Chaotic Circuits Applied to Secure Communications

Miguel García, Carlos Sánchez-Azqueta, Santiago Celma

Grupo de Diseño Electrónico (GDE)
Instituto de Investigación en Ingeniería de Aragón (I3A)
Universidad de Zaragoza, Mariano Esquillor s/n, 50018, Zaragoza, Spain.
Tel. +34-976762707, e-mail: *630277@celes.unizar.es*

Abstract

In this paper, we discuss the use of chaotic signals in cryptography. A comparative analysis of three different analogue chaotic communication systems is presented. The paper concludes with a discussion of some possible measures that could improve the security of these systems.

Introduction

In 1990, Pecora and Carrol proved that, surprisingly, two chaotic circuits can synchronize [1]. However, achieving the synchronization of two chaotic systems is not easy and it usually requires that the parameters of both circuits have almost the same exact values.

This opens a wide range of possibilities of using chaotic circuits in order to achieve secure communications, since we can use a chaotic transmitter to mask the information signal and a synchronous chaotic system to recover it (Fig. 1). The parameters of the chaotic transmitter can be seen as a key that is needed to know in order to build a synchronous chaotic receiver. Therefore, the security of the system will come from the high sensitivity of the synchronization versus parameter changes.

In our work, three different communication systems proposed in the literature have been analyzed. All of them were based on a chaotic transmitter synchronized with a chaotic receiver. The chaotic circuits were based on Chua's circuit.

Experimental set up

The first circuit that has been tested in the laboratory was proposed by Kokarev [2]. The transmitter is formed by a Chua's circuit and the receiver is formed by a slighty modified version of the Chua's circuit (Fig. 2). The experimental set up is sketched in Fig. 3. In order to mask the information signal $s(t)$, we add a chaotic signal V_{C1} generated by the Chua's circuit. The masked signal $r(t)$ is then introduced in the receiver causing a synchronous response, assuming that the information signal is small. Finally, the synchronous chaotic signal from the receiver is substracted from the masked signal.

The second circuit that has been tested was proposed by Dmitriev [3]. The main difference from the previous circuit is that, in this case, there is a symmetry between the transmitter and the receiver as shown in Fig 4. This produces that, in this case, the synchronization will be achieved regardless of the amplitude and frequency of the information signal, $s(t)$.

Finally, we implemented a circuit that was proposed by Corron [4]. In this case, the masked signal is affecting both V'_{C1} and V'_{C2} as shown in Fig. 5. By doing this, the synchronization is considerably improved.

Results

In order to test the circuits, a sine wave was introduced as an information signal. To have a good masking of the information, its amplitude was small compared to the chaotic signal and its frequency was close to the Chua's circuit oscillation.

In order to evaluate the quality of each system, we have calculated the Fast Fourier Transform of the masked signal as well as the recovered signal, measuring their signal-to-noise ratio. A good parameter that can be used in order to evaluate the quality of the system, taking into account both the masking capability and the quality of the recovered signal is:

$$\Delta(SNR) = (SNR)_r - (SNR)_m$$

where $(SNR)_r$ is the signal-to-noise ratio of the recovered signal and $(SNR)_m$ is the signal-to-noise ratio of the masked signal.

The results obtained in each case are summarized in Table 1.

Conclusions

During these experiencies, we have shown how chaotic circuits can be used in order to improve the security of a communication system. In our test, the circuit proposed by Corron et al. [4] seems to work better than the other ones.

It needs to be pointed out that, although the analysis made in this paper may suggest that these systems are secure, some papers have shown that, in fact, the security provided by these systems is fairly low. Despite being able to provide some privacy, these systems could be cracked by an observer with enough resources.

One way to improve the security of these systems could be using multiple chaotic sources to mask the information signal better. Another approach consists in using digital chaotic systems that can provide higher levels of security. Our research is currently being carried out on this second approach.

Fig. 1. (a) Eye diagram (upper: original; middle: encoded; lower: decoded). (b) Corresponding spectra (black: original; grey-upper: encoded; grey-lower: decoded.)

Fig. 2. Modified Chua's circuit schematic.

Fig 3. Block diagram of Kokarev's communication system

REFERENCES

[1]. PECORA, L.M., and CARROL, T.L. Synchronization in chaotic systems. *Physical Review Letters.* 1990, 64 (8), 821-824.

[2]. KOKAREV, LJ. et al. Experimental demonstration of secure communications via chaotic synchronization. *International Journal of Bifurcation and Chaos*. 1992, 2 (3), 709-713.

[3]. DMITRIEV, A.S., PANAS, A.I., and STARKOV, S.O. Experiments on speech and music signals transmission using chaos. *International Journal of Bifurcation and Chaos*. 1995, 5 (4), 1249-1254.

[4]. CORRON, N.J., and HAHS, D.W. A new approach to communications using chaotic signals. *IEEE Transactions on Circuits and Systems I.* 1997, 44 (5), 373-382.

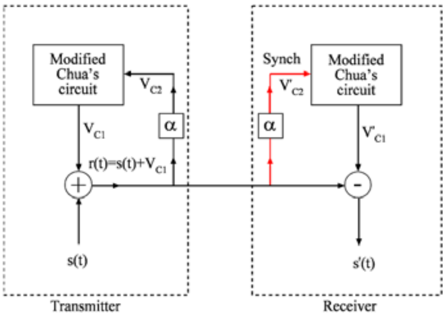

Fig. 4. Block diagram of Dmitriev's communication system

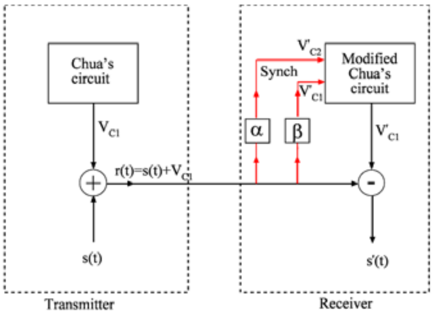

Fig. 5. Block diagram of Corron's communication system.

Table 1. Comparation between the three circuits.

Circuit	$(SNR)_r$ (dB)	$(SNR)_m$ (dB)	$\Delta(SNR)$ (dB)
Kokarev [2]	24	-25	49
Dmitriev [3]	43	-26	69
Corron [4]	65	-15	80