International Journal of Image Processing and Vision Science

Volume 1 | Issue 4 Article 5

October 2012

# CHAOTIC IMAGE ENCRYPTION USING-RC5

DHANYA B. NAIR
*Dept of Electronics & Communication Engg, Ilahia College of Engineering and Technology, Muvattupuzha, Kerala, India*, dbndhanya@gmail.com

RUKSANA MAIDEEN
*Dept of Electronics & Communication Engg, Ilahia College of Engineering and Technology, Muvattupuzha, Kerala, India*, ruksana.m@gmail.com

# CHAOTIC IMAGE ENCRYPTION USING-RC5

**DHANYA B.NAIR[1] & RUKSANA MAIDEEN[2]**

[1,2]Dept of Electronics & Communication Engg, Ilahia College of Engineering and Technology, Muvattupuzha, Kerala, India
Email: dbndhanya@gmail.com

**Abstract:-**In order to protect valuable data from undesirable readers or against illegal reproduction and modifications, there have been various data encryption techniques. Many methods have been developed to perform image encryption. The use of chaotic map for image encryption is very effective, since it increase the security, due to its random behavior. The highly unpredictable and random-look nature of chaotic signals is the most attractive feature of deterministic chaotic systems that may lead to novel (engineering) applications. This paper introduces a new cascaded structure of chaotic encryption scheme with RC-5 algorithm. In this paper 'Triple key' is used to encrypt and decrypt the data. Three different parameters which are decided by user are used to scramble the image data and so hackers get many difficulties to hack the data hence providing more security. Cascading RC-5 with triple key chaotic image encryption increases the security and the histogram can be made more uniform. For simulation MATLAB software is used. The experimental results shows that algorithm successfully perform the cryptography and highly sensitive to the small changes in key parameters.

**Keywords—** image encryption; chaotic neural network; chaotic logistic map; RC5.

## I. INTRODUCTION

Recently, with the great demand in digital signal transmission and the big losses from illegal data access, data security has become a critical and imperative issue in the multimedia data transmission applications. In order to protect valuable data from undesirable readers or against illegal reproduction and modifications, there have been various data encryption techniques. The data encryption techniques make the images invisible to undesirable readers and can be applied to protect the frames in the digital versatile disk (DVD) and the cable TV.

Cryptography is exchanging the information between the related persons without leakage of information by unauthorized one. For this secure transmission or communication, data is encrypted at transmitter and decrypted at receiver. The encryption is obtained by scrambling the phase spectrum of original one, reverse process is used for decryption. If the same key is used at both for encryption and decryption then it is called as secret or symmetric cryptography and if different key is used then called public cryptography.

In the 'Triple Key Image Encryption' [1], both position permutation and value transformation is performed. It has the potential of high data security. Here we are using three keys for encryption and decryption .In the proposed method we are combining this triple key method with RC-5 algorithm to increase the security, without affecting the quality of encryption. So in the proposed method we have four keys: three of chaotic method and one of the RC-5. Since the number of keys is increased the security also increases.

The features that make chaotic logistic maps and RC5 desirable for image encryption have been described in the following section. Then, the algorithm of the "Chaotic Image Encryption using RC5" is elaborated. The observations and results of this image encryption method are provided next.

## II. FEATURES OF CHAOTIC LOGISTIC MAPS

Chaos theory is a scientific discipline that focuses on the study of nonlinear systems that are highly sensitive to initial conditions that is similar to random behavior, and continuous system. The properties of chaotic systems are [2]: (i) Deterministic, this means that they have some determining mathematical equations ruling their behavior. (ii) Unpredictable and non-linear, this means they are sensitive to initial conditions. Even a very slight change in the starting point can lead to significant different outcomes. (iii) Appear to be random and disorderly but in actual fact they are not. Beneath the random behavior there is a sense of order and pattern.

A simple 1D map that exhibits complicated behavior is the logistic map [0,1] [0,1], parameterized by μ:

$$X_{i} = \mu * X_{i-1} (1-X_{i-1})$$

In the logistic map, as μ is varied from 0 to 4, a period doubling bifurcation occurs. In the region μ Ɛ [0, 3], the map possesses one stable fixed point. As μ is increased past 3, the stable fixed point becomes unstable and two new stable periodic points of period 2 are created. As μ is further increased, these stable periodic points in turn become unstable and each spawns two new stable periodic points of period 4.

Thus the period of the stable periodic points is doubled at each bifurcation point. Moreover, at a finite μ, the period doubling episode converges to an infinite number of period doublings at which point chaos is observed. This is depicted in the bifurcation

diagram in Fig. 1. The extreme amount of confusion can be seen to pervade at the end of the spectrum.

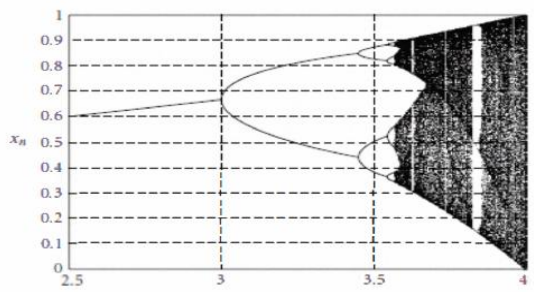


**Figure 1.Bifurcation diagram of one-dimensional logistic map**

## III. FEATURES OF RC5

The RC5 encryption algorithm [3] is a block cipher that converts input data blocks of 16, 32, and 64 bits into cipher text blocks of the same length [8-10]. It uses a key of selectable length b (0, 1, 2, ..., 255) byte. The algorithm is organized as a set of iterations called rounds r that takes values in the range (0, 1, 2, ..., 255)

An expanded key array is created out from the original key by means of a key schedule. The expanded key array is used with both encryption/decryption routines and its length is dependent on the number of rounds. The operations performed on the data blocks include bitwise exclusive-OR of words, data-dependent rotations by means of circular left and right rotations and two's complement addition/subtraction of words, which is modulo-2w addition/subtraction, where w is the word size in bits. They always affect a complete 16, 32 or 64-bit data block at a time. There are two inputs to the encryption function, which are the image to be encrypted and the expanded secret key.

For RC5 image encryption, the image header is extracted from the image to be encrypted and the image data stream is divided into blocks of 64-bit length. The first 64-bit block of image is entered as the plain image to the encryption function of RC5. The second input the RC5 encryption algorithm is the expanded secret key that is derived from the user-supplied secret key by the key schedule. Then, the next 64-bit plain image block follows it, and so on.
In the decryption process, the encrypted image (cipher image) is also divided into 64-bit blocks. The 64-bit cipher image is entered to RC5 decryption algorithm and the same expanded secret key is used to decrypt the cipher image but the expanded secret key is applied in a reverse manner. Then the next 64-bit cipher image block follows it, and so on

## IV.ALGORITHM

*A. Forming Binary Image*

1. Read the input image which is to be encrypted and convert it into binary image matrix $d_{nj}$.

*B. Generate the Chaotic Sequence*

2. The session key K consisting of 20 hexadecimal characters viz. 0 to 9 and A to F is entered.
$K=k_1k_2\ldots\ldots\ldots k_{20}$

3. Each hexadecimal character in the session key is converted into binary equivalent of four bits so that session key consists of 80 bits.
Let $k_1 = k_{11}\, k_{12}\, k_{13}\, k_{14}$ , $k_2 = k_{21}\, k_{22}\, k_{23}\, k_{24}$ ... ,
$k_{20} = k_{201}\, k_{202}\, k_{203}\, k_{204}$

4. The bits are extracted from the session key to create intermediate keys X01 and X02
X(1) = (X 01+X 02+X 03) mod 1.
Where, $X\,01=(k_{11}*2\text{^}0+\ldots\ldots..+k_{204}*2\text{^}79)/2\text{^}80$
$X02=(k_1+k_2+\ldots k_{20})/(16*20)$
X03= user entry key.

5. Enter control parameter μ.

6. Generate the chaotic sequence
$X(n + 1) = \mu X(n) (1 – X(n))$
The values of the chaotic sequence are normalized and are converted into binary matrix B. The number of elements in the chaotic sequence is equal to the number of pixels in the image. B is used to compute the weights and biases of the chaotic neural Network.

*C. Construction of Neural Network*

Using the elements in B ($b_{nj}$),the weight matrix(W) and bias matrix(θ) are found out
$W_{ij} = 0$ ; for $i \neq j$
And for i =j
$W_{ij} = -1$ ; if $b_{nj} = 1$
$\theta = 1/2$ ; if $b_{nj}=0$
$\theta = -1/2$ ; if $b_{nj}= 1$

$d_{nj}' = \text{sign}\,(\Sigma\, W_{ij} * d_{nj} + \theta)$

sign (x) = 1 ; x≥0 & sign (x)=0 ; x<0

Each row of $d_{nj}$' is converted to its corresponding decimal value. Now, $d_{nj}$' contains values ranging from 0 to 255. The one-dimensional array is converted to a three dimensional array which belongs to the chaotic encrypted image.

*C. RC5 Algorithm*

7. Enter the RC5 key and create an expanded key array.

8. Do RC5 Encryption, to create the final encrypted image.

*D. Decryption*

Decryption procedure is same as the encryption procedure, but takes place only when the RC5 key session key, initial parameter key and control parameter key are correctly entered.

## V. ANALYSIS

Simulation was done using MATLAB to explore the efficiency of this image encryption method. The results presented here contain both simulation diagrams and mathematical results. Simulation diagrams provide a physical feel of the encryption method, while the mathematical results provide statistical data. Simulation diagrams include 1) Encrypted Image Analysis 2) Histogram Analysis. Mathematical results are depicted using two new parameters: Correlation Index and Quality of Encryption.

From the encrypted image and histogram analysis as shown in Fig.2, it is clear that it is impossible to map encrypted image to the original image. Also the histogram of the encrypted image is more uniform compared to the input, showing better encryption .Correlation is a measure of the similarity that exists between two adjacent pixels in an image.

$$Cr = \frac{N\sum_{j=1}^{N}(xj * yj) - \sum_{j=1}^{N} xj * \sum_{j=1}^{N} yj}{\sqrt{\left(N\sum_{j=1}^{N} xj^2 - \left(\sum_{j=1}^{N} xj\right)^2\right) * \left(N\sum_{j=1}^{N} yj^2 - \left(\sum_{j=1}^{N} yj\right)^2\right)}}$$

CI refers to the correlation index, Ch the correlation between horizontally adjacent pixels and Cv the correlation between vertically adjacent pixels.

CI = Ch+Cv/2

The correlation coefficient of encrypted image is very less compared to input image and is shown in Table 1.The quality of encryption is determined from the following equation Higher the value of QoE better will be the encryption.

QoE = (1-CI) * 100%

## VI. CONCLUSION

In this paper, we have presented a new method of image encryption by cascading triple key method with RC5 .Here the system strength increases by including more secret keys and by maintaing good quality of encryption.We can conclude that proposed system is very effective ,as good security is achieved between two parties in case of secret communication.

## VII. REFERENCES


[1]. "Triple Key Method of Image Encryption": Srividya.G, Nandakumar.P IEEE Transactions On Circuits And Systems-I:

[2]. Salleh. M., S. Ibrahim and I. F. Isnin. 2002. "Ciphering Key Of Chaos Image Encryption" Proceeding of International Conference on AI and Engineering Technology.

[3]. "Implementation of RC5 Block Cipher Algorithm for Image Cryptosystems". International Journal of Information Technology Volume 3 Number 4.


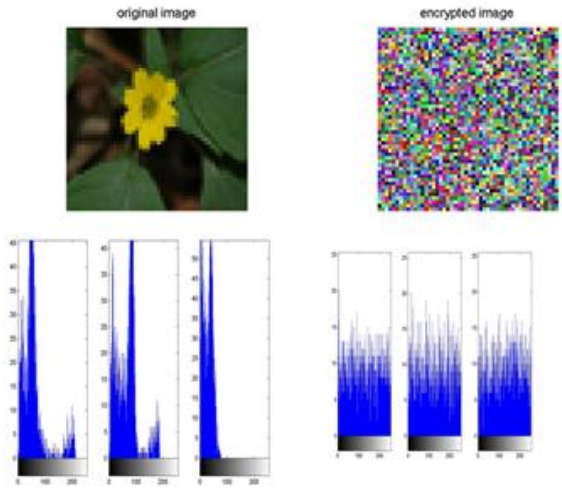


**Figure2. Encrypted Image Analysis and Histogram Analysis**

Table 1.Sensitivity to Keys

| Sl No: | Keys | | CII | CIO | QoE (%) |
|---|---|---|---|---|---|
| 1 | Session key | ABCDEF12345 | 0.5512 | 0.0285 | 97.1 |
| | Initial parameter key | 3.5 | | | |
| | Control parameter key | 3.9 | | | |
| | RC5 key | 12345 | | | |
| 2 | Session key | 1AB23C4B5CB6C7 | 0.5512 | 0.0556 | 94.4 |
| | Initial parameter key | 2.9 | | | |
| | Control parameter key | 3.81 | | | |
| | RC5 key | ZXCVBNM | | | |

◈◈◈