Memoirs of the Scientific Sections of the Romanian Academy
Tome XL, 2017

COMPUTER SCIENCE

DISCRETE-TIME BIOMEDICAL SIGNAL ENCRYPTION

VICTOR GRIGORAŞ[1] **and CARMEN GRIGORAŞ**[2,3]

[1] *"Gheorghe Asachi" Technical University of Iaşi, 700506, Romania*
[2] *"Gr.T. Popa" University of Medicine and Pharmacy of Iaşi, 700115, Romania*
[3] *Institute of Computer Science, Romanian Academy, Iaşi, 700481, Romania*
Corresponding author: crmn_g@yahoo.com

Chaotic modulation is a strong method of improving communication security. Analog and discrete chaotic systems are presented in actual literature. Due to the expansion of digital communication, discrete-time systems become more efficient and closer to actual technology. The present contribution offers an in-depth analysis of the effects chaos encryption produce on 1D and 2D biomedical signals. The performed simulations show that modulating signals are precisely recovered by the synchronizing receiver if discrete systems are digitally implemented and the coefficients precisely correspond. Channel noise is also applied and its effects on biomedical signal demodulation are highlighted.

Keywords: chaotic encryption, modulation, non-linear control, secure communications, discrete-time system.

INTRODUCTION

Transmitting biomedical data in general access networks asks for good encryption in order to avoid unauthorized access. Chaos modulation can be added to the existing encryption methods to improve data protection. Chaos synchronization is implemented in different methods, such as emitter splitting proposed by Pecorra and Carrol [1], inverse system approach for secure transmission [2], or using a state observer for a nonlinear system performing chaotically as a synchronizing receiver and then modulating the information signal onto the chaotic carrier [3]. As a demodulation method, synchronization leads to the private key encryption method, thus the receiver must have access to the exact values of the emitter parameters, to achieve decryption.

For chaos modulation, analog or discrete approaches may be used. The analogue approach ensures high complexity for the emitter system and the generated signal [4–6], along with the difficulty of precision parameter settling [7]. Digital implementation is more flexible and reliable, less costly and, most importantly, it has the capability of maintaining precise values of systemic parameters [8–10].

A correct demodulation also depends on the information signal used. This is why a targeted analysis for different classes of modulating signals is of special practical usefulness. Our approach is oriented towards the biomedical signal class, taking into account both 1D and 2D medical data. Simulations are performed in order to highlight the best demodulation, if the receiver is digitally implemented and the emitter parameters precisely known.

The next section of this contribution presents the discrete-time chaotic emitter and the corresponding synchronizing receiver, including their difference equations and resulting implementation block diagrams. Section 3 is the most detailed one, being concentrated on biomedical signals transmission, including possible, undesired, channel noise. Both 1D and 2D signals are analyzed and biomedical images' sensitivity to noise is highlighted. The concluding remarks constitute the last section of this paper

THE USED NON-LINEAR SYSTEMS

The proposed communication system is based on the modulation/demodulation principle suggested in Figure 1. The modulating emitter is a discrete-time nonlinear system, designed to have a complex dynamical behavior, of chaotic type, in order to cover the information contained in the modulating signal, *m*[*k*]. For a correct demodulation, the receiver is an inverse system synchronizing stable nonlinear system, as introduced in [11], recovering the information signal with the best approximation, ~*m*[*k*]. The transmitted signal, *y*[*k*], contains, in a hidden way, the useful information.

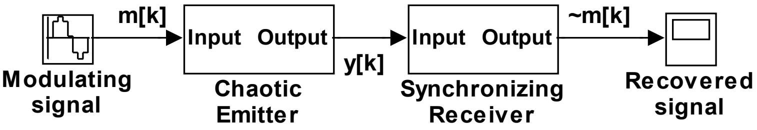

Fig. 1. Block diagram of the communication system.

The proposed nonlinear emitter is described by the discrete *N*-th order equation, (1), with *m*[*k*] input and *y*[*k*] output, leading to the diagram plotted in Figure 3:

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

The synchronizing receiver recovers the modulating signal based on equation (2), only on condition that the parameters *h*[*n*] are precisely the same as the corresponding ones in the emitter equation:

$$\tilde{m}[k] = r\left(\tilde{y}[k] + \sum_{n=1}^{N} h[n] \cdot \tilde{y}[k-n] \right) \tag{2}$$

A correct recovery of the desired modulating signal can be affected by channel perturbations, affecting the transmitted signal:

$$y[k] \neq \tilde{y}[k] \tag{3}$$

In both equations, (1) and (2), the non-linear algebraic function $r(x)$ is suggested by the complement of 2 overflow, as denoted in equation (4) and illustrated in Figure 2:

$$r(x) = x - round(x) \tag{4}$$

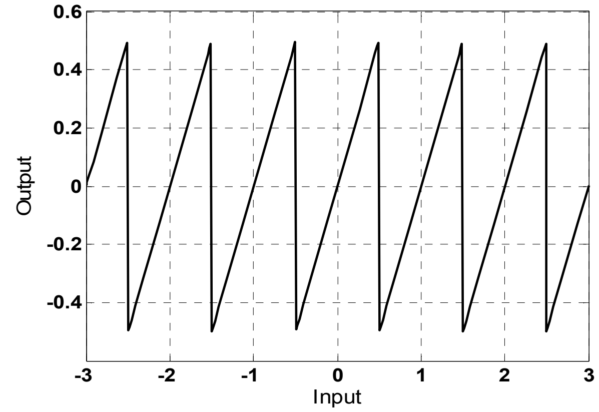

Fig. 2. Input – output graphical representation of the algebraic function r (.).

Implementation of the receiver described by (2) is given by the block diagram in Figure 4, highlighting the inverse system approach in its design.

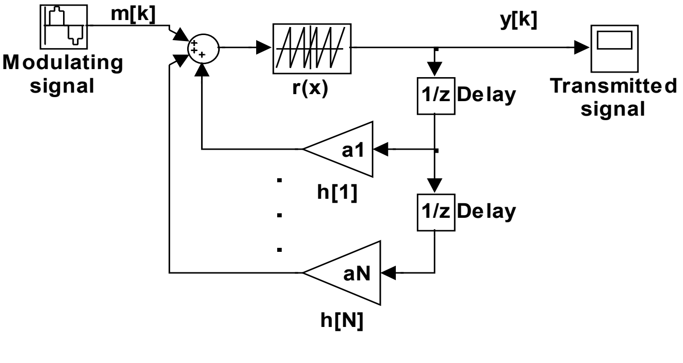

Fig. 3. Block diagram of the discrete-time emitter.

The demodulated signal, $\sim m[k]$, can be strongly affected by parameter error between receiver and emitter, ensuring extra security over classical algebraic encryption. Over this desired aspect, undesired channel noise may also affect the recovered information signal.

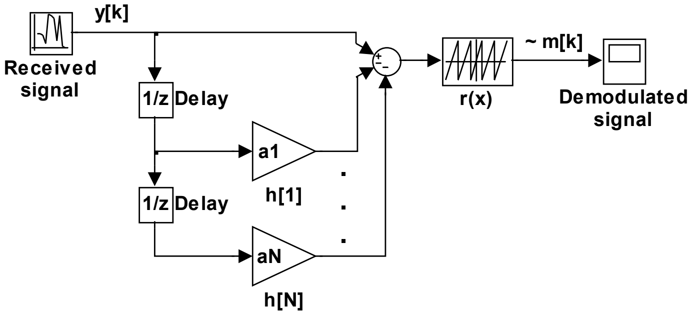

Fig. 4. Block diagram of the synchronizing discrete receiver.

This type of noise perturbation is depending on the modulating and demodulating systems, but also on the characteristics of the information signal. This is why simulation analysis for different biomedical signals is of practical usefulness for medical transmission systems' design.

BIOMEDICAL SIGNAL TRANSMISSION RESULTS

Testing of the discrete-time chaotic communication system was performed with 1D and 2D biomedical signals. ECG and EEG signals were used as 1D testing signals while, for 2D cases, X ray and rethinian images were chosen. Both the time and frequency domains were considered as relevant representations of the analyzed signals. The simulations and graphical representations used for signal analysis are normalized.

The graph plotted in Figure 5 is a typical example of ECG modulating signal, having the frequency spectrum depicted in Figure 6.

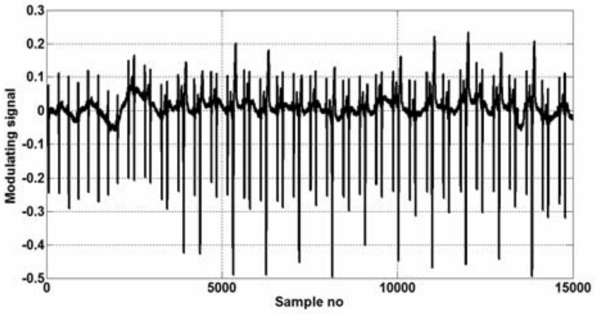

Fig. 5. Time domain representation of ECG modulating signal.

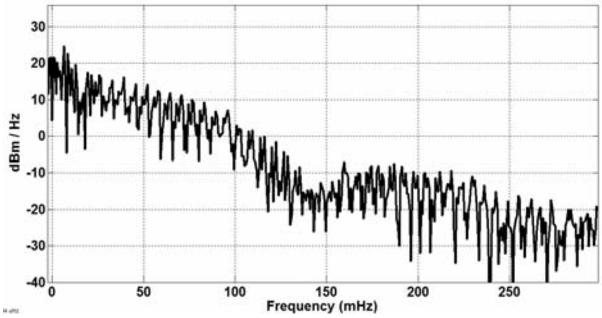

Fig. 6. Frequency spectrum of ECG modulating signal.

The modulated signal obtained from the chaotic emitter, $y[k]$, is transmitted towards the receiver. The time evolution of the received signal, zoom depicted in Figure 7, shows no similarity with the modulating signal from Figure 5. The same observation can be made regarding the frequency spectrum of the transmitted signal, represented in the same figure.

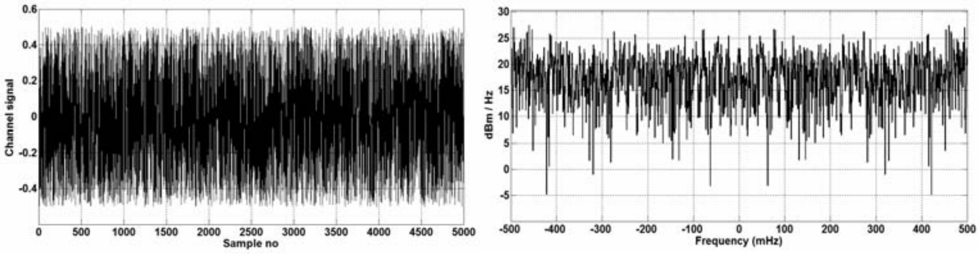

Fig. 7. The transmitted signal from the chaotic emitter (left) and its spectrum (right).

Thus, neither time nor frequency unauthorized receptions can be efficiently attacked. The authorized receiver recovers the information signal using the exact values of the coefficients in the structure of the emitter. The exact correspondence between the emitter and receiver coefficients ensures precise synchronization and modulating signal recovery. If no perturbations occur on the communication channel or the structure of the discrete chaotic emitter and synchronizing receiver enables the use of the error correction communication channel, demodulation is not affected by errors, as shown in the example given in Figure 8, where both the demodulated signal and the synchronization error are present.

For 1D EEG signals, similar results were obtained, as shown in Figures 9 to 11.

In cases of noise-affected transmission, the demodulated 1D signal is marked by synchronization errors, dependent on the noise level. The results depicted in Figure 12, show error levels in the case of noise variances of 10^{-3} and 10^{-2}, respectively. These examples highlight the increase of the demodulation error upon channel noise increase.

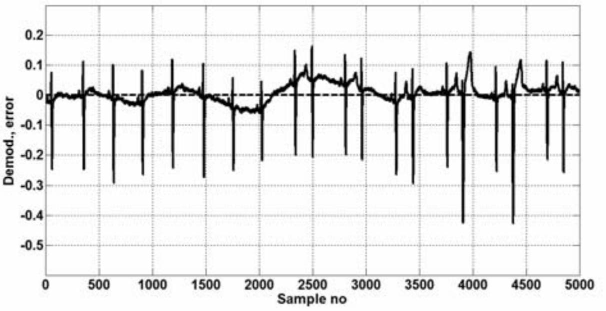

Fig. 8. Demodulated ECG and the synchronization error for the zero noise channel.

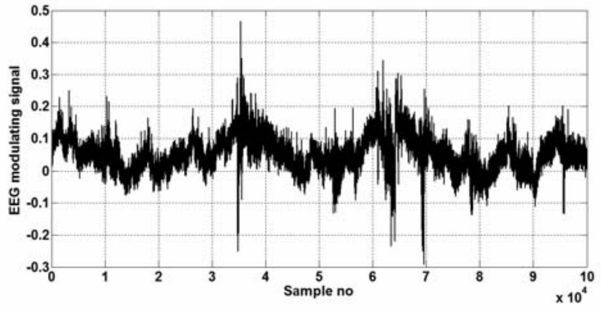

Fig. 9. EEG modulating signal.

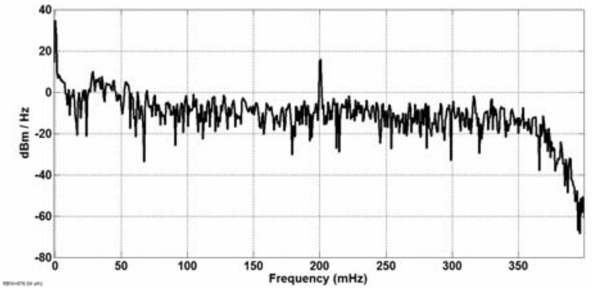

Fig. 10. Frequency spectrum of the EEG modulating signal.

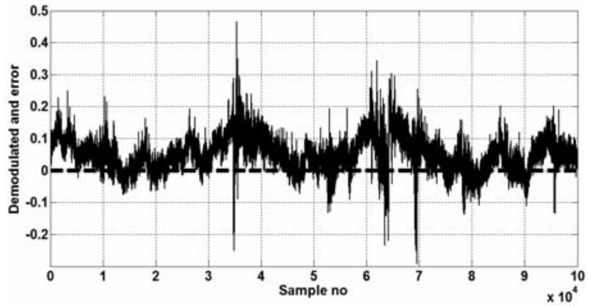

Fig. 11. Demodulated EEG and the synchronization error for the zero noise channel.

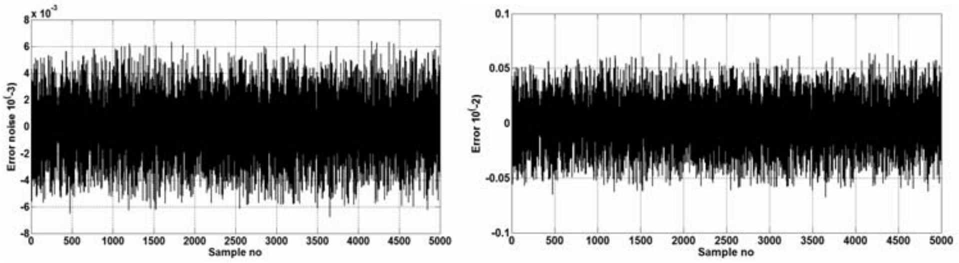

Fig. 12. The synchronization error for cases of channel noise of 10^{-3} and 10^{-2} variances.

The obtained results highlight the importance of precise channel transmission, noise reduction and digital error correction, for assuring a correct transmission and use of 1D biomedical signals.

In order to achieve transmission of 2D biomedical signals, serialization of the pixel matrix of the pictures ensure conversion of the bi-dimensional signals into one-dimensional ones. In this way, the same modulation/demodulation nonlinear discrete systems can be used, with zero transmission error in the case of a precise digital coefficient correspondence and absence of channel noise. Line by line and column by column serialization of the picture matrix gave identical results.

We chose to show noise effect on biomedical images using grayscale X ray, 352 × 470 pixels image and rethinian 130 × 150 pixels color image, and a color map of 256 RGB levels. Taking into account the importance of biomedical images reading, in both cases we had to use smaller noise levels, as depicted in Figure 13, where the channel noise has a variance of $0.3*10^{-4}$. Its corresponding frequency spectrum is shown in Figure 14.

As easily noticeable, although the noise level is lower, the demodulated biomedical 2D images are error-affected. However, such small errors, shown in Figures 15 and 16, do not make the recovered images unusable for medical applications.

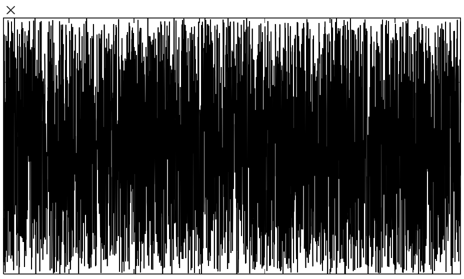

Fig. 13. Channel noise for 2D images transmission.

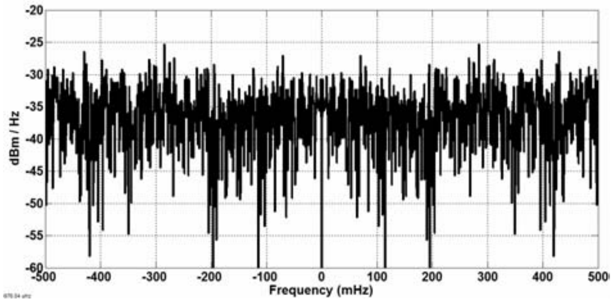

Fig. 14. Power spectrum of the applied channel noise.

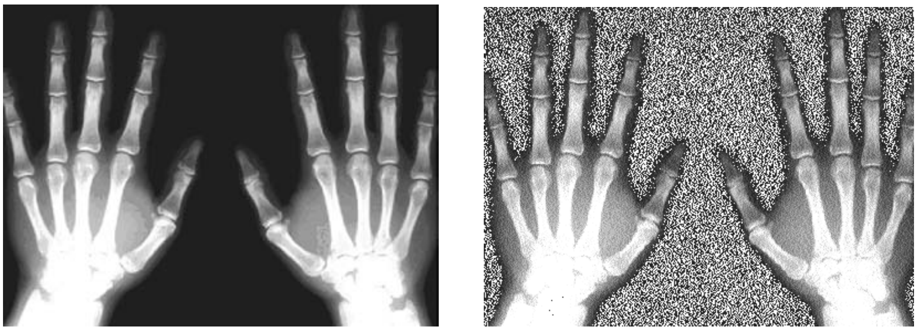

Fig. 15. Hand X-ray modulating signal (left) and noise affected demodulated one (right).

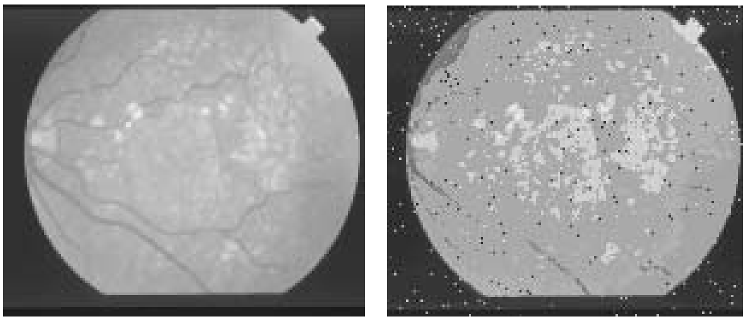

Fig. 16. Rethinian modulating signal (left) and noise affected demodulated one (right).

CONCLUSIONS

The proposed communication system is based on a discrete-time chaotic emitter and an inverse system synchronizing receiver. Our analysis aims at showing the effect of chaos modulation on 1D and 2D biomedical signals. The synchronizing receiver demodulates the information modulating signal, with a zero error if no channel noise is present. This good performance is obtained because both modulation and demodulation systems are discrete-time digitally implemented, ensuring good parameter and signal processing precision. It is highlighted that channel noise leads to synchronization errors. The smaller the noise variance, the less affected the recovered signals will be. The simulation results show that 1D signals are more resilient in the proposed chaos modulation scheme, resisting to somewhat larger channel noise levels.

Acknowledgments. We thank Vasile Apopei for the suggestion regarding biomedical application.

REFERENCES

1. CARROL T. L., PECORRA L. M., *Synchronizing Chaotic Circuits*, IEEE Transactions on Circuits and Systems, April 1991, **38** (*4*), pp. 453–456.
2. FELDMANN U., HASLER M., SCHWARTZ W., *Communication by Chaotic Signals: the Inverse System Approach*, International Journal of Circuit Theory and Applications, Wiley 1996, **24** (*5*), pp. 551–579.
3. GRIGORAS C., GRIGORAS V., *Implementation Non-Ideality Influence on the Nonlinear Dynamics of Chaotic Generators*, Buletinul Institutului Politehnic din Iasi, Sectia Automatica si calculatoare, 2014, **LX (LXIV)** (*1*), pp. 27–36.
4. TEODORESCU H.-N., COJOCARU V., *Complex signal generators based on capacitors and on piezoelectric loads*, Chaos Theory: Modeling, Simulation and Applications, 2010, World Scientific Publishing Co. Singapore, pp. 423–430.
5. ANDREATOS A. S., VOLOS C. K., *Secure Text Encryption Based on Hardware Chaotic Noise Generator*, 2nd International Conference on Cryptography and Its Applications in the Armed Forces, 2014.
6. SPROTT J. C., *A new class of chaotic circuit*, Physics Letters A, 2000, **266** (*1*), pp. 19–23, DOI:10.1016/S0375-9601(00)00026-8.
7. GRIGORAS C., GRIGORAS V., *Implementation Non-Ideality Influence on the Nonlinear Dynamics of Chaotic Generators*, Buletinul Institutului Politehnic din Iaşi, Secția Automatică şi calculatoare, 2014, **LX (LXIV)** (*1*), pp. 27–36.
8. STOJANOVSKY T., KOCAREV L., *Chaos-Based Random Number Generators – Part I: Analysis*, IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications, Mar. 2001, **48** (*3*), 281–288.
9. YALCIN M. E., SUYKENS J. A. K., VANDEWALLE J., *True Random Bit Generation From a Double Scroll Attractor*, IEEE Transactions on Circuits and Systems I: Regular Papers, Jul. 2004, **51** (*7*), 1395–1404.
10. YANG H. T., HUANG R. J., CHANG T. I., *A Chaos-Based Fully Digital 120 MHz Pseudo Random Number Generator*, Proceedings of the IEEE Asia-Pacific Conference on Circuits and Systems, Dec. 6–9, 2004, 357–360.
11. GRIGORAS V., GRIGORAS C., *Chaos Encryption Method Based on Large Signal Modulation in Additive Nonlinear Discrete-Time Systems*, Proceedings WSEAS – NOLASC'06, Bucureşti, 16-18.10.2006, 518–315