A Review on Chaotic Cryptosystems for Digital Speech Communication

Sanaa Sh. Ahmed[1], Sana A. Kadhim[1]
[1]Department of Computer Sciences, Al-Ma'moon University College, Baghdad, Iraq;
sanaa.s.ahmed@almamonuc.edu.iq
sana.a.kadhim@almamonuc.edu.iq

Abstract

Nowadays, communication via multimedia has become very prevalent and this requires protecting it from attackers and transmitting it securely to achieve reliability. Encryption and decryption techniques are helpful to provide effective security for speech signals to ensure that these signals are transmitted with secure data and prevent third parties or the public from reading private messages.

A chaotic system is the application of the mathematical chaos theory to the practice of cryptography. Because of the sensitivity of a chaotic system to the initial condition and random properties make it suitable for encrypting multimedia.

In this review paper, some chaotic speech signal algorithms are reviewed. The comparison and reports of analysis are explained to clarify the performance of the algorithm to encrypt original signals and recover them by using the decryption method.

Keywords: Cryptography, Chaotic map, Multimedia, Steganography.

1. Introduction

Rapid and enlarged growth of multimedia data replacing open networks and the Internet necessitates trustworthy and forceful security means to prevent unauthorized access to the transferred content and to provide confidentiality. One of the solutions employed is data encryption [1].

The Encryption algorithms work by changing data (i.e. image, text, voice, etc) so that they are invisible or hidden, unreadable throughout transmission. At the present time, to protect confidential information by increasing its protection and confidentiality, data encryption acting an enormous role in a variety of applications and a variety of encryption methods which are developed with the final goal.[2]

The process of transmitting data through internet networks is at risk due to the development of communication technologies. For this reason, a lot of information is transferred over networks in a verbal manner, which requires searching for new security techniques to protect voice communications.

The techniques of cryptography are used to develop protection via the transfer of verbal communication into meaningless form to an unauthorized person. The encryption of speech signals can be considered one of the great commonly used techniques to guarantee the security of vocal communications. There are many cryptography techniques have been proposed to deal with information security issues[3], like algorithms of speech encryption (i.e. Data Encryption Standard (DES), Triple Data Encryption Standard (3DES), RSA algorithm, and Advanced Encryption Standard (AES))[4][5].

Over Internet protocol (i.e. IP), the voice application (i.e. VOIP) is an IP telephony technology that allows transferring the voice data as the human voice in real-time in a mode that simulate the conventional telephone service (i.e., PSTN) [6]. A necessary requirement for voice applications over the Internet is a program (i.e. sender or receiver) has the ability to encode and decode the transmitted speech and has access to the Internet [7]. More advantages of voice applications when comparing it with the ordinary telephone service can be provided. The technology of IP telephony is cheaper comparing with other media services, can be integrated and permission to more professional bandwidth exploitation.

Consequently, the technology of IP telephony is favored by service providers as a way to reduce the costs over multimedia services. Furthermore, the IP telephony infrastructure is a solid economic ground in building more income-generating services. For this reason the IP telephony is becoming extra popular at the present time [8]. Although of the all activist features for IP telephony technology, however facing is various challenges and difficulties like packet loss, latency and security. Therefore, to proficiently control these difficulties, more advanced strategies or techniques are warranted to guarantee the quality of the IP telephony technology services (i.e., QoS) [9]. For example, the intruder's threat through IP networks is the record of security challenges in IP telephony technology. To manage security challenges and maintain data secrecy, the serves of cryptography can be used as an important tool [10]. Additionally to cryptography techniques, many methods and strategies were produced to protected transmitted voices such as Steganography [11]. There is a big difference between including information and encoding it. First, the information is hidden so that the average user will not know if there exists any part of that information. As for encryption, the user knows that there exists a hidden information, but it is encrypted which is incomprehensible. Therefore, to build an unvenerable protection system the main two technologies may be used to produce a system penetration process more complex.

The following sections of the paper will have the following. Section 2, Literature Review is presented. Section 3 includes Multimedia Cryptography Concept, Chaotic System for Voice Encryption obtained brief description about most conspicuous maps for speech signal in section 4. Section 5, presents an analysis of all reviewed algorithms. Conclusion is specified in Section 6.

2. Literature Review

In 2022, Al-Hazaimeh et al [12] proposed a new scheme for secure speech communication data by using a suggested key controlling system and Jacobian elliptic map. The Jacobian elliptic map used to improve the drawbacks encryption techniques that already used with speech, such as residual intelligibility, high computational complexity, low-key space and poor quality in decrypted signals. Using the Jacobian elliptic map a new cryptography method was applied. This method is selected to be employed in the cryptosystem applications from the chaotic maps. A block cipher scheme is used in this proposed cryptosystem. A multi keys are employing to protect all speech files against attacks and hacking and the key length used in this proposed method is (1024 bit). The results are proven that the proposed cryptosystem has greater level of security with lowest time (i.e., delay).

In 2022, Gebereselassie, S.A. and Roy, B.K [13] described a new communication technique which supposed to be secure, simple and efficient based on the mixture of hyperchaotic masking and modulation. For masking and modulation operations, one hyperchaotic system is used. The techniques of speech communication have feeble resistance to some attacks if only depended on chaotic masking. For this reason, additional chaotic modulation for encryption is applied. The encryption of the second level has improved the security of speech communication, as indication by the performance factors measures. The proposed method prove that encryption with a chaotic masked modulation is more secure than those used chaotic mask decryption.

In 2021, Zaid, O.A et al. [14] clarified two permutation algorithms applied on a file of speech signals based on chaotic map systems. The two algorithms are Arnold cat map and Baker's chaotic map with both based on permutation algorithm. The same speech signal sample is used to implement the both algorithms. The analysis criteria used to performance these algorithms are LLR, SD, CC, histogram and time for encryption and decryption. The time of encryption and decryption for both Baker and Arnold algorithm is very well and fewer than 0.36s, while the encryption and decryption times of both are very equivalent in all cases. The CC values of both algorithms is low (near 0), other than the results of CC for Arnold's algorithm are better than Baker's algorithm in all measures. The values of SD for both algorithms were very convergent perfect.

In 2021, Obaida Mohammad [15], proposed a new crypto-system for dynamic speech based on chaotic cryptography using Hénon chaotic map. The process was tested and applied on several speech files (TIMIT database) and diverse sampling rates (i.e., 5000 samples/sec, and 8000 samples/sec). The proposed system results show that the system was simple, fast, and has more random toggling behavior. To make the system sensitive to the initial condition, a higher-order of substitution is performed, linear and differential cryptanalysis attacks are infeasible.

In 2021, Adhikari, S. and Karforma, S. [16], described in work a method for audio encryption using Henon– Tent chaotic pseudo-random number generation algorithm. This paper uses a symmetric key cryptographic method, in which the secret key is represented by the random number sequence. The proposed method successfully encrypted the original audio signals because the encrypted audio file has a uniform spectrogram.

In 2021, Khaleel, A.H. and Abduljaleel, I.Q. [17], proposed a system were both quantum chaotic map and k-means clustering were employed to generate keys. Two scrambling stages were applied: the first used (BiRS, ‘binary representation scrambling’) algorithm which relied on bits and the second used (block representation scrambling BlRS) algorithm relied on k-means. Also, fractional Fourier transform (FrFT) was employed in the algorithm. The results were analysis statistically through five measures: CC, LLR, fwSNRseg, SNR and SNRseg. In the encryption process a high security was demonstrated, the high values represent fine pointer of low residual speech values.

In 2019, Kassim, S.et al [18], described a new method depended on a chaotic key generator to encryption and decryption speech. A fractional arranges chaotic map was used in a chaotic key matrix generation. The speech data is converted into an image to be encrypted using an encryption function. Using deadbeat observer, an accurate synchronization of the system was recognized and the decryption was performed. Diverse analyses were used to analyze the efficiency of the encryption system. Results of suggested method have a strong key generation method for reasonable speech communication and higher level of security against different attacks.

In 2019, Wang, X. and Su Y. [19] proposed a new encryption audio method which provides a degree of high security. This method confuses and diffuses audio files by using a chaotic method and DNA coding. The chaotic system initial value is controlled by the hash value of audio, which make the trajectory of chaotic is unpredictable. Experimental results show that using different types of audio leads to make the algorithm immune against many known types of attacks, furthermore, multi-channel audio processing can be recommended using this algorithm.

In 2018, Nagakrishnan, R. and Revathi [20], depended on DNA addition and chaotic maps speech encryption algorithm to protect speech communication. In this method the data files of speech signals are considered as input which is partitioned into four parts which have the same time duration.

Each part of speech was permuted and substituted by applying a different chaotic technique. Lastly, the segments of speech are encoded into DNA series and additional DNA operation is performed. The superior performance and quality are getting from the permutation and second level alternative. The result obtained from the proposed method algorithm suggested forcefulness, undetectable and secure against brute force attacks.

In 2018, Abbas, N.A. and Razaq, Z.H. [23], described a new chaotic system depended on combination of Arnold and Lucas maps. These maps give good results and perform the process of scrambling in good way. PSNR, SNR and correlation measures are used to evaluate this proposed system. The suggested method's output has a minimum information about the input signal if these metrics gives low values and this explain that the output file may contained amount of deviates information is too large. Additionally to the previous measures, testing robustness of the suggested method the NSCR and UACI measures are used. The propose system results compared with Arnold cat map and Fibonacci map were better.

3. Multimedia Cryptography Concept

Due to the increasing use of multimedia (i.e. Images, music, sound, videos, records, films, and animations) and more over the world, multimedia encryption became the backbone of any technology that used to achieve confidentiality and to prevent unauthorized access to confidential data. Real-time applications constraints, huge amounts, and sensitive features of multimedia signals inhibit using traditional crypto-methods over multimedia data.

Cryptography or cryptology is the process of securing media communication from harmful behavior. In general, cryptography is working on analyzing and studying methods that prevent attackers or any unauthorized party from accessing private messages. Modern cryptography was found by intersecting the disciplines of mathematics, information security, electrical engineering, computer science, digital signal processing, physics, and others. Using information security concepts like confidentiality, integrity, authentication, and non-repudiation) as a major fields of cryptosystems. Many applications are using cryptography nowadays like electronic commerce, electronic payments, military transmissions, and others.

4. Chaotic System for Voice Encryption

Securing audio files like voice, speech or siphon is an important and modern field of cryptography that used in communications of audio data through radio, telephone or IP. Chaotic cryptology is a mathematical process that is used to transmit data securely without worried about the third party intruding. There are many chaotic voices encryption system, will be illustrated in the following:

4.1 Logistic Mapping [20] [24]

Logistic mapping is a one-dimensional map that contains complex chaotic numbers introduced from the nonlinear equation (1).

$$x_{n+1=}z\, x_n(1-x_n)$$

---- (1)

Where x0 is a number between [0, 1]. The z is a control parameter.

4.2 Sine Mapping [20] [25]

The Sine map is also one dimensional map that is analogous to the Logistic map and used to produce a chaotic numbers. The mathematical representation of sin map is as in (2).

---- (2)

$$x_{n+1=}\ r_1\ \sin(\pi x_n)$$

Where, x_0 is the initial state of the function, the system parameter r_1 is various between 0 and 4. The value of x_0 is changeable between [0.25, 0.5].

4.3 Tent Mapping [20] [26] [27]

The tent mapping is simple and fast in computation, and for this reason, is chosen. The tent map mathematical function can be obtained as in (3)

$$x_{n+1} = \begin{cases} \mu\, x_n & for\, x_n < \frac{1}{2} \\ \mu(1 - x_n) & for\ \frac{1}{2} < \ x_n \end{cases} \qquad \text{---- (3)}$$

Where, x_0 is the initial value, $0 < \mu \leq 2$. This function will continue linearly within the intervals [−1, 1/2] and [1/2, 1] with value to slopes μ and −μ. To identify chaotic systems, their dynamics demonstrate a commonly used of various features.

4.4 Henon Mapping [20] [24] [27]

The Henon mapping is a chaotic map with one dimension which produces a system of nonlinear behavior. It schemes the signal of chaotic behavior. Henon mapping mathematical equation can be described in (4).

$$x_{n+1} = 1 - \left(ax^2(n)\right) + \ bx(n-1) \qquad \text{---- (4)}$$

Where, the two states 'a' and 'b' are having values (1.4) and (0.3) correspondingly.

4.5 New 4D Hyperchaotic System [22]

This hyperchaotic system represents by new four-dimension, its behavior shows a choosy set of parameter, which is distinct by:

$$\begin{cases} x_{1=}\,a(x_2 - x_1) \\ x_{2=}bx_1 - x_1x_3 \\ x_3 = -cx_3 + hx_1x_1 \\ x_4 = -ax_4 + ax_2 \end{cases}$$

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

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

---- (5)

Figure (1) shows the hyperchaotic system attractor (1). By using the initial conditions x_0 = [5.6 − 1.2 3.4 0].

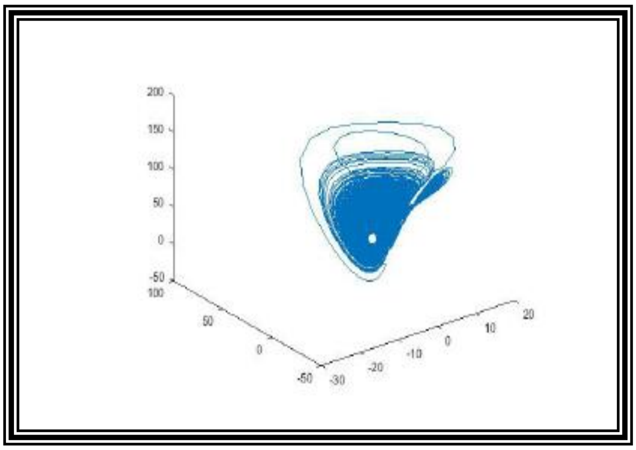


Fig (1): 4D hyperchaotic attractor

4.6 New 5D Hyperchaotic System [21] [22]

A new five dimensional hyperchaotic system can be described by adding the fifth equation to the system (1) as show bellow:

$$\begin{cases} x_{1=}\,a(x_2 - x_1) \\ x_{2=}bx_1 - x_1x_3 \\ x_3 = -cx_3 + hx_1x_1 \\ x_4 = -ax_4 + ax_5 \\ x_5 = -x_3x_4 + bx_4 + 10x_2 - 10x_5 \end{cases} \qquad \text{----(6)}$$

Figure (2) shows the hyperchaotic system attractor (2) where the initial conditions x_0= [5.6 -1.2 3.4 0 2].

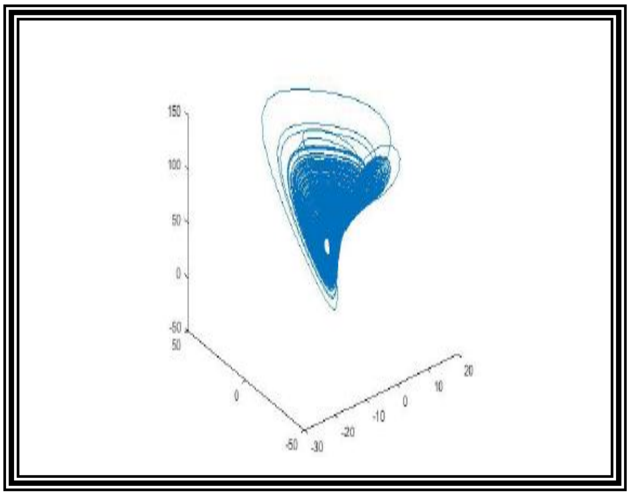


Fig (2): 5D hyperchaotic attractor

4.7 New 6D Hyperchaotic System [21] [28]

A new six dimensional hyperchaotic system can be built by adding the sixth equation to the system (2) as show bellow:

$$\begin{cases} x_{1=} - \ a\, x_1 + \ ax_2 \\ x_{2=} - x_1\, x_3 - bx_1 \\ x_3 = hx_1x_1 - cx_3 \\ \ \ x_4 = -ax_4 + ax_5 \\ \ \ x_5 = \ -x_4x_6 + \ bx_4 + 10x_2 - 10x_5 \\ x_6 = hx_1x_1 - cx_6 \end{cases} \qquad \text{---- (7)}$$

Figure (3) show the new six hyperchaotic attractor. By using the initial conditions x0= [5.6 -1.2 3.4 0 2 4].

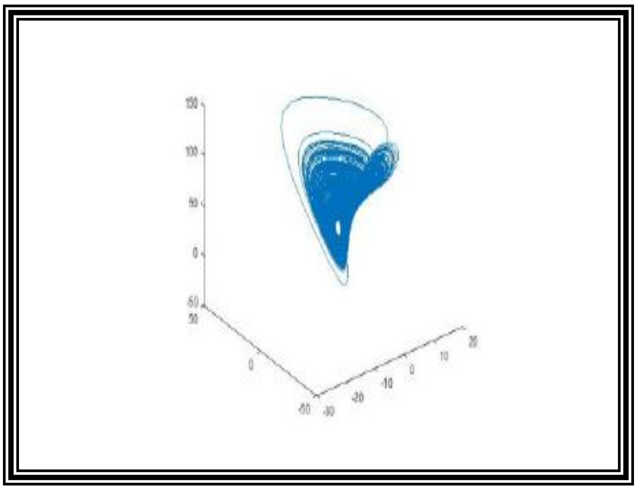


Fig (3): 6D hyperchaotic attractor

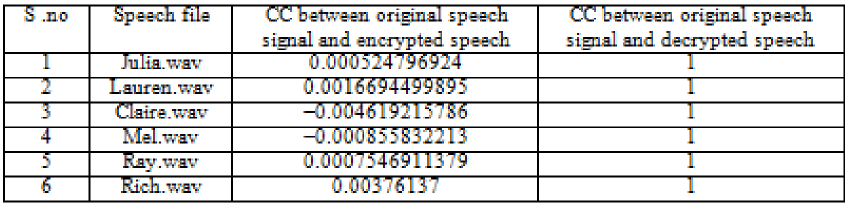
5. Comparison and Analysis Reports

The analysis report and comparison of the cryptosystem using chaotic algorithms are illustrated in the following:

Nagakrishnan, R. and Revathi, A.[20], represent the analysis report for encryption and decryption speech signals based on Correlation coefficient(CC), signal to noise ratio (SNR) and peak signal to noise ratio (PSNR) shown in table (1),table (2) and table(3). Six different speech signals are used to test these measures.

In Table (1), the result of correlation coefficient are illustrate firstly for the original and the encrypted speech, secondly for the input and decrypted speech. These results indicate that the encrypted series is fully random with high correlation because the correlation coefficient values are very low. Decrypted data is the same as the original one sine the correlation coefficient value is unity.

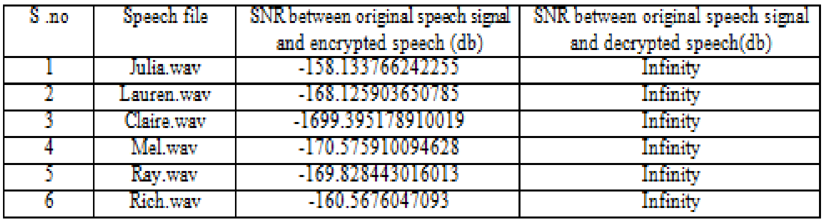
Table (1): Correlation Coefficient Result for encrypted and Decrypted speech



S .no	Speech file	CC between original speech signal and encrypted speech	CC between original speech signal and decrypted speech
1	Julia.wav	0.000524796924	1
2	Lauren.wav	0.0016694499895	1
3	Claire.wav	−0.004619215786	1
4	Mel.wav	−0.000855832213	1
5	Ray.wav	0.0007546911379	1
6	Rich.wav	0.00376137	1

Table (2) demonstrates the results of the (SNR) speech signals. The encrypted speech has high quality if SNR factor is low between the original and the encrypted speech.

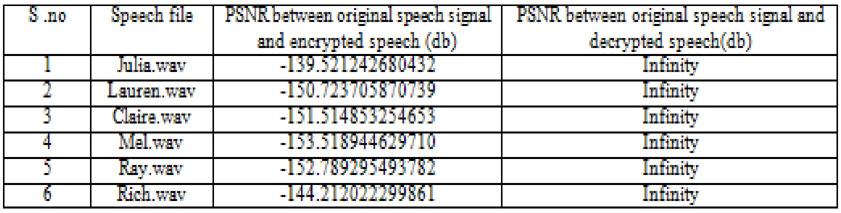
Table (2): SNR Result for encrypted and Decrypted speech



S .no	Speech file	SNR between original speech signal and encrypted speech (db)	SNR between original speech signal and decrypted speech(db)
1	Julia.wav	-158.133766242255	Infinity
2	Lauren.wav	-168.125903650785	Infinity
3	Claire.wav	-1699.395178910019	Infinity
4	Mel.wav	-170.575910094628	Infinity
5	Ray.wav	-169.828443016013	Infinity
6	Rich.wav	-160.5676047093	Infinity

The (PSNR) values are different from one another for all the six speech samples as shown in table (3). The researchers proved that, if the PSNR between the original and the encrypted speech is low, then the encrypted speech has a high quality. The whole signal's data will be recovered by decryption, which indicates that the value of PSNR is infinity between original speech and decrypted speech.

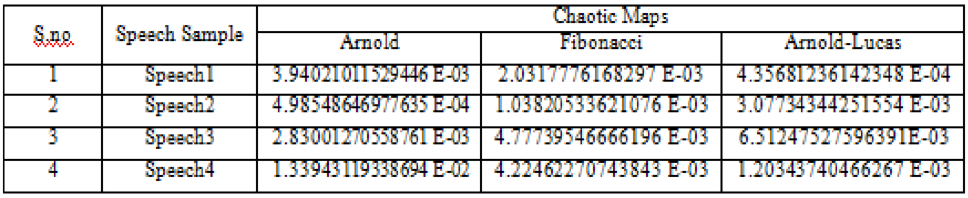
Table (3): PSNR Result for encrypted and Decrypted speech



S .no	Speech file	PSNR between original speech signal and encrypted speech (db)	PSNR between original speech signal and decrypted speech(db)
1	Julia.wav	-139.521242680432	Infinity
2	Lauren.wav	-150.723705870739	Infinity
3	Claire.wav	-151.514853254653	Infinity
4	Mel.wav	-153.518944629710	Infinity
5	Ray.wav	-152.789295493782	Infinity
6	Rich.wav	-144.212022299861	Infinity

Abbas, N.A. and Razaq, Z.H[23], also used (CC),(SNR), and (PSNR) to analyze the results of speech encryption and speech decryption process. The two samples of speech are evaluated using (CC), when the value is near zero, it means that the relation between the two samples is weak, and therefore attackers cannot predicate the secret key. In the table (4) show the result of the encryption process using (CC) for Arnold-Lucas method; (CC) value should be minimum value which means there is no relation between the original and encrypted samples. Arnold-Lucas method compared with the other two methods that the fewer values of Arnold-Lucas indicate that have best value.

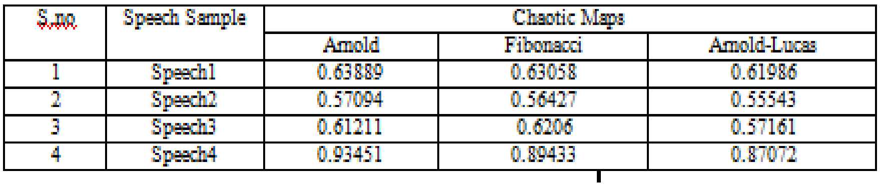
Table(4) Correlation Coefficient Result for encryption process



S.no	Speech Sample	Chaotic Maps		
		Arnold	Fibonacci	Arnold-Lucas
1	Speech1	3.94021011529446 E-03	2.0317776168297 E-03	4.35681236142348 E-04
2	Speech2	4.98548646977635 E-04	1.03820533621076 E-03	3.07734344251554 E-03
3	Speech3	2.83001270558761 E-03	4.77739546666196 E-03	6.51247527596391E-03
4	Speech4	1.33943119338694 E-02	4.22462270743843 E-03	1.20343740466267 E-03

To measure the remaining clearness in the encryption process for the encrypted signal, (SNR) is used. Table (5) represents the (SNR) value for four speech files. In general, if the value of (SNR) is low, the level of noise is higher than the level of the original speech signals.

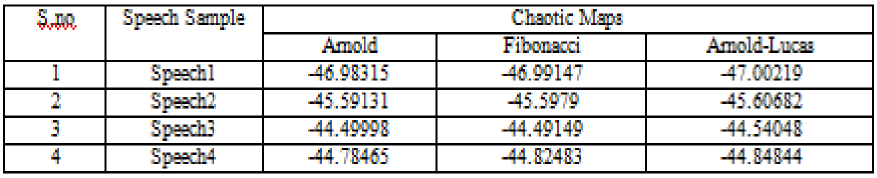
Table (5) SNR Result for encryption process



S.no	Speech Sample	Chaotic Maps		
		Arnold	Fibonacci	Arnold-Lucas
1	Speech1	0.63889	0.63058	0.61986
2	Speech2	0.57094	0.56427	0.55543
3	Speech3	0.61211	0.6206	0.57161
4	Speech4	0.93451	0.89433	0.87072

In table (6) the (PSNR) measure is used to evaluate the encryption quality of the original signal. The encryption of higher quality indicates that the (PSNR) value is high and the best quality encryption process is provided compared with other methods.

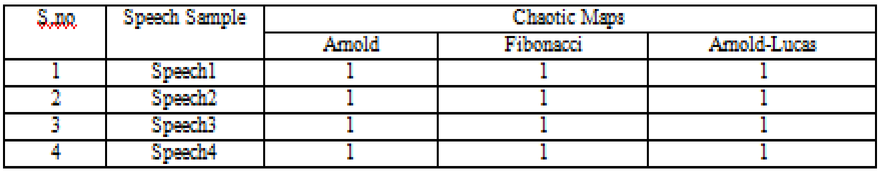
Table (6) PSNR Result for encryption process



S.no	Speech Sample	Chaotic Maps		
		Arnold	Fibonacci	Arnold-Lucas
1	Speech1	-46.98315	-46.99147	-47.00219
2	Speech2	-45.59131	-45.5979	-45.60682
3	Speech3	-44.49998	-44.49149	-44.54048
4	Speech4	-44.78465	-44.82483	-44.84844

Table (7) illustrates the (CC) for decryption process where this measure determines the cryptosystem encryption quality. The quality result of decryption process was equal ‘1’, which means that a complete correlation between original and the recovered speech signal.

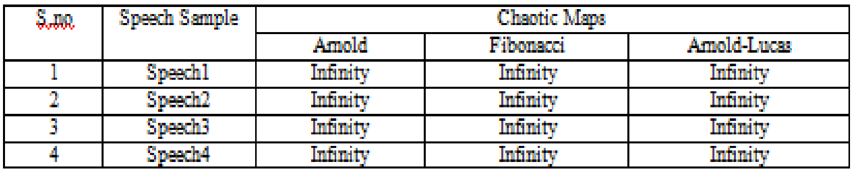
Table (7) CC Result for decryption process



S.no	Speech Sample	Chaotic Maps		
		Arnold	Fibonacci	Arnold-Lucas
1	Speech1	1	1	1
2	Speech2	1	1	1
3	Speech3	1	1	1
4	Speech4	1	1	1

In table (8) the results of (SNR) for the decryption process are obtained. Commonly, the high SNR value indicates the good quality of decrypted signals. As noted from the table below that this measure for three maps is infinity which means in the descrambling process no data is lost.

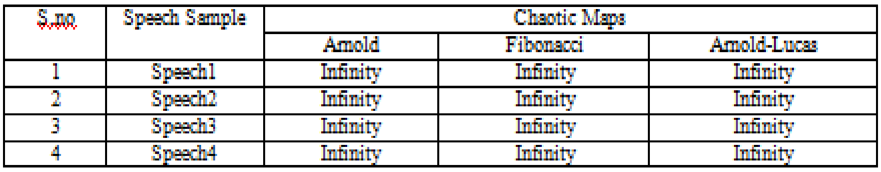
Table (8) SNR Result for decryption process



S.no	Speech Sample	Chaotic Maps		
		Arnold	Fibonacci	Arnold-Lucas
1	Speech1	Infinity	Infinity	Infinity
2	Speech2	Infinity	Infinity	Infinity
3	Speech3	Infinity	Infinity	Infinity
4	Speech4	Infinity	Infinity	Infinity

PSNR results for the decrypted process are shown in table (9). The results are also infinity as same as the results of the SNR measure.

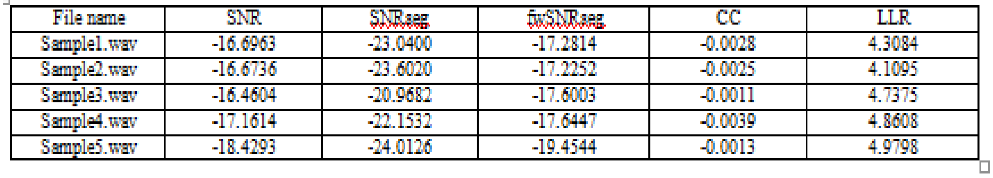
Table (9) PSNR Result for decryption process



S.no	Speech Sample	Chaotic Maps		
		Arnold	Fibonacci	Arnold-Lucas
1	Speech1	Infinity	Infinity	Infinity
2	Speech2	Infinity	Infinity	Infinity
3	Speech3	Infinity	Infinity	Infinity
4	Speech4	Infinity	Infinity	Infinity

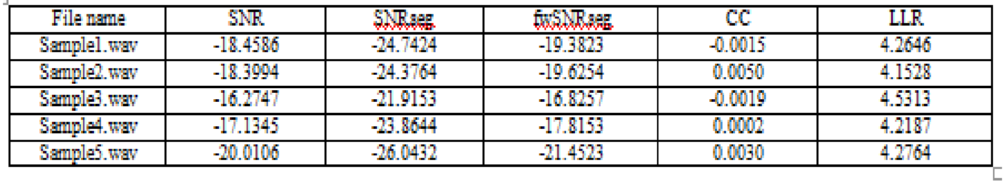
Khaleel, A.H. and Abduljaleel, I.Q.[17], evaluate the work using SNR, “Segmental Signal-to-Noise-Ratio” (SNRseq), Frequency-weighed Signal-to-Noise Ratio (fwSNRseg), CC, and Log-Likelihood Ratio (LLR)[29][30][31]. In tables 10-12 showed the results of encryption process for speech signals.

Table (10) measured results for encryption speech signal sample length 4 ms



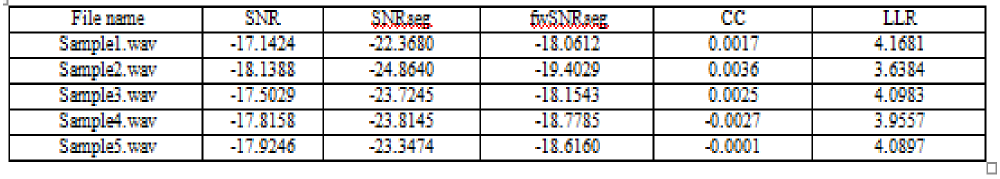
File name	SNR	SNRseg	fwSNRseg	CC	LLR
Sample1.wav	-16.6963	-23.0400	-17.2814	-0.0028	4.3084
Sample2.wav	-16.6736	-23.6020	-17.2252	-0.0025	4.1095
Sample3.wav	-16.4604	-20.9682	-17.6003	-0.0011	4.7375
Sample4.wav	-17.1614	-22.1532	-17.6447	-0.0039	4.8608
Sample5.wav	-18.4293	-24.0126	-19.4544	-0.0013	4.9798

Table (11) measured results for encryption speech signal sample length 7 ms



File name	SNR	SNRseg	fwSNRseg	CC	LLR
Sample1.wav	-18.4586	-24.7424	-19.3823	-0.0015	4.2646
Sample2.wav	-18.3994	-24.3764	-19.6254	0.0050	4.1528
Sample3.wav	-16.2747	-21.9153	-16.8257	-0.0019	4.5313
Sample4.wav	-17.1345	-23.8644	-17.8153	0.0002	4.2187
Sample5.wav	-20.0106	-26.0432	-21.4523	0.0030	4.2764

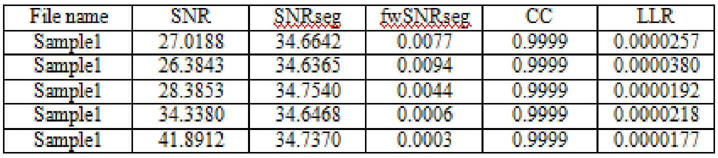
Table (12) measured results for encryption speech signal sample length 10 ms



File name	SNR	SNRseg	fwSNRseg	CC	LLR
Sample1.wav	-17.1424	-22.3680	-18.0612	0.0017	4.1681
Sample2.wav	-18.1388	-24.8640	-19.4029	0.0036	3.6384
Sample3.wav	-17.5029	-23.7245	-18.1543	0.0025	4.0983
Sample4.wav	-17.8158	-23.8145	-18.7785	-0.0027	3.9557
Sample5.wav	-17.9246	-23.3474	-18.6160	-0.0001	4.0897

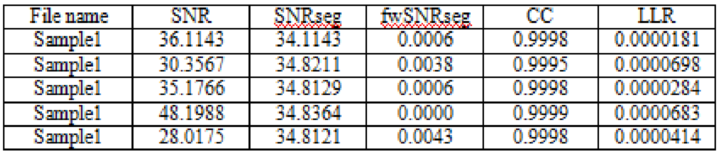
Tables (10)(11)(12) noted that the quality of the encrypted signal is high which means high security is produced in the encrypted process when the values of (SNR, SNRseg, fwSNRseg) is low, (LLR) are high and (CC) is low (near to zero). As well, tables 13-15 illustrates the results of decrypted process for speech signals.

Table (13) measured results for decryption speech signal sample length 4 ms



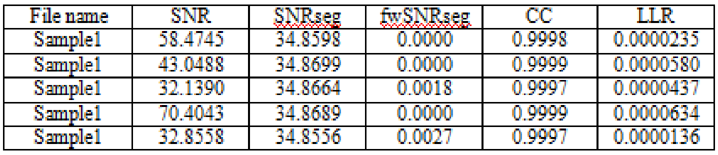
File name	SNR	SNRseg	fwSNRseg	CC	LLR
Sample1	27.0188	34.6642	0.0077	0.9999	0.0000257
Sample1	26.3843	34.6365	0.0094	0.9999	0.0000380
Sample1	28.3853	34.7540	0.0044	0.9999	0.0000192
Sample1	34.3380	34.6468	0.0006	0.9999	0.0000218
Sample1	41.8912	34.7370	0.0003	0.9999	0.0000177

Table (14) measured results for decryption speech signal sample length 7 ms



File name	SNR	SNRseg	fwSNRseg	CC	LLR
Sample1	36.1143	34.1143	0.0006	0.9998	0.0000181
Sample1	30.3567	34.8211	0.0038	0.9995	0.0000698
Sample1	35.1766	34.8129	0.0006	0.9998	0.0000284
Sample1	48.1988	34.8364	0.0000	0.9999	0.0000683
Sample1	28.0175	34.8121	0.0043	0.9998	0.0000414

Table (15) measured results for decryption speech signal sample length 10 ms

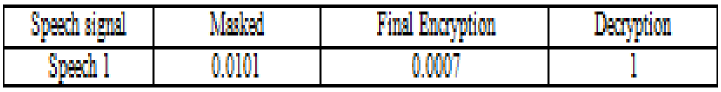


File name	SNR	SNRseg	fwSNRseg	CC	LLR
Sample1	58.4745	34.8598	0.0000	0.9998	0.0000235
Sample1	43.0488	34.8699	0.0000	0.9999	0.0000580
Sample1	32.1390	34.8664	0.0018	0.9997	0.0000437
Sample1	70.4043	34.8689	0.0000	0.9999	0.0000634
Sample1	32.8558	34.8556	0.0027	0.9997	0.0000136

Tables (13) (14) (15) observe that the value of SNR and SNRseg for each signal decrypted increases (very high), which gives a higher quality of the decrypted signal. Also, the value of LLR is tiny value with no remaining intelligibility and very noisy coded signals. Since the value of CC is close to +1, a high relationship will be found between the original and decryption signal.

Gebereselassie, S.A. and Roy, B.K[13], estimate proposed method using CC, Segmental Spectral Signal to Noise Ratio(SSSNR). Table (16) represents the result of encryption and decryption process for speech1 signal.

Table (16) the results of CC for masked, encryption and decryption process for speech1signal



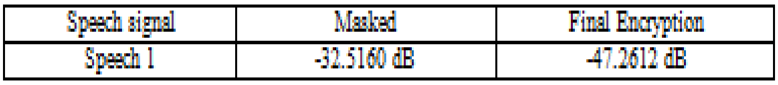
Speech signal	Masked	Final Encryption	Decyption
Speech 1	0.0101	0.0007	1

In table (16) obtain the value of CC for the encryption process(masked modulation) is close to zero (0.0007) which indicates there is no correlation between the original and masked modulated speech signals. Also, the CC value between the original and masked signals is observed as (0.0101). The masked modulation is high security from the masked signal as the results reveal.

On another side, the CC value calculated between original and decrypted speech signal is equal to (1). This explains the similarity between the original and decrypted speech signal, thus, the original speech signal is effectively restored.

In Table (17) shown the result of Segmental Spectral Signal to Noise Ratio (SSSNR) which consider another metric to evaluate the quality of speech encryption.

Table (17) the results of SSSNR for encryption process

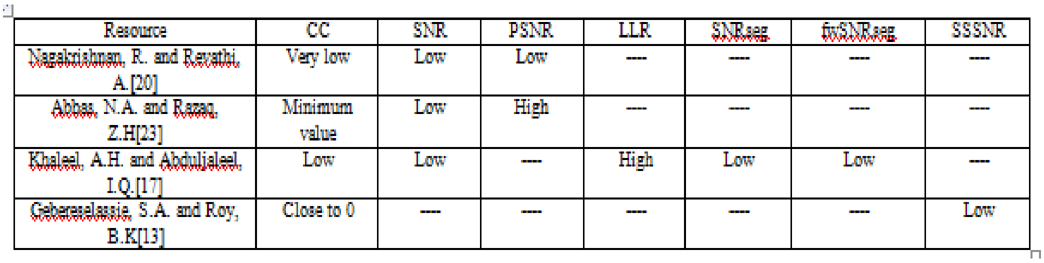


Speech signal	Masked	Final Encryption
Speech 1	-32.5160 dB	-47.2612 dB

As shown in table (17) the final encryption (masked modulated) speech signal is lower than the masked encryption speech signal. This indicates that the security of this method is improved.

Table (18) explains the comparison of different cryptosystem chaotic method for encryption speech signals.

Table (18) the comparison results of Speech Signal Encryption method

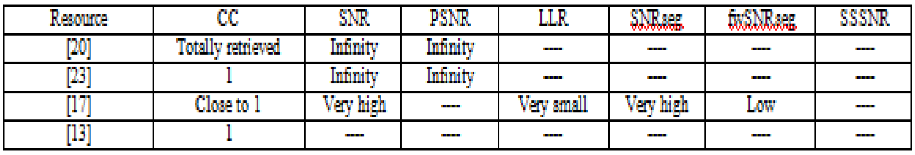


Resource	CC	SNR	PSNR	LLR	SNRseg	fwSNRseg	SSSNR
Nagakrishnan, R. and Revathi, A.[20]	Very low	Low	Low	----	----	----	----
Abbas, N.A. and Razaq, Z.H[23]	Minimum value	Low	High	----	----	----	----
Khaleel, A.H. and Abduljaleel, I.Q.[17]	Low	Low	----	High	Low	Low	----
Gebereselassie, S.A. and Roy, B.K[13]	Close to 0	----	----	----	----	----	Low

In table (18) noted that when the (CC and SNR) are low, this means that the encrypted speech signal is high and the security of the chaotic system is effective. Also, the (PSNR) is different from one method to another (Low, High) according to its results. Khaleel, A.H., and Abduljaleel, I.Q. [17] conclude the (LLR) is high and (SNRseg and fwSNRseg) are low which indicates that the speech signal is encryption correctly. Additionally, Gebereselassie, S.A. and Roy, B.K[13] found the value of (SSSNR) is low which ensures that the signal of speech is fully encrypted and the security of the system is improved.

Table (19) explains the comparison of different cryptosystem chaotic method for decryption speech signals.

Table (19) the comparison decryption method results of speech signal



Resource	CC	SNR	PSNR	LLR	SNRseg	fwSNRseg	SSSNR
[20]	Totally retrieved	Infinity	Infinity	----	----	----	----
[23]	1	Infinity	Infinity	----	----	----	----
[17]	Close to 1	Very high	----	Very small	Very high	Low	----
[13]	1	----	----	----	----	----	----

In table (19) illustrate that the (CC) is (1) which indicates that the encrypted speech signal is totally retrieved. Moreover, Nagakrishnan, R. and Revathi, A.[20] and Abbas, N.A. and Razaq, Z.H[23] found the(SNR and PSNR) value are infinity this leads to that the decrypted speech signal is recovered as original signal. Khaleel, A.H. and Abduljaleel, I.Q.[17] conclude that the value of (SNR, SNRseg) is very high, (LLR) is very small with fully noisy signal, and (fwSNRseg) is low.

6. Conclusion

Speech signals are considered one type of multimedia application. For transmission, these signals over the network in safety form will need to use a cryptosystem that protects these signals from any attacker. This review paper represents an almost chaotic algorithmic for speech signals which consider a performance approach to convert the original speech signals to encrypted signals and vies versa.

Additionally, the comparison and analysis reports are reviewed in this paper to illustrate which algorithm is selected to improve the security of a chaotic system.

References

[1] Lin, C.Y.; Yu, H.H.; Zeng, W. “Multimedia Security Technologies for Digital Rights Management”; Academic Press: Cambridge, MA, USA, 2006.

[2] Yasser, I., Mohamed, M.A., Samra, A.S. and Khalifa, F., ”A chaotic-based encryption/decryption framework for secure multimedia communications”. Entropy, 22(11), p.1253.2020.

[3] Mokhnache, S., Daachi, M.E.H., Bekkouche, T. and Diffellah, N.,” A Combined Chaotic System for Speech Encryption”. Engineering, Technology & Applied Science Research, 12(3), pp.8578-8583. 2022

[4] H. O. Alanazi, B. B. Zaidan, A. A. Zaidan, H. A. Jalab, M. Shabbir, and Y. Al-Nabhani, "New Comparative Study Between DES, 3DES and AES within Nine Factors," Journal of Computing, vol. 2, no. 3, pp. 152– 157, Mar. 2010.

[5] P. Patil, P. Narayankar, Narayan D.G., and Meena S.M., "A Comprehensive Evaluation of Cryptographic Algorithms: DES, 3DES, AES, RSA and Blowfish," Procedia Computer Science, vol. 78, pp. 617–624, Jan. 2016, https://doi.org/10.1016/j.procs.2016.02.108.

[6] Al-Hazaimeh, O.M.,”A new dynamic speech encryption algorithm based on Lorenz chaotic map over internet protocol”. International Journal of Electrical & Computer Engineering (2088-8708), 10(5). 2020.

[7] O. M. Al-Hazaimeh, ”Increase the security level for real-time application using new key management solution,”International Journal of Computer Science Issues (IJCSI), vol. 9, no. 3, pp. 240-246, 2012.

[8] O. M. Al-Hazaimeh, “New cryptographic algorithms for enhancing security of voice data,” Thesis, Universiti Utara Malaysia, 2010.

[9] R. Dantu, et al., Issues and challenges in securing VoIP”, Computers & Security, vol. 28, no. 8, pp. 743-753, 2009.

[10] O. M. Al-Hazaimeh, “Combining audio samples and image frames for enhancing video security,” Indian Journal of Science and Technology, vol. 8, no. 10, p. 940, 2015.

[11] Ahmed, S. and Abdualazize, S., “Preventing Unauthorized Access to Special Applications using Signed Audio”. International Journal of Civil Engineering and Technology (IJCIET), CiteScore, 2.

[12] Al-Hazaimeh, O.M., Abu-Ein, A.A., Nahar, K.M. and Al-Qasrawi, I.S. “Chaotic elliptic map for speech encryption”. Indonesian Journal of Electrical Engineering and Computer Science, 25(2), pp.1103-1114, 2022.

[13] Gebereselassie, S.A. and Roy, B.K. “A new Secure Speech Communication Scheme Based on Hyperchaotic Masking and Modulation”. IFAC-PapersOnLine, 55(1), pp.914-919, 2022.

[14] Zaid, O.A., Tawfeek, M.A. and Alanazi, S., “Applying and Comparison of Chaotic-Based Permutation Algorithms for Audio Encryption”. Computers, Materials and Continua, 67(3), pp.3161-3176, 2021.

[15] Al-Hazaimeh, O.M., “A new speech encryption algorithm based on dual shuffling Hénon chaotic map”. International Journal of Electrical and Computer Engineering (IJECE), 11(3), pp.2203-2210, 2021.

[16] Adhikari, S. and Karforma, S., “A novel audio encryption method using Henon–Tent chaotic pseudo random number sequence”. International Journal of Information Technology, 13(4), pp.1463-1471, 2021.

[17] Khaleel, A.H. and Abduljaleel, I.Q., “A novel technique for speech encryption based on k-means clustering and quantum chaotic map”. Bulletin of Electrical Engineering and Informatics, 10(1), pp.160-170, 2021.

[18] Kassim, S., Megherbi, O., Hamiche, H., Djennoune, S. and Bettayeb, M, “Speech encryption based on the synchronization of fractional-order chaotic maps”. In 2019 IEEE International Symposium on Signal Processing and Information Technology (ISSPIT) (pp. 1-6). IEEE, December ,2019.

[19] Wang, X. and Su, Y.” An audio encryption algorithm based on DNA coding and chaotic system”. IEEE Access, 8, pp.9260-9270, 2019.

[20] Nagakrishnan, R. and Revathi, A.,” A robust speech encryption system based on DNA addition and chaotic maps”. In International Conference on Intelligent Systems Design and Applications (pp. 1070-1080), December 2018, Springer, Cham.

[21] Fang D, Sun S. “A new secure image encryption algorithm based on a 5D hyperchaotic map”. PLoS One;15(11):e0242110. doi: 10.1371/journal.pone.0242110. PMID: 33180840; PMCID: PMC7661057. Nov 12, 2020.

[22] Lagmiri, S.N. and Bakhous, H., “Audio Encryption Algorithm Using Hyperchaotic Systems of Different Dimensions”. In CS & IT Conference Proceedings (Vol. 8, No. 15). CS & IT Conference Proceedings, November, 2018.

[23] Abbas, N.A. and Razaq, Z.H. “Speech Scrambling Based on Arnold-Lucas Mapping”. In 2018 International Conference on Advanced Science and Engineering (ICOASE) (pp. 290-295). IEEE, 2018, October.

[24] Dawood, Z.M., Aboud, M. and Hasan, F.S., “Speech encryption using finite precision chaotic maps based stream ciphers”. In Proceedings of the International Conference on Information and Communication Technology (pp. 127-133), 2019, April.

[25] Alemami, Y., Mohamed, M.A., Atiewi, S. and Mamat, M. “Speech encryption by multiple chaotic maps with fast fourier transform”. Int. J. Electr. Comput. Eng, 10(6), pp.5658-5664, 2020.

[26] Sathiyamurthi, P. and Ramakrishnan, S.” Speech encryption using chaotic shift keying for secured speech communication”. EURASIP Journal on Audio, Speech, and Music Processing, 2017(1), pp.1-11, 2017.

[27] Adhikari, S. and Karforma, S. “A novel audio encryption method using Henon–Tent chaotic pseudo random number sequence”. International Journal of Information Technology, 13(4), pp.1463-1471, 2021.

[28] Hosny, K.M., Kamal, S.T., Darwish, M.M. and Papakostas, G.A., “New image encryption algorithm using hyperchaotic system and fibonacci q-matrix”. Electronics, 10(9), p.1066, 2021.

[29] S. F. Yousif, “Speech encryption based on zaslavsky map,” Journal of Engineering and Applied Sciences, vol. 16, no. 7, pp. 6392-639, 2019.

[30] E. Hato and D. Shihab, “Lorenz and rossler chaotic system for speech signal encryption,” International Journal of Computer Applications, vol. 128, no. 11, pp. 25-33, 2015.

[31] M. Farouk, O. Faragallah, O. Elshakankiry, and A. Elmhalaway, “Comparison of audio speech cryptosystem using 2-D chaotic map algorithms,” Mathematics and Computer Science, vol. 1, no. 4, pp. 66-81, 2016.