Chaotic Map based Block Encryption

Nisha Kushwah
M.Tech (CSE)
DIT
Dehradun, India

Madhu Sharma
Asst. Prof. (CSE)
DIT
Dehradun, India

ABSTRACT

Number of cryptosystems based on chaos has been proposed, in recent years. Tao Xiang , Kwok-wo Wong, Xiaofeng Liao in 2008 proposed an improved scheme by using a symmetric key block cipher algorithm in which one-dimensional chaotic maps are used, in order to obtain chaotic sequences with better cryptographic feature. In this system, an encryption /decryption scheme was proposed, a cryptographic algorithm using one-dimensional chaotic maps and an external secret key. The chaotic map adopted in this cryptosystem is two logistic maps, and external secret key is of 128-bits. Based on the simulation result, more secure cryptosystem is proposed. As, two logistic maps are used in order to obtain chaotic sequences with improved cryptographic feature. All these advantages make this more secure cryptosystem for the use information transmission over insecure channel and secure application

General Terms

CBC mode, Chaotic Cryptography, Chaotic map, Confusion, Diffusion, Ergodicity, Logistic map, Permutation operation.

1. INTRODUCTION

Rapid development in Internet and mobile-phone networks, Modern telecommunication networks in recent year, has increased the risk of theft, unauthorized access, disclosure, disruption, modification, perusal, inspection, recording or destruction of proprietary information because of the insecure channel for information transmission. This has led to the development of various techniques of secure communication and adoption of cryptography for information transmission over insecure channel in such a way that it became unreadable by the third party.

In data and telecommunications, cryptography is necessary when communicating over any insecure channel. Cryptography is science and study of techniques for secure communication. In Cryptography transformation procedure depends on an external parameter called key such that it is only possible to recover the original message if that key is known. Cryptosystem consists of algorithms, protocols and key for encryption/decryption process. It is an implemented form of cryptographic framework to protect and secure information in computer technology and communication. Cryptosystem refers to a suite of algorithms to implement a particular for of encryption and decryption. Confusion and diffusion are two main properties for an ideal cryptosystem. Confusion reduces the correlation between the plaintext and ciphertext while diffusion transposes the data located at some co-ordinates of the input block to other co-ordinates of the output block [3].

Cryptographers and many chaotic cryptosystems, i.e. cryptosystems based on chaotic maps, show their interest in chaotic map because of the interesting relationship between chaos and cryptography. Many properties of chaotic systems such as: ergodicity, sensitivity to initial conditions/system parameters, mixing property can be considered analogous to the confusion, diffusion, according to the relationship between chaos and cryptography [6]. Chaotic Systems are basically nonlinear and exhibiting and apparently random behavior for certain range of values of system parameters. These systems appear spontaneously in nature and can be directly applied to security processes. The properties of chaotic systems have been used in very different ways to build new cryptosystems. Discrete chaotic systems, such as the logistic map, can exhibit strange attractors whatever their dimensionality. Chaotic maps are simple unstable dynamical systems .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:

$$X_{n+1} \rightarrow f(\lambda, X) = \lambda X_n(1 - X_n) \qquad X_0 \in [0, 1]$$

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.

For the study of private key cryptography with chaos many discrete chaotic cryptographic algorithms have been introduced, most of them uses one chaotic map, either the system parameter or initial condition of the chaotic map or both are used as a secret key. This algorithm is related to a digital chaotic cryptosystems, subclass of the second type of chaotic cryptosystems. In this cryptosystem one- dimensional chaotic map and external secret key is used for encryption and decryption, this external secret key determines the system parameter, initial condition of the chaotic map in a cryptosystem. Introducing chaotic map improves the security of the system as more confusion in the encryption makes cryptosystem more secure. 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; two logistic maps 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/ciphertext. Detailed step by step procedure of the encryption/decryption of the proposed cryptosystem is explained below.

2. PROPOSED ALGORITHM

First for this encryption/decryption algorithm, divide plaintext/ciphertext of any size into blocks unit of 64-bits. Plaintext and ciphertext of n blocks can be represented as:

Step.1

$$\text{Plaintext (P)} = P_1P_2P_3 \ldots . P_b \quad (1)$$

$$\text{Ciphertext (C)} = C_1C_2C_3 \ldots . C_b \quad (2)$$

Where, subscript b stands for the block number. $P_1P_2P_3 \ldots . P_b$ are plaintext block unit of 64 bits and $C_1C_2C_3 \ldots . C_b$ are ciphertext block 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 Figure 1. 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.

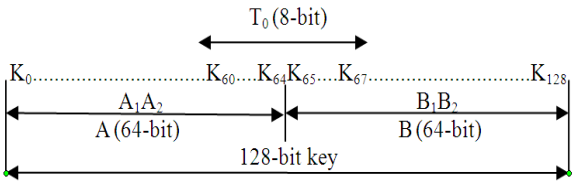


Figure.1 128-bit secret key (K)

Step.3 Now, set b=0 and this 128-bit external binary sequence determines the initial condition of two logistic maps (X_0 and Y_0). 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 a key-dependent value for T_0 was set.

Block number b = 0

Initial condition for t_1 and t_2:

$$X_0 = (0.A \oplus B)_2 \quad (3)$$

$$Y_0 = (0.A_1B_2)_2 \quad (4)$$

Initial iteration number

$$T_0 = (K_{60}\, K_{61} \ldots \ldots K_{66}\, K_{67})_2 \quad (5)$$

Where, '⊕' is bit-wise exclusive-OR (XOR) operation. $(0.A \oplus B)_2$ represents fraction written in binary mode. It has 64-bit decimal digits which are represented by $(A \oplus B)_2$. $(0.A_1B_2)_2$ has the similar meaning. K(i) denotes the i^{th} bit of K.

Step.4 For b > 0, X_b, Y_b and T_b are updated by (8), (9) and (10), respectively.

$$b = b + 1$$

$$X_b = C_{b-1} \oplus X_{b-1} \oplus (B_2A_1)_2 \quad (8)$$

$$Y_b = C_{b-1} \oplus X_{b-1} \quad (9)$$

$$T_b = z(P_{b-1}) \oplus T_{b-1} \quad (10)$$

Where, z (•) is a bit-wise XOR function between bytes, e.g. $z(X) = X_{(0\text{-}7)} \oplus X_{(8\text{-}15)} \oplus \ldots$. Initial condition for updating X_b, Y_b and T_b are determined by the 128-bit external binary sequence. So these are also key-dependent. $X_0 = (0.A \oplus B)_2$; $Y_0 = (0.A_1B_2)_2$; $T_0 = (K_{60}\, K_{61} \ldots \ldots K_{66}\, K_{67})_2$; $C_0 = (A_2B_1)_2$.

Step.5 X_b and Y_b are updated o the latest status (11) and (12) by iterating the first logistic map with the initial condition X_b from (8) by T times and second logistic map with initial condition Y_b from (9), just for once.

$$X_b = t^T(X_b) \quad (11)$$

$$Y_b = t^2(Y_b) \quad (12)$$

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

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

$$P_b = S^{-1}(P_b) \oplus C_{b-1} \oplus X_b \oplus Y_b \quad (14)$$

Where, S(•) is a permutation operation, formed by two steps, Byte-wise rotate right operation: - In this step first the rotate number is determined by the byte-wise sum modulo the length of bytes in plaintext block, for example, let $\bullet = (aabbccddee)_{16}$, denoted in hexadecimal, Rotate Number $= \big((aa)_{16} + (bb)_{16} + (cc)_{16} + (dd)_{16} + (ee)_{16} + (ff)_{16}\big) \bmod 4$. If rotate number is 2, then $s((aabbccddeeff)_{16})$ is rotated to $(ccddeeffaabb)_{16}$ for byte-wise rotation on plaintext block.

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.

And $S^{-1}(\bullet)$ is the inverse operation of s(•) used for decryption of cipher text, formed by two steps, i.e. (1) Similar bit exchange operation and, (2) Then byte-wise rotate left operation.

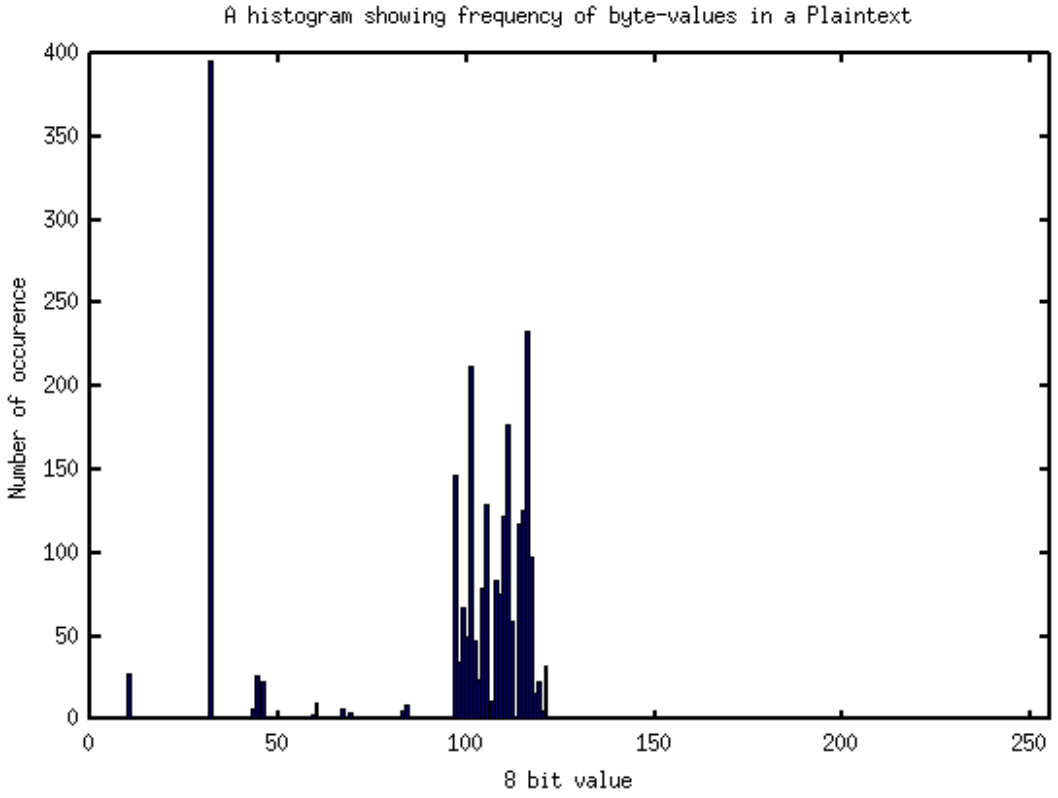
Step.7 Repeat the process (i.e. go to step (4) until the whole plaintext/ ciphertext is encrypted or decrypted.

3. SIMULATION RESULT

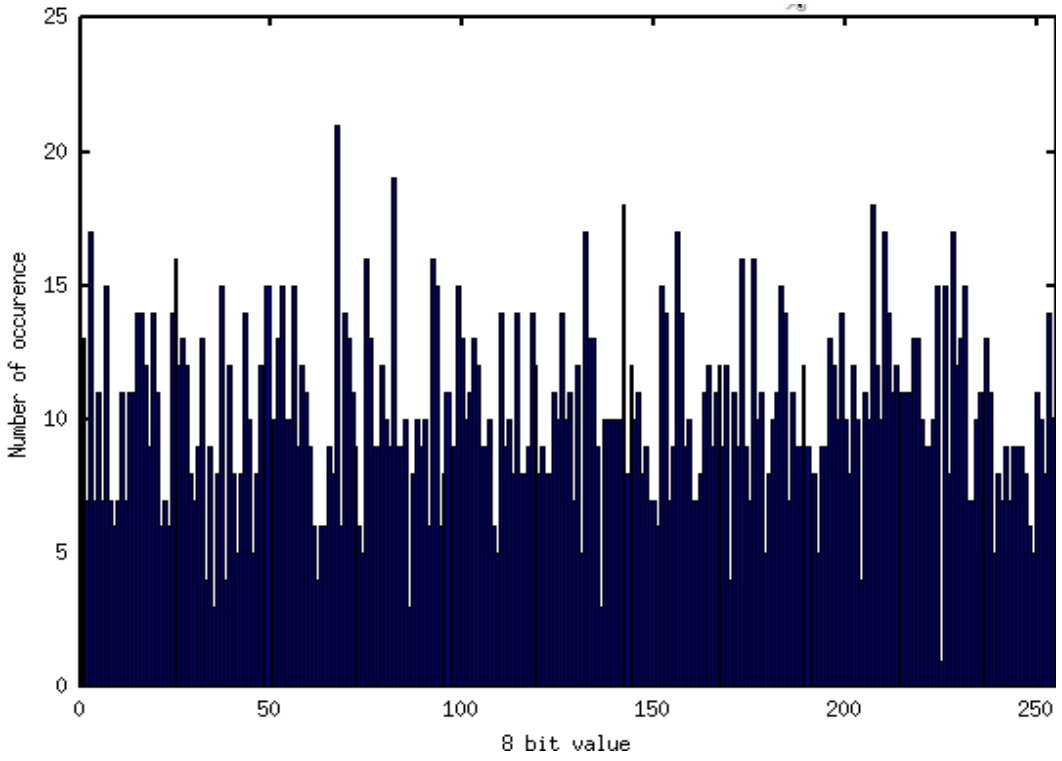
For this proposed algorithm the cipher block chaining (CBC) mode is used. A secret key (K) = $(a1b2c3d4e5f6abcdef7890abcdef1234)_{16}$ was taken and for plaintext, a simple .txt (text file) of size 2.5 kb was taken. Results are show in above Fig.2 (a, b, c) spike like modal shows frequency of occurrence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

Confusion Effect: For confusion effect of the proposed cryptosystem, the plaintext (P) = "Formatting Numbers with

C++ Output Stream" and the ciphertext (E(P,K)) generated by different cryptosystems for was plotted which is shown in below Fig.3 (a, b, c). Fig.3 (a) represents a histogram showing the frequency of occurrence of byte-value in Plaintext. While, Fig.3 (b, c), represent the frequency of occurrence of byte-value in cipher text generated by proposed cryptosystem and Xiang's cryptosystem, respectively. Plaintext and ciphertext 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.

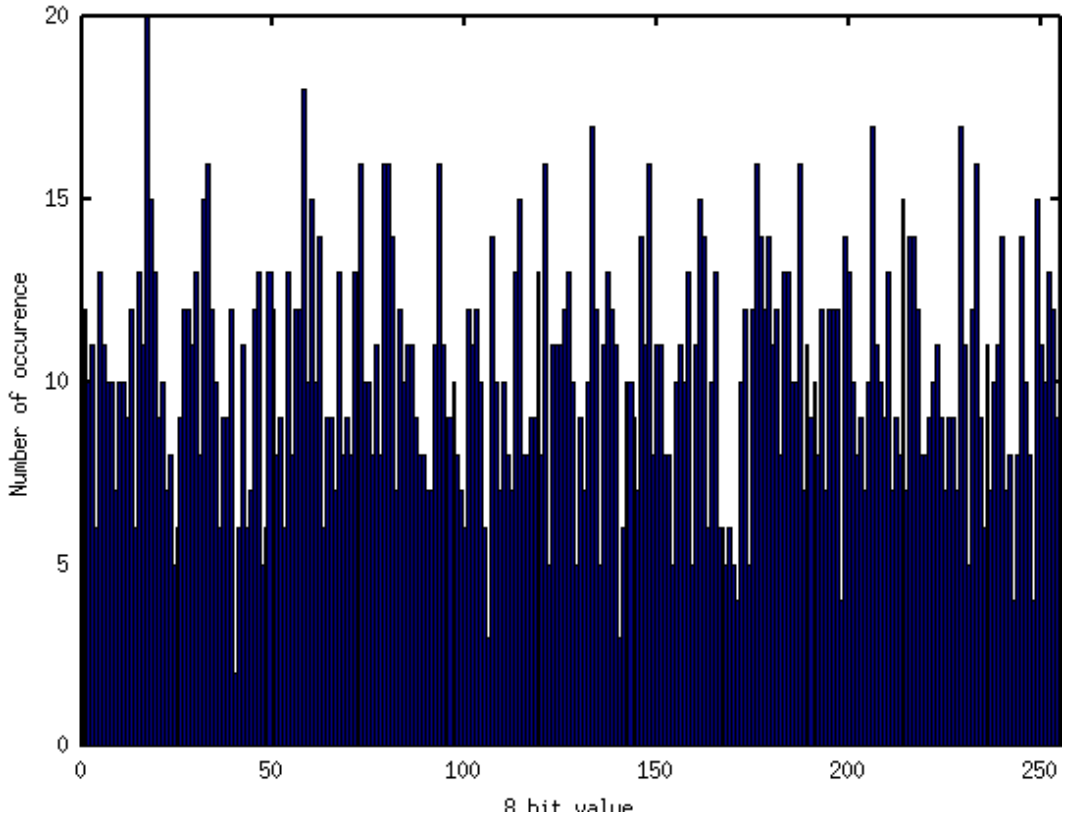


a)

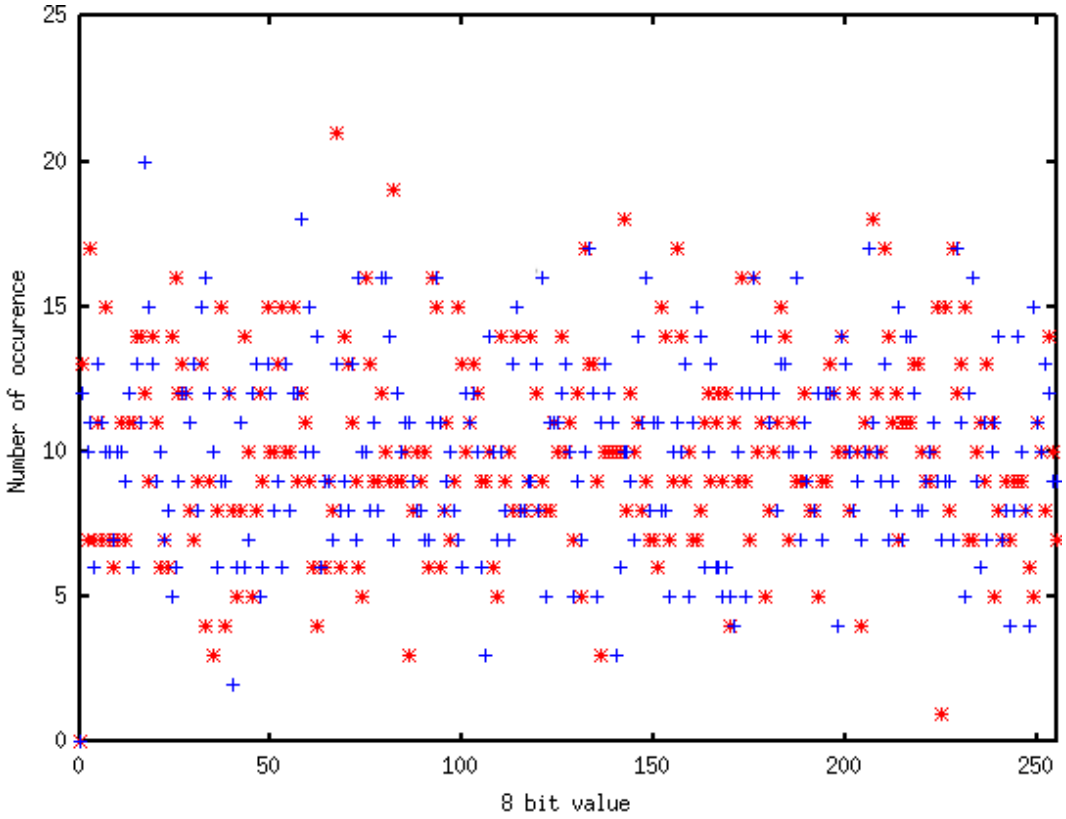


b)

Figure.2 (a) Distribution of plaintext of a 2.5kb .txt file, (b) Distribution of ciphertext using the proposed cipher,

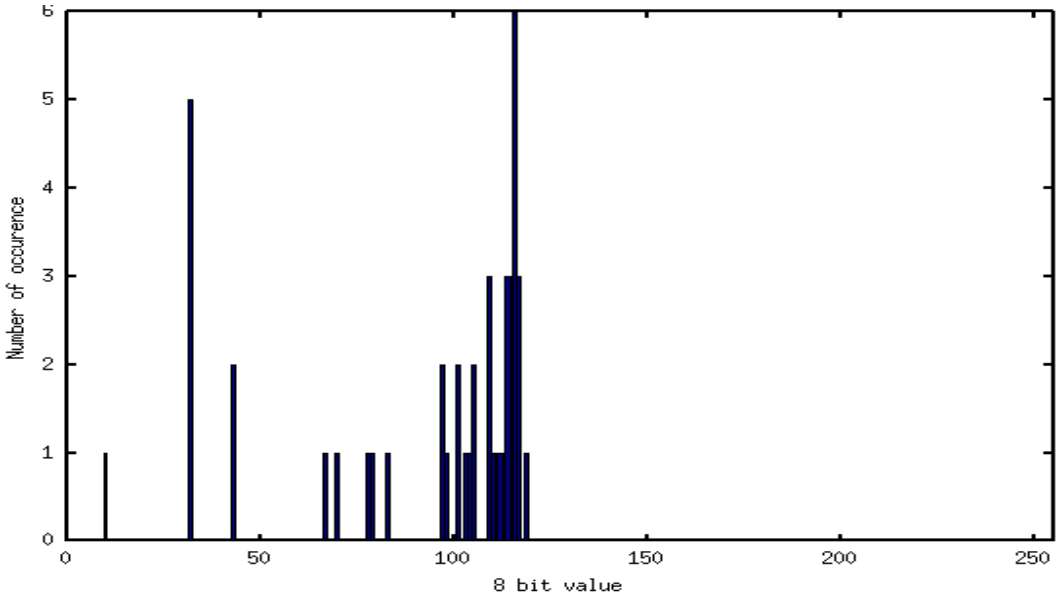


c)

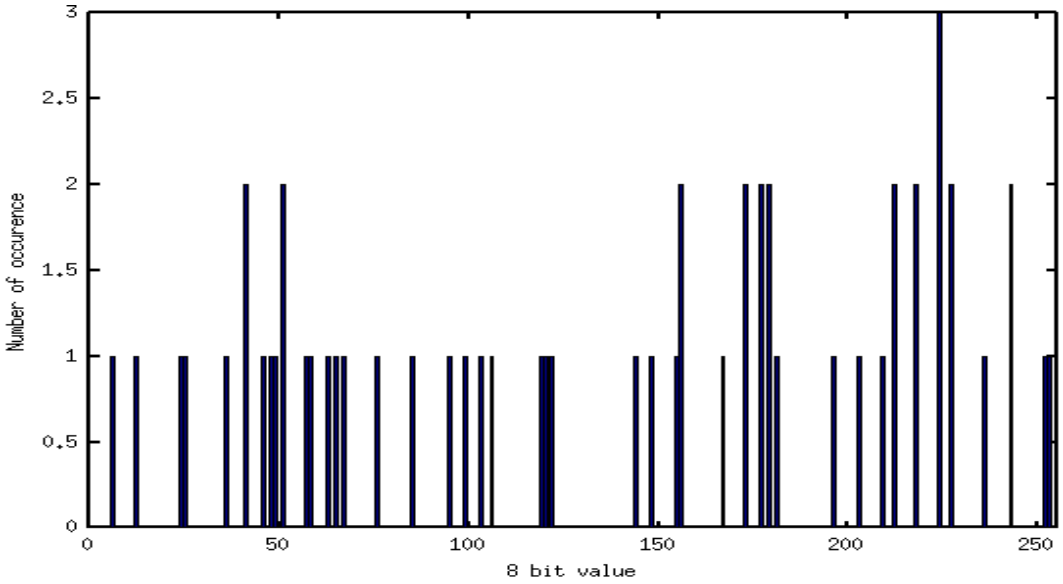


d)

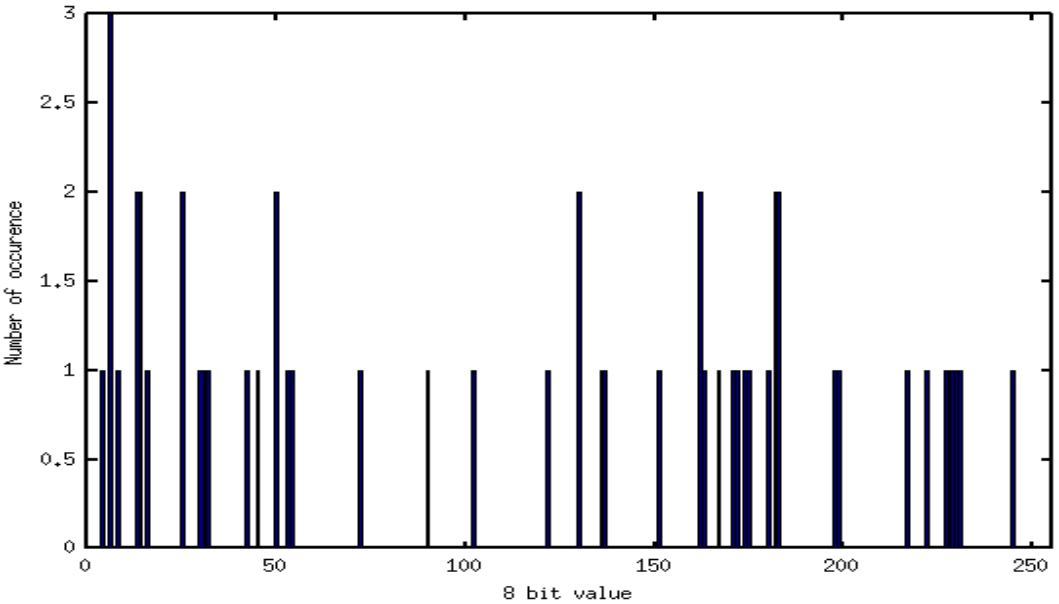
Figure .2 (c) Distribution of ciphertext using Xiang's cipher, (d) Plot of ciphertext using the proposed cipher ('*' in red) vs. Xiang's cipher ('+' in blue).



a)



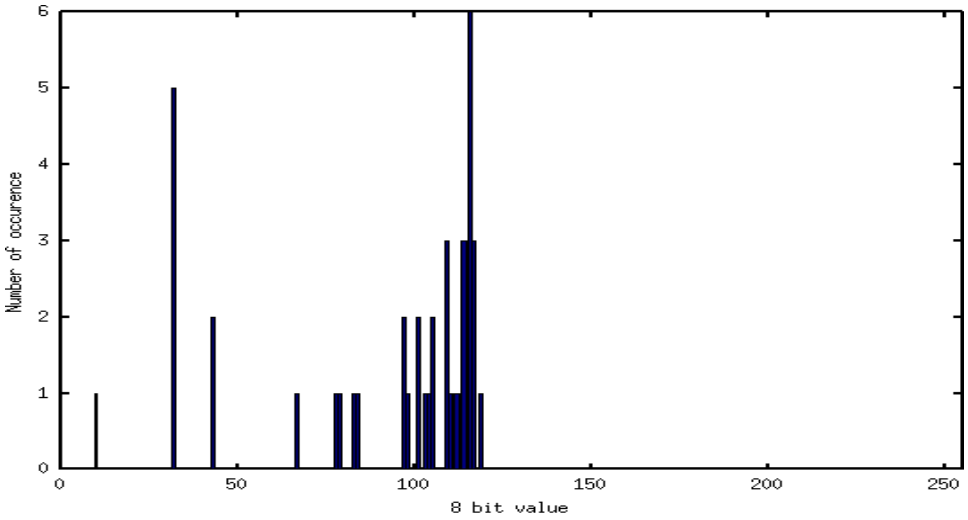
b)



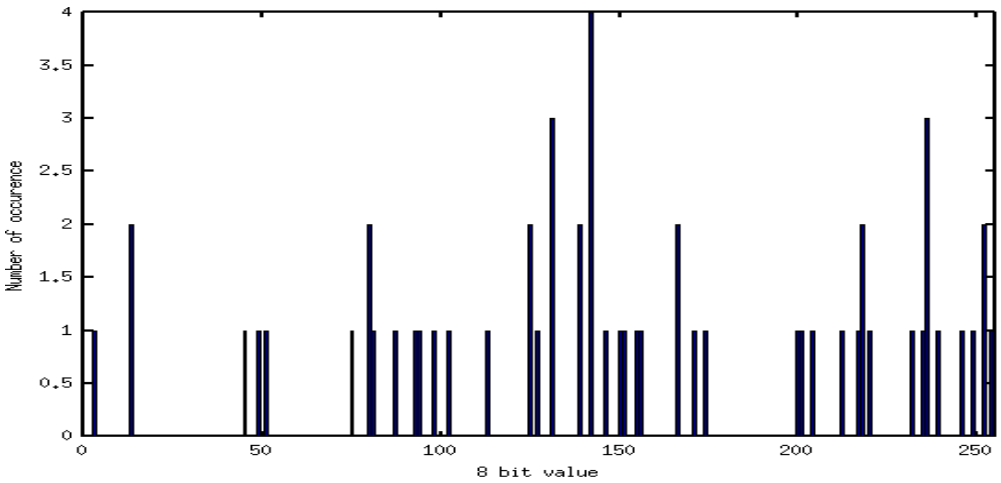
c)

Figure.3 Confusion effect in cipher generated by both systems: (a) Distribution of plaintext (P), (b) Distribution of ciphertext generated by proposed cryptosystem, (c) Distribution of ciphertext generated by Xiang's cryptosystem.

a)



b)



c)

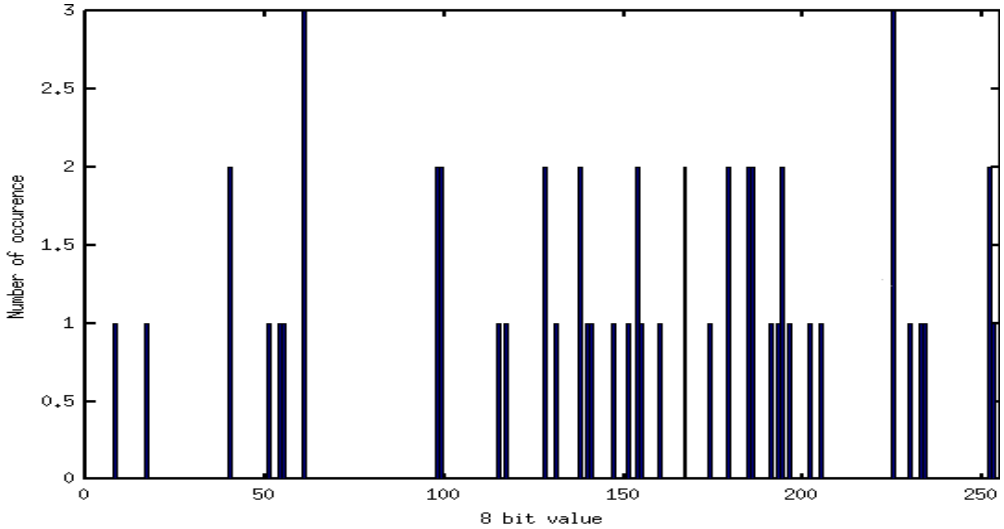
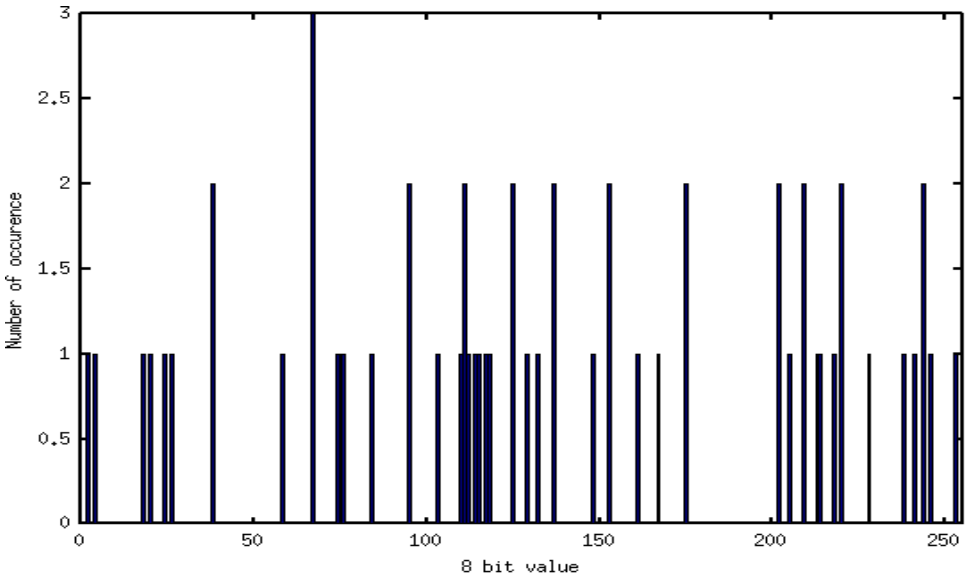
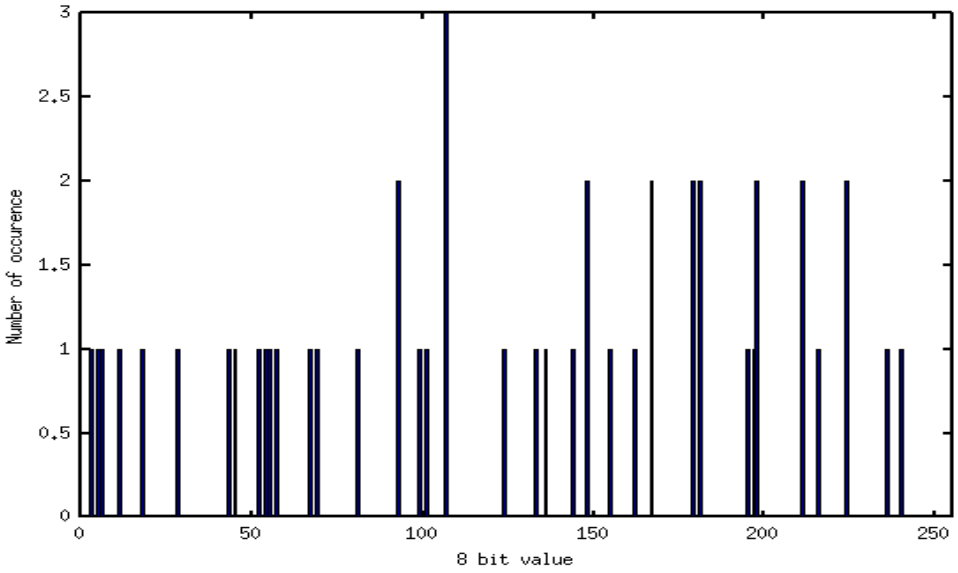


Figure.4 Diffusion effect in cipher when plaintext changed: (a) distribution of plaintext (P_0), (b) distribution of ciphertext generated by proposed cryptosystem, (c) distribution of ciphertext generated by Xiang's cryptosystem;



d)



e)

Figure.4; Diffusion effect in cipher when key (K_0) changed: (d) distribution of ciphertext generated by proposed cryptosystem, (e) distribution of ciphertext generated by Xiang's cryptosystem

Diffusion Effect: Now we change first character of plaintext from 'F' to **'T'**, let P_0 be the new plaintext. On changing the first character of the plaintext there will be always be a different ciphertext because of the cipher block chaining (CBC) mode used in both systems. The diffusion effects when plaintext is changed are demonstrated from Fig.3 (a, b, c) and Fig.4 (a, b, c). On changing the plaintext there is slight variation in the plot of plaintext (P_0) shown in Fig.4 (a) which is not even visible, but due to this change a large variation is observed in the ciphertext shown in Fig.4 (b, **c).**

Then, we change one hexadecimal number of (K) from 8 to F, here we are replacing 'a' with 'f' ((K) = ('a'1b2c3d4e5f6abcdef7890abcdef1234)$_{16}$) and let the new key be K_0. Both cryptosystems shows sensitivity to the secret key (k), but on changing the secret key slightly, Xiang' cryptosystem, show even distribution. Fig. 4(e) reveals that a little change in secret key leads to significant difference in ciphertext. In proposed crypto system, distribution and difference of ciphertext are uneven therefore when there is slight change in secret key, major difference in ciphertext is observed, shown in Fig.4 (d). From Fig.3 (b, c) and Fig.4 (d, e) diffusion effect in cipher when key (K_0) changed are demonstrated.

4. SECURITY ANALYSIS

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

By expanding the block size of plaintext/ciphertext and the precision of chaotic variable to 64 bits, much larger space (2^{64}) for the plaintext/ciphertext in a block as well as the initial condition of the chaotic map are available and this improvement gets rid of the brute-force attack that can serve as a foundation for further cryptanalysis [1]. Also X_0 and Y_0, initial conditions of the two logistic maps cannot be recovered even if they are known, as initial conditions are determined by key dependent transformations. Many chaotic cryptosystems do not possess any confusion or diffusion operation within the block. In the system permutation operation is included to provide more confusion or diffusion operation within the

block. s(•) is both plaintext and key dependent permutation operation in this proposed algorithm.

Plaintext attack can easily derive the value of single chaotic variables used to encrypt each block in Pareek's cryptosystem, these values are critical to deduce the key. This problem of the leakage of the encryption formula (7) was removed by Xiang et al. In Xiang's system initial values and updating procedures are key dependent and ciphertext dependent respectively to mask the plaintext, therefore only the value of $X_b \oplus Y_b$ one can obtain, but individually X_b or Y_b are not available to the attacker. And to improve the performance of the cryptosystem, Xiang et.al also removed the redundant operations present in the system, which contribute little to the security; this improves the encryption/decryption speed [1].

In this proposed scheme, the two logistic maps 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 ciphertext present in the Xiang' 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 in Xiang's scheme. In this improved scheme sensitivity to the secret key and uneven distribution of chaotic variable generate a ciphertext, 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. 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, on 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 four parts A_1, A_2, B_1, and B_2 are exactly identical, then initial conditions of chaotic maps becomes zeros and then under this condition no valid chaotic iterations exist.

6. CONCLUSION

On the basis of the "An improved chaotic cryptosystem with external key" by T. Xiang et al., security of the cryptosystem was improved in this scheme. A generalized description of Xiang's cryptosystems is given here and their weaknesses an also their solution to provide more security. Both proposed and Xiang's cryptosystem have same size of plaintext and ciphertext and size of ciphertext generated by both systems are similar and their encryption times are also same. From the above analyses, more secure cryptosystem is proposed. For this secure scheme, two logistic maps are used instead of two skew tent maps in order to obtain chaotic sequences with improved cryptographic feature. All these advantages make this more secure cryptosystem for the use information transmission over insecure channel and secure application.

7. ACKNOWLEDGMENTS

I am thankful to my supervisor Mrs. Madhu Sharma Assistant Professor of the Division of Computer Science and Engineering and other faculty members for giving me an opportunity to learn and to complete this paper.

8. REFERENCES

[1] 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

[2] Pareek NK, Patidar V and Sud KK, "Discrete chaotic cryptography using external key", Phys Lett A, 2003, 309:75–82.1886

[3] Pareek NK, Patidar V and Sud KK. "Cryptography using multiple one-dimensional chaotic maps", Commun Nonlinear Sci Numeri Simul, 2005, 10:715–23.

[4] Baptista MS, "Cryptography with chaos", Phys Lett A, 1998, 240:50–4.

[5] Shannon CE, "Communication theory of secrecy systems", Bell Syst Tech J, 1948, 28:656 715.

[6] 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

[7] Alvarez G, Montoya F, Romera M and Pastor G, "Cryptanalysis of a discrete chaotic cryptosystem using external key", Phys Lett A, 2003, 319:334–9.

[8] 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.

[9] Wong WK, Lee LP and Wong KW, "A modified chaotic cryptographic method", Phys Lett A, 2001, 138:234–6.

[10] B.R.Ivan, S.D.Dhodapakar and Q.V.Lavande, "Chaos based Cryptography". Newsletter No. 258, July 2005.

[11] Alvarez G and Shujun Li. "Some Basic Cryptographic Requirements for Chaos-Based Cryptosystems".

[12] David Arroyo1, Gonzalo Alvarez1, and Veronica Fernandez, "On the inadequacy of the logistic map for cryptographic applications".

[13] William Stallings "Cryptography and Network Security Principles and Practices", Fourth Edit