Image Encryption using RCES/RSES Scheme

Madhusmita Sahoo[1], Sabita Pal [2], Rina Mahakud [3]
Faculty of Electronics & Communication Engg. Department, Siksha 'O'Anusandan University, India[1,2]
Faculty of Electronics & Tele Communication Engg. Department, Biju pattnaik University of Technology, India[3]

ABSTRACT

Today the demand for secure transfers of digital images , cryptanalysis and network security is a growing field. In this paper the security of RCES is analyzed and observed that it is insecure against the known/chosen-plaintext attacks .Here two seeds are generated chaotically and XOR'ed with plain image to get cipher image . The security of RCES against the brute-force attack was overestimated.

Keywords— Cryptanalysis RCES, chosen-plaintext attacks, seeds, brute-force attack

1. INTRODUCTION

With the advancement of modern technology in field of communication, its security is of greater concern. Security is required in wireless medium during transmission and storage of digital images preventing it from being hacked. It is applicable in various fields like military, medical imaging, confidential video conferencing etc. To achieve this, codes are generated to achieve confidentiality, integrity and availability. confidentiality allows only authorized person to read the information, preventing unauthorized access. Integrity allows only authorized person to write the information. Availability makes the data available to the authorized person in a timely manner whenever required. These three factors are important for encryption to protect personal privacy.

Cryptanalysis provides the means to encrypt the message. It identifies the program used to hide message, the location of the program signature in the file, the location of the password in the file, location of the hidden message in the file and the algorithm used to encrypt the hidden message. RSES(random seed encryption system) was proposed by Chen et al .(2002) and Chen and Yen (2003)and renamed as RCES(random control encryption system). It is a chaos based image encryption scheme. It is advanced version of CKBA(Chaotic key based algorithm).RCES scheme[1],[2],[3] uses position scrambling and value changing of pixels.

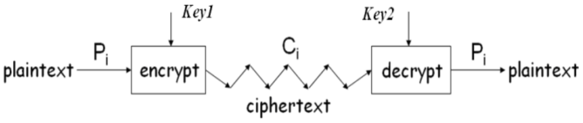
The organization of the paper is as follows: Section 2 - System overview that gives a general idea about the overall functioning of the system. Section 3 Experimental results .and Section 4 concludes the paper.

2. SYSTEM OVERVIEW

A. INTRODUCTION TO CRYPTANALYSIS :

The encryption process is carried out by cryptology. Cryptology is the art and science of making and breaking secret codes. . It consists of mainly two parts, cryptography and cryptanalysis. Cryptography deals with the making of secret codes by designing encryption algorithms while cryptanalysis deals with breaking of those secret codes to find security weakness of the algorithm. All these together form a cryptosystem or a cipher.

A cipher or cryptosystem is used to encrypt the plaintext. The result of encryption is the cipher text. We decrypt cipher text to recover plaintext. A key is used to configure cryptosystem. A symmetric key cryptosystem uses the same key to encrypt as to decrypt. A public key cryptosystem uses a public key to encrypt and a private key to decrypt.



P_i is ith "unit" of plaintext & C_i is corresponding cipher text . Here Key1 is the encryption key and key2 is the decryption key. If key1=key2 then the cipher is known as private key cipher (symmetric cipher)and the keys are transmitted from through a secret channel from transmitter to receiver side. If key1 and key2 are not equal then the cipher is known as public key cipher (asymmetric cipher), here the encryption key is public but the decryption key is private.

B. CKBA:

Here a plain image of size MXN is taken and the encryption algorithm follows following steps:

Generation of secret keys:

Secret keys such as key1 and key2 are generated chaotically using the equation x(n+1)= µ.x(n).(1-x(n)) and the initial condition is x(o)∈(0,1). According to Chaos theory the expression behaves chaotically if µ>3.5699.[1],[5],[7]

Initialization:

A chaotic sequence x(i) is generated where i = 0to(MN/8)-1. From x(i) a pseudorandom binary sequence(PRBS) b(i) is generated, where x(i) = 1.b(16i+1).b(16i+2)……….b(16i+16)

Encryption:

Let I(x,y) is the plain image ,whose size is MXN (0≤ x≤M-1) and (0≤ y≤N-1).

$$B(x,y) = 2 \times b(x \times N + y) + b(x \times N + y + 1)$$

$\otimes and \Theta$ represents EXOR and EXNOR operation respectively.

Then encrypted image (cipher image) is E(x,y) and defined as

$$E(x,y)=\begin{cases} I(x,y)\otimes key1, B(x,y)=3 \\ I(x,y)\Theta key1, B(x,y)=2 \\ I(x,y)\otimes key2, B(x,y)=1 \\ I(x,y)\Theta key2, B(x,y)=0 \end{cases}$$

This expression can also be rewritten as

$$E(x,y)=\begin{cases} I(x,y)\otimes key1, B(x,y)=3 \\ I(x,y)\otimes \overline{key1}, B(x,y)=2 \\ I(x,y)\otimes key2, B(x,y)=1 \\ I(x,y)\otimes \overline{key2}, B(x,y)=0 \end{cases}$$

Decryption:

Decryption process is reverse operation of encryption and is defined as

$$I(x,y)=\begin{cases} E(x,y)\otimes key1, B(x,y)=3 \\ E(x,y)\otimes \overline{key1}, B(x,y)=2 \\ E(x,y)\otimes key2, B(x,y)=1 \\ E(x,y)\otimes \overline{key2}, B(x,y)=0 \end{cases}$$

***Limitation of CKBA** :*

- Insecure against the known/chosen-plaintext attacks., Because equivalent key(mask image) i.e I_m can be generated by EXORing the plain image I(x,y) with the cipher image E(x,y).

- It is overestimated against Brute-force attack
- Secret key can be generated from mask image

C. RSES

RCES [1],[2],[3] is an enhanced version of CKBA, key1 and key2 are made time-variant, by introducing a simple permutation operation, Swapb(x_1, x_2), which exchanges the values of x_1 and x_2 if b = 1 and does nothing if b = 0.

RCES encrypts plain-images block by block, where each block contains 16 consecutive pixels. To simplify the following description, without loss of generality, assume that the sizes of plain-images are all M × N, and that MN can be divided by 16. Consider a plain-image , a 1-D pixel-sequence by scanning it line by line from bottom to top. The plain-image can be divided into MN/16 blocks:

{$I^{(16)(}1)$, · · · , $I^{(16)}(k)$, · · · , $I^{(16)}$(MN/16)},Where

$I^{(16)}(k)$ = {I(16k + 1), · · · , I(16k + i), · · · , I(16k + 16)} .

For the k-th pixel-block $I^{(16)}(k)$, the work mechanism of RCES is described below-

Generation of secret keys:

Secret keys such as key1 and key2 are generated chaotically using the equation x(n+1)= µ.x(n).(1-x(n)) and the initial condition is x(o)∈(0,1). According to Chaos theory the expression behaves chaotically if µ>3.5699.

Initialization:

A chaotic sequence x(i) is generated where i = 0to(MN/16)-1. From x(i) a pseudorandom binary sequence(PRBS) b(i) is generated, Here the Logistic map is realized in 24-bit fixed-point arithmetic.

Encryption:

Two pseudorandom seeds are generated

$$Seed1(k)=\sum_{i=0}^{7} b(24k+i)\times 2^{7-i}$$

$$seed2(k)=\sum_{i=0}^{7} b(24k+8+i)\times 2^{7-i}$$

Pseudorandom swapping is carried out for adjacent pixels i=0 to 7.

$$Swap_{b(24k+16+i)}(I(16k+2i), I(16k+2i+1))$$

The current plain block of image is masked using two pseudorandom seeds , for i = 0 to 15.

$$I(16k+j)=I(16k+j)\otimes seed(16k+j)$$

Where

$$seed(16k+j)=\begin{cases} seed1(k), B(k,j)=3, \\ \overline{seed1(k)}, B(k,j)=2, \\ seed2(k), B(k,j)=1, \\ \overline{seed2(k)}, B(k,j)=0 \end{cases}$$

And $B(K,j)=2\times b(24k+j)+b(24k+j+1)$

Decryption:

The decryption procedure is similar to the encryption procedure, but the masking operation is exerted before the swapping for each pixel-block.

3. EXPERIMENTAL RESULTS AND ANALYSIS:

Here statistical analysis is carried out by taking the histogram and GLCM of original and encrypted image.

Gray Level Co occurrence matrices

The cooccurrence matrix introduced by Haralick et al., originally called gray-tone spatial dependency matrices, and define textural properties of images. The cooccurrence matrix also known as Gray Level Cooccurrence Matrix (GLCM) is a directional histogram constructed by counting the occurrence of pairs of pixels separated by some vector displacements.

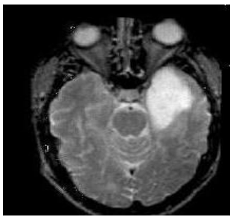
Let *I* be an image whose pixel grey levels are in the range 0,…., *L*-1. Let take an integer valued displacement vector $\overline{d}=(p,q)$, specifies the relative position of the pixels at coordinates (x,y) and $(x+p,y+q)$. A GLCM is a $L \times L$ matrix whose (i, j) element is the number of pairs of pixels of *I* in relative position $\bar{d}$ such that the first pixel has gray level *i* and the second pixel has gray level *j*. So the GLCM matrix M involves counts of pairs of neighbouring pixels. Then M is form for each of four quantized directions 0, 45, 90, and 135. So GLCM matrix can be represented as $\mathrm{M}(p,q)$ or $\mathrm{M}(\bar{d},\theta)$, where $\bar{d}$ refers to displacement distance and θ refers to particular angle. There are simple relationships exist among certain pairs of the estimated GLCM $\mathrm{M}(\bar{d},\theta)$.

Let $\mathrm{M}^T(\bar{d},\theta)$ denote the transpose of matrix $\mathrm{M}(\bar{d},\theta)$. Then

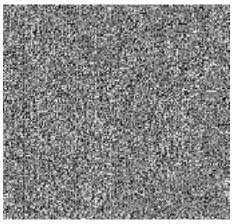
$$\mathrm{M}(\bar{d},0^0) = \mathrm{M}^T(\bar{d},180^0)$$
$$\mathrm{M}(\bar{d},45^0) = \mathrm{M}^T(\bar{d},225^0)$$
$$\mathrm{M}(\bar{d},90^0) = \mathrm{M}^T(\bar{d},270^0)$$

Thus

$\mathrm{M}(\bar{d},180^0)$, $\mathrm{M}(\bar{d},225^0)$, $\mathrm{M}(\bar{d},270^0)$, and $\mathrm{M}(\bar{d},315^0)$ adds nothing to the specification of the texture.



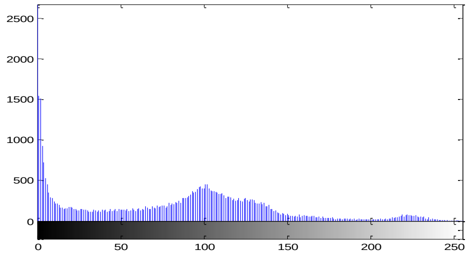
(plain image)



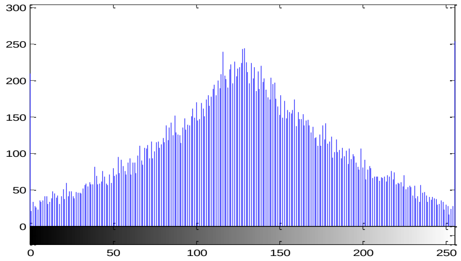
(Encrypted image)

(Decrypted image)

Fig(1) (Encrypted and Decrypted images of a brain)



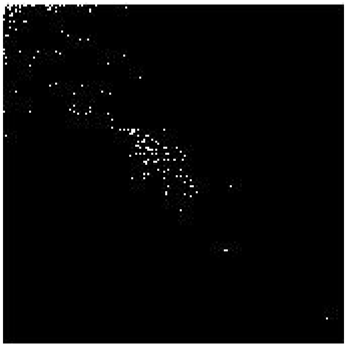
(histogram of plain image)



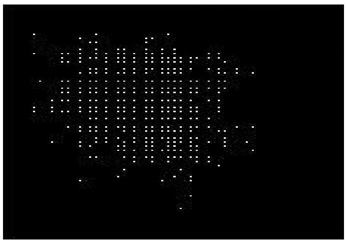
(histogram of cipher image)

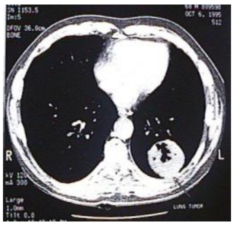
Fig2 (Histogram of plain image and cipher image of brain)

(GLCM of plain image)

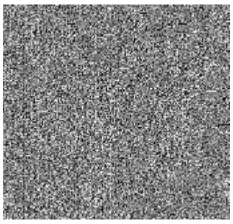


(GLCM of cipher image)

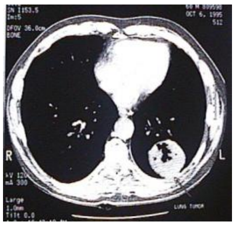




(plain image)

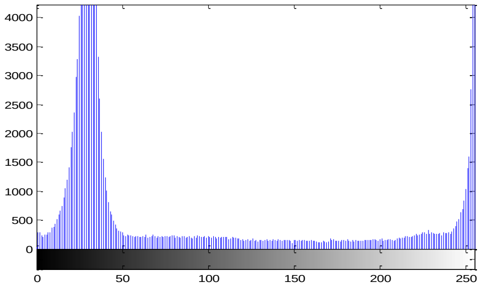


(Encrypted image)

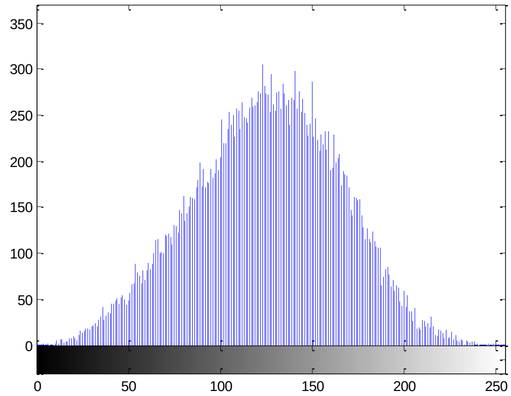


(Decrypted image)

Fig(3)((Encrypted and Decrypted images of lungs)



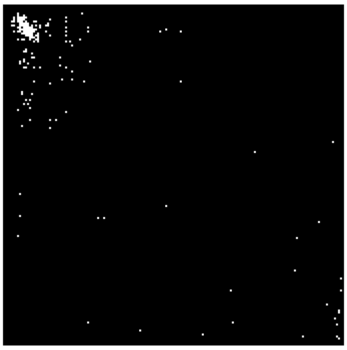
(histogram of plain image)

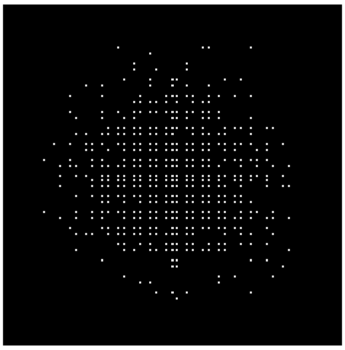


(histogram of cipher image)

Fig4 (Histogram of plain image and cipher image of lungs)

(GLCM of plain image)





(GLCM of cipher image)

The algorithm is simulated by MATLAB R2007b and the histogram shows the statistical analysis. As the histogram of the cipher image is totally different from the plain image , the attackers can’t able to hack the original image .That means the cipher image has no statistical similarity with plain image . Thus the cipher image is robust against any statistical attack. The GLCM of plain image and cipher is different which shows the texture of both the images are totally different.

4. CONCLUSION

This paper has introduced a efficient method for encrypting images. The encryption method involves five steps in the process: key generation , initialization ,seed calculation , encryption using seed values through XOR process. It can be decrypted using the reverse operation . The statistical similarity comparisons carried out by taking the histogram and it is found that cipher image and plain image are statistically different. By taking GLCM matrix texture analysis of plain image and cipher image can also be found out. GLCM matrix of the plain image and encrypted image will be different. Thus we conclude that the statistical analysis of both the images is independent.

5. REFERENCES

[1] S. Li, C. Li, G. Chen, and X. Mou, “Cryptanalysis of the RCES/RSES image encryption scheme,” 2008.

[2] C. Li and G. Chen, “On the security of a class of image encryption schemes,” Proceedings of the IEEE International Symposium on Circuits and Systems, 2008

[3] Cryptanalysis of the RCES/RSES image encryption scheme. Shujun Li, Chengqing Li, Guanrong Chen ,

Kwok-Tung Lo. The Journal of Systems and Software 81 (2008) 1130–1143.(ScienceDirect)

[4] C. Chang, M. Hwang, and T. Chen, "A New Encryption Algorithm for Image Cryptosystem," The Journal of Systems and Software , vol. 58, pp. 83–91, 2001.

[5] S. Li and X. Zheng, ―Cryptanalysis of a chaotic image encryption method,‖ in Proc. IEEE Int. Symp. Circuits and Systems (ISCAS'2002) , Arizona, vol. 2, 2002, pp. 708–711.

[6] S. Lian, J. Sun, and Z. Wang, "Security analysis of a chaos-based image encryption algorithm," Phys. Lett. A 351, pp. 645-661, 2005.

[7] Pareek NK, Patidar V, Sud KK. Image encryption using chaotic logistic map. Image Vision Comput 2006;24:926–34

[8] Gao Haojiang, Zhang Yisheng, Liang Shuyun, Li Dequn. A new chaotic algorithm for image encryption. Chaos Soliton Fract 2006;29(2):393–9.