




A Six-Dimensional Hyperchaotic Pseudorandom Sequence for Enhanced Voice Encryption

Enas Hamza Haseeb^{1*}, Sana Ahmed Kadhim², Ali Shakir Mahmood¹

¹ Computer Science Department, College of Education, University of Almustansirya, Baghdad 00964, Iraq

² Department of Bioinformatics, University of Information Technology and Communication, Baghdad 00964, Iraq

Corresponding Author Email: ann12naa@gmail.com



<https://doi.org/10.18280/isi.280425>

ABSTRACT

Received: 10 April 2023

Revised: 16 June 2023

Accepted: 10 July 2023

Available online: 31 August 2023

Keywords:

voice encryption, hyperchaotic system, pseudo-random number sequence, Libri-Speech dataset, performance evaluation, speech security.

Over recent decades, the demand for robust voice encryption algorithms has escalated to fortify the security of speech transmission over vulnerable channels such as the internet. Among the myriad of available methodologies, those underpinned by chaos theory have garnered significant attention due to their inherent pseudorandomness, acute sensitivity to initial conditions, and control parameters. These attributes render them capable of encrypting a variety of data types, encompassing but not limited to videos, images, and audio. This study presents a novel voice encryption approach predicated on a six-dimensional (6D) hyperchaotic system. In the proposed method, six unique keys are generated from the 6D hyperchaotic system. The initial three keys are employed to permute the human voice signal, while the subsequent trio is engaged in the diffusion process. The efficacy of this scheme is evaluated on several parameters: Mean Square Error (MSE), Signal-To-Noise Ratio (SNR), correlation coefficient, Peak Signal-To-Noise Ratio (PSNR), key sensitivity, key space, and entropy analysis. The Libri-Speech dataset serves as the test bench for the proposed system. The key space has been determined to be 2465. The system's performance is notable, with correlation coefficients ranging between -0.00276 and 0.002759, entropy values from 14.74399 to 14.74942, PSNR values from 4.2814 to 4.7875, SNR values from -30.3854 to -9.2364, and a nearly zero MSE range of 0.3321 to 0.3731 between original and extracted signals. This study underscores the potential of the 6D hyperchaotic system in enhancing information security, specifically for voice encryption. The findings may pave the way for more secure communication protocols in an increasingly interconnected digital world.

1. INTRODUCTION

The burgeoning exchange of multimedia data via open networks and the internet necessitates robust and reliable security measures to ensure confidentiality and prevent unauthorized access. Among various solutions, data encryption [1] has emerged as a key approach, where data is manipulated to render it unreadable, invisible, or impenetrable during transmission via encryption algorithms. As such, the importance of data encryption has been underscored in numerous applications, and several schemes have been developed to enhance the security and confidentiality of sensitive data [2].

However, despite the merits and demerits inherent in each standard encryption technique, a prevailing challenge lies in the distribution of encryption keys. Certain intrinsic characteristics of multimedia data, particularly voice, render traditional cryptographic algorithms unsuitable for protecting content from test messages, given the distinct encryption and decryption processes for voice and the issue of data redundancy [3]. In response, chaotic cryptography, known for its sensitivity and extensive key range, offers an innovative solution [4].

Chaotic cryptography, or nonlinear dynamic system cryptography, is unpredictable over extended periods and highly sensitive to initial conditions. This field of cryptography has breathed new life into speech encryption

systems with the application of chaotic maps [5, 6]. Its desirable characteristics such as nonlinearity, determinism, sensitivity to initial conditions, aperiodicity, and irregular behaviors (i.e., random-like performance) have attracted substantial attention from the research community in recent years [7, 8].

Several notable algorithms have been proposed to enhance speech encryption over unsecured channels. Parvees et al. [9] proposed a speech byte scrambling method utilizing several chaotic maps, with a key space of 10,512 and other metrics such as NBCR, UACI, MSE, and PSNR. Farsana et al. [10] introduced a model based on audio permutation using a discrete modified Henon map and a key stream produced by the modified Lorenz-Hyper chaotic model for the substitution operation, resulting in metrics such as SNR, NPCR, UACI, and CC. Hassan et al. [11] proposed a cryptography algorithm for digital voice file encryption using two chaotic maps (the Henon and gingerbread chaotic maps) with results such as MAE, MSE, PSNR, SNR, Correlation Measure, and encryption and decryption times. Mokhnache et al. [12] presented a voice encryption model combining modified chaotic maps inspired by cubic and classic logistic maps, with a key space of 2180 and metrics such as SNR and CC.

This paper proposes a novel approach based on a six-dimensional (6D) hyperchaotic system for voice encryption and decryption. It starts with the generation of six keys from the system, followed by the transformation of a 1D

uncompressed 16-bit voice file into a wavelet domain using Discrete Wavelet Transform. The voice signal blocks are then permuted using the first three keys for bit permutation in the block, followed by the use of the remaining three keys in the diffusion process.

The paper is organized as follows: Section 2 elucidates the system description, Section 3 presents the proposed human voice encryption algorithm, Section 4 illustrates the results, and Section 5 concludes the study.

2. SYSTEM DESCRIPTION

2.1 Proposed 6D hyperchaotic system

Low control parameters in conventional chaotic maps result in a confined chaotic range. On the other hand, higher dimensional maps, like the ones presented, can be utilized to expand the key space, add excessive complexity, and boost the pseudo-series randomness. Here is an analysis of the properties of the proposed 6D hyper chaotic system.

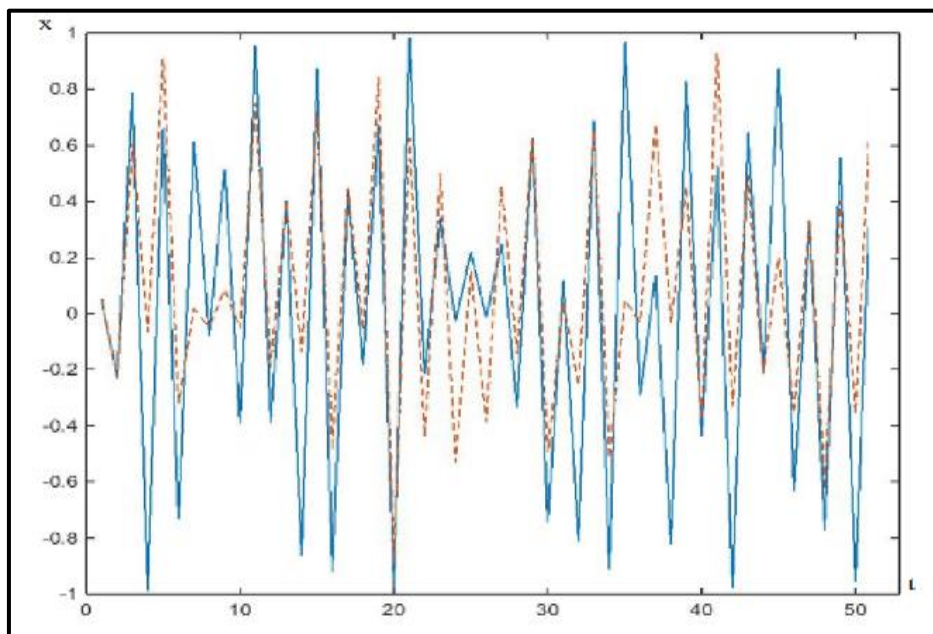
The proposed maps, in short, exhibit appealing qualities, including high sensitivity to changes in ergodicity, initial conditions, extended periodicity, and random behaviour. These characteristics are similar to the requirements for effective encryption techniques. Moreover, the suggested 6D hyper chaotic system maintains the simple structure of the classical maps in its parameter variety. In this paper, we used a set of nonlinear dynamical equations with the following mathematical definition of a 6D hyper chaotic system:

$$\begin{aligned}
 \frac{dx}{dt} &= a * (y - x) \\
 \frac{dy}{dt} &= b * (x - x * z) \\
 \frac{dz}{dt} &= c * z - d * x \\
 \frac{dw}{dt} &= a * (w + x) \\
 \frac{dv}{dt} &= -w * s + b * w + a * y - a * v \\
 \frac{ds}{dt} &= a * (x - c * s)
 \end{aligned}
 \tag{1}$$

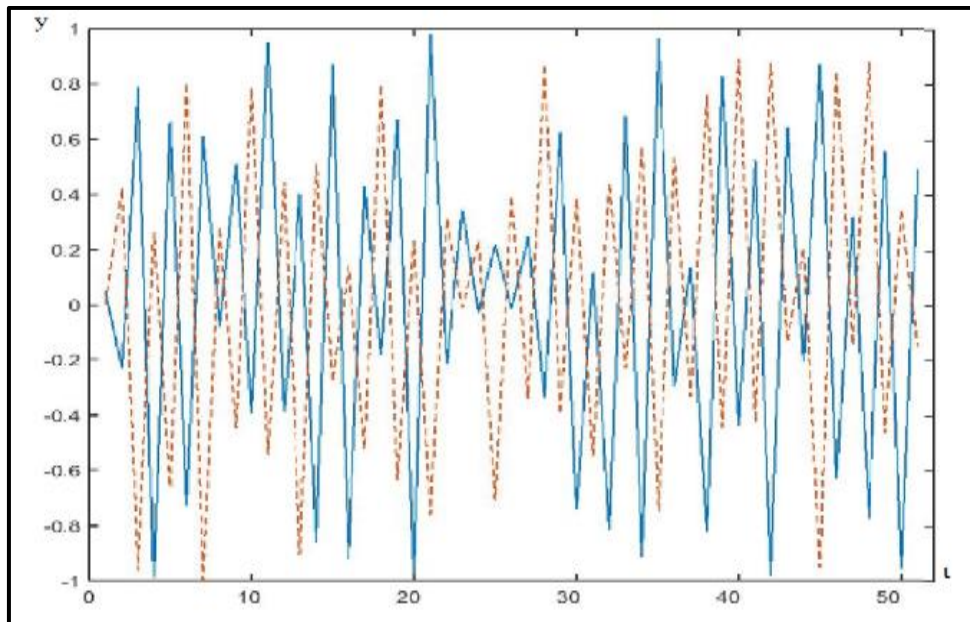
where, s, v, w, z, y, x and $t \in R^+$ known as the system states and $c, b, a,$ and d are system parameters. The R^+ indicates positive real numbers. When initial points $(X(0), Y(0), Z(0), W(0), V(0), S(0)) = (3.6, -1.2, 3.4, 0, 2.1, 1.5)$, the parameters are selected as $a=1.3, b=1.4, c=2.5,$ and $d=1.3$. The Lyapunov exponents signs are $(+, +, +, -, -, -)$. Hence system (1) demonstrated hyper chaotic states. The equilibrium points $E_0(0, 0, 0, 0, 0, 0), E_1(1.92307, 1.92307, 1.0, -1.92307, 0.98998, 0.76923)$. These are the eigenvalues that are derived for equilibrium $E_0(0, 0, 0, 0, 0, 0)$: $\lambda_1=-3.25, \lambda_2=-1.3, \lambda_3=1.3, \lambda_4=2.5, \lambda_5=-2.15,$ and $\lambda_6=0.85$. Because of this, the equilibrium $E_0(0, 0, 0, 0, 0, 0)$ is a saddle point. Hence, at point E_0 , the hyper chaotic system is unstable. It is equally simple to demonstrate that both the equilibrium point E_1 and the saddle points are unstable. The eigenvalues are: $\lambda_1=2.88, \lambda_2=1.3, \lambda_3=-0.839+0.936i, \lambda_4=-0.839-0.936i, \lambda_5=-1.3,$ and $\lambda_6=-3.25$. Where i denote the unit of imaginary number. For the equilibrium point E_1 , the results show that $\lambda_1, \lambda_2, \lambda_5$ and λ_6 are positive and negative real numbers, λ_3 and λ_4 become a pair of complex conjugate eigenvalues with negative real parts. These equilibrium points are unstable because equilibrium point E_1 is a saddle-focus point.

2.2 Sensitivity of initial conditions

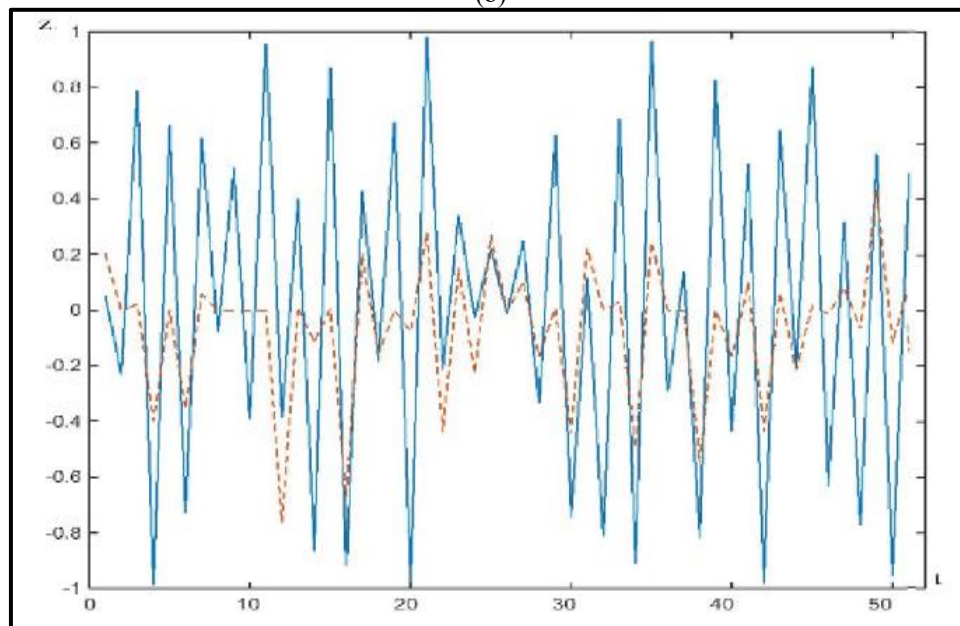
Chaos is particularly sensitive to perturbations. The butterfly effect, made popular by Edward Lorenz, was an example of this principle [13]. Unpredictability and sensitivity to the initial conditions characterize chaotic dynamical systems. Due to this, no matter how close two trajectories of initially neighboring phases were to one another, they diverged more quickly. By giving the suggested combined system two extremely similar initial conditions, it is possible to simulate the effects of the sensitivity to the initial conditions. Figure 1 (from a to f) illustrates how the two systems first develop similarly before beginning to behave differently. The system initial values are set to: $X_0=3.6, Y_0=-1.2, Z_0=3.4, W_0=0, V_0=1.5$ and $S_0=2.1$ for the solid line and $X_0=3.0000000000000006, Y_0=-1.2, Z_0=3.4, W_0=0, V_0=1.5$ and $S_0=2.1$ for the dashed line. Figure 1 illustrates test of sensitivity.



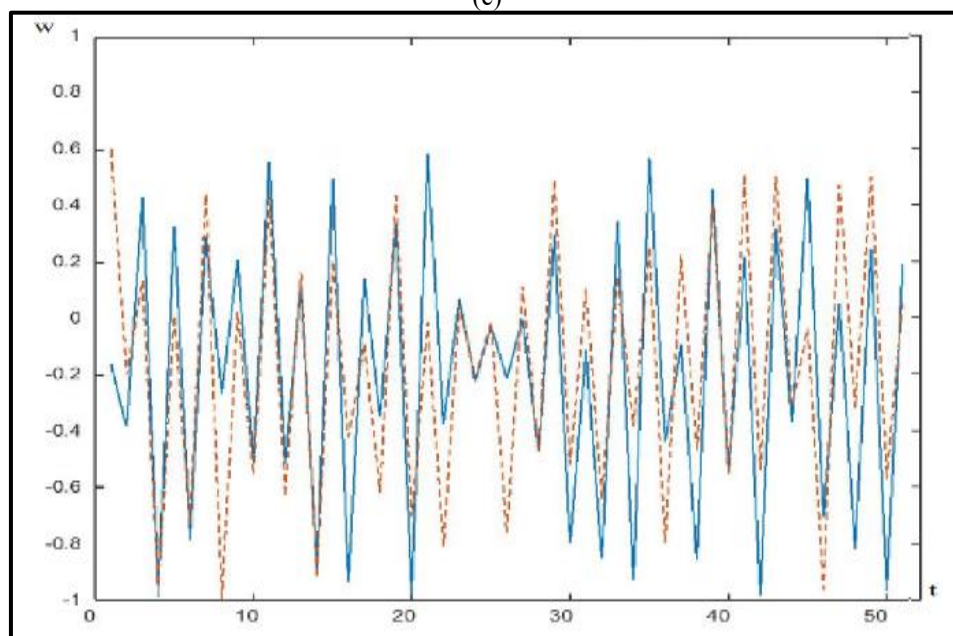
(a)



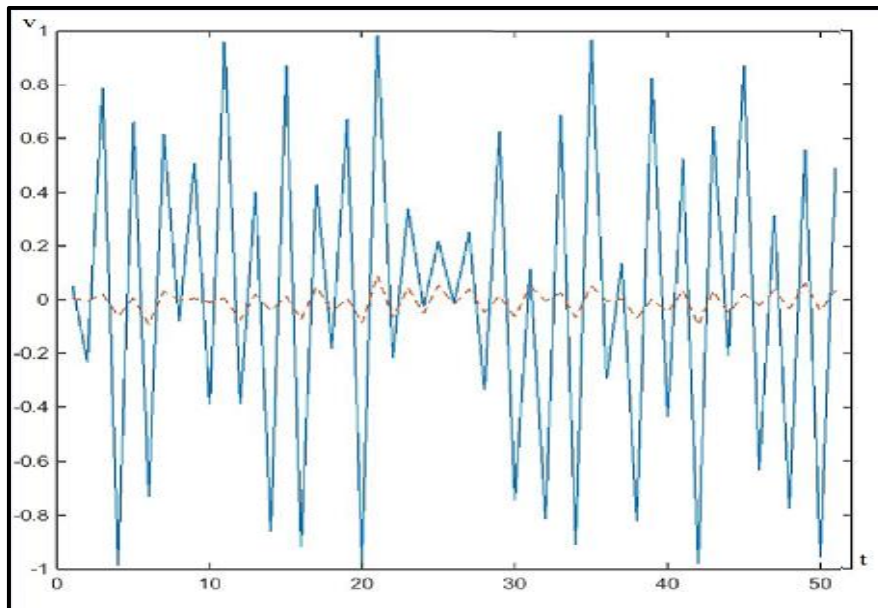
(b)



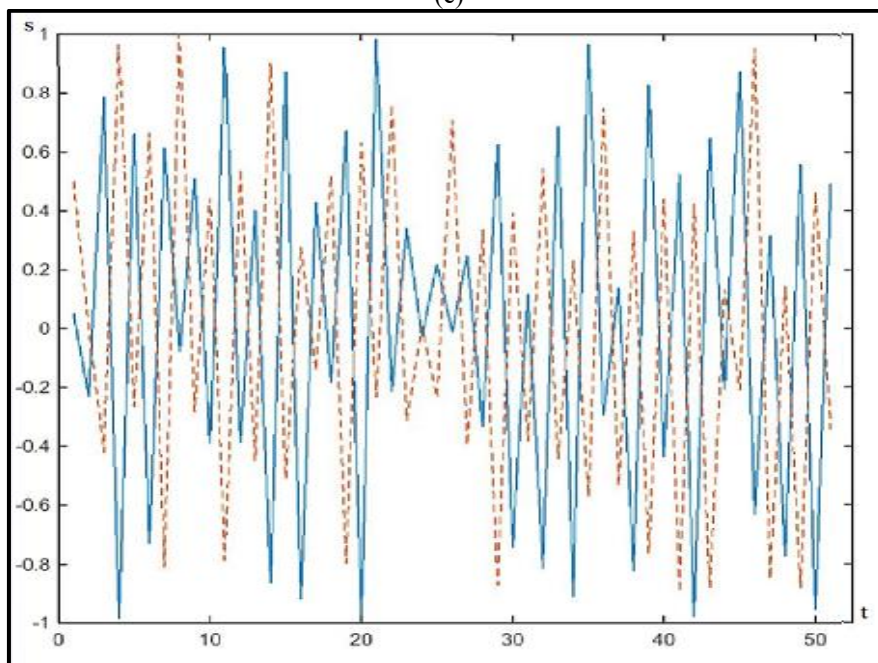
(c)



(d)



(e)



(f)

Figure 1. (a) Test of sensitivity for the system $X(t)$, (b) Test of sensitivity for the system $Y(t)$, (c) Test of sensitivity for the system $Z(t)$, (d) Test of sensitivity for the system $W(t)$, (e) Test of sensitivity for the system $V(t)$, (f) Test of sensitivity for the system $S(t)$

2.3 Key space analysis

A key space size should have more than 2^{100} possible keys [14]. An attacker tries to brute-force the system if the key space is small. However, the recommended system's sequence generation depends on the premier states $X(0)$, $Y(0)$, $Z(0)$, $W(0)$, $V(0)$, and $S(0)$, as well as the control parameters d , c , b , and a . It demonstrates that the proposed system key space is 2^{465} . This demonstrates that all produced keys are considered to be robust.

3. PROPOSED HUMAN VOICE ENCRYPTION ALGORITHM

This section describes how the proposed encryption model

uses the proposed 6D hyper chaotic system and its algorithm. A pattern of purely chaotic behaviour can also be seen in its temporal evolution.

3.1 Encryption algorithm

Following are the steps involved in the encryption process, as illustrated in Figure 2.

Step1: Recording or reading the original human voice signal.

Step2: Generation of chaotic vectors utilizing the system depend on the 6D hyper chaotic system with initial conditions $s(0)$, $w(0)$, $x(0)$, $y(0)$, $z(0)$, $v(0)$, and control parameters c , a , b , d .

Step3: Divide the speech signal into blocks of 5s. Scramble the voice signal blocks utilizing vector X for randomly altering the positions of the voice signal blocks.

Step4: Transform the scrambled block into a wavelet domain using DWT.

Step5: Scramble the bits of the transformed block based on vectors Y and Z(confusion).

Step6: For the diffusion process, perform the XOR operation bit by bit between the key produced from the vectors (w, v, s) and the scrambled vector.

Step7: Extract the encrypted speech output voice signal.

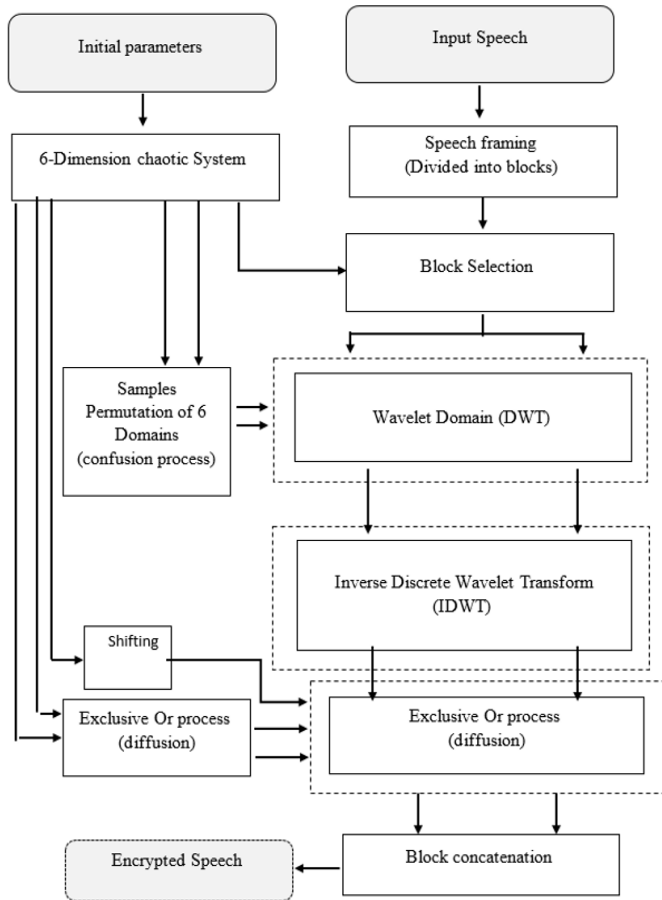


Figure 2. Proposed encryption system framework diagram

3.2 Decryption algorithm

The process employs the same steps of encryption but in reverse order after acquiring or loading the encrypted signal. Decryption algorithm steps are:

Step1: Loading the encrypted human voice signal.

Step2: Generation of chaotic vectors utilizing the system depend on the 6D hyper chaotic system with initial conditions $s(0), w(0), x(0), y(0), z(0), v(0)$, and control parameters c, a, b, d .

Step3: Divide the encrypted speech signal into blocks of 5s. Apply inverse diffusion process by performing the XOR operation bit by bit between the key produced from the vectors (w, v, s) and the scrambled vector.

Step4: Transform the scrambled block into a wavelet domain using DWT. Scramble the bits of the transformed block based on vectors Y and Z(confusion). Scramble the bits of the transformed block based on vectors Y and Z(confusion). Then, convert speech signal to time domain by applying IDWT.

Step5: Scramble the voice signal blocks utilizing vector X for randomly altering the positions of the voice signal blocks.

Step6: Extract the decrypted speech output voice signal.

4. EXPERIMENTAL RESULTS

MATLAB R2019 was utilized to execute the simulations. Different tests, such as waveform analysis, correlation tests, and SNR, were implemented to show the proposed system's security and performance. Voice signals with a sampling frequency of 8kHz were utilized as test files. The 6D hyperchaotic system parameters were: $(X(0), Y(0), Z(0), W(0), V(0), S(0))$ are (3.6, -1.2, 3.4, 0, 1.5, 2.1) respectively. Five speech signals with different duration and sizes selected from the Libri-Speech dataset [15] to evaluate the system.

4.1 Encryption efficiency

SNR ratio serves as a measurement for the amount of noise present in the encrypted data signal. To encrypt the substance of the signal, cryptographic analysts constantly work to make the signal noisier. Maximization masks the encrypted signal, and an SNR greater than 0dB indicates that the signal is clearer than the background noise. A lower PSNR value is needed for the encrypted voice file since it indicates that it contains a lot of noise and is, therefore, very resistant to attack [16]. PSNR and SNR between two different human voice signals are illustrated below [17, 18].

$$SNR = 10 * \log_{10} \sum_{i=1}^N \frac{X_i^2}{\sum_{i=1}^N (x_i - y_i)^2} \quad (2)$$

$$PSNR = 10 * \log_{10} \left(\frac{\max^2}{MSE} \right) \quad (3)$$

$$MSE = \frac{1}{N} \sum_{i=1}^N (x_i - y_i)^2 \quad (4)$$

where, X_i refers to the original speech, y_i presents the encrypted speech, N refers to the length of the speech signal, and MAX indicates the maximum value in the data stream. PSNR, SNR, MSE results are illustrated in Table 1.

Table 1. PSNR, SNR, MSE results

Voice Signal	SNR	PSNR	MSE	Size (KB)
SPEECH1.wav	-20.3607	4.7143	0.3377	85.5
SPEECH2.wav	-30.3854	4.7828	0.3324	230
SPEECH3.wav	-29.8023	4.7755	0.3330	286
SPEECH4.wav	-9.2364	4.2814	0.3731	338
SPEECH5.wav	-27.2478	4.7875	0.3321	400

4.2 Correlation coefficients

The correlation coefficient represents the dependence between the sample values of two human voice files. When the readings fall between $|0.3-0|$, the correlation is regarded as weak. A good encryption algorithm with acceptable resistance features has a lower correlation value [19, 20].

$$CC = \frac{cov(A, B)}{\sigma_A * \sigma_B} \quad (5)$$

where, $cov(B,A)$, r_B and r_A are the standard deviation and covariance between two speech files B and A.

The correlation coefficient values in Table 2 are found to be close to 0 or negative. As the original and encrypted files do

not depend on one another, our encryption method is effective and has the desired resistant quality.

Table 2. Results of correlation coefficient

Voice Signal	File Length(s)	Size (KB)	CC
SPEECH1.wav	5	85.5	0.002759
SPEECH2.wav	10	230	0.001893
SPEECH3.wav	15	286	-0.002755
SPEECH4.wav	20	338	-0.002034
SPEECH5.wav	25	400	0.000553

4.3 Waveform analysis

Visual investigation of speech's descriptive acoustic examination can be done in the time-frequency plane in the energy distribution and the waveform in the time domain [21, 22]. The waveform of an encrypted signal was consistently distributed and considerably unlike the original signals, as seen in Figure 3. The original signal's ability to be understood was lost, making it impossible to understand at all.

4.4 Entropy analysis

Higher entropy demonstrates higher resistance to statistical attacks [23, 24]. Table 3 shows that the information entropy for 5 distinct encrypted audio files was low for the original audio files and rises steadily during the encryption process.

Table 3. Results of entropy analysis

Voice Signal	Original	Permutation	Confusion	Decrypted
SPEECH1.wav	12.069319	11.91352	14.74506	12.05065
SPEECH2.wav	9.9890620	9.864283	14.74524	9.983513
SPEECH3.wav	12.415461	12.41661	14.74942	12.46003
SPEECH4.wav	13.694517	13.44405	14.74399	13.67252
SPEECH5.wav	13.694517	13.44235	14.74399	13.67252

4.5 Performance comparison

Table 4 illustrates a comparison between proposed and previous works based on key space, SNR, PSNR, and correlation coefficient.

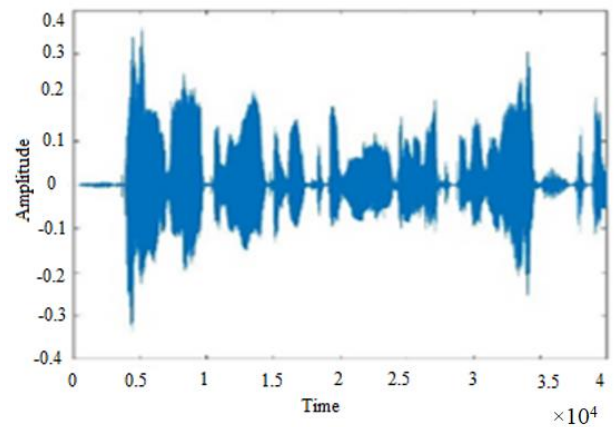
Table 4. Comparison of proposed method with four different works

References	Encryption Operations	Key Space	SNR	PSNR	CC
[9]	Diffusion and confusion	10512	-	27.30448	-
[11]	Permutation XOR,AND operation	-	7.020	12.881	0.4703
[10]	Permutation, substitution	$2^{548.11}$	-133	-	0.0009
[12]	Diffusion and confusion	2^{180}	45.1425	-	0.0032
OURs	Diffusion and confusion	2^{465}	-	4.2814	0.00043

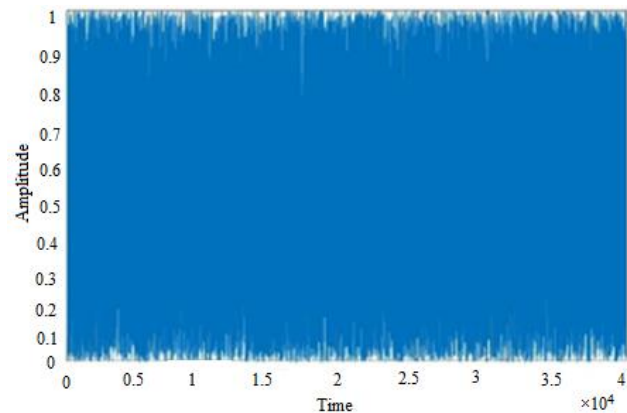
The proposed algorithm has a larger key space than the ref [12] algorithm, so it can withstand all types of brute-force attacks. Among all algorithms, the proposed algorithm has the lowest correlation coefficient. The SNR values revealing that encrypted human voice files have a high SNR. Such an SNR analysis demonstrates that all techniques suggest that the

information content fades out for encrypted human voice files. This indicates that attackers cannot use attacks to access sensitive data. These PSNR analyses reveal that all algorithms produce small PSNR values, meaning that encrypted audio files have a high noise level and are more secure against attacks.

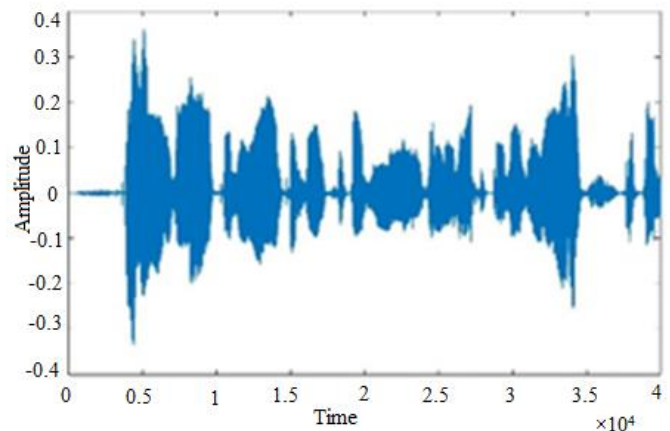
The correlation coefficient values are found to be close to 0 or negative. As the original and encrypted files do not depend on one another, our encryption method is effective and has the desired resistant quality. The SNR values are less than zero indicating that the encrypted signal is noisy, and PSNR value is very small indicating that the encrypted speech signal have a high noise level and are more secure against attacks.



(a) Original



(b) Encrypted



(c) Decrypted

Figure 3. Voice wave

5. CONCLUSIONS

This paper examines a novel method for audio encryption and decryption that uses a secret key that is a chaotic pseudo-random number. According to the experimental results, the approach is resistant to all forms of security threats. The approach is resistant to brute force attacks since the primary key is made up of a huge number of total keys. The permutation and scrambling up the security of a voice signal while making cryptanalysis challenging. So, the scrambling and permutation is first performed on the blocks of speech signal using the first key, then the second and the third key are utilized for bit permutation within the block. The keys pace is 2^{465} so that a brute-force attack is useless, and key sensitivity refers to convenience for our algorithms and a high level of security. The results of the system are: coefficients of correlation results belong to the range [-0.00276, 0.002759], high entropy values belong to the range [14.74399, 14.74942], PSNR has small values in the range [4.2814, 4.7875], SNR results are in range [-30.3854, -9.2364], and MSE results between original and extracted very close to zero in range [0.3321, 0.3731]. The suggested system is highly secure, according to performance analysis. The suggested system is highly secure, according to performance analysis. For future work, encryption algorithm will be improved by updating diffusion process.

REFERENCES

[1] Al-hazaimeh, O.M., Abu-ein, A.A., Nahar, K.M., Al-qasrawi, I.S. (2022). Chaotic elliptic map for speech encryption. *Indonesian Journal of Electrical Engineering and Computer Science*, 25(2): 1103-1114. <https://doi.org/10.11591/ijeecs.v25.i2.pp1103-1114>

[2] Al-Smadi, M., Abdulrahim, K., Salama, R.A. (2019). Dynamic features descriptor for road user recognition using hierarchal graph dynamic gradient pattern. *International Journal of Recent Technology and Engineering*, 6(s2): 414-418.

[3] Mohammad, O. (2021). A new speech encryption algorithm based on dual shuffling Hénon chaotic map. *International Journal of Electrical and Computer Engineering*, 11(3): 2203-2210. <https://doi.org/10.11591/ijeecs.v11i3.pp2203-2210>

[4] Jamal, M., Hassan, T.A. (2022). Speech coding using discrete cosine transform and chaotic map. *Ingénierie des Systèmes d'Information*, 27(4): 673-677. <https://doi.org/10.18280/isi.270419>

[5] Sadkhan, S.B., Al-sherbaz, A., Mohammed, R.S. (2014). Chaos based cryptography for voice encryption in wireless communication literature survey. In 2013 International Conference on Electrical Communication, Computer, Power, and Control Engineering (ICECCPCE), Mosul, Iraq, pp. 191-197. <https://doi.org/10.1109/ICECCPCE.2013.6998760>

[6] Saeed, N.A., Al-Ta'i, Z.T.M. (2020). Heart disease prediction system using optimization techniques. In International Conference on New Trends in Information and Communications Technology Applications, Baghdad, Iraq, pp. 167-177. https://doi.org/10.1007/978-3-030-55340-1_12

[7] Hameed, A.S. (2021). Speech compression and encryption based on discrete wavelet transform and

chaotic signals. *Multimedia Tools and Applications*, 80: 13663-13676. <https://doi.org/10.1007/s11042-020-10334-5>

[8] Nassan, W. A., Bonny, T., Baba, A. (2020). A new chaos-based cryptosystem for voice encryption. In 2020 3rd International Conference on Signal Processing and Information Security (ICSPIS), DUBAI, United Arab Emirates, pp. 1-4. <https://doi.org/10.1109/ICSPIS51252.2020.9340132>

[9] Parvees, M.M., Samath, J.A., Bose, B.P. (2018). Audio encryption—a chaos-based data byte scrambling technique. *International Journal of Applied Systemic Studies*, 8(1): 51-75. <https://doi.org/10.1504/IJASS.2018.091847>

[10] Farsana, F.J., Devi, V.R., Gopakumar, K. (2020). An audio encryption scheme based on Fast Walsh Hadamard Transform and mixed chaotic keystreams. *Applied Computing and Informatics*, 19(3/4): 239-264. <https://doi.org/10.1016/j.aci.2019.10.001>

[11] Hassan, N.F., Al-adhami, A., Mahdi, M.S. (2022). Digital speech files encryption based on hénon and gingerbread chaotic maps. *Iraqi Journal of Science*, 63(2): 830-842. <https://doi.org/10.24996/ijss.2022.63.2.36>

[12] Mokhnache, S., Daachi, M.E.H., Bekkouche, T., Diffellah, N. (2022). A Combined Chaotic System for Speech Encryption. *Engineering, Technology & Applied Science Research*, 12(3): 8578-8583. <https://doi.org/10.48084/etasr.4912>

[13] Lorenz, E.N. (1963). Deterministic nonperiodic flow. *Journal of Atmospheric Sciences*, 20(2): 130-141. [https://doi.org/10.1175/1520-0469\(1963\)020%3C0130:DNF%3E2.0.CO;2](https://doi.org/10.1175/1520-0469(1963)020%3C0130:DNF%3E2.0.CO;2)

[14] Marzog, H.A., Mohsin, M.J., Therib, M.A. (2021). Chaotic systems with pseudorandom number generate to protect the transmitted data of wireless network. *The Indonesian Journal of Electrical Engineering and Computer Science*, 21(3): 1602-1610. <https://doi.org/10.11591/ijeecs.v21.i3.pp1602-1610>

[15] Panayotov, V., Chen, G., Povey, D., Khudanpur, S. (2015). LIBRISPEECH: An ASR corpus based on public domain audio books. In 2015 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), South Brisbane, QLD, Australia, 2015, pp. 5206-5210. <https://doi.org/10.1109/ICASSP.2015.7178964>

[16] Shah, A., Bangash, J.I., Khan, A. W., Ahmed, I., Khan, A., Khan, A., Khan, A. (2022). Comparative analysis of median filter and its variants for removal of impulse noise from gray scale images. *Journal of King Saud University-Computer and Information Sciences*, 34(3): 505-519. <https://doi.org/10.1016/j.jksuci.2020.03.007>

[17] Abdullah, H.N., Hreshee, S.S., Jawad, A.K. (2015). Design of Efficient noise reduction scheme for secure speech masked by chaotic signals. *Journal of American Science*, 11(7): 49-55.

[18] Alazawi, M.K.M., Kadhim, J.Q. (2013). Speech scrambling employing Lorenz fractional order chaotic system. *Journal of Engineering and Sustainable Development*, 17(4): 195-211.

[19] Adhikari, S., Karforma, S. (2021). A novel audio encryption method using Henon - Tent chaotic pseudo random number sequence. *International Journal of Information Technology* volume, 13(4): 1463-1471. <https://doi.org/10.1007/s41870-021-00714-x>

- [20] Albahrani, E.A., Alshekly, T.K., Lafta, S.H. (2022). A review on audio encryption algorithms using chaos maps-based techniques. *Journal of Cyber Security and Mobility*, 11(1): 53-82. <https://doi.org/10.13052/jcsm2245-1439.1113>
- [21] Zhen, K., Lee, M.S., Sung, J., Beack, S., Kim, M. (2020, May). Efficient and scalable neural residual waveform coding with collaborative quantization. In *ICASSP 2020-2020 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, Barcelona, Spain, pp. 361-365. <https://doi.org/10.1109/ICASSP40776.2020.9054347>
- [22] Khaleel, A.H., Abduljaleel, I.Q. (2021). A novel technique for speech encryption based on k-means clustering and quantum chaotic map. *Bulletin of Electrical Engineering and Informatics*, 10(1): 160-170. <https://doi.org/10.11591/eei.v10i1.2405>
- [23] Raducanu, M., Cheroiu, D., Nitu, C.M. (2022). Sound encryption algorithm with perfect reconstruction using tent map and multidimensional Arnold chaotic systems. In *2022 45th International Conference on Telecommunications and Signal Processing (TSP)*, Prague, Czech Republic, pp. 264-267. <https://doi.org/10.1109/TSP55681.2022.9851365>
- [24] Ahmed, Z.J., George, L.E., Hadi, R.A. (2021). Audio compression using transforms and high order entropy encoding. *International Journal of Electrical and Computer Engineering*, 11(4): 3459-3469. <https://doi.org/10.11591/ijece.v11i4.pp3459-3469>