# Encryption Image by Using RC6 and Hybrid Chaotic Map

**Zahraa Faisal***
Assistant Lecturer, Department of Quality Assurance & Performance Evaluation, University of Kufa, AL-Najaf, Iraq. E-mail: zahraaf.shouman@uokufa.edu.iq

**Esraa H. Abdul Ameer**
Department of Computer Sciences, College of Education for Girls, Kufa University, Iraq.

*Received June 05, 2020; Accepted August 04, 2020*
*ISSN: 1735-188X*
*DOI: 10.14704/WEB/V17I2/WEB17024*

## Abstract

Cryptography is data processed in a way that becomes incomprehensible and unavailable to unauthorized persons. In this paper instructed method to encryption image by using RC6 algorithm and generated key by using hybrid chaotic map (tent and logistic map). Used some measures such as frequency test within a block, entropy, serial test (two-bit test), and frequency test (monobit test); to demonstrate the strength of the algorithm proposed in the image coding and protection. The MATLAB program was used as a work environment.

## Keywords

RC6, Tent Map, Logistic Map, Randomness Evaluation.

## Introduction and Literature Review

Wireless networks are implemented in conversation systems, wherein they can more than users to connect without physical link. Data of computer are transpose from the one device to another throughout an insecure canal. This channel may be risky to attack lead to steal the information or changed. For this reason, demand secure of the information transmitted through insecure channels [1]. Cryptography converts messages into an unreadable form with encryption algorithms. The cryptography is interested with many goals are confidentiality, integrity, availability, and authentication [2]. Cryptography is used to warranty the privacy and the reliability of data through different technologies and algorithms. Theory of chaos is the study of the stochastic behavior of systems, it is a blanketing theory that include mathematics, physics, biology, Communication, computer science etc. A chaotic system is very sensitive for initial conditions, where the simple difference in the initial condition will produce high difference in the chaotic values [3]. According to Lian, et al. (2015), the block cipher is based on the "chaotic fashionable

map", which is composed of 3elements: confusion technique rely on chaotic fashionable map, diffusion characteristic and key generator. A high-pace diffusion function is designed, and the chaotic skew tent map represents a base for the key generator[4]. According to AlZain, et al. (2017), a new virtual chaotic photo cryptosystem can be built by 'Chaotic Tent Map' (CTM). CTM has properties that are appropriate for the layout of encryption schemes. The assessment of security of CTM-based photo cryptosystem is opposite to brute-force, differential, and statistical attacks [5].

## Methods

In this section, explain encryption method:

### 1) Block Cipher

It is a group of simple textual content letters is encrypted collectively to generating a collection of cipher textual content. In a block cipher, there is a block of plaintext treated as an entire and utilized to produce cipher textual content block of identical length [2]. There are many block cipher algorithms like (DES, AES, Blowfish, RC5, CAST-128, and RC6….etc.).There are two types of cryptography; symmetric, which is simpler to put into effect in low computation devices and asymmetric which is used for cipher and decipher two exclusive keys. The key used for encryption the text is public key. Receiver has the private decryption key to obtain the original message [2].

### a) RC6 Algorithm

A block cipher is operating on fixed-length of bits called a block, it is important in the design of cryptographic protocols and implement encryption of data. RC6 is Block cipher and an evolutionary development of RC5, designed to satisfy the necessities of the Advanced Encryption Standard (AES). RC6 has an encryption algorithm; a decryption algorithm; a key growth algorithm.

$$\mathrm{RC6} - \mathrm{w/r/b}$$

Where (w) is the word size
(r) is the non-terrible quantity of rounds
(b) is the byte size of the encryption key

RC6 is primarily based on seven primitive operations as shown in table 2.1. Size of the block 128 bits, the important thing bytes are then loaded into an array L of size c word, form$(2r + 4)$ words are saved in key array S, the base of herbal logarithms $e = (2.718281828459 \ldots)$ and the golden ratio$ø = (1.618033988749 \ldots)$. Figure1 shows

RC6 encryption algorithm. Successful block coding designs often incorporate ideas of confusion and diffusion. Confusion: obscure relationship between cipher text and key such as substitution. Diffusion is a bit change spread from one block to other blocks, where a small change within the plaintext leads to most important changes inside the ciphertext such as transposition (permutation). To increasing of change between rounds, used a quadratic equation. To achieve the security goals used equation (1) twice in each round [6]:

$$F(x) \equiv x\,(2x + 1)\ \%\ 2^{w} \quad (1)$$

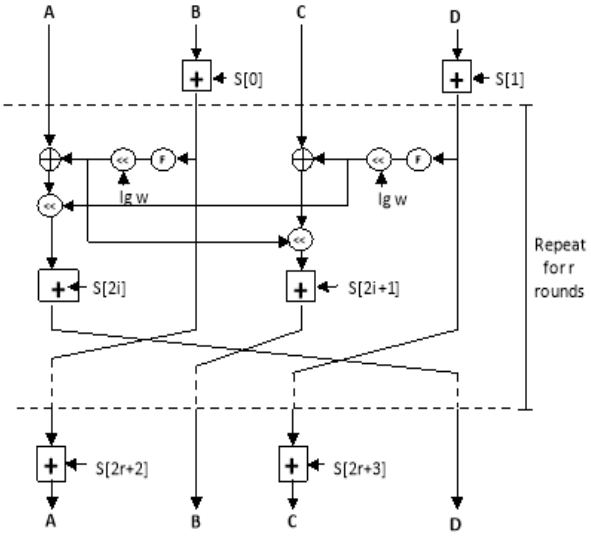



**Figure 1 RC6 Encryption Algorithm**

The table next display primitive operations of the RC6 algorithm.

| **Operation** | **Description** |
|---|---|
| $a + b$ | Integer addition modulo $2^w$ |
| $a - b$ | Integer subtraction modulo $2^w$ |
| $a \oplus b$ | Bitwise exclusive-or (XOR) of w-bit words |
| $a \times b$ | Integer multiplication modulo $2^w$ |
| $a <<< b$ | Rotate the $w$-bit (a) word a to the left by ($b=\log_2 w$) |
| $a >>> b$ | Rotate the $w$-bit (a) word a to the right by ($b=\log_2 w$) |
| **Enc**: $(A, B, C, D) = (A, B, C, D)$<br>**Dec**: $(A, B, C, D) = (D, A, B, C)$ | Parallel setting of values on the right for recordings on the left. |

## 2) Chaos

Chaos is a "a periodic long-term behaviour in a deterministic system that exhibits sensitive dependence on initial conditions" [7, 8]. Chaotic Map: Chaotic is a description that comes from the name "Chaos," concept complete and total confusion or lack of order. Chaos theories had been extensively studied inside the past; a sizeable range of numerous varieties of mathematical fashions are derived and investigated. Descents of chaotic maps come from a number of numerous directions. It may be a complicated or clean manage system, a mathematical equation which include a differential equation, or a easy circuit modeling like Chua circuit. [9, 10, and 11].

## 3) Typical Chaotic Systems

Chaos occur broadly in nature. Through the studies and improvement of chaos concept, researchers set up many chaotic dynamics models, and several of them are normal for the chaos principle and application studies, inclusive discrete_ chaotic maps, continuous_ chaotic systems, and hyper chaotic systems. We will talk the mathematical version and its fundamental properties of several normal chaotic Systems [12].

### a) Discrete_ Chaotic Map

The physical concept is that a discrete map defined via a nonlinear variation equation, which can typically be executed through a software program or sampler [12], generates chaos.

- **Logistic Map**

Logistic map is the unpretentious chaos logistic maps used to undergo chaotic signals. This map has been used in lots of applications inclusive virtual communications. Its homes have been broadly studied.

In order to acquire this logistic map 1 to a chaotic logistic map, the initial circumstance for g0 has to be inside the interval $[-1, 1]$l, and its equation is [11]:

$$g_{n+1} = 1 - 2(g_n^2)(2)$$

- **Tent Map**

It is one of discrete chaotic maps that is typically used to generate chaotic series and ultimately be used chaotic unfold, spectrum communication, chaotic encryption system, chaotic most excellent algorithm, and so on. Its equation is:

$$x_{n+1} = \begin{cases} \dfrac{x_n}{a}, x_n \in [0, a] \\ \dfrac{1 - x_n}{1 - a}, x_n \in (a, 1] \end{cases} \quad (3)$$

Tent map is piecewise linear, reason a characteristic this makes "the tent map" easier to analyses than "the logistic map".

Nevertheless, Even though the format of the tent map is easy and the equations are linear, for certain parameter values the map can yield "complex and chaotic". Behavior when the system parameter a is in (0, 1), in which case the variable$x_n$ would be in (0, 1) [12]..

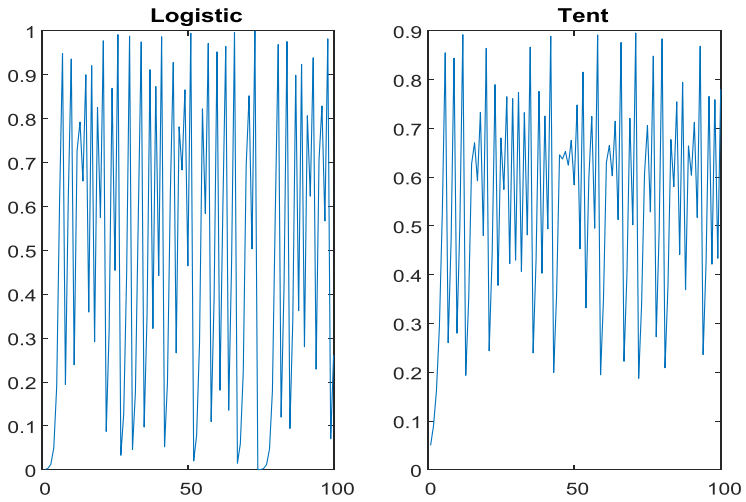



**Figure 2 Logistic and tent map**

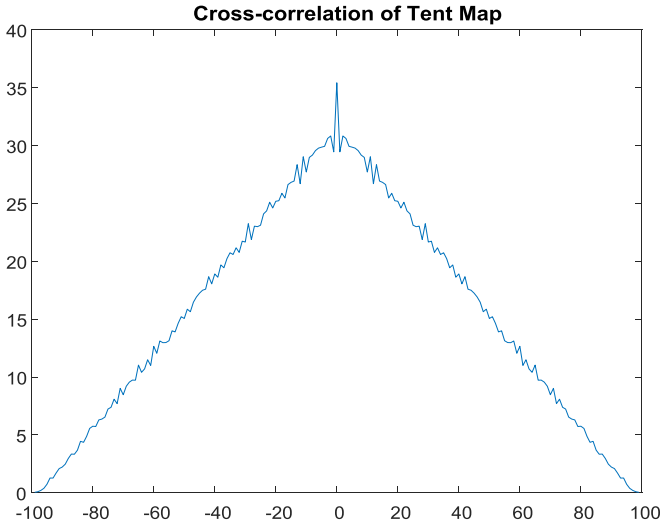



**Figure 3 Correlation of tent map**

### b) Continuous-Chaotic System

Two types of continuous-chaotic systems have been identified; autonomous system and non autonomous. Autonomous system includes Lorenz system; Chua system; and Rössler system.

Non autonomous system is the second kind; like van der Pol oscillator; and Duffing oscillator.

## 4) Randomness Evaluation

To determine the randomness in the text used several measures such as statistical measure, NIST measure, and other measures. Find statistical measures that are usually used to locate whether the binary sequence (text) has several features that make it a random text. National Institute of Standards and Technology (NIST) tests consisted of 15 measures that were developed to check the randomness of binary concatenation [13]. Will explain some measures, which used to randomness test as follows:

### a) Frequency Test within a Block (FTWB)

It is one types NIST tests. Converge of the measure is the rate of ones within M bit blocks. The goal is determining if the recurrence of ones in M bit block is roughly$\mathrm{M}/2$ or not. The result of test shall exceed the threshold (0.01) for that test until passed.

### b) Entropy Measure

In 1948, Claude Shannon first suggested the notion of Shannon entropy. It gauges the randomness and quantifies the foreseeable value of the information contained in a text, generally in bit units. The Shannon entropy equation based on the frequency of zeros values and one's values in ciphertexts. Shannon entropy equation is [14]:

$$H(x) = -\sum_{i=1}^{N} p_i \log_2 p_i (4)$$

Where $H(x)$ when closer to one lead to more randomness.

### c) Serial Test (Two-Bits Test (ST))

Serial test is one type the statistical tests. The main aim is to find the frequency of the occurrence of $(00, 10, 10 \text{ and } 11)$ in the sequence. If we assume that$n_{00}$, $n_{01}$,$n_{10}$,$n_{11}$ represent (00,01,10,11), respectively, Two-Bits Test (ST) can be computed as in equation 5 below [15]:

$$X_2 = \frac{4}{n-1}(n_{00}^2 + n_{01}^2 + n_{10}^2 + n_{11}^2) - \frac{2}{n}(n_0^2 + n_1^2) + 1(5)$$

The result of test shall not exceed the threshold (5.9915) for that test until passed.

### d) Frequency Test (Monobit Test (MB))

It is one type of statistical measures. The goal of this measure is find the rate ofzeros 0's, ones 1's in the data entered with length (n), and one type the statistical measures.$\boldsymbol{n_1}$ Represented number of 1's, and $\boldsymbol{n_0}$ represented number of 0's. Calculated this measure as in the following equation[15].

$$X_1 = \frac{(\boldsymbol{n_0} - \boldsymbol{n_1})^2}{\boldsymbol{n}}(6)$$

The result of test shall not exceed the threshold (3.8415) for that test until passed.

## Proposed Method

Contain this part on explain algorithm used.

### 1) Generated Key of RC6

This section explain key expansion algorithm after generated by using hybrid chaos (logistic and tent map) any the first halve of key generated by using logistic map and second halve generated by using tent map; the key convert to integer as equation (7,8) and convert to binary as equation (9) then using key expansion algorithm. This key used in encryption algorithm and it is used in decryption algorithm.

$$N = \lfloor m \times ch_{num} + 1 \rfloor (7)$$

$$N = N + I \bmod m + 1(8)$$

$$Bin = N \bmod 2(9)$$

$$Where\ m = 128, ch_{num}\ is\ chaos\ number, and\ I = 1,2, \ldots, 128.$$

**Algorithm (1): Key Expansion of RC6**

**Input:** Array L[0,……,c-1], c is words of key user, $r$ number of rounds,
$P_w$ = Odd ((e – 2) $2^w$), and $Q_w$ = Odd ((ه – 1) $2^w$).
**Output:** w-bit round keys S [0, … (2r+3)].

//Registers A, B, C, and D is input message in binary.
//W is size of word where (w=32).
//L user key.

$S[0] = P_w$
$for\ i = 1\ to\ (2r + 3)\ do$
$S[i] = S[i-1] + Q_w$
$(A = B = i = j) = 0$
$v = 3 * \max\{c, 2r + 4\}$
$for\ s = 1\ to\ v\ do$
{
$A = S[i] = (S[i] + A + B) \lll 3$
$B = L[j] = (L[j] + A + B) \lll (A + B)$
$i = (i + 1)\ \%\ (2r + 4)$
$j = (j + 1)\ \%\ c$
}

## 2) RC6 Encryption Algorithm

This section explain RC6 algorithm to encryption data, where input data is gray image or color image after it convert to gray Results should be clear and concise.

**Algorithm (2):RC6 Encryption**
**Input:** Plaintext stored in four w-bit input registers (A, B, C, D), r number of Rounds w-bit keys S [0, …, (2r+3)].
**Output:** Cipher text stored in (A, B, C, D).
$B = B + S[0]$
$D = D + S[1]$
$for\ i = 1\ to\ r\ do$
{
$t = \mathrm{B} * (2B + 1) \lll \log(w)$
$\mathrm{u} = \mathrm{D} * (2D + 1) \lll \log(w)$
$A = ((A \oplus t) \lll \mathrm{u}) + S[2i]$
$C = \big((C \oplus u) \lll \mathrm{t}\big) + S[2i + 1]$
$(\mathrm{A}, \mathrm{B}, \mathrm{C}, \mathrm{D}) = (\mathrm{B}, \mathrm{C}, \mathrm{D}, \mathrm{A})$
}
$A = A + S[2r + 2]$
$C = C + S[2r + 3]$

### 3) RC6 Decryption Algorithm

This section explain RC6 algorithm to the decryption data.

**Algorithm (3):RC6 Decryption**
**Input:** Cipher text stored in four w-bit input registers $(A, B, C, D)$, w-bit round keys S [0, …,(2r+3)], and r is number of rounds.
**Output:** Plaintext stored in $(A, B, C, D)$.

$C = C - S[2r + 3]$
$A = A - S[2r + 2]$
$for i = r downto\ 1\ do$
{
$(A, B, C, D) = (D, A, B, C)$
$u = D * (2D + 1) \lll \log(w)$
$t = B * (2B + 1) \lll \log(w)$
$C = ((C - S[2i + 1] \ggg t) \oplus u$
$A = ((A - S[2i] \ggg u) \oplus t$
}
$D = D - S[1]$
$B = B - S[0]$

## Results & Discussion

This algorithm was used to encrypt gray image or color images after it convert to gray image as note in Figure 4 where the results were good coding. Two types of measurements were used in the first type to measure the strength of the image and include the (entropy, SNB, Monobit, ST). The second type measures the similarity of data before and after encryption to see whether the encoder effect on the data or not includes (PSNR, RMSE, SNR).

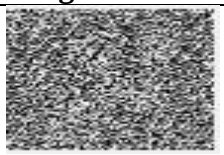
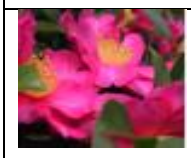
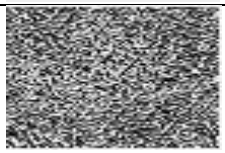
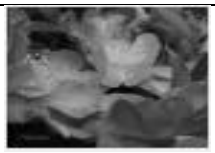
| Origin image | Encryption image | Decryption image |
|---|---|---|
|  |  |  |
|  |  |  |
|  |  |  |

**Figure 4 Encryption Image Using RC6.**

**Table 2 Some Measure of Encryption Image.**

| Image | PSNR | RMSE |
|---|---|---|
| Image 1 | Inf | 0 |
| Image 2 | Inf | 0 |
| Image 3 | Inf | 0 |

**Table 3 Test Randomly of Image Encryption.**

| Image | entropy | FTWB | MB | ST |
|---|---|---|---|---|
| Image 1 | 1 | 0.7012 | 0.9984 | 17.0460 |
| Image 2 | 1 | 0.0001 | 0.9999 | 21.5864 |
| Image 3 | 1 | 2.6059 | 0.9854 | 3.9640 |

These metrics give a good indicator of the strength of encryption and the difficulty of breaking the code.

## Conclusion

Encryption the images by using RC6 algorithm and generated key by using tent and logistic map; then the key expansion by using RC6 expansion algorithm. Used some measures to explain powerful of encryption; these measures given a very good indicator of the strength of encryption and the difficulty of breaking the code as explain in results table (2) and table (3).

## References

Stinson, D.R. (2005). *Cryptography: theory and practice*. Chapman and Hall /CRC.

Stallings, W. (2014). *Cryptography and network security: principles and practice, international edition: principles and practice.* Pearson Higher Ed.

Owuor, D.L. (2012). *Chaos based Secure Communication and system design*. Thesis Msc., Tshwane University of technology, South Africa.

Lian, S., Jinsheng, S., & Zhiquan, W. (2005). A block cipher based on a suitable use of the chaotic standard map. *Chaos, Solitons & Fractals*, *26*(1), 117-129.

AlZain, M.A., & Osama, S.F. (2017). Efficient Chaotic Tent Map-based Image Cryptosystem. *International Journal of Computer Applications*, *975*: 8887.

Rivest, R.L., Matthew, J.B.R., Ray, S., & Yiqun, L.Y. (1998). The RC6TM block cipher. *In First Advanced Encryption Standard (AES) Conference*.

Kharel, R. (2011). *Design and implementation of secure chaotic communication systems.* PhD diss., Northumbria University.

Strogatz, S.H. (1994). *Non linear dynamics and chaos: Preseus Books Publishing*. LLC.

Heidari-Bateni, G., & McGillem, C.D. (1992). Chaotic sequences for spread spectrum: An alternative to PN-sequences. *In IEEE International Conference on Selected Topics in Wireless Communications*, 437-440.

Heidari-Bateni, G., & McGillem, C.D. (1994). A chaotic direct-sequence spread-spectrum communication system. *IEEE Transactions on communications*, *42*(234), 1524-1527.

Lau, Y. (2006). *Techniques in Secure Chaos Communication.* A PhD Thesis, School of Electrical and Computer Engineering Science, Engineering and Technology Portfolio RMIT University Melbourne, Victoria, Australia.

Sun, K. (2016). *Chaotic secure communication: principles and technologies.* Walter De Gruyter GmbH & Co KG.

Rukhin, A., Soto, J., Nechvatal, J., Smid, M., & Barker, E. (2008). *A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications.* National Institute of Standards and Technolo.

Wu, Y., Noonan, J.P., & Agaian, S. (2011). Shannon entropy based randomness measurement and test for image encryption. *arXiv preprint arXiv:1103.5520.*

Katz J. (1996). *Handbook of applied cryptography.* CRC press.