International Journal For Technological Research In Engineering
Volume 1, Issue 7, March-2014 *ISSN (Online): 2347 - 4718*

ENCRYPTION USING CHAOTIC MAPS

Sangeeta Yadav[1], Abhishek Didel[2], Nisha Khushwah[3]
Department of Computer Science and Engineering
Rajasthan Technical University
Rajasthan, India.

Abstract: **The use of chaotic systems for secure or private communications has been an active area of research in the past few years. It is based on the facts that chaotic signals are usually noise-like and chaotic systems are very sensitive to initial conditions. In recent years, external key was introduced to chaotic cryptography by Pareek et al. and find its application in several discrete chaotic cryptosystems.**
In 2013 an improved symmetric encryption scheme using one dimensional chaotic map in order to obtain chaotic sequences with better cryptographic features was proposed by Nisha Khushwah. We propose a modified version of the chaotic cryptographic method based on iterating a skew tent map and logistic map.
Keywords: **Cryptography, skew tent map, logistic map, confusion, diffusion, permutation operation.**

I. INTRODUCTION

Computer Application and Internet service have been contributing extensively to our life experiences. Internet also allows users to access information, wherever they may be and provides communication services, with or without computer security. This rapid development of internet and communication network increased the risk of theft, unauthorized access, disclosure, disruption, inspection, recording or destruction of proprietary information because of the insecure channel through which two different parties communicate with each other. This led to the development of various techniques for secure communication and adoption of cryptography so that the information can be transmitted in unreadable format.
In the field of cryptography the use of chaotic maps has been very popular in now days. And the cryptography procedure is basically depends on the external factor key that is used to encrypt the plaintext into cipher text.
Cryptosystem refers to a suite of algorithms to implement a particular form of encryption and decryption. In an ideal cryptosystem confusion reduces the correlation between the plaintext and cipher text while diffusion transposes the data located at some co-ordinates of the input block to other co-ordinates of the output block [4]. In recent years, many researchers' shows there interest in studying the behavior of chaotic systems. An interesting relationship between chaos and cryptography has been developed during last two decades, according to which many properties of chaotic systems such as: periodicity, sensitivity to initial conditions/system parameters, mixing property, deterministic dynamics and structural complexity can be considered analogous to the confusion, diffusion.
For designing of new digital chaotic cryptosystems, logistic map is the most widely used. Baptista uses logistic map in his system in which iterates are generated using the equation:

$$X_{n+1} \rightarrow f(\lambda, x) = \lambda X_n(1-X_n) \qquad Xo \in [0,1]$$

Chaotic Cryptography can be classified into two parts, which are analog chaos-based cryptosystems and digital chaos-based cryptosystems. First type of chaotic cryptosystems is based on the chaotic synchronization technique, whereas digital chaotic cryptosystems are based on one or more chaotic maps in such a way that the secret key is either given by the control parameters and the initial conditions or determines those values. The inclusion of more than one 1D maps increases the confusion in the encryption process and results in a more secure cryptosystem due to the fact that more confusion in encryption makes the cryptosystem more secure. We have found that the present cryptosystem is faster than the existing chaotic cryptosystems. We have used only two prototype chaotic maps in the present algorithm however; it can be easily extended to any number of 1D chaotic maps.

$$\boldsymbol{T(x)} = \begin{cases} \dfrac{\boldsymbol{x}}{\boldsymbol{p}}, & \boldsymbol{x} \in [\boldsymbol{0}, \boldsymbol{p}) \\ \dfrac{\boldsymbol{1-x}}{\boldsymbol{1-p}}, & \boldsymbol{x} \in (\boldsymbol{p}, \boldsymbol{1}] \end{cases}$$

The skew tent map and the logistic map are topologically conjugate, and thus the behaviors of the two maps are in this sense identical under iteration. Because of the above advantages of both the maps, here in this project we are using logistic and skew tent map both, in the recently proposed cryptosystem.
The proposed system is a symmetric key block cipher algorithm, in which plaintext is rearranged to form a groups of fixed length i.e. of 64 bits (size of each block). These blocks are encrypted sequentially; one logistic map and one skew tent map are used here for encryption. And 128-bit external secret key determines number of iterations and initial condition for the chaotic maps. The whole process of block by block encryption/decryption of 64- bit block, depend on number of iterations and initial condition and encryption of previous block of plaintext/cipher text. Detailed step by step procedure of the encryption/decryption of the proposed cryptosystem is explained below.

II. PROPOSED ALGORITHM

Step 1: First for encryption/decryption in this algorithm, we divide plaintext/cipher text of any size into blocks unit of 64-bits. Plaintext and Cipher text of any size are rearranged in the block unit of 64 bits Plaintext and cipher text of n blocks can be represented as:

Plaintext (P) = $P_1P_2P_3 \ldots P_b$ (2)
Cipher text (C) = $C_1C_2C_3 \ldots C_b$ (3)

Where, the subscript b stands for the block number.
$P_1, P_2, P_3, \ldots, P_b$ is plaintext block unit of 64 bits
$C_1, C_2, C_3 \ldots$ Cbareciphertextblock unit of 64 bits

Step 2: Now Secret key of 128-bits is dived in into blocks of 64-bits named as session keys, as using a secret key of 128-bit is long and inconvenient for encryption/decryption. Secret key is in hexadecimal mode, so a 128-bits key will contain total 32 alphanumeric characters (out of 0 to 9 and A to F). This session key of 64 bit is further sub divided to determine the initial conditions two maps and iteration number, as show below. The secret key (K) is chosen from a 128-bit external binary sequence, and is represented in Fig1.

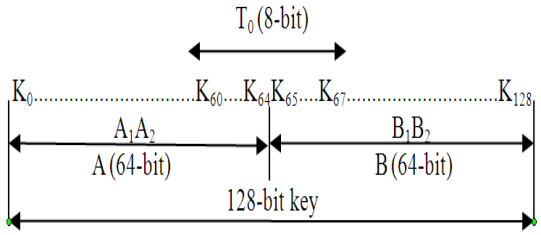

Fig.1 Representation of 128-bit secret key (K)

Where, K =$(A_1A_2B_1B_2)_2$
A_1, A_2, B_1, and B_2 are 32-bit blocks
A= $(A_1 A_2)_2$, B = $(B_1 B_2)_2$ are 64-bit blocks.
This 128-bit external binary sequence determines the initial condition of two maps (X0 and Y0), as well as the initial iteration number (T0).

Step 3: Now, set b = 0, and this 128-bit external binary sequence determines the initial condition of two maps logistic and skew tent (X_0 and Y_0) respectively. 128-bit key is converted to the valid value range of initial condition of chaotic maps [0, 1] with 2^{64} possible values. And also determine chaotic iteration, for this we set a key-dependent value for T_0.

Block number b = 0

Initial condition for t_1 and t_2:

$X_0 = (0.A \oplus B)_2$ (4)
$Y_0 = (0.A_1B_2)_2$ (5)

Initial iteration number (T_0):
$(T_0)= (K_{60} K_{61} K_{62} K_{63} K_{64} K_{65} K_{66} K_{67})_2$ (6)

Where, ⊕ is bit-wise exclusive-OR (XOR) operation. (0.A⊕B) 2 represents fraction written in binary mode. It has 64-bit decimal digits which are represented by (A⊕B) 2. (0.A1B2) 2 has the similar meaning's (i) denotes the ith bit of K.
In this way, 128-bit key is converted to the valid value range of initial condition of chaotic maps [0, 1] with 264 possible values. Also for the chaotic iteration we set a key-dependent value for T0.

Encryption of Plaintext and Decryption of Cipher text

For b = 0
$X_0 = A \oplus B$
$Y_0 = A_1B_2$
$T_0 = (K_{60} K_{61} K_{62} K_{63} K_{64} K_{65} K_{66} K_{67})_2$
$C_0 = (A_2B_1)_2$

Step 4: For, b> 0, X_b, Y_b and T_b are updated by (7), (8) and (9), respectively

b=b + 1
$X_b = C_{b-1} \oplus X_{b-1} \oplus (B_2A_1)_2$ (7)
$Y_b = C_{b-1} \oplus X_{b-1}$ (8)
$T_b = z(P_{b-1}) \oplus T_{b-1}$ (9)

Where, z(•) is a bit-wise XOR function between bytes, e.g. $z(X) = X_{(0-7)} \oplus X_{(8-15)} \oplus \ldots$

Step 5: X_b and Y_b are updated to the latest status (10) and (11) by iterating the first logistic map with the initial condition X_b from (7) by T times and second skew tent map with initial condition Y_b from (8), just for once.

$X_b = t^T(X_b)$ (10)
$Y_b = t^2(Y_b)$ (11)

Step 6: Now b^{th} plaintext is encrypted by using updated/Y_b. The updated X_b/ Y_b is also used to decrypt the b^{th} cipher text .

$C_b = S(P_b) \oplus C_{b-1} \oplus X_b \oplus Y_b$ (12)
$P_b = S^{-1}(P_b) \oplus C_{b-1} \oplus X_b \oplus Y_b$ (13)

Whereas (•) is a permutation operation, formed by two steps, i.e. Byte-wise rotate right operation: In this step the rotate number is determined by the byte-wise sum modulo the length of bytes in plaintext block and then byte- wise rotation is performed on plaintext block.
For example, • = $(AABBCCDD)_{16}$, which is denoted in hex, the rotate number is$((AA)_{16} + (BB)_{16} + (CC)_{16} + (DD)_{16})$ mod 4. If this result is 2, s$((AABBCCDD)_{16})$ is rotated to $(CCDDAABB)_{16}$ [1].
Bit exchange operation: - In bit exchange operation, dividing length is determined by the number of non-zero bits in A_1B_2 and then swapping the left part of certain length in the block with the remaining right part.
S^{-1}(•) is the inverse operation of s(•),formed by two steps, i.e Similar bit exchange operation and, then byte-wise rotate left operation.
Step 7: Repeat the process (i.e. go to step (3)) until the whole

plaintext/ cipher text is encrypted or decrypted.

III. SIMULATION RESULT

For this proposed algorithm the cipher block chaining (CBC) mode is used. A secret key (K) = (a1b2c3d4e5f6abcdef7890abcdef1234)16 was taken and for plaintext, a simple .txt (text file) of size 2.5 kb was taken. Results are show in above Fig.2 (a, b, c) spike like modal shows frequency of occurrence of 8-bit value. Proposed cryptosystem shows uneven distribution while Nisha's system shows flat distribution. This uneven distribution contributes to difficulty of predicting variables.

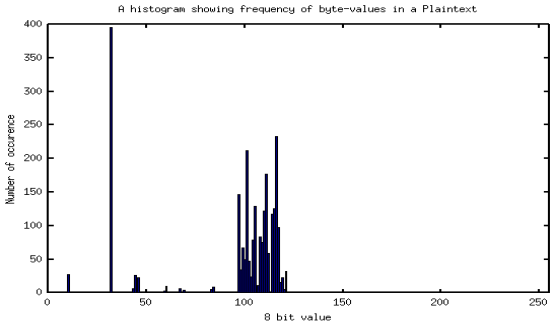

Fig.2. (a) Distribution of plaintext of a 2.5kb .txt file

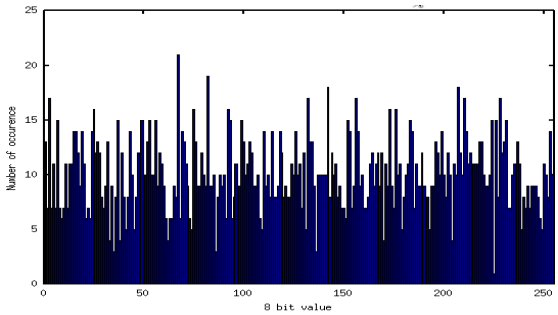

Fig.2 (b) Distribution of cipher text using Nisha Khushwah's cipher

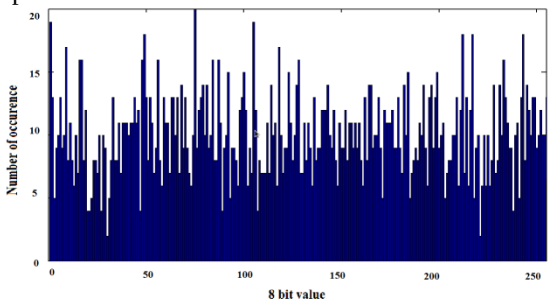

Fig.2(c) Distribution of cipher text using the proposed cipher

Confusion effect: For confusion effect of the proposed cryptosystem, for this first we plot the plaintext (P) = "Formatting Numbers with C++ Output Stream" and the cipher text (E (P, K)) generated by different cryptosystems which is shown in below Fig.3 (a, b, c).

Fig.2 (a) represents a histogram showing the frequency of occurrence of byte-value in Plaintext. While, Fig.2 (b, c), represent the frequency of occurrence of byte-value in cipher text generated by Nisha Khuswah's cryptosystem and proposed cryptosystem, respectively.

Plaintext and cipher text generated by the both cryptosystem are totally different both in byte-value and number of occurrence of byte value. Fig.3 shows confusion effect clearly in cipher generated by both the cryptosystems.

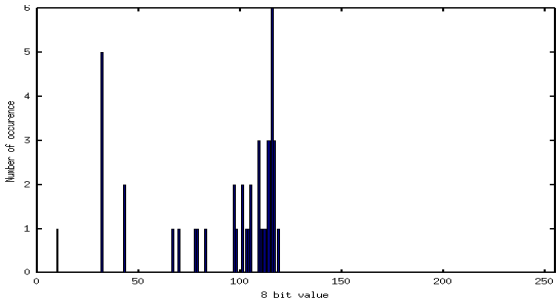

Fig.3 (a) Distribution of plaintext (P)

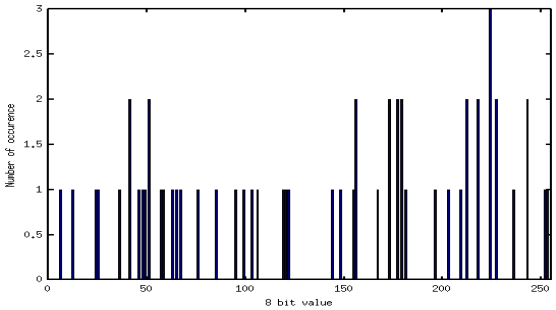

Fig.3 (b) Distribution of ciphertext generated by Nisha Khushwah's cryptosystem.

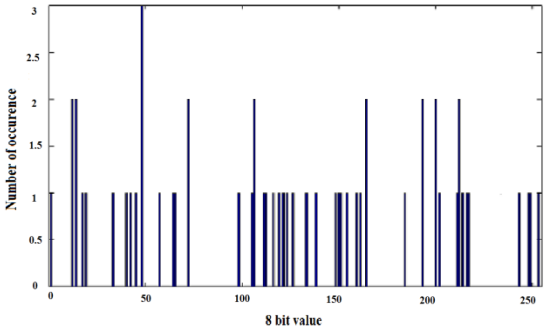

Fig.3 (c) Distribution of ciphertext generated by proposed cryptosystem.

IV. SECURITY ANALYSIS

Nisha Khushwah's schemes eliminated all the existing weaknesses of the cipher based on Xiang's scheme. The proposed cipher is based on Nisha Khushwah's schemes, so all the advantages of the Nisha Khushwah's system is kept and problem of even distribution of chaotic variable is removed.

By expanding the block size of plaintext/cipher text and the precision of chaotic variable to 64 bits, provides much larger space (2^{64}) for the plaintext/cipher text in a block as well as the initial condition of the chaotic map, while in 8-bit block

size and only 256 possible values for X_0 in the original schemes, this improvement gets rid of the brute-force attack that can serve as a foundation for further cryptanalysis. Initial conditions of the two maps X_0 and Y_0 are determined by key dependent transformations so they cannot be recovered by an adversary [13].Many chaotic cryptosystems do not possess any confusion or diffusion operation within the block. Permutation scheme into the plaintext block is included in the system to provide further confusion or diffusion operation within the block. s(•) is both plaintext and key dependent permutation operation in our proposed algorithm.

In our proposed scheme, the one logistic map and one skew tent map are adopted for the chaotic iteration which is also key dependent, whose initial values are related to the key and are adopted for the encryption and decryption of the plain text, for the elimination of the even distribution and difference of cipher text present in the Nisha Khuswah's scheme that causes only significant difference in cipher text that may cause the easy prediction of chaotic variable by the attackers. Logistic map shows uneven distribution of chaotic variable and remove the problem of easy prediction. And Skew tent map have the uniform invariant density. In this improved scheme sensitivity to the secret key and uneven distribution of chaotic variable generate a cipher text, in which predicting a chaotic variable is quite impossible and therefore, risk of plaintext attack is removed. Hence, security level is further enhanced in proposed scheme by using the advantages of both the maps. The performance of the cryptosystem is improved according to the observation made from the simulation result and security analysis. While selecting the secret key practically, one should take care that not to take a secret key whose four parts A_1, A_2, B_1, and B_2 are exactly identical. If we take four parts A1, A2, B1, and B2 exactly identical, then initial conditions of chaotic maps becomes zeros and then under this condition no valid chaotic iterations exist. Here in this paper we have shown the difference between plots of plaintext and cipher text. Among confusion and diffusion only confusion effect has been shown in it, the diffusion effect will be in further results.

V. CONCLUSION

On the basis of the study of paper an improved chaotic cryptosystem with external key by Nisha Kushwah ,we have improve the security of the cryptosystem in this scheme by using the advantages of both maps i.e, Logistic map and Skew tent map. A generalized description of Nisha Kushwah's cryptosystems is given here and their weaknesses and also their solution to provide more security. We have notice that both proposed and Nisha Kushwah's cryptosystem have same size of plaintext and cipher text and size of cipher text generated by both systems are similar and their encryption time are also same. Based on the above analyses, more secure cryptosystem is proposed. For this secure scheme, one logistic and one skew tent map are used instead of two logistic maps in order to obtain chaotic sequences with improved cryptographic feature. All these advantages make this more secure cryptosystem for the use of information transmission over insecure channel and secure application. An improved scheme with all existing deficiencies and redundancies eliminated is proposed. Theoretic analysis and numerical simulation both verify its superiority
And security.

REFERENCES

[1] NishaKhushwah, MadhuSharma,"Chaotic Map based Block Encrption", International journal of Computer Applications,vol.71-No.16 ,0975-8887, June 2013.
[2] Tao Xiang, Kwok-wo Wong and Xiaofeng Liao, "An improved chaotic cryptosystem with external key", Communications in Nonlinear Science and Numerical Simulation 13, (2008), 1879–1887
[3] Pareek NK, Patidar V and Sud KK, "Discrete chaotic cryptography using external key", Phys Lett A, 003, 309:75–82.1886
[4] Pareek NK, Patidar V and Sud KK. "Cryptography using multiple one-dimensional chaotic maps", Commun Nonlinear Sci Numeri Simul, 2005, 10:715–23.
[5] Baptista MS, "Cryptography with chaos", Phys Lett A, 1998, 240:50–4.
[6] Shannon CE, "Communication theory of secrecy systems", Bell Syst Tech J, 948, 8:656 7 5.
[7] Vinod Patidar and K. K. Sud, "A Pseudo Random Bit Generator Based on Chaotic Logistic Map and its Statistical Testing", Informatica 33, (2009), 441–452 441
[8] Alvarez G, Montoya F, Romera M and Pastor G, "Cryptanalysis of a discrete chaotic cryptosystem using external key", Phys Lett A, 003, 3 9:334–9.
[9] Wei J, Liao XF, Wong KW and Zhou T, "Cryptanalysis of a cryptosystem using multiple one-dimensional chaotic maps", Commun Nonlinear Sci Numeri Simul, 2007, 12:814–22.
[10] Wong WK, Lee LP and Wong KW, "A modified chaotic cryptographic method", Phys Lett A, 00 , 38: 34–6.
[11] B.R.Ivan, S.D.Dhodapakar and Q.V.Lavande, "Chaos ased Cryptography". Newsletter No. 58, July 005.
[12] Alvarez G and Shujun Li. "Some Basic Cryptographic Requirements for Chaos-Based Cryptosystems".
[13] David Arroyo1, Gonzalo Alvarez1, and Veronica Fernandez, "On the inadequacy of the logistic map for cryptographic applications".
[14] William Stallings "Cryptography and Network Security Principles and Practices", Fourth Edit.

