# Chaos Encryption Method Based on Large Signal Modulation in Additive Nonlinear Discrete-Time Systems

VICTOR GRIGORAS[1] , CARMEN GRIGORAS [2]
[1] Faculty of Electronics and Telecommunications,
'Gh. Asachi' Technical University Iasi
1 Blvd. Carol I, 700506 Iasi
ROMANIA
[2] Faculty of Medical Bioengineering,
'Gr. T. Popa' Univerity of Medicine, Iasi
16 Universitatii, 700403 Iasi
ROMANIA

*Abstract:* - The present contribution deals with digital data encryption by means of discrete-time chaos synchronization. By this combination of analog nonlinear dynamics with digital signal processing, a larger number of encryption keys and higher computational complexity to break the code is expected compared to standard digital encryption techniques. The chaos synchronization system is based on an emitter structure similar to that of a recursive digital filter with single, piece-wise linear, periodic type nonlinearity. The use of additive nonlinearities simplifies the design of the system, allowing easy calculation of the emitter Lyapounov exponents and straightforward, inverse system design of the synchronizing receiver. Moreover, the problem of noise sensitivity, present in analog chaos synchronization setups, is totally removed by using channel quantization. The large modulating signal approach, combined with large maximum Lyapounov exponent of the emitter and use of an output bit shuffling circuit, helps cover some of the previously noticed drawbacks of the chaotic approach to digital signal encryption.

*Key-Words:* - chaos encryption, chaos synchronization, additive nonlinear discrete-time systems

## 1 Introduction

Chaos synchronization, pioneered by Pecorra and Carroll, spurred the search for the application of chaotic systems in the communication field [1, 2]. Synchronous chaos modulation proved to be too sensitive to both channel noise and system parameters to offer a viable alternative to digital spread spectrum modulation. Digital signal encryption on the other hand seems a more promising application of chaos synchronization [9 - 11]. The main advantages of the chaotic encryption approach include: high flexibility in the encryption system design, good privacy due to both non-standard approach and vast number of variants of chaotic systems, large, complex and numerous possible encryption keys and simpler design methods. The analogue alternative for chaotic encryption was ruled out because of the small dimension of analog chaotic systems and little freedom in choosing system parameters, together with high design complexity, large computational requests and privacy drawbacks. The discrete time counterpart proved easier to design up to large system dimensions, gives high freedom in choosing system parameters and ensure also better secrecy.

The present paper proposes a discrete-time chaos synchronization system, aimed at encryption goal, based on additive nonlinear discrete-time systems (ANDS). To achieve chaos synchronization, in the chosen environment, the inverse system approach is applied. This leads to floating point encryption and decryption algorithms that have higher resistance to known attacks. The ANDS approach is highly efficient due to the intrinsic ease of design, the possibility of using large order chaotic systems, with good cryptographic results, ease of computing Lyapounov exponents of the emitter system and precisely controllable quantization results.

The use of large input signal, treated for the first time here, gives the extra advantage of naturally providing some extra output bits to be used in the output shuffling process. The ease of designing the

chaotic encryption system to have large Lyapounov exponents also helps cover some of the previously noticed drawbacks of the chaotic approach to digital signal encryption.

The next paragraph presents the main result of the paper, regarding the large modulating signal approach to chaos synchronization method used for encryption purposes. The following one exposes several structural aspects regarding the proposed encryption method and argues its better secrecy performance. The concluding part highlights the advantages of the proposed method and suggests some further directions to speed-up its implementation.

## 2 ANDS Chaos Synchronization

The proposed encryption method starts from a chaos synchronization setup, composed of a discrete-time non-linear emitter system, exhibiting chaotic dynamics, and a globally asymptotically stable receiver system, designed to synchronize with the emitter. When synchronization is achieved, in order to make use of this connection, the aspects regarding chaos modulation must be addressed. Thus we take the inverse system approach and apply the information-bearing, or modulating, signal, **m[***k***]**, to the emitter input, transmit the chaotic output, **y[***k***]**, and recover an approximation of the modulating signal, $\tilde{\mathrm{m}}[k]$, at the receiver output, as suggested in Fig. 1.

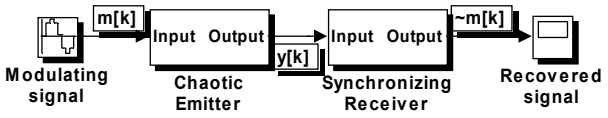


Fig. 1. The general chaos encryption setup

To achieve the desired encryption performance, we concentrate on the particular case of ANDS of the Lure type. Such a system is built in a feedback loop, connecting a discrete-time linear filter around the algebraic nonlinear function. Additivity is achieved by using a particular algebraic function, namely the symbolic residue function, **r(***x***)**, suggested by the two's complement overflow characteristic in digital filters, [3], depicted in Fig. 2 and given by the equation (1):

$$\mathrm{r}(x) = x - \mathrm{round}(x) \tag{1}$$

In the following we denote the symbolic quotient function by **k(***x***)**, as given by equation (2):

$$\mathrm{k}(x) = \mathrm{round}(x) \tag{2}$$

We can conclude that any real number, $x$, can be decomposed as a sum of the two symbolic functions, as given in equation (3):

$$x = \mathrm{k}(x) + \mathrm{r}(x) \tag{3}$$

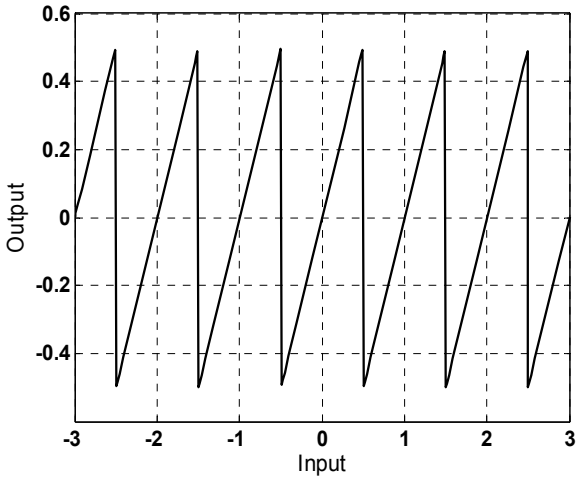


Fig. 2**.** The residue algebraic nonlinear function used in the chaotic emitter.

The discrete-time linear filter, included in the feedback loop, is of the FIR type, described by the transfer function:

$$\mathrm{H}(z) = \sum_{n=1}^{N} \mathrm{h}[n] \cdot z^{-n} \tag{4}$$

The coefficients, $\mathrm{h}[n], n = 1, .., N$, in equation (4), represent the impulse response samples of the FIR filter. This leads to the nonlinear difference equation describing the behavior of the emitter:

$$\mathrm{y}[k] = \mathrm{r}\left( \mathrm{m}[k] + \sum_{n=1}^{N} \mathrm{h}[n] \cdot \mathrm{y}[k-n] \right) \tag{5}$$

That gives in turn the block diagram of the emitter implementation depicted in Fig. 3:

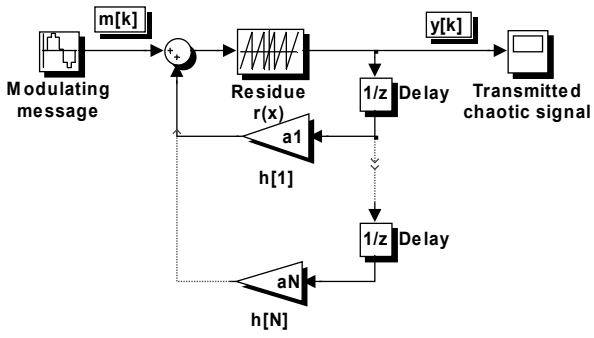


Fig. 3. Generic topology of the additive chaotic emitter

In [6] it is demonstrated that, if the linear prototype of the ANDS, described by the transfer function in equation (6), is unstable, than, the nonlinear system has a chaotic dynamic behavior.

$$\mathrm{H}(z)=\frac{1}{1+\sum_{n=1}^{N}\mathrm{h}[n]\cdot z^{-n}} \tag{6}$$

By using the inverse system approach, and taking into account the additivity property of the emitter system, the receiver system is a finite memory one, described by the difference equation (7):

$$\tilde{\mathrm{m}}[k]=\mathrm{r}\left(\mathrm{y}[k]-\sum_{n=1}^{N}\mathrm{h}[n]\cdot\mathrm{y}[k-n]\right) \tag{7}$$

The corresponding synchronizing receiver, which implements equation (7), has the feedforward topology presented in Fig. 4.

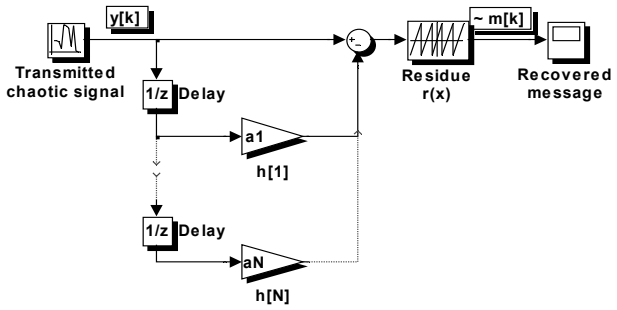


Fig. 4. Block diagram of the synchronizing receiver

As demonstrated in ref. [7], if the emitter and receiver share the same set of coefficients, no matter the differences in initial conditions, the receiver synchronizes to the emitter in finite time. The synchronization transient lasts for a time interval equal to the order of the two systems, *N*, after that the modulating and recovered signals will be identical, as suggested in the example simulation in Fig. 5.

In [4,9] it is demonstrated that the described receiver synchronizes with the chaotic emitter only if the input (modulating) signal is bounded to the maximum output value of the symbolic residue function, $\mathrm{r}(x)$. Taking normalized values, as in equation (1) and Fig. 2, the maximum admissible value of the input is $|y_{\mathrm{Max}}|<0.5$. For larger input values, the inverse system deduced using additivity is no longer valid, and the general form of the inverse must be used, as in equation (8):

$$\tilde{\mathrm{m}}[k]=\mathrm{r}^{-1}\left(\mathrm{y}[k]\right)-\sum_{n=1}^{N}\mathrm{h}[n]\cdot\mathrm{y}[k-n] \tag{8}$$

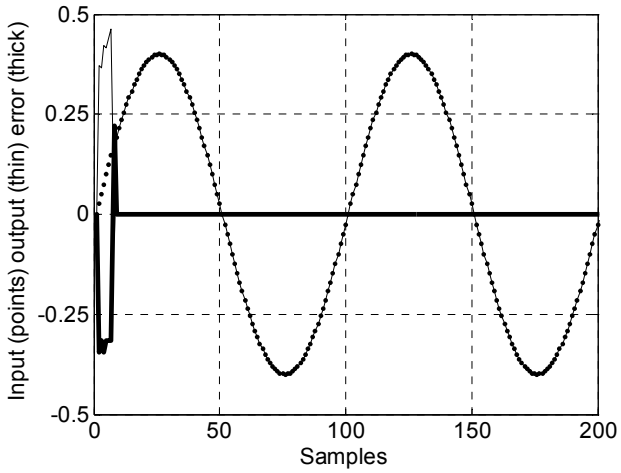


Fig. 5. Synchronization transient: modulating signal (dot) recovered message (thin) and error (thick)

Obviously, the symbolic residue algebraic function, **r(***x***)**, by itself is not invertible. Thus, extra information is needed to calculate the argument *x* from the value **r(***x***).** This additional information is given by the symbolic quotient function, **k(***x***)**; the pair **(r(***x***), k(***x***))** is invertible as suggested by equation (3).

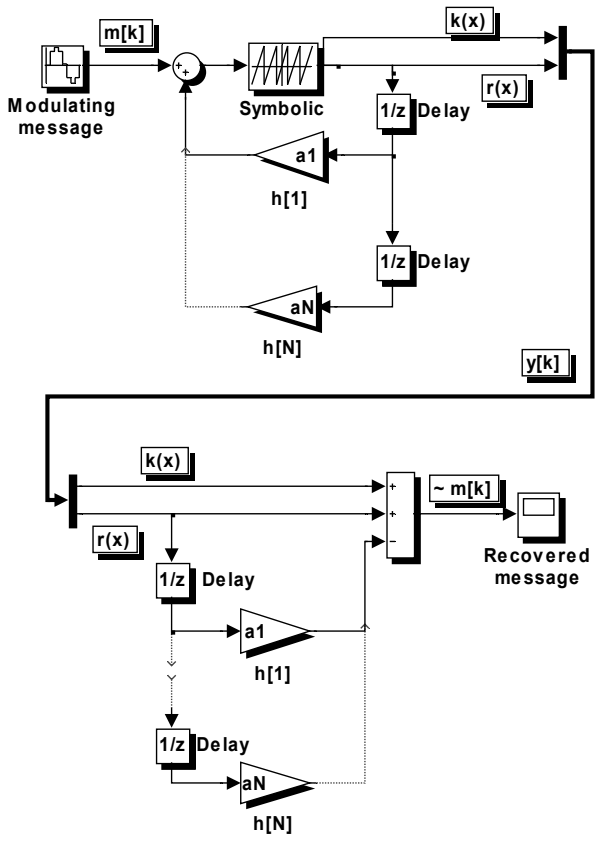


Fig. 6. The block diagram of the complete synchronization setup, valid for large modulating signals

Multiplexing the integer (quantized) values of **k(*x*),** with the chaotic transmitted signal **y[*k*],** leads us to the complete synchronization setup, valid for modulating signals larger than the additive limit, $|y_{\mathrm{Max}}| > 0.5$, as presented in Fig. 6.

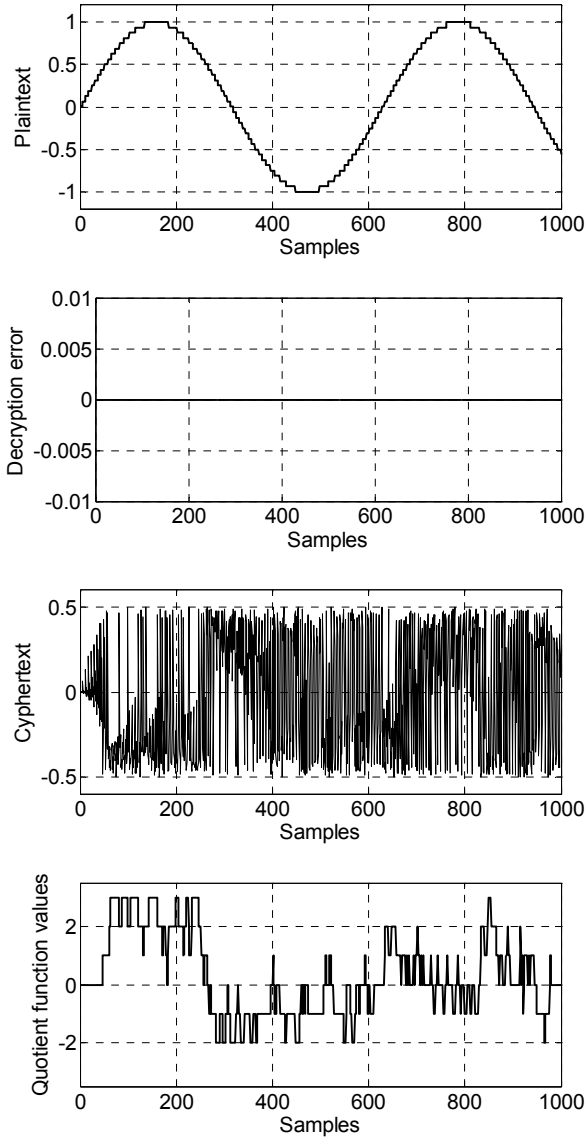


Fig. 7. Simulation results on large signal chaos synchronization

A simulation example is given to highlight the correct operation of the proposed large signal synchronization method. Both emitter and receiver systems are of small order, $N$ = 7, with initial condition on all delay elements set to zero. The coefficients vector for both emitter and receiver is chosen $\underline{\mathbf{h}}$ = [1, 1.1, 1, 1, 1, 1, 1.2].

As can be seen in the top graph of Fig. 7, both emitted and recovered plaintext signals have double of the amplitude (+/- 0.5) allowed by the additivity condition. The recovered plaintext is identical to the emitted one, thus the decryption error in the second graph is null. The ciphertext, presented in the third graph of Fig. 7, does not reveal the plaintext characteristics. The last graph shows the time evolution of the symbolic quotient function, represented on three bits.

# 3 Encryption Method

In the following, the previous results are used for encryption purposes. We model the input alphabet as a finite set of integer values, obtainable by quantizing the input signal. This signal is large, but bounded at the normalized value $M$. Quantization is performed with a specified, normalized quantization step, $q$. This leads to an alphabet comprising $C = 2M/q$ characters, in binary representation, $B_M \geq \log_2(C)$ bits. The encrypted text is also quantized, in this case of the emitter output, the number of channel bits being denoted by $B_C$. This way, the channel noise, that affects analog chaos modulation, is no longer to be taken into account as we use from now on only digital channels. Instead, the quantization noise, that has known limited amplitude, has to be taken into account.

In ref. [8] it is demonstrated that, if the channel noise is given only by the quantization process, in order to achieve perfect synchronization, the number of supplementary bits, i.e. the difference between the number of bits used for the message, $B_M$, and the (larger) one for the channel quantization, $B_C$, depends on the sum of absolute values of the filter coefficients:

$$\Delta B = B_C - B_M \geq \log_2\left(2 \cdot \sum_{n=1}^{N} |\mathrm{h}[n]|\right) \qquad (9)$$

The advantage of additive systems lies in the analytic relation between their Lyapounov exponents and the eigenvalues of the state transition matrix of the linear prototype, or the poles of the transfer function of the linear system. Denoting by $L_n$ the Lyapounov exponents of the nonlinear additive system and by $\lambda_n$ the poles of the linear prototype, the relation between them is given in Eq. (10):

$$L_n = \log_2(|\lambda_n|) \quad n = 1,\ldots,N \qquad (10)$$

The larger the largest Lyapounov exponent of the ANDS, the larger the sensitivity of the chaotic emitter and the better the privacy ensured by the chaotic encryption system. But large Lyapounov exponents mean large poles of the linear prototype so larger filter coefficients. Thus better secrecy is

achieved at the cost of larger data volume to be transmitted.

Under the new conditions, with large input signal, the data transmitted has to further increase with the amount necessary to code the symbolic quotient function, **k(*x*)**:

$$B_k \geq 1 + \log_2\left( M + \sum_{n=1}^{N} \left| \mathrm{h}[n] \right| \right) \qquad (11)$$

The extra $B_k$ bits can be appended to the $B_C$ channel bits, or inserted among them. For better secrecy, we propose to use them as command bits in a combinational, memory-less, bit shuffling circuit. This is a look-up table that shuffles channel bits, inserts the extra $B_k$ bits among the previous ones and, moreover, it does so in different ways, depending on the value of the symbolic quotient function, coded on $B_k$ bits. De-shuffling can be done at the receiver end only with full knowledge of the look-up table.

The resulting block diagram, for the proposed encryption / decryption system is presented in Fig. 8.

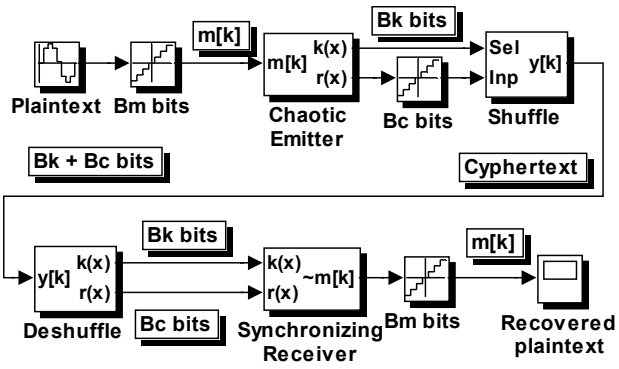


Fig. 8. Block diagram of the large signal synchronization setup, achieving encryption/decryption

In order to further increase transmission secrecy, the system parameters that form the symmetric encryption key can be periodically changed. Taking into account that the initial condition of the emitter can be appended to the key, the first N samples of the message are natural candidates for a 'safer place' where the index of the key table can be transmitted.

Taking into account all aspects discussed till now, we deduce that the chaos encryption method we propose is a recursive one with private key, if necessary with periodic key change. The encryption key must contain:

- The system order $N$;
- The number of message bits $B_M$;
- The modulation signal amplitude increase, $B_k$;
- The shuffling look-up table(s);
- The system coefficients $\mathbf{h}[n]$, $n = 1, .. , N$;

and, if necessary for key change signaling:

- The initial conditions $\mathbf{x_0}[n]$, $n = 1, .. , N$.

Most values, in the encryption key, are specific for any chaotic ANDS encrypted communication. The large signal method proposed here adds the shuffling look-up table(s), which increases the transmission security.

# 4 Conclusions

A chaos encryption method was proposed, based on large input (modulating) signal chaos synchronization in additive, discrete-time, Lure systems. The recursive structure of the chaotic encryption system gives a further security advantage, due to a dynamic relation between the ciphertext and plaintext. Discrete time additive systems ensure ease of design, analytical relations between linear system poles and non-linear system Lyapounov exponents and high order encryption/decryption systems. Supplementary, the proposed large signal approach enables the introduction of an extra shuffling circuit, further improving encryption performance. The way to improve encryption secrecy by the correct choice of the largest Lyapounov exponent and the complexity of the encryption key are briefly dealt with. The huge number of possible encryption keys, high computational complexity necessary to break a chaotic code and the good resistance to known types of attacks can be further enhanced by periodic key modification. The proposed system is easily cascadable with existing encryption / compression / error-correction systems to increase the overall communication performance.

The only foreseeable drawback of the proposed encryption method is its higher computational complexity, compared to short - key, fixed - point actual methods, due to the need of floating point calculation inside the emitter and receiver. Fortunately, the systemic approach for the proposed design makes hardware acceleration straightforward, in order to improve speed.

*References:*

[1] L. M. Pecorra, T. L. Carroll: 'Synchronization in Chaotic Systems', *Physical Review Letters*, Vol. 64, No. 8, February 1990, pp. 821-924.

[2] L. M. Pecorra, T. L. Carroll: 'Synchronizing Chaotic Circuits', *IEEE Transactions on Circuits and Systems*, Vol. CAS 38, No. 4, April 1991, pp. 453-456.

[3] L.O. Chua, T. Lin: 'Chaos in Digital Filters', *IEEE Transactions on Circuits and Systems*, Vol. CAS-35, No. 6, June 1988, pp. 648-658.

[4] K. Kelber, T. Kilias: 'Analysis of an Encoder-Decoder-System Based on Digital Filter Structures with Two's Complement Overflow Characteristic', *Proceedings of the International Symposium on Circuits and Systems, ISCAS'96*, 12-15 May 1996, Atlanta GA, pp. III 166-169.

[5] V. Grigoras, L. Goras: 'Additive Nonhomogeneous Discrete Systems', *Proceedings of Nonlinear Dynamics in Electronic Circuits, NDES'94*, Krakow 29-30 July 1994, pp. 185-189.

[6] V. Grigoras, L. Goras: 'A Z-Transform Approach to Additive Nonlinear Discrete Systems Analysis', *Proceedings of European Conference on Circuit Theory and Design, ECCTD'95*, Istanbul 29-31 August 1995, pp. 415-418.

[7] A. Leuciuc, V. Grigoras, 'Finite Time Chaos Synchronization in Bijective Triangular Form Systems', *International Journal of Chaos Theory and Applications*, No. 1, Vol. 2, May 1997, pp. 3-16.

[8] V . Grigoras: 'Noise Sensitivity Measures For Chaos Synchronization In Discrete-Time Additive Non-Linear Systems', *Proceedings ECIT 2000, 1st European Conference on Intelligent Systems and Technologies*, Iasi, Romania, September 17-18, 2000.

[9] V. Grigoras, 'Digital Encryption Based on Exact Chaos Synchronization', *International Journal on Chaos Theory and Applications*, No. 4, Vol. 4, December 1999. pp. 15-20.

[10] K. Kelber, W. Schwartz, 'General Design Rules for Chaos-Based Encryption Systems' Proceedings NOLTA 2005, International Symposium on Nonlinear Theory and its Applications, Bruges, Belgium, October 18-21, 2005.

[11] L. Kocarev, 'Chaos-Based Cryptography: A Brief Overview', IEEE Circuits and Systems Magazine, Vol. 1, No. 3, 2001.