Advances in Computer Science and Information Technology (ACSIT)
p-ISSN: 2393-9907; e-ISSN: 2393-9915; Volume 3, Issue 6; October-December, 2016, pp. 535-539
© Krishi Sanskriti Publications
http://www.krishisanskriti.org/Publication.html

Image Security with Chaos based Key in Digital World

Monica Pant[1] and A. K. Mohapatra[2]

00503102013 Mtech (ECE) Indira Gandhi Technical University for women Kashmere Gate, Delhi
[2]Dept of IT Indira Gandhi Technical University for women Kashmere gate, Delhi
E-mail: [1]monaa11pant@gmail.com, [2]mohapatra.amar@gmail.com

Abstract—*Everyday we hear the news of data getting stolen, modified and money scams online. As the threat to the information continuous we have to think out ways to make our information safe and secure. Most of the techniques covered are based on the concepts of confusion, diffusion, scrambling and shuffling. Some of the algorithms are DES, AES, RSA and with them are added different scrambling techniques based on Logistic, Baker's and Tent mapping. In the recent times Chaos theory has gained much acknowledgement because of its easy implementation and faster response. Chaos theory shows the dependence on initial conditions and hence much variation due to large number of control parameters.*
The method proposed in this paper is based on Lorenz equation key generation and logical bitxor operation to increase the feasibility of our Cipher image.

Keywords*: Security; Lorenz 6D; Logistic; Bitxor; Chaos; random (key words)*

1. INTRODUCTION

Security is one of the major concerns these days as there is widespread internet connectivity available. The major concerns are about confidentiality, integrity and availability of the data and information. To maintain these 3 factors there is a strong need for enhancing our security mechanisms.

It is not possible to have secured digital data over public channels available all the time. Depending on critical requirements various level of security are required for an image, text or any other data. There are a large number of encryption methods available consisting of logical xor operation, image mapping using any method such as baker's, Arnold cat map, shift and scrambling an image. Shift operation has simplicity in its implementation and is more efficient hence is used in cryptography schemes.

Prior to this we have seen three times Logistic mapping of an image as proposed by Xing, Sheng and Ying [1]. Next to it we have used 3D Lorenz equation where through these equations are used to generate key and circular shift add on to complexity.

Here we have described an image encryption algorithm based on Chaos theory. In this paper random matrix is generated based on Lorenz chaotic equations. We have utilized lorenz chaotic 6D system to generate key by varying the initial conditions and control parameters of equations. A large key space can resist brute force attacks and a secure image is having both confusion and diffusion features. Further this key is used in bitxor operation with the image, bitxor is the binary exclusive or operation implemented on software. After the bitxor operation the image is shifted in one dimension and further shifted to generate the shuffled image. This image is further bitxor with logistic equation thus producing our final cipher image.

This paper is organized as follows the section 1 gives a brief introduction about the need for encryption followed by section 2 which introduces the concept of Chaos theory, followed by image encryption based on pixel manipulation, section 3 gives the result generation with shift and shuffle operations and section 4 gives performance and result analysis.

2. RANDOM NUMBER GENERATION

Related work

Chaos theory has been widely used for the key generation as it has easy implementation. Chaos dependency on initial conditions and random behavior is an aperiodic motion and has got non linear characteristic. With a pseudorandom number generation and by iterating chaotic map we forms the key which is xored with an image. The cipher which is obtained satisfies the NPCR and UACI parameters in image analysis.

In the previous paper [1] written by Xing, Sheng and Ying the author has utilized one dimensional Logistic mapping for the generation of random numbers. There image scrambling was done on the original image followed by circular shifting and again scrambling using logistic mapping and finally again Logistic mapping was done for raising image security. One dimensional chaotic maps are having a smaller key space and hence less security. In [2] paper written by Shu, Xiu Ru, Yi and Yu utilized Prof. G. Chen 3 dimension equation to improve upon the absolute dynamic behaviors. To improve upon three dimensional chaotic system was introduced where one have more than 1 initial conditions and hence control parameters. As the number of dimensions are increased the depth of randomness increases and hence the complexity of the system

The equations by Prof. G. Chen presented in Chen's chaotic system [2]:

$$\begin{cases} \dot{x} = a(y - x) \\ \dot{y} = (c - a)x - xz + cy \end{cases}$$

(1a – 1c)

$\dot{z} = xy - \exp(bz)$

The equations used in this system are similar to Lorenz 6D equations presented in [12]

$$\begin{cases} \dot{x} = exp(a - c) * (y - x) + e(x1 - x) \\ \dot{y} = \exp(c - a) * (y - x\dot{)} + y1 - xz + e(y1 - y) \\ \dot{z} = xy - \exp(b) * z + e * (z1 - z) \\ \dot{x}1 = -a * x1 + a * y1 + d * (x - x1) \\ \dot{y}1 = -x1 * z1 + \exp(\dot{b}1) * x1 + d * (y - y1) \\ \dot{z}1 = x1 * y1 - \exp(\dot{b}1) * z1 + d * (z - z1) \end{cases}$$

(2a – 2f)

These are some changes due to the exponential terms in front of $x,\ \dot{y}$ and $\dot{z}$.

The interdependence between two systems is driven by the d and e parameters. Hence the two systems will be affecting each other such that initial conditions of x_0, y_0, z_0 will affect x_1, y_1, $z_{1.}$

The values of the parameters are a = 32, b = 3.22, c varies in the range of 26 to 29, b_1 =3, d = 7, e = 6 and the step size is chosen as 0.001 with these values the system start showing complete random aperiodic behavior. These are the 6D Lorenz equations based on chaos theory and can be solved by Runga Kutta 4th order method.

3. RANDOM NUMBER GENERATION

Here we will discuss the random number sequence generation generated by Lorenz system. The number Key are of type double point are generated using the Equation (2a-2f)

Key(r, c) = mod((abs(y)- floor(abs(y)))*10^{14}, 256) (3)

y(r, c) is the key generated using the Lorenz equations described above. The abs operation returns the absolute value of y and floor operation rounds the elements of y to nearest integers less than or equal to y .Further the modular operation [2] returns the remainder after division, the division is done by 256 as it is the highest grey values in a grey image.

y(r, c) is the random number matrix generated on iterating values by varying the values of c, b, b_1. The generated random key created by CCS will have initial conditions as = (x_0, y_0, $z_{0,}$ x_1, y_1, z_1) = (-25.965, 20, 14.551, 25.51, 12.55, -25.751). The x_0, y_0, $z_{0,}$ x_1, y_1, $z_{1,}$ c are the initial values of x, y, z, x_1, y_1, z_1 and c is the equation parameter.

The runstest returns a test decision for the null hypothesis that the values in the data vector say x come in random order, against the alternative that they do not. This is done in matlab on the bitxor result to test whether it is random do not and the result of runstest came out to be zero.

4. IMPROVEMENTS IN THE ENCRYPTION SCHEMES

First a logical bitxor operation is performed between a key and our sample image. After the bitxor operation, the image is circularly shifted along a specified dimension. Suppose we have an image v whose contents are to be shifted by a number in both the row and column direction in a matrix. After this the contents of the matrix are further transposed.

It is not necessary to have both column and row shift to be equal. Then we shuffle the elements of the image matrix by random permutation. Finally we have a shuffled image which is again bit xored with the key generated by Logistic equation.

$\dot{x} = a\mathrm{x}0(1 - \mathrm{x}0)$ (4)

x is the simulated series, a is a constant having value of 3.689 and x_0 is the initial value of time series. The first 200 values are rejected due to repetitive behavior. This way we have got 2 keys which increase the key space and can resist brute force attack. This equation generates a series of numbers and these numbers are circularly shifted. After shifting by certain number we obtain sequence of numbers used for bitxor with the Shifted sequence. This is our Key 2 that is used for bitxor with the shuffled image. As in [13] which uses linear feedback shift register.

This gives us our cipher image and we check for the histogram of the image which should show equal distribution of information.

l = circshift(k,5); . (5)

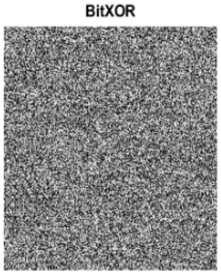
l is the circularly shifted key sequence generated by Logistic and k is the key sequence originally generated.

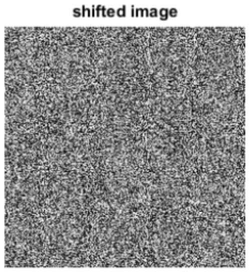
Now bit xor of both k2 and l is performed to generate the final key2

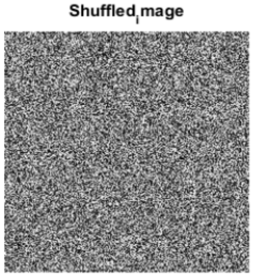
key2 = bitxor(l,k2); (6)

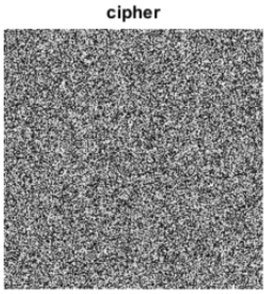
Cipher = bitxor(key2 ,shuffled_image); (7)

This is our final cipher image which is to be transmitted across the channel.



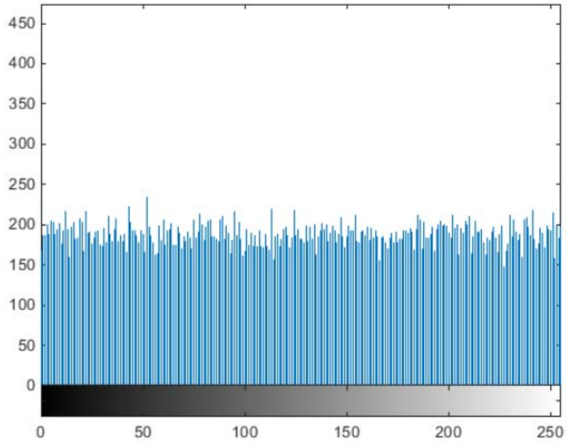


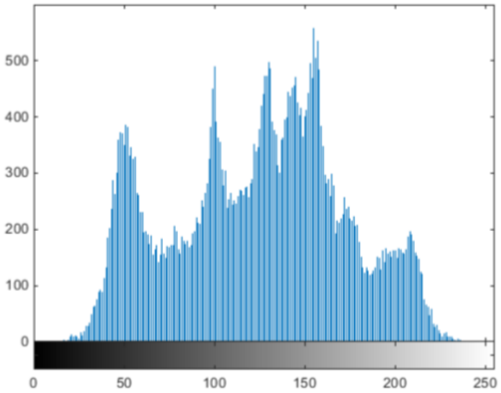


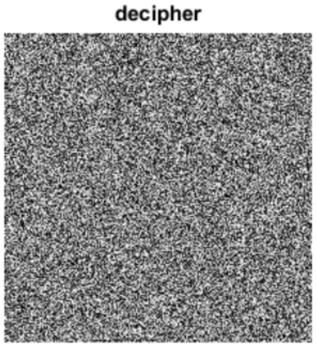


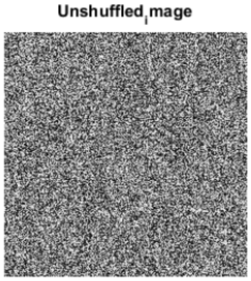
The results of various processes are shown above from (5a - 5f)

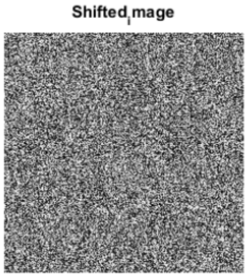
Clockwise we have our original image following it we have bitxor operated image then is our circular shifted operation and finally shuffled image. The last cipher image is the result of Logistic bit xor and finally is the histogram of the cipher.

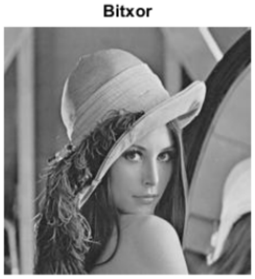












The decryption process is just opposite of the above series of operations.

1. First inverse bit xor of cipher producing decipher.
2. Than perform the inverse shuffling operation
3. After this we have inverse circular shift operation.
4. Lastly we perform the bit xor with the key and generate the output.

Clockwise (6a- 6d) the inverse of our Encryption process i.e. Decryption process . Decipher the decrypted image after bitxor with logistic generated key.6b is the Unshuffled image, 6c is the inverse shifted image and finally we have our image 6d resulted after bit with Lorenz equation generated key.

5. EXPERIMENTAL RESULTS AND PERFORMANCE ANALYSIS

The simulation output and the performance analysis is done in this section. This algorithm is implemented on MatlabR 2014b installed in Dell laptop Intel(R) Core(TM) i3 CPU X64 based processor M350 @ 2.27GHZ with 3GB RAM and 500 GB hard-disk memory space. The original image used in this algorithm is Lena.jpg 220 X 220 matrix w.ith 220 grey levels encrypted individually. The image cannot be retrieved using a wrong key for encryption.

6. PERFORMANCE ANALYSIS

In this scheme the secret space the initial values of Lorenz criteria, we have taken 220 X 220 image as a sample here. The key = ($x_{0,}$ y_0, z_0, $x_{1,}$ y_1, $z_{1,}$ c) is used to create diffusion and confusion in an image.

For a good encryption algorithm the key space should be large enough to resist brute-force attack. The key space for this includes the initial values and control parameters. The key space should not be smaller than 2^{100} ~10^{120} to achieve high level of security. To increase the level of security we have used 2 keys generated by Lorenz equation and Logistic equation hence we have a large key space to resist brute force attack.

7. STATISTICAL ANALYSIS

By looking at the histogram we can see that we have a uniform distribution of information. In order to check the correlation amongst the two adjacent pixels of our original image and ciphered image the following methods are used. Randomly we select pairs of adjacent (Horizontal, vertical and diagonal) pixels from our image and calculate the correlation coefficient of each pair.

$$\mathrm{Cov}(x,\ y) = \frac{1}{N}\sum_{i=1}^{N}(xi - E(x))\ (y_i - E(y)) \qquad (8)$$

$$r_{xy} = \frac{\mathrm{Cov}(x,\ y)}{\sqrt{D(x)\ D(y)}} \qquad (9)$$

where x and y are the gray scale values of two adjacent pixels in the image.

Direction	Correlation coefficient		
	Horizontal	***Vertical***	***Diagonal***
Ciphered image	(0, 0)	(0, 0)	(0, 0)
Original image	0.26732	0.26732	0.26568

$$E(x) = \frac{1}{N}\sum_{i=1}^{N} xi \qquad (10)$$

$$D(x) = \frac{1}{N}\sum_{i=1}^{N} \left(xi - E(x)\right)^2 \qquad (11)$$

Here x and y are the gray scale values of two adjacent pixels in an image.

For numerical analysis the above formulas were used. In the analysis the correlation between the vertical, horizontal and diagonal pixels is found to be zero.

8. DIFFERENTIAL ANALYSIS

For differential analysis the following formulas were used. The change rate i.e. Number of pixel change rate (NPCR) and Unified Average Changing Intensity (UACI) are used.

$$NPCR=\sum_{i=1}^{M}\sum_{j=1}^{N} D(i,j)(\frac{100\ \%}{M\ X\ N}) \qquad (12)$$

NPCR value came out to be .998

$$UACI = \frac{1}{M\ X\ N}[\sum_{i=1}^{M}\sum_{j=1}^{N} | m1(i,j) - \ m2\ (i,j) |]\frac{100}{255} \qquad (13)$$

UACI value came out to be 0.337

where m_1 and m_2 are two different ciphered images. If m_1(i, j) = m_2(i, j) , D(i, j) = 0; otherwise D(i, j) = 1

S. No	Name	NPCR	UACI	Entropy
1.	Xing	99.7	33.66	7.988
2.	Jiang	99.6	33.1	7.977
3.	Khanzadi	99.6	33.46	7.989
4.	Our	99.8	33.76	7.9961

The matlab runstest tells about the randomness and it came out to be 0.

In this proposed method the key of Logistic method is also made complicated by using circular shift and bitxor method.

With Lorenz equations the exponential component has made significant changes in the randomness of the key making it secure.

9. CONCLUSIONS

In this paper we propose an image encryption based on shuffling, cyclic shift and xor operation based on Chaos. The image security can be further increased by using Lorenz equations with increased dimensions as they can be upto 12 dimensions increases the complexity of cipher. Also we can increase the image security using Logistic mapping or tent mapping.In this scheme we tried to increase the security of an image and efficiency of encryption scheme hence it can be applied to images for secure data transmission.

REFERENCES

[1] Novel image encryption algorithm based on cyclic shift and chaotic system by Xing – Yuan Wang, Sheng – Xian Gu, Ying – Qian Zhang.

[2] An improved chaotic cryptosystem based on circular bit shift and XOR operations by Shu – Jiang Xu, Xiu – Bo Chen, Ru Zhang, Yi – Xian Yang, Yu – Cui Guo.

[3] Image Encryption Using Random Bit Sequence Based on Chaotic Maps by Himan Khanzadi, Mohammad Eshghi, Shahram Etemadi Borujeni

[4] New Image Encryption Algorithm Based on Logistic Map and Hyper – chaos by LEI Li – hong, BAI Feng – ming, HAN Xue – hui.

[5] A new image encryption scheme based on a chaotic function by M. Francois, T.Grosges, D. Barchiesi, R.Erra.

[6] A novel chaotic block image encryption algorithm based on dynamic random growth technique by Xingyuan Wang, Lintao Liu, Yingqian Zhang.

[7] A novel color image encryption algorithm based on chaos by Xing Yuan Wang, Lin Teng, Xue Qin.

[8] A new image encryption algorithm based on non – adjacent coupled map lattices by Zhang Ying – Qian, Wang Xing – Yaun.

[9] A New Modified Version of Advanced Encryption Standard Based Algorithm for Image Encryption by Seyed Hossein Kamali, Reza Shakerian, Maysam Hedayati and MMohsen Rahmani

[10] A novel image encryption method based on total shuffling scheme by Guoji Zhang, Qing Liu.

[11] A new chaotic attractor with quadratic exponential nonlinear term from Chen's attractor by Iftikhar Ahmed_, Chunlai Mu, and Fuchen Zhang

[12]Dynamics of coupled Lorenz systems and its geophysical implications by Andrzej Stefanski, Tomasz Kapitaniak, John Brindley.

[13]Image encryption and decryption using chaotic key sequence generated by sequence by Logistic map and sequence of states of linear feedback shift register by Rohith S, K N Hari Bhat, A Nandini Sharma.

[14.] Cryptanalysis of color image encryption algorithm based on chaos by Guangyou Tu, Xiaofeng Liao, Tao Xiang.

[15] A pixel based scrambling scheme for digital medical images protection by Jiankun Hu, Fengling Han.

[16.] Image encryption using random pixel permutation by chaotic mapping by G.ASathishkumar, Srinivas Ramachandran and Dr. K.Bhoopathy Bagan.