International Journal of Information & Computation Technology.
ISSN 0974-2239 Volume 4, Number 7 (2014), pp. 741-746

http://www. irphouse.com

A New Algorithm of Encryption and Decryption of Images Using Chaotic Mapping

[1]Mayank Mishra, [2]Prashant Singh, [3]Chinmay Garg

[1, 2] Project Engineer, [3]Technical Officer
[1, 2, 3]Centre for Development of Advanced Computing, Noida, India

Abstract

In this paper a novel image encryption algorithm is proposed based on combination of pixel shuffling and three chaotic maps. This algorithm is based on pixel scrambling where in the randomness of the chaos is utilized to scramble the position of the data. Shuffling is used to expand diffusion in the image and dissipate the high correlation among image pixels. Due to sensitivity to initial conditions, chaotic maps have a good potential for designing dynamic permutation map. In the proposed algorithm, the plain-image is first decomposed into 8x8 size blocks and then the block based shuffling of image is carried out. After that the shuffled image is encrypted using chaotic sequence generated by one another chaotic map. In order to evaluate performance, the proposed algorithm was measured through a series of tests. Experimental results illustrate that the scheme is highly key sensitive and shows a good resistance against brute-force and statistical attacks.

Keywords—Image encryption, chaotic maps, image shuffling, logistic map, transposition technique.

1. INTRODUCTION

Internet has evolved rapidly and thus the amount of data present on the internet is growing exponentially. The data shared in the form of text, images and other form may contain highly sensitive and confidential information. This gives an opportunity to attackers to exploit the information available at such ease. This has created a dire need for secure image transmission in public networks like internet. Internet is a public network and is not so secure for the transmission of confidential images. To meet this challenge, cryptographic techniques need to be applied. Cryptography is a tool for secure communication in presence of adversaries.

The common method of protecting the digital documents is to scramble the content so that the true message of the documents is unknown. There are various techniques to achieve this for example compression, digital watermarking, steganography and cryptography. In this paper we focus on chaos based methods used for image Encryption. Chaos refers to randomness and it is defined as a study of nonlinear dynamic system. The characteristics of chaos systems are characterized mainly sensitivities to initial conditions and other system parameters. Due to this sensitiveness, the system acts very randomly. The main advantages of the chaotic encryption approach include: high flexibility in the encryption system design, availability of huge number of variants of chaotic systems, large, complex and numerous possible encryption keys and simpler design. This promises to provide strong encryption without compromising the usability system in terms of speed and robustness.

The properties of chaotic systems are [1]:

- Chaos based encryption is deterministic, they have some determining mathematical equations ruling their behavior.
- They are unpredictable and non-linear, sensitive to initial conditions and even a very slight change in the starting point can lead to significant different outcomes.
- They appear to be random and disorganized but actually they're not. Beneath the random behavior there is a sense of order and pattern.

The highly unpredictable and random–look nature of chaotic output is the most attractive feature of deterministic chaotic system that may lead to various novel applications [2]

The organization of the paper is as follow. In Section 2, we discuss the methodology of proposed chaos based scheme. The performances and analysis of the proposed image encryption scheme are studied in Section 3. Finally, conclusion remarks are drawn in Section 4.

2. METHODOLOGY

In this section, we describe all the steps for encryption and decryption of the image using both chaotic logistic maps. Complete process is described in the following steps:

The encryption process uses an 80 bit external secret key, the key is divided into blocks of 8-bit each, called session keys. Session keys referred as:

$K = k1k2…..k20$ (in hexadecimal), (1)

Here, ki's are alphanumeric characters. Thus, each group of two alphanumeric characters represents a session key.

We use following two logistic maps for encryption [12]

$Xn+1 = 3.9999Xn (1-Xn)$, (2)

$Yn+1 = 3.9999Yn (1-Yn)$, (3)

Using these logistic maps initial conditions for each logistic map, namely (X0 and Y0) are calculated.

X0 is calculated using X01 and X02 where:

X01 is binary representation of three blocks of session keys e.g. K4K5K6. Thus,

$X01 = (K41 \times 2^0 + K_{42} \times 2^1 + \ldots. + K_{61} \times 2^{16} + K_{62} \times 2^{17} + \ldots.$
$+ K_{68} \times 2^{23}) / 2^{24}$ (4)

$X_{02} = ((k_{13})_{10} + (k_{14})_{10} + (k_{15})_{10} + \ldots + (k_{18})_{10}) / 96$ (5)

Here k_i's are parts of secret key in hexadecimal mode as explained in equation 1.

Now initial condition X_0 is calculated as:

$X_0 = (X_{01} + X_{02}) \bmod 1.$ (6)

Similarly, we calculate the initial condition Y_0 for the second logistic map,

$Y_{01} = (B_2)_{10}/2^{24}$ (9)

Where B is the binary string of session keys. And

$Y02 = (B_2[P_1] \times 2^0 + B_2[P_2] \times 2^1 + B_2[P_3] \times 2^2 + \ldots\ldots\ldots..$
$+ B_2[P_{24}] \times 2^{23)} / 2^{24}$ (10)

And $Y_0 = (Y_{01} + Y_{02}) \bmod 1.$ (11)

Next step is to read three consecutive bytes, these three bytes represent the values of red, green and blue (RGB) color respectively. Then we perform encryption on first 16 bits of the image using the following formula:

$((R)_{10} + (K_4)_{10} + (K_5)_{10}) \bmod 256, ((G)_{10} + (K_5)_{10} + (K_6)_{10})$
$\bmod 256, ((B)_{10} + (K_6)_{10} + (K_4)_{10}) \bmod 256$ (12)

After encryption of the 16 bit block, we modify the session key using the formula:

$(K_i)_{10} = ((K_i)_{10} + (K_{10})_{10}) \bmod 256,$
$(1 \leq i \leq 9).$ (14)

3. SECURITY ANALYSIS

3.1 Sensitivity Analysis

The most prominent feature of chaos based encryption is its sensitivity to initial parameters. Therefore, the ideal image encryption should be very sensitive with respect to the secret key i.e. the secret key should produce a completely different encryption even if its single bit is altered. Figure 2 is the encrypted image obtained using secret key 'A3BB39C4D9E3F2BCD6E1' whereas Figure 3 is obtained using 'B3BB39C4D9E3F2BCD6E1'. The difference in images is clearly visible but we calculated the correlation coefficients to test the difference in images and found that there is absolutely no correlation between the encrypted images.

Figure 1: Original Image

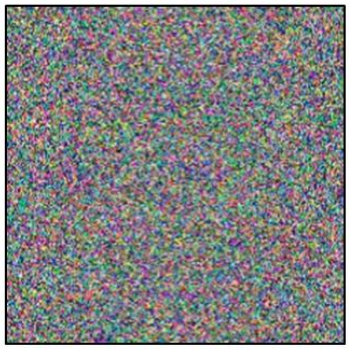

Figure 2: Encrypted Image 1

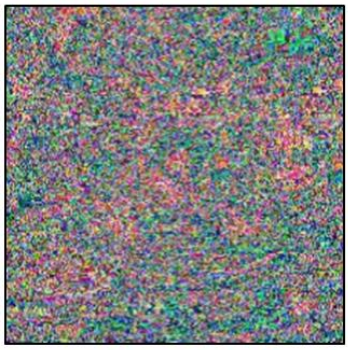

Figure 3: Encrypted Image 2

3.2 Key Space Analysis

Since this encryption technique depends heavily on the secret key, therefore we have to ensure that the key is secure and that the key space should be large enough to make the brute force attack infeasible. Since, we have used an 80 bit key, the total number of possible combinations for secret key are 2^{80} making it fairly difficult to crack by using brute force. A larger key can be used but the trade-off will be in terms of computational complexity.

3.3 Time Analysis

Chaos based encryption enables secure and fast mode of communication. We tested the above algorithm on a system running on Core 2 duo processor with 1 GB RAM. The average encryption and decryption times are shared in table 1:

Table 1

Image Size	Encryption/ Decryption time(s)
512 x 512	0.13 – 0.15
1024 x 1024	1.41 – 1.44
2048 x 2048	6.35 – 6.39

4. CONCLUSION

In this communication, a new way of image encryption scheme have been proposed which utilizes two chaotic logistic maps and an external key of 80-bit. The initial conditions for both the logistic maps are derived using the external secret key by providing weightage to its bits corresponding to their position in the key. In the

proposed encryption process, eight different types of operations are used to encrypt the pixels of an image and which operation will be used for a particular pixel is decided by the outcome of the logistic map. To make the cipher more robust against any attack, the secret key is modified after encrypting a block of sixteen pixels of the image. We have carried out statistical analysis, key sensitivity analysis and key space analysis to demonstrate the security of the new image encryption procedure. Finally, we conclude with the remark that the proposed method is expected to be useful for real time image encryption and transmission applications.

5. REFERENCES

[1] N. Bourbakis, C. Alexopoulos, Picture data encryption using SCAN pattern, Pattern Recogn.

[2] Refregier, B Javidi, Optical image encryption based on input plane and fourier plane random encoding, Opt. Lett. 20 (1995)

[3] H.K.L. Chang, J.L. Liu, A linear quad tree compression scheme for image encryption, Signal Process. 10 (4) (1997)

[4] Fridrich Jiri, Symmetric ciphers based on two dimensional chaotic maps, Int. J. Bifurcat Chaos 8 (6) (1998)

[5] J. Scharinger, Fast encryption of image data using chaotic Kolmogrov flow, J. Electronic Eng 7 (2) (1998)

[6] J.C. Yen, J.I. Guo, A new image encryption algorithm and its VLSI architecture, in: Proceedings of the IEEE workshop signal processing systems, 1999,

[7] J.C. Yen, J.I. Guo, An efficient hierarchical chaotic image encryption algorithm and its VLSI realization, IEE Proc. Vis. Image Process. 147 (2000)

[8] H. Cheng, X.B. Li, Partial encryption of compressed image and videos, IEEE Trans. Signal Process. 48 (8) (2000)

[9] J.C. Yen, J.I. Guo, A new chaotic key based design for image encryption and decryption, Proceedings of the IEEE International Symposium Circuits and Systems, vol. 4, 2000

[10] Salleh, M., S. Ibrahim, and I. F. Isnin. 2002. “Ciphering Key of Chaos Image Encryption”. Proceeding of International Conference on AI and Engineering Technology. UNIMAS, Sabah, Malaysia.

[11] Jakimoski, G. and L. Kocarev. 2001. “Chaos and Cryptography: Block Encryption Ciphers Based on Chaotic Maps”. IEEE Transactions On Circuits And Systems—I: Fundamental Theory And Applications. 48(2).

[12] N.K. Pareek a, b, Vinod Patidar a, K.K. Sud Image encryption using chaotic logistic map