Chaotic Secure Communication Schemes employing Chua's Circuit

I.A. Kamil
Department of Electrical & Electronic Engineering
University of Ibadan
Ibadan, Nigeria
ismaila.kamil@mail.ui.edu.ng

O.A.Fakolujo
Department of Electrical & Electronic Engineering
University of Ibadan
Ibadan, Nigeria
ao.fakolujo@mail.ui.edu.ng

Abstract—In recent years, chaotic secure communication systems have attracted significant interest due to their higher unpredictability over conventional secure communications systems and simplicity of implementation. This study presents the modeling of four chaotic modulation techniques. The techniques are Chaotic Masking (CM), Chaos Shift Keying (CSK), Chaos On-Off Keying (COOK), and Differential Chaos Shift Keying (DCSK). Simulations were carried out using Simulink in Matlab environment to implement these techniques. A qualitative evaluation of the transmitted signal waveforms in all the cases considered showed that DCSK gives the highest level of security followed by CSK while COOK gives the least level of security. The data transmission rate of the other three techniques was however twice that of DCSK.

Keywords-chaotic secure communication, modulation scheme

I. INTRODUCTION

In recent years, there has been appreciable growth in personal communications most especially in the area of mobile communication and the internet. Data encryption and security are essential ingredients of personal communication that are recently receiving attention because of the need to ensure that the information being sent is not intercepted by an unwanted listener. Besides, these are very essential for protecting the content integrity of a message as well as its copyright [1].

Chaos based secure communication has been of much interest in the recent time since it offers potential advantage over conventional methods due to its simplicity [2] and high unpredictability which means higher security. Besides, analog implementation is possible [3].

Many chaotic secure communication schemes have been reported in literature but only a few of them have actually witnessed practical implementation. This paper attempts to model and simulate four of these schemes using Simulink in Matlab. The choice of Simulink was to bring the schemes as close to practical implementation as possible since each Simulink block can easily be replaced by a practical unit. The four schemes considered were Chaotic Masking, Chaos On-Off Keying, Chaos Shift Keying and Differential Shift Keying.

II. THEORY

A. Background

Chaos communication is rather a new field in the communication research. It evolved from the study of chaotic dynamical systems, not only in mathematics, but also in physics or electrical engineering somewhere at the beginning of 1990 [4].

Chaotic signals are irregular, aperiodic, uncorrelated, broadband, and impossible to predict over long times. These properties coincide with the requirements for signals applied in conventional communication systems, in particular spread-spectrum communications, multi-user communications, and secure communication.

B. Chaotic System

The chaotic system employed in this work is the Chua's circuit which is a 3rd order autonomous dissipative electrical circuit consisting of a linear inductor L, two capacitors C_1 and C_2, a linear resistor R and a non-linear resistor N_R often referred to as the Chua's diode [5].

The state equations for the Chua's circuit are given by:

$$\begin{aligned} \frac{dv_{c1}}{dt} &= \frac{G}{C_1}(v_{c2} - v_{c1}) - \frac{1}{C_1}h(v_{c1}) \\ \frac{dv_{c2}}{dt} &= \frac{G}{C_2}(v_{c1} - v_{c2}) + \frac{1}{C_2}i_L \\ \frac{di_L}{dt} &= \frac{1}{L}v_{c2} \end{aligned} \quad (1)$$

where v_{c1}, v_{c2} and i_L are the voltages across C_1, the voltage across C_2 and the current through L, respectively, $h(v_{c1})$ is the piece-wise linear v-i characteristic of the Chua's diode and is given by :

$$h(v_{c1}) = G_b v_{c1} + \frac{1}{2}(G_a - G_b)(|v_{c1} + B_p| - |v_{c1} - B_p|) \quad (2)$$

where B_p is the breakpoint voltage of the Chua's diode and G_a and G_b are the slopes of the inner and outer regions respectively.

C. Chaos Modulation Schemes

Four modulation schemes considered in this paper are Chaotic Masking (CM), Chaos On-Off Keying (COOK), Chaos Shift Keying (CSK) and Differential Chaos Shift Keying (DCSK).

1) Chaotic Masking

In chaotic masking, two identical chaotic are used: one at the transmitter end and the other at the receiver. As shown in Fig. 1, the message signal m(t) is added to the chaotic mask signal c(t) giving the transmitted signal s(t). The chaotic system at the receiver end produces another copy of the chaotic mask signal $\hat{c}(t)$ which is subtracted from the transmitted signal r(t) to obtain the recovered message signal $m'(t)$.

Assuming a noise free channel and perfect synchronization between the two chaotic systems, $s(t)=r(t)$, $c(t)=\hat{c}(t)$ and $m(t)=m'(t)$. For higher security of the message signal, Yang reported that the message signal is typically made about 20dB to 30dB weaker than the chaotic signal [6].

2) Chaos Shift Keying

In this modulation scheme, the message signal, which is a digital signal, is used to switch the transmitted signal between two statistically similar attractors $c_0(t)$ and $c_1(t)$ which are respectively used to encode bit 0 and bit 1 of the message signal. The two attractors are generated by two chaotic systems with the same structure but different parameters [7].

At the receiver end, the received signal is correlated with a synchronized reproduction of any of the two chaotic signals used in the transmitter. The message signal is recovered by low-pass filtering and threshholding the synchronization error. The block diagram representation of the scheme is shown in Fig. 2.

3) Chaos On-Off Keying

Chaos On-Off Keying is similar to CSK in all respects except that only one chaotic signal is used in transmission of message signal. When the message signal is bit 1, the chaotic signal is transmitted, but when the message signal is bit 0 no signal is transmitted. The same procedure is used in demodulating the received signal as in CSK as shown in Fig. 3.

4) Differential Chaos Shift Keying

In Differential Chaos Shift Keying, no synchronization is required as in the other three schemes earlier described.

The same chaotic signal used at the transmitter (called reference signal) is transmitted and used to demodulate the message signal at the receiver end. This is illustrated in Fig. 4.

In this scheme, every bit is transmitted two sample functions. The first sample function serves as the reference while the second one carries the information. Thus, bit 1 is sent by transmitting the reference signal twice in succession and bit 0 is sent by transmitting the reference signal followed by an inverted copy of the reference signal. The two sample functions are correlated in the receiver and the decision is made by thresholding [7].

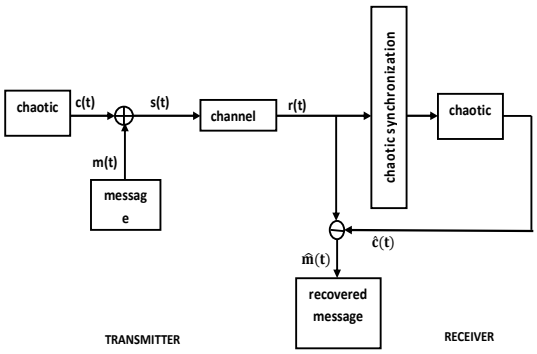

Figure 1. Chaotic Masking

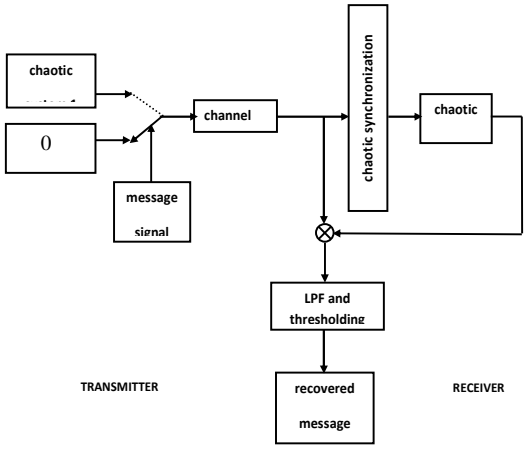

Figure 2. Chaos On-Off Keying

III. SIMULATION

A. Chua's Circuit

With the component values for Chua's circuit given as follows: C1=10nF, C2=100nF, L=18mH, G= 1/1655 S, Ga=-0.756mS, Gb=-0.409mS and Bp=1.08V, Chua's equations can be re-written as:

$$\begin{aligned} \frac{dv_{c1}}{dt} &= (10)(0.604)(v_{c2} - v_{c1}) - 10\,h(v_{c1}) \\ \frac{dv_{c2}}{dt} &= (0.604)(v_{c1} - v_{c2}) \\ \frac{di_L}{dt} &= -(5.6)v_{c2} \end{aligned} \tag{3}$$

where v_{c1} and v_{c2} have been expressed in volts but i_L in milliampere. The time series for the three state variables is shown in Fig. 5.

B. Self Synchronization of Chua's Circuits

The receiver is made up of two stable subsystems decomposed from the original system using Pecora & Carrol Scheme [8]. The first subsystem,(v'_{c2}, i'_L) referred to as the first response subsystem, is driven by v'_{c1} from the transmitter to give an output v'_{c2}:

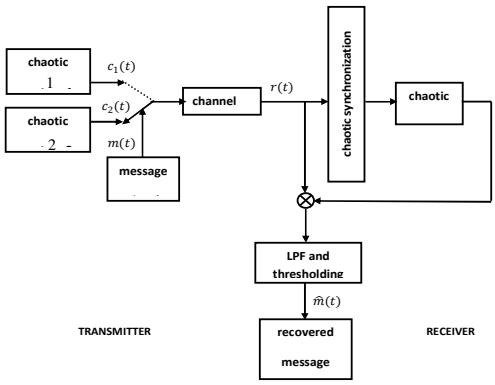

Figure 3. Chaos Shift Keying

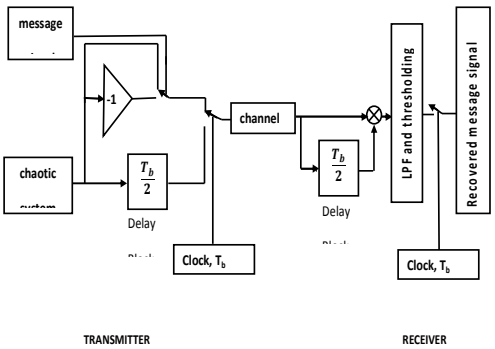

Figure 4. Differential Chaos Shift Keying

$$\frac{dv'_{c2}}{dt} = \frac{G}{C_2}(v_{c1} - v'_{c2}) + \frac{1}{C_2} i'_L$$
$$\frac{di'_L}{dt} = \frac{1}{L} v'_{c2} \quad (4)$$

The second subsystem, (v'_{c1}) referred to as the second response subsystem is driven by v'_{c2} to give v'_{c1} as output:

$$\frac{dv'_{c1}}{dt} = \frac{G}{C_1}(v'_{c2} - v'_{c1}) - \frac{1}{C_1} h(v'_{c1}) \quad (5)$$

Since the Lyapunov exponents of the response systems is negative, $v_{c1} \approx v'_{c2}$ and synchronization is thus achieved. The receiver is therefore given by:

$$\frac{dv'_{c1}}{dt} = \frac{G}{C_1}(v'_{c2} - v'_{c1}) - \frac{1}{C_1} h(v'_{c1})$$
$$\frac{dv'_{c2}}{dt} = \frac{G}{C_2}(v_{c1} - v'_{c2}) + \frac{1}{C_2} i'_L \quad (6)$$
$$\frac{di'_L}{dt} = \frac{1}{L} v'_{c2}$$

The transmitter and the receiver systems were modeled with Simulink. For the transmitter, the initial conditions were $v_{c1}(0)=0.001$; $v_{c2}(0)=-0.05$ and $i_L(0)=-0.02$ and for the receiver, the initial conditions were: $v'_{c1}(0)=1.0$; $v'_{c2}(0)=-0.05$ and $i'_L(0)=-0.02$. The trajectories produced after simulation are illustrated in Fig. 6 with bold curve representing the transmitter signal and dashed curve the receiver's.

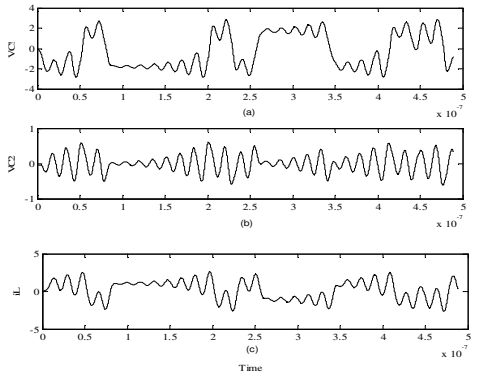

Figure 5. Chua's Circuit time series (a) V_{C1} (b) V_{C2} (c) i_L

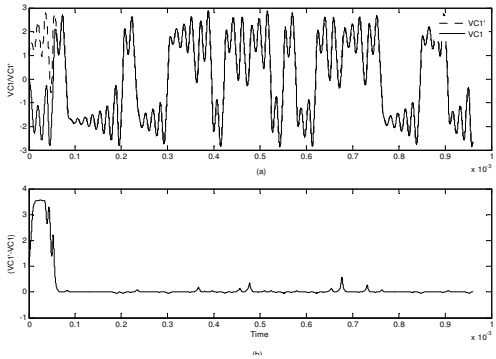

Figure 6. Self synchronization of two Chua's circuits using v_{C1} as drive signal with different initial conditions and parameter values, (a) Time series of v_{C1} and v'_{C1}, (b) Synchronization Error.

A parameter variation of 0.1 was also introduced between the transmitter and receiver systems. The time series and orbit difference for the two systems are as shown in Fig. 6

C. Chaos Modulation Schemes

The four schemes earlier described were modeled and simulated with Simulink using self-synchronized Chua's circuits. The simulation results are shown in Figs. 7 to 10.

IV. DISCUSSIONS

The results obtained in Fig 6 showed that a difference in initial conditions and slight parameter variation that would otherwise have caused the two chaotic systems (transmitter and receiver) to produce divergent time series, had no effect when the two were synchronized using self synchronization approach as the two trajectories converged within a very short.

Figs. 7, 8, 9 and 10 confirmed the effectiveness of the four modulation schemes as the message signals were recovered at the receiver.

The transmitted signal waveform in Fig. 9 showed that COOK has the lowest security as it is quite easy for an intruder to guess when different bit values are transmitted.

Fig. 8 showed that it is a little more difficult to guess the bit values in CSK especially if the two chaotic systerms used are very different from one another.

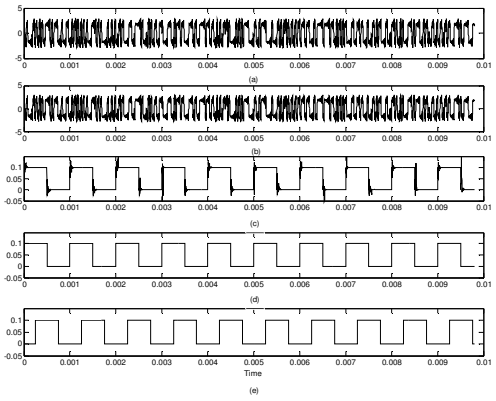

Fig.ure 7. Chaotic Masking using Chua's circuits (a) chaotic signal (b) transmitted signal (c) recovered message signal with synchronization error (d) transmitted message signal (e) recovered message signal

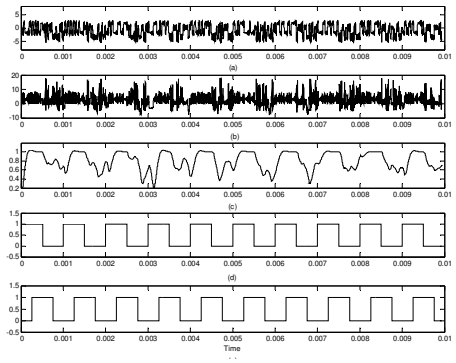

Figure 8. Chaos Shift Keying using Chua's circuits (a) transmitted signal (b) correlated signal (c) thresholded and filtered signal (d) transmitted message signal (e) recovered message signal

Fig.7 showed that if the magnitude of the message hidden in the chaotic sugnal is not high, Chaotic Masking is more secure than CSK as it is more difficult to distinguish the part of the waveform representing bit 1from that respresenting bit 0.

Fig 10 showed that in DCSK the nature of the transmitted bit is not reflected at all in the transmitted waveform. Thus it is almost impossible for any intruder to guess the transmitted message. Thus, DCSK provided the highest security followed by chaotic masking while COOK provided the lowest level of security.

It was observed in Fig. 10 that twice the time used for transmitting a bit in other three schemes was used in DCSK Thus the transmission rate of DCSK was twice those of others.

V. CONCLUSIONS

We have discussed in this paper the use of Simulink to demonstrate various chaotic secure communication schemes. We have assumed an ideal noiseless communication channel in this study. Further work is on going to demonstrate same for a practical noisy channel.

REFERENCES

[1] M. P., Kennedy, R. Rovatti, and G. Setti,, Chaotic Electronics in Telecommunications. Boca Raton: CRC Press LLC, 2000.

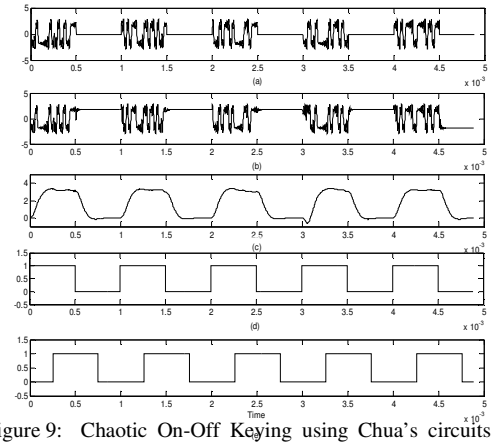

Figure 9: Chaotic On-Off Keying using Chua's circuits (a) chaotic signal (b) transmitted signal (c) correlated and filtered signal (d) transmitted message signal (e) recovered message

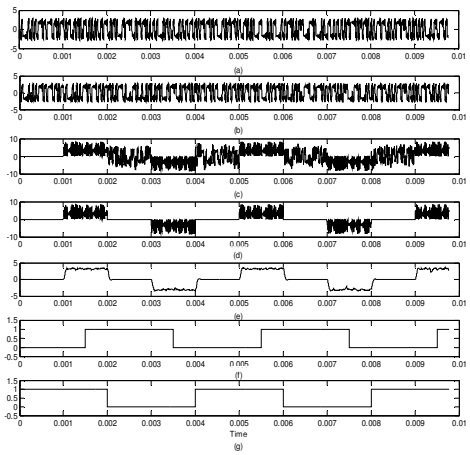

Figure 10: Differential Chaos Shift Keying using Chua's circuits (a) chaotic signal (b) transmitted signal (c) correlated signal (d) thresholded signal (e) filtered signal (f) transmitted message signal (g) recovered message signal

[2]` M. Itoh, "Spread Spectrum Communication Via Chaos," Int. Jour. of Bifurc. & Chaos, Vol. 9, No.1, pp. 155-213, 1999.

[3] L. S. Tsimring, and R. Tenny, "Security Issues in Chaos-based Communication and Encryption," Proc. of Winter School on Chaotic Communication, Institute for Nonlinear Science, UCSD, 2003

[4] A. Abel and W. Schwarz, "Chaos Communications – Principles, Schemes and Systems." Proc. IEEE, vol. 90, no. 1, pp. 691-709, 2002.

[5] M. Mulukutla and C. Aissi, "Implementation of Chua's Circuit and its Applications," Proc. ASEE Gulf-Southwest Annual Conf., Session IVB5, 2002

[6] T.Yang, "A Survey of Chaotic Secure Communication Systems," Int. Jour. of Comp. Cognition, Vol. 2, No. 2,, pp 81-130, 2004.

[7] G. Kolumban, M. P. Kennedy, and L. O. Chua, "The Role of Synchronization in Digital Communications Using Chaos – Part II: Chaotic Modulation and Chaotic Synchronization," IEEE Trans. Circuits & Syst. I: Fund. Theory & Appli., Vol. 45, No. 10, pp. 1129-1140, 1998.

[8] K. M. Cuomo, A. V. Oppenheim, and S. H. Strogatz, "Synchronization of Lorenz-Based Chaotic Circuits with Applications to Communications," IEEE Trans. Circuits & Syst. II - Analog & Digital Signal Processing, Vol. 40, No. 10, pp. 626-633, 1993.