ISSN: 0067-2904

Digital Speech Files Encryption based on Hénon and Gingerbread Chaotic Maps

Nidaa Flaih Hassan[1]*, Ayad Al-Adhami[1], Mohammed Salih Mahdi[2]
[1]Department of Computer Science, University of Technology, Iraq
[2]BIT Department, Business Information College, University of Information Technology and Communications, Iraq

Received: 20/4/2021 Accepted: 6/7/2021

Abstract

Speech encryption approaches are used to prevent eavesdropping, tracking, and other security concerns in speech communication. In this paper, a new cryptography algorithm is proposed to encrypt digital speech files. Initially, the digital speech files are rearranged as a cubic model with six sides to scatter speech data. Furthermore, each side is encrypted by random keys that are created by using two chaotic maps (Hénon and Gingerbread chaotic maps). Encryption for each side of the cube is achieved, using the based map vector that is generated randomly by using a simple random function. Map vector that consists of six bits, each bit refers to one of the specific chaotic maps that generate a random key to encrypt each face of the cube. Results show that the pseudo-random keys created by using chaotic maps for cryptographic speech file have an acceptable characteristic concerning randomness tests, which is confirmed in this paper by using five statistical tests. The final evaluation of the speech encryption algorithm is measured by using different quality metrics, and the results show that the algorithm can achieve resist encryption.

Keywords: Speech Encryption, Secure Communication, Chaotic Map, Permutation

تشفير ملفات الصوت الرقمي بالاعتماد على خرائط هينون والزنجبيل الفوضوية

نداء فليح حسن[1] *, أياد حازم ابراهيم [1], محمد صالح مهدي [2]
[1]علوم الحاسوب ,الجامعه التكنولوجيه , بغداد , العراق
[2] ادارة معلوماتية الاعمال, جامعة تكنولوجيا المعلومات والاتصالات , بغداد , العراق

الخلاصة

ان ارسال ملفات الصوت نحتاج الى استخدام أساليب تشفير الكلام لمنع التنصت والتعقب والمخاوف الأمنية الأخرى. في هذا البحث ، تم اقتراح خوارزمية تشفير جديدة لتشفير ملف الصوت الرقمي . في البداية ، يتم إعادة ترتيب ملفات الصوت الرقمية كنموذج مكعب بستة جوانب لتشتيت بيانات الكلام. علاوة على ذلك ، يتم تشفير كل جانب بمفاتيح عشوائية ، يتم إنشاؤها باستخدام خريطتين فوضويتين (خرائط Hénon و Gingerbread الفوضوية). يتم تحقيق التشفير لكل جانب من جوانب المكعب ، باستخدام متجه الخريطة المعتمد الذي يتم إنشاؤه عشوائيًا باستخدام دالة عشوائية بسيطة. متجه الخريطة سوف يتكون من ستة بتات ، كل بت يشير إلى واحدة من الخرائط الفوضوية المحددة التي تولد مفتاحًا عشوائيًا لتشفير كل وجه من وجوه

*Email: 110020@uotechnology.edu.iq

المكعب. أظهرت النتائج أن المفاتيح شبه العشوائية التي تم إنشاؤها باستخدام الخرائط الفوضوية لملف الصوت المشفر لها صفة مقبولة فيما يتعلق باختبارات العشوائية ، والتي تم تأكيدها في هذا البحث باستخدام خمسة اختبارات إحصائية. تم قياس التقييم النهائي لخوارزمية تشفير الكلام باستخدام مقاييس جودة مختلفة ، وقد ظهرت النتائج أن الخوارزمية يمكنها تحقيق التشفير المقاوم.

1. Introduction

Encryption is a method of altering information from its typical identifiable (plain text) into unintelligible formula (ciphertext). Encryption can be used to avert illegal access to digital info [1].

The current technologies altered the technique; information is being directed just because the information is currently bits transported in computer networks around the world [2]. Images, audio, and video are digitized at a low cost to be stored or transferred, and any type of unauthorized access to digital information may result in financial or political loss. Therefore, a new investigation into multimedia security is essential [3].

Encryption systems are known for their rigidity, slow speed, complexity, and inapplicability for real-time usage. Chaotic systems offer solutions to these limitations via probability and randomness. Chaos can be defined by special characteristics such as unpredictability and nonlinearity, topological mixing, randomness, self-similarity, dense periodic orbits, ergodicity, and irregularity [4, 5].

Random performance and sensitivity are the advantages of using a chaotic system that lies in initial and parameter settings This made chaotic functions very significant in cryptography to achieve cryptographic requirements, such as confusion, disorder, and diffusion. Variance in the initial state and parameter setting of these systems can achieve vast changes in the last state of the system with few repetitions. Sequences of Chaotic have some good properties comprising easiness of key creation, sensitive dependency on the initial state and parameter settings. Implementing chaos into cryptography contributes to developing the safety of data owing to the good properties obtained from chaotic sequences [6]. When encrypted speech data needs to be sent, it is required to use a general key that should be identified in the communication system by the receiver [7]

Due to the significance and sensitivity of speech data, implementing confidentiality for data is a desirable method to offer high voice communication secrecy. Several methods have been suggested lately for voice encryption using different procedures, such as chaotic, hashing, and mixing. Chaotic maps are extensively used in speech encryption, due to random-like performance and high sensitivity in initial states.

In this paper, the speech file is rearranged in a new model to make it more unsystematic, which results in a speech file with fewer statistical characteristics, thus speech data is divided into six cubic faces. In addition, a new approach of a random key generator is presented to increase the complexity degree against the attacker task by consuming more time to achieve analytical process depending on the state and number of keys used.

The paper is presented as follows. Section 2 describes major research on secure voice files based on the application of chaos theory and encryption. Section 3 states the basic idea of a chaotic system and presents the two chaos maps used in this proposal with their equations. In section 4, the proposed algorithm is illustrated in detail with encryption and decryption modules. Section 5 presents the experimental results, demonstrated with figures and objective criteria. The final section concludes the proposed algorithm with some recommendations for future works.

2. Related Works

Many publications concentrate on securing speech files by using speech encryption,

biometric, chaos theory, and some other techniques to improve the security of the data. The following section presents important works that are done to obtain secure speech files.

In [8], S. B. Sadkhana et al., modified a unified chaotic map that has a periodic shape problem. The modification produced random sequences used for encryption voice. The proposal had been examined by Lyapunov Exponents (LEs), and the results achieved an increase in chaos compared with a unified chaotic map. FIPs, NIST, subjective and objective tests used to test encrypted voice, and the results showed the success of the proposed map. Encryption of a voice call, before transmitting over mobile network, was implemented by Hazem M. El Bakry in [9], the clue of the system was using encryption without using any safe servers or any midway systems between mobile phone and the GSM network. The encryption takes place before accessing the mobile phone. To make security robust, AES is added as another layer of security. Moreover, a private key is altered by the user before a call is done. Merging chaotic maps and block ciphers to encrypt audio is presented by Ekhlas Abbas Albahrani in [10], complexity of the encryption process was increased by using permutation, XOR, and substitution stages. Test results insured that the proposal was secure because of its great key space, identical histograms, low rate of PSNR and correlation with high MSR and entropy.

Real-time encryption was implanted by Cristina-Loredana in [11]. Three-voice encryption algorithms were allocated as two sets: asymmetric ciphers, NTRU, and RSA and symmetric ciphers (AES). Parameters are considered for assessment between ciphers, decipher, delay time, complexity, loss of packet, and level of security. Proposal algorithms were applied on Blackfin and TMS320C6x processors to optimize between hardware and software levels. Also, the delay time of encryption and decryption that consumed energy was reduced. Chaotic shift keying-based encryption of speech and decryption approach was used by P. Sathiyamurthi [12], in the chaotic shift keying method. The input speech signals were segmented into four levels, namely L0, L1, L2, and L3. Each level was permuted by 4 chaotic maps: logistic, tent, quadratic, and Bernoulli's maps. A chaotic shift keying allocated logistic map for L0, tent map for L1, quadratic map for L2, and Bernoulli's map for L3. In addition, the Chen map was used to permute sampled values. Results proved that the proposed method was highly safe against attackers with great diffusion and confusion techniques.

Z. N. Al-Kateeb and S.J. Mohammed suggested a new algorithm for audio ciphering and deciphering applying wavelet transform to exploit the pro of the characteristics of adaptive context which based on lossless audio coding. Also, biometrics was applied to offer a major level of classification and good quality, because the proposal has numerous qualities and points of interest. The suggested algorithm estimated properties of hand geometry as keys for coding and decoding the audio file. Results proved that quality metrics confirmed the efficiency and quality of the suggestion [13].

Voice encryption used three different schemes to gain strength and flexibility for the proposed encryption algorithm presented by Hamidreza [14]. The proposed algorithm used two encoding structures: DNA encryption method with permutation function to achieve fast and safe voice encryption. Evaluation of this algorithm was concluded using different measures: signal to noise ratio, peak signal to noise ratio, keyspace, coefficient of correlation, signal similarity, and signal frequency content. Evaluation results showed that the algorithm is safe and fast. Another real-time voice encryption was developed by Aishwarya Agarwal [15]. Input speech file was encoded to be decoded by only authentic people, and AES was used for encryption since it had specific construction to deal with sensitive information. Also it is practical whether it's used in hardware or software. Input was taken from audio using a microphone. This input was transferred over the channel to the receiver after it's converted into text form. AES was used to encrypt the converted text to produce a ciphertext. Then the ciphertext was transferred to the receiver over the channel. On the other side, the receiver

demands to implement decryption of encrypted text only if he has the valid secret key, else the request is failed. About 2128 tries are required to break 128 bits, which makes this algorithm very problematic to hack, and as a result, it's considered a safe protocol.

Cloud-local joint decoding framework that permits secrecy preservative of speech recognition was suggested by Shi-Xiong Zhang in [16]. The suggested algorithm allowed people to transfer their voice in an encrypted arrangement to confirm confidentiality of transferred data. The server can then do voice recognition on their behalf without knowing the content. Also, a deep polynomial network was efficiently trained using unencrypted data and makes forecasts in real-time of the encrypted speech. The framework had acceptable performance, but latency and degradation were increased related to outmoded cloud based DNNs.

Encryption of speech algorithm was introduced by F.J. Farsana at el., [17] who concentrated on parametric Lorenz-hyper-chaotic system and improved Hénon map. Improved Hénon map increased permutation process associated with the seed map and this led to decrease in correlation between plain and encrypted speech files. Choice of the hyper-chaotic system removed chaotic weak trajectories and smaller chaotic series. The proposed algorithm has keyspace, which defends the proposed algorithm counter to numerous statistical bouts, such as brute force bout. Also, dynamic keystream produced with hyper-chaotic system removed the likelihood of discrepancy attacks. Additionally, Fast Walsh Hadamard Transform (FWHT) developed the efficacy of the algorithm by decreasing the computational complications.

O.M. Al-Hazaimeh, introduced speech encryption, which used Lorenz chaotic map over internet protocol to improve the applications facilities in real-time, such as increasing security level and decrease Latency. The proposed algorithm was split it into two processes: dynamic processes for key generation using 128-bit hash value to change initial secret keys dynamically, and encryption and decryption process via Lorenz system. Performance evaluation was carried out using effective simulations and executions of statistical measurement. The average time delay in the proposed algorithm and some of the related algorithms such as AES was compared. The achieved results concluded that, the proposed algorithm was effectively secure in contradiction of several cryptanalysis attacks and has valuable cryptographic properties such as diffusion and confusion for good voice communication on the Internet [18]

3. Basic Concepts of Chaotic Map Systems

Stream cipher uses a series of random numbers to cipher plaintext with similar length, (bit-by-bit). Using truly random execution is considered impossible; in practice, pseudorandom numbers are used as an alternative [19]. Thus, the generation of pseudo-random numbers with optimal properties that meet the requirement of a key stream becomes a problem. Pseudorandom Number Generator (PRNG) is commonly used.

In many low dimensional chaos's based cryptographic algorithms, the cipher data directly depends on the chaotic orbit of a single chaotic system [20]. Chaotic systems have extensive power spectra and are highly sensitive to slight differences of initial settings. Thus, chaotic systems can create orbits that are not divergent from truly random orbits. Consequently, Chaotic Pseudorandom Number Generators (CPRNG) have attracted more consideration [3].

Function owns chaotic behavior, defined as a chaotic function or map in mathematics. The output of the map is used as the input in the next calculation, which is called iteration. The iteration is similar to encryption sequences of a cryptographic algorithm that leads to diffusion and confusion features of the algorithm [21]. Designing a chaotic map setting is usually difficult, but generally creates secure and efficient protocols [22].

Thus Chaos theory is utilized to construct nonlinear dynamical systems using mathematical models [23], its focuses on explaining the behaviour of a nonlinear dynamic system with a high sensitivity to beginning circumstances [24] .

There are many chaotic maps, such as Logistic map, Sine Chaotic map, LLS chaotic map and Qi hyperchaotic map [25], Hénon Chaotic Map [26], Duffing map, Tinkerbell Map, and Gingerbread man Map [27]. The following is a description of the two chaotic maps used in this paper:

2.1 *Hénon Chaotic Map*: The Hénon map is a discrete-time scale n=1, 2, (i.e. it is a map) system. Hénon map consists of two dimensional real planes with two control parameters (a, b). It is a dynamic system that exhibits chaotic behavior. The Hénon map takes a point (X_n ,Y_n) in the plane and maps it to a new point X_{n+1}, Y_{n+1}. However, the complete depiction of all likely forks under the alteration control parameters is remote from the finishing point. Hénon Chaotic equation system is :

$$X_{n+1} = 1 - a.X_n^2 + Y_n \quad (1)$$

$$Y_{n+1} = b \cdot X_n \quad (2)$$

Where a = 0.3, b ∈ [1.07, 1.4], the system is chaotic, consequently, this property is very valuable in encryption [28].

2.2 *Gingerbread Man Map*: In dynamical systems theory, the Gingerbread man map is a chaotic 2D map [29]. It is given by the following transformation represented in equations 4 and equation 5:

$$x_{n+1} = 1 - y_n + |x_n| \quad (3)$$

$$y_{n+1} = x_n \quad (4)$$

4. The Proposed Chaotic System

The proposed chaotic system is a cryptography algorithm that is used to encrypt digital speech files using Hénon Chaotic Map and Gingerbread Man Map. The plain digital speech file is rearranged using one of the geometrics models, which is the cubic model, whose six sides are encrypted using random keys. To make the encryption process for each side more robust, two types of chaotic maps are used to produce random keys (Hénon Chaotic Map and Gingerbread Man Map).

Map vector generated randomly is used to determine which chaos maps are to be applied on each cube side. The following two main modules are described the core model of the proposed algorithm.

3.1 *Encryption Module*

In this module the speech file is partitioned into six sides to be like cubic shape, these six sides are arranged from side one to side six. Consequently, side one to side four represent cubic sides, while the two other sides represent top and bottom sides of cubic. The block diagram of the Encryption module is shown in Figure 1.

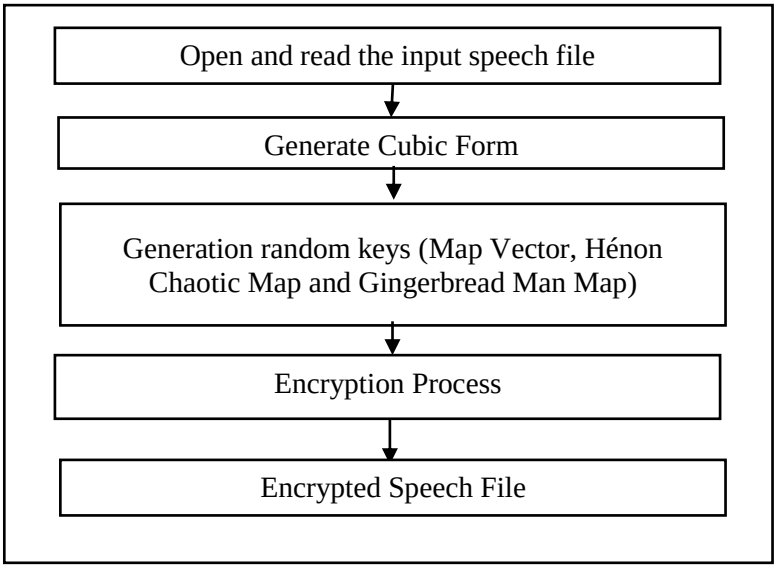

Figure 1- Encryption module of proposal algorithm

The steps of the proposed encryption algorithm are explained as follows:

Input: Plain Digital Speech File

Output: Encrypted Digital Speech File

1. Begin

2. Open the input speech file.

3. Get the raw data of the input speech file.

4. Divide raw data by 6 number of sides for cubic shape (A, B, C, D, E, F, and G), area side for each face is identified by the following equation :

$$\text{Cubic Area} = \text{Integer (length of plain speech file / 6)} \quad (5)$$

5. Construct a two-dimensional array for each side, according to the following equation:

$$\text{Face Area} = \text{Integer (Square Root (Cubic Area))} \quad (6)$$

6. Create Map Vector (MV) as explained in the following equation:

$$M = \text{Integer } ((7 \times \text{Rnd}) + 1) \text{ Mod } 2 \quad (7)$$

Where M is an integer value, and it's either (1 or 0), and Rnd is a simple random function.

7. Convert each side of cubic from ASCII into binary form

8. Generate two keys (K1, K2) from two chaotic maps (Hénon Chaotic Map and Gingerbread Man Map)

9. Convert K1, K2 into binary form to produce two keys, these two keys are scattered by exchanging each byte with the next byte, scattering makes two unsystematically keys and close to randomness as illustrated in Table(1) and Table (2).

10. Scattered two keys by exchanging each byte with the next byte

11. For each side, (A,B,C,D,E,F and G) of cubic form are XOR-ed with binary elements of chaotic maps

12. Convert the elements for each side to its ASCII.

13. Merge the six sides of a cube into one encrypted speech file, transmit it to the receiver side

14. End

One of the new ideas in this paper that made speech encryption robust, is that speech data is portioned in an undetectable way. Speech data spread on six cubic sides as declared in Equation 5 and Equation 6. In addition, two different chaotic maps are used to generate two

different keys used to encrypt sides of the cube with an undetectable map generated by Equation 7.

3.2 *Decryption Module*

In this section, encrypted speech file is converted back to plain speech file; it is a reverse of the encryption process. Figure 2 illustrates the block diagram of the decryption module.

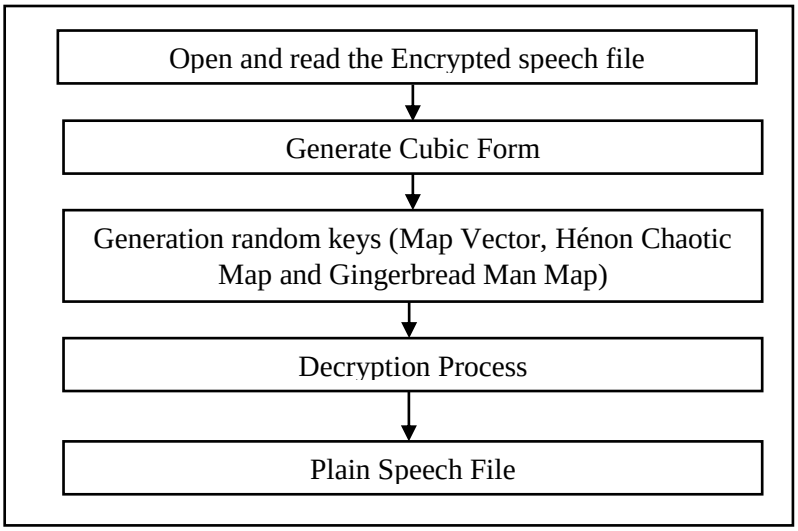

Figure 2-Decryption Module of Proposal Algorithm.

The overall module has reverse of steps in encryption module, the proposed decryption algorithm are explained as follows:

Input: Encrypted Digital Speech File

Output: Plain Digital Speech File

1. Begin
2. Open the encrypted speech file
3. Read the encrypted data of the speech file.
4. Divide decrypted speech data by 6 number of sides for cubic shape (A, B, C, D, E, F, and G), area side for each face is identified Equation 5,
5. Construct a two-dimensional array for each side performed by Appling Equation 6.
6. Convert each side of cubic from ASCII into binary form
7. Generation random keys: random keys are generated in the same way as in the Encryption module
8. Generate two keys (K1, K2) from two chaotic maps (Hénon Chaotic Map and Gingerbread Man Map)
9. For each Hénon Chaotic Map and Gingerbread Man Map, these items are converted from ASCII into binary key
10. Binary keys are obtained from two Chaotic Maps, for each key's bytes exchanged is done to obtain scatter keys
11. All binary elements for each side of cubic form are XOR-ed with the binary key of chaotic maps, obtained from the previous stage. The type of chaotic maps is applied according to the output of Map Vector (MV) results from Equation 7, All decrypted binary elements are converted to their ASCII
12. ASCII elements are again reformed to six sides (A, B, C, D, E, F, and G) of cubic form
13. Merge the six sides of cubic into one decrypted (plain) speech file.
14. End

5. Results and Discussion

A new cryptography algorithm is suggested in this paper to encrypt digital speech files. The results of the algorithm are considered from two issues: The first test focused on testing the randomness of the key generated from two chaotic maps, and the second test evaluates the performance of the proposed speech cryptography algorithm.

The first test evaluates the randomness of the sequence generated from chaotic maps using five bench tests. The tests include a statistical set to evaluate the randomness of quantity sequences produced by cryptographic random or pseudo-random number generators [30].

Tables 1 and 2 show evaluation results from applying five bench tests on the proposed two chaotic maps indicating that the data are generated by the PRNG based on the Hénon Chaotic Map and Gingerbread man respectively.

Table 1-Five bench randomness tests and their passing values for key generated from Hénon chaotic map

Randomness Test		**Freedom Degree**	**Key Size = 64 bits**	**Key Size = 128 bits**	**Key Size = 256 bits**	**Key Size = 512 bits**
Frequency Test		3.84	0.563	0.000	0.063	0.281
Runs Test	*T0*	13.784	5.125	5.563	1.125	6.125
	T1	12.309	6.000	6.625	5.281	7.844
Poker Test		11.1	4.550	4.225	6.575	7.463
Serial Test		7.81	2.250	2.750	2.125	3.313
Auto Correlation Test	*Shift No. 1*	3.84	0.778	0.008	1.133	1.881
	Shift No. 2		2.323	0.000	0.252	0.502
	Shift No. 3		0.803	1.352	2.091	1.228
	Shift No. 4		0.600	3.226	0.063	0.197
	Shift No. 5		0.153	2.350	0.896	0.570
	Shift No. 6		0.069	2.098	0.784	0.640
	Shift No. 7		1.421	0.207	1.161	0.335
	Shift No. 8		0.000	0.033	2.726	4.960
	Shift No. 9		1.473	3.706	0.490	0.575
	Shift No. 10		3.630	4.881	0.146	2.040

Table 2 - Five bench randomness tests and their passing values for key generated from Gingerbread man map

Randomness Test		**Freedom Degree**	**Key Size = 64 bits**	**Key Size = 128 bits**	**Key Size = 256 bits**	**Key Size = 512 bits**
Frequency Test		3.84	0.063	0.031	0.563	1.758
Runs Test	*T0*	13.784	0.750	4.563	10.906	11.578
	T1	12.309	0.750	9.688	5.938	8.125
Poker Test		11.1	4.550	7.350	14.450	14.744
Serial Test		7.81	1.250	0.125	1.125	3.656
Auto Correlation Test	*Shift No. 1*	12.309	0.143	0.071	2.075	0.699
	Shift No. 2		2.323	5.365	8.331	0.635
	Shift No. 3		1.328	2.888	0.889	0.018
	Shift No. 4		0.267	0.516	1.286	0.504
	Shift No. 5		2.051	5.081	2.490	0.239
	Shift No. 6		1.724	4.721	2.304	0.198
	Shift No. 7		2.965	5.165	3.378	0.661
	Shift No. 8		0.643	0.033	2.323	0.960
	Shift No. 9		0.164	0.008	0.684	0.097
	Shift No. 10		1.185	1.661	0.260	0.797

The computational complexity of a properly secure cipher is equal to the keyspace. The keyspace is the set of all potential keys and reflects the entire number of permutations

utilizing all secret key bits. As it is known, the number of bits n that define the size of the entire keyspace 2^n is called key-size. As previously stated, the suggested method comprises two secret keys, each of which is applied individually. The two secret keys are: - K1 and K2. two keys (Héno Chaotic Map and Gingerbread Man Map) are produced from two chaotic maps. Each keyspace is 2^{512}, and this keyspace is large enough to resist against all sorts of brute-force attacks. Table 3 compares key spaces for encrypting speech files with four related publications.

Table 3- Keyspace comparison

Ref. No.	Key Space
The Proposal Algorithm	2^{512}
[10]	2^{319}
[31]	2^{238}
[32]	2^{149}
[33]	2^{256}

Three speech samples are being evaluated as part of the proposed encryption testing; these samples have different sizes. Figures 3, 4, and 5 show these three samples' original speech single (plain) and corresponding Encrypted speech.

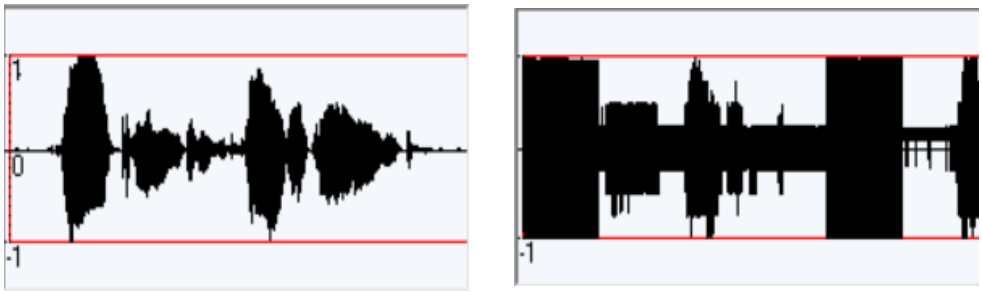

Figure 3-Shows speech single signal (Sample_1) and corresponding Encrypted speech.

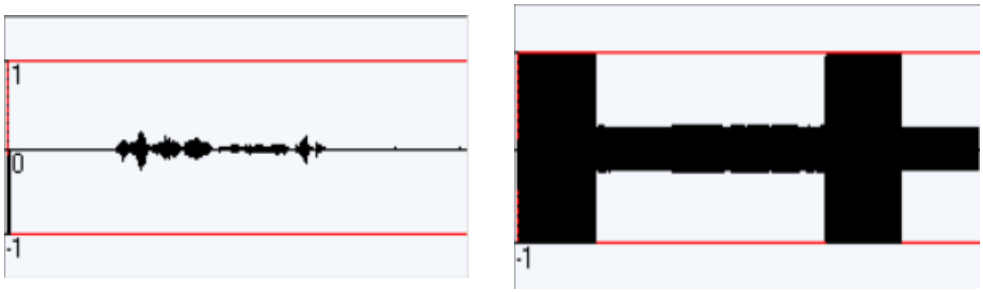

Figure 4-Shows speech single signal (Sample_2) and corresponding Encrypted speech

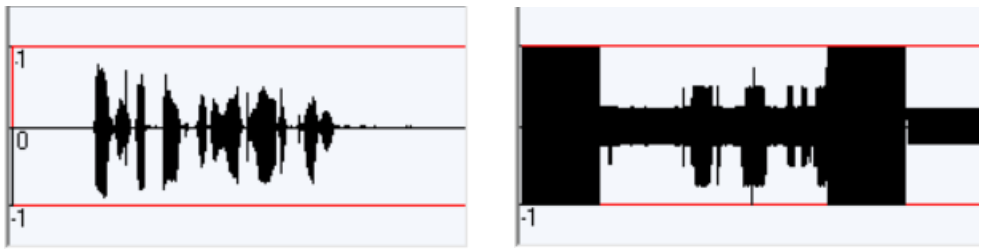

Figure 5-Shows speech single signal (Sample_3) and corresponding Encrypted speech

From the above figures, it's obvious that the difference between plain speech single and corresponding encrypted speech single is a sign of powerful difference and the plain speech single cannot be returned even slightly. Objective measures tests are applied to test the proposed encryption performance. These types of measures are used for testing the quality of

manipulated files and detect the error between the original plain speech file and the corresponding encrypted speech file.
The objective measures used in this proposal are: Mean Absolute Error (MAE), Mean Squared Error (MSE), Peak Signal to Noise Ratio (PSNR), Signal to Noise Ratio (SNR), and Normalized Cross-Correlation (NCC) [34] . Results of applying objective measures are in the following table

Table 4-Objective evaluation for three speech samples

Test Speech File	Test Speech File Size	MAE	MSE	PSNR	SNR	Correlation Measure
Sample_1	69 KB	40.889	3348.839	12.881	7.020	0.4703
Sample_2	79 KB	35.127	2818.977	13.630	7.602	0.277
Sample_3	138 KB	37.656	2992.931	13.370	7.396	0.290

From Table (4), it's obvious that all the test results point to speech encryption algorithm being secure; because measures indicate high MSE, low PSNR, low SNR, and low correlation measure. All these results showed that the proposed algorithm proved it was a good choice to use Hénon Chaotic Map and Gingerbread Man Map with scattering data obtained by distributed speech data as a cubic model.
Table 5 shows the computational time of the proposed approach for three different voice files. The time ranges from 0.05 to 0.2 seconds, and it rises as the size of the speech file rises. The findings show that the suggested technique is quicker and can be utilized in real-time.
Table 5 Computational time for the proposed encryption and decryption process

Test Speech File	File Size (KB)	Encryption Time in Sec.	Decryption Time in Sec.
Sample_1	69	≈ 0.05	≈ 0.05
Sample_2	79	≈ 0.06	≈ 0.06
Sample_3	138	≈ 0.14	≈ 0.14

6. Conclusion

In this paper, a new cryptographic algorithm is proposed and presented for a firm and safe speech encryption. Speech data are scattered according to rearranging speech data files into a cubic model; thus, the speech file is divided into six cube sides, these sides are encrypted with one of two chaotic maps. Pseudo-random number sequences are produced by using parameters of two chaotic maps, Hénon Chaotic Map and Gingerbread Man Map. Numbers are generated by chaotic maps that are converted into binary form. The sequence of binary bit is exchanged to make bit sequences unsystematically. These keys are XORed with a speech file depending on a simple random map vector. Results of the randomness test indicate two chaotic maps clue to a very difficult performance that infers optimal pseudo-random arrangement and a great space for a random key. The generated key produced a diffusion and confusion for cryptography speech data. The plots of the tested three speech files display the variations in encrypted speech files compared with the original speech single signal. The statistical evaluation shows a significantly decreasing correlation between plain speech files and encrypted files, also it sets that the cryptogram demonstrates a high degree of unpredictability.
As future work, speech data can be rearranged unsystematically, using a new geometric or three-dimensional model, also three or more chaotic maps can be used to generate an unsystematically random key to decrypt speech data.

References

[1] Mulani, P. B. Mane," Watermarking and Cryptography Based Image Authentication on Reconfigurable Platform", *Bulletin of Electrical Engineering and Informatics*, vol. 6, no. 2, pp. 181-187, June 2017,. Available : https:// beei.org/index.php /EEI/ article /view/651.

[2] Kordov,"A Novel Audio Encryption Algorithm with Permutation-Substitution Architecture", *Electronics* 2019.Available : https://www.mdpi.com/2079-9292/8/5/530

[3] ondal and T. Mandal "A light weight secure image encryption scheme based on chaos & DNA computing", *Journal of King Saud University – Computer and Information Sciences*, Vol. 29, Issue 4, Pages 499-504, 2017. Available : https:// www .scienc edirect . com/science/article/pii/S1319157816300027

[4] aopin, G. Zhang and J. Jiang, "Multimedia Security: A Survey of Chaos-Based Encryption Technology", Multimedia - *A Multidisciplinary Approach to Complex Issues*,2012.Available:https://www.intechopen.com/books/multimedia-a-multidis ciplin ary-approach-to-complex-issues/multimedia-security-a-survey-of-chaos-based- encryption- technology

[5] Sadkhan and R. Saad Mohammed, "Chaos-Based Cryptography for Voice Secure Wireless Communication." *International Conference on Electrical Communication, Computer, Power, and Control Engineering (ICECCPCE)*, 17-18 Dec. 2013.

[6] janarayanan and A. Pushparaghavan, "Recent Developments in Signal Encryption – A Critical Survey", *International Journal of Computational Intelligence and Informatics*, Vol. 2: Issue 6, June 2012.

[7] bdulRazzaq Hussein, M. K. Khashan and A. K. Jawad," A high security and noise immunity of speech based on double chaotic masking", *International Journal of Electrical and Computer (IJECE)*, Vol. 10, No. 4, August 2020, pp. 4270-4278 .

[8] Sadkhan and R. Saad Mohammed, "Proposed random unified chaotic map as PRBG for voice encryption in wireless communication", *International Conference on Communication, Management and Information Technology (ICCMIT 2015*, Vol. 65, pp. 314-323, 2015. Available: https://www.sciencedirect.com /science/article/pii /S1877050915029191.

[9] . El bakry, A. E. Taki_El_Deen and A. Hussein El Tengy, "Implementation of an Encryption Scheme for Voice Calls", *International Journal of Computer Applications* , Vol. 144, No. 2, pp. 24-27, 2016.Available:https: //www.ijcaonline.org/archives / volume 144 /number2/25153-2016910116

[10] bbas Albahrani, "A new audio encryption algorithm based on chaotic block cipher", *Annual Conference on New Trends in Information & Communications Technology Applications*-(NTICT'2017) 7 - 9 March 2017.

[11] redana Duta, L. Gheorghe and N. Tapus , "Real-time DSP Implementations of Voice Encryption Algorithms", *Proceedings of the 3rd International Conference on Information Systems Security and Privacy (ICISSP 2017)*, pp. 439-446. Available: https://www.scitepress.org/Papers/2017/62083/62083.pdf

[12] thiyamurthi and S. Ramakrishnan," Speech encryption using chaotic shift keying for secured speech communication", *EURASIP Journal on Audio, Speech, and Music Processing, 2017*.Available : https://link.springer.com/article/10.1186/s13636-017-0118-0

[13] Al-Kateeb and S. J. Mohammed, "Encrypting an audio file based on integer wavelet transform and hand geometry" TELKOMNIKA Telecommunication, Computing, Electronics and Control Vol. 18, No. 4, August 2020, pp. 2012-2017

[14] kaei Kate. J. Razmara and A. Isazadeh, " A Novel Fast and Secure Approach for Voice Encryption Based on DNA Computing", *3D Research Center, Kwangwoon University*

and Springer-Verlag GmbH Germany, part of Springer Nature, 2018.

[15] garwal, P. Raj Singh and S. Katiyar, "Secured Audio Encryption using AES Algorithm", *International Journal of Computer Applications (0975 – 8887)*, Vol. 178, No. 22, pp. 29-33, June 2019

[16] hang, "Encrypted Speech Recognition Using Deep Polynomial Networks", DOI: 10.1109/ICASSP.2019.8683721, Conference: *ICASSP 2019 - 2019 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP).*

[17] arsana, V.R. Devi and K. Gopakumar, "An audio encryption scheme based on Fast Walsh Hadamard Transform and mixed chaotic key streams", *Applied Computing and Informatics*, 2019.Available: https://www.emerald.com/insight/content/ doi/10.1016 /j. aci. 2019.10.001/full/html

[18] . Al-Hazaimeh, "A new dynamic speech encryption algorithm based on Lorenz chaotic map over internet protocol" , *International Journal of Electrical and Computer Engineering (IJECE)* ,Vol. 10, No. 5, pp. 4824-4834, October 2020.

[19] alih Mahdi and N. Flaih Hassan. "Design of keystream Generator utilizing Firefly Algorithm", *Journal of Al-Qadisiyah for computer science and mathematics*, Vol.10, No.3, pp. 91-99, 2018.

[20] . Prajwalasimha and L. Basavaraj, "Performance analysis of transformation and bogdonov chaotic substitution based image cryptosystem" *International Journal of Electrical and Computer Engineering (IJECE)*, Vol. 10, No. 1, pp. 188-195 February 2020.

[21] . H. Alwahbani and E.B. M. Bashier, "Speech Scrambling Based on Chaotic Maps and One Time Pad", 2013 International Conference on Computing, Electrical and Electronic Engineering (Icceee).
able: https://www.hindawi.com/journals/jcnc/2017/2721910/

[22] ahat, A. A. Tahat, M. Abu-Dalu, R.B. Albadarneh, A. E. Abdallah and O. M. Al-Hazaimeh," A new RSA public key encryption scheme with chaotic maps", *International Journal of Electrical and Computer Engineering (IJECE)* , Vol. 10, No. 2, pp. 1430-1437, April 2020.

[23] aqi and S. M. Hameed "A new Color image Encryption based on multi Chaotic Maps", *Iraqi Journal of Science*, Vol. 59, No.4B, pp: 2117-2127, 2018.

[24] . Ibrahem and H. A. Kassim, "VoIP Speech Encryption System Using Stream Cipher with Chaotic Key Generator", *Iraqi Journal of Science*, 2021, Special Issue, pp: 240-248, 2021.

[25] aqi, S. M. Hameed , " A new Color image Encryption based on multi Chaotic Maps ", *Iraqi Journal of Science*, Vol. 59, No.4B, pp. 2117-2127, 2018.

[26] ishra and R. Saharan, " A Fast Image Encryption Technique Using Henon Chaotic Map" , *Progress in Advanced Computing and Intelligent Engineering, Advances in Intelligent Systems and Computing* , Vol.1, pp. 329-339.

[27] aj and S. Garg, " Image Encryption using Chaotic Maps and DNA Addition Operation and Noise Effects on it" , *American International Journal of Research in Science, Technology, Engineering & Mathematics*, pp. 111-116, 2014.

[28] lawida, A. Samsudin, J. Sen Teh and W. Hamdan Alshoura, "Digital Cosine Chaotic Map for Cryptographic Applications" , *IEEE Access 7*, October 2019 .
lable: https://www.researchgate.net/publication/336574045

[29] i Khana, J. Ahmeda, J. Sher Khanb, J. Ahmadc and M. A. Khand, "A novel image encryption based on Lorenz equation, Gingerbreadman chaotic map and S8 permutation", *Journal of Intelligent and Fuzzy Systems* , October 2017.

[30] ulih Mahdi and N. Flaih Hassan," A Suggested Super Salsa Stream Cipher", *Iraqi Journal for Computers and Informatics (ijci)* , Vol.44 , No.2, 2018.

[31] o & D.Shihab," Lorenz and Rossler Chaotic System for Speech Signal Encryption ", *International Journal of Computer Applications*, Volume 128 – No.11, October 2015.

[32] Kordov, "A Novel Audio Encryption Algorithm with Permutation-Substitution Architecture", *Electronics*, MDPI, 2019. 10.3390/electronics805053.

[33] laih Hassan and R. W. Abd Aljabar " Encryption VoIP based on Generated Biometric Key for RC4 Algorithm", *Engineering and Technology Journal*, Vol. 39, Part B ,No. 01, Pages 209-221, 2021

[34] Jorj, H. Saleh and N. Flaih Hassan, "Data Hiding in Audio File by Modulating Amplitude ", *Engineering and Technology Journal*, Vol.28, No.5, 2010.