Cryptographic study of functional message using two chaotic models

Berguellah Nourelhouda[*]
Department of Mathematics
University of Constantine 1
Constantine 25000
Algeria
berguellahnour85@hotmail.com

Hamri Nasr-Eddine
Department of Science and Technology
University Center of Mila
Mila 43000
Algeria
n.hamri@centre-univ-mila.dz

Abstract. In this paper we present two chaotic models used for secure transmission of a functional message which is the function $\sin \omega t$, without forgetting the role of synchronization mechanisms of chaotic systems to the success of these transmissions.

Keywords: chaos, synchronization, cryptography, CSK modulator, CSK demodulator.

1. Introduction

Hide specific information to certain persons always been a major interest of people. Thus, we have sought to establish technics called "encryption" in order to make this information incomprehensible to those who do not have access to a secret "key." In the past century, several researchers have examined the unusual behavior of chaotic dynamical systems and it was found that some systems showed very strange nature of instabilities. It was the discovery of chaotic signals whose behavior completely deterministic but are reminiscent of gaits pseudo-random. A universal definition of chaos exists not really, mathematicians who study chaotic systems use certain characteristics of stability system (Lyapunov exponents) for defining a chaotic behavior [2].

In 1990, Pecora and Carroll published a paper [1] in which they present theoretical and experimental demonstration of the ability to synchronize two chaotic systems. Here, the synchronization means that two chaotic systems with the same structure but of course with initial conditions different are led to reproduce the same chaotic signal. This phenomenon appeared to be impossible for systems chaotic [2] [3] (these are very sensitive to disturbances on their

[*]. Corresponding author

trajectories) was a revolution in the community scientific, thus the use of the chaos in cryptography [4].

Initially, several electronic assemblies simulating synchronization of Lorenz and Rössler systems were achieved [5]. They were followed by numerous configurations to allow transmission of signals "secure" [6], the most notably those of Cuomo [7] in 1992 that used a transmission by masking and spread spectrum. In the decade that followed there were many other configurations and improvements of existing ones [8]. In our report we will study on detail the use of two chaotic models; "Four scroll" model [10],[12],[13] and Lorenz model [11],[14] to secure a functional message which is the function $\sin \omega t$ by using Chaos Shift Keying method [9].

2. Characterization of the chaotic systems

2.1 Four-scroll model

Consider the Four-scroll pattern [12],[13]:

$$\begin{cases} \dot{x}_1 = ax_1 + y_1 z_1 \\ \dot{y}_1 = -by_1 + x_1 z_1 \\ \dot{z}_1 = -cz_1 + x_1 y_1 \end{cases} \tag{1}$$

x, y and z are state variables, and a, b and c real parameters, consistent and positives. In the following numerical data : $a = 0,4,\ b = 12\ et\ c = 5$, the system four scroll (1) have the chaotic attractor of Figure 1.

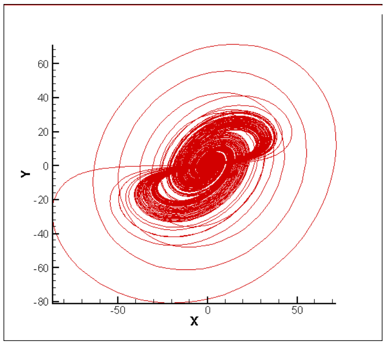

Figure 1: Four-scroll attractor

2.2 Lorenz model

Consider the Lorenz pattern [14]:

$$\begin{cases} \dot{x}_1 = a(y_1 - x_1) \\ \dot{y}_1 = bx_1 - x_1 z_1 - y_1 \\ \dot{z}_1 = x_1 y_1 - c z_1 \end{cases} \tag{2}$$

x, y and z are state variables, and a, b and c real parameters, consistent and positives. In the following numerical data : $a = 10$, $b = \frac{8}{3}$ *et* $c = 28$, the Lorenz system (2) have the chaotic attractor shows in Figure 2.

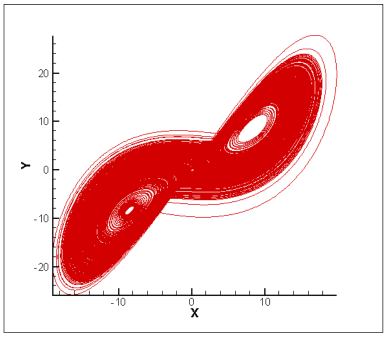

Figure 2: Lorenz attractor

3. Using the chaotic models for secure communications

The basic idea is to blur a message adequately with the chaos at the transmitter level, in order to conceal intruder before forwarding it to its destination, which will be the only able to decipher it. So in this work we will have an encrypted functional message using two chaotic systems fourscroll model [11],[12] and Lorenz model [14] by Chaos Shift Keying method [9] which noted by CSK.

3.1 CSK modulator

This method proposed for the first time by the Dedieu group [9], and its current denomination known by "Chaos shift keying: CSK". The CSK method defined as a digital modulation, it's inspired by the classical techniques of modulation such as FSK (frequency shift keying) ASK (amplitude Shift keying) and the PSK (phase shift keying). Then the masked system by CSK method is consisting CSK modulator at the transmitter and a CSK demodulator at the receiver connected by a router channel of the signal as shown in the figure (3).

So, its basic idea is the same as the classical digital modulation, that is to associate with each symbol of the message not a sinusoidal carrier, but a different chaotic carrier, moving in duration T. The elements of the digital signal message

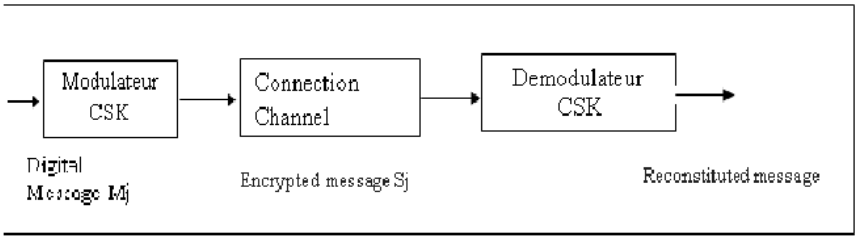

Figure 3: Simplified schema of a CSK method for encryption system

include in the area of M-level symbols modulated by CSK method are defined by:

$$S(t) = \sum_{j=1}^{n} m_j g_i(t) \tag{3}$$

where: m_j are the elements of the message signal vector and $g_i(t)$ are the chaotic carrier. And $j = 1, 2......N$; $i = 1, 2......M$ et $N \leq M$

$$m_j = \sin \omega t \tag{4}$$

Figure (4) shows the shape of the message signal mj before the modulation.

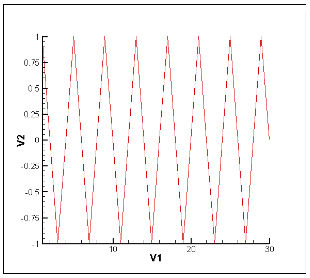

Figure 4: The appearance of the message signal before encryption (Message to the encrypted signal).

3.1.1 CSK modulator using Four-scroll model

Because the speed of the message signal (which we will mask it) is limited by the time of synchronization T second of the chaotic oscillators (5 second in our case [10]) we choose in our simulation the function $\sin \omega t$, with $\omega = \frac{\pi}{2}$ generating sequences 1 and -1, and we adjusted its flow T second equal to 15 second more than the synchronization time T second for the probability of occurrence of 1 and -1.

It has been verified [10] that the system (1), which considered as master system synchronizes identically with a slave system whose state equations are given by :

$$\begin{cases} \dot{x}_2 = ax_2 + y_2z_2 + u \\ \dot{y}_2 = -by_2 + x_2z_2 \\ \dot{z}_2 = -cz_2 + x_2y_2 \end{cases} \tag{5}$$

where : u is the coupling control chosen by :

$$u = -y_1z_1 + y_2z_2 - (a+1)(x_2 - x_1)$$

With the parameters given in the reference [10]. At time $t = 5$ second, it was found that the timing error between the systems (1) and (5) tending towards 0 second. So we will consider the synchronization Time T second around 15 second.

In our simulation, we used two chaotic oscillators $G1$ (master system) and $G2$ (slave system) to code the 1 and -1 message signal. They are similar but statistically different. Concerning their parameters were chosen respectively:

1. System $G1$: $x_1(0) = 0, \ \ y_1(0) = 1, \ \ z_1(0) = 1$
2. System $G2$: $x_2(0) = -5,6, \ \ y_2(0) = 13,6, \ \ z_2(0) = -12,5$

At the reception, the synchronization blocks $G1$ and $G2$ whose state equations are those of the systems (1) and (5) respectively, the parameters are identical to systems $G1$ and $G2$. At the output of the CSK modulator, the signal $S(t)$ is shown in Figure (5).

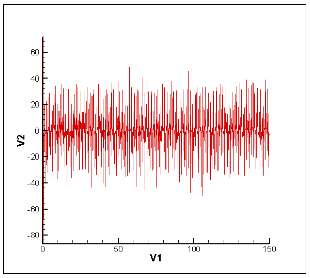

Figure 5: The appearance of the message signal after CSK encryption using Four-scroll model

3.1.2 CSK modulator using Lorenz model

By the same idea of CSK modulator, the message signal will be encrypted. In this case the synchronization time will be adjusted flow T second equal to 15 second more than the synchronization time (4 second in our case [14]) for the probability of occurrence of 1 and -1, because the speed of the message signal (which we will mask it) is limited by the time of synchronization. It has been verified [14] that the system (2), which considered as master system synchronizes identically with a slave system whose state equations are given by :

$$\begin{cases} \dot{x}_2 = a(y_2 - x_2) + C_1 \\ \dot{y}_2 = bx_2 - x_2z_2 - y_2 + C_2 \\ \dot{z}_2 = x_2y_1 - cz_2 + C_3 \end{cases} \tag{6}$$

where : C_1, C_2 and C_3 are three coupling control functions. With properly choice of C_1, C_2 and C_3 and with the parameters given in the reference [14], at time $t = 4$ second, it was found that the timing error between the systems (2) and (6) tending towards 0 second. So we will consider the synchronization Time T second around 15 second.
In our simulation, we used two chaotic oscillators $G1$ (master system) and $G2$ (slave system) to code the 1 and -1 message signal. They are similar but statistically different. Concerning their parameters were chosen respectively:

1. System $G1$: $x_1(0) = 1, \;\; y_1(0) = 1, \;\; z_1(0) = 0$
2. System $G2$: $x_2(0) = 0,2, \;\; y_2(0) = 0,3, \;\; z_2(0) = 0,1$

At the reception, the synchronization blocks $G1$ and $G2$ whose state equations are those of the systems (2) and (6) respectively, the parameters are identical to systems $G1$ and $G2$. At the output of the CSK modulator, the signal $S(t)$ is shown in Figure (6).

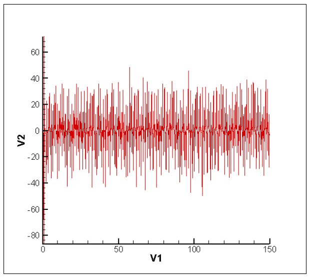

Figure 6: The appearance of the message signal after CSK encryption using Lorenz model

3.2 CSK demodulator

3.2.1 CSK demodulator using Four-scroll model

Assuming that the encrypted message signal $S(t)$ is received by the authorized receiver, shown in Figure (6), without disturbance. At this level we have a synchronization of the two oscillators $G1$ or $G2$ respectively, with the signal received $S(t)$, depending on whether the value of the message signal mj equal 1 or -1. This result is identified by canceling error signal of synchronization e_1, as shown in Figure (7).

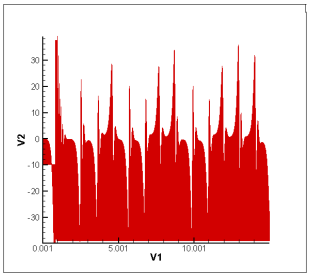

Figure 7: Detecting synchronization areas of $G1$ and $G2$ for Four-scroll model

From this synchronization error, we will take the decision of retrieve the message signal in the decision block.

The processing procedure in this block can be summarized as follow:

1. whatever the error sign of the identical synchronization between two chaotic signals, the basic rule is the zero error involves the synchronization. Figure (7) represents the detection of the synchronization areas of $G1$ and $G2$, and the signals of the function $\sin \omega t$ which are enveloping the chaotic carrier. To detect these envelopes, we proceeded as in classical demodulation, clipping our signal in the interval $[-10, 10]$ by the limiting stage. This will provide the signal shown in Figure (8).

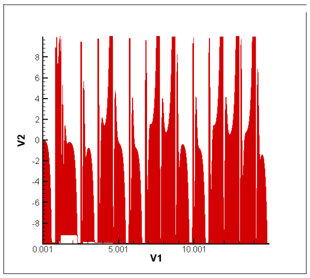

Figure 8: Limited values of synchronization error signal for Four-scroll model.

2. Then these signals are filtered by low-pass filters, to mitigate the chaotic carrier and keep the envelopes of $\sin \omega t$. The filtered signal is shown in Figure (9).

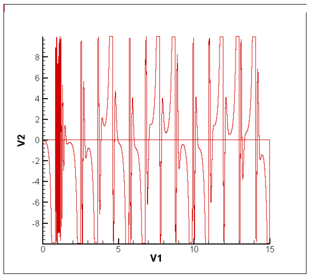

Figure 9: Filtering the error signal for Four-scroll model.

3. The signals of the function $\sin \omega t$ results of signal error, will be shown in Figure (10) by thresholding and comparison. We have used for this the comparator stage performing the following operation :

$$\begin{cases} 1 \Rightarrow signal \geq 0 \\ -1 \Rightarrow signal < 0. \end{cases}$$

We will have the signal shown in Figure (10).

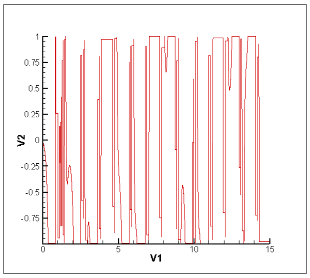

Figure 10: Thresholding and comparison of error signal for Four-scroll model.

4. To reconstruct the original signal, we have performed detecting the error signal rising edges as shown in the figure (10) by the detector rising edges stage. This signal becomes as shown in Figure (11).

5. By comparing the signal shown in Figure (11) with the original signal message mj shown in Figure (4), It was noted that the message signal was slightly tilted according to the error signal $\sin \omega t$. So to recover the original message signal, this signal will be injected into an T flip-flop.

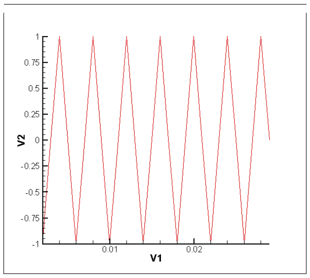

Figure 11: Detection of the rising edge for Four-scroll model.

Figures (12) represent the signal reconstructed by the decrypting operation using Four-scroll model and the original signal respectively. So they are identique.

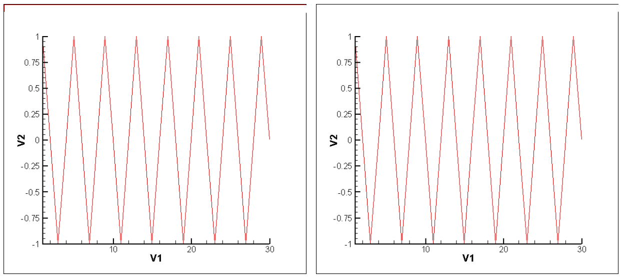

Figure 12: Message after decryption for Four-scroll model at the right and the original message at the left.

3.2.2 CSK demodulator using Lorenz model

Now, we will decrypt the signal message which we masked it using Lorenz model by the same steps of CSK demodulator. Firstly, whatever the error sign of the identical synchronization between the two chaotic signals, the basic rule is the zero error involves the synchronization. Figure (13) represents the detection of the synchronization areas of $G1$ and $G2$, and the signals of the function $\sin \omega t$ which are enveloping the chaotic carrier. To detect these envelopes, we proceeded as in classical demodulation, clipping our signal in the interval $[-10, 10]$ by the limiting stage as we done on the Four-scroll model. This will provide the signal shown in Figure (13).

Then these signals are filtered by low-pass filters, to mitigate the chaotic carrier and keep the envelopes of $\sin \omega t$. The signals of the function $\sin \omega t$ results of signal error, will be shown in Figure (14) by filtring, thresholding and comparison. We do it as the same as we done in the Four-scroll model.

We will have the signal shown in Figure (14).

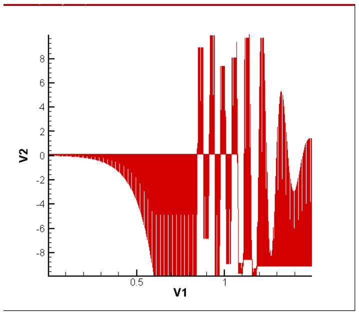

Figure 13: Detecting synchronization areas of $G1$ and $G2$, and limiting them for Lorenz model

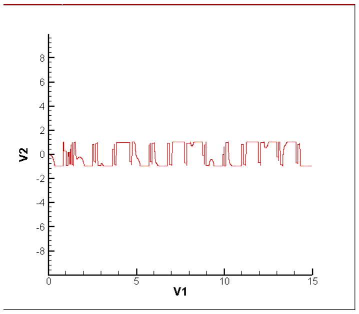

Figure 14: Filtring, thresholding and comparison of error signal for Lorenz model

To reconstruct the original signal, we have performed detecting the error signal rising edges as shown in the figure (15) by the detector rising edges stage. This signal becomes as shown in Figure (15).

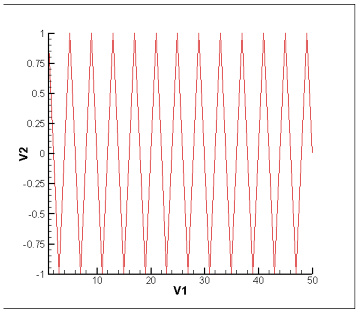

Figure 15: Detection of the rising edge for Lorenz model.

By comparing the signal shown in Figure (15) with the original signal message mj shown in Figure (4), we noted that there was a small difference between them. So, to recover the original message signal, we will have injected it into an T flip-flop. Figures (16) represent the signal reconstructed by the decrypting operation using Lorenz model and the original signal respectively. So they are identical.

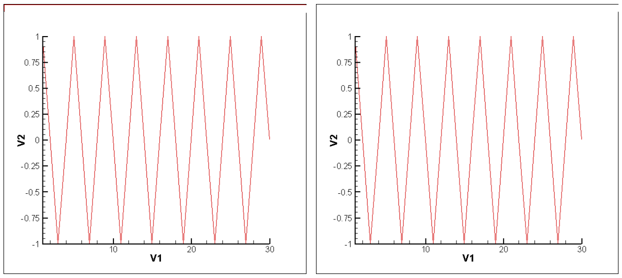

Figure 16: Message after decryption for Lorenz model at the right and the original one at the left.

4. Results discussion

Through this analysis study of the chaotic cryptosystem of the function $\sin \omega t$ using the CSK method by the both systems separately, Lorenz system and Four-scroll system, it was found that we can encrypt the functional message using the two systems. For the encryption we have obtained almost the same results, but for decryption , it was depended on the speed of the synchronization of each system. As well as the speed of the decryption in Lorenz System was slightly faster than the speed of decryption in Four-scroll System. On this basis, we conclude that the encryption and the decryption system depended on the speed of synchronization. However, in our analysis study the process of encryption and decryption using CSK method in both cases was completely successful and we have obtained a very good results.

5. Conclusion

We have located first the problems in crypto systems currently used. An emphasis has been made on the safety limits of this cryptosystems. We noticed through our study, review the cryptosystems the most used currently, and this computational security, since it is based on algebraical calculations. It's one of the reasons that triggered the need to seek alternative, the use of chaos in our work, is one of the proposed solutions.

References

[1] L. M. Pecora, T. L. Carroll, *Synchronization in chaotic systems*, Physical Review Letters, 64, 1990.

[2] H.D.I. Abarbanel, N.F. Rulkov, Mikhail M. Sushchik, *Generalized synchronization of chaos: the auxiliary system approach*, Physical Review E, 53 (1995), 4528-4535

[3] G. Alvarez, L. Hernández, J. Muñoz. Montoya, S. Li, *Security analysis of communication system based on the synchronization of different order chaotic systems*, Physics Letters A, 345 (2005), 245-250.

[4] R. Dumont, *Introduction a la cryptographie et a la sécurité informatique*, Note de cours, Université de Liége, 2006-2007.

[5] X. Bavard, *Numérisation du chaos et applications aux systèmes de communication sécurisés par chaos en longueur d'onde*, Thèse de doctorat, Université de Franche-Comté, 2004.

[6] S. Boccaletti, J. Kurths, G. Osipovd, D.L. Valladares, C.S. Zhou, *The synchronization of chaotic systems*, Physics Reports, 366 (2002), 1-101.

[7] K.M. Cuomo, A.V. Oppenheim, S.H. Isabelle, *Spread spectrum modulation and signal masking using synchronized chaotic systems*, MIT Tech. Rep, 570 (1992).

[8] K.M. Cuomo, A.V. Oppenheim, S.H. Strogatz, *Synchronization of Lorenzbased chaotic circuits with applications to communications*, IEEE Transactions on Circuits and Systems II, 40 (1993), 626-633.

[9] H. Dedieu, M.P. Kennedy, M. Hasler, *Chaos shift keying: modulation and demodulation of a chaotic carrier using self-synchronizing Chua's circuits*, IEEE Transactions on Circuits and Systems I, 40 (1993), 634-642.

[10] Ali Khan Mohammad, *Synchronization of different 3D chaotic systems by generalized active control*, ISSN 1746-7659, England, UK Journal of Information and Computing Science, 7 (2012), 272-283.

[11] E. Lorenz, *Deterministic nonperiodic flow*, J. Atmos. Sci., 20, 130-141.

[12] W. Liu, G. Chen, *Can a three-dimensional smooth autonomous quadratic chaotic system generate a single four-scroll attractor?*, Inte. J. Bifur. Chaos, 14 (2004), 1395-1403.

[13] J. Lü, G. Chen, D.Z. Chen, *A new chaotic system and beyond: The generalized Lorenz-like system*, Internat. J. Bifur. Chaos, 14 (2004), 1507-1537.

[14] G.H. Tigan, *A note on chaos synchronization between two differential three-dimensional systems*, Differential Geometry-Dynamical Systems, 7 (2005), 105-110.

Accepted: 7.07.2017