International Journal of Engineering & Technology, 7 (3) (2018) 1049-1055

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET
doi: 10.14419/ijet.v7i3.11695
Research paper

Hyperchaos for improving the security of medical data

S. N. Lagmiri [1] *, J. Elalami [2], N. Sbiti [1], M. Amghar [1]

[1] Computer and Production Systems, Mohammadia School Engineering, Mohamed V University, Rabat, Morocco
[2] LASTIMI , Higher School of Technology of Sale, Mohamed V University, Rabat, Morocco
**Corresponding author E-mail: najoua.lagmiri@gmail.com*

Abstract

Because of the widespread use of medical images and signals in hospitals and healthcare communities, information security and medical data encryption are becoming more important. Cryptography has a specific role, is to protect data against unauthorized access. In this paper, we propose an efficient encryption scheme for medical data using a new hyperchaotic system applied with two algorithms: the first based on random key generation from initial conditions to encrypt a brain MRI and the second algorithm using chaotic masking technique to encrypt the heartbeat signal. The scheme achieves secure encryption and his robustness is measured by various metrics such as histogram analysis, key sensitivity, correlation coefficient and PSNR test. We conclude from the experimental results that the scheme promises stronger resistance against diverse forms of common attacks and high sensitivity to the security keys.

Keywords: *Medical Data; Encryption; Hyperchaotic System; Random Permutation; Chaotic Masking; Initial Conditions.*

1. Introduction

Until now, the sole responsibility of keeping patients records in confidence was with the Physicians. However, with the advent of recent computer technology, and it's permeation into the Medical field through E-health [2], Telemedicine [3-6], to name but a few, the challenges of confidentiality arising from the storage and transmission of medical data cannot be left to physicians alone. Telemedicine is important because it enables consultations by remote specialists, loss-free and immediate availability of individual patient information, and improved communication between partners in a health care system [7].

Indeed, transferring medical data obtained via diverse imaging technologies of computed tomography, X-ray radiology, magnetic resonance imaging, ultrasonography, etc. [1] without applying security techniques means low level of privacy for patients. Besides with modified images might result in irreversible wrong diagnostic consequences since such data do not give true reflections of patients' medical conditions [9].

However, information security imposes three mandatory characteristics: confidentiality, reliability and availability. Moreover, the security techniques must be robust enough to resist attacks of diverse forms; such as passive and active attacks; while possessing high execution speed. For example, intercepting and eavesdropping on the communication channel can be regarded as passive attack, which is an unauthorized access to the information. Contrariwise, the active attacks involve the change of the information in some way, such as, modifying the information in an unauthorized manner, alteration of authentication data, unauthorized deletion of data and denial of access to information for legitimate users.

In fact, most existing security techniques that have been used in medical imaging systems are based on the conventional encryption techniques which are not ideal for practical image encryption [5]. However, there are many encryption techniques available currently to secure the data. Traditional encryption schemes such as DES and many others do not work for multimedia data because of the large data size, high redundancy and correlation of pixels with the low resolution [4].

In order to overcome the challenges associated with data encryption, many researchers have proposed chaos based methods. The fundamental properties of a chaotic system have attracted the attention of many researchers and centers, including its ergodicity, sensitivity to initial conditions, system parameters, mixing properties, etc. These properties are very important and are needed in cryptography to obtain high quality encryption results. Chaotic systems are defined using pseudorandom sequences and created by nonlinear dynamics systems.

Our aim in this work is to improve the security of medical data. The rest of paper is organized as follows. Section 2 describes the proposed encryption schemes for image and audio data. In section 3, proposed hyperchaotic system is described. The experimental part, and discusses the corresponding results are presented in section 4. The last section concludes the paper.

2. Proposed algorithms for data encryption

Chaotic functions are sensitive to initial conditions. Slight changes in the initial conditions therefore result in massive alterations in the final outcome. Diverse chaotic maps have been used for image encryption in different schemes; in this work a four dimensional hyperchaotic system is combined with two algorithms to encrypt medical data presented thereafter.

2.1. Random permutation for image

This section introduces a chaos-based image encryption algorithm. It is based on the permutation pixel position only without changing the pixel value. First, the initial conditions for each system allow generating the output chaotic encryption sequence. Thereafter the image encryption steps are quoted. The decryption of image is done by simply reversing the process using the same key [12].

Copyright © 2018 S. N. Lagmiri et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

This encryption algorithm contains five steps:
Step 1: Load the original image I [M, N];
Step 2: Initializing the hyperchaotic system;
Step 3: Generating the chaotic sequences at length of M*N, then starts to generate the chaotic sequences for image encryption;
Step 4: Calculating the new index pixel position based on key sequence;
Step 5: Permute the pixel positions on the original image then gat the encrypted one;

2.2. Chaotic masking for audio signal

In this section, a cryptosystem based on synchronized chaotic systems is described. The aim is to transmit encrypted audio signal from transmitter A to remote receiver B as is depicted in Figure 1. An audio signal m is to be transmitted over an insecure communication channel [14].

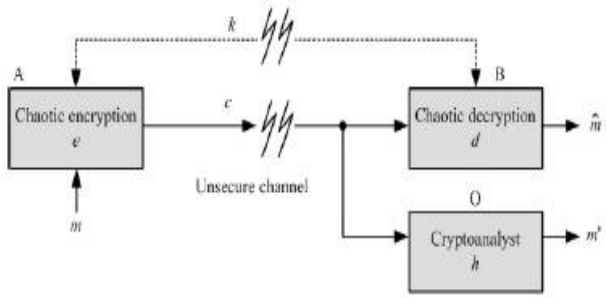


Fig. 1: Chaotic Cryptosystem for Audio Communication.

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

$$c = e(m, k) \tag{1}$$

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:

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

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.

3. New hyperchaotic system

In the part of the chaotic sequence generator, the system is used to generate the output chaotic sequence. In our case, the function in Eqn. (3) represents the novel four dimensional hyperchaotic system utilizes as an encryption chaotic sequence generator.

$$\begin{cases} \dot{x}_1 = -ax_1 + ax_2 \\ \dot{x}_2 = bx_1 - x_1x_3 \\ \dot{x}_3 = -cx_3 + hx_1x_4 \\ \dot{x}_4 = -ax_4 + ax_2 \end{cases} \tag{3}$$

When $a = 10, b = 20, c = 0.5$ and $h = 1$ the system (3) is hyperchaotic.

3.1. 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. The two time series stay close together, but after eight iterations, they are diverging [11].

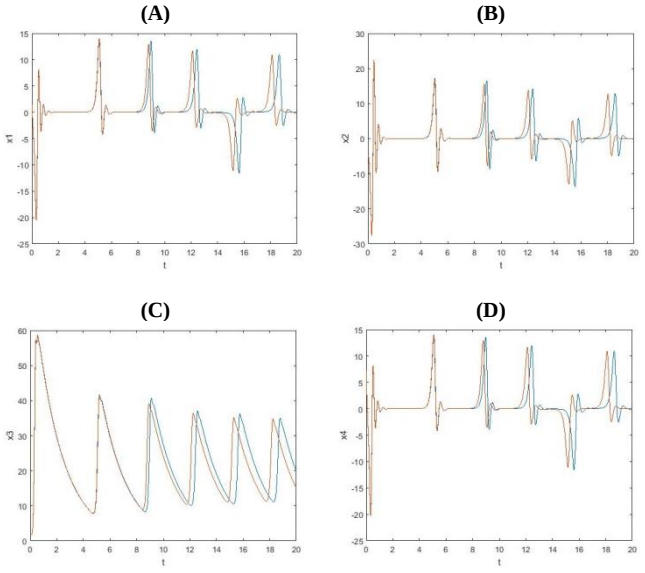


Fig. 2: Sensitivity to Two Initial Conditions [1 -5 2 7] and [1.5 -5.5 1.8 7.2]: (A): x_1 (B): x_2 (C): x_3 (D): x_4.

4. Simulation results and security analysis

A secure encryption algorithm should be robust against all types of attacks such as cryptanalytic, statistical and brute force attacks. Here we discuss the security analysis of the proposed algorithms by addressing key sensitivity analysis, statistical analysis and differential analysis. The resistance against different types of attack is useful measure for the performance of a cryptosystem.
Some security analysis results are incorporated in the following sections to establish the strength of our proposed scheme.

4.1. Image analyzing methods

To demonstrate the strength of our proposed scheme, the encryption and decryption algorithms are implemented in MATLAB for a brain MRI of size 256x256. The simulation results of the proposed algorithm shows good performances in image encryption.
The initial conditions for the 4D hyperchaotic system given in (3) are $x_0 = [1; 2; 5; -4]$. The encrypted image in Figure 3(b) is completely different from the original image and cannot be recognized. The decrypted image in Figure 3 (c), getting from the decryption process, is the same as the original image in Figure 3 (a). This figure shows the success of the encryption and decryption algorithm for the medical image.

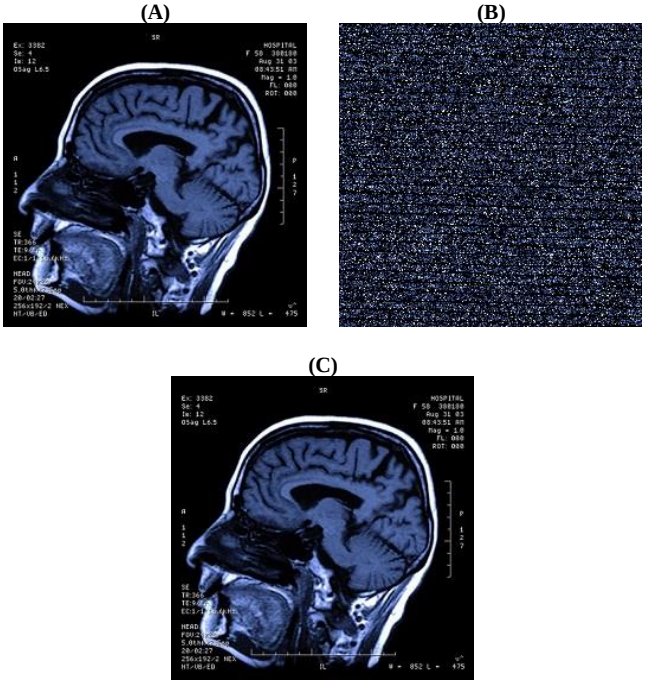


Fig. 3: (A) Original Image, (B) Encrypted Image, (C) Decrypted Image with the Same Key.

4.1.1. Statistical analysis

To improve the performance of the proposed encryption algorithm, we present in this section some security analysis including statistical analysis (histogram, PSNR and correlation) and differential analysis (UACI and NPCR). Finally, we present the robust encryption algorithm against a type of cryptanalysis which is the known plaintext attack.

4.1.2. Histogram analysis

An efficient encryption scheme should have a uniform histogram in order to make it impossible for an attacker to extract any meaningful information from the histogram since the histogram's distribution reveals the pixel value distribution within the image [4]. Mathematically, the histogram is a discrete function and its grey levels are in the range [0, L - 1] as in the following equation [10]:

$$hist(r_k) = \frac{n_k}{N}$$

Where r_k is the kth grey level, and n_k is the number of pixels in the image with that grey level. N is the total number of pixels in the image. It may be noted that $k = 0, 1, \ldots, L-1$.
The histogram of an image shows the number of occurrences for each grey level in the medical image. So having a narrow histogram of the image means that the image is poorly visible, because the difference in grey levels presents in the image is generally low [16]. In the same way, a widely distributed histogram means that almost all the grey levels are present in the image, and thus the overall contrast and visibility increases.
In Figure 4(a), a histogram of the original brain MRI image is given, while Figure 4(b) presents a histogram of the encrypted image. The experiment results show that the histogram of the encrypted brain MRI is fairly different from the original one.

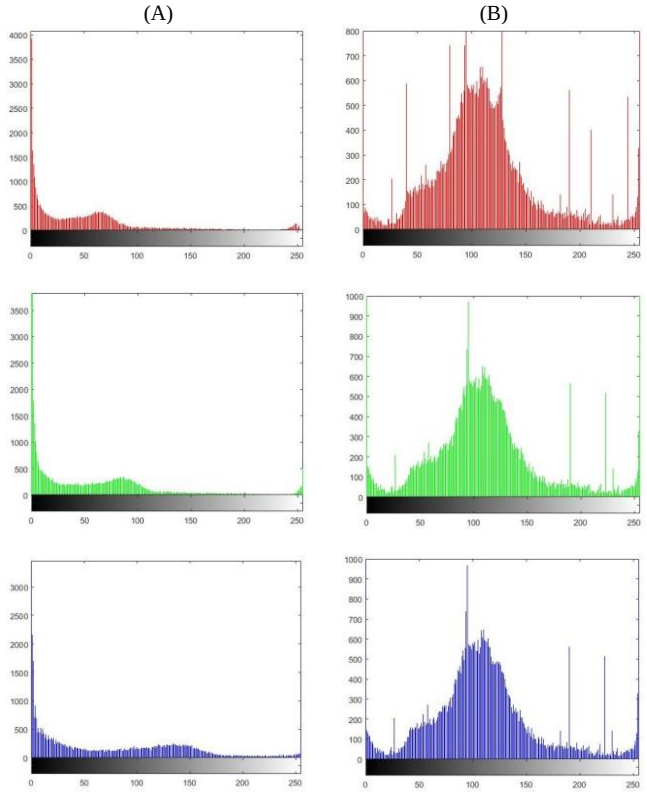


Fig. 4: (A) Original and (B) Encrypted Image Histogram of Three Channels RGB.

4.1.3. Correlation of two adjacent pixels

The correlation coefficients of adjacent pixels of an image give information about the image. High correlation coefficients of adjacent pixels are evidence that, information can be extracted from the image. It is therefore necessary that correlation coefficients of adjacent pixels in cipher images are very low. In images, the horizontal, vertical, diagonal and anti-diagonal correlations between pixels are high. Cipher images must reduce these relationships among the adjacent pixels. The correlation coefficients among adjacent pixels are calculated with (4), (5), (6) and (7) [18]

$$E(x) = \frac{1}{N}\sum_{i=1}^{N} x_i \tag{4}$$

$$D(x) = \frac{1}{N}\sum_{i=1}^{N}(x_i - E(x))^2 \tag{5}$$

$$cov(x,y) = \frac{1}{\mathrm{N}}\sum_{\mathrm{i}=1}^{\mathrm{N}}(\mathrm{x_i} - \mathrm{E(x)})(\mathrm{y_i} - \mathrm{E(y)}) \tag{6}$$

$$\mathrm{r_k} = \frac{\mathrm{cov(x,y)}}{\sqrt{\mathrm{D(x)} \times \sqrt{\mathrm{D(y)}}}} \tag{7}$$

Where x and y are the grayscale values of two adjacent pixels of the image, (x) is the variance, $cov\ (x, y)$ is the covariance and (x) is the mean. We randomly selected 3000 pairs of adjacent pixels from both original and encrypted images and calculated their horizontal, vertical, diagonal and anti-diagonal correlation coefficients. The results of the correlation coefficients of adjacent pixels for the original image, encrypted and decrypted one show that there is very good correlation between adjacent pixels in the image data [13], [15], while there is only a small correlation between adjacent

pixels in the encrypted image. Table 1 shows the Correlation coefficient comparing to another encryption system define in [21].

Table 1: Correlation Coefficient for Brain MRI Image Comparison

		Horizontal	Vertical	Diagonal	Anti-diagonal
Encrypted image	Current work	-0.0004	-0.0017	0.0025	0.0003
	Ref [21]	-0.0027	-0.0077	-0.0038	0.0013
Decrypted image	Current work	0.9955	0.9973	0.9933	0.9933
	Ref [21]	0.9955	0.9973	0.9933	0.9933

4.1.4. PSNR analysis

Fidelity refers to the amount of distortion produced in the original cover image due to embedding. The effects of embedding can be evaluated in terms of Peak-Signal-to-Noise Ratio (PSNR). This section evaluates the PSNR value of the original image and the encrypted that is revealed at the end using the formula [17]:

$$MSE = \frac{1}{mn}\sum_{i=0}^{m-1}\sum_{j=0}^{n-1}[I(i,j) - K(i,j)]^2 \quad (8)$$

Where "I" is a noise free image of size (m x n) and K is the noisy share. The PSNR is defined as:

$$PSNR = 10\,log_{10}(\frac{MAX^2}{MSE)}) \quad (9)$$

Where $\mathrm{MAX} = 255$ when pixels are represented using 8-bit representation. For binary images $\mathrm{MAX} = 1$. Higher the PSNR value better is the fidelity and hence, lower distortion of the image.

Table 2: PSNR Coefficient for Medical Image

	PSNR (1)	PSNR (2)	PSNR (3)
Encrypted	16.4815	15.7102	13.7296
Decrypted with same key	Inf	Inf	Inf
Decrypted with added noise	31.1942	Inf	Inf
Decrypted with key error	17.6093	16.7562	14.6495

High PSNR means: Mean Square Error (MSE) between the original image and reconstructed image is very low. It implies that the image been properly restored. In the other way, the restored image 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 image and encrypted image is very high. It implies that the image 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 image are identical. The value of PSNR means that the decrypted image is identical to original image.
- The correlation coefficients for the original and encrypted image are very different. The PSNR (Original/Encrypted) means that the encrypted image is totally different of the original image.

4.1.5. NPCR and UACI analysis

Sensitivity of a cipher image to slight changes in plain image is one way to measure the resistance of image encryption algorithms to differential cryptanalysis. The two metrics used are the NPCR and UACI which are defined as:

$$\mathrm{NPCR} = \frac{1}{\mathrm{M}\times\mathrm{N}}\left(\sum_{\mathrm{i,j}} \mathrm{D(i,j)}\right) \times 100\% \quad (10)$$

$$\mathrm{D(i,j)} = \begin{cases} 0 & \mathrm{C_1(i,j) = C_2(i,j)} \\ 1 & \mathrm{C_1(i,j) \neq C_2(i,j)} \end{cases} \quad (11)$$

$$\mathrm{UACI_{R,G,B}} = \frac{1}{\mathrm{M}\times\mathrm{N}}\left[\sum_{\mathrm{i,j}} \left|\frac{\mathrm{C_1(i,j) - C_2(i,j)}}{255}\right|\right] \times 100\% \quad (12)$$

Where $\mathrm{C_1}$ and $\mathrm{C_2}$ are two encrypted images which have one pixel difference in their corresponding plain images. $\mathrm{C_2(i,j)}$ is their pixel values and *M* and *N* represent their dimensions. An attacker would inverse a pixel in the plain image and observes the corresponding change in the cipher image. If the changes in the plain image do not lead to non-uniform changes in the cipher image, the differential attack fails [8], [19], [20]. The results of our experiment are shown in Table II. It is obvious our scheme is resistant to differential attacks.
The NPCR and UACI of the plain image shown in Figure 4(a) are calculated and presented in Table 3. The objective of this analysis is to show that a small change in the image clearly introduces a major change in encrypted the image.

Table 3: NPCR and UACI result

	NPCR %	UACI %
Brain MRI	0.9960	0.3346

Given the results found after our test (NPCR over 99% and the UACI is over 33%), we can conclude that our proposed method is resistant to differential attacks.

4.1.6. Error decrypted image

To recover our image, we apply the inverse of the algorithm proposed in section 2.1. For a good decryption, we used the same key as the encryption. The result is already shown in section 4.1. But in the practical case, we find situation where the encrypted image will be attacked. In this part of work we present two cases.

a) Cannel attack: white noise

In practice, the transmission of information is done through the channel with noise. So to analysis the performance of our algorithm and our hyperchaotic system, we have added a white noise to the encrypted image, then we have decrypted it with the same key in the encryption step. The results are shown in figure 5.

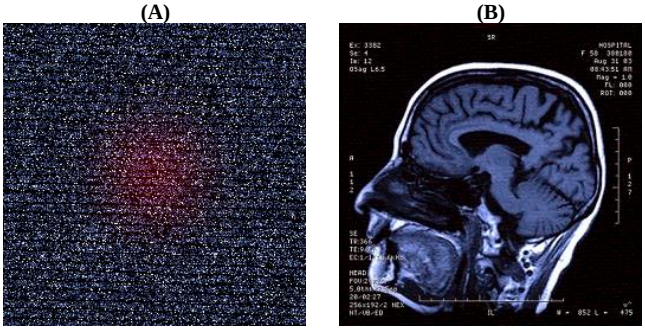


Fig. 5: (A) Encrypted Image with Added White Noise, (B) Corresponding Decrypted Image.

We observe that the decrypted image is the same as the original one. That means the algorithm is robust against the white noise, that is confirmed by the PSNR value equal to Inf in section 4.1.4.

b) Key analysis

The Key analysis metrics: key space analysis and key sensitivity test are used to measure the strength of encryption algorithms.

Key sensitivity ensures that partial guesses of the key aimed at decrypting the cipher image fail. With the incorrect keys, the guessed key should not provide any pattern of information in the wrongly decrypted image. This means that if two different keys are used to encrypt the same plain image, the resulting cipher images must be different. We made slight changes (10^{-5}) in the seed keys for decrypting the same cipher image. In Figure 6, it is evident that if the wrong key is applied to decrypt the image, the resulting image still different of the original image.
This result confirms performance of our algorithm using hyperchaotic system sensitive to initial conditions.

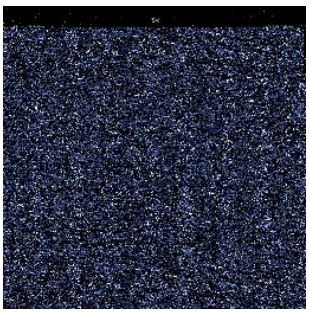


Fig. 6: Decrypted Image with 4D and $x_0 = [1.00001; 2; 5; -4]$

4.1.7. Processing time

Processing time for encryption and decryption is also an important issue in real-time multimedia applications. To estimate the execution time of the proposed encryption scheme, different tests are performed. Tests results of encryption time and decryption time are shown in Table 4. We conclude from the results of input image that the proposed encryption system is of high-speed and flexible for various applications.

Table 4: Time Encryption and Decryption Comparison

		Encryption	Decryption	Decryption with noise	Decryption with key error
Time	**Current work**	0.5467	0.4976	0.5293	0.5121
	Ref [21]	2.0481	1.9420	2.9685	1.7161

4.2. Audio signal encryption results

In this section, we perform some statistical analysis to ensure that the proposed encryption scheme is resistant to different kinds of attacks. In fact, the encrypted signal remains secured under the process of data transmission because the key space, which is based on the initial conditions of the four dimensional hyperchaotic system and the parameters a, b, c and h, has been chosen to be large enough. The security analysis comprising the histogram, the power spectrum, the correlation and the key sensitivity analysis. To this end, we consider a digital audio file (.wav format) as in Figure 7(a). The audio signal m(t) is a heartbeat of frequency 94.019 KHz and 8.5278 second duration. The mentioned audio signal is to be encrypted and transmitted to the receiver.
We use as transmitter and receiver the hyperchaotic system given in (3) for initial conditions $x_0 = [0, 1, 0, 1]$.
Figure 7 shows results of the heartbeat encryption process through our four hyperchaotic system. Original audio signal 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 8 shows the histogram for encrypted (a), decrypted (b) and recovered (c) audio signal. In figure 9, the power spectrum of $m(t), c(t)$ and $\hat{m}(t)$ is presented. And figure 10 shows the correlation coefficient.

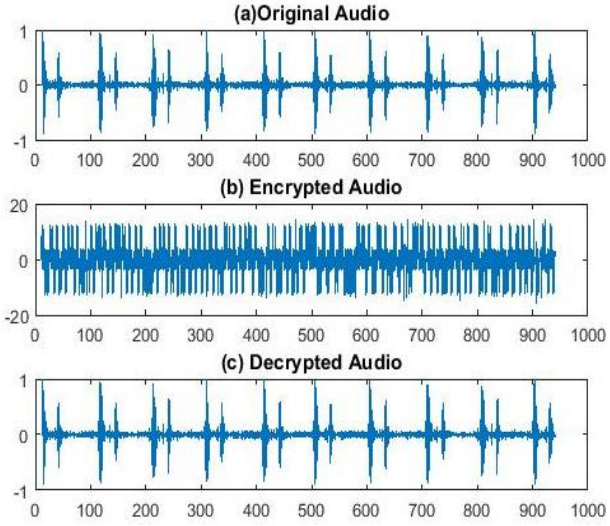


Fig. 7: Encrypted/Decrypted Heartbeat Signal.

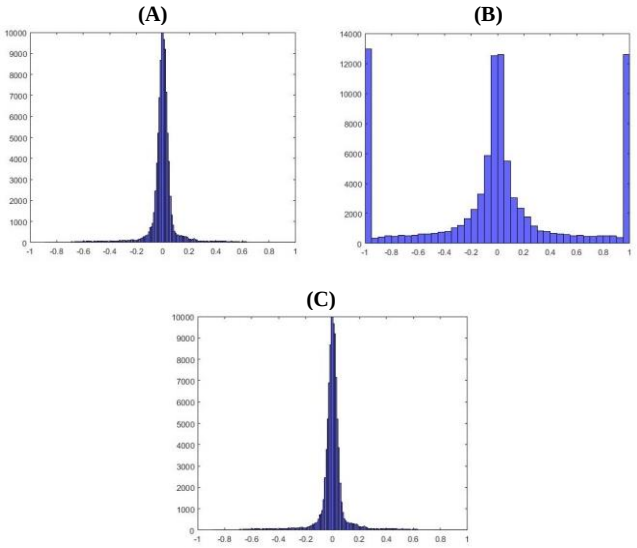


Fig. 8: Histogram of Heartbeat (A) Original (B) Encrypted (C) Decrypted.

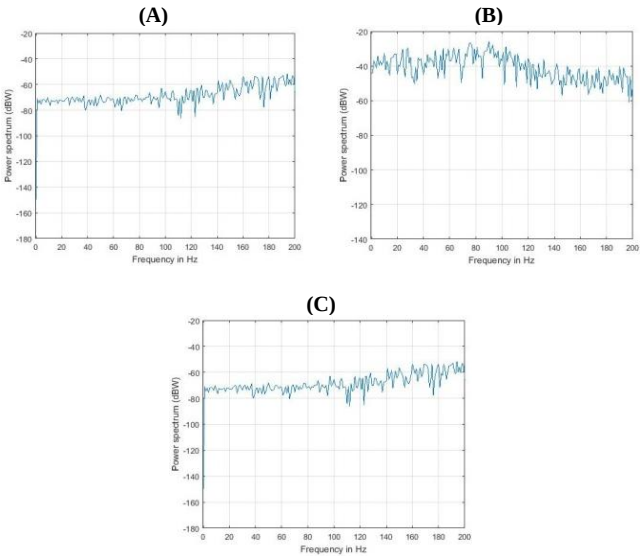


Fig. 9: Power Spectrum Audio Communication (A) Original (B) Encrypted (C) Decrypted.

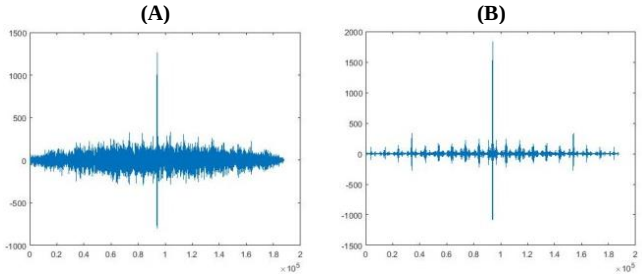


Fig. 10: Correlation Audio Communication (A) Original/Encrypted Image. (B) Original/Decrypted Image.

Table 5: Time of Encryption and Decryption of Heartbeat Signal

	Encryption	Decryption
Time	0.1372	0.1326

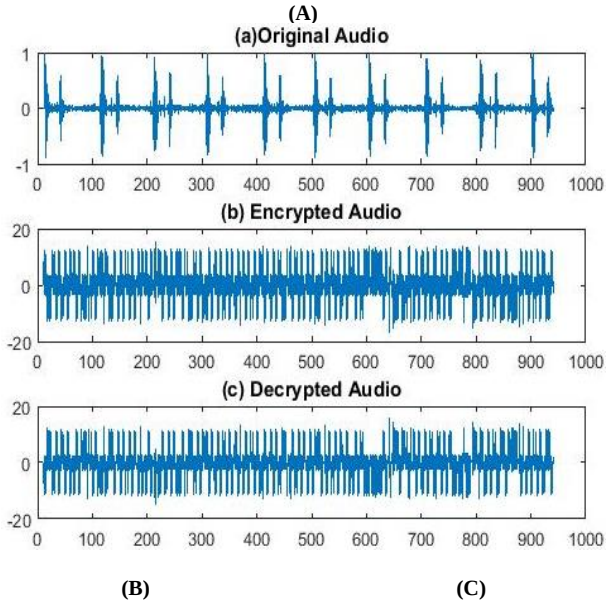
Tests results of encryption time and decryption time are shown in Table 5. The results show that the proposed encryption system is of high-speed heartbeat encryption using hyperchaotic generator is a proven model. In this method, the four dimensional hyperchaotic system is applied. The histogram of the encrypted signal shows that more sensitivity entails more security. We have found the same histogram for the original and the decrypted image. The decrypted signal is very similar to the original heartbeat as it shows the stability of reconstruction of original signal.

- Security analysis

For testing the sensitivity of the proposed cryptosystem, the encrypted signal is decrypted with the reverse process of encryption method using the four hyperchaotic system by modifying the initial conditions of the system (3) with 10^{-9} as $x_{02} = [1, 0, 1, 0.000000001]$.

The decrypted signal is totally wrong, as shown in figure 11 (a) (bottom). The corresponding histogram in figure 11(b), cross-correlation (c) and power spectrum (d) prove that the decrypted signals are totally different from the original ones.

It is shown that even a small change of the key development can not help recover the original audio file, i.e., the encryption is free from any brute force attack.



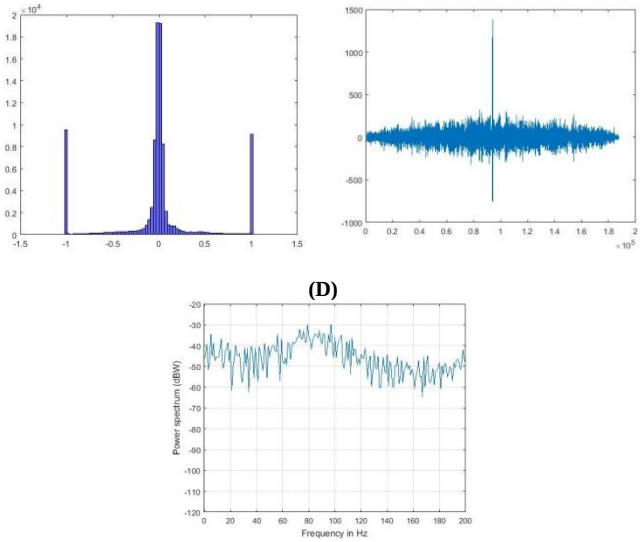


Fig. 11: Decrypted Audio Signals With $x_{02} = [1, 0, 1, 0.000000001]$.

5. Conclusion

Security becomes more important as the performance of computers increases. Devise a secure algorithm to protect medical data is complicated because of the special concerns of the medical community. First, for medical images the algorithm must recover the exact image with no change in any pixel value. Second, the algorithm should have a short processing time with high security that can stand for a long time.

In this paper, two algorithms for medical image and heartbeat signal encryption were designed utilizing the new four dimentional hyperchaotic system. The results obtained by the proposed system are highly screened from attackers. The simulation results showed that the image algorithm was capable of achieving in terms of encryption and decryption process. The proposed scheme provides sensitivity to very small change in the initial conditions (10-5). The security analysis shows that the proposed system has good security and complexity. It is observed that image encryption using this technique given good results.

Also, it is verified that the heartbeat signal proposed encryption method has high level of security and can recover the original signal quickly with high audio quality. The results endorse that the heartbeat signal is highly masked from eavesdroppers.

References

[1] M. Y. M. Parvees, J. A. Samath, and B. P. Bose, “Secured Medical Images-a Chaotic Pixel Scrambling Approach,” *J. Med. Syst.*, Vol. 40, No. 11, (2016), pp: 232. https://doi.org/10.1007/s10916-016-0611-5.

[2] "National E-Health Transition Authority: About Us". National E-Health Transition Authority. (2013). Retrieved 2013-23-09.

[3] Berman. M; Fenaughty. A,"Technology and managed care: patient benefits of telemedicine in a rural health care network", Health Economics, Vol. 14, No. 6. Wiley. (June 2005), pp: 559-573, https://doi.org/10.1002/hec.952.

[4] Joshua C. Dagadu, Jianping Li, Emelia O. Aboagye, Xuedzi Ge, “Chaotic Medical Image Encryption Based on Arnold Transformation and Pseudorandomly Enhanced Logistic Map”, Journal of Multidisciplinary Engineering Science and Technology, Vol. 4 Issue 9, September 2017, pp: 8096-8103.

[5] Al-Husainy. M. A. F, “A novel encryption method for image security,” Int. J. Secur. Its Appl., Vol. 6, No. 1, (2012).

[6] Conde, Jose G.; De, Suvranu; Hall, Richard W.; Johansen, Edward; Meglan, Dwight; Peng, Grace C. Y, "Telehealth Innovations in Health Education and Training". Telemedicine and e-Health, vol. 16, No.1, (January/February2010), pp: 103- 106, https://doi.org/10.1089/tmj.2009.0152.

[7] Yu-zeng. W, Shi-chao. G, Yu-jun. F, and Zhi- quan. F., “Research the Compression and Transmis- sion Technology of Medical Image

Base on the Remote Consultation," in The 2nd International Conference on Bioinformatics and Biomedical En- gineering (ICBBE), Shanghai, China, (2008), pp. 2142–2145.

[8] Enayatifar. R, Sadaei. H. J, Abdullah; A. H, Lee. M, and Isnin. I. F, "A novel chaotic based image encryption using a hybrid model of deoxyribonucleic acid and cellular automata," Opt. Lasers Eng., vol. 71, (2015), pp: 33- 41. https://doi.org/10.1016/j.optlaseng.2015.03.007.

[9] Omala. A. A, Robert. N, and Li. F, "A provably-secure transmission scheme for wireless body area networks," J. Med. Syst., vol. 40, No. 11, (2016), pp: 247. https://doi.org/10.1007/s10916-016-0615-1.

[10] Laurence E. Sigler (trans.). Fibonacci's Liber Abaci. Springer-Verlag. (2002), pp: 402 - 403.

[11] Lagmiri. S. N, Elalami. N, Elalami. J, "Three Dimensional Chaotic System for Color Image Scrambling Algorithm". International Journal of Computer Science and Information Security (IJCSIS), Vol. 16, No. 1, (January 2018), pp: 8-20.

[12] Lagmiri. S. N, Elalami. N, Elalami. J, "Color and gray images encryption algorithm using chaotic systems of different dimensions". IJCSNS International Journal of Computer Science and Network Security, Vol.18 No.1, (January 2018), pp: 79-86.

[13] Gámez-Guzmán. L, Cruz-Hernández. C, López-Gutiérrez. R.M, and García-Guerrero. E.E, "Synchronization of Chua's circuits with multiscroll attractors: Application to communication", Commun. Nonlinear Sci. Numer. Simulat. Vol. 14, (2009), pp: 2765–2775. https://doi.org/10.1016/j.cnsns.2008.10.009.

[14] Lagmiri. S. N, Elalami. N, Elalami. J, "Encryption & Decryption Audio Communications in Mobile Networks based on a New Hyperchaotic System". London Journal of Research in Computer Science and Technology Volume 18,| Issue 1, (April 2018).

[15] Lagmiri. S. N, Elalami. N, Elalami. J, "Novel Chaotic System for Color Image Encryption Using Random Permutation". International Journal of Computer Networks and Communications Security, Vol. 6, No. 1, (January 2018), pp: 9–16.

[16] Mao. Y and Chen. G, "Chaos-based image encryption," Handbook of Geometric Computing, (2005), pp: 231–265. https://doi.org/10.1007/3-540-28247-5_8.

[17] Abraham. L, Daniel. N, "An improved color image encryption algorithm with Pixel permutation and bit substitution" International Journal of Research in Engineering and Technology. Vol. 2, Issue: 11, (Nov-2013).

[18] El-Alfy. E.-S. M, Thampi. S. M, Takagi. H, Piramuthu. S, and Hanne. T, Advances in Intelligent Informatics. Springer, (2015).

[19] Enayatifar. R, Abdullah. A. H, and Isnin. I. F, "Chaos-based image encryption using a hybrid genetic algorithm and a DNA sequence," Opt. Lasers Eng., vol. 56, (2014), pp : 83–93.

[20] Enayatifar. R., Abdullah. A. H, and Lee. M, "A weighted discrete imperialist competitive algorithm (WDICA) combined with chaotic map for image encryption," Opt. Lasers Eng., vol. 51, no. 9, (2013), pp: 1066–1077. https://doi.org/10.1016/j.optlaseng.2013.03.010.

[21] Lagmiri. S. N, Elalami. N, Elalami. J, "A Multimedia Encryption Algorithm based on Hyperchaotic Systems". The 1st International Conference on Networking, Information Systems & Security, April 27-28, 2018, Tangier, Morocco.