Cumhuriyet Üniversitesi Fen Fakültesi
Fen Bilimleri Dergisi (CFD), Cilt:36, No: 3 Özel Sayı (2015)
ISSN: 1300-1949

Cumhuriyet University Faculty of Science
Science Journal (CSJ), Vol. 36, No: 3 Special Issue (2015)
ISSN: 1300-1949

Self-adaptive image encryption using Choquet fuzzy integral and chaotic system

Asie MOHAMMADİ[1,*], Ali ZAGHİAN[1]

[1]*Department of Mathematics, MalekAshtar University*

Received: 01.02.2015; Accepted: 05.05.2015

Abstract. In this paper, a self-adaptive encryption algorithm using by chaotic systems and Choquet fuzzy integral is presented. This algorithm has been designed considering classic of permutation-diffusion, combination of two one-dimension (1D) chaotic maps and Choquet fuzzy integral. To avoid the definite plaintext attack or chosen plaintext attack, keys which are produced for two stages (permutation and diffusion stages) are associated plain image. Thus, different keys are produced for different images. Key which is produced in permutation stage, corresponded with chaotic map and key which is made in diffusion stage based on Choquet fuzzy integral.

Keywords: image encryption, self-adaptive technique, chaotic system, Choquet fuzzy integral

1. INTRODUCTION

Nowadays, with development of communicative technology, it has been became widespread the use of digital images more than before. The transmitted images may be involve application such as military, commercial usage or even medical usages. Therefore, to maintaining their security and avoiding inadmissible accesses to these images, its encryption before sending is necessary. Due to images properties such as bulky data capacity, high redundancy, and high correlation between image pixels, traditional techniques such as AES, Des, RSA and etc, are not suitable for real-time encryption of images.

Considering the images intrinsic properties, the numerous algorithms for their encryption based on different techniques such as SCAN [1], circular random grids [2], elliptic curve ElGamal [3], gray code [4] wave transmission [5], chaotic [6-12] and Choquet fuzzy integral [13-14] has been presented. Among proposed techniques, one of the very effective and best encryption techniques is chaotic systems due to characteristics of chaotic system itself such as parameter setting, random behavior, ergodic state, and sensitivity to initial condition. Choquet fuzzy integral involves behavior similar to chaotic systems but it is limited used in image encryption and is mostly applied in image processing.

Security is first and basic principle in an image encryption algorithm. To reach high security, the encryption algorithm ought to be able to create small change in one plain image pixel or any negligible change in initial condition, it is concluded the complete distinguishable cipher image.

* Corresponding author. *Email address*: *asiemohammadi13@gmail.com*

Special Issue: The Second National Conference on Applied Research in Science and Technology

http://dergi.cumhuriyet.edu.tr/cumuscij

It can be divided the security faults sustained cryptography systems into two classes: small key space and little sensitivity to plain image.

Now, we are briefly presenting security fault on some of encryption algorithms. In [11], Zhu is suggested an encryption model with only two diffusion circles which chaotic sequence is made using one 4D hyper chaotic system with four initial conditions such as x_0, y_0, z_0, w_0. The security of this algorithm was investing by Li et.al [12] and suggested a cryptanalysis method known-plaintext. They recognized that it can be found the used secret keys based on two pairs of known plain-image and available cipher images [12]. In [13], Liu et.al are used the improved sequence based on Choquet fuzzy integral for color image encryption. In this method, the fuzzy integral inputs are obtained by a 128 bit's key, which generated using PWLCM map, and four values obtained Lorentz hyperchaotic system. Yang Zhang [14] could be obtained secret key by presentation of a chosen plaintext attack.

The pictorial encryption algorithm which is presented in this paper involves permutation-diffusion classic structure. Its means that encryption process has been formed two permutation and diffusion stages. One separate key is generated for each stage, which each key is depended on plain image; thus, the suggested algorithm is resistant against known plaintext attack or chosen plaintext attack. Key which is generated in permutation stage, it's based on LSS improved chaotic sequence [10], which is composed of two 1D chaotic maps Sine and Logistic. Key which is generated in diffusion stage, it's based on Choquet fuzzy integral improved sequence.

The continuation of this paper has classified as follow. In section 2, it's explained the suggested self-adaptive image encryption algorithm. In section 3, it's presented the suggested algorithms' numerical tests. Section 4 is related to algorithm implementation and finally the results are explained in section 5.

2. SELF-ADAPTIVE IMAGE ENCRYPTION ALGORITHM DESIGN

2.1. Chaotic system

The chaotic systems generally can be divided into two categories: one-dimension (1D) and multi-dimension (MD). The MD chaotic maps have increasing applications in image security due to having complicated structure and several parameters. But the existence of several parameter, are caused to increase hardware/software implementation problems and calculation complication. On other hand, 1D maps have simple structure and simple implementation method. They also have three problems including: (1) the limited or/and discontinuous range of chaotic behaviors; (2) the vulnerability to low- computation-cost analysis using iteration and correlation functions; and (3) the non-uniform data distribution of output chaotic sequences.

Considering above discussion, we are used chaotic map which suggested by Zhou in [10].This is composed of two chaotic maps including Sine and Logistic that are denoted as LSS1. This map general form is as follows:

$$X_{n+1}=\left(L(r,X_n)-S\left((4-r),X_n\right)\right) \bmod 1=\left(rX_n(1-X_n)+(4-r)\sin\frac{(\pi X_n)}{4}\right) \bmod 1 \quad \text{Where } r\in(0,4] \quad (1)$$

Figures. 1(a) and 1(b) show its bifurcation diagram and Lyapunov exponent results. The chaotic behaviors of the LSS exist in the whole range of parameter control and its chaotic sequences have a uniform-distribution with in [0,1].

2.2. Model presented for permutation

Permutation is operation which can be disrupted or high correlation among pixels by change of pixels position in the plain image. The different techniques for permutation function have been presented [6-8]. But, the showed models is only based on key, thus, as it has been showed in Figure 2, due to non-depended key to plain image, despite change of an pixel value, the permutation pattern is not change and pixel which changed its value is replaced prior pixel. We are presented model for permutation that resulted from Huang and et.al suggested technique in [9]. Technique which has been presented in [9], it is based on 2D Logistic map. But, as stated in section 1.2, MD chaotic map have hard implementation and many calculation complication. Thus, considering suitable condition for LSS map [10] which stated in section 1.2, we are using this map for production of permutation key.

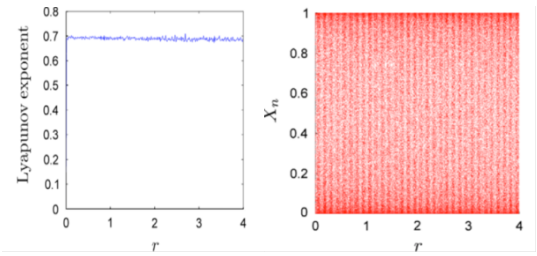

Figure 1. (a) The Lyapunov Exponent; (b) The Bifurcation diagrams

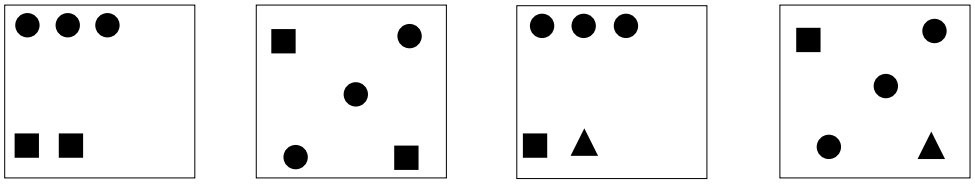

Figure 2. (a) plain image; (b) permutation image (a); (c) the image (a) with a bit change; (d) permutation image (c)

[1] . Logistic-Sine system

In permutation operation, before using permutation key, first we shift each row with scale row number from right to left and each column with scale of column number from down to up, namely it is shifted row number (i) with scale i from right to left and column (j) with scale j from down to up. To creating improved key sequence dependence to plain image, control parameter α which is equal to sum of plain image pixels value to sum of pixels value square, is obtained as follows:

$$\alpha = \frac{\sum_{i,j} A(i,j)}{\sum_{i,j} A(i,j)^2} \tag{2}$$

We are using α to update the chaotic map initial condition. This update is performed as follow:

$$x_0 = x_0 + \alpha \tag{3}$$

If x_0 value get out of defined range, we are using subtraction operation. Otherwise, we're using sum operation. Not only Eq. (3) is utilized for chaotic map initial condition but also for each output of system, namely system output at n^{th} is utilized as follow:

$$x_n = x_n + \alpha.$$

Considering initial condition x_0 and then its update by Eq. (2), we're obtained iteration set $\{x_0, x_1, x_2, x_3, \ldots\}$ with respect to (1). With ignoring above set first component S and chaotic m+n values, we're obtained an chaotic set $p = \{p_1, p_2, p_3, \ldots, p_{m+n}\}$. Then for p-set elements transformation with suitable values for plain image, we're performing as follow:

$$p_i = \begin{cases} \lceil p_i \times 10^{14} \rceil \bmod n & i = 1, .., m \\ \lceil p_i \times 10^{14} \rceil \bmod m & i = m+1, \ldots m+n \end{cases} \tag{4}$$

We suppose the first m values of p (denoted as $\overline{\mu}$) for rows permutation operation and the final n values of this set (denoted as μ) are used for columns permutation. This means that rows permutation operation is performed in such way which i^{th} row elements with $\overline{\mu}_i$ value are shifted into left hand. Also, we have for columns that j^{th} column elements with $\overline{\mu}_j$ value are shifted into up hand. When permutation stage is ended that all rows and columns have shifted. Thus, it is obtained permuted image B.

2.3. Fuzzy measure

2.3.1. Fuzzy measured and Choquet fuzzy integral

Measure is one of the most important concepts in mathematics, for example, concept of integration with related to a given measure. In the classical definition of measure we use

additive property. Additivity is very effective in many applications, but in many real world problems we do not require measure with respect to the additive feature, for example in fuzzy logic, artificial intelligence and etc.

To solving these problems, Sugeno [15] presented fuzzy measure concept and fuzzy integral. Sugeno substituted normal additivity statutes by weaker monotonicity and continuity. Sugeno considered λ-fuzzy measures that is justified in λ-additivity axiom that is special case of fuzzy measure. λ-fuzzy measures have numerous applications in artificial intelligence, neural networks and image process.

Definition of fuzzy measure (monotonic): Suppose that is a measureable space, a fuzzy measure is a function $\mu:\Gamma \to [0,\infty]$ such that the following properties are held:

1) $\mu(\emptyset)=0$
2) If $A,B\in\Gamma$ and $A\subseteq B$ then $\mu(A)\leq\mu(B)$
3) If $A_i\in\Gamma$ and $A_1\subseteq A_2\subseteq\ldots$ then $\lim_{n\to\infty}\mu(A_n)=\mu(\lim_{n\to\infty}A_n)$

Sugeno fuzzy measure: A Sugeno fuzzy measure is a function $\mu:\Gamma \to [0,1]$, so that:
1) $\mu(\emptyset)=0$
2) If $A\subseteq B$ then $\mu(A)\leq\mu(B)$
3) If $A_i\in\Gamma$ and $A_1\subseteq A_2\subseteq\ldots$ then $\lim_{n\to\infty}\mu(A_n)=\mu(\lim_{n\to\infty}A_n)$

Definition of Sugeno λ-fuzzy measure: Let $X=\{x_1,x_2,\ldots,x_n\}$ be a finite set and consider $\lambda\in(-1,\infty)$, a λ-measure is a function of $g_\lambda:2^X \to [0,1]$, such that it satisfied the following condition:
1) $g_\lambda(X)=1$
2) If $A,B\in 2^X$ then $g_\lambda(A\cup B)=g_\lambda(A)+g_\lambda(B)+\lambda g_\lambda(A)g_\lambda(B)$ with $A\cap B=\emptyset$

2.3.2. Choquet fuzzy integral

Fuzzy integral is a non-linear function which can be stated based on any fuzzy measure. Choquet fuzzy integral based on g-fuzzy measure is defined as follow.

Definition of Choquet fuzzy integral: suppose g is a fuzzy measure on X, so fuzzy integral of a function $h:X \to [0,\infty]$ to g-measure is defined as follow:

$$\int h\,dg = E_g(h) = \sum_{i=1}^{n}\left[h(x_i)-h(x_{i-1})\right]g(A_i) \quad \text{where for } A_i\subset X,\ i=1,\ldots,n \qquad (5)$$

where $\{h(x_1),\ldots,h(x_n)\}$ are the ranges and they are defined as where $h(x_1)\leq h(x_2)\leq\ldots\leq h(x_n)$ and $h(x_0)=0$. Also, $g(A_i)=\{x_i,x_{i+1},\ldots,x_n\}$. Fuzzy measure is here used, is Sugeno λ-fuzzy measure.

2.4. The presented model for diffusion

Diffusion is an necessary feature in encryption algorithm, in this section, we'll explain this process. Similar improved key at permutation stage based on plain image, we're applied this procedure for generating key at diffusion stage. To making this dependence, we're divided

permutated image into four blocks, namely $B=[B_1,B_2,B_3,B_4]$. An adaptive control parameter β is calculated by (6) according to the last block B_4.

$$\beta=\frac{\sum_{i,j} B_4(i,j)}{\sum_{i,j} B_4(i,j)^2} \tag{6}$$

As before stated, key used in diffusion stage, is based on pseudo-random sequence based on Choquet fuzzy integral. First, it should be determined initial values and membership function for calculation of this integral. For purposed, we're performed as follow.

First, we are used one $S_{3\times4}$ random matrix which each image is different with another image for generation of 96 bits key. The initial input (h_{01},h_{02},h_{03}) is obtained as follow.

$$\begin{cases} h_{01}=[S(1,1)\oplus S(1,2)\oplus S(1,3)\oplus S(1,4)]-\beta \\ h_{02}=[S(2,1)\oplus S(2,2)\oplus S(2,3)\oplus S(2,4)]-\beta \\ h_{03}=[S(3,1)\oplus S(3,2)\oplus S(3,3)\oplus S(3,4)]-\beta \end{cases} \tag{7}$$

For determination of Choquet fuzzy integral inputs membership function, different techniques have been presented that we are used technique present in [16]. This techniques is as follow:

$$g_{ij}=\frac{1}{1+h_{0j}},\ j=1,2,3. \tag{8}$$

Integral inputs in each stage is update as follow:

$$\begin{cases} h_{i1}=g_{i1}\times\beta+i \\ h_{i2}=g_{i2}\times\beta+i\times2 \\ h_{i3}=g_{i3}\times\beta+i\times3 \end{cases} \tag{9}$$

For determination of initial inputs and membership functions and integral calculation at high level, 3 matrices K_1, K_2 and K_3 having the same size as B_1, B_2 and B_3 are generated. Finally, the cipher image C is obtained as follow:

$$\begin{cases} C_1=B_1\oplus K_1 \\ C_2=B_2\oplus K_2\oplus C_1 \\ C_3=B_3\oplus K_3\oplus C_2 \\ C_4=B_4\oplus K_4\oplus C_3 \\ C=C_4\oplus C_2 \end{cases} \tag{10}$$

To set up self-adaptive property on update integral inputs, $K_4=0$ and $\oplus$ are modular addition operation.

2.5. Encryption process

1-Read the plain image;

2-Shifting the rows with row number from right to left hand, also to shifting columns with column number from dawn to up hand;

3-Compute α according to Eq. (5);

4-Updating initial condition of LSS chaotic map by Eq. (3);

5-Generating LSS chaotic sequence and performing permutation operation;

6-Dividing permuted image into four blocks;

7-Compute β according to Eq. (6);

8-Generating random matrix S of Choquet fuzzy integral's initial inputs;

9-Generating pseudo-random sequence by Choquet fuzzy integral by Eq. (5) and key generation.

10-Obtaining cipher image by Eq. (10).

Due to encryption algorithm symmetric structure, the cryptography process as encryption is performed in converse direction.

3. NUMERICAL TESTS

In this section, we're presented suggested algorithm function by conducting several tests. We're supposed initial condition $x_0=0.3$ and control parameter r=1.3 for LSS chaotic map and following random matrix for Choquet fuzzy integral.

$$S=\begin{bmatrix}0.1067 & 0.7749 & 0.0844 & 0.8001\\ 0.9619 & 0.8173 & 0.3998 & 0.4314\\ 0.0046 & 0.8687 & 0.2599 & 0.9106\end{bmatrix}$$

All of tests have been performed by Matlab 7.8 at an Win 8 PC with an Intel® Core™ i5-3337U 1.8 GHz CPU. In Figure 3(a) has been presented Peppers cropped image with 254×254 measure which adopted as the original plain image. Figure 3(b) is cipher image with suggested algorithm and Figure 3(c) is showed decryption image with correct key.

4. IMPLEMENTATION

4.1. Key sensitivity and space analysis

One of direct techniques for analysis a cipher image is complete exploring attack but having enough time. Thus, we're considered large key space until it will possible. Key space size is equal to number all of separate keys which can be used in cipher system. Our algorithm key

space is made based on initial condition and control parameter of the LSS map and random matrix 96 bits, so general space of suggested algorithm is 10^{124} which it is an big space.

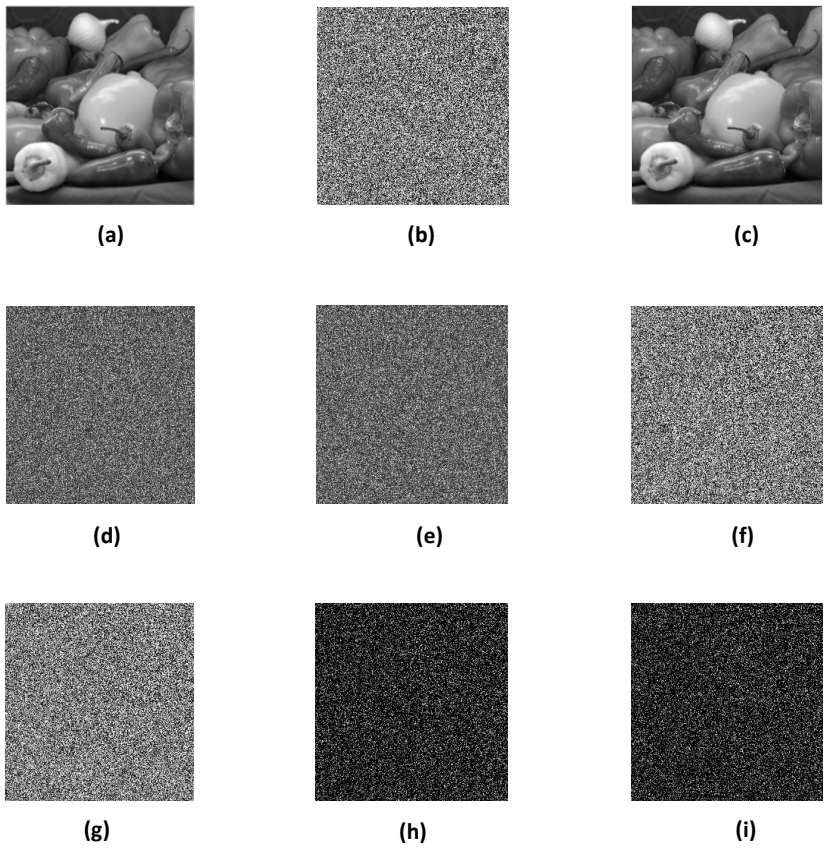

Figure 3. Test of Peppers image (a) plain-image; (b) cipher-image; (c) correct decryption; (d) decryption with 10^{-14} changed in x_0; (e) decryption with 10^{-14} changed in r; (f) cipher-image with 10^{-14} changed in x_0; (g) cipher-image with 10^{-14} changed in r; (h) difference between (b) and (f); (i) difference between (b) and (g);

The key high sensitivity is one of useful cipher system and obtained two forms: (1) when two keys with negligible difference are used for plain image encryption, it should be different obtained cipher images; (2) if there is few difference between decryption and encryption key, so it cannot decrypted correctly.

4.2. Statistical analysis

If one attacker cannot decrypted cipher image using key space exploring; So, statistical analysis is applied. Histogram is showed pixels distribution at one image. Figure 4(a) is indicated Peppers original plain image histogram. By using our algorithm, novel distribution of image pixel has been presented in Figure 4(b). As seen in figure, pixels distribution is nearly uniform which can be ineffective the statistical attack.

In an encryption algorithm, NPCR (Number of Pixel Change Rate) is defined as Eq. (11), it is measured by study of change effect rate of one pixel at plain image to corresponding cipher image. You suppose that C_1 and C_2 are two cipher images correspond with plain images P_1 and P_2, thus there is one difference in pixel. Table 1 is indicated separate images NPCR using suggested algorithm.

$$NPCR = \frac{\sum_{i,j} D(i,j)}{M \times N} \times 100\% \tag{11}$$

which if $C_1(i,j)=C_2(i,j)$, so $D(i,j)=0$, otherwise $D(i,j)=1$.

4.2.1 Correlation and Entropy

We are randomly chosen 4200 pair of adjacent pixels (vertical, horizontal and diagonal) at plain image and cipher image correspond to it. Correlation between two adjacent pixels is calculated as follow:

$$r_{xy} = \frac{cov(x,y)}{\sqrt{D(x)}\sqrt{D(y)}} \tag{12}$$

which, $cov(x,y) = \frac{1}{N}\sum_{i=1}^{N}\left(x_i - E(x)\right)\left(y_i - E(y)\right)$, $E(x) = \frac{1}{N}\sum_{i=1}^{N} x_i$ and $D(x) = \frac{1}{N}\sum_{i=1}^{N}\left(x_i - E(x)\right)^2$.
Table 2 is showed Peppers cipher image and plain image correlation coefficients. Results are indicated that correlation between two adjacent pixels at plain image is sufficiently big, whereas, it is very small in cipher image. Thus, encryption has influence very well.

Information entropy, is most important redundancy feature. You suppose that m is informational resource, calculation formula of information entropy is based on equation (13).

$$H(m) = \sum_{i=0}^{2^n - 1} p(m_i) \log_2 \frac{1}{p(m_i)} \tag{13}$$

which $p(m_i)$ is indicative m-symbol probability. We are used Eq. (13) for cipher images entropy calculation. Table (3), is showed entropy values for different images. As best entropy value for randomization of information is 8, Table 3 values are indicative randomization of cipher images.

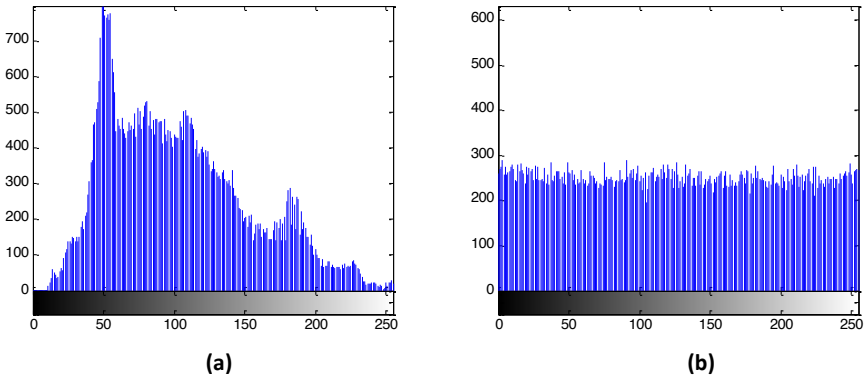

Figure 4. Histogram (a) plain-image of Peppers; (b) cipher-image of Peppers

Table 1. NPCR for different images.

Images eight	peppers	cameraman	trees	football
NPCR 99.1883	99.6249	99.6170	99.5748	99.5520

Table 2. Correlation coefficients between adjacent pixels.

Directions	Horizontal	Vertical	Diagonal
Plain-image	0.9865	0.9829	0.9678
Cipher-image	0.0067	-0.0137	-0.0065

Table 3. The results of information entropy.

Directions football	peppers	cameraman	trees
Plain-image 6.7134	7.5295	7.0097	5.6388
Cipher-image	7.9650	7.9623	7.91967.9569

5. CONCLUSION

We planned a self-adaptive image encryption algorithm. It was used an chaotic system composed of two 1D, Sine and Logistic maps and Choquet fuzzy integral for key sequence generation. However, different from existing algorithms, the keystreams generated in the permutation and diffusion stages are both dependent on the plain-image. It can solve the fixed keystream problem. In each round, the keystream is also different, due to the self-adaptive updating method. Finally, all tests are indicated that suggested algorithm can be meet high level of security.

REFRENCES

[1] . R.-J. Chen, S.-J.Horng, (2010), "Novel SCAN-CA-based image security system using SCAN and 2-D von Neumann cellular automata", Signal Process.: Image Commun. 25(6), pp 413–426.
[2] T.-H. Chen, K.-C. Li, (2012), "Multi-image encryption by circular random grids", Inf. Sci. 189(0), pp 255–265.
[3] L. Li, A.A. Abd El-Latif, X.M. Niu, (2012), "Elliptic curve Elgamal based homomorphic image encryption scheme for sharing secret images", Signal Process.92(4), pp 1069–1078.
[4] Y. Zhou, K. Panetta, S. Agaian, C.L.P. Chen, (2013), "(n,k,p)-gray code for image systems", IEEE Trans. Cybern. 43(2), pp 515–529.
[5] X. Liao, S. Lai, Q. Zhou, (2010), "A novel image encryption algorithm based on self-adaptive wave transmission", Signal Process. 90, pp 2714–2722.
[6] Abd El-Latif AA, Li L, Wang N, Han Q, Niu XM, (2013), "A new approach to chaotic image encryption based on quantum chaotic system", exploiting colors paces. Signal Process. 93, pp 2986–3000.
[7] Bin Muhaya FT, "Chaotic and AES cryptosystem for satellite imagery", (2013), Telecommun Syst52, 573–81.
[8] Zhang YS, Xiao D, "Cryptanalysis of S-box-only chaotic image ciphers against chosen plaintext attack", (2013), Nonlinear Dyn 72, 751–6.
[9] Xiaoling Hung, Guodong Ye, "An efficient self-adaptive model for chaotic image encryption algorithm", (2014), Commun Nonlinear Sci Numer Simulat19, pp 4094–4104.
[10] Yicong Zhou, long Bao,C.L. Philip Chen,"A new 1D chaotic system for image encryption", (2014), Signal Processing 97, pp 172–182.
[11] Zhu CX. "A novel image encryption scheme based on improved hyperchaotic sequences", (2012), Opt Commun 285, pp 29–37.
[12] Li CQ, Liu YS, Xie T, Chen MZQ. "Breaking a novel image encryption scheme based on improved hyperchaotic sequences", (2013), Nonlinear Dyn73, 2083–9.
[13] Hongjun Liu, Xingyuan Wang, Abdurahman Kadir, "Color image encryption using Choquet fuzzy integral and hyper chaotic system", (2013), optic124, pp 3527-3533.
[14] Yong Zhang, "Comments onColor image encryption using Choquet fuzzy integraland hyper chaotic system", (2014), Optic125, pp 5560-5565.
[15] M. Sugeno, "Fuzzy measures and fuzzy integrals: a survey", (1977) Fuzzy AutomataDecision Process, 89–102.
[16] S. Medasani, J. Kim, R. Krishnapuram, "An overview of membership function generation techniques for pattern recognition", (1998) , Int. J. Approx. Reason. (19) (3–4), pp 391–417.