L. Dolendro Singh . Int. Journal of Precious Engineering Research and Application
www.ijpera.com
ISSN : 5456-2734, Vol. 1, Issue 2, Sep.2016, pp.18-22

RESEARCH ARTICLE OPEN ACCESS

Cryptanalysis of Image Encryption Scheme Based on Chaotic Tent Map

L. Dolendro Singh[1,*], Kh. Manglem Singh[1]
[1](*Department of Computer Science and Engineering, National Institute of Technology, Manipur, India)*

ABSTRACT
With the development of chaos theory, many image encryption algorithmshave been designed using the properties associated withthechaotic map. The chaotic map shows high sensitivity to initial conditions and the sequence generated using chaotic map are unpredictable making it a good choice for performing encryption operation. But, without proper encryption algorithm design, encryption scheme designed based onthechaotic map can be cryptanalyzed to reveal the plain image. In this paper, an image encryption scheme based on chaotic tent map is cryptanalyzed using chosen-plaintext. Simulation results are shown where the plain image is successfully revealed from the cipher image without using the initial key used during encryption.
Keywords C*haotic tent map, chosen-plaintext attack, cryptanalysis, cryptography, image encryption*

I. INTRODUCTION

With the advancement in information technology, sharing or digital data is just at a tip of our hand. Data are shared with ease from any geographic location to another near or distant location within a very short time. In order to safeguard the data sent across the insecure network, data a sent after ciphering them using cryptographic operation. Lately, one the most convenient technique used for encryption of image is chaotic cryptography. The properties associated withachaoticmap such as sensitive to initial conditions, unpredictability and ease of implementation in both hardware and software makes chaos-based encryption scheme a suitable choice foracryptographic operation. Various authors have used chaotic cryptography for image encryption operation [1-7]. Though chaotic map shows important properties associated withcryptography, poor design of encryption scheme using chaotic map can be cryptanalyses to compromise the security and reveal the plain data from the cipher data. Various authors have successfully cryptanalyzedchaos-based encryption schemes which were poorly designed [8-11].

In this paper, an image encryption scheme based on chaotic tent map designed by Chunhu *et al.* [12] is cryptanalyzed usingthechosen-plaintext attack. Section 2 explains the encryption scheme proposed by Chunhu *et al.* Cryptanalysis of Chunhu *et al.* is given in Section 3. Simulation results are shown in Section 4. The conclusion is given in Section 4.

II. CHUNHU ET AL. ENCRYPTION SCHEME

The encryption scheme proposed by Chunhu *et al.* uses chaotic tent map to generate a chaotic sequence. The generated chaotic sequence is XOR with pixel values obtained from the plain image to yield the cipher image. Chaotic tent is given as:

$$x_{i+1} = f(x_i, \mu) \tag{1}$$

$$f(x_i, \mu) = \begin{cases} f_L(x_i, \mu) = \mu x_i, & If\, x_i < 0.5 \\ f_R(x_i, \mu) = \mu(1 - x_i), & otherwise \end{cases} \tag{2}$$

Where,
$x_i \in [0, 1]$, for i$\geq$ 0 and initial parameter $x_0$is used as key.
μ: Control parameter. Value ranged from $[0, 2]$.

In Chunhu *et al.* encryption scheme the precision of x_0 and μ is taken as 10^{-16} providing a key space of2^{106}.

1.1 Chunhu *et al.* encryption algorithm

1) Import the plain image and get the image dimension $m \times n$ and number of color channel c.
2) Initialize control parameter μ and input secret encryption keyx_0. Iterate chaotic map for N rounds, where $N = m \times n \times c$ to get the key

arrayx_n, n = N.Convert $x_n$to byte value by multiplying with 10^{16} and taking the floor value after performing modulo operation with 256.

3) Perform XOR operation between the pixel values of plain image *PI* and the key array x_n to get the cipher image *CI*.

$$CI = PI \oplus x_n \quad (3)$$

Flowchart for encryption algorithm is given in Fig. 1.

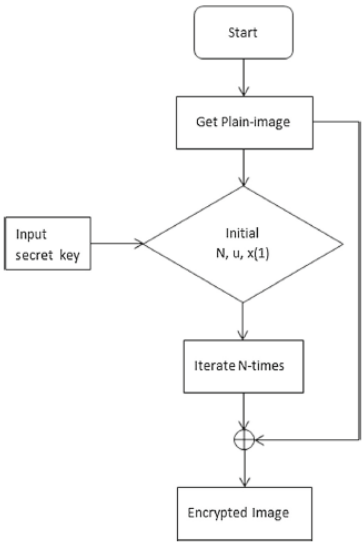

Fig.1 Flowchart for Chunhu *et al.* encryption algorithm[1]

1.2 Chunhu *et al.* decryption algorithm

1) Import the cipher image *CI*and get the image dimension $m \times n$ and number of color channel c.
2) Initialize control parameter μ and input secret decryption keyx_0 same as the one used during encryption. Iterate chaotic map for N rounds, where $N = m \times n \times c$ to get the key arrayx_n, n = N.Convert $x_n$to byte value by multiplying with 10^{16} and taking the floor value after performing modulo operation with 256.
3) Perform XOR operation between the pixel values of cipher image *CI* and the key array x_n to get the plain image *PI*.

$$PI = CI \oplus x_n \quad (4)$$

Flowchart for decryption algorithm is given in Fig. 2.

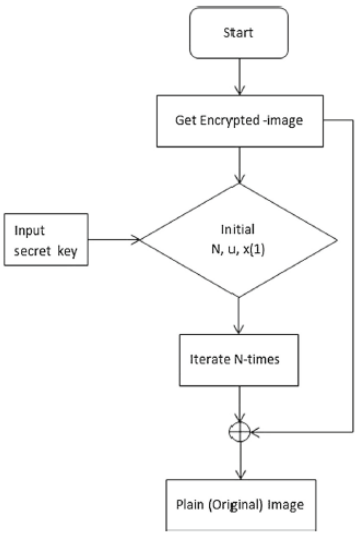

Fig.2 Flowchart for Chunhu *et al.* decryption algorithm[1]

III. CRYPTANALYSIS OF CHUNHU*EL AL.*ENCRYPTION SCHEME

Cryptanalysis of Chunhu's *et al.* encryption scheme is performed usingthechosen-plaintext attack. According to Kerckhoffs's principle [13], the encryption system is known to all. The security of the encryption system lies with the key or keys used. Inachosen-plaintext attack, the attacker can somehow get a copy of cipher text for a plaintext of his choice. In the cryptanalysis performed in this paper, an image of attacker's choice is given as input and the corresponding cipher image is obtained. Suppose the attacker use a totally black image with pixel values as all 0 (zero). On performing XOR operation between the secret array x_n and pixel values 0(zero), the resulting cipher image pixel values will consist of the secret arrayx_n. Though the attacker has no information of the initial key used, the values obtained after chosen-plaintext attack can be used to reveal other plain images from cipher images generated using Chunhu *et al.*encryption scheme by performing XOR operation withx_n.

3.1 Steps for cryptanalysis

1) Take an image with pixel values as all 0(zero).
2) Get the corresponding cipher image using chosen-plaintext attack and collect the pixel valuesx_n.
3) Get a cipher image *CI* encrypted using Chunhu *et al.* encryption scheme.
4) Perform XOR operation between *CI* and x_n obtained in Step 2 to reveal the corresponding plain image from cipher image obtained in Step 3.

IV. SIMULATION

The simulation was performed on a core i7 2.20 GHz laptop using Mathematica version 10. The sample images are obtained from a freely available database [14]. The simulation was performed with multiple images. Few of them are shown in this paper. Let $\mu = 1.8044701871607653$ and $x_0 = 0.0484348873272233$ be the keys used to encrypt two plain images as shown in Figs. 1a, 1b and 1c of which Fig 1a is known to the attacker. Figs 1d, 1e and 1f are the corresponding cipher images generated using Chunhu *et al.* encryption scheme for Figs 1a, 1b and 1c respectively.

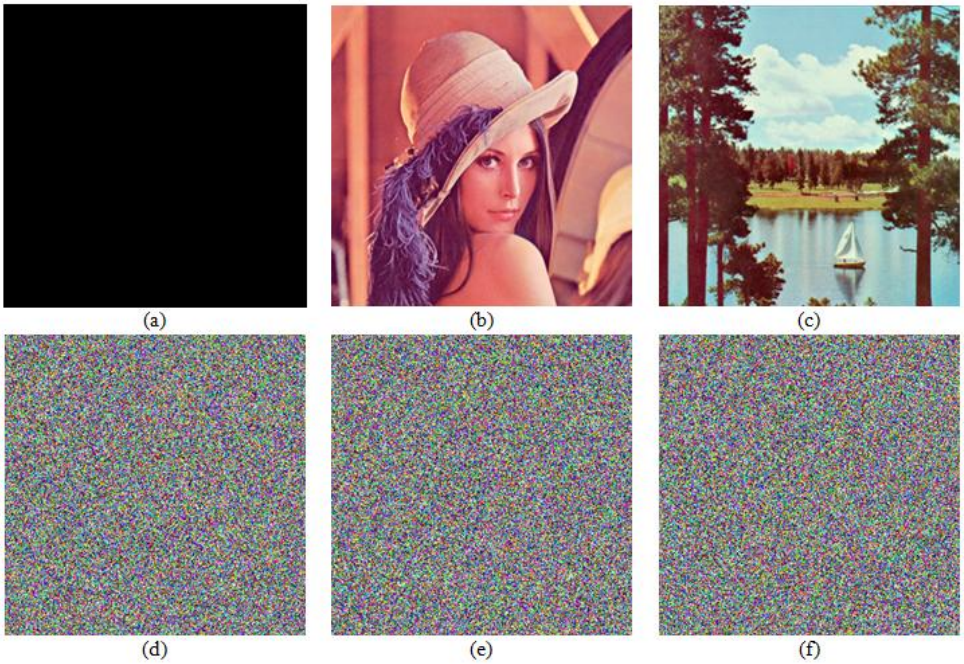

Figure 1. (a) Attacker chosen plain image (b) Plain image Lena (c) Plain image lake (c) Cipher image attacker chosen plain image (d) Cipher Lena (e) Cipher image lake

The pixels value in Fig. 1(a) is exactly the same as secret arrayx_n. Once the secret arrayx_n is obtained, cipher images are given as input and cryptanalyzed to get their corresponding plain images. The cipher image given in Fig 1(e) and 1(f) arecryptanalyzed to reveal the corresponding plain images using the following operations. The pixel values of the cipher image in 1(d) and 1(f) and secret array$x_n$obtained from chosen-plaintext attack is operated with XOR operation. The resulting matrix value is represented as an image and shown in Fig. 2(a) and 2(b) respectively. From fig 2(a) and 2(b), we can see that the exact plain image can be revealed.

Fig. 2. (a) Successfully cryptanalyzed Lena image (b) Successfully cryptanalyzed Lake image.

V. CONCLUSION

The paper successfully cryptanalyze the encryption scheme proposed by Chunhu *et al.*using thechosen-plaintext attack. Simulation results show that the exact plain image can be successfully revealed without using the initial secret key. The necessity fortheinitial secret key is compromised through achosen-plaintext attack from which the secret array key is obtained which can be used to cryptanalyze cipher images encrypted using Chunhu *et al.* encryption scheme.

REFERENCES

[1] L. Wenhao, S. Kehui andZ. Congxu, A fast image encryption algorithm based on chaotic map, *Optics and Lasers in Engineering,84* (2016) 26-36.

[2] W. Xingyuan, Z. Jianfeng andL. Hongjun, A new image encryption algorithm based on chaos, *Optics Communications*, (2012) *285 (5)* 562-566.

[3] C. Zhu, A novel image encryption scheme based on improved hyperchaotic sequences, *Optics Communications*, (2012) *285* 29-37.

[4] Wang X, Teng L & Qin X, A novel color image encryption algorithm based on chaos, *Signal Processing*, (2012) *92(4)* 1101-1108.

[5] Eslami Z & Bakhshandeh A, An improvement over an image encryption method based on total shuffling, *Optics Communications*, (2013) *286* 51--55.

[6] Dai Y, Wang H & Wang Y, Chaotic Medical Image Encryption Algorithm Based on Bit-Plane Decomposition, *International Journal of Pattern Recognition and Artificial Intelligence*, (2016) *30(4)* 1657001-1657015.

[7] Qzkaynak F, QzerA B, Cryptanalysis of a new image encryption algorithm based on chaos, *Optik - International Journal for Light and Electron Optics*, (2016) *127(13)* 5190-5192.

[8] Ozkaynak F, Ozer A B & Yavuz S, Cryptanalysis of a novel image encryption scheme based on improved hyperchaotic sequences, *Optics Communications*, (2012)*285* 4946-4948.

[9] Tu G, Liao X & Xiang T, Cryptanalysis of a color image encryption algorithm based on chaos, *Optik*, (2013) *124* 5411-5415.

[10] Akhavan A, Samsudin A & Akhshani A, Cryptanalysis of "an improvement over an image encryption method based on total shuffling", *Optics Communications*, (2015) *350* 77-82.

[11] Bechikh R, Hermassi H, Ahmed A A E, Rhouma R & Belghith S, Breaking an image encryption scheme based on a spatiotemporal chaotic system, *Signal Processing: Image Communication*, (2015) *39* 151-158.

[12] L. Chunhu, L. Guangchun, Q.Ke and L. Chunbao, An image encryption scheme based on chaotic tent map, *Nonlinear Dynamics*, DOI 10.1007/s11071-016-3030-8

[13] Kerckhoffs A, La cryptographiemilitaire, *Journal des sciences militaires*, (1883) *9* 5-38.

[14] Sample Images,http://sipi.usc.edu/database/