Improved RC6 Algorithm using Two Types of Chaos Maps

Ziyad Tariq Mustafa Al-Ta'I , Ebtisam Jumaa

Abstract— RC6 (Rivest cipher 6) is keyblock chipher which consider symmetric imitative from RC5. It was intended to encounter the needs competition of the Advanced Encryption Standard (AES) . The aim of this work is to add new security layer to RC6 (Rivest Cipher 6) algorithm, because there is some insufficiency in the Key Scheduling Algorithm (KSA) of RC6. This paper presents improved RC6 (IRC6) key generation based on two types of chaotic maps (Chebyshev,2d logistic) to generate N key to N users. The results prove that the average secrecy of IRC6 is better than of traditional RC6, in which: for 32 bits' key length, and 256 bits' plaintext size, the average secrecy of IRC6 is (0.536 - 3.907) while for RC6 is (0.254 constant).

Keywords— Average secrecy, key scheduling algorithm, chaotic maps, RC6 Algorithm.

I. INTRODUCTION

In the era of communications technology, wired and wireless networks have exploded and the need for an effective and secure system has become very important. There is a greater need for integrity and confidentiality of information passed across these networks, Encryption algorithms play a great role in achieving these Cryptographic techniques include symmetric key cryptosystems and asymmetric key cryptosystems [1]. In symmetric-key cryptography both sender and receiver employs an exactly identical key to encrypt and decrypt the data. The study of symmetric-key cipher associates primarily to examine the block ciphers and stream ciphers, Figure (1) depicts the classification of cryptography [2]. Asymmetric key cryptosystems use two related keys, one for encryption and other for decryption. The encryption key, i.e. public key is known to everyone, only the decryption key, i.e. private key is maintained secretly by the owner [1]

key is maintained secretly by the owner [1].

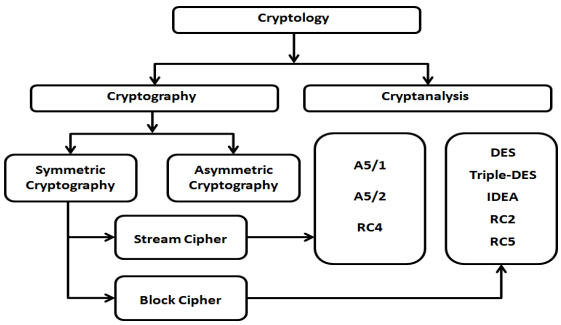

Figure (1): Classification of Cryptology [2].

RC6 and RC5 is a symmetric block cipher acquiesced to NIST for respect as the new Advanced Encryption Standard (AES). RC5 intended to be appropriate for both software and hardware application. The properties of the algorithm parameterized, with a flexible block size, number of rounds is variable, and key length is also variable. This offers the chance that the characteristics of performance and the security level be flexible [3].

RC6 algorithm was designed by Ron Rivest, Matt Robshaw, Ray Sidney and Yiqun Lisa Yin [4]. The algorithm was also acquiesced to the NESSIE and CRYPTREC projects, it is a proprietary algorithm, patented by RSA security, RC6 is consequent from RC5. The difference between RC6 and RC5 is that the former integer multiplication inclusion and instead of two w-bit, it uses four w-bit working registers [4]. The advantage of using RC6 block cipher is low time delay and computational complexity is also low that fit the real-time constrain [5].

Therefore, the diffusion of RC6 is much quicker than RC5, which allows RC6 to be implemented with less rounds at improved security and throughput also better [3].

In this paper an improvement of RC6 algorithm using two types of chaotic map is presented.

II. RELATED WORK

Kirti Aggarwalin (2014) [6], they compared the symmetric Block cipher RC6 with the two more versions of RC6. Modified RC6 and Enhanced RC6 provide some improvements of RC6, the basic difference between the three algorithms is that RC6 works on block size of 128 bits, Enhancement of RC6 (RC6e) works on block size of 256 bits and Modified RC6 (MRC6) works on block size of 512 bits. Dr. S. J. Jereesha Maryet. al. in (2018) [7], they planned model for RDM system that is a combination of Improved Rational Dither Modulation (IRDM) for watermarking and Enhanced Modified Rivet Cipher 6 (EMRC6) for encryption, modeled using EMRC6 ciphering algorithm and IRDM watermarking scheme is more robust than the existing models. A. I. Sallam,et.al. in (2017) [5], they presented an efficient RC6-based HEVC SE technique that encrypts the sensitive video bits with the features of low complexity overhead, fast encoding time for real-time applications and keeping the HEVC constant bitrate with format compliant. These features result from using the low computational complexity RC6 block cipher for encrypting the selective video bins. N.JOishi, et.al. in(2016)[8] ,they gave an efficient algorithm that enhances the performance of Blowfish algorithm by adding a function of RC6 with it.

Revised Manuscript Received on January 5, 2020

Ziyad Tariq Mustafa Al-Ta'I , computer science, University of Diayla, Baquaba, Iraq , hawhra11888@gmail.com

Ebtisam Jumaa , computer science, University of Diayla, Baquaba, Iraq , hawhra11888@gmail.com

The adding process is trickily handed here that makes the proposed algorithm as fast as Blowfish and also secured like existing AES. H. KVermaet.al. in (2012) [9] they analyzed the performance of RC6, Twofish and Rijndael block cipher algorithms on the basis of execution time and resource utilization.

III.RC6 ALGORITHM

The purpose of designing RC6 algorithm is to eliminate the disadvantages of the stream cipher RC4 and block cipher RC5 projected by Rivest [7]. RC6 designed to fit the better security necessities and improved performance. RC6 algorithm has three parts: Key expansion, Encryption and Decryption as shown in Figure (2). The steps for - Key-Expansion RC6 Algorithm are shown in algorithm (1). The steps for encryption RC6 algorithm are shown in algorithm (2). The steps for decryption RC6 algorithm are shown in algorithm (3) [6].

Key-Expansion Parameter: Use two magic constants Pw and Qw are defined for arbitrary w as follows:

Pw = Odd ((e-2)2w ... (1)

Qw=Odd ((ø-1)2w ... (2)

Where:

e = 2.718281828459 (base of natural logarithm)

ø = 1.618033988749 (golden ratio)

Odd(x) is the odd integer nearest to x

Algorithm (1): Key-Expansion RC6 Algorithm

Input: b byte key that is preloaded into c word array L [0,1, …, c-1],

r denotes the no of rounds.

Output: w-bit round keys S [0,1, ..., 2r+3]

Step1: S [0] = Pw

Step2: Repeat step 3 for i= 1 to 2r +3 do

Step3: S[i] = S [i- 1] + Qw

Step4: A = B = i = j = 0.

Step5: Iteration = 3 × max (c, 2r +4)

Step6: RepeatStep7to10forj=1toIterationdo

Step7: A = S[i] = (S[i] + A+ B) <<< 3

Step8: B = L[j] = (L[j] + A + B) <<< (A + B)

Step9: i = (i + 1) mod (2r +4)

Step10: j = (j + 1) mod c

Algorithm (2): Encryption RC6 algorithm

Input: plaintext stored in four w-bit input registers (A, B, C, D),

r Number of rounds, w-bit round keys S [0 … 2r+ 3]

Output: cipher text stored in (A, B, C, D)

Step1: B = B +S [0]

Step 2: D = D +S [1]

Step3: repeat step 4 to 8 for i = 1 to r do

Step4: t = (B × (2B + 1)) <<<log w

Step5: u = (D × (2D + 1)) <<< log w

Step6: A = ((A ⊕t) <<< u) + S[2i]

Step7: C = ((C ⊕u) <<< t) + S [2i + 1]

Step8: (A, B, C, D) = (B, C, D, A)

Step9: A = A + S [2r + 2]

Step10: C = C + S [2r + 3]

Algorithm (3): Decryption RC6 algorithm

Input: Cipher text stored in four w-bit input registers A, B, C, D

Number r of rounds, w-bit round keys S [0, …, 2r + 3]

Output: Plaintext stored in A, B, C, D

Step1: C = C -S [2r + 3]

Step2: A = A - S [2r +2]

Step3: Repeat step 4 to 8 for i = r down to 1 do

Step4:(A, B, C, D) = (D, A, B, C)

Step5: u = (D × (2D + 1)) <<<log w

Step6: t = (B × (2B + 1)) <<<log w

Step7: C = ((C -S [2i + 1]) >>> t) ⊕u

Step8: A = ((A - S[2i]) >>> u) ⊕t

Step9: D = D -S [1]

Step10: B = B -S [0]

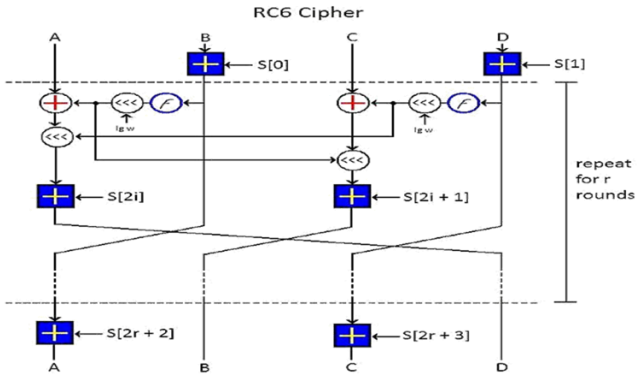

Fig.2: The Encryption and Decryption of RC6[6].

IV. CHAOTIC MAP

The chaotic sequences have various useful features of application based on security. These features are: (1) the chaotic is dynamic system in discrete time to generate complicated sequence which behaves randomly in easy and simple way. (2) the chaotic signal is not random but it is deterministic, this feature let us to renewal it. (3) The chaotic signal has high sensitivity of initial condition this lead any change in initial condition create other sequence. (4) the chaotic sequence path has random behavior in the specific space, this causes the restoration of this sequence is impossible in its specific space. Chaotic maps are separated into two classes, 1d (one-dimensional) and multidimensional maps [13]. There are many types of chaotic map, but in this study Chebyshev,2d logistic map have been used.

Chebyshev 1D Chaotic Map

Chebyshev is one of the most usually used security mechanisms in authentication methods because it contains a semi-group property. The Chebyshev polynomial is Presented in three definitions as follows:

Def.1 The Chebyshev polynomial in degree n is determined as:

$T_n(x) = \cos(n * \arccos(x))$ … (3)

where n is integer number, $x \in [1,-1]$

Def.2 Semi-group features for Chebyshev can achieved as:

$T_{rs}(x) = T_r(T_s(x)) = T_s(T_r(x))$ … (4)

Def.3 The Chebyshev polynomial in n degree, present :(x,Tx(x))

Figure (3) shows the statistical correlation curves for Chebyshev map [10].

Figure (3): The Statistical Correlation Curves for Chebyshev Map [10].

V. (2D) LOGISTIC MAP

The logistic map is a polynomial mapping and is an instance of non-linear recursive algorithm that produce chaotic relations. It was early promoted by Robert May in 1976. There are two kinds of logistic: 1D and 2D, 2D uses two 1D to produce chaotic numbers that are used in process of diffusion. This process reasons the encrypted image to possess histogram much more uniform and may also be used as symmetric-key in process of decryption. The 2D is used with original image in to produce chaotic (M×N) matrix that large key space generated as it has been use as a secret-key so it would be considered secure and confident. The two-dimensional logistic Map is shown in equations (5 and 6).

$$〚 x 〛_{(n+1)} = \lambda (〚 3y 〛_{n+1}) x_n (1-x_n) \quad \cdots (5)$$

$$〚 y〛_{(n+1)} = \lambda (〚3x〛_{(n+1)+1}) y_n (1-y_n) \quad \cdots (6)$$

where λ is considered to be equal to (3.7) and the algorithm initialized at (0.5,0.5) corresponding to (x0, y0) bifurcation diagrams of the Logistic mapexplains in Figure (4) [11].

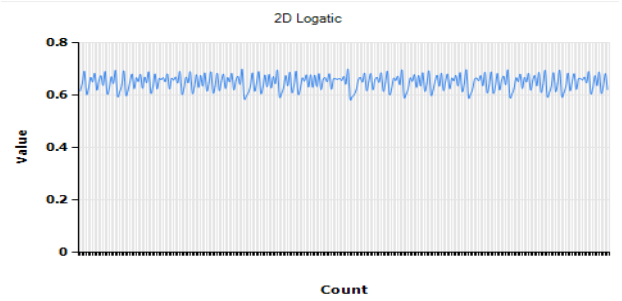

Fig.Bifurcation Diagrams of the Logistic Map [11].

VI. THE PROPOSED MODEL:

The proposed model is to establish an improvement to KSA (Improved key scheduling algorithm) as an enhancement version of KSA for RC6. The structure of the proposed model is shown in block diagram of Figure (5).

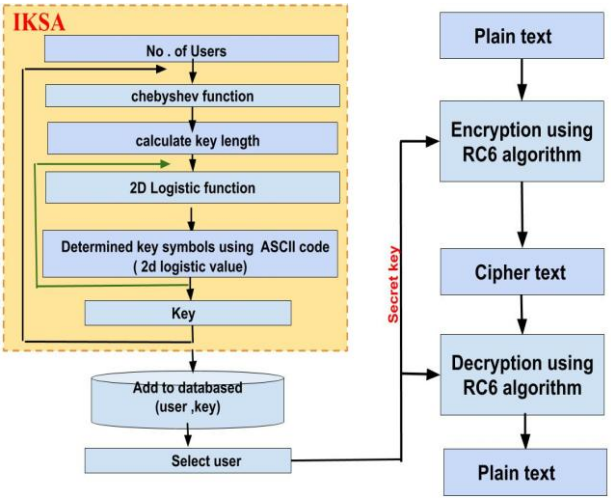

Fig. Block Diagram of the Proposed Model

The proposed algorithm can work with different word size (denoted by w), number of rounds (denoted by r) and length of block (denoted by b). Hence the short-notation IRC6-w/r/b is used to refer to word size, number of rounds and length of block. IRC6-w/r/b uses same structure for RC6 in encryption and decryption process.

The proposed IKSA uses the chebyshev and 2d logistic maps to design the chaotic key schedule for RC6 to produce unpredictable, uncorrelated and highly randomness rounds keys using a deterministic function that can generate the same sequence at both encryption and decryption methods identically. The outputs of IKSA is N keys for N of users stored in database of an administer side. The administer selected user to assign to him a unique key, this key is used in both process RC6 encryption and decryption.

VII. IMPROVED KEY SCHEDULING ALGORITHM (IKSA)

Chaotic map is employed in the proposed model at key scheduled stage, more over to enhance security of the system in a perfect manner. The used chaotic systems are chebyshev maps and 2d logistics. Chebyshev and 2d logistic maps are used to create a N number of keys to N of users with variable lengths as shown in algorithm (4).

Algorithm (4) Improved Key scheduling algorithm (IKSA)

Input (No)Number of users, ((X_0) initial value ,(n) degree of chebyshev polynomial))parameter of chebyshev function.
((X_{00}) initial value, (λ) control parameter) parameter of logistic function.
Output database(user, key)

Initialize IKSA by enter the (No) number of users to provide each of them a unique key
For (User=1 to No)
While (! Key length < =3)
Calculate $Chevbyshev_{value}$ by equation (3)
Swap (X_0 , $Chevbyshev_{value}$)
Data = Split ($Chevbyshev_{value}$, '.') and take only digits after the dot '.'
Key length= Convert 'Data' to integer number of 64-bits
End while
For (i=1 to key length)
Calculate logistic $_{value}$ by equation (5) and (6)
Swap (X_{00}, Logistic $_{value}$)
Convert Logistic $_{value}$ to integer number 64-bits
Key [i]= Convert Logistic $_{value}$ to its ASCII equivalent value
End For
Add to databased (user, key)
End For

The main function of proposed IKSA is generate N key for N users with variable length. In order to achieve this, IKSA can be divided into two parts:

1- Determine key length using chebyshev map, where the minimum limit for key length that is not equal and less than (3 symbols) to avoid create short keys that are not secure to be used for IRC6 algorithm.

Chebyshev function used parameter as inputs to its function, these parameter are: X_0 (initial value) = 0.2 and n = 5 and number of round [0-255], i.e. if the chebyshev value = 0.334612078527893, spilt this value and take digits after dots '.' (334612078527893) and converted to integer number 64-bits using Mod operation then key length = Mod (334612078527893) = 9 .

2- Determine the key symbols using 2d logistic map, here the key represent as vector and length of this vector is equal key length value and each key symbol can be represented using logistic value after converted to Asci code that its equivalent value. Chebyshev function used parameter as inputs to its function, these parameters are: X_{00} (initial value) = 0.4 and λ=0.7 and number of round [0-255]. i.e, since the key length = 9, must be generate 9 logistic value using 2d logistic function and stored in array vector as V =(1,1,1,1,242,98,242,169,1) then convert each value in V to its equalized Ascii code to produce key = _ h _ &

VIII. Encryption /Decryption Process in IKSARC6 Algorithm:

The input of encryption algorithm are four registers include plains text denoted by: A, B, C, and D each of which is of length w words. In additional to the keys generated from the IKSA, b= [0,…,2b + 3] and number of rounds (r). The administer selected user from data base to get (user, key), then encryption algorithm (3) is used to convert the plain-text populated in the four registers to the cipher-text

In the decryption algorithm (4), the four registers A, B, C, and D contains the cipher-text are fed into IRC6 along with the number of round (r) and same key is used in encryption process which is get from database. The output of IRC6 decryption is the plaintext.

IX. The Results

Secrecy of ciphers is calculated in terms of the key equivocation (conditional entropy of key given cipher) as shown in equation (7) [12]:

$$H\left(K/C\right) = \sum_{i=1}^{L}\sum_{i=1}^{n} q_i \; P_{ij} \log P_{ij} \quad \ldots. \textbf{(7)}$$

Where

qi = Pr (C = ci), Pij = Pr (K=ki / C = ci).

L is the key length n is the cipher text length

• **Average secrecy:** the original RC6 algorithm with KSA, using a fixed plaintext size (128,192,256 bits) and fixed key length for each phase (16,24,32bits)Show the higher value of the average secrecy=0.308519593 by using the same key with key length 24 bits and plaintext size192 bits ,The improvement RC6 algorithm with IKSA has better average secrecy than the original RC6 algorithm with KSA, using a fixed plaintext size (128,192,256 bits) and variable key length for each phase (16,24,32bits) Show the higher value of the average secrecy= 3.90689059560852by using the different key with key length 32 bits and plaintext size256 bits, The average secrecy of RC6 and IRC6 is shown in Table (1).

Table (1): average security for RC6 and IRC6 where represent higher value for average security.

Keys Length\Bits	Plaintext Size\Bits	Average Secrecy for RC6	Average Secrecy for IRC6	Users
16	128	0.244180662225532	0.47208261363603	User1
		0.244180662225532	0.60114843260142	User2
		0.244180662225532	0.536421545192909	User3
		0.244180662225532	0.469552084845776	User4
		0.244180662225532	0.439525192005959	User5
24	192	0.308519593782412	0.374410348745816	User1
		0.308519593782412	0.602312300156314	User2
		0.308519593782412	0.6654873641583	User3
		0.308519593782412	0.519366922674611	User4
		0.308519593782412	0.373634437042554	User5
32	256	0.253823661470507	3.90689059560852	User1
		0.253823661470507	0.828662428160286	User2
		0.253823661470507	0.553476167711207	User3
		0.253823661470507	0.600760476749789	User4
		0.253823661470507	0.536033589341278	User5

The method proposed in this study generates N keys for N user but was taken in comparison to the highest value of the values in Tables (1). Figures (6, 7, 8) explain that the average secrecy of the proposed algorithm (IRC6), which are indicate that IRC6 is better than the original algorithm (RC6).

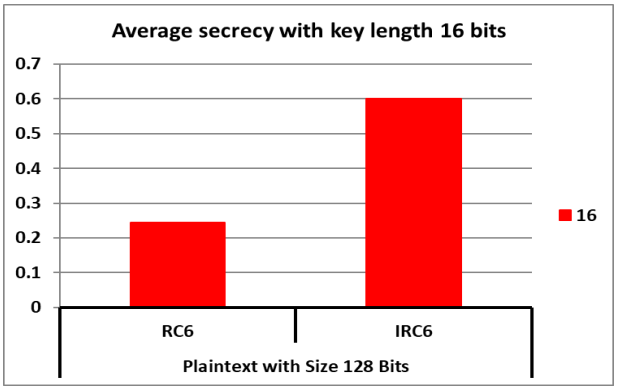

Fig6 Comparison Between IRC6 and RC6 Depending on the Key Length 16 bits and plain text size 128 bits.

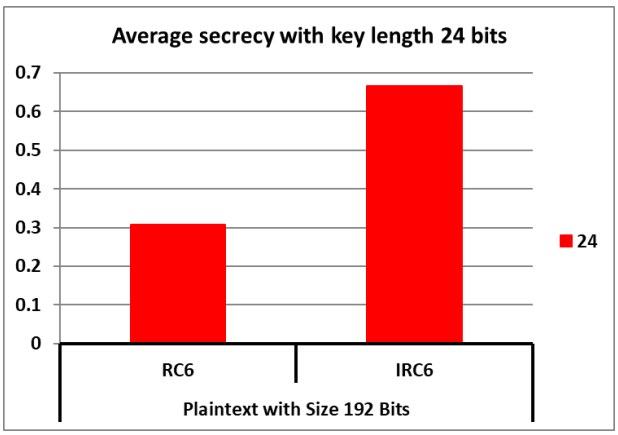

Fig7 Comparison between IRC6 and RC6 depending on the key length 24 bits and plain text size192 bits.

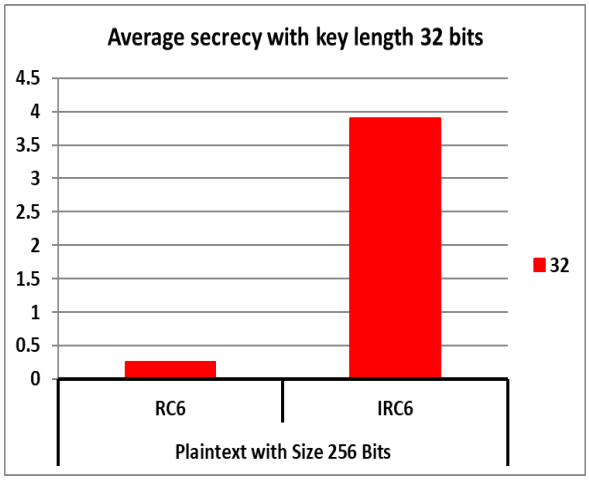

Fig.8 Comparison between IRC6 and RC6 depending on the key length 32 bits and plain text size256 bits.

X. CONCLUSION

This work presents improved RC6 (IRC6) key generation depending on two kinds of chaotic maps (Chebyshev,2d logistic) to generate N key to N users. The proposed algorithm eliminates the original RC6 weakness with KSA. The average secrecy is used for comparison using a fixed plaintext size (128,192,256 bits) and variable key length for every phase (16,24,32 bits). The proposed algorithm is best than the original algorithm as shown in Table (1) and Figures (6,7, and 8). IRC6 benefits from the randomness of chaotic maps (Chebyshev,2d logistic). Therefore, IRC6 is considered as a new better version of RC6.

REFERENCES

1. M. Srinivas, S. Porika,"Encryption and Decryption Using Elliptic Curves for Public Key Cryptosystems," International Conference on Intelligent Computing and Control Systems ICICCS, pp:1300-1303, 2017.
2. H. S.Gill, "Selection of Parameter 'r' in RC5 Algorithm on the basis of Prime Number," RAECS pp: 06 – 08, 2014.
3. man young Rhee, "wireless mobile intent security '', second edition ,2013.
4. N. Liu, J. C. Xiaojuan Zeng, G. Lin, J. Chen,"Cryptographic Performance for Rijndael and RC6 Block Ciphers," IEEE pp:36-39, 2017.
5. A. I. Sallam, O.S. Faragallah, S. M. Rabaie ,"HEVC Selective Encryption Using RC6 Block Cipher Technique,",IEEE ,2017
6. KirtiAggarwal,"Comparison of RC6, Modified RC6 & Enhancement of RC6,"International Conference on Advances in Computer Engineering and Applications (ICACEA), pp:444-449 ,2014.
7. S. J. JereeshaMary,S.Sebastin Antony Joe,"IRDM WATERMARKING WITH EMRC6 ENCRYPTION FOR DRM SYSTEM", IEEE, 2018.
8. Nusrat Jahan Oishi, Md.Arafin Mahamud,Asaduzzaman,"Short Paper: Enhancing Wi-Fi Security Using a Hybrid Algorithm of Blowfish and RC6," IEEE,2016.
9. Harsh Kumar Verma and Ravindra Kumar Singh,"Performance Analysis of RC6, Twofish and Rijndael Block Cipher Algorithms,"International Journal of Computer Applications (0975 – 8887),Volume 42– No.16,pp:1-7, March 2012.
10. Chunyi Quan1, Jaewook Jung1, Hakjun Lee1, Dongwoo Kang1 and Dongho Won2,"Cryptanalysis of a Chaotic Chebyshev Polynomials Based Remote User Authentication Scheme", pp:438-441,2018 IEEE.
11. R. M. Saffari, S. Mirzakuchaki, "A Novel Image Encryption Algorithm Based on Discrete Wavelet Transform Using Two Dimensional Logistic Map," (ICEE), pp:1785-1790,2016.
12. Naji Mutar Sahib, Ali Hussein Fadel and Noora Shihab Ahmed "Improved RC4 Algorithm Based on Multi-Chaotic Maps" Journal of Applied Sciences, Engineering and Technology pp: 1-6, 2018.
13. Rui Ye, "Image Watermarking using Chaotic Watermark Scrambling and Perceptual Quality Evaluation", 2013. <hal-00861068>