Proc. od the Second Intl. Conf. on Advances in Computer and Information Technology - ACIT 2013
Copyright© Institutue of Research Engineers and Doctors. All rights reserved.
ISBN:978-981-07-6261-2

An Image Encryption Approach Using Quantum Chaotic Map

A. Akhshani
School of Physics, Universiti Sains Malaysia, 11800 USM, Penang, Malaysia

S. Behnia
Department of Physics, Urmia University of Technology, Orumieh, Iran
A. Akhavan
School of Computer Sciences, Universiti Sains Malaysia, 11800 USM, Penang, Malaysia
S-C. Lim Z. Hassan
School of Physics, Universiti Sains Malaysia, 11800 USM, Penang, Malaysia

***Abstract*—The topic of quantum chaos has begun to draw increasing attention in recent years. Dissipative quantum maps can be characterized by sensitive dependence on initial conditions, like classical maps. By using significant properties of quantum chaotic map such as ergodicity, sensitivity to initial condition and control parameter, one-way computation and random like behavior, we present a new scheme for image encryption. Based on all analysis and experimental results, it can be concluded that, the proposed scheme is efficient and secure. Although the chaotic map presented in this paper aims at image encryption, it is not just limited to this area and can be widely applied in other information security fields.**

I. Introduction

Since 1990s, many researchers have noticed that there exist a close relationship between chaos and cryptography [1], [2]. Chaotic systems have many important properties, such as the sensitive dependence on initial conditions and control parameters and random like behavior. These are the key properties which are exploited in secure communication and cryptography [3]. The major core of these chaotic cryptosystems consists of one or several chaotic maps serving the purpose of encrypting of image [5], [6], [7], [8]. In recent years, many algorithms based on logistic map [9], [10], piecewise linear/nonlinear chaotic maps [14], [15], [16], [17], [18], [19], random map [20] and hyperchaotic system [21] have been proposed. Since the late 1970s there has been concerns that what happens if a classical chaotic system becomes quantized, a subject that has now come to be called "quantum chaos". One aim of the field of quantum chaos is the study of quantum versions of classical chaotic systems. Quantum maps are eventually the quantized of classical maps. Thus quantum maps may be thought of as the quantum equivalents of canonical transformations. The quantization schemes for maps are different and many classically chaotic maps have been quantized including the standard map [18], [19], logistic map [20], baker map on the torus [21], [22], [23] and on sphere [24]. In this paper, a novel image encryption scheme based on modified quantum logistic map is proposed. The proposed algorithm takes advantage of a quantum chaotic map, which has high complexity and also randomness of the sequences generated by this type of map is very high. Also in this algorithm the initial conditions and control parameters of the map are modified during the encryption process, and the high sensitivity of this map to very small changes in initial conditions and control parameters provides a very secure encryption algorithm.

II. Chaotic Map

In order to better understand the meaning of quantum chaos, one can choose the quantum analog of these classical systems and observe their behavior. In the context of quantum chaos, the δ-kicked rotor model has been extensively used. The quantum version of the kicked rotator has been used to unfold chaotic features in quantum mechanics such as quantum resonance, diffusion, and dynamical localization [25]. It is given by:

$$H = \frac{1}{2J} j_z^2 + V(\theta) \sum_n \delta(t - nT) \tag{1}$$

where, J is the moment of inertia of the rotator, $V(\theta)$ is the perturbation parameter, and j_z is the angular momentum of the rotator. A quantum kicked rotator system may represent a new quantum map which demonstrates positive lyapunov exponents [26], [27]. The derived map demonstrated a period-doubling route to chaos. This chaotic map with lowest-order quantum corrections is governed by the following equations:

$$x_{n+1} = r(x_{(n)} - x_{(n)}^2 - y_{(n)}) \cos^k(-\lambda \frac{e^{-mb}}{b}) \tag{2}$$

Where λ is a number between 0 and 1: $0 < \lambda < 1$ and as to the Yukawa potential, m is the screening parameter. Note that for small values of the coupling strength ($c \to 0$), or equivalently $b \to \infty$, the map reduces to the classical logistic map. The above equation demonstrates a map with four control parameters (r,m,k and b) [27].

III. Proposed Algorithm

In this section, Eq. (2) is selected from the chaotic maps to be used in encryption/decryption process: The proposed cryptosystem is a block cipher algorithm based on the proposed quantum chaotic map. The image encryption algorithm proposed in this paper consists of the following major steps:

- Step 1: First the Plain images M (with $m \times n$ pixels size) is imported and transformed into an matrix $M(1]times(m \times n/32))$ each block containing 32 bits.
- Step 2: The keys for the algorithm which are initial conditions and control parameters (r, k, m, b and λ) are input.
- Step 3: In order to remove the possible transient effect behavior, first 1000 iterations of the map Eq (2) is ignored.
- Step 4: In this step the map is iterated once and the new generated values for the initial conditions are employed to encrypt a 32bit block of the Matrix M (M_i) using the following equation.

$$C_i = [floor(X_i \times 2^{16})mod \quad 2^{16}]concat[floor(Y_i \times 2^{16})mod \quad 2^{16}]xorM$$

- Step 5: The main objective of this step is to create a connection between cipher image and the keys, in such a way that a very small modification in any of the keys or the plain image would result a completely different cipher image (to prevent known cipher text, and plaintext attack). In this step the control parameters r, b, m, λ and k are modified using the new generated Ci (note that the new values for all control parameters are in the chaotic region).
- Step 6: The operations above are repeated for each of the element of matrix M until the Matrix exhausted. Then the values of the Matrix C are reversed and replaced with M one more time so that the image is encrypted twice (once from beginning to the end, and second time from the end to the beginning).

The decryption process is almost the same as the encryption just with reversed steps. Since both encryption and decryption procedures have similar structure, they essentially have the same algorithmic complexity and time consumption. The length of the ciphertext is the same as thought the plaintext. This features is among the most important features of our introduced cryptosystem.

IV. Experimental results

The following experimental results are presented to demonstrate the efficiency of the proposed image encryption algorithm. The standard gray scale and color images "House" (Fig. 1) with the size 256×256 pixels is used for this experiment. The plain image is shown in Fig. 1 and corresponding cipher image is shown in Fig. 2.

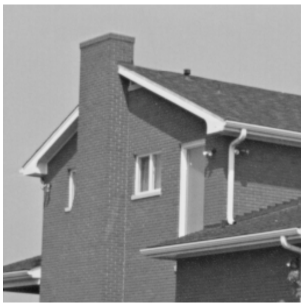

Fig. 1. Plain image.

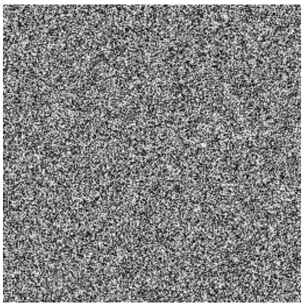

Fig. 2. Ciphered image.

V. Security Analysis

A. Distribution of the ciphertext

With a statistical analysis of "House" image and its encrypted image, their grey-scale histograms are given in Figs. 3 and 4. Fig. 4 shows uniformity in distribution of grey-scale of the encrypted image.

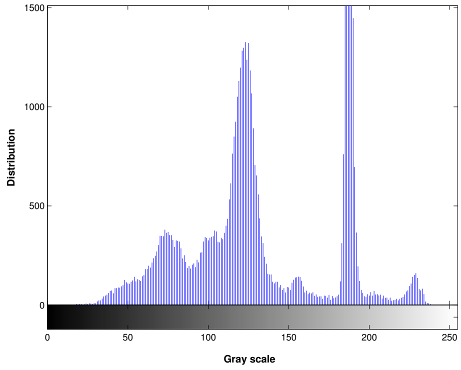

Fig. 3. Ciphered image.

B. Key space analysis

Key space size is the total number of different keys that can be used in the encryption. A good encryption scheme should be sensitive to the secret keys, and the key space should be large enough to make brute-force attacks infeasible.

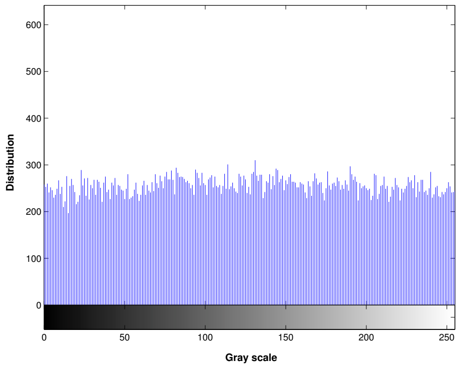

Fig. 4. Ciphered image.

The key space for a cryptographic algorithm should not be less than 2^{128} in order to resist brute force attacks [28]. The presented chaotic map is highly sensitive to the all parameters mentioned above. In this chaotic map the intervals of initial conditions and control parameters are: $x_0 \in [0,1]$, $r \in [3.78,4]$, $m \in [1,4]$,$b \in [6,\infty)$, $k \in [1,\infty)$. If the precision is 10^{-16}, therefore, the size of the key space is 10^{80} $\approx 2^{265}$. Apparently, the key space is large enough to resist all kinds of brute force attacks.

C. Block Entropy

Information theory is a mathematical theory of data communication and storage founded in 1949 by Claude E. Shannon. The quality of image encryption is commonly measured by the Shannon entropy over the ciphertext image. However, this measurement does not consider to the randomness of local image blocks [31]. In this section, block entropy is used to measure the quality of image encryption. The block entropy is the total Shannon entropy of length-L sequences [30]. To calculate the block entropy H(B), we have:

$$H_B(X) = \sum_{l=0}^{2^N-1} P_l \log_2 \frac{1}{P_l} = \sum_{l=0}^{2^N-1} \frac{\aleph(l)}{MN} \log_2 \frac{MN}{\aleph(l)}, \quad (3)$$

$$\overline{H_B(X)} = \sum_{i=1}^{K} \frac{H(B_i)}{K}, \quad (4)$$

where $H(B_i)$ denotes the information entropy for the ith image block and $\overline{H_B(X)}$ is sample mean of block entropy for randomly selected image blocks. Denote the number of pixels within image X at pixel intensity scale l as $\aleph(l)$. Then P_l= $\frac{\aleph(l)}{MN}$ [31]. Note that MN=16-by-16=256 block size is considered for gray image L=256. Theoretical mean and STD of the block entropy for an ideally encrypted image (block size= 16-by-16=256) as follows: Meanμ_B=7.17496635253268 and Stdσ_B=0.0524379986136107 [29]. The value of critical point $H^\star$ and block entropy for different K with the significant level (α=0.001) are represented in Table I. By comparing H_B with the corresponding critical value $H^\star$, it is able to accept or reject the hypothesis that the test image is ideally encrypted within a certain confidence level [29].

TABLE I
THE VALUE OF CRITICAL POINT $H^\star$ AND BLOCK ENTROPY FOR DIFFERENT K

K	K=36	K=49	K=64	K=81	K=100
$H^\star$	7.14945268	7.15287541	7.15536289	7.15724564	7.15935445
$\overline{H_B(X)}$	7.18123456176687	7.18288215150470	7.18646554207311	7.19175501599527	7.19590992334254
K	K=121	K=144	K=169	K=196	K=225
$H^\star$	7.16165495	7.16287564	7.16324890	7.16495347	7.16513288
$\overline{H_B(X)}$	7.19765031183149	7.20027336533953	7.20092406405891	7.20107608770999	7.20140849084107
K	K=256	K=289	K=324	K=361	K=400
$H^\star$	7.16548596	7.16560258	7.16589752	7.16656488	7.16976402
$\overline{H_B(X)}$	7.20336420835976	7.20472133151398	7.20566117860653	7.20682056354978	7.20754488862332

If the block entropy score of an encrypted image is less than $H^\star$, then the null hypothesis is rejected. Hence, the encrypted image is not random as a random image [31]. From the rows of $\overline{H_B(X)}$ in Table I, it is clear that the block entropy test scores matches our expectation of image randomness. So that, the information leakage in the encryption process is negligible, and so the encryption system is secure against the entropy attack.

D. Avalanche criterion

In order to prove the claimed sensitivity to the plaintext, we may generate two plain images with just one-pixel difference. Figs. 5 and 6 show the difference between two plain images and their corresponding cipher image. The bits change rate of the cipher is 49.991%, and very close to the ideal value of 50%.

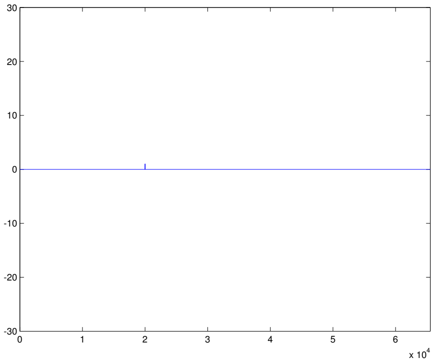

Fig. 5. Difference in plain image.

E. Differential Attack

In order to resist differential attack, a minor alteration in the plain-image should cause a substantial change in the cipher-image. To test the influence of one-pixel change on the whole image encrypted by the proposed algorithm, two common measures were used: $NPCR$ and $UACI$ [14], [15]. NPCR represents the change rate of the ciphered image provided that only one pixel of plain image changes. $UACI$ which is the unified average changing intensity, measures the average intensity of the differences between the plain-image and the ciphered image. For calculation of $NPCR$ and $UACI$, let us

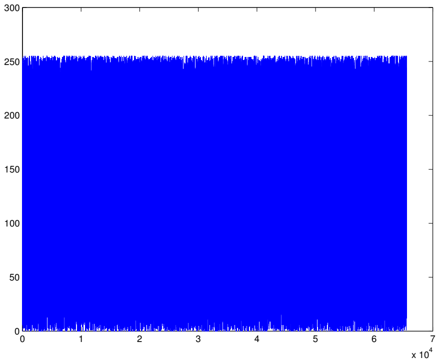

Fig. 6. (Difference in cipher image.

assume two ciphered images C_1 and C_2 whose corresponding plain images have only one-pixel difference. Label the grey-scale values of the pixels at grid (i, j) of C_1 and C_2 by $C_1(i, j)$ and $C_2(i, j)$, respectively. Define a bipolar array, D, with the same size as image C_1 or C_2. Then, $D(i, j)$ is determined by $C_1(i, j))$ and $C_2(i, j)$, namely, if $C_1(i, j) = C_2(i, j)$ then $D(i, j) = 1$; otherwise, $D(i, j) = 0$. $NPCR$ and $UACl$ are defined by the following formulae [14], [15]:

$$NPCR = \frac{\sum_{i,j} D(i,j)}{W \times H} \times 100\% \tag{5}$$

$$UACI = \frac{1}{W \times H}\left[\sum_{i,j} \frac{|C_1(i,j) - C_2(i,j)|}{255}\right] \times 100\% \tag{6}$$

where W and H are the width and height of C_1 or C_2. Tests have been performed on the proposed scheme by considering the one-pixel change influence on a 256 grey-scale image of size 256×256. We obtained $NPCR = 0.00324(1-NPCR = 0.99676)$ and $UACI = 0.33$. The percentage of pixel changed in encrypted image is over 99% even with one-bit difference in original plain-image. The results show that a swiftly change in the original image will result in a significant change in the ciphered image.

F. Speed Analysis

Apart from the security considerations, some other issues on image encryption are also important, such as the running speed for real-time image encryption/decryption. We have also analyzed the speed of the proposed image encryption/decryption technique on an Intel Core 2 Duo 2.66 GHz CPU with 1 GB RAM running on Windows 7 and using Visual C++ .NET compiler. The average time used for encryption/decryption on 256 gray-scale images of size 256×256 is shorter than 16 ms (decryption and encryption speed are the same). It seems that the proposed algorithm is very fast. It should be noted that, the encryption/decryption speed are the same.

G. Tests for randomness

To ensure the security of a cryptosystem the cipher must have some properties such as good distribution, long period, high complexity and efficiency. In this paper, we used various types of tests to examine the quality of our proposed pseudo random number generator algorithm based on chaotic function, Eq. (2), and to draw conclusions on the randomness of the sequences produced by deterministic processes. Several tests are used to examine the randomness of the presented algorithm, these tests are DIEHARD [32], NIST statistical test suite [33] and ENT test suite. ENT test is a collective term for the three tests which are the Entropy, Chi-square, and Serial correlation coefficient (SCC) test. To apply statistical random tests such as NIST and DIEHARD, a sufficiently large size of data is required. If the statistical tests are conducted on small size samples, then tests will yield an inaccurate inference. Therefore, to avoid this problem a gray-scale sample image with the size 3872×2592 pixels is used for the cipher text randomness test. According to Tables II-IV which present NIST, DIEHARD and ENT test results respectively, the introduced generator passes all the tests and demonstrates better results in comparison to the other chaotic pseudo random number generators such as the logistic map [34], [35].

TABLE II
RESULTS OF THE SP800-22 TESTS SUITE FOR THE 32-BIT PROPOSED PRBG.

Test name	P-value	Result
Frequency	0.036184	Success
Block-frequency	0.378215	Success
Cumulative sums-Forward	0.164720	Success
Cumulative sums-Reverse	0.123825	Success
Runs	0.946902	Success
Long runs	0.978065	Success
Rank	0.643709	Success
FFT	0.476515	Success
Non-periodic templates	0.544686	Success
Overlapping templates	0.749475	Success
universal	0.324545	Success
ApEn	0.427691	Success
Serial p-value 1	0.457324	Success
Serial p-value 2	0.822545	Success
Linear complexity	0.912896	Success
Approximate Entropy $(m = 10)$	0.352368	Success
random-excursions		
X=-4	0.965568	random-excursions
X=-3	0.585359	random-excursions
X=-2	0.354880	random-excursions
X=-1	0.524458	random-excursions
X=1	0.138618	random-excursions
X=2	0.172546	random-excursions
X=3	0.941584	random-excursions
X=4	0.527786	random-excursions

TABLE III
RESULTS OF THE SP800-22 TESTS SUITE FOR THE 32-BIT PROPOSED PRNG.

Random excursions variant (state X)		
X=-9	0.041587	Success
X=-8	0.972564	Success
X=-7	0.248596	Success
X=-6	0.246587	Success
X=-5	0.845785	Success
X=-4	0.392456	Success
X=-3	0.604512	Success
X=-2	0.361453	Success
X=-1	0.117458	Success
X=1	0.586253	Success
X=2	0.224856	Success
X=3	0.392456	Success
X=4	0.545648	Success
X=5	0.456495	Success
X=6	0.324564	Success
X=7	0.866756	Success
X=8	0.634893	Success
X=9	0.581575	Success

TABLE IV
DIEHARD TESTS SUITE FOR THE 32-BIT PROPOSED PRNG.

Test name	Average Value	Result
Birthday spacing	0.9354845	Success
Overlapping permutation	0.9955468	Success
Binary rank 31×31	0.464974	Success
Binary rank 32×32	0.957564	Success
Binary rank 6×8	0.494486	Success
Bitstream	0.635675	Success
OPSO	0.74456	Success
OQSO	0.42956	Success
DNA	0.51982	Success
Count the ones 01	0.156859	Success
Count the ones 02	0.939478	Success
Parking Lot	0.684256	Success
Minimum distance	0.382220	Success
3DS spheres	0.269830	Success
Squeeze	0.931761	Success
Overlapping sum	0.789258	Success
Runs	0.725698	Success
Craps	0.24940	Success

TABLE V
MAX GRADE OF ENT TEST SUITE.

Test name	Average Value	Result
Entropy	7.999986	Success
Arithmetic mean	127.6768	Success
Monte Carlo	3.136987000	Success
Chi-square	749.64	Success
Serial Correlation Coefficient	0.000368	Success

VI. CONCLUSION

Recently, we proposed an image encryption algorithm based quantum logistic map [36], [27]. In this paper, a novel image encryption scheme based on modified quantum logistic map is proposed. The aim of this paper is to evaluate that the quantum maps can be used in cryptography. Experimental results indicate that the proposed scheme possesses the advantages of acceptable encryption speed, large key space and high level of security, and can be implemented efficiently.

REFERENCES

[1] R. Brown, LO. Chu, “Clarifying chaos: examples and counterexamples”, Int. J. Bifurcat. Chaos 1996;6:219.

[2] J. Fridrich. “Symmetric ciphirs based on two-dimensional chaotic maps”, Int. J. Bifurcat. Chaos 1998;8:1259.

[3] C.E. Shannon. “Communication theory of secrecy systems”, Bell Syst. Tech. J. 1949;28:656.

[4] M.S. Baptista. “Cryptography with chaos”, Phys. Lett. A 1998;240:50.

[5] A. Akhavan, H. Mahmodi, A. Akhshani. “A new image encryption algorithm based on one-dimensional polynomial chaotic maps”, Lect Notes Comput Sci 2006;4263:963-71.

[6] A. Akhshani , H. Mahmodi, A. Akhavan. “A novel block cipher based on hierarchy of one-dimensional composition chaotic maps”, IEEE Int Conf Image Process 2006:1993-6.

[7] L. Kocarev, G. Jakimoski. “Logistic map as a block encryption algorithm”, Phys Lett A 2001;289:199.

[8] J. Lang, R. Tao, Y. Wang. “Image encryption based on the multiple-parameter discrete fractional Fourier transform and chaos function”, Opt. Commun. 2010;283:2092.

[9] V. Patidar, NK. Pareek, KK. Sud. “A new substitution-diffusion based image cipher using chaotic standard and logistic maps”, Commun Nonlinear Sci Numer Simul 2009;14(7):3056.

[10] N. Masuda, K. Aihara. “Cryptosystems with discretized chaotic maps. IEEE Trans”, Circuits Syst. Part I 2002;49(1):28.

[11] H. Liu, X. Wang. “Color image encryption based on one-time keys and robust chaotic maps”, Comput. Math. Appl. 2010;59:3320.

[12] G. Zhang, Q. Liu. “A novel image encryption method based on total shuffling scheme”, Opt. Commun. 2011;284:2775.

[13] S. Behnia, A. Akhshani, S. Ahadpour, H. Mahmodi, A. Akhavan. “A fast chaotic encryption scheme based on piecewise nonlinear chaotic maps”, Phys Lett A 2007;366:391.

[14] A. Akhshani, S. Behnia, A. Akhavan, H. Abu Hassan, Z. Hassan. “A novel scheme for image encryption based on 2D piecewise chaotic maps”, Opt. Commun. 2010;283:3259.

[15] A. Akhavan, A. Samsudin, A. Akhshani. A symmetric image encryption scheme based on combination of nonlinear chaotic maps, J. Franklin Inst. 2011;348:1797.

[16] S. Behnia, A. Akhshani, S. Ahadpour, A. Akhavan, H. Mahmodi. “Cryptography based on chaotic random maps with position dependent weighting probabilities”, Chaos Solitons Fract 2009;40:362.

[17] N. Smaoui, A. Karouma, M. Zribi. “Secure communications based on the synchronization of the hyperchaotic Chen and the unified chaotic systems”, Commun. Nonlinear Sci. Numer. Simul. 2011;6:3279.

[18] G. Casati, B.V. Chirikov and F.M. Izrailev. “Stochastic behavior of a quantum pendulum under a periodic perturbation”, J. Ford, Lect. Notes Phys. vol. 93, pp.334-52, 1979.

[19] D. L. Shepelyansky, “Localization of Quasienergy Eigenfunction in Action Space”, Phys. Rev. Lett. vol.56, pp.677-80, 1986.

[20] M. E. Goggin, B. Sundaram and P. W. Milonni, “Quantum logistic map”, Phys. Rev. A vol.4, pp.5705-5708, 1900.

[21] N. L. Balazs, A. Voros, “The quantized bakers transformation”, Ann. Phys. vol.190, pp.1-31, 1989.

[22] A. Lakshminarayan, “On the quantum baker’s map and its unusual traces”, Ann. phys. vol.239, pp.272-95, 1995.

[23] M. Fannes, P. Spincemaille, “Multiple return times in the quantum baker map”, Phys. Lett. A vol.294, pp.74, 2002.

[24] P. Pakonski, A. Ostruszka, K. Zyczkowski, “Quantum baker map on the sphere”, Nonlinearity vol.12, pp.269, 1999.

[25] K. M. Frahm and D. L. Shepelyansky, “Diffusion and localization for the Chirikov typical map”, Phys. rev. E 80, pp.016210-20, 2009.

[26] E. Ott, “Chaos in dynamical system”, Cambridge university pess, Canada,(1993).

[27] S. Behnia, P. Ayubi, W. Soltanpoor. “Image encryption based on quantum chaotic map and FSM transforms”, Telecommunications Network Strategy and Planning Symposium (NETWORKS), 2012 XVth International. pp. 1-6.

[28] ECRYPT II Yearly Report on Algorithms and Keysizes, 2010. http://www.ecrypt.eu.org/documents/D.SPA.13.pdf.

[29] Wu, Y., Zhou, Y., Saveriades G., Agaian, S., Noonan, J.P., Natarajan P., 2013. Local Shannon entropy measure with statistical tests for image randomness. Information Sciences 222, 323-342.

[30] Feldman, D.P., McTague, C.S., Crutchfield, J.P., 2008. The organization of intrinsic computation: Complexity-entropy diagrams and the diversity of natural information processing. Chaos, 18, 043106-15.

[31] Wu, Y., Yang, G., Jin, H., Noonan, J.P., 2012. Image encryption using the two-dimensional logistic chaotic map. Journal of Electronic Imaging 21, 013014.

[32] G. Marsaglia, Computer code DIEHARD, 1997, available at, http://stat.fsu.edu/pub/diehard/.

[33] National institute of standards and technology, computer code available at http://csrc.nist.gov/rng/SP800-22b.pdf.

[34] F. James, A review of pseudorandom number generators, Comput. Phys. Commun. 60 (1990) 329344.

[35] A. Kanso, N. Smaoui, Logistic chaotic maps for binary numbers generations, Chaos Solitons Fract 40 (2009) 25572568.

[36] A. Akhshani, A. Akhavan, S.-C. Lim, Z. Hassan. “An image encryption scheme based on quantum logistic map”, Commun Nonlinear Sci Numer Simulat 17 (2012) 46534661.