I. J. Computer Network and Information Security, **2015, 5, 34-40**
Published Online April 2015 in MECS (http://www.mecs-press.org/)
DOI: 10.5815/ijcnis.2015.05.05

Improving Security of the Baptista's Cryptosystem Using Two-step Logistic Map

Balram Nitharwal
Dept. of Computer Science and Engineering
Central University of Rajasthan, INDIA
Email: nit.balram@gmail.com

Mamta Rani
Dept. of Computer Science
Central University of Rajasthan, INDIA
Email: mamtarsingh@curaj.ac.in

Hukam Chand Saini
Dept. of Computer Science and Engineering
Central University of Rajasthan, INDIA
Email: hukamchand@curaj.ac.in

***Abstract*—**Over last 3 decades, many cryptography algorithms based on chaos have been proposed that are very fast in computation. Chaos is used for secured communication in two ways as analog secured communication and digital chaotic ciphers. This paper is mainly focused at digital chaotic cryptosystem. In symmetric cryptosystems, same key is used for both encryption and decryption purpose. In 1998, Baptista gave the most used symmetric cryptosystem based on Ergodic property of logistic map. Later on, many refinements were done in Baptista's algorithm. By going through later proposed refinements in this cryptosystem, some flaws are observed. Proposed scheme has a two-step logistic map that is a feedback mechanism using an extra variable to come over these flaws. At last, there is comparison between proposed scheme and other version of Baptista type cryptosystem, which shows that the proposed scheme is better than previous ones and it is resist against behavior analysis attack and partial key recovery attack.

***Index Terms*—**Chaos, Baptista's Cryptosystem, Ergodic, Two-step logistic-map, Secured communication**.**

I. Introduction

In last 4-5 decades, chaos theory has been developed by the efforts of many researchers by analyzing the behaviour of dynamical systems that are deterministic in nature but fully unpredictable. These are behaviourally random look like systems. Chaos theory has many applications in the field of physics, mathematics, chemistry, engineering etc [6]. Equally chaos is also used in random number generation [13], hash function [14] and cryptography [7], [9] etc. Chaotic cryptography is nowadays thrust area of research in data security (See, for instance, [1]–[10], [12], [15]–[17]).

In last 2-3 decades, many different chaotic encryption schemes have been proposed. The most used symmetric cryptosystem based on ergodic property of chaotic maps was given by M. S. Baptista [5] in 1998. The purpose of this paper is to propose the use of two-step logistic map to enhance the security of Baptista type cryptosystem.

In section II, Baptista's algorithm and concept of dynamic look-up table in context of Baptista's algorithm has been given. Also, two-step logistic map has been described. In section III, improved algorithm has been proposed in section IV, comparison of improved algorithm with previous schemes has been proposed. Finally, the paper has been concluded in Section V.

II. Related Work

In 1998, Baptista [5] proposed a chaotic encryption-decryption scheme using ergodic property of chaos, which attracted the researchers to make a fast and secure chaotic encryption-decryption scheme due to its simplicity and less complex structure. In the literature survey, we observed that first mapping of text characters with real values is done and then the algorithms are applied to encrypt the message. Decryption is performed by iterating map and then corresponding symbol for real values is obtained. The control parameter or initial seed or both were used as a secret key in all these chaotic cryptosystems [5], [16], [17]. Baptista type chaotic cryptographic algorithms covered in literature survey are described in next section.

A. M.S. Baptista's Chaotic Cipher

In 1998, Baptista [5] gave a symmetric encryption scheme based on ergodic property of chaos. In this scheme a logistic map $F : X \rightarrow X$ as $x_n = r * x_{n-1}(1 - x_{n-1})$ [5] is used as chaotic source. The logistic map's output range is divided into intervals $[Xmin, Xmax) \subseteq X$. The number of intervals are S (where S is the number of symbols can be used in plaintext) and the range of each interval is ϵ. So the each interval i is $X_i = [X_{min} + (i - 1) * , X_{min} + i * \epsilon)$, where $\epsilon = (Xmax - Xmin)/S$.

Assume plain text is composed of S different characters $\{C_{a1}, C_{a2} \ldots C_{aS}\}$, use a one to one onto mapping $f_S : X_t = \{X_1, X_2, \ldots, X_S\} \longleftrightarrow A_t = \{C_{a1}, C_{a2}, \ldots, C_{aS}\}$ to associate S different intervals with S different characters.

The procedure of encryption and decryption is as follows:

Given a plain text: $T = \{t_1, t_2. \ldots t_i, \ldots \quad \}(t_i \subset A_t)$.

The secret key: The initial condition x_0 and the control parameter r of Logistic map [5]

Encryption: For the first plain-character t_1: Iterate logistic map from initial condition x_0 to find a chaotic state x_n that satisfies that $x_n = t_1 \rightarrow A_t \rightarrow X_t$, and record the iteration number as the first cipher-text c_1 if recorded value is greater than the base value else the process of iteration will continue till the conditions are satisfied.

For the i^{th} plain-character t_i: Iterate the logistic map using previous x_n as initial seed and find the chaotic state x_n that satisfy that $x_n = t_i \rightarrow A_t \rightarrow X_t$, and record the iteration number as the cipher-text c_i if recorded value is greater than the base value else the iteration process will continue. Perform this process for remaining plain text characters. This will give the cipher text corresponding to the plain text.

Decryption: For each value of cipher text, iterate the logistic map from previous condition and control parameters and get the corresponding plain text character as $x_n = X_t \rightarrow A_t \rightarrow t_i$.

In 2001, Li et. al. [8] analyzed chaotic cryptographic schemes and found that these systems are vulnerable to behavior analysis attack and guess of the initial condition. So in these chaotic cryptosystems all four types of cryptanalysis attack possible as cipher text only attack, chosen cipher text attack, chosen plain text and known plain text are possible [8]. They also proposed that rather than using a simple map a complex map can be used.

Alvarez et. al. [1] examined encryption schemes of Baptista [5]. They found three types of cryptanalysis attack on Baptista's cipher: one-time pad attacks (chosen plain text), entropy attack and key recovery attacks [1]. They proved that it was a weak cryptosystem.

B. K. W. Wong's fast chaotic cryptographic scheme with dynamic look-up table

In 2002, K.W. Wong [16] gave a modified version of Baptista's [5] chaotic cipher. Wong found that Baptista's chaotic cipher was slow due to some extra comparisons and the scheme was not secure. Wong proposed a new scheme with a look-up table that was dynamically updated via swapping the associated symbols between two intervals [16]. Initially the lookup table was initialized according the ASCII values of characters. Update in the look-up table will be performed after each block of plain text encryption and decryption. This scheme has a logistic map as the chaotic source and the initial condition and control parameter of logistic map as the secret key. The dynamic look up table's i^{th} entry will be swapped with j^{th} entry using (1) as.

$$j = \left(i + \frac{X - Xmin}{Xmax - Xmin} * N\right) \; mod \; N \qquad (1)$$

Where X is the current value and N is the number of entries in table. Other process will be same as original Baptista's [5] chaotic cipher.

Alvarez et. al. [2] examined encryption schemes of Wong's[16] look-up table and observed that the attacker can easily get the next position of the symbols without knowledge of the exact current value of X [2].

C. Improving the security of dynamic lookup table

In 2006, Xiao, Liao and Wong [17] worked on dynamic look up table of Wong [16] and found vulnerabilities in the lookup table. They simplified (1) by updating as (2).

$$2 * I \; mod \; N \;\leq \boldsymbol{J} \leq\; 2 * \boldsymbol{I} + 1 \; mod \; N \qquad (2)$$

Where J is the new index position for I^{th} symbol and N is the total number of possible symbols in the plain text.

Further, to enhance the security of dynamic look up table to make Baptista's algorithm more secure, they picked up third, fourth and fifth digit of the current value of X parameter for updating the dynamic lookup table entries [17]. Then I^{th} indexed entry will be swapped with J^{th} entry using (3).

$$\boldsymbol{J} = \left(\boldsymbol{I} + 3^{rd}digit * 100 + 4^{th}digit * 10 + 5^{th}digit\right) mod \; N \qquad (3)$$

Where N is the total number of possible symbols in the plain text. Rest of the process will be same as Baptista's algorithm [5].

D. Two step Logistic map

In 2009, Rani and Agarwal [11] gave a new study of the stability of logistic map, in which they enhanced the capabilities of logistic map via superior iterations. It is a two-step feedback mechanism in which new iterated value of x is calculated using previous two values of x with factor $B \in (0, 1]$ as (4).

$$y_n = r * x_{n-1}(1 - x_{n-1})$$

$$x_n = B * y_n + (1 - B) * x_{n-1}$$

$$\text{where } x \in (0, 1] \text{ and } r \in [3.86, 4) \qquad (4)$$

By using two-step logistic map, factor B also can be a part of the key by which key space will increase the security of such type of chaotic cryptosystems. So in the proposed scheme, we shall use a two-step logistic map to enhance the capabilities of chaotic cryptosystem.

III. Use Of Two Step Logistic Map In Baptista’s Cryptosystem

Baptista’s type symmetric encryption schemes have less key space that is vulnerable to brute force attack. Behaviour of map varies with the change in values of control parameter by which behaviour analysis attack is possible. In addition, these are also insecure, as its present value acts as a seed for next condition. By which an adversary can get all next conditions, if present initial condition is known to him. The proposed scheme is a symmetric encryption scheme.

The scheme is as:

a) Take a 160 bit key as $K_0K_1K_2$.......... K_{159}.

b) Take two logistic maps in two steps [11] as (5) and (6) first for encrypting data and second for updating the lookup table.

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

$$x_n = b_1 * x_n + (1 - b_1) * x_{n-1} \tag{5}$$

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

$$y_n = b_2 * y_n + (1 - b_2) * y_{n-1} \tag{6}$$

c) Fix control parameter r1 and r2 between 3.86 and 4.

d) Take keys values as (7), (8), (9) and (10).

$$x_0 = \sum_{i=0}^{31} k_i \;/2^{i+1} \tag{7}$$

$$y_0 = \sum_{i=32}^{63} k_i \;/2^{i-31} \tag{8}$$

$$b_1 = \sum_{i=64}^{95} k_i \;/2^{i-63} \tag{9}$$

$$b_2 = \sum_{i=95}^{127} k_i \;/2^{i-95} \tag{10}$$

e) Rest 32 bits of key will be used as updating parameters as (11), (12), (13) and (14).

$$KU_1 = K_{128} \ldots K_{135} \tag{11}$$

$$KU_2 = K_{136} \ldots K_{143} \tag{12}$$

$$KU_3 = K_{144} \ldots K_{151} \tag{13}$$

$$KU_4 = K_{152} \ldots K_{159} \tag{14}$$

f) Update the key after encryption of a block of data as

Discard left 16 bit x_0. Then add keys KU_1 and KU_2 at the last of new x_0. Now get the float initial condition x_0 from it and add with second logistic map output. This will be new initial condition for first map.

Discard left 16 bit $y_0$and add the key KU_3 and KU_4 at the last of new x_0. Then get float initial condition y_0 from it for second map.

g) Updating parameter will be updated as (15), (16), (17) and (18).

$$KU_1 = KU_1 \oplus KU_2 \oplus KU_4 \tag{15}$$

$$KU_2 = (\sim KU_1) \oplus KU_3 \wedge KU_4 \tag{16}$$

$$KU_3 = KU_2 \vee KU_3 \oplus (\sim KU_4) \tag{17}$$

$$KU_4 = KU_1 \vee (\sim KU_2) \vee KU_3 \tag{18}$$

h) Update the Look up table via shuffling the entries and get the new associated intervals for the symbols based on second map value by iterating it number of times the symbols previous position and J^{th} entry will be swapped with i^{th} entry using (19).

$$j = \left(i + \frac{x - Xmin}{e * e2} * N\right) mod\ N \tag{19}$$

Where e is interval, e2 is the current value of initial parameter of second map and N is the total number of possible symbols in plain text. The associated interval will be *[Xmin + i ∗ e + e2, Xmin + (i + 1) ∗ e + e2).*

i) In proposed scheme, the Lookup table will be as Fig.1. This is the fully dynamically updated look-up table, which will be the part of security. In this lookup table, there will be *N + 1* interval where *N* is the total number of possible symbols in plain text. So the value of e will be calculated as (20).

$$e = \frac{Xmax - Xmin}{N+1} \tag{20}$$

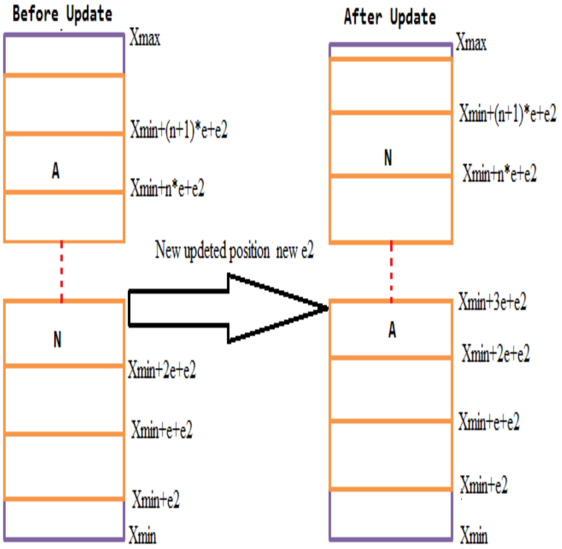

Fig. 1. Fully dynamically updated lookup table

j) Other process will be same as original Baptista’s chaotic cryptosystem. The encryption process can be seen in Fig. 2.

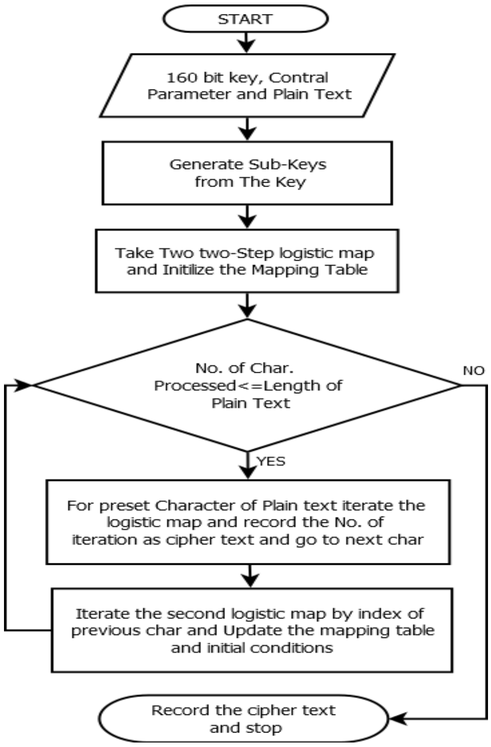
START
160 bit key, Contral Parameter and Plain Text
Generate Sub-Keys from The Key
Take Two two-Step logistic map and Initilize the Mapping Table
No. of Char. Processed<=Length of Plain Text
NO
YES
For preset Character of Plain text iterate the logistic map and record the No. of iteration as cipher text and go to next char
Iterate the second logistic map by index of previous char and Update the mapping table and initial conditions
Record the cipher text and stop

Fig. 2. Proposed encryption process

k) Decryption process will be same as encryption. It can be seen in Fig. 3.

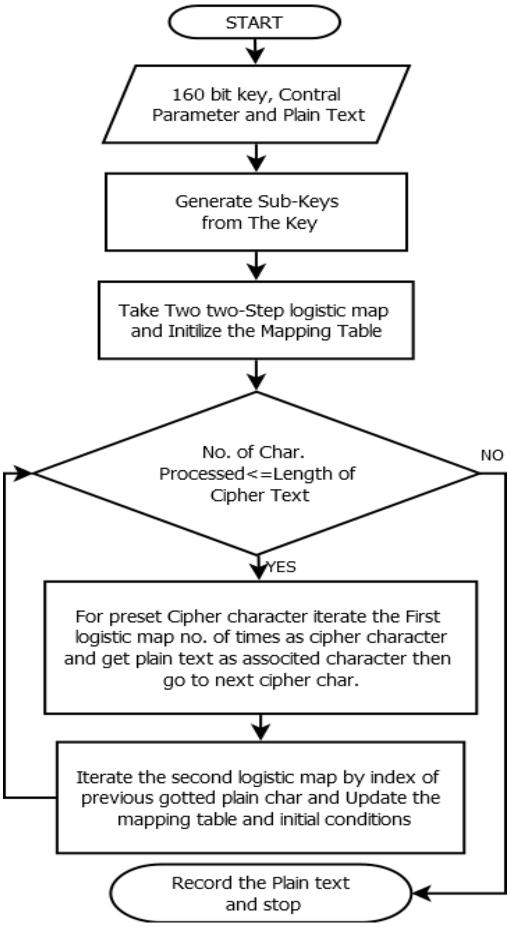
START
160 bit key, Contral Parameter and Plain Text
Generate Sub-Keys from The Key
Take Two two-Step logistic map and Initilize the Mapping Table
No. of Char. Processed<=Length of Cipher Text
NO
YES
For preset Cipher character iterate the First logistic map no. of times as cipher character and get plain text as associted character then go to next cipher char.
Iterate the second logistic map by index of previous gotted plain char and Update the mapping table and initial conditions
Record the Plain text and stop

Fig. 3. Proposed decryption process

IV. Comparison With Existing Schemes

The proposed scheme has been implemented and tested using Java development kit (jdk 1.7.0) on windows platform. System configuration consists of Intel Pentium dual core (1.86GHz), CPU with graphic and 2GB RAM. This scheme with existing schemes: Baptista's cipher, Dynamic look-up table cipher (DLT) and improved dynamic lookup table cipher (IDLT) has been compared using similar conditions and plaintexts. Then the results are compared to see the performance of proposed scheme. The first two comparisons shows the avalanche effect that if small number of bits are changed in plain text or the keys then it should show the large number of bits change in cipher text

A. Hamming code distance comparison

Hamming code distance is defined as the number of different bits in two strings. In other words if str1 and str2 are two strings, then number of bits required to change the first string str1 to str2 is known as hamming code distance. For the proposed scheme, key = "qwertyuio pasdfghjklz" and control parameter r = 3.897654321 has been chosen. For other schemes also, similar generated initial condition x_0 *=0.4432280925102532* and control parameter *r = 3.897654321*has been chosen. These have been used for different plain text inputs and then cipher-text outputs have been analysed by calculating hamming code difference. The plain texts str1, str2and str3 are as:

str1: "hi security hi cryptography"
str2: "hi tecurity hi cryptography"
str3: "hi teduruty hi cryptography"

Table 1. Hamming Code Difference Comparison for Different Plaintext

String	H.distance	Baptista	DLT	IDLT	PROPOSED
str1 str2	3	19	39	37	78
str1 str3	5	12	56	57	96
str2 str3	2	10	17	20	76

From Table 1 we can see that the new proposed scheme has more Hamming code distance than the previous one Baptista type cryptosystem for change in the plaintext. This means that the proposed scheme have more avalanche effect that makes it more secure. Also, we have observed the hamming code distance for small change in the key for proposed scheme as Key1="qwertyuiopasdfg hjklz", key2= "rwertyuiopasdfghjklz" and key3="ruerty uiopasdfghjklz", and control parameter *r = 3.897654321*. For other schemes, we used the similar generated initial conditions x_{01} *= 0.4432280925102532*, x_{02} *=0.447134342 5102532* and x_{03} *=0.4471038249321282* and control parameter *r = 3.897654321*. Same plain text is taken as "hi security hi cryptography". The comparison of results is shown in the Table 2.

Table 2. Hamming Code Difference Comparison for Different Keys

Keys	H. distance	Baptista	DLT	IDLT	PROP OSED
Key1 Key2	2	42	46	47	55
Key1 Key3	4	54	62	69	72
Key2 Key3	2	40	42	41	44

From Table 2, we can see that proposed scheme has also more hamming code distance than the previous one Baptista type cryptosystems with small change in key.

B. Levenshtien distance/Edit distance comparison

If str1 and str2 are two strings then edit distance or Levenshtien distance is the number of characters replacements to covert str1 to str2. For comparison, we choose the key as "qwertyuiopasdfghjklz" for proposed scheme and similar generated initial condition x_0 = *0.4432280925102532* and control parameter r = *3.897654321* for all other schemes. We chose three different plain text strings as:

str1: "hi security hi cryptography"
str2: "hi tecurity hi cryptography"
str3: "hi teduruty hi cryptography"

Table 3 shows the comparison of output cipher texts for different schemes, the results of this table shows that the proposed scheme gives better results.

Table 3. Edit Distance for Different Plaintexts

String	H.distance	Baptista	DLT	IDLT	PROPOSED
str1 str2	1	12	26	28	68
str1 str3	2	8	37	35	67
str2 str3	1	5	11	9	62

C. Cipher text Distribution

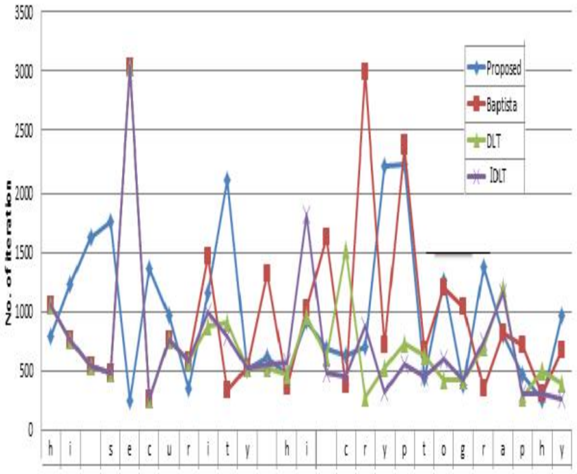

Fig. 4. Cipher text distribution comparison

To compare the cipher text distribution, we choose the same plain text as "hi security hi cryptography". For proposed scheme, the key is taken as "qwertyuiopasdfghjklz" and control parameter r = 3.897654321. For other schemes similar generated initial condition x_0 = 0.4432280925102532 and control parameter r = 3.897654321 has been used. Fig. 4 shows similar cipher text distribution for different schemes and the proposed scheme.

D. Performance Comparison

Performance analysis is done on the basis of time required to perform the encryption and decryption operations. For this purpose, we have chosen key = "qwertyuiopasdfghjklz" and control parameter r = 3.897654321 for other schemes similar generated initial condition x0 = 0.4432280925102532 and control parameter r = 3.897654321. By using ten strings of different length as plain text input, we have calculated encryption and decryption time for proposed scheme as well as existing schemes.

From Table 4 and Figs. 5 and 6, it can be observed that proposed scheme require some more time *to* perform encryption-decryption operations

Table 4. Execution Time Comparison in Microseconds

String Size in Bytes	BAPTISTA		DLT		IDLT		PROPOSED	
	Enc.	Dec	Enc.	Dec.	Enc.	Dec.	Enc.	Dec.
10	2130	941	2999	1380	2345	955	3451	1453
20	5328	2743	6967	2773	5091	2234	7984	3142
30	6426	4431	7804	6054	8946	6256	9638	6801
40	9726	6246	12711	6270	12910	6289	17145	6965
50	12763	4536	14005	5603	13688	5742	17269	7219
60	15136	5187	15294	7695	18352	7529	24058	8351
70	27812	9795	28568	6262	30866	12540	39865	15460
80	110944	8923	110673	11779	110286	13261	115917	18609
90	111902	8624	101492	10015	111048	9628	117672	17809
100	118999	10589	118350	10605	118710	10421	181938	17079

From Table 4 and Fig. 5, it can be observed that the encryption time of proposed scheme is less than 1.5 times of the previous schemes and sometimes it is nearer to the previous schemes.

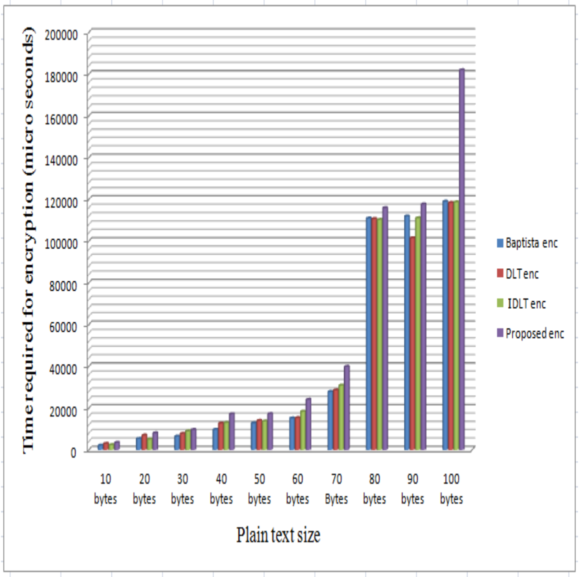

Fig. 5. Encryption time comparison

From Table 4 and Fig. 6, it can be observed that time for decryption process is about 1.4 times of the previous schemes, so decryption time is slightly more than previous schemes.

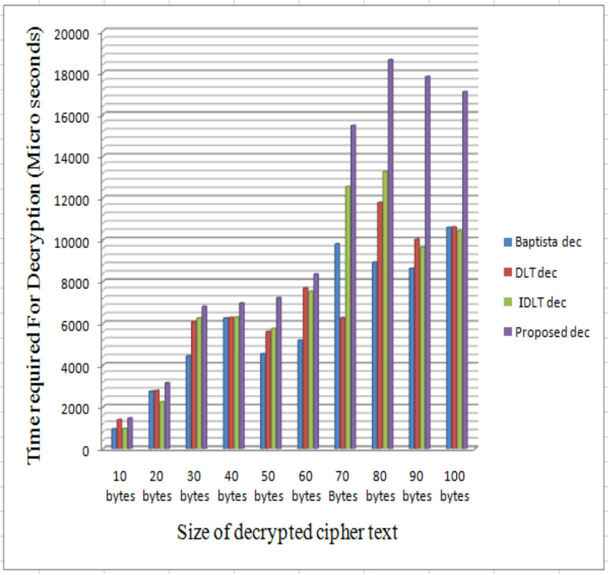

Fig. 6. Decryption time comparison

V. Conclusion

Proposed scheme has two two-step logistic map, one for encryption and another for updating the initial condition and the table entries. The proposed system has 160 bit key that provide 2160 different key combinations. It resists the proposed cryptosystem against Brute−force attack. The experimental results shows that the proposed scheme require some more time for encryption and decryption of data then Baptista's cryptosystem, Wong's dynamic look-up table cryptosystem and Improved dynamic look-up table cryptosystem. The comparisons based on Hamming code distance and edit distance shows that the proposed cryptosystem have more avalanche effect than Baptista's cryptosystem, Wong's dynamic look-up table cryptosystem and improved dynamic look-up table cryptosystem. Updating the initial condition after each encryption makes it secure from known initial condition and control parameter i.e., known partial key. The control parameter is also fixed in this scheme, so map behaviour is fixed in all states. This resists proposed scheme against behaviour analysis attack and partial key recovery attack.

The proposed method has been tested with only text information. It has a future work that it can be implemented for other types of information like images, video etc. Further, it can be used with some more feedback factors by making the new iterated value based on more than two previous values. Such type of mechanism can also be developed for making a chaotic hash function

Acknowledgment

This work was supported in part by a grant from Research and Development Cell under ICT Cell Central University of Rajasthan. The authors want to thank the Coordinator and members of this cell for their valuable support.

References

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

[2] 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.

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

[4] 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.

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

[6] William Ditto and Toshinori Munakata, Principles and applications of chaotic systems, Commun. ACM 38(11), 96–102, 1995.

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

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

[9] 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.

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

[11] Mamta Rani and RashiAgarwal, A new experimental approach to study the stability of logistic map,Chaos, Solitons, Fractals, 41(4), 2062 – 2066, 2009.

[12] Rhouma Rhouma, Ercan Solak, David Arroyo, Shujun Li, Gonzalo Alvarez, and Safya Belghith, Comment on modified baptista type chaotic cryptosystem via matrix

secret key [phys. lett. a 372 (2008) 5427], Physics Letters A, 373(37), 3398 – 3400, 2009.

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

[14] Yong Wang, Maokang Du, Degang Yang, and Huaqian Yang, One-way hash function construction based on iterating a chaotic map, In Computational Intelligence and Security Workshops, 2007, CISW 2007, 791–794, 2007.

[15] Jun Wei, Xiaofeng Liao, Kwok woWong, 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.

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

[17] 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.

Authors' Profiles

Balram Nitharwal has received Bachelor of Technology in Computer Engineering from Engineering College Bikaner, Rajasthan affiliated to Rajasthan Technical University Kota in 2011 and Master of Technology in Computer Science and Engineering with specialization in information security from Central University of Rajasthan in 2013. His area of interest includes information security, cryptography, chaotic cryptography and network security.

Mamta Rani is Associate Professor in Department of Computer Science at Central University of Rajasthan from last 3 years. Before it she has worked in many educational organizations at different posts. She has received Ph.D. in Computer Science from Gurukula Kangri Vishwavidyalaya, Haridwar, Uttarakhand in 2002. Her area of interest is Fractal Graphics and Chaos. She has published more than 40 research publications in reputed International and National Journals. She has also presented more than 15 research articles in National and International Conference Proceedings.

Hukam Chand Saini has received Bachelor of Technology in Information Technology from Engineering College Ajmer, affiliated to Rajasthan Technical University Kota in 2010 and Master of Technology in Computer Science and Engineering with specialization in information security from Central University of Rajasthan in 2013. His area of interest includes image processing, image encryption, chaotic cryptography and network security.

How to cite this paper: Balram Nitharwal, Mamta Rani, Hukam Chand Saini,"Improving Security of the Baptista's Cryptosystem Using Two-step Logistic Map", IJCNIS, vol.7, no.5, pp.34-40, 2015.DOI: 10.5815/ijcnis.2015.05.05