2-Step Logistic map Chaotic Cryptography using Dynamic Look-up Table

Yamini Goyal
M.Tech CSE
RCEW, Jaipur

Geet Kalani
Assistant Professor
RCEW, Jaipur

Shreya Sharma
Assistant Professor
RCEW, Jaipur

ABSTRACT
Encryption is to reorganize the message into discrepancy form so that the message is keep secret. The goal of encryption is to give an easy and inexpensive means of encryption and decryption to all authoritative users in possession of the suitable key and difficult and expensive means to estimate the plain text without use of the key. The Baptista proposed a Chaotic Encryption technique, which seems to be much better than traditional encryption methods used today. Chaotic encryption is the new trend of cryptography. It makes use of chaotic system properties such as sensitive to initial condition and lot of information. It is possible to encrypt a message (a text composed by some alphabet) using the Ergodic property of the simple low-dimensional and chaotic logistic equation. But it still has several problems, such as slow in speed and suffering from floating point operations and has less security. This paper is to overcome these problems with dynamic loop up table.

General Terms
Ergodic property, Security, Chaotic Cryptography.

Keywords
Encryption, Decryption, Cryptography, Chaotic cryptography, logistic map, look up table.

1. INTRODUCTION
Chaos is the set of disordered states. When chaos is used in the secret writing it is called as chaotic cryptography. Chaotic cryptography is the excitatory research area to develop a fast and secure cryptosystem. In recent years the use of chaos in cryptography attracted the researcher, mathematician and scholars to replace the conventional cryptographic algorithms with the chaotic cryptographic schemes. The chaotic systems and cryptographic algorithms have many similarities that make it possible to encrypt the information using the chaos that is also randomized. In last two decades chaos is used to design the secure communication in two ways. First is secure analog communication and second is digital chaotic cryptosystem. This scheme describes the digital chaos only and digital chaos is used as the chaotic cryptography.

Cryptography is a mathematical formulation to perform the secret writing. There are two type of cryptographic schemes based on the use of keys as symmetric key cryptography and asymmetric key cryptography. Based on the size of plain text processed at a time, cryptography has two types as stream cipher and block cipher. In this symmetric stream cipher using chaos (Chaotic stream cipher) is mainly focused.

2. RELATED WORK
In 1998, a scheme was given by Baptista [6] based on ergodic chaos cryptographic property of symmetric encryption. This property shows the similar allotment for any input for unchanging control parameters. The initial seed or control parameters were utilized as a secret key in all the above chaotic cryptosystem [6, 21]. This scheme provides a logistic map as a chaotic source. Here logistic map is divided that range different output in different interval. Consider a plain text having N different characters set$\{C_{a1},C_{a2},...C_{aN}\}$, use a one to one onto mapping $f_N : X_t = \{X_1,X_2,...,X_N\} \longleftrightarrow A_t = \{Ca_1,Ca_2,...,Ca_N\}$ to associate the N different $\in$ intervals with N different characters. Given a plain text $T = \{t_1,t_2,...,t_i,...\}(t_i \subset A_t)$.

In 2001 method given by Baptista chaotic cryptographic scheme was examined by Li et. al. [11]. These systems were elevated to a susceptible behavior analysis attack and these parameters used in that method are guess by intruder. The possible type of attacks in chaotic cryptosystem is cipher text only attack, chosen cipher text attack, chosen plain text and known plain text are possible [11]. After examined it, they planned to use complex mapping rather than simple mapping to increase security.

In 2002, a modified version of Baptista [6] chaotic cipher given by K.W. Wong [21] and compare this method to Baptista's method. After examined it he found that the method given by Baptista is very slow by doing many comparison and this scheme was unsecure to access. K.W. Wong planned a new method with the look-up table. In this method table was updated vigorously updated via exchanging the related symbols between two intervals [21]. Look-up table values are initializing to character ASCII values. The look-up table will be updated after encrypting and decrypting each block of plain text. So plain text will update after each step and it is more secure. By using this scheme, weakness of the previous formula can be removed which have been updated. By updating the formula next position of the symbols is about two times mod N of previous index. So it is typical for intruder to access the next position of characters.

In 2003 Encryption scheme of Baptista were examined by Alvarez et. al. [2]. after examined he analyze that Baptista's system is weak cryptosystem because in this he found three types of cryptographic attacks i.e; one-time pad attack (chosen plain text), entropy attacks and key recovery attacks [2].

In 2005, Pareek et. al. [13] designs a new symmetric encryption system using multiple chaotic sources. They proposed that instead of using one chaotic map multiple one dimensional chaotic maps [13] as logistic map, cubic map, sine map, exponential map, tent map etc. can be used. In this cryptosystem they use three look-up tables as first map table that has control parameter and map number, second for map number and initial condition and third for character block number, map number and associated number of iterations for iterating map [13]. After getting the all the associated information, iterate the map for the associate fix number of iteration and then get cipher text for each plain character using Eq. [13] $C_i = (P_i + ⌊X_{new} * 10^5⌋) \bmod 256$ The plain text from

cipher text is taken as Eq. [13] $P_i = (C_i + 256 - \lfloor X_{new} * 10^5 \rfloor) \bmod 256$.

In 2006, Xiao et. al. [22] simplified the updating formula as Eq. $2 * I \bmod N \leq J \leq 2 * I + 1 \bmod N$ by using dynamic look-up table of Wong [21] here J is used as next index position of I^{th} symbol and N is the plain text space.

In addition there are third, fourth and fifth digits of the current value of x are included for dynamic updating of look-up entries. These could enhance security of dynamic look-up table and Baptista's algorithm efficiently.

In this case I^{th} indexed entry will be interchanged with J^{th} entry using Eq. J = (I + 3rd digit * 100 + 4th digit * 10 + 5th digit) mod N Here N is the total possible symbols in the plain text.

In 2007 Wei et. al [20] analyzed the proposed scheme and observed that in proposed scheme the dynamic updating mechanism is vulnerable because the updated values for two different plain text are same for the same key means it is only dependent on key [20]. It is vulnerable to known plain text attack. They proposed a remedy for it that updating of seed values, number of required iteration etc. should be dependent on the plain text.

In 2008, Ariffin et. al. [5] proposed a chaotic encryption system that was modified version of the Baptista's cryptosystem [6]. In this cryptosystem they use a secret invertible matrix with the original Baptista's cryptosystem. The encryption procedure was as: Get the total possible symbols in plain text. For example S4 = {s1,s2, s3, s4} and take their decimal representation and associated interval as in mapping table 3.1 [5] .(a) Take the plain text of length m as P = s1, s3, s2, s4, s2, s1, s4, s3. (b) Invertible matrix key A and A^{-1} of K × K where m/k. (c) Divide the plain text into k length blocks and get distorted plain text using $Dp = A * P \bmod$ Here N is the possible symbols in the plain text or phase space.

In 2009, Rhouma et. al [15] analyzed the modified Baptista type chaotic cryptosystem using shared matrix secret key. They observed that it was a not invertible chaotic encryption scheme. So it doesn't satisfy the basic requirement of cryptography that the encrypted message should be decrypted. They observed that it was also suffered with partial key recovery attack [5]. They proposed it in invertible form as Divide plain text into different vector sets P_j of equal length $k \varepsilon N$ where j = 1,2,...,m/k and m is length of plain text.

3. PROBLEM STATEMENT

Baptista's type symmetric encryption schemes have less key space that is vulnerable to brute force attack. The behavior of map gets varied with the change in values of control parameter.

This behavior makes it more vulnerable to behavior analysis attack. In addition, these are also unsecured, as its present value acts as a seed for next condition. This makes it easy for an adversary to get into the next condition, as it has the present initial condition.

To overcome this problem the proposed scheme has large key space of 160 bits and the value of control parameter is fixed. These resist the proposed scheme against the brute force attack and analyzing the behavior. In this scheme two two-step logistic maps are used and the next initial condition is also updated to make it independent from the previous value of the seed.

This scheme also uses a fully updated dynamic look up table, in which the entries as well as the associated interval are also updated for every encryption and decryption operation for a character. The update in the dynamic look up table is done using second logistic map using the previous character index value to make it dependent on the plain text as well as on key.

4. PROPOSED WORK

Encryption scheme is used as :

1. Take a 160 bit key as $K_0 K_1 K_2 \ldots\ldots\ldots K_{159}$

2. Consider two logistic map in two steps [14] initially for encrypting data and secondly for updating the look-up table

$$x_n = r_1 * x_{n-1}(1 - x_{n-1})$$

$$x_n = b_1 * x_n + (1 - b_1) * x_{n-1} \quad \text{(I)}$$

$$y_n = r_2 * y_{n-1}(1 - y_{n-1})$$

$$y_n = b_2 * y_n + (1 - b_2) * y_{n-1}$$

3. Fix control parameter r between 3.86 to 4.

4. Take keys as Eq

$$x_0 = \sum_{i=0-63} k_i / 2^{i+1}$$

$$y_o = \sum_{i=32-95} k_i / 2^{i-31} \quad \text{(II)}$$

$$b_1 = \sum_{i=74-127} k_i / 2^{i-73}$$

$$b_2 = \sum_{i=96} k_i / 2^{i-95}$$

5. Remaining 32 bits of key will be used as Eq

$$KU_1 = k_{128} \ldots\ldots\ldots K_{135}$$

$$KU_2 = k_{136} \ldots\ldots\ldots K_{143} \quad \text{(III)}$$

$$KU_3 = k_{144} \ldots\ldots\ldots K_{151}$$

$$KU_4 = k_{152} \ldots\ldots\ldots K_{159}$$

6. After encrypting the block of data update the key by discarding left 16 bit x_0, then add the key KU_1 and KU_2 at the last of new x_0 and again get the new float initial condition x_0.

Finally add this x_0 to second logistic map output and build a new initial condition for the first map. Left 16 bit y_0 bit is discarded and the key KU_3 and KU_4 are added at the last of new x_0. After all for the second map new initial condition for y_0 are retrieved.

7. Following parameters are updated as Eq.

$$KU_1 = KU_1 \oplus KU_2 \oplus KU_4$$

$$KU_2 = (\sim KU_1) \oplus KU_3 \wedge KU_4$$

$$KU_3 = KU_2 \vee KU_3 \oplus (\sim KU_4) \quad \text{(VI)}$$

$$KU_4 = KU_1 \vee (\sim KU_2) \vee KU_3$$

8. The look-up table is updated by interchanging the entries and getting new associative intervals for symbols depending upon second map value received by iterating its value number of times as the symbols in previous position as: j^{th} entry will be interchanged with i^{th} entry using updating formula as Eq.

$$j = ((i+(x-x_{min}/e*e_2)*N) \bmod N \qquad (V)$$

here,

e: interval

e_2: the current value of initial parameter of second map

N: number of symbols in the plain text

Thus the associated interval will be

$$[x_{min} + i *e + e_2, x_{min} + (i + 1)* e + e_2)]$$

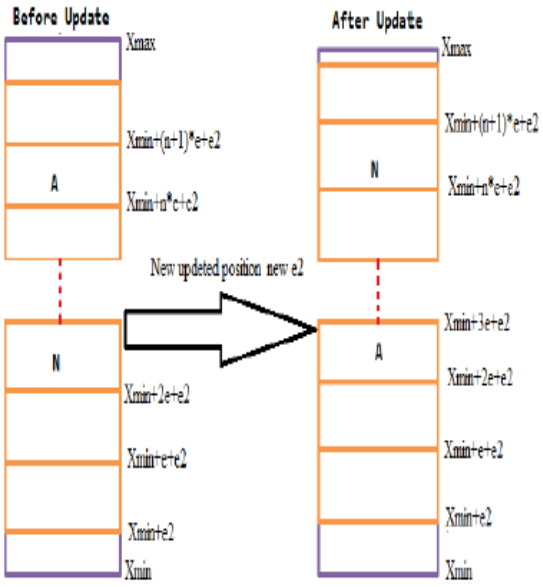

Fig 4.1 Lookup table

9. Dynamically updated look-up table is shown in the figure 4.1 which is enough secure here in this table there are N+1 intervals where N represents total number of symbols in the plain text. Its values are calculated as Eq.

$$E = (X_{max} – X_{min}) / (N+1) \qquad (VI)$$

10. The next procedure is similar to original Baptista chaotic cryptosystem as shown in the figure 4.2

11. The process of decryption is similar to encryption as shown in figure 4.2

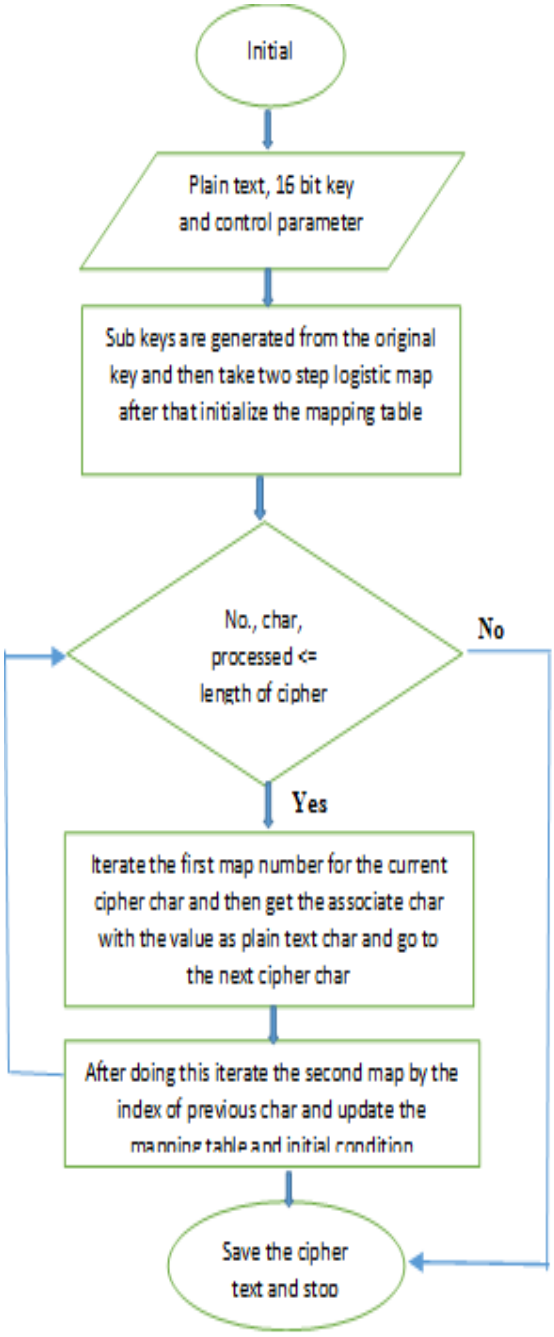

Fig 4.2 Proposed encryption process

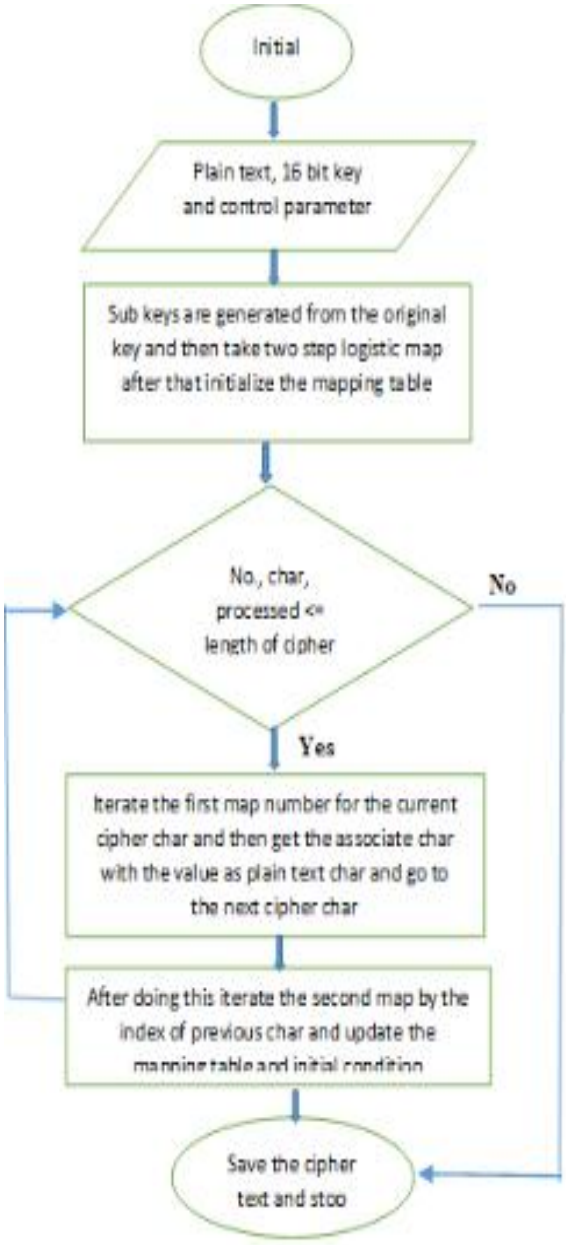

Fig 4.3 Proposed decryption scheme

5. IMPLEMENTATIOB & RESULT

Implementation of proposed scheme performed using Java programming language. The implemented proposed scheme using Java development kit (jdk 1.7.0) on windows platform. System configuration consists of Intel Pentium dual core (1.86 GHz), CPU with graphic and 2 GB RAM. System has Windows 7 ultimate operating system installed. The implemented proposed scheme include three other chaotic cipher as Baptista's chaotic cipher, Dynamic-lookup table cipher and improved dynamic lookup table cipher for comparison of results. Different initial conditions, different control parameter, and feedback factor values with different plain text has been used for the testing purpose of the propose scheme. Then some same type of values is taken for proposed scheme as well as other implemented chaotic cryptographic schemes for comparison of results and performance. As the proposed scheme has 160 bit long key so it requires 2^{160} total number of key combination that will years to test all key combination. So it is resist against brute force attack.

This scheme shows that the new position of the symbols is purely dynamic so it has a secure dynamic lookup table. The results also show that the initial condition in proposed scheme is not same as previous iterated value. If a initial condition is known to the adversary then it will be not use able to him further because the next initial condition in dependent on second logistic map, input plain text as well as the renaming sub-keys. So adversary can't get the further exact plain text.

5.1 PERFORMANCE ANALYSIS

The time required to perform encryption and decryption operation is basis for performance analysis, Here selected key values as "qwertyuiopasdfghjklz" and control parameter as r = 3:997654321. Similarly in other schemes for initial condition x_0 = 0:5432280925102532 and control parameter r = 3:997654321. For implemented proposed scheme calculated the encryption and decryption time by using ten string of different length as plain text input.

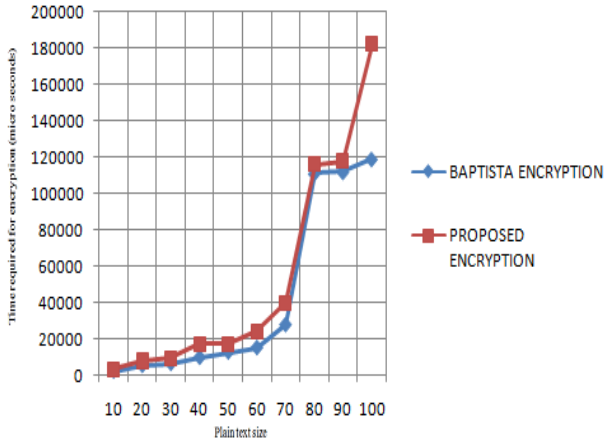

Fig4.4 Encryption time comparison

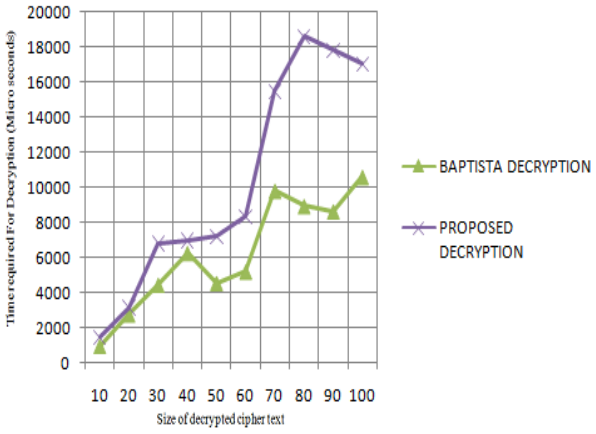

Fig 4.5 Decryption time comparison

6. ACKNOWLEDGMENTS

This work was supported by the Research Lab of Computer Science & Engineering Department at RCEW Jaipur. We would like to thank anonymous reviewers who helped us in giving comments to this paper.

7. CONCLUSION

With the advent of technology chaotic cryptography is gaining a great attention by researchers all around. The ease of having a secure, randomized and fast cryptosystem has developed to great extent. Here with this proposed scheme time for

encryption and decryption operation has been reduced. The particular scheme is resistant to key recovery attack, Brute−force attack and behavior analysis attack. The data confidentiality, security, integrity and authenticity are maintained by using distance parameter and execution time. Here Hamming code distance shows more avalanche effect on comparison with existing system. Time required performing the encryption and decryption operation is the basis for analysis of performance. Thus a secure and fast cryptosystem is used in order to secure our information and data security. The proposed scheme has been tested only for text information. The testing via other type of information like images, videos etc can be implemented in future using chaotic hash function.

8. REFERENCES

[1] Logistic map bifurcation diagram http://hyperchaos.wordpress.com/2011/04/27/logistic-map-bifurcation-diagram/, 2011.

[2] G Alvarez, F Montoya, M Romera, and G Pastor. Cryptanalysis of an ergodic chaotic cipher. Physics Letters A, 311(23):172 - 179, 2003.

[3] G. Alvarez, F. Montoya, M. Romera, and G. Pastor. Cryptanalysis of dynamic look-up table based chaotic cryptosystems. Physics Letters A, 326(34):211 -218, 2004.

[4] Gonzalo Alvarez and Shujun Li. Some basic cryptographic requirements for chaos-baces cryptosystem. International Journal of Bifurcation and Chaos, 16(08):2129-2151, 2006.

[5] M.R.K. Ariffin and M.S.M. Noorani. Modified baptista type chaotic cryptosystem via matrix secret key. Physics Letters A, 372(33):5427 - 5430,2008.

[6] M.S. Baptista. Cryptography with chaos. Physics Letters A, 240(12):50 -54,1998.

[7] William Ditto and Toshinori Munakata. Principles and applications of chaotic systems. Commun. ACM, 38(11):96-102, November 1995.

[8] G. Cairns G. Davis J. Banks, J. Brooks and P. Stacey. On devaney's definition of chaos. The American Mathematical Monthly, 99(4):332-334, April 1992.

[9] James A. Yorke Kathleen T. Alligood, Tim D. Sauer. Chaos : an introduction to dynamical systems. Springer, New York, 2000.

[10] L. Kocarev. Chaos-based cryptography: a brief overview. Circuits and Systems Magazine, IEEE, 1(3):6{21, 2001.

[11] Shujun Li, Xuanqin Mou, and Yuanlong Cai. Improving security of a chaotic encryption approach. Physics Letters A, 290(3-4):127{133, 2001.

[12] G. Millerioux, J.M. Amigo, and J. Daafouz. A connection between chaotic and conventional cryptography. Circuits and Systems I: Regular Papers, IEEE Transactions on, 55(6):1695{1703, 2008.

[13] N.K. Pareek, Vinod Patidar, and K.K. Sud. Cryptography using multiple one-dimensional chaotic maps.Communications in Nonlinear Science and Numerical Simulation, 10(7):715 { 723, 2005.

[14] Mamta Rani and Rashi Agarwal. A new experimental approach to study the stability of logistic map. Chaos, Solitons Fractals, 41(4):2062 { 2066, 2009.

[15] Rhouma Rhouma, Ercan Solak, David Arroyo, Shujun Li, Gonzalo Alvarez, and Safya Belghith. Comment on modi ed baptista type chaotic cryptosys-tem via matrix secret key [phys. lett. a 372 (2008) 5427]. Physics Letters A, 373(37):3398 { 3400, 2009.

[16] B. Schneier. Applied cryptography: protocols, algorithms and source code in C. John Wiley and Sons, New York, 1995.

[17] William Stallings. Cryptography and network security : principles and prac-tices. Pearson Education Dorling Kindersley, Delhi, 2006.

[18] T. Stojanovski and L. Kocarev. Chaos-based random number generators-part analysis [cryptography]. Circuits and Systems I: Fundamental Theory and Applications, IEEE Transactions on, 48(3):281{288, 2001.

[19] Jun Wei, Xiaofeng Liao, Kwok wo Wong, and Tsing Zhou. Cryptanalysis of a cryptosystem using multiple one-dimensional chaotic maps. Communications in Nonlinear Science and Numerical Simulation, 12(5):814 { 822, 2007.

[20] K.W Wong. A fast chaotic cryptographic scheme with dynamic look-up table. Physics Letters A, 298(4):238 { 242, 2002.

[21] Di Xiao, Xiaofeng Liao, and Kwok-Wo Wong. Improving the security of a dynamic look-up table based chaotic cryptosystem. Circuits and Systems II: Express Briefs, IEEE Transactions on, 53(6):502{506, 2006.

[22] Kavita Chaudhary, Shiv Saxena. New Encryption Method Using Chaotic Logistic Map. Volume 4, Issue 8, August 2014.