Scan to know paper details and
author's profile

Encryption & Decryption Audio Communications in Mobile Networks based on a New Hyperchaotic System

S. N. Lagmiri, J. Elalami & N. Elalami

Mohammed V University

ABSTRACT

With the significant development of digital communications and networking technologies, there is need to protect the sensitive data (such as digital audio signals, images, and videos) from unauthorized access, getting leak or misused. Cryptography plays a major role within the field of network security. There are many encryption techniques available currently to secure the data. Traditional encryption such as DES and many others perform poorly for multimedia data because of the large data size and high redundancy. Due to the random-like property and high sensitivity for initial values and control parameters, hyperchaotic systems are usually proposed as a solution to data encryption. In this paper, a study on security of audio data encryption based on a new six dimensional hyperchaotic system is presented. The experimental results on audio data encryption / decryption over open networks, key sensitivity tests, and statistical analysis show that the proposed cryptosystem have excellent encryption performance, high sensitivity to the security keys and can be applied for secure real time encryption.

Keywords: NA

Classification: K.6.5

Language: English

London
Journals Press

LJP Copyright ID: 975711
Print ISSN: 2514-863X
Online ISSN: 2514-8648

London Journal of Research in Computer Science and Technology

24UK

Volume 18 | Issue 1 | Compilation 1.0

Encryption & Decryption Audio Communications in Mobile Networks based on a New Hyperchaotic System

S. N. Lagmiri α, J. Elalami σ & N. Elalami ρ

I. ABSTRACT

With the significant development of digital communications and networking technologies, there is need to protect the sensitive data (such as digital audio signals, images, and videos) from unauthorized access, getting leak or misused. Cryptography plays a major role within the field of network security. There are many encryption techniques available currently to secure the data. Traditional encryption such as DES and many others perform poorly for multimedia data because of the large data size and high redundancy. Due to the random-like property and high sensitivity for initial values and control parameters, hyperchaotic systems are usually proposed as a solution to data encryption. In this paper, a study on security of audio data encryption based on a new six dimensional hyperchaotic system is presented. The experimental results on audio data encryption / decryption over open networks, key sensitivity tests, and statistical analysis show that the proposed cryptosystem have excellent encryption performance, high sensitivity to the security keys and can be applied for secure real time encryption.

Author α: SIP, Mohammadia School Engineering Mohammed V University, Rabat, Morocco.

σ: LASTIMI, Higher School of Technology of Sale Mohamed V University, Rabat, Morocco.

ρ: LAII, Mohammadia School Engineering Mohamed V University, Rabat, Morocco.

II. INTRODUCTION

A secure communication is one of the most important of our needs in digital world. Many studies on hiding data types like text, image, audio and video have been accomplish in order to meet such need. Speech cryptography can be defined as the art or science of altering information, so that the real information is hard to extract during transfer over any unsecured channel. The strength of the Encryption technique comes from the fact that no one can read or steal the information without altering its content [1].

In general, there are two types of encryption schemes namely symmetric encryption and asymmetric encryption. Symmetric key otherwise known as secret key or shared key or private key is one of the encryption methods [5] which use one key for encryption as they do for decryption process. Asymmetric cryptography [2, 3] uses different encryption keys for encryption and decryption.

Therefore, the efficient voice security design will has new challenges. Can the proposed system provide high security to the voice signal? To realize this, a number of voice encryption techniques have been studied [3-16]. Some of these included directly hiding audio files while others included methods of hiding the information by embedding some other data in the audio files. The general objective of all these studies is to prevent the possession of data by undesired people far [6, 13, 15, 17].

During the last decades, chaotic systems have received great attention from mathematicians, physicists, biologists, control engineers, etc. see e.g. [7, 9]. This interest has been greatly motivated by the possibility of encrypted information transmission by using a chaotic carrier; see e.g. [4, 8-14].

From these researches, the chaotic system was regarded as an efficient technique for voice data. They provide high secure techniques. This is because of that the chaotic techniques have a high sensitivity to any change in its initial conditions, in addition to the other properties such as random behavior, ergodicity, and the long periodicity.

In this paper, we discuss an alternative symmetric-key encryption algorithm for securing audio message. One level of security is used to encrypt the input signal which this level is digital chaotic system in order to increase the key space.

The organization of this paper is as follows. Section 2 describes the proposed six hyperchaotic system. In section 3, proposed encryption algorithm is described. Section 4 presents the experimental part, and discusses the corresponding results. The last section concludes the paper.

III. HYPERCHAOTIC PROPOSED SYSTEM

2.1 Novel hyperchaotic system

The novel six-dimensional hyperchaotic, that exhibit hyperchaotic behavior for a selective set of its parameter, is defined by:

$$\begin{cases} \dot{x}_1 = -\mathrm{a}x_1 + \mathrm{a}x_2 \\ \dot{x}_2 = -x_1x_3 + \mathrm{b}x_4 \\ \dot{x}_3 = -\mathrm{c}x_3 + \mathrm{h}x_1x_2 \\ \dot{x}_4 = \mathrm{a}x_2 - \mathrm{a}x_4 \\ \dot{x}_5 = -x_3x_6 + \mathrm{b}x_4 + 10x_2 - 10x_5 \\ \dot{x}_6 = -\mathrm{c}x_6 + \mathrm{h}x_4x_5 \end{cases} \quad (1)$$

Where:

- x_i are the state variables and a, b, c and h are positive constants.

When $a = 5$, $b = 20$ $c = 1$ and $h = 3.5$, the system (1) is hyperchaotic.

By using the initial conditions x_0=[1, 0, 3, -1, 2, 4]. Figure 1 shows the attractor of our new hyperchaotic system.

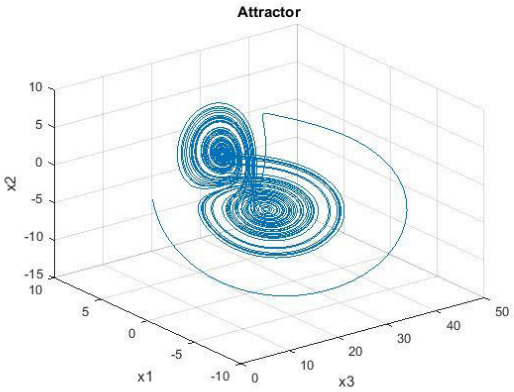
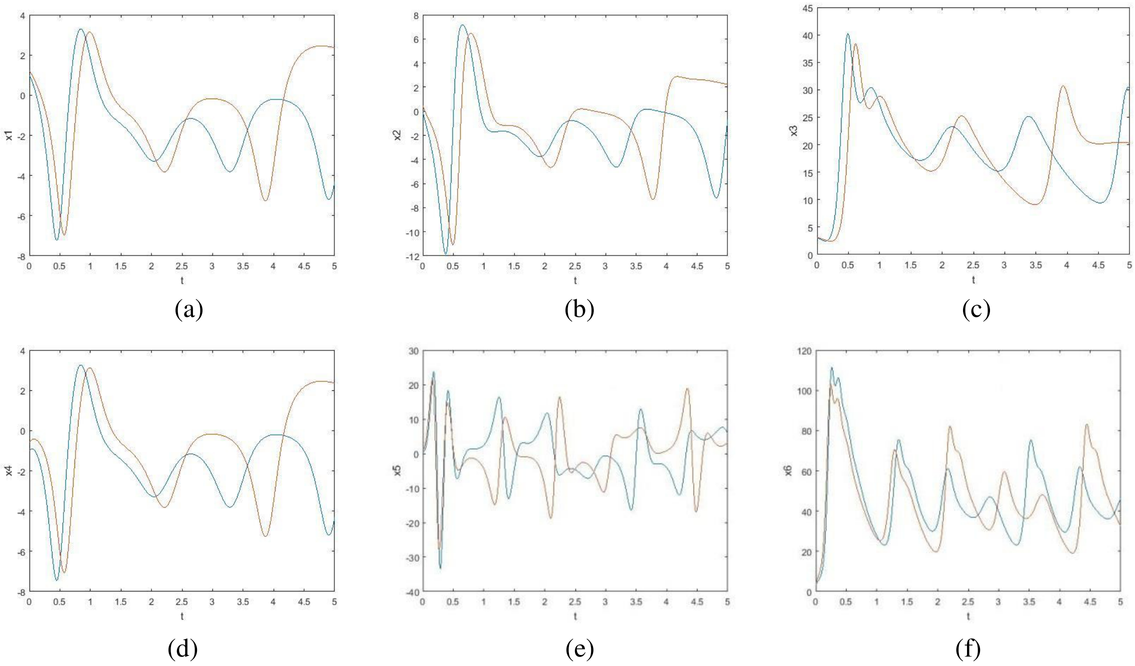


Fig. 1: Hyperchaotic attractor

One of the fundamental principles of chaotic functions is sensitive dependence, or sensitivity to initial conditions and highly complex random-like nonlinear behaviors. The performance of the system must be studied in this important feature.

2.2 Sensitivity to initial conditions

Sensitivity to initial conditions means that each point in a chaotic system is arbitrarily closely approximated by other points with significantly different future paths, or trajectories. Thus, an arbitrarily small change, or perturbation, of the current trajectory may lead to significantly different future behavior. The figure 2 compares the time series for two litely different initial conditions for the six states. The two time series stay close together, but after that, they are pretty much on their own. [10].



(a) (b) (c)

(d) (e) (f)

Fig. 2: Sensitivity to two initial conditions [1 0 3 -1 2 4] and [1.2 0.5 3.1 -0.6 2.7 4.2]

(a): x_1 (b): x_2 (c): x_3 (d): x_4 (e): x_5 (f): x_6

III. AUDIO ENCRYPTION IN MOBILE NETWORKS COMMUNICATIONS

With rapid advances in circuit design and prime focus on miniaturization, mobile phones have kept shrinking in size with each passing day. Hence power consumption and charge storage assume particular importance in mobile technology. Any design of a mobile communication block must take this into full account.

Enlargement of the mobile community has increased the call for secure data transmission. A computationally simple technique can be implemented easily using few components and hence consumes less power, but has limitations in the amount of security it can provide. The task of this paper is to choose an efficient and simple chaos-based encryption [12, 19, 20] strategy to meet the requirements of users.

3.1 Proposed audio encryption scheme

In this section, a cryptosystem based on synchronized chaotic systems is described. The aim is to transmit encrypted audio messages from transmitter A to remote receiver B as is depicted in Figure 3. An audio message m is to be transmitted over an insecure communication channel [18].

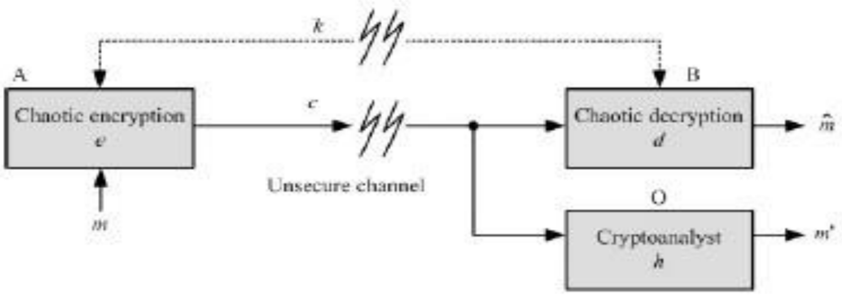


Fig. 3: Chaotic cryptosystem for audio communication

To avoid any unauthorized receiver located at the mentioned channel; m is encrypted prior to transmission to generate an encrypted message c:

$$c = e(m, k) \tag{2}$$

by using a chaotic system e on transmitter A. The encrypted message c is sent to receiver B, where m is recovered as $\hat{m}$ from the chaotic decryption d, as:

$$\hat{m} = d(c, k) \tag{3}$$

If e and d have used the same key, then at receiver end B it is possible to obtain $\hat{m} = m$. A secure channel is used for transmission of the keys, k. Generally, this secure communication channel is a courier and is too slow for the transmission of m. Our chaotic cryptosystem is reliable, if it preserves the security of m, i.e. if $\hat{m} \neq m$ for even the best cryptanalytic function $\hbar$, given by

$$m' = h(c)$$

To achieve the proposed chaotic encryption scheme, we appeal to an hyperchaotic system for encryption/ decryption purposes (c and d, respectively).

The novel six dimensional hyperchaotic system have a number of parameters determining their dynamics; such parameters and initial conditions are the coding "key", k.

IV. SIMULATION RESULTS AND SECURITY ANALYSIS

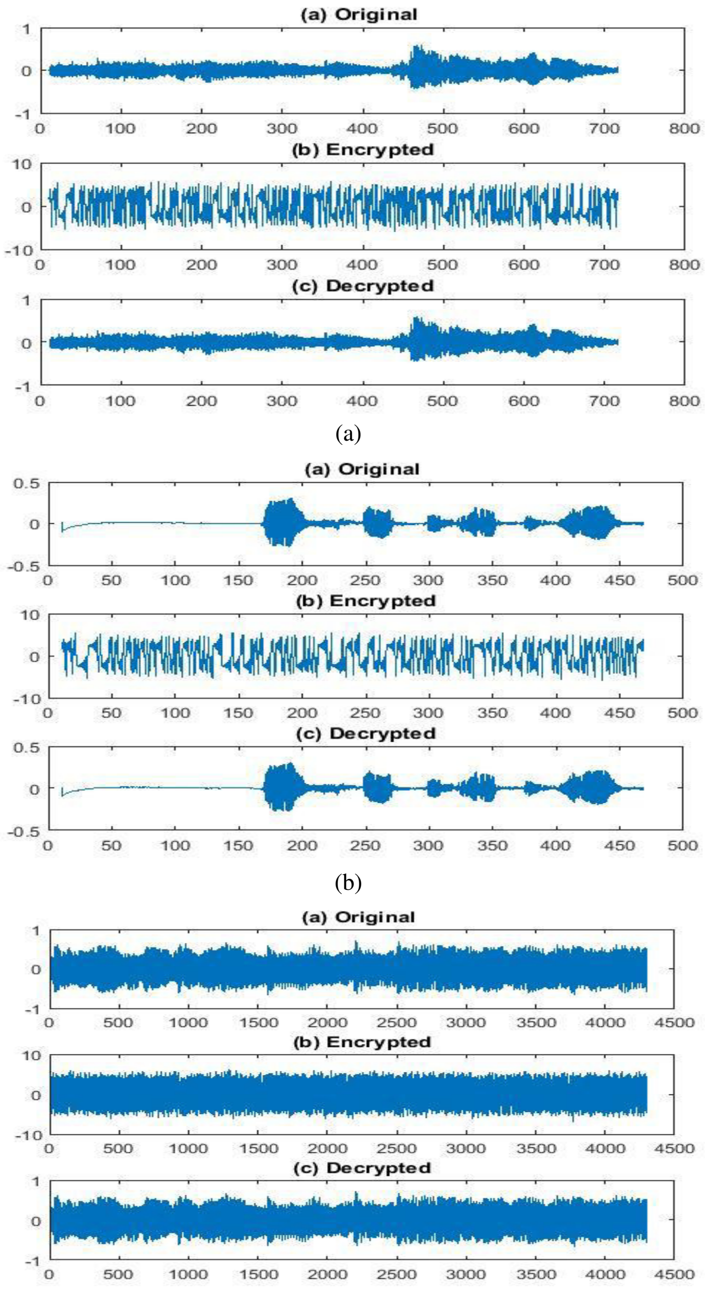
In this part, via numerical simulations, we illustrate the encrypted audio transmission. We use as transmitter and receiver the hyperchaotic system given in (1) for initial conditions x_{01} = [1, 0, 3, -1, 2, 4].

The properties of the three audio signals used in this paper are presented in Table 1.

Table 1: Audio Signals Properties

	Number Channels	Frequency (KHz)	Duration (sec)
Music	1	22.05	3.2503
Speech 1	1	22.05	2.1246
Speech 2	1	48	8.9634

Figure 4 shows audio communication via the hyperchaotic system given in (1). Original audio message m(t) to be encrypted and transmitted (top of figure), transmitted hyperchaotic signal c(t) (middle of figure), and recovered audio message m ̂(t) (bottom of figure). For the three audio data, we observe that the encrypted message is very different of the original one and looks like a white noise.



(a)

(b)

(c)

Fig. 4: Encryption results of the audio communication
(a) Music - (b) Speech 1 - (c) Speech 2

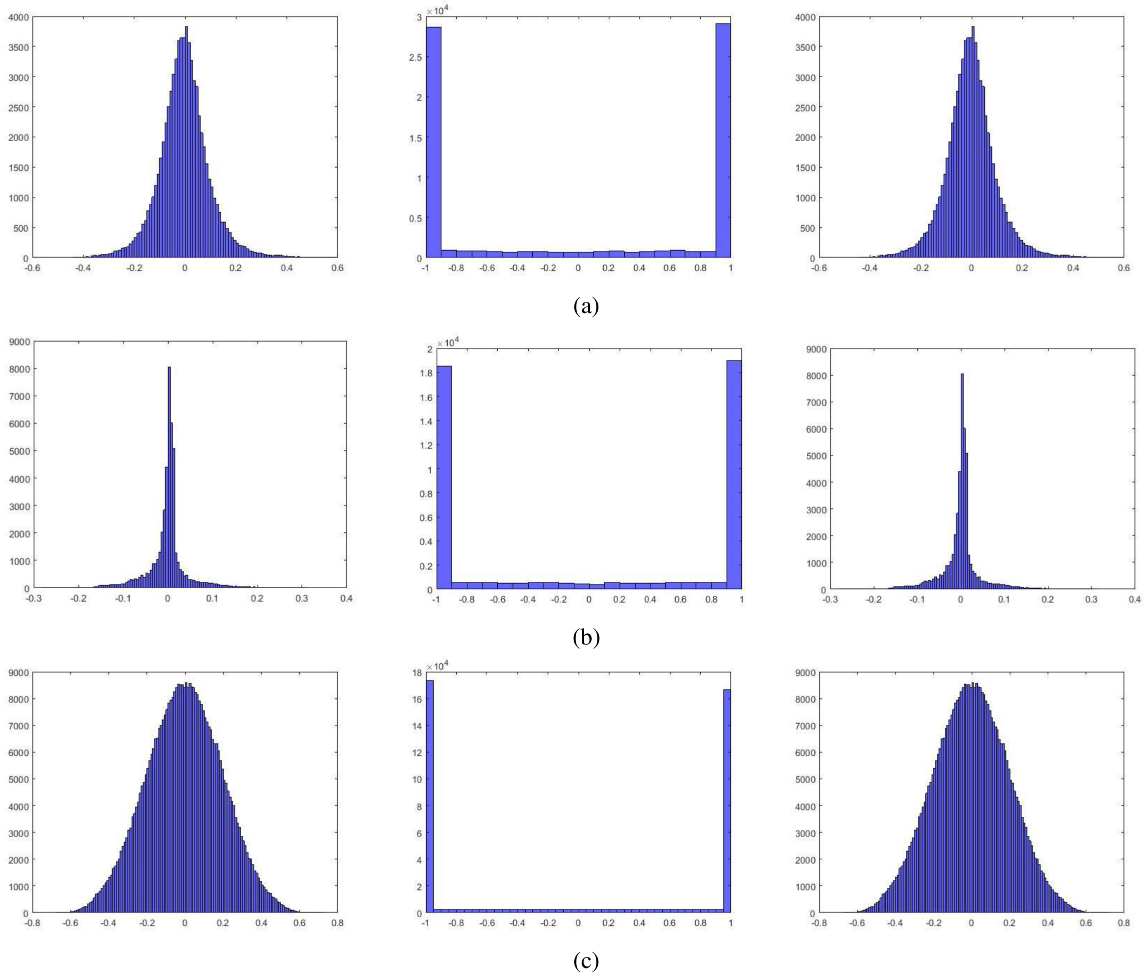
4.1 Security Analyses of Encryption Applications

Encryption processes may have been performed successfully. Yet, security analyses must be carried out in order to assess the reliability of encryption processes. Encrypted data with disappointing results in security analyses will not be preferred as they are so vulnerable to be decrypted. Key space analysis, key sensitivity analysis, chaos effect and histogram were performed in order to compare the chaotic systems utilized in this study.

4.2 Histogram analysis

Distributions of data values in a system comprise the histogram. Histogram analyses can be made by examining data distributions in many different fields. In encryption practices, if the distributions of numbers that represent encrypted data are close, this means encryption has been performed well. The closer the data distributions are, the more difficult it will be to decrypt the encrypted data [25].

Exploring the histogram of audio data in Figure 5. a), b) and (c), one can see that the distribution in Middle is totally different of the one in Left Therefore, it can be concluded that encryption with our new six hyperchaotic system is successful, and that's confirmed by the decrypted data in Right that have the same histogram as the original message.



(a)

(b)

(c)

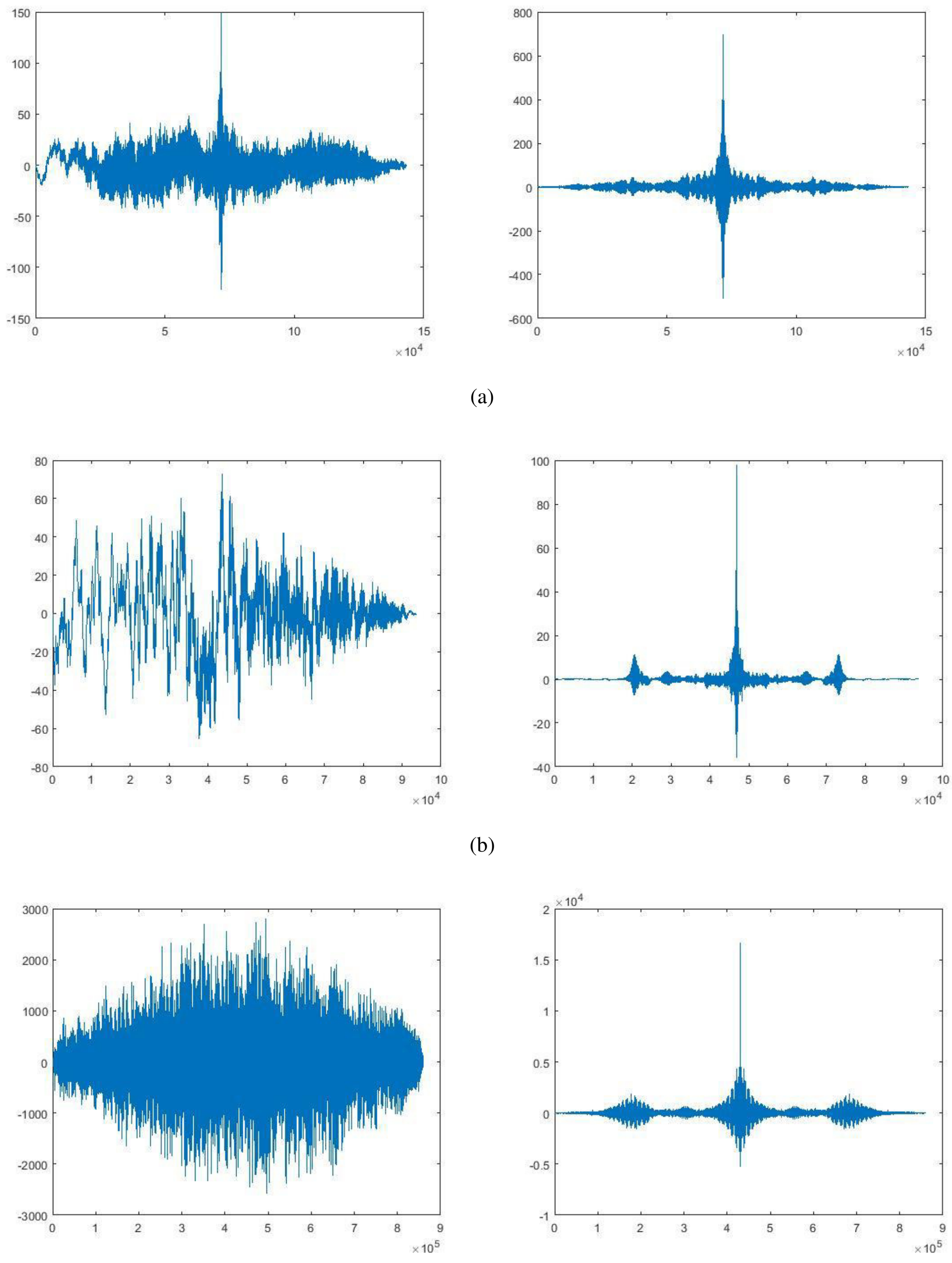
Fig. 5: Audio signals histogram (Original in Left – Encrypted in Middle – Decrypted in Right)
(a) Music (b) Speech 1 (c) Speech 2

4.3 Correlation test

The auto-correlation function identifies the chaotic system that produces a strong encryption [23]. A useful measure to assess the encryption quality of any cryptosystem is correlation coefficient between similar segments in the original signal and the encrypted signal. It is calculated as [16]:

$$r_{xk} = \frac{C(x,k)}{\sqrt{V(x)}\sqrt{V(k)}}$$

Where c (x, k) is the covariance between the original signal x and the encrypted signal k.v (x) and V (K) are the variances of the signals x and k.



(a)

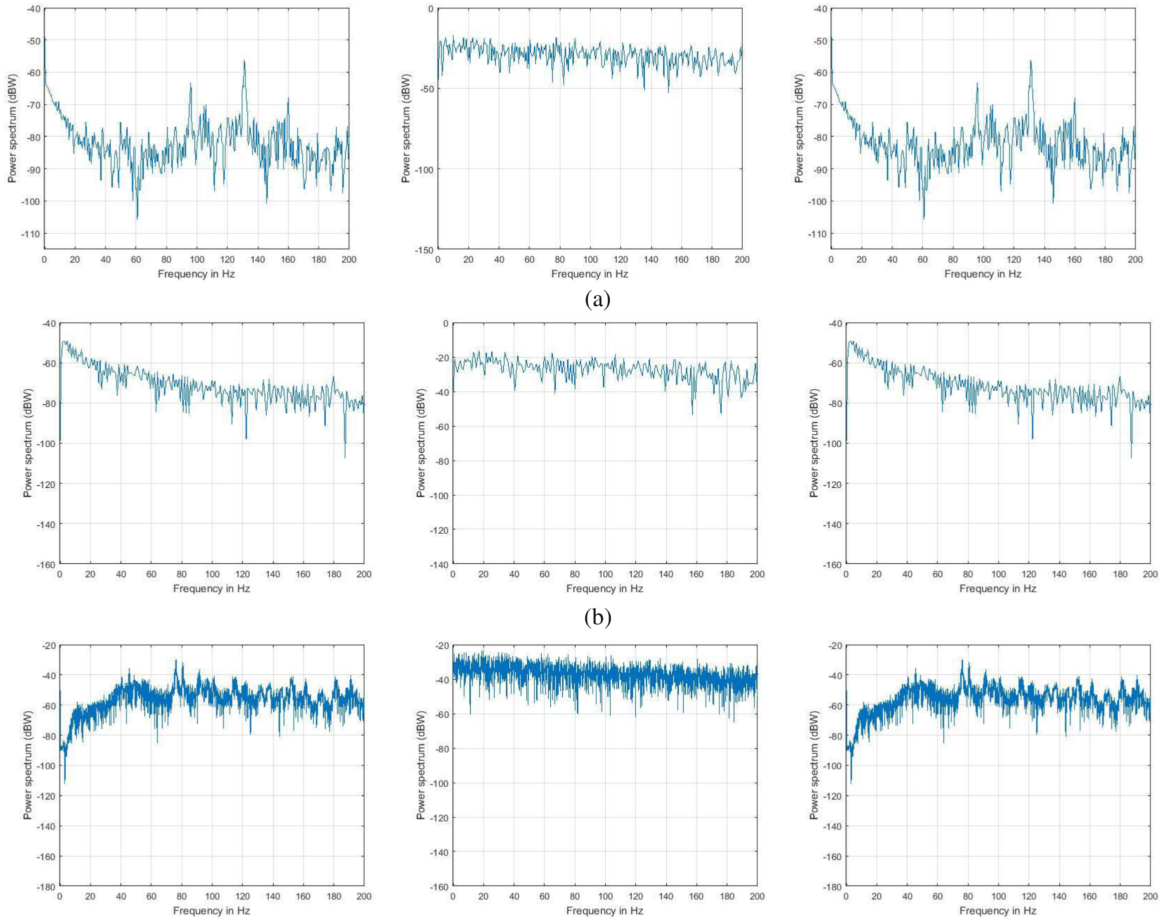
(b)

(c)

Fig. 6: Audio signals correlation: Original/Encrypted (Left) and Original/Decrypted (Right)
(a) Music (b) Speech 1 (c) Speech 2

4.4 Power spectrum

The following figures show that the power spectrum of original (a) and decrypted (c) audio signal are identical [21].



(a)

(b)

(c)

Fig. 7: Power spectrum of audio signals (Original in Left – Encrypted in Middle – Decrypted in Right) (a) Music (b) Speech 1 (c) Speech 2

4.5 PSNR test

Peak signal-to-noise ratio (PSNR) is the ratio between the maximum possible power of original speech signal and the power of encrypted signal [22]. PSNR is a calculation of encryption quality of the original signal. A higher PSNR indicates that the encryption or reconstruction is of higher quality. The PSNR is obtained from:

Table 2: PSNR Coefficient For Audio Data

	Encrypted	Decrypted
Music	47.3372	Inf
Speech 1	47.3837	Inf
Speech 2	47.2371	Inf

PSNR high means: Mean square error between the original and reconstructed signal is very low. It implies that the audio data been properly restored. In the other way, the restored signal quality is better; in our case, the value of PSNR is as follow:

PSNR (Original/Decrypted) = Inf

Contrariwise, a low PSNR means: Mean square error between the original signal and encrypted signal is very high. It implies that the audio data been correctly encrypted. In our case the value of PSNR is shown is Table 2.

The result is much closed with the correlation coefficient.

- The correlation coefficients for the original and decrypted signal are identical. The value of PSNR (Original/Decrypted) means that the decrypted audio data is identical to original data.
- The correlation coefficients for the original and encrypted signal are very different. The PSNR(Original/Encrypted) means that the encrypted audio data is totally different of the original data.

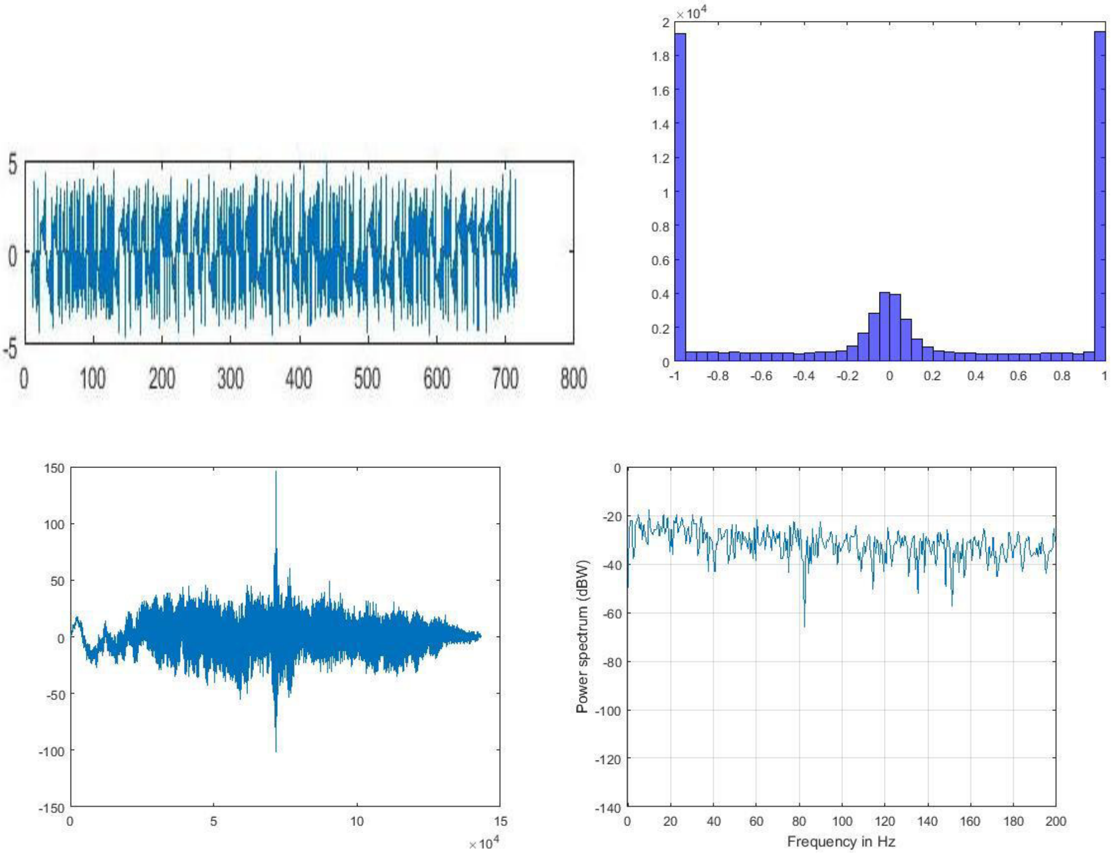
4.6 Security analysis

For testing the sensitivity of the proposed cryptosystem, the encrypted signal is decrypted with the reverse process of encryption method using the six hyperchaotic system by modifying the initial conditions of the system (1) with 10^{-9} as $_{O2} = [1, 0, 3, -1, 2, 4.000000001]$.

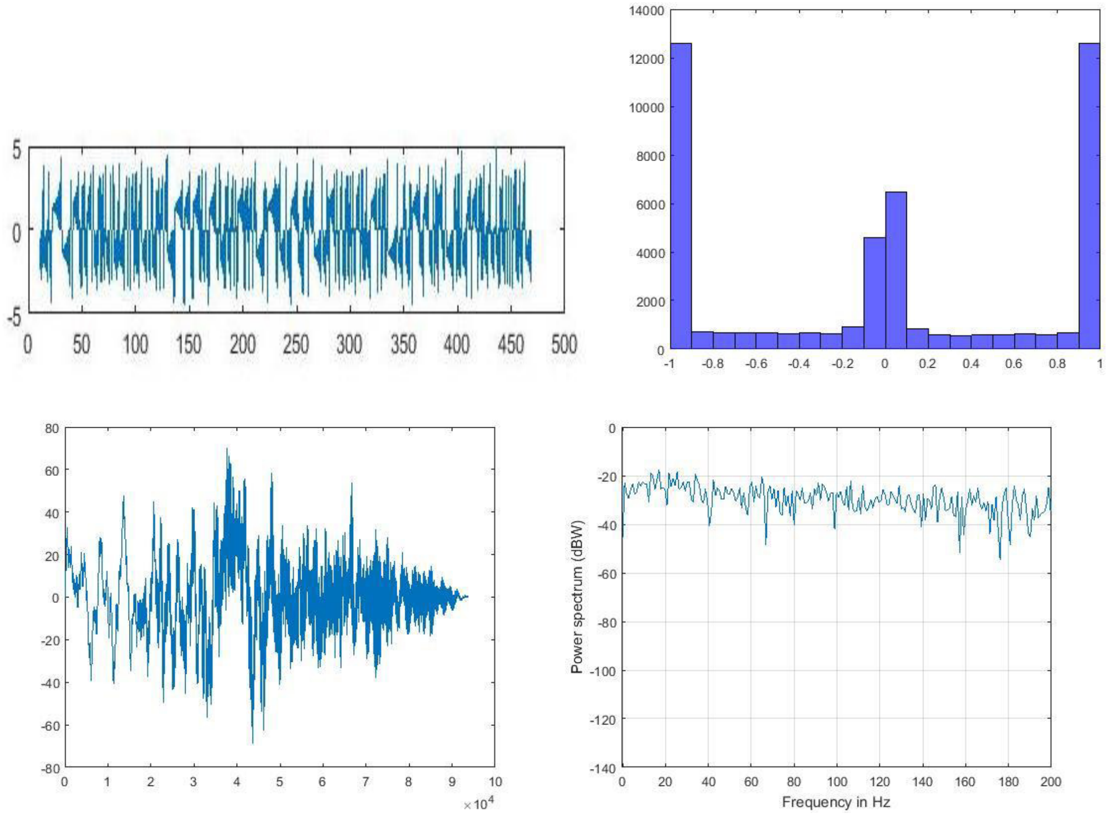
The decrypted signals are totally wrong, as shown in figure 8(a) (b) (c) (Top Left). The corresponding histogram, cross-correlation and power spectrum prove that the decrypted signals are totally different from the original ones. The Table 3 shows that the PSNR values are close to the encrypted signals. Hence the sensitivity of the encryption key is proven.

Table 3: PSNR Coefficient for Wrong Decrypted Audio Data

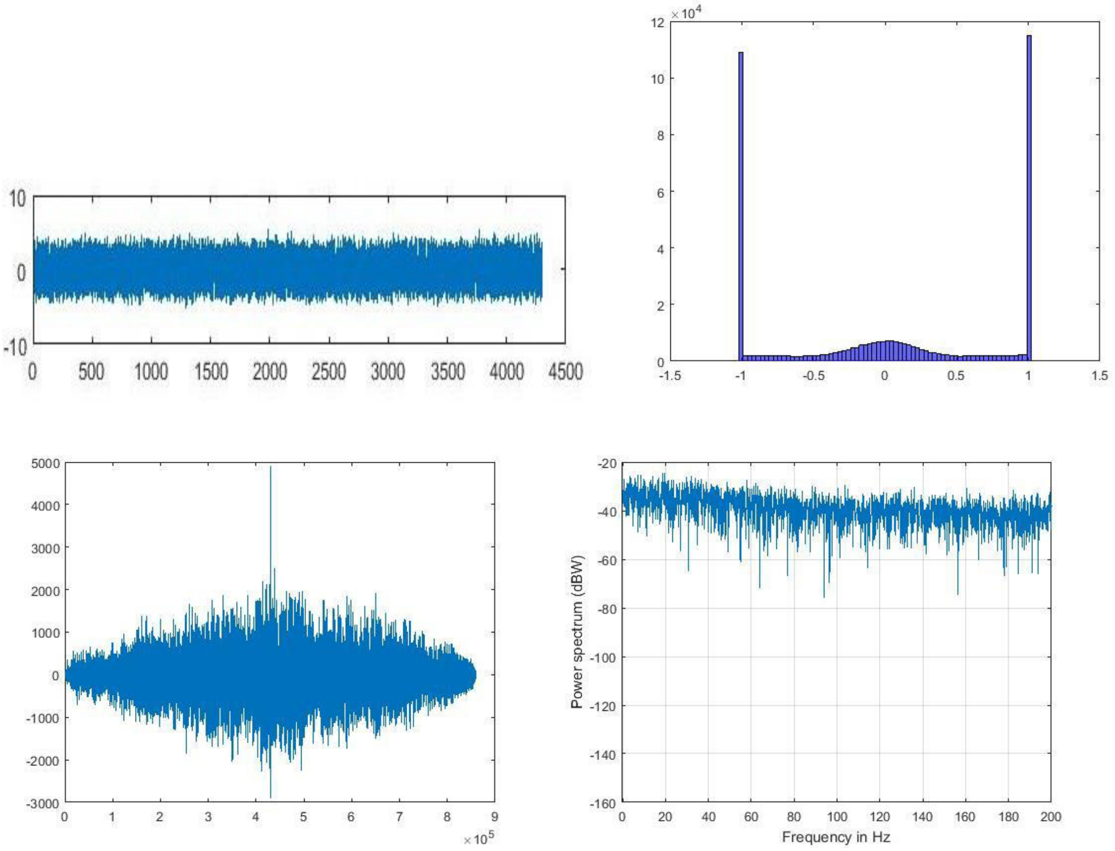
	Decrypted with wrong key
Music	48.7479
Speech 1	48.9013
Speech 2	48.6589



(a)



(b)



(c)

Fig. 8: Decrypted audio signals with $_{O2}$ = [1, 0, 3, −1, 2, 4.000000001]

V. CONCLUSION

A new encryption system for audio files was presented. Speech encryption using hyperchaotic generator is a proven model. In this method, the three different audio data are tested. The histogram of the encrypted signal shows that more sensitivity entails more security. The simulation results showed the audio signal proposed encryption method has high level of security and can recover the original signal quickly with good audio quality. The results endorse that the speech signal is highly masked from eavesdroppers. Statistical analysis using histograms, PSNR, correlation, and power spectrum showed that the algorithm is powerful.

REFERENCES

1. Bhaskar Mondal and Tarni Mandal, "A Multilevel Security Scheme using Chaos based Encryption and Steganography for secure audio communication", Jharkhand.
2. Anoop (2007), "Public key cryptography—applications algorithm and mathematical explanations".
3. T. Thongpon & K. Sinchai. "Accelerating asymmetric-key cryptography using parallel-key cryptographic algorithm". 6th International Conference on Computer and Information Technology, 2, 812–815, (2009).
4. D. López-Mancilla & C. Cruz-Hernández, "Output synchronization of chaotic systems: model-matching approach with application to secure communication", Nonlinear Dynamics and Systems Theory, 5 (2), 141- 15 (2005).
5. J. Fridrich. "Symmetric ciphers based on two-dimensional chaotic maps". International Journal of Bifurcation and Chaos, Volume 8(6), 1259–1284, (1998).
6. KG. Gopalan, DS. Benincasa, SJ. Wennd. "Data embedding in audio signals". IEEE Aerospace Conference Proceedings (Cat. No.01TH8542). Vol. 6, pp. 2713–2720, (2001).
7. C. Cruz-Hernández & A.A. Martynyuk, "Advances in chaotic dynamics with applications", Cambridge Scientific Publishers Ltd., Vol. 4, (2009).
8. U. Feldmann, M. Hasler and W. Schwarz, "Communication by chaotic signals: the inverse system approach", Int. J. Circuits Theory and Applications, 24, 551-579 (1996).
9. L. M. Pecora and T.L. Carroll, "Synchronization in chaotic systems", Phys.
10. S. N. Lagmiri, N. Elalami, J. Elalami. "Three Dimensional Chaotic System for Color Image Scrambling Algorithm". International Journal of Computer Science and Information Security (IJCSIS), Vol. 16, No. 1, January 2018.
11. M. Delgado-Restituto, M. Linan and A. Rodriguez-Vazquez, "CMOS 2.4pm chaotic oscillator: experimental verification of chaotic encryption of audio", *Electronics Letters,* Vol. 32, Issue 9, pp.795-796, 1996.
12. Wenwu Yu and Jinde Cao, "Cryptography based on delayed chaotic neural networks", *Physics Letters A*, Vol. 356, Issues 4-5, pp. 333-338, August 2006.
13. Chang CC, Lee RTC, Xiao GX, Chen TS (2003). "A new Speech Hiding Scheme based upon sub-band coding". Proceedings of the 2003 Joint Conference of the Fourth International Conference on Information, Communications and Signal Processing and Fourth Pacific Rim Conference on Multimedia. Vol. 2, pp. 980– 984.
14. L. Gámez-Guzmán, C. Cruz-Hernández, R.M. López-Gutiérrez, and E.E. García-Guerrero, "Synchronization of Chua's circuits with multiscroll attractors: Application to communication", Commun. Nonlinear Sci. Numer. Simulat. 14, 2765–2775 (2009).
15. Chen S, Leung H, Ding H (2007). " Telephony Speech Enhancement by Data Hiding". IEEE Transactıons On Instrumentatıon And Measurement. Vol. 56, no. 1, pp. 63–74.
16. Shujun Li, Guanrong Chen, Kwok-Wo Wong, Xuanqin Mou and Yuanlong Cai, "Baptista-type chaotic cryptosystems: problems and countermeasures", Physics Letters A, Vol. 332, Issue 5-6, pp 368-375, November 2004.

17. Dipu KHM, Alam SB (2010). “Hardware based real time, fast and highly secured speech communication using FPGA”. IEEE International Conference on Information Theory and Information Security, pp. 452–457.
18. L. M. Pecora and T.L. Carroll, “Synchronization in chaotic systems”, Phys.
19. Shujun Li, Guanrong Chen, Kwok-Wo Wong, Xuanqin Mou and Yuanlong Cai, “Baptista-type chaotic cryptosystems: problems and countermeasures”, *Physics Letters A*, Vol. 332, Issue 5-6, pp 368-375, November 2004.
20. Xiaogang Wu, Hanping Hu and Baoliang Zhang, “Analyzing and improving a chaotic encryption method”, *Chaos, Solitons & Fractals*, Vol. 22, Issue 2, pp. 367-373, October 2004.
21. S. N. Lagmiri, J. Elalami, N. Elalami. "Hyperchaotic system for encryption & decryption audio communications". The 17th IEEE International Conference on Trust, Security and Privacy in Computing and Communications (IEEE TrustCom-18), 1-3 August, 2018. New York, USA.
22. S. N. Lagmiri, N. Elalami, J. Elalami. "Audio encryption algorithm using hyperchaotic systems of different dimensions”. 1st International Conference on Networking, Information Systems & Security, April 27-28, 2018, Tangier, Morocco.
23. Matej Salamon (2012), “Chaotic Electronic Circuits in Cryptography, From the book Applied Cryptography and Network Security”, InTech.
24. S. N. Lagmiri, N. Elalami, J. Elalami. "Color and gray images encryption algorithm using chaotic systems of different dimensions". International Journal of Computer Science and Network Security, Vol.18, No.1, January 2018.
25. S. N. Lagmiri, N. Elalami, J. Elalami. "Three Dimensional Chaotic System for Color Image Scrambling Algorithm". International Journal of Computer Science and Information Security, Vol.16, No.1, January 2018.