I.J. Computer Network and Information Security, **2014, 6, 25-33**
Published Online May 2014 in MECS (http://www.mecs-press.org/)
DOI: 10.5815/ijcnis.2014.06.04

Secure and Fast Chaos based Encryption System using Digital Logic Circuit

Ankur A. Khare
Computer Science & Engineering, University of Information Technology, Bhopal, India
Email: khareankur94@gmail.com

Piyush B. Shukla and Sanjay C. Silakari
Computer Science & Engineering, University of Information Technology, Bhopal, India
Email: {pphdw, ssilakari}@yahoo.com

Abstract—Chaotic system based message encryption system for wired and wireless networks broadly used in computer engineering, communication and network security, such as robotic systems, encryption, synchronization and genetic network. The main motive for developing the chaos based cryptosystem is to attain encryption with several compensation over the conventional encryption algorithms such as high security, speed, complexity, cost and quality assurance. These challenges encourage the researchers to develop novel chaos based data encryption techniques with digital logics dealing with encryption of messages for fast and secure communication networks. This effort provides a modified version of traditional data encryption algorithms to provide good quality and performance in a secure communication network environment. A cryptology technique is widely used in network security during communication. An avalanche effect is the attractive property of cryptography in which two different keys produce different cipher text for the same data information and also some Important properties related to chaotic systems are sensitivity to initial condition and nonlinearity, which makes two similar or slightly different keys to generate completely different cipher text to produce confusion. It has been proposed a novel fast & secure encryption Technique which uses the chaotic map function to generate the different multiple keys and shows that negligible difference in parameters of chaotic function generate completely different keys as well as cipher text. Cryptanalysis of the proposed algorithm shows the strength and security of algorithm and keys.

Index Terms—Cryptology, Encryption Technique, Chaos Function, Logistic Map, Cipher text, Digital Logic Circuit.

I. Introduction

Rapid development of computer and network technology arise the importance of the network management and security. Network security defined over network containing data integrity, authentication, secrecy, data repudiation and data controllability [1], [2]. The data is secured using some techniques like as cryptology. Cryptology is used for studying the cryptosystem and cryptanalysis [3], [4]. The encryption and decryption algorithms are used for converting the data information into unreadable and readable form in cryptographic system for secure communication [5].

A new Chaotic based Cryptographic Technique is proposed in this paper using digital logic circuits. So the speed of encryption is enhanced. Chaotic maps are used to provide a high degree of randomization and hence increase the confusion and diffusion of the system.

The rest of the paper is organized as follows. In section II, chaos theory, cryptography, chaos based cryptography and literature survey are described. In section III, the proposed cryptosystem is described. In section IV, Proposed cryptosystem has been explained by example. Then, in section V, analysis of security of keys of the proposed approach is provided. In section VI, methodology is checked against all four cryptanalysis attacks. Finally, the paper is concluded in section VII.

II. Technical Description

A. Cryptography

A cryptosystem has four important components [5]. *Plain text* is the original message for transferring. *Cryptographic system* is the combination of encryption and decryption system. *The ciphertext* is the yield of applying an encryption technique to the original message. *The key* is a combination of bits using in encrypting and decrypting processes [6].

A cryptographic system is represented by:

$$E_k(P) = C$$
$$D_k(C) = P$$

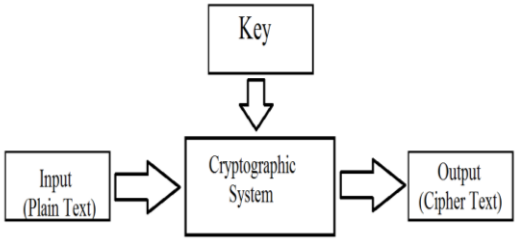

Fig. 1. Cryptographic System

B. Cryptanalysis

Cryptanalysis is a procedure which is used to split the code and deduce a particular plain text or the key being used. All future and past information about message encrypted with that key are compromised.

Table 1. Ciphertext Attack

Type of Attack	Known to Cryptanalyst
Ciphertext only	• Encryption algorithm • Ciphertext to be decoded
Known plain text	• Encryption algorithm • Ciphertext to be decoded • One or more plain text-cipher text pairs formed with the secret key
Chosen plain text	• Encryption algorithm • Ciphertext to be decoded • Plain text message chosen by cryptanalyst, together with its corresponding cipher text generated with the secret key
Chosen cipher text	• Encryption algorithm • Ciphertext to be decoded • The purported cipher text chosen by cryptanalyst, together with its corresponding decrypted plain text generated with the secret key
Chosen text	• Encryption algorithm • Ciphertext to be decoded • Plain text message chosen by cryptanalyst, together with its corresponding cipher text generated with the secret key The purported cipher text chosen by cryptanalyst, together with its corresponding decrypted plain text generated with the secret key

The table contains the several types of cryptanalysis attacks depend upon the amount of information identified by the cryptanalyst.

C. Chaos Theory

Chaotic system or chaos for short is meddling between rigid regularity and randomness based on possibility [7]. Chaos can be defined by some typical characteristics.

Nonlinearity [8] in this property, the smallest change in data at any instant can result in a change in the same or a different data at a later time, that is not depended to the change at the initial time [9], [10].

Determinism it has provided determinism which is controlled by exact rules with no element of chance.

Sensitivity to initial condition Negligible changes in its initial variable can give completely different final variable [11], [12].

Irregularity the behavior of chaos is not predictable. It is provided irregularity.

Long term prediction chaos gives long term uncontrolled dynamic prediction. Chaos can be controlled conditionally [13].

A useful feature of chaotic systems is their capability of producing complex patterns of behavior [14]. This is performed by simple real systems with a small set of evolution equations [14]. These features have made a chaotic system useful for several applications in many disciplines, such as biology, economics, engineering, neural network and others [15].

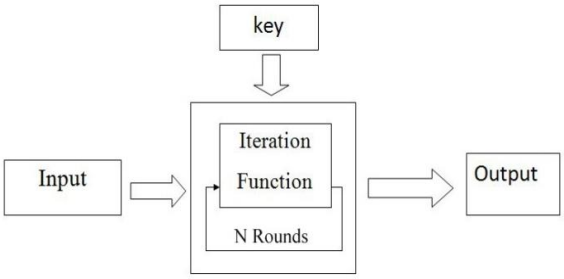

Fig. 2. Chaos Iterative Function

D. Chaos And Cryptology

Chaos and cryptology are related with each other by some features: Both (chaotic and encryption techniques) are deterministic in nature [16]. Both are provided with highly complex and unpredictable variables [17]. It means random nature for any external observer, not having any prior knowledge of the algorithm and initial condition – key [18], [19].

Chaos is sensitive to initial conditions ie. Negligible difference in any variable totally changes the outputs [20]. Cryptography is depending on confusion and diffusion with key dependency ie. Updating of 1 bit of the plaintext or key should change all bits of the cipher text with 60% probability [21].

Chaos is topological transitive and repetitive process and cryptography is multiple round transformations and repetitive transformations with a single logistic map function [22].

Chaos is also different from cryptology: Chaos based systems are defined on bounded continuous space and cryptography is defined over finite discrete space.

Chaos theory has found a way for understanding the asymptotic performance of repetitive process, whereas cryptography based on the properties of first few repetitions [23].

Table 2. Chaos Theory Vs. Cryptography

Chaos Theory	Cryptography
Chaos based system	Pseudo-chaos based system
Random transformation	Random transformation
Infinite number of stages	Finite number of stages
Infinite number of repetitions	Finite number of repetitions
Initial stage	Plain text
Final stage	Ciphertext
Initial circumstances and/or parameters	Key
Asymptotic liberty of initial and final stages	Confusion
Compassion to initial circumstances and parameter mixing	Diffusion

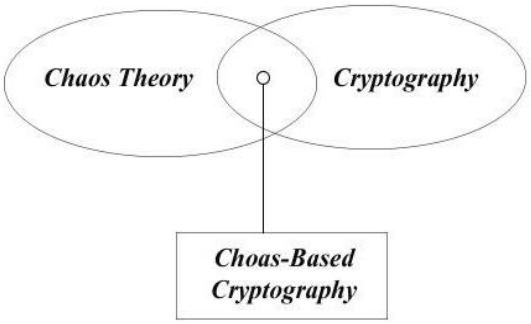

Fig. 3. Relation between Chaos and Cryptography

E. Motivation

Chaos theory for cryptosystem has been broadly discussed for secure communication in the last few years. Chaos system is generally defined in a symmetric encryption system with some complex mathematical function [23]. It will illustrate that the keys with negligible change produce different cipher texts. Cryptanalysis shows the resistivity against several attacks and stronger than existing encryption technique [24]. Cryptanalysis shows that there are negligible changes in key generate diffusion. A block encryption technique used dynamic sequences by single and multiple chaotic systems [25], [26]. Several one-dimension logistic maps are used to provide pseudo-random sequences, which are independent, nonlinear and approximately uniform [27]. The chaotic masking technique is used for encrypting the transmitting messages with a binary sequence extracted from a logistic map [28]. A symbolic sequence generated by another skew tent chaotic map is provided the masked message sequence which is tracked [28], [29]. The theoretical and simulation results explain many characteristics such as high speed, easy implementing, accuracy and high security. Therefore, it is suitable for practical use in the secure communication between two private parties [30], [31].

The chaotic properties such as ergodicity, sensitive dependency on initial conditions and system parameters have been properly utilized in encryption [31]. The recent advance researches on information security technique are getting more imperative to the development of network management and security technique. Today, Most of data information is transmitted in the form of a stream of bits over the internet. Jinhong Luo proposes a way of adjusting the corresponding sequence of key encryption and plain message to get the best anti decryption signed and shows its advantages and disadvantages by analyzing this arithmetic [32].

The parameter of the chaotic Lorenz system is also used in a two-channel cryptosystem first the geometrical properties of the Lorenz system and second the parameters which are precisely determined - directly from the cipher text - through the minimization of the average jamming noise power generated by the encryption procedure [32], [33].

Chaotic encryption schemes are provided superior level of security than conventional ciphers [34]. A chaotic system is also used with ECG signal to provide higher speed and security with encryption [35]. The hardware implementation of chaotic system details over Xilinx Virtex - 6 FPGA is provided [36]. Logistic map has high potential to be used to design a stream cipher for real-time embedded systems [37], [38]. Fu's chaotic cipher is secure and the information leak of chaos map is discovered [39].

A new scheme is used which performs lossless compression is based on the arithmetic coding (AC) as well as encryption of data is based on a pseudo random bit generator (PRBG). The standard logistic map based PRBG and the Engel Continued Fraction (ECF) map to generate a key stream with both chaotic and algebraic characteristics. The effectiveness of the BAC in lossless data compression and the compensation of chaotic theory in data encryption to offer a method used in many applications such as multimedia applications and medical Imaging [39], [40].

III. Proposed Methodology

It has been proposed a Symmetric key encryption technique which is used one or more than one key for encryption and decryption process. But these keys are similar for encryption and decryption process at any instant of time. It means different keys are used for different messages for enhancing the security. Firstly generates the number of keys by using the chaos logistic function (logistic map) providing only initial condition [40].

For n=1 to j

$$X_{n+1} = \{A * X_n (X_n - 1)\} MOD 256$$

A= any integer (1, 2, 3,.....)

X_n = initial value of chaotic function which is 2, 3,.....
j = Number of keys

X_{n+1} = keys $K_1, K_2, K_3, ...K_j$, (after applying gray code on X_{n+1})

These keys are controlled by providing some satisfactory condition. So the whole letters of the message are encrypted with these keys. Using multiple keys are enhanced the security and it is not necessary that any repeated letters in the message are encrypted by the same key [40].

It has been provided multiple different keys for different messages and also applied some digital circuit system concept of the keys to increase the complexity of the keys and speed of the encryption and decryption so the intruder is not found that how keys are coming [41].

The following notations are used in the key generation encryption and decryption scheme.

P_i = Plain text
C_i = Cipher text
$E(P_i)$ = Encryption the plaintext P_i.
$D(C_i)$ = Decryption the ciphertext C_i
For n=1 to j

$$X_{n+1} = \{A * X_n (X_n - 1)\} MOD 256$$

A= any integer (1, 2, 3,.....)
X_n = initial value of chaotic function which is 2, 3,4,……
j = Number of keys

X_{n+1} = keys $K_1, K_2, K_3, ...K_j$ (after applying gray code on X_{n+1})

A. Key generation Scheme

1. Firstly generates the pseudo random numbers by using the logistic map function at both ends (sender and receiver) by using an equation.
   For n=1 to j

$$X_{n+1} = \{A * X_n (X_n - 1)\} MOD 256$$

2. Then generate different multiple values of X_{n+1} (used for keys after applying gray code on these values of X_{n+1}) and fixed the random numbers by using some specific condition j.
3. Complexity of keys is increased by applying a gray code on X_{n+1} so keys are independent with each other.
4. The keys are shown in 8 bit binary form.

B. Encryption Scheme

Each character is shown in ASCII character format. Then ASCII characters are converted into 8 bit binary numbers with respect to their decimal numbers after that these characters are encrypted by using a digital logic XOR function. Then perform XOR operation on each character by a single binary coded key. Keys are also repeated for encrypting the whole message.

P_1 = ASCII (character1)
P_1 converted into 8 bit binary numbers.

$$E_{k_1}(P_1) = C_1$$

P_2 = ASCII (character 2)
P_2 is converted in 8 bit binary numbers.

$$E_{k_2}(P_2) = C_2$$

P_i = ASCII (character i)
P_i is converted in 8 bit binary numbers.

$$E_{k_m}(P_i) = C_i$$

Where m = 1 to j

C. Decryption Scheme

The cipher texts are decrypted (converted into plain text) by using the reverse process of encryption scheme**.**

$$P_1 = D_{k_1}(C_1)$$

P_1 is converted into ASCII(P_1) with respect to its decimal value.

Character1 = ASCII(P_1)

$$P_2 = D_{k_2}(C_2)$$

P_2 is converted into ASCII(P_2) with respect to its decimal value.

Character2 = ASCII(P_2)

$$P_i = D_{k_m}(C_i)$$

Where m= 1 to j
P_i is converted into ASCII(P_i) with respect to its decimal value.

Character i = ASCII(P_i)

D. Algorithm for key generation

1. Decide the values of parameter (M, A, X_n).
2. Generate the pseudo random numbers from the equation.
   For n=1 to j

$$X_{n+1} = \{A * X_n(X_n - 1)\} MOD 256$$

3. Apply gray code on these random numbers which are generated from X_{n+1} to build up the keys $K_1, K_2, K_3, ...K_j$.
4. Keys are represented in 8 bit binary form.

E. Algorithm for encryption

1. Each character is shown in ASCII character, P_i = ASCII(character i).
2. ASCII character P_i is converted into 8 bit binary form.
3. Using the equation $E_{k_m}(P_i) = C_i$ for all i>0, and m = 1 to j for encryption, Where $E_{k_m}(P_i)$ is bit wise XORing on plaintext P_i with single key K_m.
4. Find the 1`s complement of ciphertext (C_i).

F. Algorithm for decryption

1. Find the 1`s complement of receiving ciphertext (C_i).
2. Using the equation $P_i = D_{k_m}(C_i)$. Where m=1 to j for decryption, where $D_{k_m}(C_i)$ is bit wise XORing on cipher text C_i with single key K_m.
3. Plain text P_i is converted into ASCII(P_i) with respect to its decimal value.
4. Then Character i = ASCII (P_i).

IV. EXAMPLE

Given plain text – ANKURA

Letter	*ASCII*	*Binary Number*
A	65	01000001
N	78	01001110
K	75	01001011
U	85	01010101
R	82	01000001
A	65	01000001

A. Key Generation

$$X_{n+1} = \{A * X_n(X_n - 1)\} MOD 256$$

Let A=2, X_n =3, j=4
Xn+1 = 12, 8, 112, 32.

The keys are generated by applying a gray code on random numbers X_{n+1}.

12 = 00001100
Gray code (0,0 XOR 0,0 XOR 0, 0 XOR 0, 0 XOR 1, 1 XOR 1, 1 XOR 0, 0 XOR 0) =00001010= 10
8=00001000 gray code = 00001100 = 12
112=01110000 gray code = 01001000 = 72
32= 00100000 gray code = 00110000 = 48
Keys (K_1 = 10, K_2 =12, K_3 =72, K_4 = 48)

B. Encryption Algorithm

Encryption algorithm converts the plain text into cipher text by using multiple keys.

Table 3. Cipher Text For Giving Plain Text

Plain text (ASCII)	XOR	Key K_j	Cipher Text	1`s complemented Cipher Text
A *65* *01000001*	*XOR*	*10* *00001010*	*01001011*	*10110100* *180* ┤
N *78* *01001110*	*XOR*	*12* *00001100*	*01000010*	*10111101* *189* ╜
K *75* *01001011*	*XOR*	*72* *01001000*	*00000011*	*11111100* *252* ⁿ
U *85* *01010101*	*XOR*	*48* *00110000*	*01100101*	*10011010* *154* Ü
R *82* *01010010*	*XOR*	*10* *00001010*	*01011000*	*10100111* *167* º
A *65* *01000001*	*XOR*	*12* *00001100*	*01001101*	*10110010* *178* ▓

Ciphertext - ┤╜ⁿÜ▓

C. Decryption Algorithm

Decryption algorithm converts the cipher text into plain text by using the same key.

Cipher Text: ┤╜ⁿÜ▓

Table 4. Plain Text For Cipher Text

Received Cipher Text	1`s complemented cipher text	XOR	Key K_j	Plain text (ASCII)
┤ 180 10110100	01001011	XOR	10 00001010	01000001 65 A
╝ 189 10111101	01000010	XOR	12 00001100	01001110 78 N
ⁿ 252 111111100	00000011	XOR	72 01001000	01001011 75K
Ü 154 10011010	01100101	XOR	48 00110000	01010101 85 U
º 167 10100111	01011000	XOR	10 00001010	01010010 82 R
▓ 178 10110010	01001101	XOR	12 00001100	01000001 65 A

Plain text – ANKURA

V. Analysis of Security of Keys

To find all the values (M, A, X_n) is hard to compute. In this section we show the sensitivity of the secret key with negligible difference in the key parameters.

$$X_{n+1} = \{A * X_n(X_n - 1)\} MOD 256$$

Plain text: - ANKURA

Parameter (j, A, X_n)

Keys ($K_1, K_2, K_3, \ldots\ldots\ldots\ldots K_j$)

A. Sensitivity of number of keys j

It has been claimed that if a number of keys are changed, then the cipher texts are also completely changed from one another for same plain text.

Table 5. Sensitivity Of Number Of Keys j

J	A	X_n	X_{n+1}	KEYS (K_j)	CIPHER TEXT	1`s Complemented cipher Text
1	2	3	12	10,10,10,10,10,10	KDA_XK	┤╗╛ áº┤
2	2	3	12,8	10,12,10,12,10,12	KBAYXM	┤╝╛ ª▓
3	2	3	12,8,112	10,12,72,10,12,72	KBETX_^TAB	┤╝ⁿáí÷
4	2	3	12,8,112,32	10,12,72,48,10,12	KBETXeXM	┤╝ⁿÜº▓
5	2	3	12,8,112,32,192	10,12,72,48,160,10	KBETXe>=K	┤╝ⁿÜCR┤

In table 5 negligible differences in the j (number of keys) produced different cipher text.

B. Sensitivity of constant A

It is claimed that negligible changes in constant A generated totally different keys so cipher text are also different from each other.

Table 6. Sensitivity Of Constant A

J	A	X_n	X_{n+1}	KEYS (K_j)	CIPHER TEXT	1`s Complemented cipher Text
4	2	3	12,8,112,32	10,12,72,48,10,12	KBETXeXM	┤╝ⁿÜº▓
4	3	3	18,150,234,238	27,221,159,153,27,221	Zô ┗╠I£	Ñl+3╟c
4	4	3	24,160,128,0	20,240,192,0,20,240	U╛ ïUF▒	¬At─┤N
4	5	3	30,254,30,254	17,129,17,129,17,129	P═Z ┗CL	»0Ñ+╝?
4	6	3	36,136,80,32	54,204,120,48,54,204	w ëed ì	ê}╠Ü¢r

In table 6 it has been represented that small difference in the values of constant A generated different cipher text.

C. Sensitivity of Initial condition Xn

It has been represented that the small changes in initial condition Xn generated totally different keys, so cipher texts are totally different, it is called confusion.

$$X_{n+1} = \{A * X_n(X_n - 1)\} MOD 256$$

Plain text: - ANKURA

Parameter (j, A, X_n)

Keys ($K_1, K_2, K_3, \ldots\ldots\ldots\ldots K_j$)

Table 7. Sensitivity Of Initial Condition X_n

J	A	X_n	X_{n+1}	KEYS (K_j)	CIPHER TEXT	1`s Complemented cipher Text
4	2	3	12,8,112,32	10,12,72,48,10,12	KBETXeXM	┤╝ⁿÜº▓
4	2	4	24,80,96,64	20,120,80,96,20,120	U6;5N9	¬╔─╨▒╠
4	2	5	40,48,160,192	60,40,240,160,60,40	}f╗⌡ni	éÖDLF æ î
4	2	6	60,168,48,160	34,252,40,240,34,252	c▓cÑJ╝	£M £Z ÅB
4	2	7	84,120,144,224	126,68,216,144,126,68	?LFôσ,ENQ	┗⌡lSUB╚.

In table 7 it has been represented that small difference in values of initial variable X_n generated totally different ciphertext.

VI. Cryptanalysis

Cryptanalysis is used to check the security of algorithm by breaking the codes and find the possible keys and plain text as well.

A. Ciphertext only attacks

Parameter (j=4, A=2, X_n =3)
Keys (10,12,72,48)
Given.

$$C_1 = E_{k_1}(P_1), C_2 = E_{k_2}(P_2), ..., C_i = E_{k_m}(P_i)$$

Where m = 1 to j.
Deduce: - Either $P_1, P_2, P_3, ...P_i$;
K_1, K_2, K_3, K_4;
Or an algorithm to infer P_{i+1}
From $C_{i+1} = E_{k_m}(P_{i+1})$
Keys (10,12,72,48)
Example

P_1 =N then $C_1 = E_{k_1}(P_1) = E_{10}$ (N)= ╕

P_2 =NN then $C_2 = E_{k_{1,2}}(P_2) = E_{10,12}$ (NN)= ╕╨

P_3 =NNN then $C_3 = E_{k_{1,2,3}}(P_3) = E_{10,12,72}$ (NNN)= ╕╨·

P_4 =NNNN then $C_4 = E_{k_{1,2,3,4}}(P_4) = E_{10,12,72,48}$ (NNNN) = ╕╨·ü

P_5 =NNNNN then $C_5 = E_{k_{1,2,3,4,1}}(P_5) = E_{10,12,72,48,10}$ (NNNNN) = ╕╨·ü╕

From the above example, it would be said that if any character is repeated many times, the cipher text is not same for same letter N. The Cipher text of character N occuring as the first letter is different from N occuring as nth character in plaintext.

B. Known plain text attack

Parameter (j=4, A=2, X_n =3)
Keys (10, 12, 72, 48)
Given-

$$P_1, C_1 = E_{k_1}(P_1), P_2, C_2 = E_{k_2}(P_2), ...P_i, C_i = E_{k_m}(P_i)$$

where m = 1 to j
Deduce: - Either K_1, K_2, K_3, K_4;
Or an algorithm to infer P_{i+1}
From $C_{i+1} = E_{k_m}(P_{i+1})$
Keys (10, 12, 72, 48)
Example

P_1 =M then $C_1 = E_{k_1}(P_1) = E_{10}$ (M)= ╕

P_2 =MM then $C_2 = E_{k_{1,2}}(P_2) = E_{10,12}$ (MM)= ╕╡

P_3 =MMM then $C_3 = E_{k_{1,2,3}}(P_3) = E_{10,12,72}$ (MMM)= ╕╡·

P_4 =MMMM then $C_4 = E_{k_{1,2,3,4}}(P_4) = E_{10,12,72,48}$ (MMMM) = ╕╡·é

P_5 =MMMMM then $C_5 = E_{k_{1,2,3,4,1}}(P_5) = E_{10,12,72,48,10}$ (MMMMM) = ╕╡·é╕

From the example it can be said that there are several cipher text for several plaintexts. It is difficult to deduce the key or the algorithm for decrypting plaintexts encrypted with the keys. Keys are created by very controlling and sensitive parameters. Cipher text of character M occuring as first letter is not same as M occuring as nth character in the plaintext.

C. Chosen plaintext attacks

Parameter (j=4, A=2, X_n =3)
Keys (10,12,72,48)
Given-

$$P_1, C_1 = E_{k_1}(P_1), P_2, C_2 = E_{k_2}(P_2), ...P_i, C_i = E_{k_m}(P_i)$$

Where the cryptanalysis gets to choose $P_1, P_2, P_3, ...P_i$ and m= 1 to j.
Deduce: - Either $P_1, P_2, P_3, ...P_i$;
Or an algorithm to infer P_{i+1}
From $C_{i+1} = E_{k_m}(P_{i+1})$
Keys (10,12,72,48)
Example

P_1 = XY then ciphertext $C_1 = E_{k_{1,2}}(P_1) = E_{10,12}$ (XY)= ¡¬

P_2 = YX then ciphertext $C_2 = E_{k_{1,2}}(P_2) = E_{10,12}$ (YX) = ½¼

It is hard to deduce the key or the algorithm to decrypt the plaintext encrypted with the same keys.

D. Chosen ciphertext attack

Parameter (j=4, A=2, X_n =3)
Keys (10,12,72,48)
Given-

$C_1, P_1 = D_{k_1}(C_1), C_2, P_2 = D_{k_2}(C_2), ..., C_i, P_i = D_{k_m}(C_i)$

where m = 1 to j
Deduce: - K_1, K_2, K_3, K_4;
Example

C_1 = ¡¬ then plaintext $P_1 = D_{k_{1,2}}(C_1) = D_{10,12}$ (RU) = XY

C_2 = ½¼ then plain text $P_2 = D_{k_{1,2}}(C_2) = D_{10,12}$ (ST) = YX

Keys are generated by two different parameters X_n and A which are very sensitive and different. So it is difficult to compute the keys by knowing the cipher text and its decrypted plaintext.

VII. Conclusion

There is an enormous literature of chaotic function based cryptographic techniques. In this paper a new chaotic encryption algorithm is developed using the properties of a chaotic map (sensitivity of parameters) like constant A and initial condition X_n. Cryptosystem is also depending on the number of keys which are generated by the use of logistic map. It has been also shown that completely different keys are generated when parameters are slightly changed. This enhanced the security of keys. Cryptanalysis is showing that there is a negligible modification of parameters is generated great confusion and diffusion. The algorithm is also worked and analyzed against all four cryptanalysis attack cipher text only, known plain text, chosen plaintext and chosen cipher text attacks and fast computing. Time complexity is reduced by using digital circuits ie. Gray code, XOR gate, and 1`s complement etc. Fast computing is also achieved by digital logics.

Acknoledgement

We grateful to Dr. Piyush Kumar Shukla and Dr. Sanjay Silakari for stimulating discussions.

References

[1] Yong Peng Xiao and Yi Han, “An Encrypt Approach Using Dynamic Encrypt keys”, IEEE, pp. 3273-3277, 2007.

[2] Sundarapandian Vaidyanathan, “Complete Synchronization Of Hyperchaotic Xu And Hyperchaotic Lu Systems Via Active Control”, International Journal of Computer Science & Engineering Survey (IJCSES), Vol.3, No.3, pp. 1-15, 2012.

[3] Brad Aimone and Stephen Larson “Chaotic Circuits and Encryption”, Neurophysics Lab, pp. 1-12, 2006.

[4] A. Masmoudi, W. Puech and M.S. Bouhlel, “A new joint lossless compression and encryption scheme combining a binary arithmetic coding with a pseudo random bit generator”, (IJCSIS) International Journal of Computer Science and Information Security, Vol. 8, No. 1, pp. 170-175, 2010.

[5] G. Alvarez, F. Montoya, M. Romera and G. Pastor, “Cryptanalysis Of A Chaotic Encryption System”, pp. 191-196, 2000.

[6] A. Palacios and H. Juarez, “Cryptography with cycling chaos”, ELSEVIER, pp. 345-351, 2002.

[7] Ercan Solak, and Cahit Cokal, “Cryptanalysis of a cryptosystem based on discretized two-dimensional chaotic maps”, Elsevier, pp. 6922-6924, 2008.

[8] J M Blackledge,”Cryptography using Deterministic Chaos: Application to Symmetric Encryption”, Lecture Notes, Warsaw University of Technology, pp. 1-86, 2011.

[9] Roland Schmitz, “Use of chaotic dynamical systems in cryptography”, ELSEVIER, pp. 429-441, 2001.

[10] Bassem Bakhache and Kassem Ahmad and Safwan el Assad,“A New Chaotic Encryption Algorithm to Enhance the Security of ZigBee and Wi-Fi networks”, International Journal of Intelligent Computing Research (IJICR), Vol. 2, Issues 4, pp. 219-227, 2011.

[11] R. Hasimoto-Beltran, “Low-complexity chaotic encryption system”, Revista Mexicana De Fisica , Vol. 53, No. 1, pp. 58-65, 2007.

[12] ShujunLi , Gonzalo Alvarez, Zhong Li and Wolfgang A. Halang, “Analog Chaos-based Secure Communications and Cryptanalysis: A Brief Survey”, pp.1-6, 2007.

[13] Amit Pande, Joseph Zambreno, “A chaotic encryption scheme for real-time embedded systems: design and implementation”, Springer, pp. 1-11, 2011.

[14] Tao Yang., “A Survey of Chaotic Secure Communication Systems”, International Journal of Computational Cognition, Vol. 2, No. 2, pp. 81–130, 2004.

[15] Fei Peng, Xiao-wen Zhu, and Min Lon, “An ROI Privacy Protection Scheme for H.264 Video Based on FMO and Chaos”, IEEE Transactions on Information Forensics and Security, VOL. 8, NO. 10, pp. 1688-1699, 2013.

[16] Kristina Kelberand Wolfgang Schwarz, “General Design Rules for Chaos-Based Encryption Systems”, NOLTA, pp. 465-468, 2005.

[17] P. Jhansi Rani and S. durgaBhavani, “Symmetric Encryption using Logistic map”, RAIT, pp. 1-5, 2012.

[18] K. Prasadh, K. Ramar and R. Gnanajeyaraman, “Public key cryptosystems based on chaotic Chebyshev polynomials”, Journal of Engineering and Technology Research, Vol.1, pp. 122-128, 2009.

[19] Mohamed I. Sobhy and Alaaedin R. Shehata, “Chaotic Algorithm for Data Encryption”, IEEE, pp. 997-1000, 2001.

[20] Dalia H. Elkamshoushy, A. KhairyAboulsoud, “Cryptographic Schemes Using Chaotic System”, National Radio Science Conference NRSC, pp. 1-6, 2008.

[21] GoceJakimoski and LjupcoKocarev, “Chaos and Cryptography: Block Encryption Ciphers Based on Chaotic Maps”, IEEE, Vol. 48, No. 2, pp. 163-169, 2001.

[22] Guoping Tang, Xiaofeng Liao, Di Xiao and Chuandong Li, “A Secure Communication Scheme Based on Symbolic Dynamics”, IEEE, pp. 13-17, 2004.

[23] LjupcoKocarev,“Chaos-Based Cryptography : A Brief Overview”, IEEE, pp. 1-16, 2011.

[24] C. Wang and S.S. Ge, “Adaptive synchronization of uncertain chaotic systems via backstepping design”, Elsevier, pp. 1199-1206, 2001.

[25] Long JyeSheu, Wei Ching Chen, Yen Chu Chen and Wei Tai Weng, “A Two-Channel Secure Communication Using Fractional Chaotic Systems”, World Academy of

Science, Engineering and Technology, pp. 1057-1061, 2010.
[26] BhavanaAgrawal and HimaniAgrawal, "Survey Report On Chaos Based Cryptography", IJREAS, Vol. 2, Issue 2, pp. 921-939, 2012.
[27] I.A. Kamil and O.A. Fakolujo, "Lorenz-Based Chaotic Secure Communication Schemes", Ubiquitous Computing and Communication Journal, Vol. 7, No. 2, pp. 1248-1254, 2008.
[28] JinhongLuo and HaiyiShi , "Research of Chaos Encryption Algorithm Based on Logistic Mapping", IEEE, pp. 1-3, 2006.
[29] A.B. Orue, V. Fernandez, G. Alvareza, G. Pastor, M. Romera, Shujun Lib, F. Montoya, "Determination of the Parameters for a Lorenz System and Application to Break the Security of Two-channel Chaotic Cryptosystems", Physics Letter, pp-5588-5592, 2008.
[30] Daniel-Ioan Curiac, Daniel Iercan, Octavian Dranga, Florin Dragan, Ovidiu Banias, "Chaos-Based Cryptography: End of the Road", IEEE, pp. 71-76, 2007.
[31] Bin Zhang, Chenhui Jin, "Cryptanalysis of a Chaos-based Stream Cipher", IEEE, pp. 2782-2785, 2008.
[32] Zheng-Guang Wu and Peng Shi, "Sampled-Data Synchronization of Chaotic Lur'e Systems With Time Delays", Vol. 24, No. 3, pp. 410-421, 2013.
[33] Ching-Kun Chen and Chun-Liang Lin, "Text Encryption Using ECG signals with Chaotic Logistic Map", IEEE, pp. 1741-1746, 2010.
[34] Ahmed M. Elshamy, Ahmed N. Z. Rashed, Abd El-Naser A. Mohamed, Osama S. Faragalla, Yi Mu, Saleh A. Alshebeili, and F. E. Abed El-Samie, "Optical Image Encryption Based on Chaotic Baker Map and Double Random Phase Encoding", Journal Of Lightwave Technology, IEEE, VOL. 31, NO. 15, pp. 2533-2539, 2013.
[35] William Ditto and Toshinori Munakata, "Principles and Applications of Chaotic System", ACM, vol. 38, no. 11, pp. 96-102, 1995.
[36] Ercan Solak," Cryptanalysis of Observer Based Discrete-Time Chaotic Encryption Schemes", International Journal of Bifurcation and Chaos, Vol. 15, No. 2, pp. 653-658, 2005.
[37] Bassem Bakhache, and Kassem Ahmad, Safwan EI Assad, "Chaos based improvement of the security of ZigBee and WI-Fi networks used for industrial controls", IEEE, pp. 139-145, 2011.
[38] Filali Rania Linda, Sonia Hammami, Mohamed Benrejeb, and Pierre Borne, "Synchronization of discrete-time hyperchaotic maps based on an aggregation technique for encryption", IEEE, pp. 1-6, 2012.
[39] Ahmed M. Elshamy, Ahmed N. Z. Rashed, Abd El-Naser A. Mohamed, Osama S. Faragalla, Yi Mu, Saleh A. Alshebeili, and F. E. Abd El-Samie, "Optical Image Encryption Based on Chaotic Baker Map and Double Random Phase Encoding", Journal Of Lightwave Technology, IEEE, VOL. 31, NO. 15, pp. 2533-2539, 2013.
[40] J.M. Amigo, L. Kocarev and J. Szczepanski, "Theory and practice of chaotic cryptography", ELSEVIER, pp. 211-216, 2007.
[41] Ibrahim S. I. Abuhaiba1, Amina Y. AlSallut, Hana H. Hejazi, and Heba A. AbuGhali, "Cryptography Using Multiple Two-Dimensional Chaotic Maps",IJCNIS, MECS, PP. 1-7, 2012.

Authors' Profiles

Ankur A. Khare received his Bachelor`s degree in Computer Science and Engineering, MPCT, Gwalior, India in 2011. At present he is pursuing his M.E. Degree in Computer Science & Engineering from UIT-RGPV, Bhopal, India.

His research areas are Computer Networks, Network Security and Chaotic System. He is also working on cryptovirology and intrusion detection system. Currently he is working on network simulators for modifying some routing and transmission protocols. His interesting areas of research are also compiler, Theory of computation and algorithm designs.

Dr. Piyush B. Shukla received his Bachelor's degree in Electronics & Communication Engineering, LNCT in 2001, Bhopal, M. Tech (Computer Science & Engineering) in 2005 from SATI, Vidisha, Ph.D. (Computer Science & Engineering) in 2013 from RGPV, Bhopal. M.P. India. He is a member of IACSIT. He has published more than 15 papers in reputated International Journals and 10 papers in International Conferences.

At present, he is working as an Assistant Prof. in Department of Computer Science & Engineering, UIT-RGPV, Bhopal Since July 2007.

Dr. Sanjay C. Silakari received his Bachelor's degree in Computer Science & Engineering from SATI, Vidisha in 1991. M.E. (Computer Science & Engineering) from DAVV, Indore in 1998. Ph.D. (Computer Science & Engineering) in 2006 from B.U. Bhopal (M.P.) India. He is a member of various AcadamicSociety.

At present, he is working as Joint Director in UIT-RGPV and Prof. & Head of CSE Department, UIT-RGPV, Bhopal. He has several research publications to his credit in different reputed national and international conferences & journals. He has edited the proceeding of different international conferences including IEEE conference, & also organized & attended several international & national conferences. He is a life member of India Society for Technical Education (ISTE), Computer Society of India (CSI), the Indian Science Congress Association & International Association of Engineers (IAENG), & a member of IEEE and ACM.

How to cite this paper: Ankur A. Khare, Piyush B. Shukla, Sanjay C. Silakari,"Secure and Fast Chaos based Encryption System using Digital Logic Circuit", IJCNIS, vol.6, no.6, pp.25-33, 2014. DOI: 10.5815/ijcnis.2014.06.04

