AUDIO ENCRYPTION ALGORITHM USING HYPERCHAOTIC SYSTEMS OF DIFFERENT DIMENSIONS

S. N. Lagmiri[1], H. Bakhous[2]

[1,2]IRSM, Higher Institute of Management Administration and Computer Engineering, Rabat, Morocco

ABSTRACT

Data security has become an important concern for communication through an insecure channel because the information transferred across the networks has a large chance of unauthorized access. The available encryption algorithms that are primarily used for text data may not be suitable for multimedia data such as sound. Hyperchaotic systems are generally proposed as a solution to multimedia encryption, because of their random properties and the high sensitivity of initial conditions and system parameters.

In this paper, audio data encryption with different dimensional hyperchaotic systems has been presented. The proposed hyperchaotic systems exhibit excellent chaotic behavior. To demonstrate its application to the processing of multimedia encryption, the three systems are applied with an algorithm based on the key generation from the initial conditions for encryption and decryption process. The results of encryption, decryption and statistical analysis of the audio data show that the proposed cryptosystem has excellent encryption performance, high sensitivity to security keys and can be applied for secure real-time encryption.

KEYWORDS

Audio signal, Hyperchaotic system, Encryption algorithm, Histogram, Correlation, Power spectrum.

1. INTRODUCTION

With the increasing use of digital techniques, confidentiality, integrity as well as authenticity has become a major concern. Multimedia data transferred through these digital techniques is used in various fields such as medical, military, science, engineering, ect.

To meet this need, many studies on the masking of data types such as text, image, audio and video have been carried out. Security can be defined as the hiding of information in fact to be difficult to extract real information when transferring on an 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]. Thus, many studies on the encryption of audio data have been published so far [16, 17, 18, 19]. Some of these included direct masking of audio files, while others included methods to hide information by incorporating other data into the audio files. The general objective of all these studies is to prevent the possession of data by unwanted persons.

Natarajan Meghanathan et al. (Eds) : DaKM, SIPP, CCSIT, NCWMC - 2018
pp. 99–111, 2018. © CS & IT-CSCP 2018 DOI : 10.5121/csit.2018.81507

Similarly, traditional encryption methods are less effective in securing real-time multimedia data encryption systems and have certain drawbacks and weaknesses with respect to high-speed data encryption [3, 4]. On the contrary, chaos-based encryption algorithms have many advantages for the random properties of chaotic systems, such as sensitivity to initial conditions and ergodicity of states [2]. In recent decades, mathematicians, physicists, biologists, control engineers, etc, have a great attention to chaotic systems. [5, 7]. This interest was greatly motivated by the possibility of encrypted transmission of information using chaotic support; see for example [6, 8, 14].

This article discusses a chaos-based symmetric key encryption algorithm for securing audio signals.

The organization of this paper is as follows. Section 2 presents audio encryption in mobile network communications. Section 3 describes the different proposed hyperchaotic systems. Section 4 describes the proposed encryption algorithm. Section 5 presents the experimental part and discusses the corresponding results. The last section concludes the paper.

2. 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 [9, 12, 21] strategy to meet the requirements of hardware implementation standards [11].

3. HYPERCHAOTIC PROPOSED SYSTEMS

The first step in designing an encryption algorithm is to choose the adequate chaotic system with good cryptographic properties. In this section, three chaotic systems of different dimensions are presented. One of the fundamental principles of hyperchaotic functions is sensitivity to initial conditions and highly complex random-like nonlinear behaviors. The performance of the system must be studded in those two important features.

3.1 New 4D Hyperchaotic System

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

$$\begin{cases} \dot{x}_1 = a(x_2 - x_1) \\ \dot{x}_2 = bx_1 - x_1x_3 \\ \dot{x}_3 = -cx_3 + hx_1x_1 \\ \dot{x}_4 = -ax_4 + ax_2 \end{cases} \quad (1)$$

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

When $a = 10$, $b = 40$ $c = 2.5$ and $h = 4,$ the system (1) is hyperchaotic.

By using the initial conditions $x_0 = [5.6 \quad -1.2 \quad 3.4 \quad 0]$. Figure 1 show the attractor of the hyperchaotic system (1).

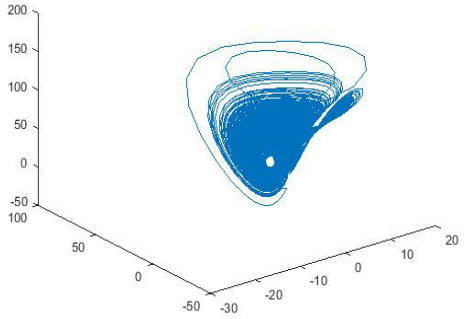


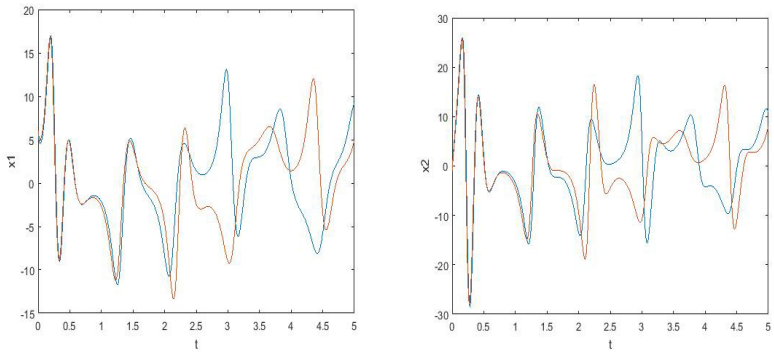
Fig. 1. 4D hyperchaotic attractor

Sensitivity to Initial Conditions:

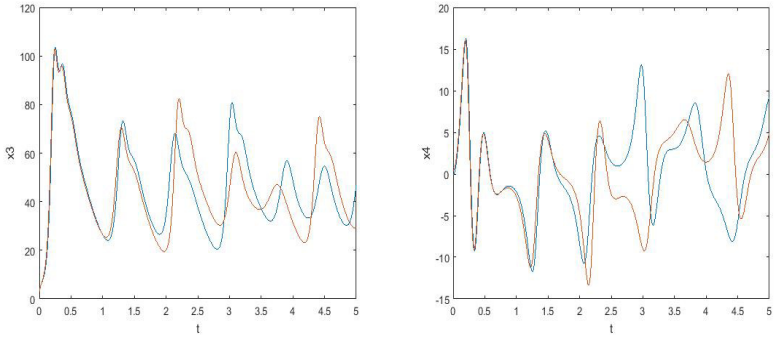
The phenomenon of sensitivity to initial conditions was discovered by Poincaré in his study of the the n-body problem, then by Jacques Hadamard using a mathematical model named geodesic flow, on a surface with a non-positive curvature, called Hadamard's billards. A century after Laplace, Poincaré indicated that randomness and determinism become somewhat compatible because of the long term unpredictability [10].

A very small cause, which eludes us, determines a considerable effect that we cannot fail to see, and so we say that this effect Is due to chance. If we knew exactly the laws of nature and the state of the universe at the initial moment, we could accurately predict the state of the same universe at a subsequent moment. But even If the natural laws no longer held any secrets for us, we could still only know the state approximately. If this enables us to predict the succeeding state to the same approximation, that is all we require, and we say that the phenomenon has been predicted, that It Is governed by laws. But this is not always so, and small differences in the initial conditions may generate very large differences in the final phenomena. A small error in the former will lead to an enormous error in the latter. Prediction then becomes impossible, and we have a random phenomenon.

This was the birth of chaos theory.



(a) (b)



(c) (d)

Fig. 2. Sensitivity to two initial conditions [5.6 -1.2 3.4 0] and [6 -1 3 0.5]

(a):x_1 *(b):* x_2 *(c):* x_3 *(d):* x_4

3.2 New 5D Hyperchaotic System

By adding the fifth equation to the system (1), we obtain a new five hyperchaotic system as follow:

$$\begin{cases} \dot{x}_1 = a(x_2 - x_1) \\ \dot{x}_2 = bx_1 - x_1x_3 \\ \dot{x}_3 = -cx_3 + hx_1x_1 \\ \dot{x}_4 = -ax_4 + ax_5 \\ \dot{x}_5 = -x_3x_4 + bx_4 + 10x_2 - 10x_5 \end{cases} \quad (2)$$

Figure 3 shows the attractor of the system (2) using the initial conditions $x_0 = [5.6\ -1.2\ 3.4\ 0\ 2]$.

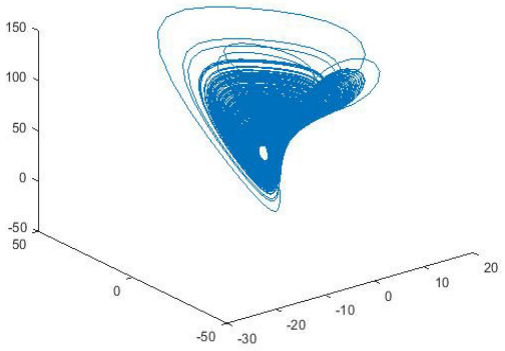


Fig. 3. 5D hyperchaotic attractor

Sensitivity to Initial Conditions: As it defined in section 3.1the sensitivity to initial conditions for the five hyperchaotic system is shown in figure 4.

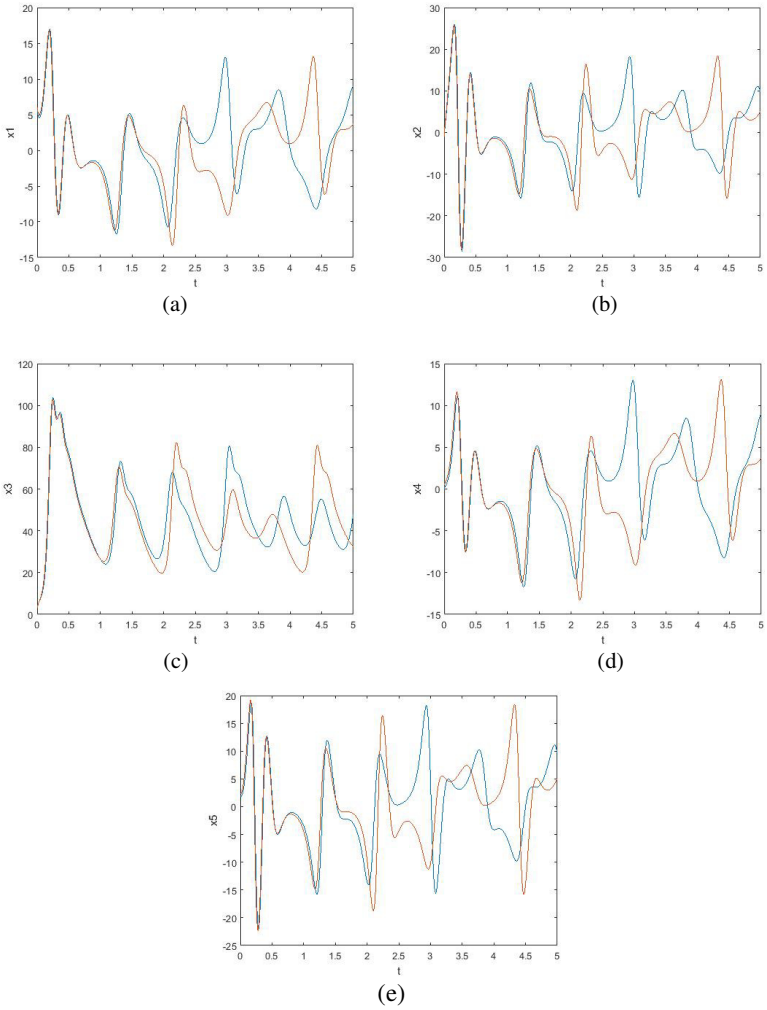


Fig. 4. Sensitivity to two initial conditions [5.6 -1.2 3.4 0 2] and [6 -1 3 0.5 2.3]

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

3.3 New 6D Hyperchaotic System

The new six-dimensional hyperchaotic, is built by adding the least equation to the system (2):

$$\begin{cases} \dot{x}_1 = -\mathrm{a}x_1 + \mathrm{a}x_2 \\ \dot{x}_2 = -x_1x_3 + \mathrm{b}x_1 \\ \dot{x}_3 = \mathrm{h}x_1x_1 - \mathrm{c}x_3 \\ \dot{x}_4 = -\mathrm{a}x_4 + \mathrm{a}x_2 \\ \dot{x}_5 = -x_4x_6 + \mathrm{b}x_4 + 10x_2 - 10x_5 \\ \dot{x}_6 = \mathrm{h}x_1x_1 - \mathrm{c}x_6 \end{cases} \tag{3}$$

By using the initial conditions $x_0 = [5.6 \;\; -1.2 \;\; 3.4 \;\; 0 \;\; 2 \;\; 4]$. Figure 5 show the attractor of our new six hyperchaotic.

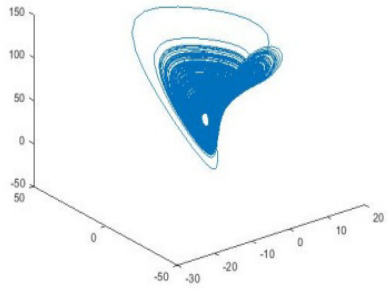


Fig. 5. 6D hyperchaotic attractor

Sensitivity to Initial Conditions: As it defined in section 3.1 the sensitivity to initial conditions for the four hyperchaotic system is shown in figure 6.

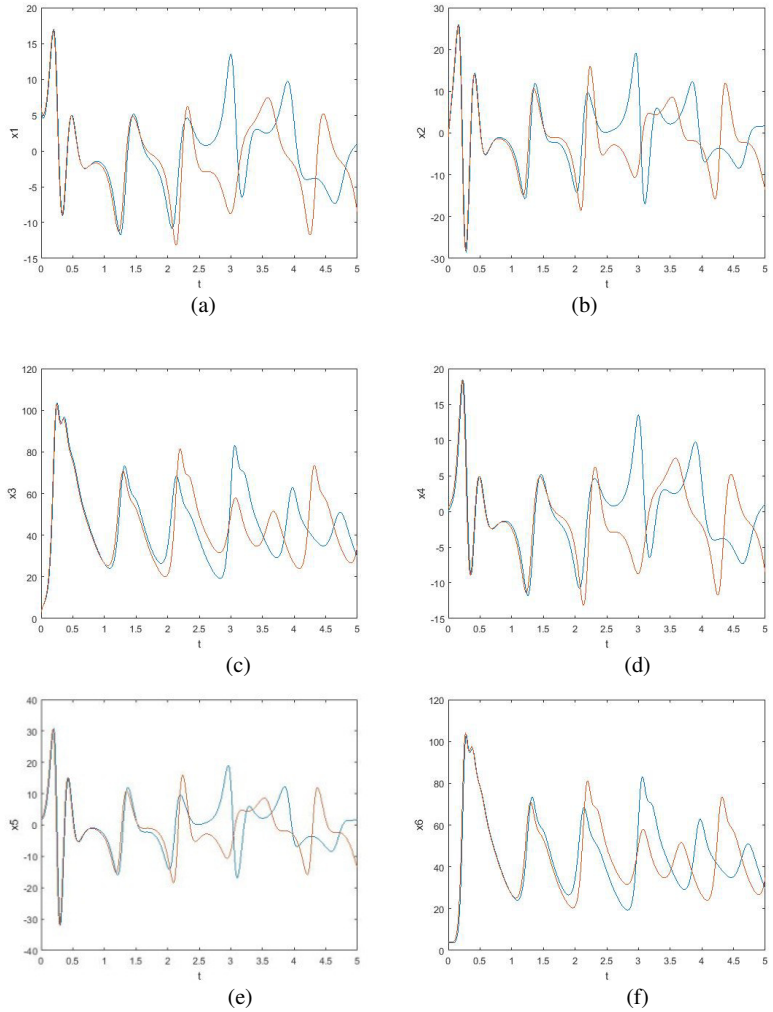


Fig. 6. Sensitivity to two initial conditions [5.6 -1.2 3.4 0 2 4] and [6 -1 3 0.5 2.3 4.2]

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

4. 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 7. An audio message m is to be transmitted over an insecure communication channel.

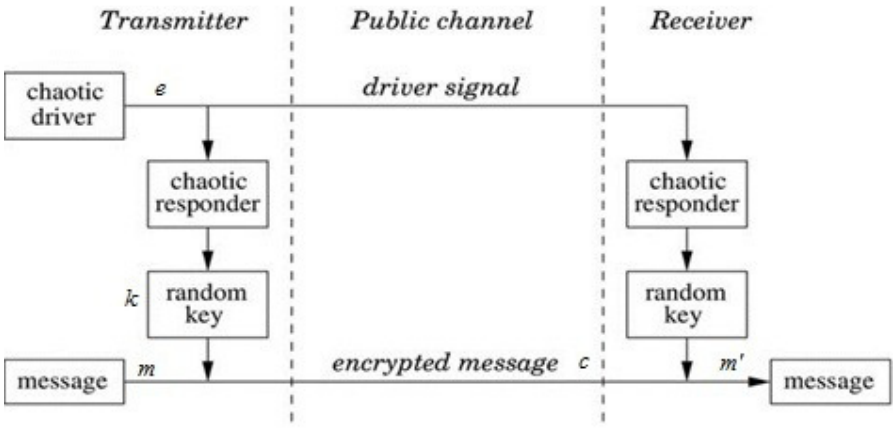


Fig. 7. Chaotic cryptosystem for audio communication [22]

To avoid any unauthorized receiver located at the mentioned channel; m is encrypted prior to transmission to generate an encrypted message$c$ [13]:

$$c = e(m, k) \tag{4}$$

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:

$$\hat{m} = d(c, k) \tag{5}$$

If e and d have used the same key k, 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 h, 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 four dimensional hyperchaotic system have a number of parameters determining their dynamics; such parameters and initial conditions are the coding "key", k.

5. 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 respectively in (1), (2) and (3) for initial conditions$x_{01} = [-1, 1, -3, 1]$, $x_{02} = [-1, 1, -3, 1, 0]$and $x_{03} = [-1,1, -3,1,0,2]$.

The original audio signal $m(t)$ is 22 KHz. The mentioned audio message is to be encrypted and transmitted to the receiver.

Figure 8 shows audio communication via the hyperchaotic system given in (1) (a), (2) (b) and (3) (c). 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 $\hat{m}(t)$ (bottom of figure). Figure 9 shows the histogram for original (a), encrypted (b) and recovered (c) audio signal.The figure 10, the power spectrum of $m(t), c(t)$and$\hat{m}(t)$is presented.And figure 11 presents the correlation coefficient.

5.1 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. Kkey sensitivity analysis, chaos effect, corrlation test, PSNR test and histogram were performed in order to compare the hyperchaotic systems utilized in this study.

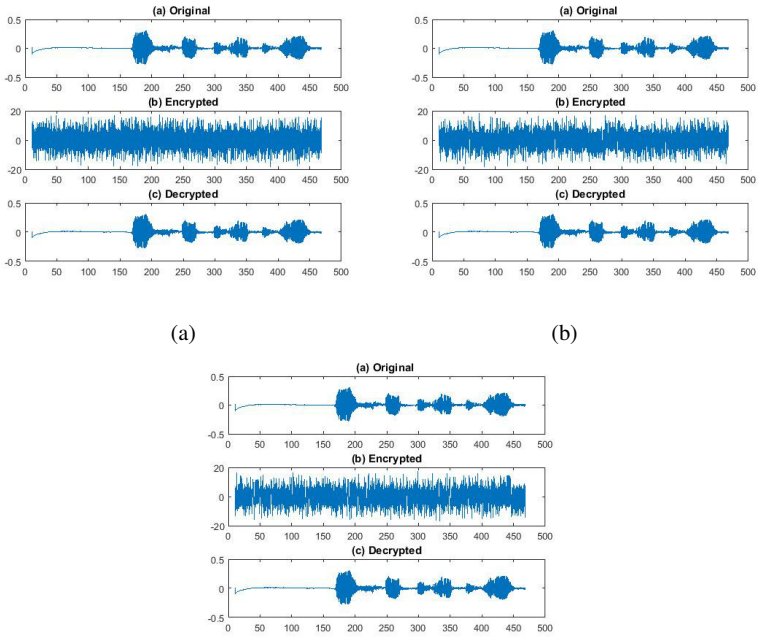


Fig. 8. Original/Encrypted/Decrypted audio communication
(a) 4D system - (b) 5D system - (c) 6D system

5.2 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 [15].

Examining the histogram diagrams of audio data in Figure 9, we can see that the histogram of original (a) and encrypted (b) audio signal are totally different. Therefore the histogram of decrypted signal (c) is identical to the histogram (a).

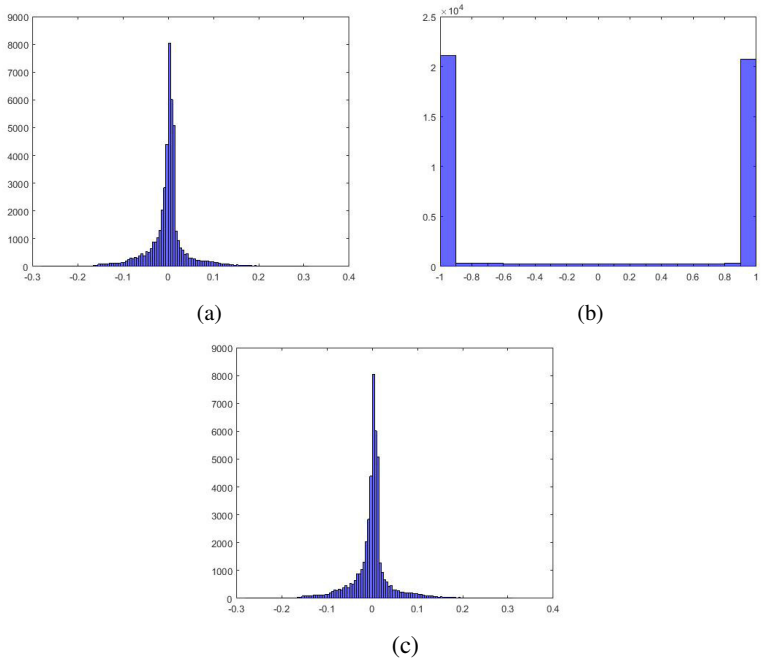


Fig. 9. Histograms audio signal (a) original (b) Encrypted (c) Decrypted

5.3 Power Spectrum

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

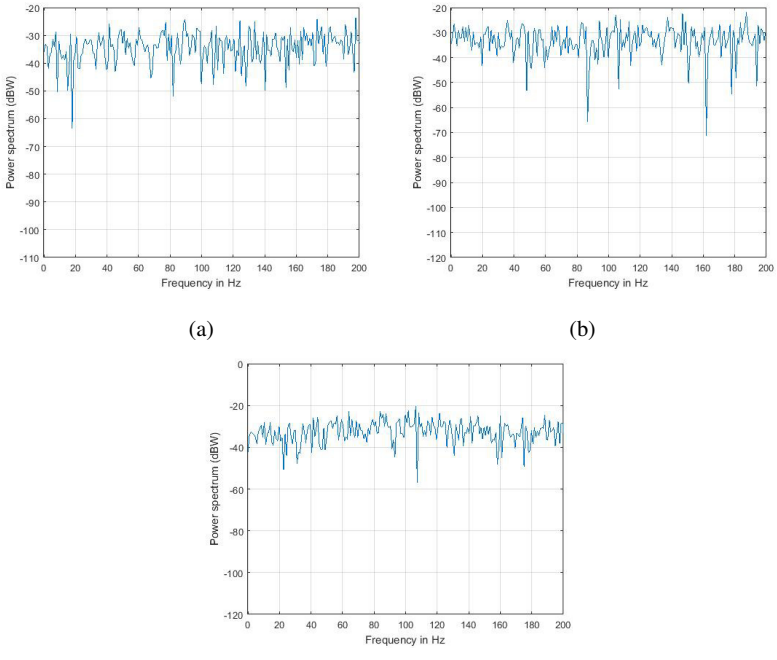


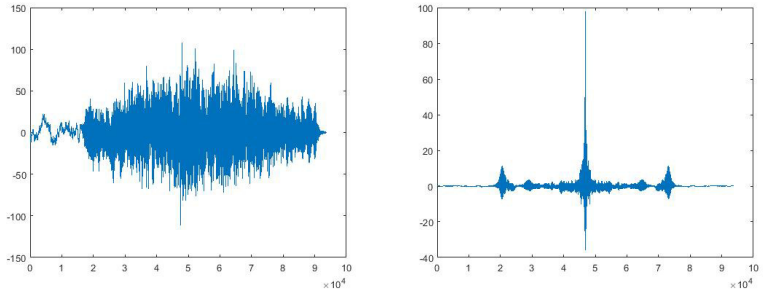
Fig. 10. Power spectrum audio signal: (a) Original (b) Encrypted (c) decrypted

5.4 Correlation Test

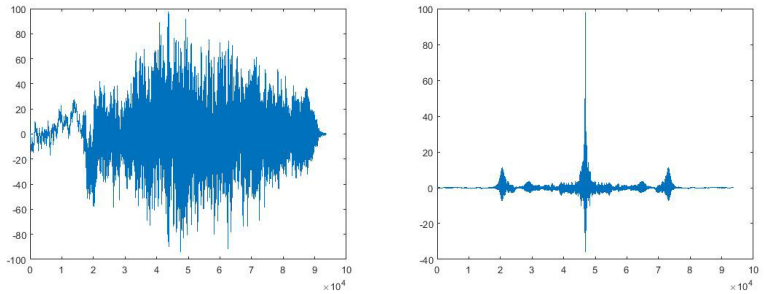
The auto-correlation function identifies the chaotic system that produces a strong encryption [20]. A usefulmeasure to assess the encryption quality of any cryptosystem is correlation coefficient between similar segmentsin the clear signal and the cipher signal. It is calculated as [20]:

$$r_{xk} = \frac{C(x,k)}{\sqrt{V(x)}\sqrt{V(k)}} \tag{6}$$

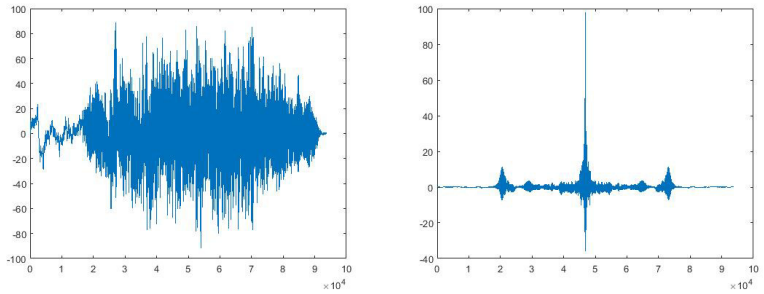
where $C(x,k)$ is the covariance between the original signal x and the encrypted signal k. $V(x)$ and $V(k)$ are thevariances of the signals x and k.



(a)



(b)



(c)

Fig. 11. Correlation audio signal : Encrypted and Decrypted(a) 4D system(b) 5D system (c) 6D system

5.5 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 [20]. 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:

$$PSNR = 10 \log \frac{nx^2}{\|x-k\|^2} \tag{7}$$

TABLE 1 PSNR COEFFICIENT FOR AUDIO DATA

	PSNR(4D)	**PSNR(5D)**	**PSNR(6D)**
Original/ Encrypted	47.0638	47.0558	47.0454
Original / Decrypted	Inf	Inf	Inf

PSNR high means: Mean square error between the original and reconstructed sigal 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 1.

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.

Speech encryption using hyperchaotic generator is a proven model. In this method, the three different dimensional hyperchaotic systems are applied. The histogram of the encrypted signal shows that more sensitivity entails more security. We have found the same histogram for the original and the decrypted audio data. The decrypted signal is very similar to the original speech as it shows the stability of reconstruction of original signal. Correlation test and PSNR testing methods are applied to estimate the performance of the system.

6. CONCLUSION

In this article, an audio signal encryption/ decryption algorithm was designed using the three proposed hyperchaotic systems. The results of the simulation showed that the encryption method offered by the audio signal was highly secure and that it could quickly recover the original signal with good audio quality. The results show that the vocal signal is highly masked by indiscreet ears. Statistical analysis using histograms, PSNR, correlation and power spectrum showed that the algorithm is powerful. From these results we will extend our studies to secure video frames as well as real-time transmissions using the 7 dimensional hyperchaotic system.

REFERENCES

[1] Bhaskar Mondal and Tarni Mandal, "A Multilevel Security Scheme using Chaos based Encryp-tion and Steganography for secure audio communication, Jharkhand.

[2] S. Lian, Y. Mao, and Z. Wang, "3D Extensions of Some 2D Chaotic Maps and Their Usage in Data Encryption," in Control and Automation, 2003. ICCA '03. Proceedings. 4th International Conference on, 2003, pp. 819-823.

[3] M. Y. Roueida , " A Cryptographic Scheme For Color Images" , M.Sc. Thesis, Iraqi Commission For Computers & Informatics, Informatics Institute For Postgraduate Studies 2006.

[4] C. Yun, Q. Runhe, F. Yuzhe , "Color Image Encryption Based On Hyper-Chaos" ,Information And Technology Department, Donghua University, Shanghai, China, pp.1-6, IEEE 2009.

[5] L. M. Pecora and T.L. Carroll, Synchronization in chaotic systems, Phys.

[6] D. López-Mancilla and 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).

[7] C. Cruz-Hernández and 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 sys-tem ap-proach, Int. J. Circuits Theory and Applications, 24, 551-579 (1996).

[9] Xiaogang Wu, Hanping Hu and Baoliang Zhang, "Analyzing and improving a chaotic encryp-tion method", Chaos, Solitons & Fractals, Vol. 22, Issue 2, pp. 367-373, October 2004.

[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"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, (2003).

[14] L. Abraham, N. Daniel, "An improved color image encryption algorithm with Pixel permutation and bit substitution" International Journal of Research in Engineering and Technology. Vol: 02, Issue: 11, Nov-2013.

[15] S. N. Lagmiri1, J. Elalami, N. Sbiti, M. Amghar, " Hyperchaos for improving the security of medical data", International Journal of Engineering & Technology, 7 (3) , June 2018 1049-1055.

[16] 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.

[17] 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.

[18] 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.

[19] L. M. Pecora and T.L. Carroll, "Synchronization in chaotic systems", Phys Rev Lett. Vol. 64, No. 8, (1990),pp: 821-824.

[20] P. Sathiyamurthi* and S. Ramakrishnan. "Speech encryption using chaotic shift keying for secured speech communication". Sathiyamurthi and Ramakrishnan EURASIP Journal on Audio, Speech, and Music Processing (2017) 2017:20.

[21] Matej Salamon (2012), "Chaotic Electronic Circuits in Cryptography", From the book Applied Cryptography and Network Security, InTech.

[22] 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.

[23] L.Keuninckx, M. C. Soriano, I. Fischer, C. R. Mirasso, R. M. Nguimdo & G. Van der Sande, "Encryption key distribution via chaos synchronization", Scientific Reports volume 7, Article number: 43428 (2017).

AUTHORS

Dr. Souad Najoua LAGMIRI received the PhD degree in Computer Science, Networks and Security from Mohammadia School Engineering, Mohamed V University in Rabat, Morocco. Her research interests include cryptographie of image, audio and video.

Pr. Hassane BAKHOUS
Consultant Engineer in Information System and Computer Project Management.
Professor and Pedagogical Manager
Higher Institute of Management Administration and Computer Engineering