Performance Analysis of Chaos based Cryptographic Transmission and Chaotic Synchronization

[1]Prof. Gouri Halde, [2]Prof.S.Wasnik, [3]Prof.S.I.Parihar

Assistant Professor
Department of Electronics and Communication Engineering
P.I.E.T. R.T.M. Nagpur University

***Abstract*— Applications of multimedia broadcasting and mobile communication are the new generation communication networks which demands for more number of users to be serviced through the network every day. For these multiuser applications transmitted data security is very important in wireless communication network. So in this paper a methodology for the transmission of data using chaotic encryption algorithm is proposed to increase the security of the data. A proposed new structure is based on coupling of chaotic system through a robust synchronization technique called Impulsive synchronization. We combine the text message with the chaotic signals to reduce the attack and improve the security of the data. A new method of impulsive synchronization for a class of chaotic systems is proposed and boundaries of stability region also estimated. The performance of BER in AWGN channel are verified and analyzed with MATLAB toolbox.**

Keywords: **Chaotic encryption algorithm, Impulsive synchronization, Data Security**

I. INTRODUCTION

The field of chaotic communications has gone through various periods of intense interest, initiated by Shannon's 1947 recognition that the channel capacity of a communications link can be optimized by the use of a noise-like maximal entropy signal [1] and further solidified by Chua in 1990 implementation of a chua's oscillator for generation of chaotic sequences practically [2]. Chaotic sequences are characterized by widespread random signal generation, sensitivity to initial conditions and parameter mismatches. So chaotic systems resemble direct sequence spread spectrum communication systems in that the data is spread across a relatively wide transmission bandwidth and then de spread by the intended receiver with a time-synchronized spreading sequence. These systems tend to be more computationally complex than conventional spread spectrum systems, yet they provide advantageous multipath mitigation and multi-user spectral re-use capabilities. The chaotic sequence based communication systems shows analytically better performance than direct sequence based communication systems and may in general be viewed as a generalization of direct sequence approaches. As a chaotic sequence or system evolves in a seemingly random fashion, while the direct sequence system is limited to a small finite set of values, the data security with these systems is more. The most significant limitation of chaotic communication systems is the extreme precision needed to accurately synchronize and track two independent instantiations of an "identical" chaotic circuit as used at a transmitter and a receiver. For years chaotic systems and there use in communication was absurd until the paper by Pecora and Carroll[3] who proposed a master slave synchronization of two coupled identical chaotic systems. In the early 1990s the synchronization Active research in chaotic communications was revived in the early 1990s when various chaotic circuit synchronization methods were demonstrated, leading to limited communications capabilities; each of the proposed methods had drawbacks that limited their practical implementations. During this period, the theoretical performance of chaotic communications has been shown by various authors [4][5][6][7] to exceed that of direct sequence systems. Chaotic synchronization can be viewed to be evolved through various generations and methods of synchronization. Impulsive synchronization belongs to the fourth generation of chaotic synchronization and is considered the most robust synchronization method.

The proposed work presents an impulsive synchronization approach to traditional chaotic communications to harness analog chaotic circuits' limitations for robust synchronization. Topics include a comparison of analog and digital chaotic circuits; implementation of digital chaotic circuits for use in chaotic communications; analytical, simulation, and measured hardware results for a prototype coherent communication system; and generalization of the fundamental chaotic waveform to multipath mitigation techniques, multiple access communication systems, permission-based communication systems, and a new class of maximal entropy amplitude modulated chaotic waveform hybrids for use in specific applications.

II. FORMULATION OF CHAOTIC SYSTEMS

Chaotic motion is governed by state space model using ordinary differential equations or difference equations. Accordingly chaotic motions are classified as chaotic flows represented by differential equations and chaotic maps represented by difference equations. We consider here the Newton-Leipnik system characterized by multiple attractors [9]. Newton Leipnik system is derived from Eulers rigid body equations with modification.

$$\left.\begin{aligned} \dot{x_1} &= -ax_1 + \dot{x_2} + 10x_1x_3 \\ \dot{x_2} &= -x_1 - 0.4x_2 + 10x_1x_3 \\ \dot{x_3} &= b\dot{x_3} - 5x_1x_2 \end{aligned}\right\} \quad (1)$$

Above system behaves chaotically with a=0.4 and b=0.175 as parameters and initial conditions [0.349 0 -01]

III. THEORY OF IMPULSIVE SYNCHRONIZATION

Consider a non linear system

$$\left.\begin{aligned} \dot{x} &= Ax + Bf(x) \\ y &= Cx \end{aligned}\right\} \quad (2)$$

Where $f(x)$ is matrix representing control input and nonlinearirities. This is a chaotic transmitter.
Receiver is actually designed as a non linear observer: $\dot{\hat{x}} = A\hat{x} + Bf(\hat{x}) + K(y - \hat{y})$ (3)

Error dynamics for this system are:

$$\dot{e} = \dot{x} - \dot{\hat{x}}$$

$$\left.\begin{aligned} \dot{e} &= A(x - \hat{x}) + B\big(f(x) - f(\hat{x})\big) - KC(x - \hat{x}) \\ \dot{e} &= Ae + B\big(f(x) - f(\hat{x})\big) - KCe \end{aligned}\right\} \quad (4)$$

i.e. (4)

At stead state $\dot{e} \to 0$

Solution of error dynamic equation is

$$\dot{e} = (A - KC)e + B\big(f(x) - f(\hat{x})\big) = 0$$

Let $f(x) - f(\hat{x}) = \varphi(x)$

Then $$\dot{e} = (A - KC)e + B\varphi(x) t \neq \tau_i \quad (A)$$

As per theory of impulsive control, Eqn A shows the error dynamics of the system when transmitted samples are not available to the system. i.e. when $t \neq \tau_i$.

$$\Delta e = Ket = \tau_i, i = 1,2, \dots \dots \quad (B)$$

The observer gain matrix K is chosen such that real part of all eigen values of the (A-KC) matrix lie in left half of plane.

IV. ENCRYPTION DECRYPTION

The proposed scheme can be distributed by a coupled chaotic system. The input message signal *M* is masked by the chaotic state variables and transmitted. The equations of encryption for transmitter and decryption for receiver systems are mentioned as follows:

Encrypt side (transmitter): ẋ □ □Ax □ □g(x,v) □ □Lzx. (5)

where *v* □ □*x*1 □*M*

Decrypt side (receiver): y □ □Ay □ □g(y,v)□ □ □ □Lzy. (6)

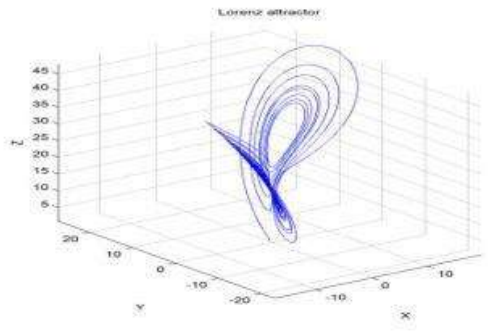


Fig. 1: The Lorenz chaotic attractor

where x €R^n , y €R^n are the state vectors. Ax and Ay are the linear part the system, g(x,v) and g(y,v) are the nonlinear part of the system, L is the controller gain of the system, K>0 is the coupling strength between master and slave system, zx and zy are the feedback signal.

From Eqs. (5) and (6), at wired chaotic security system, the encrypted message and decrypted message are shown in Fig. 2, respectively. The parameters are set at *r*=*28*, *s*=10, *b*=8/3, *h*=0.01, *l*1=0, *l*2=38, *l*3=0. The initial states of transmeter are

[$x10$,$x20$,$x30$]=[0.1,0,0] and states of slave are [$y10$,$y20$,$y30$]=[0.15,0,0].InFig.2,the decrypted message is identical to encrypted one. However, in environment like wireless, the decrypted message is critically damaged as shown in Fig. 3 due to the propagation delay, uncertainty signal fading and so on. Furthermore, the Gaussian distribution noise will be added into the transmitted chaotic signal and damaged its primal state in AWGN (Additive White Gaussian Noise) channel.

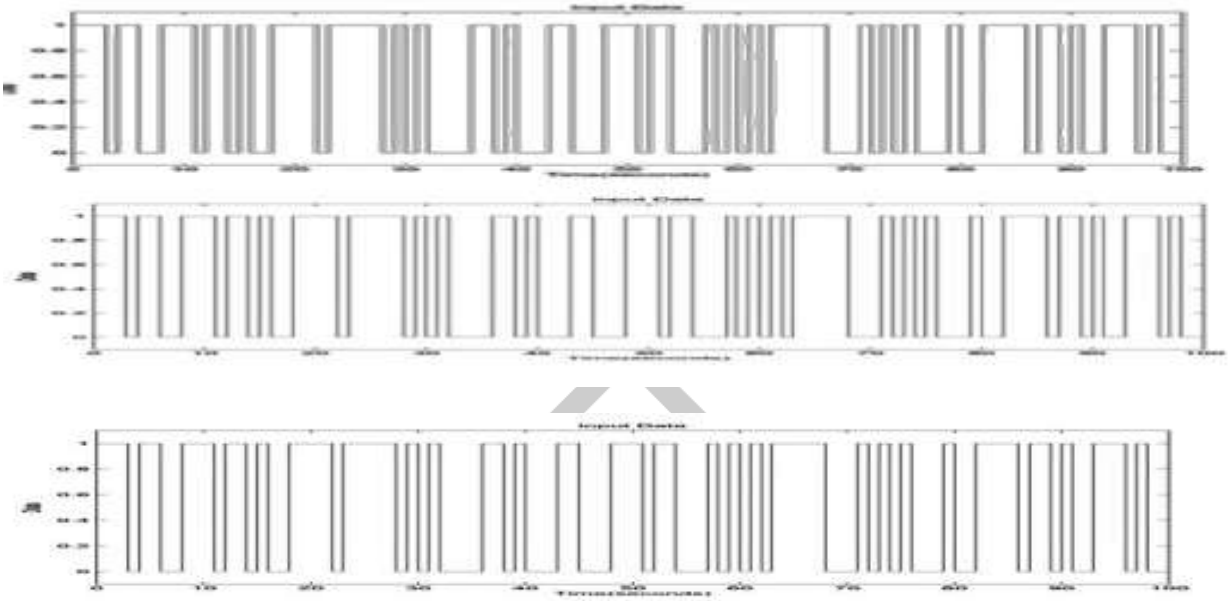


Fig. 2: for perfectly decrepted data

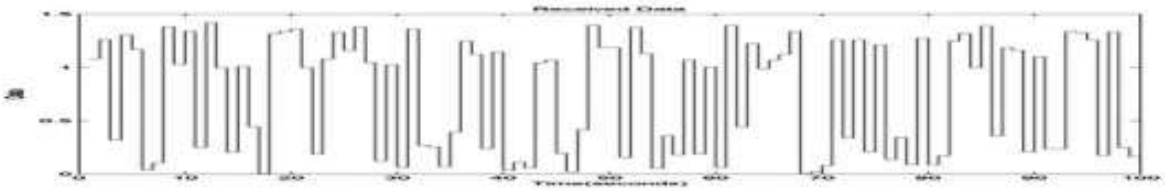


Fig. 3: Cryticaly damaged decrypt message

III. PROPOSED ALGORITHM

Following is the outline for proposed text based Chaotic Communication algorithm.

(1) Input the text message M.

(2) Using Encryption algorithm rules (5) and(6) apply chaotic encryption algorithm for encoding of the text document.
V=x+M

(3) Transmit encrypted data samples V through the transmitter channel.

(4) Receiving data from different n number of receivers ,first the impulsive observer will estimate the state variables(y) and parameters from the available samples.

(5) Apply chaotic decryption algorithm as:
M=V-y.

IV. FLOWCHART OF PROPOSED METHOD

In digital transmission, the number of bit errors is the number of received bits of a data stream over a communication channel that has been altered due to noise, interference, distortion or bit synchronization errors. The bit error rate or bit error ratio (BER) is the number of bit errors divided by the total number of transferred bits during a studied time interval. BER is a very important performance measure for any digital transmission system. The recovered message at the receiver can be subject to various factors such as noise, channel interference, channel delays and fading. BER performance of any communication system is generally evaluated as a function of SNR expressed in dB or E_b/N_o where E_b is energy per bit and N_o is noise power spectral density.
Lets see the details of flow chart which is shown in figure 4

Step 1: Take an input text message to be transmitted through the communication network. In message stream words are converted according to their ASCII values and the those ASCII numbers are converted into binary number for the transmission through the network.

Step 2: Appling Chaotic communication encryption algorithm for breaking the text message in number of data packets in encrypted form.
Step 3: Transmit encrypted data packets th though different n transmitters.
Step4: Receive data packets from n receivers.
Step 5: Find the BER and combine messages from n receivers.
Step 6: Find the threshold value and apply decryption rule to get output message.

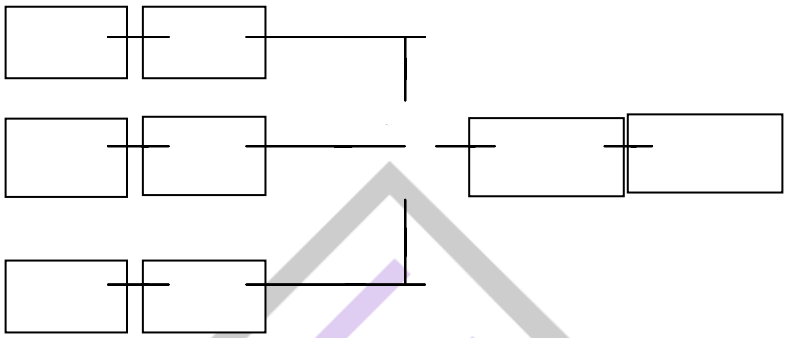


Fig. 4: Block diagram of the proposed Text Based Chaotic Communication

V. BER CALCULATION

BER peformance is important performance evaluation parameter for any digital communication system. BER is the difference in recovered bits that from transmitted one. The transmitted data through the channel is subject to change due to various influencing factors like channel noise, channel delays, multipath propagation, other channel interference etc. BER is generally expressed as a function of noise by plotting SNR versus BER. Here the BER performance is represented in terms of variance for different number of couplings at different noise level for data length of 36 bits. The noise level here is nothing N0/2 ; double sided power spectral density.

Coupling	Data Length	Noise Level	Variance
1	36	10	0.06
1	36	15	0.243
1	36	25	0.32
2	36	10	0.03
2	36	15	0.111
2	36	25	0.227
3	36	10	0.015
3	36	15	0.055
3	36	25	0.113
4	36	10	0.008
4	36	15	0.027
4	36	25	0.056
5	36	10	0.003
5	36	15	0.013
5	36	25	0.028

Table 1: BER Performance

The simulation results are also shown for depth of synchronization for different parameter mismatches. The synchronization will also affect the recovery of the original text message and the BER performance of the result.

.

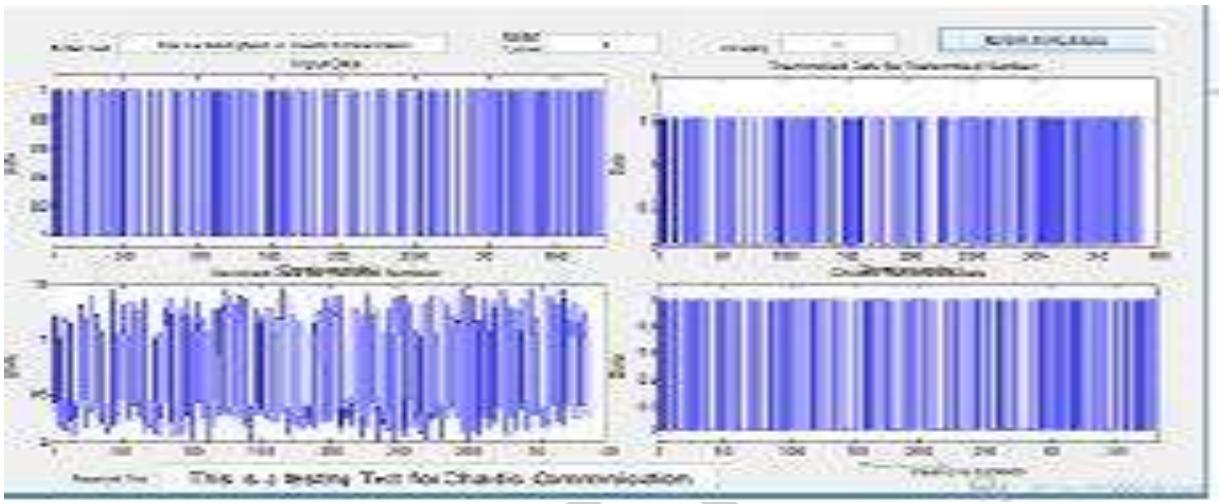


Fig. 5: Simulation Result for coupling 1 and noise level 10 with Lorentz chaotic

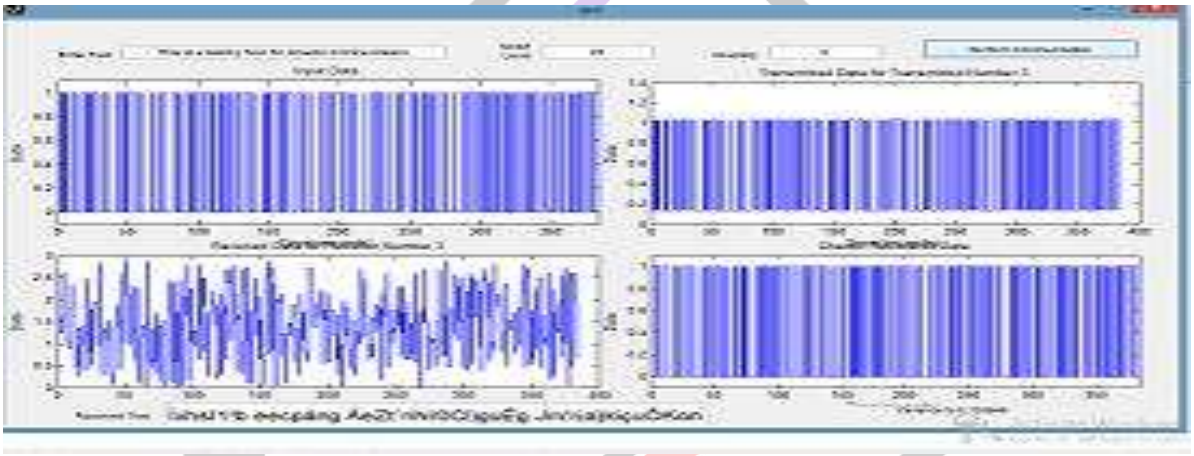
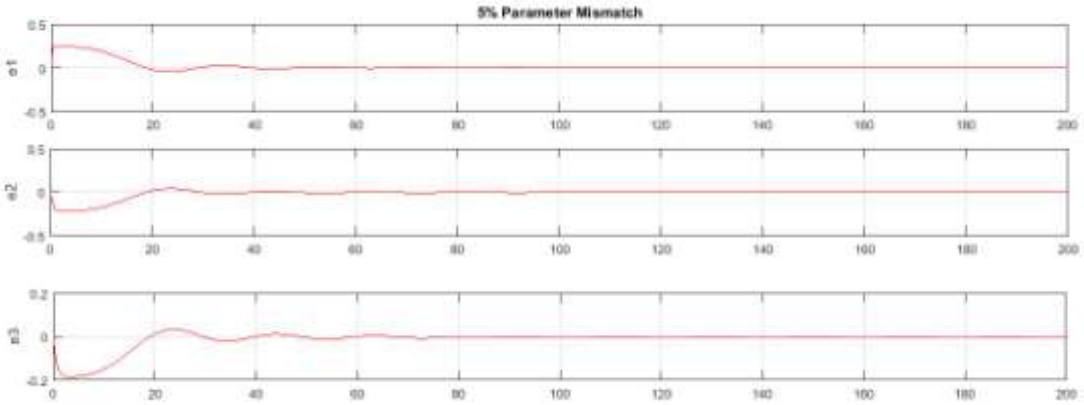


Fig. 6: Simulation Result for coupling 1 and noise level 10 without Lorentz chaotic

Following results shows the synchronization error for parameter mismatches. The parameter mismatches tend to increase the level of synchronization error. However once the error gets stabilised synchronization is said to be achieved. Thus the BER performance is a function of number of coupling, noise level and synchronization error between transmitter and receiver states

BER performance may also get affected by the level of synchronization achieved for different parameter mismatches. Following graph shows the synchronization errors for different parameter mismatches.



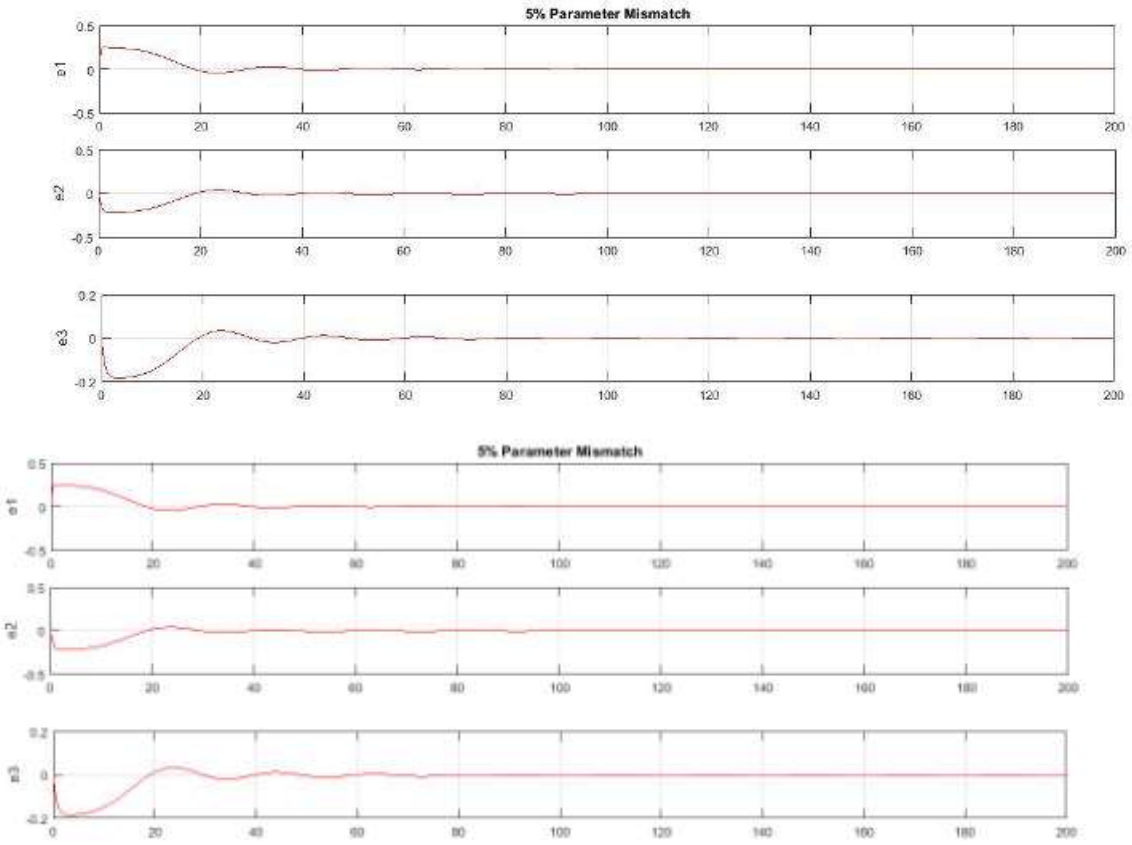


Fig. 7: Simulation Results for synchronization errors of impulsive observer

VI. CONCLUSION

The proposed work presents the methodology to secure the wireless communication. For this we used the chaotic communication system. For transferring the data from one place to another we first used encryption method and break the data into n number of packets by using chaotic encryption mechanism. We add the data packets with chaotic signals to increase the security of data transfer in the communication network. The proposed work gives the comparison of transmission of data with and without chaotic signals and we observed that the BER performance of the transmitted data is reduced with the use of impulsively controlled chaotic synchronization. Use of chaotic in the encryption and decryption has also improved security. Graph shows that we are able to transfer the data with the noise and received it on the receiver side successfully. In the simulation results, the relativity BER and number of Encrypt/Decrypt system analysis is discussed.

REFERENCES

[1] C. Shannon, "Communication in the presence of noise," Proc. Inst. Radio Eng., vol. 37, pp. 10–21, Jan 2011.
[2] L. Chua, "Dynamic nonlinear networks: State-of-the-art," IEEE Transactions on Circuits and Systems,vol. 27, pp. 1059–1087, Nov 1980.
[3] self-synchronizing chua's circuits," IEEE Transactions on Circuits and Systems II, vol. 40,pp. 634–642, 1993.
[4] R. Pickholtz, D. Schilling, and L. Milstein, "Theory of spread spectrum communications – a tutorial," IEEE Transactions on Communications, vol. 30, pp. 855–884, May 2012.
[5] G. Kolumban, M. Kennedy, and L. Chua, "The role of synchronization in digital communications usingchaos: Fundamentals of digital communications," IEEE Transactions on Circuits and Systems I: Funda-mental Theory and Applications, vol. 44, no. 10, pp. 927–936, Oct 1997.
[6] M. Hasler and Y. Maistrenko, "An introduction to the synchronization of chaotic systems: coupled skewtent maps," IEEE Transactions on Circuits and Systems I:Fundamental Theory and Applications, vol. 44,no. 10, pp. 856–866, Oct 1997.
[7] Pravin Mawale, Vrushali Shirpurka and Gouri Halde, "A Secure Chaotic Communication System" , IJSRD - International Journal for Scientific Research & Development| Vol. 2, Issue 07, 2014 | ISSN (online): 2321-0613
[8] R. Scholtz, "The origins of spread-spectrum communications," IEEE Transactions Communications,vol. 30, pp. 822–854, 2008.
[9] Sprott JC. Some simple chaotic flows. Phys Rev E 1994;50:R647–50.
[10] D. Ghosh, A. Roy Chowdhury, "Nonlinear observer based impulsive synchronization in chaotic systems with multiple attractors", Nonlinear Dyn(2010) 60:607-613.
[11] Gouri Halde, Dr.A.S.Gandhi, " Impulsive Observer Based Chaotic Synchronization with Application to Interleaved Chaotic Differential Peaks Keying", IEEE TENCON 2015,978-981.