SECURE ANALOG DATA TRANSMISSION BASED ON RÖSSLER CHAOTIC SYSTEM BEHAVIOR

Daniel CURIAC, Ioan FILIP, Florin DRAGAN

" Politehnica" University of Timisoara – Romania, Department of Control Engineering
curiac@aut.utt.ro

Abstract: This paper describes a new methodology for increasing the security of analog data transmission based on a mixture of the original analog signal with one of the state variables of Rössler chaotic system. The method is described emphasizing on the practical implementation aspects.

Keywords: data transmission, encryption, chaotic system, fuzzy synchronizer.

1. INTRODUCTION

Chaos theory is based on simple deterministic systems that demonstrate random behavior. In a chaotic system, even tiny changes in initial conditions eventually lead to major changes in state; this is called "sensitive dependence on initial conditions". This feature of chaotic systems is used in this paper for improving the security of analog transmission.

Uncertainties in information about this kind of systems become magnified by the nonlinearity of the equations in the system, resulting in unpredictability of the system after a very short time. Some chaotic systems, like the Rössler system, are absolutely deterministic and for the same initial conditions, the systems produce the same results. So, even if the results are random, they are repeatable.

The proposed methodology is based on addition of a chaotic signal x to the original signal s at the sender's end and the reverse transformation at the receiver's end (x is the output signal of two synchronized Rössler systems).

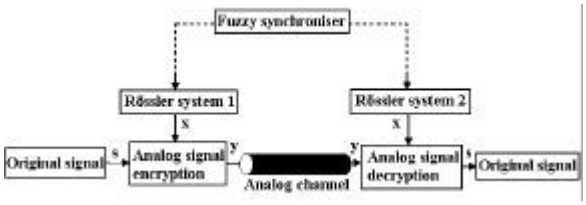

Fig.1. Structure of the secure data transmission using Rössler systems

The proposed strategy, presented in figure 1 is divided in two major steps:

- the initialisation step when the transmission set-up is performed (dotted line in Fig. 1); In this step we have to solve the problem of secure transmitting of the Rössler system parameters (a, b, c) and after that the synchronising problem of the two Rössler chaotic systems through fuzzy control.

This paper was recomended for publication by D. Aiordachioaie

- the secure on-line transmission procedure which includes the encryption/decryption process (continuous line in Fig. 1).

2. THE RÖSSLER CHAOTIC SYSTEM

We can use for spreading and despreading of the transmitted signal two Rössler systems (like in Fig. 1). Rössler system (Rössler, 1976) is described by following equations:

$$(1)\ \begin{cases} x' = -y - z \\ y' = x + a \cdot y \\ z' = x \cdot z - c \cdot z + b \end{cases}$$

where parameters a, b and c for a chaotic behaviour could be 0.2, 0.2 respectively 5.7.

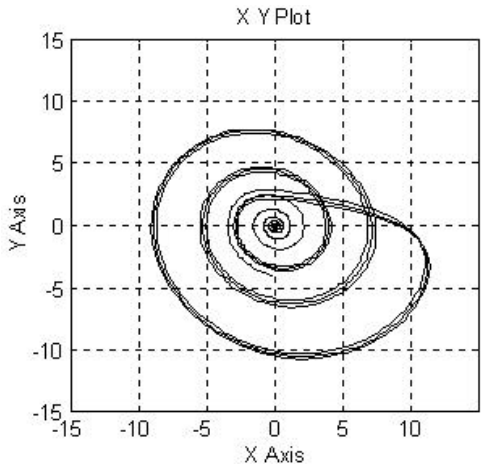

Fig.2. Behavior of the Rössler system with (0,0,0) initial conditions

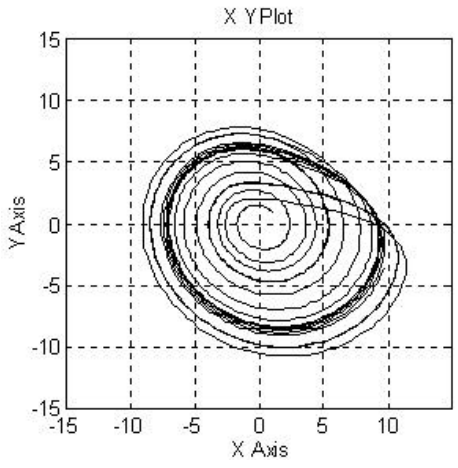

Fig.3. Behavior of the Rössler system with (1,1,1) initial conditions

If we want to control this system we can provide an input u by adding it in second equation. From (1) we obtain:

$$(2)\ \begin{cases} x' = -y - z \\ y' = x + a \cdot y + u \\ z' = x \cdot z - c \cdot z + b \end{cases}$$

For obtaining a chaotical signal we can use either x, y or z state variables.

In case that the Rössler system is started from a set of initial conditions (x_0,y_0,z_0) (for example (0,0,0) in Fig. 2) and (1,1,1) in Fig. 3) one can see that the state space orbits are different (this is one of the main features of the chaotic systems).

3. FUZZY SYNCHRONIZING STRATEGY

In transceivers the spreading and despreading of the transmitted signal is performed by a pseudorandom sequence while the modulation is performed independently from spreading by using a conventional modulation technique. This approach suffers from serious disadvantages like: the signal used for despreading at receiver has to be synchronized perfectly with the signal applied at transmitter for spreading; the synchronization error that always appears under poor propagation conditions results in a high performance degradation. With fuzzy synchronizer presented in this paper we can avoid these difficulties.

So, a fuzzy based synchronizer (simulated using MATLAB with Simulink) has been used. It is depicted as follows.

In Fig. 4 a PI structure for fuzzy controller is described. The two input signals (the fuzzy state variables) considered are error (differences between the pre-determined set speed and the actual speed) and error changing rate (positive if the speed is rising and negative if the speed is falling).

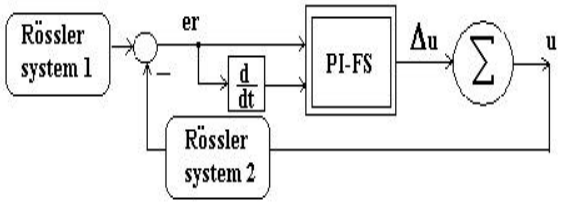

Fig.4. PI fuzzy synchronizer

For defining the membership functions in fuzzification period of certain information we used programs for triangular shape functions and for trapezoidal ascending and descending shape functions, afferent of the linguistics terms used for the fuzzification of error and error changing rate (the inputs for the synchroniser). The linguistic terms chosen for each linguistic variable are: BN, SN, Z, SP, BP (Fig. 5).

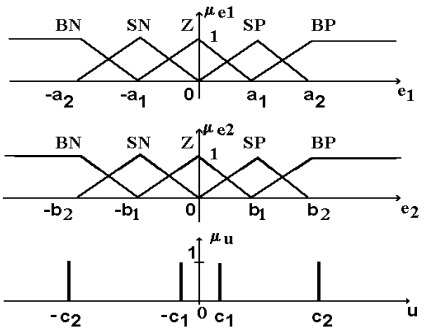

Fig.5. Membership functions

The inference table proposed for regulator is shown in figure 5. The control strategy has as essential element the inference method adopted. The inference connect the measured inputs (fuzzy inputs variable, linguistic shown). The inference operation is implementing with inference table or decision table (Fig. 6) which practically describe the linguistic rules adopted.

u		er				
		BN	SN	Z	SP	BP
di	BN	BN	BN	BN	SN	Z
	SN	BN	BN	SN	Z	SP
	Z	BN	SN	Z	SP	BP
	SP	SN	Z	SP	BP	BP
	BP	Z	SP	BP	BP	BP

Fig.6. Inference table

Based on this table it is possible to deduct softly the linguistics rules. For example (for er - error and di – error changing rate):

IF er is big-negative(BN) and di is big-negative(BN) THEN u is big-negative(BN)

The example shown in figure 5 uses a MAX-MIN inference. As a defuzzification strategy we used the centroid (centers) of area method based on singletons presented in equation 3).

$$(3)\quad u = \frac{\sum_{i=1}^{4} m_i f_i}{\sum_{i=1}^{4} m_i}$$

In Fig. 7 is presented the Simulink scheme for fuzzy controller used for synchronising of Rössler systems noted by *Rössler system 1* and *Rössler system 2.* Those two systems could be replaced by two continual systems with chaotic behaviour, which are used for data transmission/reception with good results.

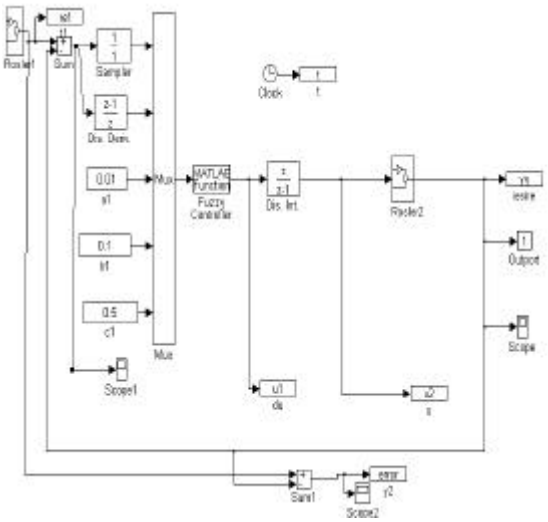

Fig.7. Fuzzy synchronizer simulation in Simulink

If the fuzzy synchronization procedure is applied we obtained the results presented in figure 8a and b. In this figure is shown a quick synchronisation of the second Rössler system with the first, even they started from initials different values ((0,0,0) respectively (1,1,1) for (x,y) couple)

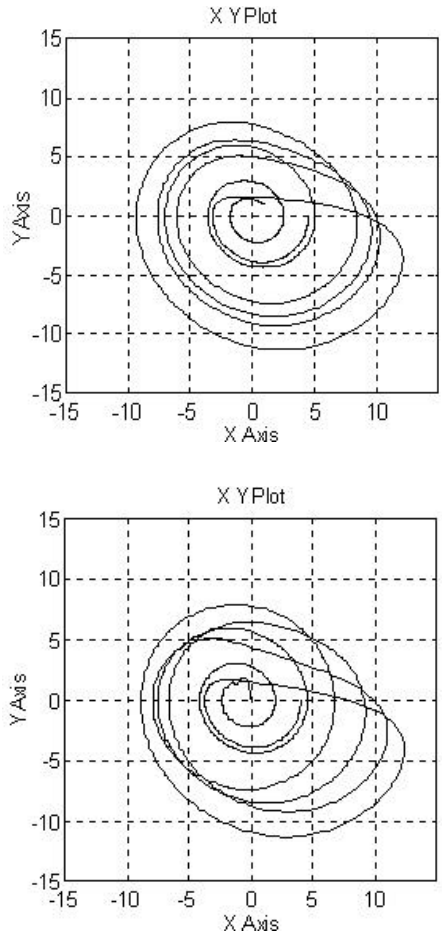

Fig.8. The behaviour of two synchronised Rössler systems

4. ANALOG SIGNAL ENCRYPTION/DECRYPTION

Encryption is the process of transforming a signal or message into a form that is meaningless to everyone except the intended receiver.

Considering: (-n, +n) the range of the original signal s; (-m, +m) the range of the x state variable of Rössler system, for example (-12V, +12V); (-max, +max) the maximum range of the transmitted signal y, we can use as an encryption formula the following equation:

$$(4)\quad y = \frac{\max}{2}\left(\frac{s}{n} + \frac{x}{m}\right)$$

We notice that this relation is invertible, so that we can obtain an equation for the decryption process, which is:

$$(5)\quad s = n \cdot \left(\frac{2y}{\max} - \frac{x}{m}\right)$$

5. CONCLUSIONS

The strategy presented in this paper is an efficient one, mainly for short analog transmissions, in which there is no need for resynchronization of the two chaotic systems.

The fuzzy controller used for synchronization of two Rössler systems gave very good results. Synchronization is made in a very short period of time and in this way we could ensure an adequate security of data transmission with no affect from time factor. We believe that using chaotic systems in data transmissions means a simplification of the secure transmission process due to a quickly and softly synchronization with presented fuzzy synchronizer.

Basically, the proposed methodology could be applied also for digital signal transmission with some changes upon the chaotic system. We have to use a discrete chaotic signal, for example one of the state variables of Henon chaotic system (Henon, 1976)., which will be compared with a range and a centerpoint. If the iterated results are in the top of the range, a digital 1 is assigned and if they are in the lower half of the range, a digital 0 is assigned.

6. REFERENCES

Blank M., (1997) "Discreteness and Continuity in Problems of Chaotic Dynamics", Oxford University Press;

Crilly A. J., Earnshaw R. A., Jones H. (1993) "Applications of Fractals and Chaos", Springer-Verlang;

Curiac D.I., Filip I., Prostean O., Dragan F., (1999) "Fuzzy Based Synchronizer for Chaotic Systems", INES'99 the 3rd IEEE International Conference on Intelligent Engineering Systems, November 1-3, 1999, Stara Lesna, Slovacia, Proceedings

Curiac D.I., (2001) "Algoritmi de criptare pentru securizarea datelor", Editura Orizonturi Universitare Timisoara..Colectia Calculatoare Informatica 12.

Filip I., Prostean O., Curiac D.I., "Implementing Fuzzy Controllers Using SIMNON Package", Buletinul Stiintific UPT, Seria Automatica si Calculatoare, 1996, **Tom41(55)**.

Henon M., (1976) "A Two Dimensional Mapping With a Strange Attractor", Comm.Math.Phys. 50, p. 69-77.

Hilborn R. C., (1994) "Chaos and Nonlinear Dynamics", Oxford University Press;

Kapitaniak T., (1998) "Chaos for engineers. Theory, Applications and Control", Springer-Verlang;

Kuhn T., Wernstedt J. (1995) "Fuzzy Adaptive Controlled PID Controllers", Proceedings of The Third EUFIT'95 European Congress, Aachen, **vol 2**, p 889-896.

Rössler O. E., (1976) "An equation for continuous chaos". Phys. Lett. 35A:397-398.

Zimmermann H. J., (1985) "Fuzzy Set Theory - and Its Applications", Kluwer-Nijhoff Publishing.