Implementation of secure communication system using various chaotic systems

S Suchit
Dept. of Electronics and Communication Engineering
Delhi Technological University
Delhi, India
suchit981@gmail.com

Piyush Goenka
Dept. of Electronics and Communication Engineering
Delhi Technological University
Delhi, India
piyushgoenka12@gmail.com

Deva Nand
Dept. of Electronics and Communication Engineering
Delhi Technological University
Delhi, India
devkamboj@dce.ac.in

***Abstact*—This paper conducts a comparative study among various chaotic systems, implementing a secure communication system. The chaotic communication system incorporates specific synchronization and masking schemes, contributing to achieving the objectives of secure communication. This comparative analysis aims to identify the optimal choice for this application, evaluating multiple crucial parameters integral to the design. The simulation for the design has been carried out in Xilinx Vivado using Verilog HDL.**

***Keywords*—Chaotic system, Synchronization, Masking, Xilinx Vivado, Verilog HDL.**

I. INTRODUCTION

Since the advent of chaos theory, discovered by Edward Lorenz in 1963 [1], there have been a lot of discussions surrounding it and its applications. It has found its use in wide range of areas like stock markets, literary theory, music and electronics as well [2]. An example of its application in electronics is the Chua's circuit, which is a simple oscillator circuit exhibiting a variety of bifurcations and chaos [2].

Chaotic behavior, presents as irregular, aperiodic, uncorrelated, broad-band signals that defy prediction over extended periods [3]. These distinctive characteristics of chaotic systems, coupled with their sensitivity to initial conditions, makes them suitable for application in communication systems as well. This is also beneficial as the power spectrum of chaotic systems is similar to that of white noise. Several chaotic systems have been studied since the discovery of the Lorenz chaotic system.

A secure communication scheme that has been implemented, has been explored in detail in [4], and will be discussed briefly in the subsequent sections as well. Such a chaotic communication system was made possible through the self-synchronizing [5] capability of chaotic systems as well as a modulation scheme like the chaotic masking [6].

In this paper, we intend to find out the more suitable chaotic system by comparing their implementation in such a secure communication system. This comparison will be based on the synthesis results, timing information and the self-synchronizing ability of the respective chaotic systems.

To conduct this study, we have implemented the earlier mentioned design using five different chaotic systems, i.e., Lorenz, Rossler, Nose'-Hoover, Sprott-C and Rabinovich Chaotic systems [7-11].

The succeeding portions of the paper are organized as follows: Section II provides a brief exploration of the implemented design for communication and a comparison between chaotic systems. In Section III, the paper delves into the results derived from the conducted simulations, along with the conclusions drawn from these results. Lastly, Section IV explores potential avenues for future work related to the undertaken study.

II. METHODOLOGY

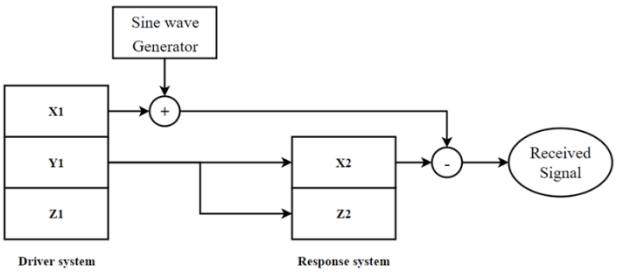

Fig. 1. Block Diagram for the Implemented Design

As shown in Fig. 1, The communication system consists of a Driver system and a Response System [4]. Both are implemented using Chaotic Systems.

The Driver system encodes the message signal, i.e., sinusoidal signal using the chaotic samples generated using the chaotic system. The Response system receives the transmitted signal and generates the same chaotic samples as the Driver to recover the original signal.

Here, the subsequent chaotic samples are generated by both Driver and Response systems by the implementation of the differential equations of the respective chaotic systems. This is done by using the Runge-Kutta 4th order method as it's an efficient method for the above purpose [12]. This approach depends on the equations that define each state within the Finite State Machine (FSM) shown in Fig 2 where, X, Y, Z represent state variables, while Fx(X, Y, Z) denotes the derivative of the state variable X. The step size, designated as h, signifies the interval between successive samples within the chaotic system. Additionally, KX1, KX2, KX3, and KX4 represent the intermediate slopes of X state variable involved in the process. Similarly, Y and Z have their intermediate slopes in the same fashion. Also, X0, Y0 and Z0 are the initial conditions.

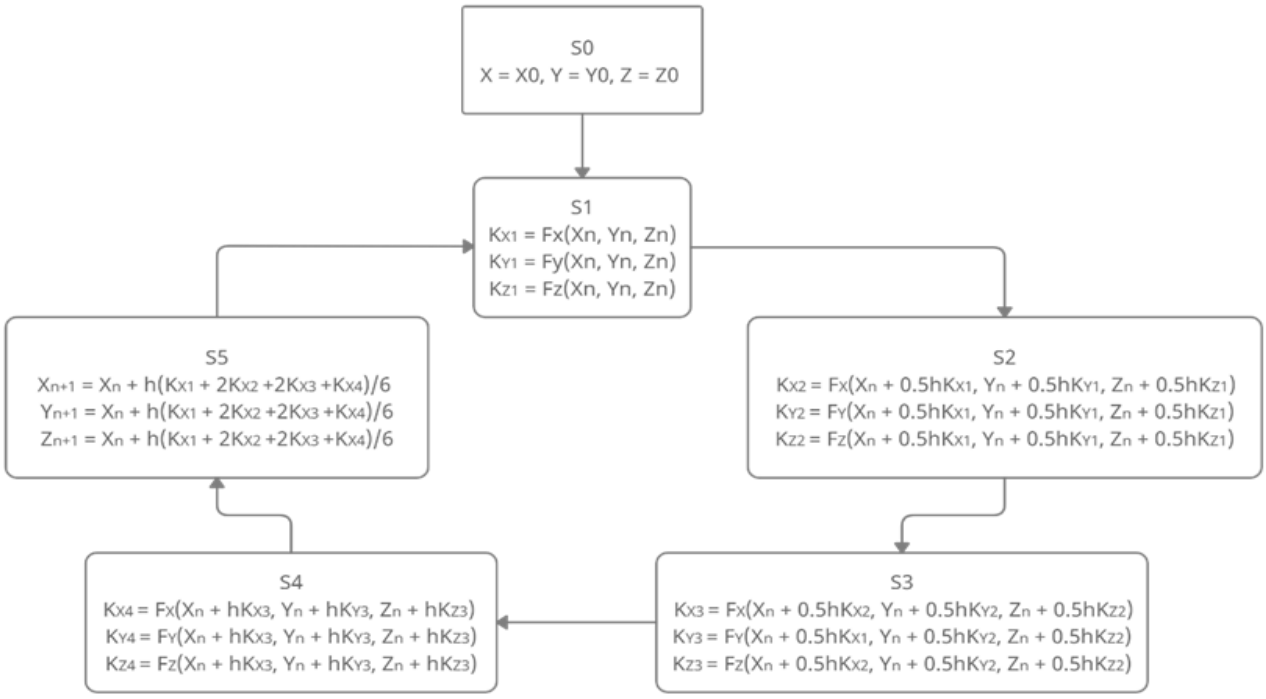

Fig. 2. Finite State Machine illustrating the implementation of a chaotic system through the RK4 method

The FSM in Fig. 2., through which the above method is being applied to generate chaotic samples in Driver and Response systems, has been implemented in Verilog HDL.

For communication to occur, synchronization between the Driver and Response systems is essential. Both systems must be capable of generating identical chaotic samples. The synchronization method employed here is 'Complete Replacement Synchronization.' In this approach, a state variable serves as the driving signal, transmitted through the communication channel to the response system alongside the actual transmitted signal. Each sample in the driving signal replaces the corresponding state variable in the response system, ensuring it produces the same sample as the driving system.

A crucial element for ensuring a secure communication method involves implementing a modulation scheme for the encryption and decryption of a message signal. This requirement is fulfilled by employing the Chaotic Masking Scheme. In this scheme, the chaotic sample generated by the driver system is added to the sinusoidal signal intended for encryption. Subsequently, in the response system, the identical chaotic sample is subtracted from the received signal to retrieve the original sample [13]. The success of this scheme depends on the synchronization of chaotic systems at both the driver and response ends, ensuring the generated chaotic samples are identical.

III. Results and Conclusions

The design was executed by employing five distinct Chaotic Systems, each characterized by three state variables and specific variable parameters. The equations corresponding to these systems are outlined below.

1. Lorenz Chaotic System:

$$x'=a(y-x) \qquad (1a)$$

$$y'=x(c-z)-z \qquad (1b)$$

$$z'=xy-cz \qquad (1c)$$

Where a=10, b=28, c=8/3 and initial conditions were (0,2,0).

2. Nose-Hoover Chaotic System:

$$x'=y \qquad (2a)$$

$$y'=-x+ yz \qquad (2b)$$

$$z'=x^2-ay^2+b \qquad (2c)$$

Where a=9, b=2 and initial conditions were (1,1,1).

3. Rossler system:

$$x'=-y-z \qquad (3a)$$

$$y'=x+ay \qquad (3b)$$

$$z'=a+z(x-c) \qquad (3c)$$

Where a=0.2,b=5.7 and initial conditions were (0,0,0).

4. Spott C system:

$$x'=y \qquad (4a)$$

$$y'=-x-yz \qquad (4b)$$

$$x'=y2-a \qquad (4c)$$

Fig. 3. Waveforms of State Variables of both Transmitter and Receiver

Where a=1 and initial conditions were (0,0.01,0).

5. Rabinovich system:

$$x'=y(h+z)-ax \qquad (5a)$$

$$y'=-x(h-z)-by \qquad (5b)$$

$$z'=-cz+xy \qquad (5c)$$

Where a=1.5, b=-0.3, c=1.67 and initial conditions were (5,5,5).

As noted in the preceding section, the application of the RK4 method is employed for implementing each chaotic system, with dependence on the step size 'h'. In this instance, the specific value assigned to 'h' is 0.0078125, and the design operates with a clock frequency of 20MHz.

The state variable Y serves as the driving signal to facilitate synchronization between the chaotic systems in both the drive and response systems. Additionally, samples derived from the state variable X execute chaotic masking on the message signal.

Communication between the Driver system and Response system was achieved successfully for all the mentioned chaotic systems and the simulation results of the design for the case of the Lorenz Chaotic system have been shown in Fig. 3. and Fig. 4. Here we can observe that the chaotic samples at both Driver and Response Systems have been generated successfully. As the Driver and Response chaotic samples are identical, we can conclude that both are synchronized successfully.

Further, it can be observed that the original message signal has been recovered. Hence secure communication has been achieved.

The design corresponding to each chaotic system has been synthesized on the xc7a200tffv1156-1 device using Xilinx Vivado, and the results have been compiled and compared in Table 1.

From Table 1., We can observe that the time taken to synchronize the Driver and Response system is the least in the case of the Lorenz Chaotic System but the Flip-Flops and DSPs utilized are at par. However, in the communication scheme employed, the synchronization time holds the utmost importance in establishing efficient communication. Due to such requirements of the design, as well as considering the trade-offs, the Lorenz Chaotic System is the preferred choice for such a secure communication system.

IV. Future Research Direction

The comparative analysis conducted herein, involving the deployment of a secure communication system as elucidated in preceding sections, offers valuable insights into the necessity of chaotic systems in communication., and the Lorenz Chaotic System stands out for its ability to achieve near-instantaneous synchronization, as demonstrated in previous sections.

Further work can be done to optimize the current design to efficiently utilize the hardware which may assist in lowering the delays as well.

Additional efforts can be directed towards implementing an enhanced synchronization scheme, potentially leading to improved security for the communication system. Exploring alternative masking schemes for the same purpose may also be considered.

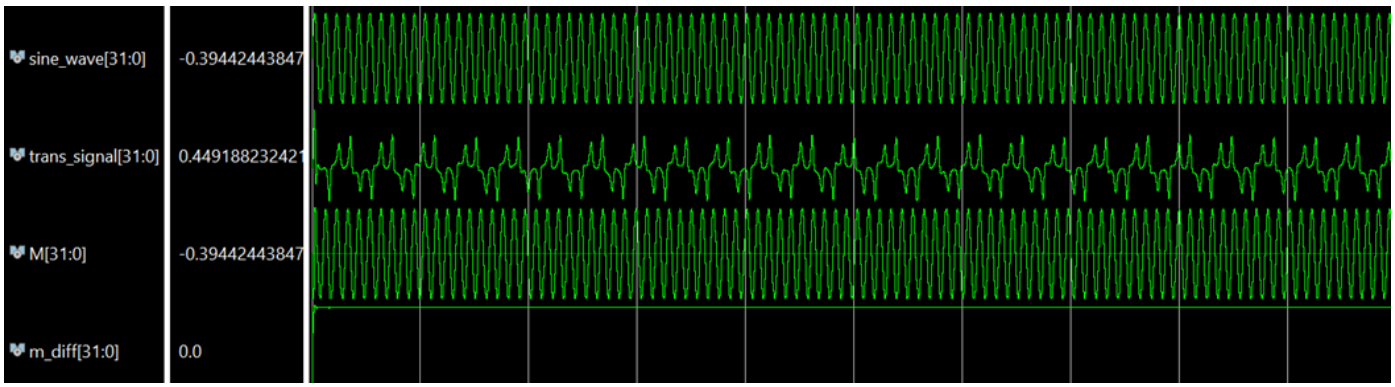

Fig. 4. Message, Transmitted, Receiver Signal and M_diff Signal

TABLE 1. Simulation and Synthesis Results

S.No.	Chaotic Systems	LUTs (in %)	FFs (in %)	DSPs (in %)	Delay (ns)	Time taken to synchronize (ms)
1.	Lorenz	9.51	0.373	23.78	50.852	0.842
2.	Nose-Hoover	7.53	0.372	26.48	55.243	123.197
3.	Rossler	8.16	0.375	20	50.497	57.850
4.	Sprott C	5.85	0.372	20.54	46.159	116.043
5.	Rabinovich	14.05	0.38	25.94	53.161	7.405

REFERENCES

[1] Lorenz, N. Edward “Deterministic Nonperiodic Flow". Journal of Atmospheric Sciences 20.2 (1963): 130-141.

[2] H.R. Biswas, M.M. Hasan and S.K. Bala. Chaos theory and its applications in our real life. *Barishal University Journal Part, 1*(5), pp.123-140, 2018.

[3] A. Abel and W. Schwarz, "Chaos communications-principles, schemes, and system analysis," in Proceedings of the IEEE, vol. 90, no. 5, pp. 691-710, May 2002, doi: 10.1109/JPROC.2002.1015002.

[4] S. Suchit and K. Suneja, "Implementation of Secure Communication System Using Chaotic Masking," 2022 IEEE Global Conference on Computing, Power and Communication Technologies (GlobConPT), New Delhi, India, 2022, pp. 1-5, doi: 10.1109/GlobConPT57482.2022.9938303.

[5] L. M. Pecora and T. L. Carroll, ‘‘Synchronization in chaotic systems,’’ Phys. Rev. Lett., vol. 64, pp. 821–823, Feb. 1990

[6] K. M. Cuomo and A. V. Oppenheim, ``Circuit implementation of synchronized chaos with applications to communications," *Phys. Rev. Lett.*, vol. 71, pp. 65_68, Jul. 1993. Signal masking

[7] O. E. Rossler, An equation for continuous chaos, Phys. Lett. A 57 (1976) 397-398.

[8] J. C. Sprott, Some simple chaotic flows, Phys. Rev. E 50 (1994) 647-650.

[9] İ. Pehlivan and Y. Uyaroglu, A new chaotic attractor from general Lorenz system family and its electronic experimental implementation, Turk. J. Elec. Eng. Comp. Sci. 18 (2010) 171-184

[10] A.S. Pikovski, M.I. Rabinovich, V.Y. Trakhtengerts. Onset of stochasticity in decay confinement of parametric instability, Sov. Phys. JETP, 47: 715-719, 1978.

[11] B.L. Holian,W.G. Hoover,:Numerical test of theLiouvilleequation. Phys.Rev. 34(5), 4229–4237(1986)

[12] A. Garg, B. Yadav, K. Sahu, and K. Suneja , "An FPGA based Realtime Implementation of Nosé hoover Chaotic System using different numerical Techniques," 2021 7th International Conference on Advanced Computing and Communication Systems (ICACCS), 2021, pp. 108-113, doi10.1109/ICACCS51430.2021.9441923.

[13] K. M. Cuomo and A. V. Oppenheim, ``Circuit implementation of synchronized chaos with applications to communications," *Phys. Rev. Lett.*, vol. 71, pp. 65_68, Jul. 1993. Signal masking