Integration of chaotic sequences uniformly distributed in a new image encryption algorithm

Nassiba Wafa ABDERRAHIM , Fatima Zohra BENMANSOUR and Omar SEDDIKI

Telecommunication Laboratory, Faculty of Technology
Abou-Bekr Belkaïd University, Tlemcen, 13000, Algeria

Abstract

In this paper we propose a new chaotic secret key cryptosystem, adapted for image encryption in continuous mode, which is based on the use of tow one-dimensional discrete chaotic systems: Bernoulli map and Tent map. The pseudorandom sequences generated by the two maps are characterized by independence of their states, uniformly distributed, so hear integration provides excellent properties of confusion and diffusion, and large space for the secret key, because it consists of parameters and initial states of the chaotic maps. The security tests results of our cryptosystem are very satisfactory.

Keywords: *chaos, image encryption, secret key, chaotic maps, pseudorandom sequences.*

1. Introduction

The utilization of chaos in cryptography, brings improvement over standard methods of encryption (DES, IDEA, AES), in particularly to transmit large amounts of secure information in real time, such as images and videos [1].

The advantage of using chaotic systems in data encryption lies in the dynamic behavior attached to chaotic systems, and their random nature. Indeed a chaotic system is described by a set of nonlinear dynamical and deterministic equations. Although these equations define completely its evolution, it is unpredictable in the long term, this non-predictability comes from the fact that chaotic systems are very sensitive to initial conditions [2] [3].

These properties have motivated many researchers to the study of systems for generating chaos, in order to develop new encryption algorithms with high level security [4][5][6], especially for images encryption [7] [8][9]. However, various cryptanalysis have exposed some inherent drawbacks of chaotic cryptosystems [10][11]. Recent studies show that the attackers can extract useful information from the ciphertext when it is generated directly from the digital cipher, which is constructed from simple chaotic orbit [10]. Therefore, the use of a good chaotic generator, with desirable dynamical statistical properties, is very important to design a safe cryptosystem [12]

On our side we propose a chaotic cryptosystem for images encryption, where the choice of chaotic systems is focused on the two one-dimensional chaotic systems: Bernoulli and tent maps. Despite their mathematical simplicity and ease of implementation, these maps generate chaotic behavior rich enough. The integration of the pseudorandom sequences generated from these tow chaotic maps in the operations of confusion and diffusion, makes the procedure adopted for encryption more complex and stronger against the various attacks.

The rest of the paper is organized as follows. In the second section we describe the chaotic systems employed. Then, in the third section we present encryption algorithm in details. The security of the algorithm is analyzed in the fourth section. Finally, conclusions are given in section five.

2. Description of chaotic systems

In order to optimize our cryptosystem in terms of efficacy and security, we chose to integrate the two one-dimensional chaotic maps: Bernoulli map and Tent map. This in order to obtain complex chaotic dynamics based on simple mathematical models.

Bernoulli map [13] and Tent map [14] are defined by the recursive equations (1) and (2), respectively in [0, 1]:

$$x_{n+1} = (p * x_n) \; mod \; 1 \quad (1)$$

$$y_{n+1} = p(1 - |1 - 2y_n|) \quad (2)$$

Where b and p are the critical parameters that direct the behavior of both systems. However, for obtain chaotic behavior, b must be in [1, 5], and p in [0, 1].

The chaotic sequences generated by the two maps and the simulation of their distribution are presented in the figure (1) and (2) respectively. Also the simulation results of statistical dependence of the states sequence using auto/cross correlation functions are shown in figure (3).

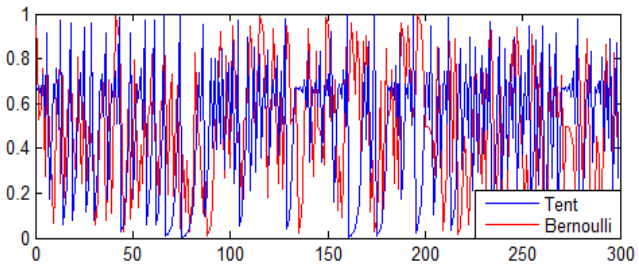

Fig. 1 Chaotic sequences generated by the two maps.

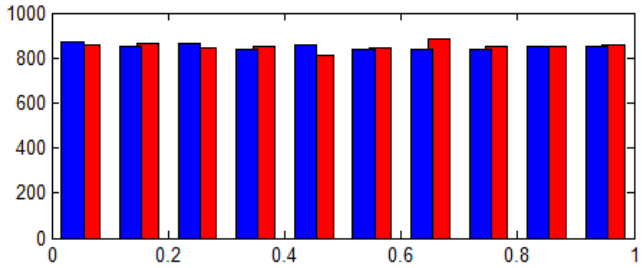

Fig. 2 Distribution of the sequences generated by the tow maps after 8500 iteration.

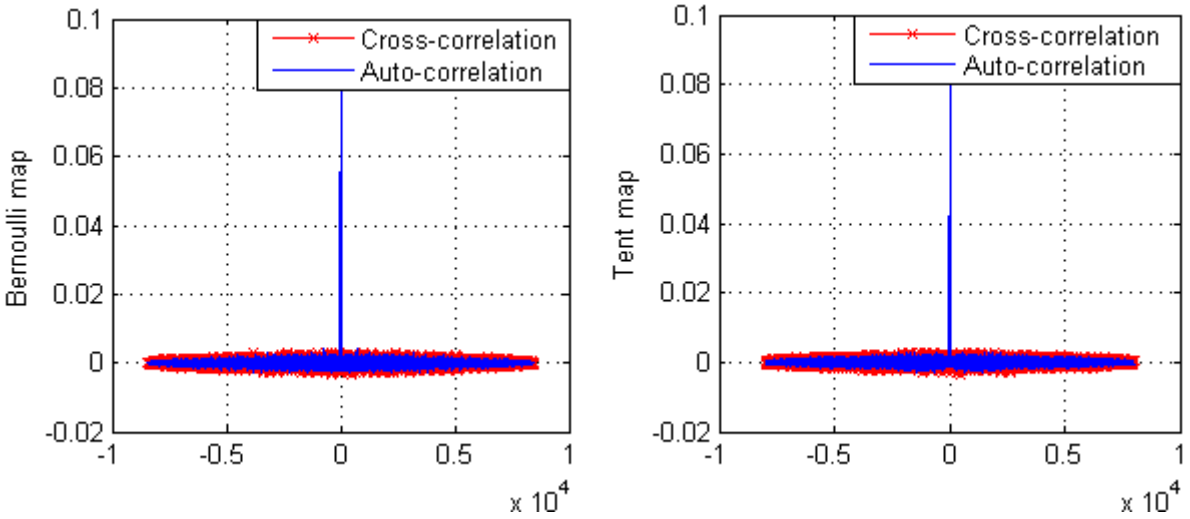

Fig. 3 The simulation results of the auto/cross correlation functions after 8500 iteration.

From (fig. 2) we can see that the chaotic sequences generated by the two maps are characterized by a uniform distribution, which is necessary for encryption, to mask the redundancy of the original data for good confusion.
We also observe from (fig. 3) that the chaotic sequences have excellent auto/cross correlation performance: the autocorrelation function is approximate delta function, and the cross-correlation is near to zero, which means that the sequences are uncorrelated. These characteristics are very interesting to remove the statistical relationship between clear and encrypted images, which corresponds to diffusion.

Therefore the integration of these chaotic sequences in encryption algorithm makes it very difficult to distinguish the sequences of the points from each chaotic map, and decryption becomes impossible without the exact knowledge of initial values and parameters of the two maps.

3. Principle of the proposed algorithm

The proposed algorithm is based on the use of pseudo-random number sequences generated from the two chaotic systems: Bernoulli map and Tent map, used some in confusion and other in diffusion. The algorithm is as follows:

- The first step is to generate arrays of the same size, containing decimal values (0-255), the size of these tables depends on the size *d* of the processed image, it is equal to M × N × V, where M and N respectively the numbers of rows and columns of the image and V the bytes number for each pixel.

The first table X corresponds to chaotic sequence generated by Bernoulli map, while the second Y corresponds to the chaotic sequence generated by Tent map.

$$X = \{x_1, x_2, x_3 \dots x_d\} \quad (3)$$

$$Y = \{y_1, y_2, y_3 \dots y_d\} \quad (4)$$

The values of the two tables are normalized in [0..255] using the formulas (5) and (6), then for be integrated in a chaotic image with uniform distribution of the same size as the original image according to (7).

$$x_k = mod(floor(x_k * 10^{15}), 256), \qquad k\ 1..d \quad (5)$$

$$y_k = mod(floor(y_k * 10^{15}), 256), \qquad k\ 1..d \quad (6)$$

$$C_{i,j} = \begin{cases} x(k), if\ mod\ (x_k + y_k, 2) = 0 \\ y(k), if\ mod\ (x_k + y_k, 2) = 1 \end{cases} \quad (7)$$

Where $k = 1$ .. d and $C_{i,j}$ are the pixel value of i[th] row and j[th] column of the image chaotic. This chaotic image will be used for confusion.

- To complete the encryption process a rearrangement step of pixels is added to change the original location of input pixel values. This is achieved by switching the positions pixels of the original image two to two. The indices selection of rows and columns of pixels to switch is performed by the chaotic sequences (9) and (10) respectively.

$$z = (x \oplus y) mod\ 256 = \{z_1, z_2, z_3 \ldots z_d\} \quad (8)$$

$$z1 = mod\ (LSB(z_k) \times i, N) \quad (9)$$

$$z2 = mod\ (MSB(z_k) \times j, M) \quad (10)$$

These chaotic sequences are calculated from the two previous tables, where the transition of (8) to (9) and (10) required converting the array elements Z in binary, to extract the least significant bits and the most significant bits to each array element Z.
This step allows the introduction of diffusion. However, it is best to run it several rounds (λ times), to increase its effectiveness.

- The last step is to combine the chaotic image to the swapped original image by the addition modulo 2 (XOR bitwise). The following diagram illustrates the complete process of the encryption algorithm.

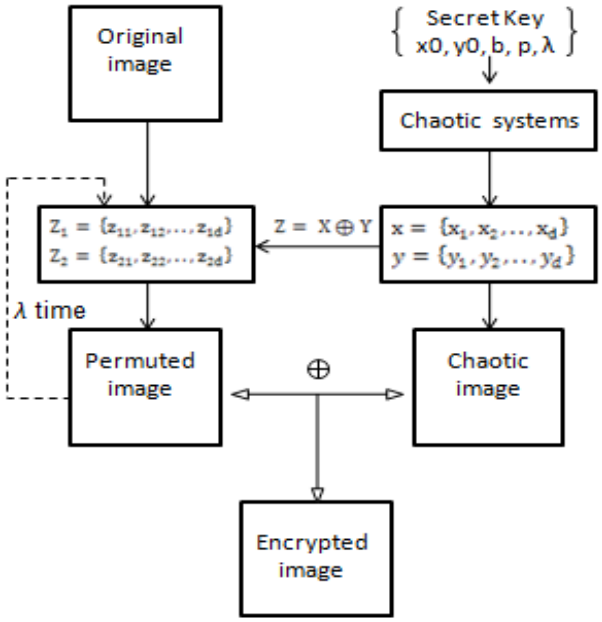

Fig. 4 Schematic description of the encryption algorithm

The iterations number λ, initial conditions x0 and y0, and the parameters b and p are the secret key of our cryptosystem.

The decryption algorithm is almost the same as encryption, but a number of instructions are swapped and we use the inverse operations of confusion and diffusion.

4. Security analysis

An encryption algorithm is considered secure if an adversary who has intercepted an encrypted data does not a feasible technique to retrieve information on the original data, or the key used, specifically, it must resist to all kind of statistic and exhaustive attacks.

Under these conditions a series of tests is applied to multiple images using the secret key {x_0 = 0.3352647527, y_0 = 0.3159865486, b = 2.999555, p = 0.995899, λ = 3}. The overall results of these tests give an idea of the robustness degree of the proposed algorithm.

4.1 Analysis of histograms

The histogram of an image shows the frequency distribution of pixels by gray level in the image, for this reason, the histogram associated to the encrypted image should hide the frequency distribution of the original image.

Figure (4) shows the three channels histograms associated to the resulting images during the encryption process: from the original image to the encrypted one.

By comparison, the histogram of the encrypted image is fairly uniform and differs significantly from that of the original image. The encryption algorithm proposed makes the statistical dependence between the encrypted image and the original image almost random.

On the other hand, these visual results can be confirmed by an entropy calculation.

4.2 Calculation of entropy

The entropy value of an image indicates the probability distribution of gray levels constituting the image. This value is calculated from the formula (11) [15]:

$$h(k) = -\sum_{i=1}^{n} p(k_i) log_2(p(k_i)) \quad (11)$$

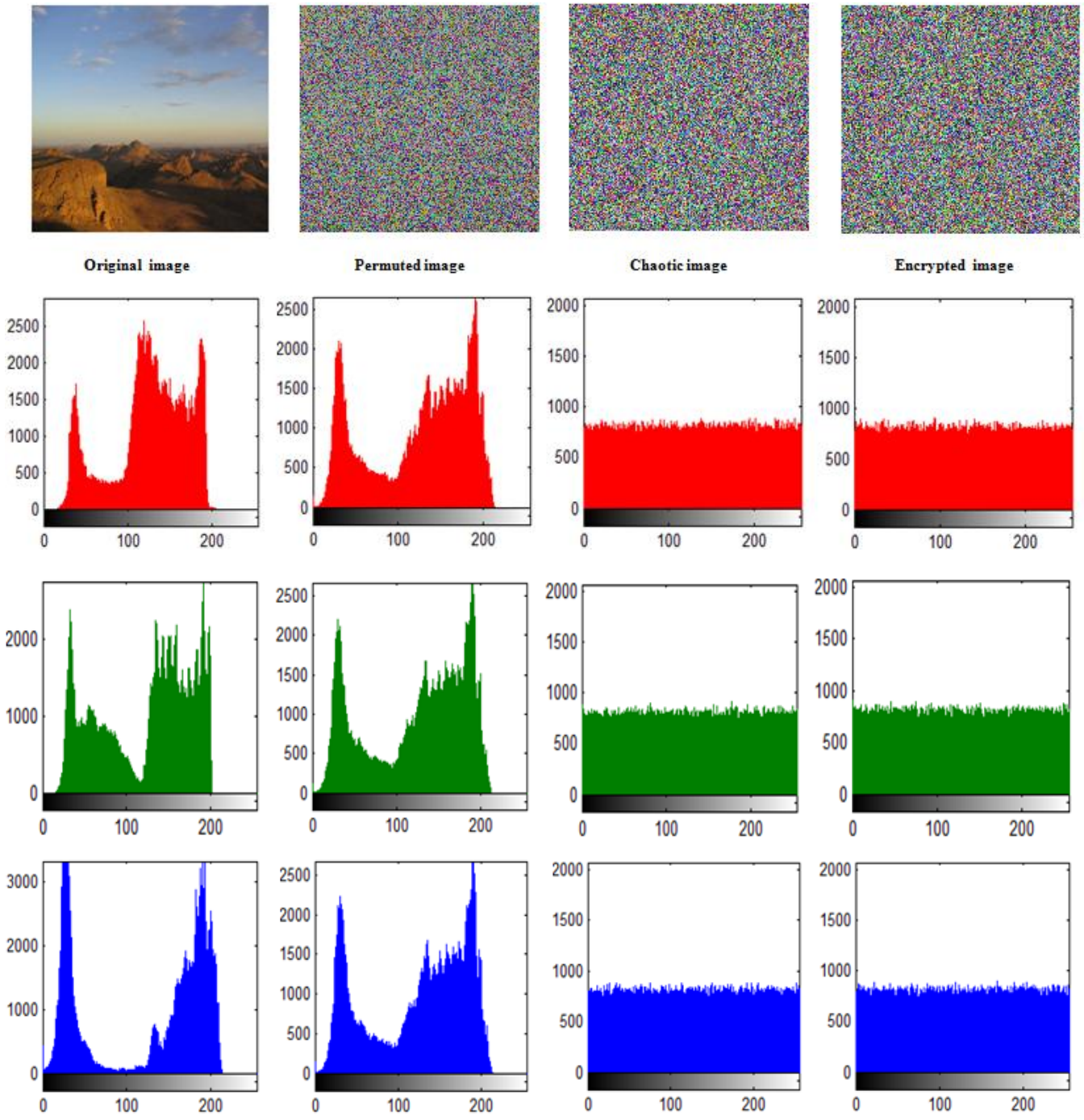

Fig. 5 Histograms visualization

Where $p(k_i)$ denotes the pixel value probability of k_i in the image. In case where the probability distribution of image pixels are identical, $p(k_i) = \frac{1}{n}$, and maximum entropy $h_{max} = log_2(n)$. h_{max} should be equal to 8 for perfect encrypted image. The entropy measures calculated for several images are presented in table1.

4.3 Correlation analysis

The image data are characterized by their high correlation between adjacent pixels. This measure is calculated from the formula (12) [16]:

$$C(r) = \frac{\sum_{i=1}^{N}((x_i - \overline{x})(y_i - \overline{y}))}{\sqrt{(\sum_{i=1}^{N}(x_i - \overline{x})^2)(\sum_{i=1}^{N}(y_i - \overline{y})^2)}} \quad (12)$$

Where x_i and y_i represent the values of adjacent pixels belonging to the original image and its encrypted image respectively. For good security, the correlation of the encrypted image should be negligible and very close to zero.

Table (1) contains the values of the different measures of correlation and entropy, obtained after the tests performed on several original images (IO) and their encrypted versions (IC).

Table 1: Measures of entropy and correlation

Images	*Entropy IO*	*Entropy IC*	*Correlation*
Image 1	7.4375	7.9997	-0.0029
Image 2	7.6972	7.9995	-0.0030
Image 3	7.8856	7.9996	-0.0025
Image 4	7.5029	7.9996	-0.0015
Image 5	7.9171	7.9998	-3.2106e-004

These two statistical measures give us an idea of the capacity of the cryptosystem to resist attacks that reduce the space of an exhaustive search.

From these results we can conclude that the proposed algorithm has good skills for the confusion and the diffusion.

4.4 Analysis of the size of the key space

To prevent brute force attacks the encryption algorithm must uses a key large enough. The secret key of our cryptosystem consists of two initial conditions, two control parameters of chaotic systems and an integer number of iteration. This last must be carefully chosen to establish the compromise between efficiency and security of the cryptosystem.

After numerous tests of the encryption algorithm we found that a space of 2^4 is the most suitable for the iterations number, and with a precision of $10^{16} \approx 2^{53}$ for the rest mentioned elements, we obtain a size of 2^{216}. The total key length is large enough to ensure security against brute force attacks.

4.5 Analysis of sensitivity to changes in the secret key

To test the sensitivity of the proposed cryptosystem to the secret key, we encrypted and decrypted an image using two slightly different secret keys. This is to introduce a variation of 10^{-16}. Figure (4-c) shows the decrypted image obtained.

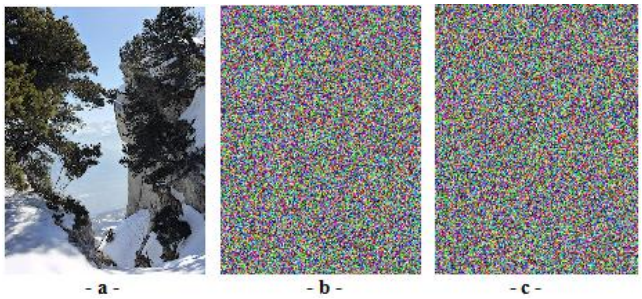

Fig. 6 Sensitivity to changes in the secret key, (a) source image, (b) encrypted image, (c) decrypted image.

The encrypted image is absolutely different from the original, and gives no useful information for decryption. This sensitivity to the secret key resulting of chaos characteristics and the structure of the proposed algorithm.

5. Conclusion

In this paper we presented a new chaotic secret key cryptosystem, adapted for images encryption in continuous mode, based on the integration of chaotic pseudorandom sequences generated by two chaotic maps, where their parameters and initial states constitute the secret key of our cryptosystem. The results of security tests obtained show the robustness of the algorithm proposed against the various attacks. This is due to the complexity of the combination of confusion/diffusion adopted, and its high sensitivity to the secret key.

REFERENCES

[1] R. Mizanur, H. Anwar and M. Hussein, "A real-time privacy-sensitive data hiding approach based on chaos cryptography". IEEE, 2010.
[2] X. Tao, W. Kwok-wo, and L.Xiaofeng, "Swlective image encryption using a spatiotemporal chaotic system", Chaos, 2007, vol. 17, pp. 023115-1- 023115-12.
[3] W. Xianyong and G. Zhi-Hong , "A novel digital watermark algorithm based on chaotic maps", Physics Letters A, 2007, vol. 365, pp. 403-406.
[4] K.Ganesan, R.Muthukumar, K.Murali. "Look-up Table Based Chaotic Encryption of Audio Files", Trans Circ Systems , APCCAS 2006, IEEE, pp. 407-7.
[5] L.Kocarev," Chaos Based Cryptography: A Brief Overview" , IEEE Circuits and Systems Magazine, 2001, vol. 3, pp. 6- 21.
[6] M. Lakshmanan, "Nonlinear dynamics: Challenges and perspectives", Pramana J. Phys, 2005, Vol. 64, N°4, pp. 617-632.
[7] S. Liu and f. SunF, "Spatial chaos-based image encryption design". College of Control Science and Engineering, China, vol. 52, N°2, 2009, pp. 177-183.
[8] H. Mao-Yu and H. Yueh-Min, " Image Encryption Algorithm Based on Chaotic Maps", IEEE, 2010.
[9] DJ .Goumidi and F. Hachouf, "Modified confusion-diffusion based satellite image cipher using chaotic standard, logistic and sine maps", IEEE, 2010.
[10] S. J. Li, and X. Zheng, "Cryptanalysis of a chaotic image encryption method, Proc. IEEE Int. Symposium Circuits and Systems, 2002, vol. 2, pp. 26-29.

[11] P. Pisarchik, N. J. Flores–Carmona and M. Carpio–Valadez, " Encryption and decryption of images with chaotic map lattices", Chaos, 2006, vol. 16, pp. 033118.
[12] Awad, S. ElAssad, D. Carragata . "A Robust Cryptosystem Based Chaos for Secure Data". IEEE, International Symposium on Image/Video communications over fixed and mobile networks, Bilbao, Spain 2008.
[13] H.G. Schuster and W. Just, "Deterministic chaos: an introduction" Weinheim: Wiley-VCH, 4th Edn, 2005.
[14] G. Jakimoski and L. Kocarev , "Chaos and cryptography: block encryption ciphers based on chaotic maps". Circuits and systems. In: Fundamental theory and application, IEEE Transaction, 2001, vol. 48, N°2, pp. 163-169.
[15] L. Dong, J. Zhaohui and Huanqing F, "A novel fuzzy classification entropy approach to image thresholding". Pattern Recognition Letters, 2006, vol. 27, pp. 1968-1975.
[16] G. Chen, Y.B. Mao and C.K. Chui, "A Symmetric Image Encryption Scheme Based on 3D Chaotic Cat Maps", Chaos Solitons Fractals, 2004, vol. 12, pp. 749-761.