© 2016 IJSRSET | Volume 2 | Issue 2 | Print ISSN : 2395-1990 | Online ISSN : 2394-4099
Themed Section : Science and Technology

New Text Encryption Algorithm Based on Block Cipher and Chaotic Maps

Ekhlas Abass Albhrany[1], Dr. Luma Fayeq Jalil[2], Prof. Dr. Hilal Hadi Saleh[3]

[1]Department of Computer Science, Mustansiriyah University, Baghdad, Iraq
[2,3]Department of Computer Science, University of Technology, Baghdad

ABSTRACT

In this paper, new algorithm for text encryption based on block cipher and chaotic maps is proposed. The proposed algorithm is encrypted and decrypted a block size of (8×8) byte. The nonlinear substitution S-box component that previously designed based on the method in [16], which is depends on 2d Logistic map and 2d Cross chaotic map, is used in this algorithm. Each block is first permuted by using Standard map and then substituted by the bytes in S-box. The resulted block is then Xored with the key. A random key generator based on Tent map is proposed to generate the key sequences that used in the encryption and decryption process. The result from key space analysis, differential attack analysis, information entropy analysis, correlation analysis of the plaintext and ciphertext characters have proven that the proposed algorithm can resist cryptanalytic, statistical and brute force attacks, and achieve higher level of security.

Keywords: text encryption, block cipher, chaotic map, S-Boxes, 2d Logistic map, 2d Cross map, 2d Standard map, 2d Tent map.

I. INTRODUCTION

The principle motivation behind this paper to plan a novel block text encryption algorithm by using chaos theory. Chaos theory reliably assumes a dynamic part in current cryptography. The primary point of interest of the chaos-based method lies on the arbitrary behavior and the affectability to the initial conditions and control parameters. An important difference between chaos and cryptography lies on the fact that systems used in chaos are defined only on real numbers [1], while cryptography deals with systems defined on finite number of integers [2]. The close relationship between chaotic maps and cryptosystems has been observed in [3,4,5]. This relationship can be built up: first ergodicity in chaos versus confusion in cryptography. Second: sensitive reliance on beginning conditions and control parameters of chaotic maps versus dissemination property of a decent cryptosystem for a little change in the plaintext and in the mystery key. Third: chaotic random-like behavior can be used for producing pseudorandom sequences as a key in cryptography. In a years ago, individuals use the Internet to transmit and store information in content setup. Web is a confortable media to transmit data regardless, meanwhile it is hazardous in light of the way that the data are revealed likewise, can be stolen by software engineers to use them in an unlawful route as blackmail, theft, warlike purposes, and other. One response for this security issue; its goal is making ciphertext from plaintext utilizing a symmetric calculation (one mystery key).

Numerous researchers have attempted endeavors to explore piece encryption calculation so as to advance short preparing time in encryption and decryption. The DNA traits have been proposed for text encryption where the four DNA reason are depicted by binary data, DNA supplement operations are used for data encryption; besides, groupings are used as secret key. The reference [7] has proposed procedure on matrix scrambling which depends on arbitrary capacity, moving and switching methods of round line. This strategy empowers the dispersion handle and is having a one of a kind method of unscrambling it back to the plaintext and is anything but difficult to actualize utilizing network scrambling system. Ultimately, in [8] present symmetric cipher for text algorithm taking into account disorder; they utilize a 128 piece mystery key, two logistic maps with advanced pseudorandom sequences, plain text characteristics, and only one permutation-diffusions

round. In this paper, a new block and chaotic encryption / decryption system for text is suggested. The proposed algorithm consists of three transformations which implemented based on the chaotic system.

The remaining part of the paper is sorted out as takes after: section 1 the basic theory of the chaotic functions, section 2 the propped algorithm. Section 5 presents the statistical analysis. The security analysis of the proposed algorithm is achieved in Section 6, before conclusions.

1. Basic theory.

In this paper five chaotic maps are used: 2d logistic map, 2d cat map, 2d cross map, 2d standard map and 2d tent map.

1.1 2D Logistic Map.

One of the most known and widely used chaotic systems is the 1D Logistic map, which is defined as follows [9]: -

$$f(x) = \mu\chi(1-\chi) \qquad \chi \in (0,1) \tag{1}$$

where μ is the control parameter. The system is in chaos on condition that 3.569<μ<4.0.

1D logistic map is extended to the 2D logistic map. The extended logistic map has extensive key space and more reliance on control parameters. The extended logistic map is more complex to estimate the secret information. It additionally indicates more amount of chaotic behavior on the producing of sequence [10]. In overall, it increases the complexity of the algorithm. The 2D logistic map is defined as follows: -

$$f(x) = \begin{cases} \chi_{i+1} = \mu_1\chi_i(1-\chi_i) + \gamma_1 y_i^2 \\ y_{i+1} = \mu_2 y_i(1-y_i) + \gamma_2(\chi_i^2 + \chi_i y_i) \end{cases} \tag{2}$$

When 2.75 <μ_1<=3.4, 2.75 < μ_2<=3.45, 0.15 <γ_1<=0.21, 0.13 <γ_2<=0. 15, the system is in chaotic state and can generate two chaotic sequences in the region (0, 1].

1.2 2D Cat Map.

A 2D Cat map is first presented by V.I. Arnold in the research of ergodic theory [11]. Let the coordinates of a positions P = {(x, y) | x, y = 1, 2, 3, . . ., N}, a 2D Cat map with two control parameters is as follows [11]:

$$\begin{cases} \chi_{i+1} = (x + ay) \bmod N \\ y_{i+1} = (bx + (ab+1)y) \bmod N \end{cases} \tag{3}$$

Where, a, b are control parameters which are positive integers and (χ_{i+1}, y_{i+1}) is the new position.

1.3 2D Cross Map.

Cross-chaotic map is defined as following:

$$\begin{cases} \chi_{i+1} = 1 - \mu y^2 \ , \\ y_{i+1} = \cos(k.\cos^{-1}\chi_i), \quad \chi, y \in [1.-1] \end{cases} \tag{4}$$

Where μ and k are the control parameters of the system, respectively. When μ=2 and k=6, this system exhibits a great variety of dynamics behavior [12].

1.4 2D Standard map.

The so-called standard map was introduced in [13], [3], and is described by: -

$$\begin{cases} a_{i+1} = (a_i + b_i) \bmod 2\pi \ , \\ b_{i+1} = (b_i + K\sin(a_i + b_i)) \bmod 2\pi, \end{cases} \tag{5}$$

here the both ith states a_i and b_i take real values in [0,2π) for all i and K is the control parameter and k > 0. The standard map was discretized in a directed manner by exchanging x = aN/2 π, y = bN/2π, K = kN/2π into Eq. (4), which maps from [0,2 π) * [0,2π) to N * N. After It discretization, the map becomes

$$\begin{cases} x_{i+1} = (x_i + y_i) \bmod N \ , \\ y_{i+1} = (y_i + K\sin\frac{x_{i+1}N}{2\pi}) \bmod N \ , \end{cases} \tag{6}$$

where K is a positive integer. This discretized map properties may not be as good as the original one, but it can be executed in the integer domain, which reduces the computational complexity. In addition it is more appropriate for real-time data encryption. The standard map is used to implement data permutation [3].

In the standard map the corners pixels of a square image have some particular properties. For example, after any number of iterations, the pixel at location (0, 0) stays unchanged. In order to avoid it, [15] a method to avoid this weakness, the location of pixels at the corners (0, 0), (N- 1, 0) , (N- 1,N - 1) and(0,N -1) is modified. That is, the normal scan order is changed into a random one. After the iteration of chaotic map, an arbitrary-pair (r_x,

r_y) is created, which represents the location of an arbitrary chosen pixel in the square image.

The two parameters r_x and r_y both belong to range [0.. N-1] and the modified chaotic map becomes

$$\begin{cases} x_{i+1} = (x_i + r_x + y_i + r_y) \bmod N, \\ y_{i+1} = (y_i + r_y + K \sin \frac{x_{i+1} N}{2\pi}) \bmod N. \end{cases} \quad (7)$$

Through the study and the experience of Standard map equation, its inverse is calculated using the proposed equation

$$\begin{cases} y_i = \left(y_{i+1} - r_y - K \sin \frac{x_{i+1} N}{2\pi}\right) \bmod N, \\ x_i = (x_{i+1} - r_x - y_i - r_y) \bmod N. \end{cases} \quad (8)$$

1.5 2 D Tent map.

Tent map is a discrete time chaotic system described by relation [16]:-

$$x_{n+1} = f(x_n) = \begin{cases} \frac{x_n}{a}, & \text{if } x \in [0, a], \\ \frac{(1 - x_n)}{(1 - a)}, & \text{if } x \in (a, 0] \end{cases} \quad (9)$$

where, $a \in [0,1]$ is the control parameter and x_n is the current state of the system. Tent map has uniform invariant probability density in [0, 1] interval.

2. The proposed algorithm.

The proposed algorithm for text encryption consists of two major algorithms: encryption algorithm and decryption algorithm. Each algorithm has three main steps which are:-

- Create the Substitution S-Boxes.
- Generation of key using the proposed Pseudo Random Number Generator.
- Encryption and Decryption algorithms.

We will describe each step in details in the next section.

2.1 Create the Substitution S-Boxes.

In the proposed algorithm, the S-box that is created based on the method in [17] is used. The proposed S-box is a table of 16 × 16 integer values (256 bytes). The S-box is created by using 2d Logistic map and 2d Cross map.

2.2 The Proposed Pseudo Random Number Generator.

The core of Pseudo Random Number Generator (PRNG) is the Tent chaotic map. Four integer numbers are generated in each round of the generator. The main idea of the proposed PRNG consists of the following major steps

Step 1 : Input the initial condition (x_0) and control parameters (a) which are floating point numbers where the precision is 10^{-16}, to the Tent map. These numbers are considered as the keys of the generator.

Step 2 : Tent map is iterated 100 times and the results are ignored in order to eliminate the transient effect of chaotic map.

Step 3 : Iterate Tent map two times. The two outputs are Xored to produce one output.

Step 4 : The resulted floating number output is translated to binary sequence of random length.

Step 5 : The binary sequence is translated to four integer numbers. Each number is in the rang [0..255]. The first number (8-bit number) is started from the bit at the location (1) of the sequence. The second number is started from the bit at the location (10) of the sequence. The third number is started from the bit at the location (20) of the sequence. The last number is started from bit at the location (30) of the sequence.

Step 6 : Repeat from step 3 until the desired number of integer numbers is reached. When the number of generated keys of one block (64 byte) plus to the control values and parameters of chaotic maps (Standard map (r_1, r_2, k) and Cat map (a, b)) is reached to 69 byte, the parameters of Tent map x_0 and a are modified using simple addition operation between the initial and last value of these parameters in order to increase the complexity of detect the keys.

2.3 Encryption Algorithm

The design tools of the proposed text encryption are based on chaotic map with non-linear transformation functions. The main steps of the proposed encryption algorithm are

Step 1 : Input the plaintext file into T array which is a one dimensional array, the initial parameters (x_0,y_0) to create the S-box and lastly the initial parameter (x_0) and the control value(a) for the PRNG. These parameters numbers are floating point numbers where the precision is 10^{-16} and considered as the keys of the algorithm.

Step 2 : Create the S-box in the method discussed in [17].

Step 3 : Generate the key by using the proposed PRNG algorithm. The generated key is transformed into blocks $K_1K_2K_3K_4\ldots.K_t$, where B_i $(1\leq i \leq t$) denotes the i-th key block with size 8×8 byte. In addition, for each block five parameters that are necessary for permutation using Standard map and form byte substituted in S-box are generated also by the proposed PRNG.

Step 4 : T array is divided into blocks $B_1B_2B_3B_4\ldots.B_t$, where B_i $(1\leq i \leq t$) denotes the i-th plaintext block with size 8×8 byte. When the last block of the plaintext is less than 8×8 pixels, it treats as special array B (1×L) where L is the number of byte in this block.

Step 5 : For each block do three transformation :-

Permutation transformation: each block is diffused using Standard map.

Mixing transformation: each byte in resulted block is Xored with the byte in the key block.

Substitution transformation: each byte in the resulted block is substituted using S-box.

Step 6 : The output ciphertext is saved in file.

2.4 Decryption Algorithm

The main steps of the decryption algorithm are:-

Step 1 : Input the ciphertext file into C array which is a one dimensional array, the initial parameters (x_0,y_0) to create the S-box and lastly the initial parameter (x_0) and the control value(a) for the PRNG.

Step 2 : Create the S-box.

Step 3 : Generate the key by using the proposed PRNG algorithm. The generated key is transformed into blocks $K_1K_2K_3K_4\ldots.K_t$, where B_i $(1\leq i \leq t)$ denotes the i-th key block with size 8×8 byte. In addition, for each block five parameters that are necessary for inverse Standard map permutation and for inverse byte substituted in S-box, are generated also by the proposed PRNG.

Step 4 : C array is divided into blocks $B_1B_2B_3B_4\ldots.B_t$, where B_i $(1\leq i \leq t)$ denotes the i-th ciphertext block with size 8×8 byte.

Step 5 : For each block do three inverse transformations :-

Invers Substitution transformation: each byte in the ciphertext block is substituted using inverse substitute S-box.

Mixing transformation: each byte in the resulted block is Xored with the byte in the key block.

Invers Permutation transformation: each block is return to its original positions using inverse Standard map.

Step 6 : The output plaintext is saved in file.

3. Experiment result.

The proposed algorithm is implemented using Delphi 7 programming language and the tests are performed on a Laptop with an Intel (R) Pentium(R) CPU B960 @2.20 GH and 2 GB RAM running on Windows 8.1.

3.1 Encryption.

The proposed algorithm has the ability to encrypt and decrypt any character from ASCII table. Figure (1) demonstrates a case of plaintext of size 154 characters and its relating ciphertext utilizing the proposed algorithm and the key are: -

For S-box the parameters are:- x_0=0.9542316752453422, y_0=0.2879675436523319.

For the proposed PRNG the parameters are: - kx_0=0.5467654430043221, a=0.3555400254899316.

3.2 The Security Analysis

The security analysis on the proposed encryption algorithm can be done by analyses

Key space analysis: -In order to make brute-force attacks infeasible, the proposed algorithm ought to have an extensive key space. The size a key space that is smaller than 2^{128} is not secures enough [18]. Here, the

key space is constructed form the parameters that needs for creating the S-box (initial values x_0 and y_0) and parameters values (kx_0 and a) that are needed for generating the key. These parameters are floating point numbers, where each one belongs to [0, 1]. If the precision of each parameter is 10^{-16}, the total space of keys is $2^{213}((10^{16})^4)$. The key space is adequately far reaching to contradict an extensive variety of brute-force attacks.

Key Sensitivity Analysis: - A decent cryptosystem must be sensitive at secret keys this implies two ciphertext created utilizing somewhat diverse keys ought to be altogether different. In Table 1 the plaintext of size 305 characters is encoded utilizing three slightly different keys. The ciphertext with inaccurate key does not demonstrate any data related with plaintext, hence the proposed algorithm is sensitive to secret key.

Plaintext

We can get them to display all in a line going down using Memo1.lines.add and a nested loop statement.

Ciphertext

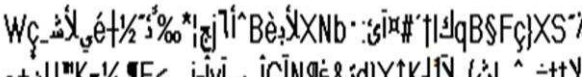
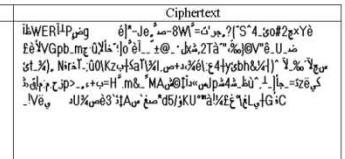
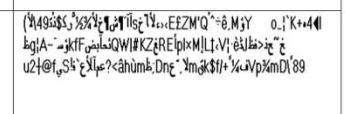
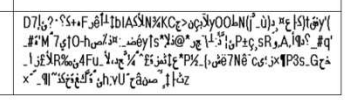


Figure (1): Example of Proposed Encryption

Table 1: Key Sensitivity Example

Plaintext	Encrypted key	Ciphertext
Information security becomes a hot problem which is concerned by our society. Security of the information over the insecure mode of communication. Internet, has been an area of research for years. There have been several techniques developed for encryption/decryption of the information over the years	x_0=0.7698045333215892 y_0=0.1187435556350017 kx_0=0.8869443655400213 a=0.3007654432198765	
	x_0=0.7698045333215893 y_0=0.1187435556350017 kx_0=0.8869443655400214 a=0.3007654432198765	
	x_0=0.7698045333215892 y_0=0.1187435556350018 kx_0=0.8869443655400213 a=0.3007654432198766	

3.3 Statistical Attack Analysis

The statistical analysis of the plaintext and the encrypted image can be considering by:

- Histogram analysis: - indicates how often an image shows up in the content. The histogram can offer information to find the plaintext, the secret key or both. On the off chance that the histogram of the all images in figure content is reasonably equally circulated over the scale, no data about the plaintext can be can be accumulated through histogram examination. The histogram of the plaintext of size 2000 characters is shown in Figure 2 (a). In Figure 2(b), the ciphertext histogram is shown; it is uniform, so the proposed scheme is powerful against histogram attacks in addition to frequency attacks.
- Correlation coefficient analysis: Correlation evaluation is to check the relationship between plaintext and ciphertext. The correlation distribution of two horizontally adjacent bytes in the plaintext of size 2000 characters its ciphertext are shown in Figure3 (a)-(b). This Figure shows that the ciphertext is uniform compared with the plain text correlation Figure. In addition the result of correlation coefficient of this plaintext and its cipher text is **-0.0193** which means the correlation between the plaintext and its cipher text is very small.

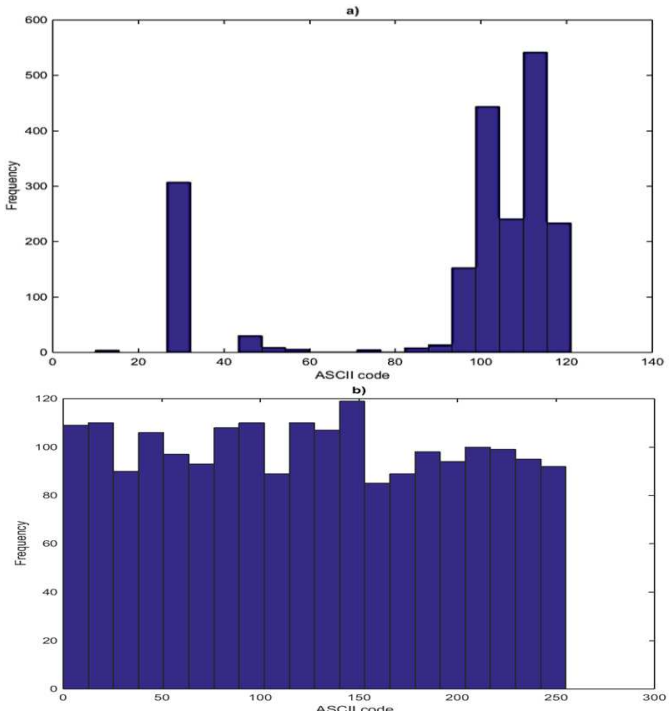


Figure (2): Histograms of : a-plaintext and b-ciphertext

3.4 Differential attack analysis.

A decent encryption algorithm that stays away the known-plaintext attack and the chosen-plaintext attack ought to have the alluring property where little distinction of the plaintext ought to be diffused to the entire cipher text. In differential attack, attackers frequently roll out a little improvement for the plaintext, and use the proposed algorithm to encrypt for the plaintext before and after changing, through standing out two ciphertexts from make sense of the relationship

between the plaintext and the ciphertext. There are two measurements to decide this robustness [6,19]:

- NPCR (Net Pixel Change Rate): - measures the quantity of characters that are diverse between two ciphertexts C1 and C2 from two similar plaintext, the value of NPCR is represented in percentage, where 100% means both cipher texts are totally different. The NPCR is calculated with

$$\mathrm{NPCR} = \frac{\sum_{i=1}^{N} W(i)}{N} \times 100\% \quad (10)$$

where N is the text length and

$$W(i) = \begin{cases} 0, & \text{if } C_1(i) = C_2(i) \\ 1, & \text{if } C_1(i) \neq C_2(i) \end{cases} \quad (11)$$

Where $C_1(i)$ and $C_{2(i)}$ are the symbol value of the cipher text C1 and C2.

- UACI (Unified Average Changing Intensity): - is the intensity difference average between two ciphertexts C1 and C2, where 100% indicates both texts are totally different in amplitude. The UACI is calculated as follows:

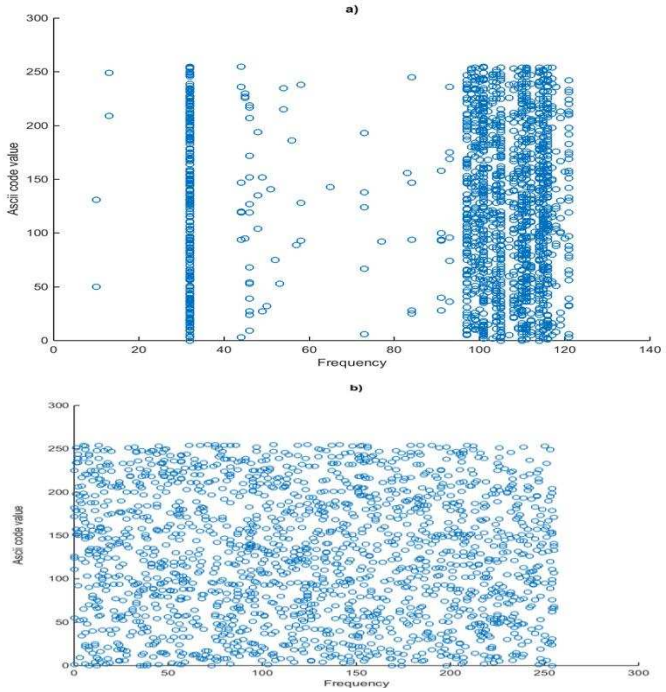


Figure (3) : correlation analyses: a) plaintext correlation and b)ciphertext

$$\mathrm{UACI} = \frac{100}{N \times 95} \sum_{i=1}^{N} |C_1 - C_2| \quad (12)$$

In the proposed algorithm, the NPCR and UACI are acquired with the accompanying steps: to begin with, the plaintexts from Figures (1),(2) and Table 2 are encrypted with the required keys to produce the cipher text C1,C2 and C3; after that, the first symbol of each plaintext is changed to next character (for instance, the first symbol of plaintext in Figure (1) is changed from 'W' to 'X') and the encryption process is repeated with the same keys to produce the new ciphetexts NC1, NC2 and NC3. In Table 2 demonstrates the result of NPCR and UACI. Therefore, the proposed algorithm is robust against differential attacks.

Table 2: The results of UACI and NPCR.

plaintext	NPCR	UACI
Plaintext in Figure (1)	99.5500	32.7982
Plaintext in Table (1)	98.6494	33.0866
Plaintext in Figure (2)	99.5000	33.1067

3.5 Information Entropy Analysis.

Information theory is a scientific hypothesis of information correspondence and capacity. The information entropy H(m) of a plaintext sequence can be computed as [20]: -

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

where N is the number of bits of the message m, 2^N means all possible symbols, $p(m_i)$ represents the probability of m_i and the entropy is expressed in bits. If a message is encrypted with 2^N possible symbols, the entropy should be H(m) = N ideally. In the proposed algorithm, there are 255 different characters, so the maximum entropy is equal

Table 3: Results of entropy analysis of the proposed algorithm

The ciphertext	Entropy
Ciphertext in Figure (1)	7.99648965524622
Ciphertext in Table (1)	7.19648965524622
Ciphertext in Figure (2)	7.29907499110329

II. CONCLUSION

In this paper, new text encryption scheme based on combination of a chaotic map and block cipher is presented. The main idea is to encrypt and decrypt a block size of 8X8 byte based on permutation and substitution the byte in S-box. A random key generator based on Tent map generates key sequences that used in the encryption and decryption process. Security analyses indicate that the proposed algorithm has desirable properties such as the key space analysis; statistical attack analysis and differential attack analysis are performed numerically and visually. All the experimental results show that the proposed encryption scheme is secure because of its large key space; it's highly sensitivity to the cipher keys and plaintext. All these agreeable properties make the proposed algorithm a potential possibility for encryption of multimedia data such as images, audios and even videos.

III. REFERENCES

[1] J. Gickenheimer and P. Holmes, "Nonlinear Oscillations, Dynamical Systems and Bifurcations of Vector Fields". Berlin, Germany: Springer, 1983.

[2] B. Schneier, Applied Cryptography: "Protocols, Algorithms, and Source Code in C". New York: Wiley, 1996.

[3] J. Fridrich, "Symmetric Ciphers Based on Two-Dimensional Chaotic Maps", International Journal Bifurcation Chaos, vol. 8, no. 6, June 1998, pp.1259-1284.

[4] L. Kocarev, "Chaos-based cryptography: A brief overview", IEEE Circuits and Systems Magazine, vol. 1, no. 3, pp. 6-21.

[5] X.Y. Wang and Yu Q., "A Block Encryption Algorithm Based on Dynamic Sequences of Multiple Chaotic Systems". Communications in Nonlinear Science and Numerical Simulation, 2009, vol. 14, no. , pp. 574-581.

[6] L. XueJia, L. MingXin, Q. Lei, H. JunSong and F. XiWen, "Asymmetric Encryption and Signature Method with DNA Technology", Science China Information Sciences, 2010, vol. 53, no. 3, pp. 506-514.

[7] M. Kiran Kumar, S. Mukthyar Azam and Shaik Rasool, "Efficient Digital Encryption Algorithm Based on Matrix Scrambling Technique", International Journal of Network Security & Its Applications (IJNSA), October 2010, vol.2, no.4. pp. 31-41.

[8] M. A. Murillo-Escobar, F. Abundiz-Pérez, C. Cruz-Hernández and R. M. López-Gutiérrez, "novel symmetric text encryption algorithm based on logistic map", Proceedings of the 2014 International Conference on Communications, Signal Processing and Computers.

[9] M. Raj and S. Garg, "An Innovative Approach: Image Encryption with Chaotic Maps using DNA Addition Operation", International Journal of Software and Web Science, IJSWS 14-337, August 2014, pp. 50 - 56.

[10] M. Ahmad and M. Alam, "A New Algorithm of Encryption and Decryption of Images Using Chaotic Mapping", International Journal on Computer Science and Engineering, vol. 2, no. 1, 2009, pp. 46-50.

[11] C. Fu, J. Huang, N. Wang, Q. Hou and W. Lei, "A Symmetric Chaos-Based Image Cipher with an Improved Bit-Level Permutation Strategy", Entropy, vol. 16, 2014, pp. 770-788.

[12] L. Wang, Q. Ye, Y. Xiao, Y. Zou and B. Zhang, "An Image Encryption Scheme Based on Cross Chaotic Map", Image and Signal Processing, IEEE, May 2008, pp. 22 - 26.

[13] E. A. Jackson, Perspectives in Nonlinear Dynamics, Cambridge University Press, vol. 1, Reprint Edition, 1991.

[14] F. Rannou, "Numerical Study of Discrete Plane Area-Preserving Map", Astron & Astrophys: vol. 31, 1974, pp. 289–301.

[15] S. Lian, J. Sun and Z. Wang, "A Block Cipher Based on a Suitable Use of the Chaotic Standard Map", Chaos, Solitons and Fractals, 2005, vol. 26, pp. 117–129.

[16] A. Luca, A. Ilyas and A. Vlad, "Generating Random Binary Sequences Using Tent Map". Proc. IEEE Int. Symposium on Signals, Circuits and Systems (ISSCS), Iasi, Romania, June 30-July 1, 2011, pp. 81-84.

[17] F. J. Luma , H. S. Hilal and A. Ekhlas, " New Dynamical Key Dependent S-Box based on Chaotic Maps". IOSR Journal of Computer Engineering (IOSR-JCE) e-ISSN: vol. 17, N4, 2015, pp. 91-101.

[18] M. François, T. Grosges, D. Barchiesi and R. Erra, "Pseudo- random number generator based on mixing of three chaotic maps", Communications in Nonlinear Science and Numerical Simulation, vol. 19, no. 4,2014, pp. 887–895.

[19] G. Chen, Y. Mao and C. K. Chui, "A Symmetric Encryption Scheme Based on 3D Chaotic Cat Map", Chaos, Solitons & Fractals, vol. 21, July 2004, pp. 749-761.

[20] A. Jolfaei and A. Mirghadri, "Image Encryption Using Chaos and Block Cipher", Computer and Information Science, vol. 4, no. 1, January 2011, pp. 172 – 185.