit: Sciences and Technologies of Image and Telecommunications Higher Institute of Biotechnology Sfax, Tunisia. 2013; 241-146.

[13] Tasneem SM, Salsabil A, Iqbalur RR. *Transmitter Implementation Using DS-CDMA Technique in FPGA Using Verilog HDL*. ICEECE'2011 International Conference on Electronically Electronics and Civil Engineering. 2011; 204-207.

[14] Lahieb MJ, Ghazali S. A Novel Dynamic Secret Key Generation for an Efficient Image Encryption Algorithm. *Modern Applied Science*. 2015; 9(13): 85-97.

[15] Rastogi S, Thakur S .Security Analysis of Multimedia Data Encryption Technique Using Piecewise Linear Chaotic Maps. *IJRITCC International Journal on Recent and Innovation Trends in Computing and Communication.*2013; 1(5): 458 -461.

[16] Deng H, Zhu Q, Song x, Tao J. Chaos-Based Image Encryption Algorithm Using Decomposition.*TELKOMNIKA (Telecommunication Computing Electronics and Control).* 2014; 12(1): 575- 583.

[17] Qiang G, Hua Y, Hongye Y. The Research of Chaos-based Mary Spreading Sequences. *TELKOMNIKA (Telecommunication Computing Electronics and Control).* 2012; 10(8): 2151-2158.

[18] Shujun L, Qi L, Wenmin L, Xuanqin M, Yuanlong C. *Statistical Properties of Digital Piecewise Linear Chaotic Maps and their Roles in Cryptography and Pseudo-Random Coding*. Proceedings of the 8th IMA International Conference ,Springer-Verlag . 2001; 2260: 205-221.

[19] Zhang Y, Xia Jilali, Cai Peng, Chen Bin.Plaintext Two-level Secret Key Image Encryption Scheme.*TELKOMNIKA (Telecommunication Computing Electronics and Control).* 2012; 10(6): 1254-1262.

[20] Gharpure M. chaos theory .I.S.Information technology Group C2.(Roll Numbers:54-60).A report Submitted in Partial Fulfillment of the Requirement of Communication and Presentation Techniques Syllabus:Report writing. 2012.

[21] Robert MM. Simple Mathematical Models with very Complicated Dynamics. Nature.1976;1-9.

[22] Zhou H, Ling XT. Problems with the Chaotic Inverse System Encryption Approach. *IEEE Trans Circuits Systems I: Fundamental Theory and Applications*. 1997; 44(3): 268-271.

[23] Stephen L. Dynamical systems with applications using matlab. New York: Springer Science –Busines Media, LLC. 2004; 48-54.

[24] Pallavisini.A. A Radio Frequncy Interference System for Chaos Cryptography applied to Radio Transmissions .Doctor Thesis. France. Engineering sciences physics. University Doctor Rank.2007.

[25] Math Works. Image Processing Toolbox™ User's Guide . U.S. 2014;1-664.

[26] Tu L, Jia L, Zhang C, Guo S. A New Image Encryption Algorithm Based on Two dimensional Coupled Chaotic Map. *TELKOMNIKA (Telecommunication Computing Electronics and Control)*. 2014; 12(12):8229-8237.

[27] Qiaomei Ma, Lijun Wu, Jianhong Du, Gouxi Chen, Qiuxiang Yang. An Adaptive All-odd Transformation Watermark Scheme. *TELKOMNIKA (Telecommunication Computing Electronics and Control).* 2014; 12(5): 4107-4114.

[28] Gengaje PS. Contemporary Full Reference Image Quality Assessment Metrics. *IJIRCCE International Journal of Innovative Research in Computer and Communication Engineering*. 2016; 4(3): 4074-4082.