Speech Scrambling Employing Lorenz Fractional Order Chaotic System

Prof. Maher K. M. AlAzawi
University Of Al – Mustansiriya
College Of Engineering
Electrical Engineering Department

Jaafar Qassim Kadhim
University Of Al – Mustansiriya
College Of Engineering
Electrical Engineering Department

Abstract :

This paper presents techniques of speech scrambling based-fractional order chaotic system which is used due to many properties; first of all using fractional order as key will increase key space which makes it is very difficult to decrypt by a 3d-party. It is a random like noise behavior; it is defined over continuous number fields, which leads to possibility of using many nonlinear functions in encryption. A one channel with chaotic masking is used to encrypt low level speech signal. The low level speech signal problem is solved by using two-channel secure communication. In a two channel method, one channel is used for transmitting a pure driving signal to achieve faster synchronization while a highly nonlinear function is used to encrypt the speech signal and transmit it in the other channel. The simulation results show that scrambled speech is unintelligible, preserving bandwidth, the dynamic response of fractional order chaotic system is highly sensitive to fractional order values and the variation of a parameter, chaotic trajectory is very unpredictable, key space is expanded and guaranteed higher security. The results show that, the speech scrambling based fractional order chaotic system is highly secure compared with classical speech scrambling techniques. Some security measures are used for comparison.

Keywords: - Speech Scrambling, Fractional Order Chaotic System, Synchronization

تشفير الكلام باستخدام نظام لورينز الفوضوي ذي الرتب الكسرية

أ. ماهر خضير محمود العزاوي
الجامعة المستنصرية / كلية الهندسة
قسم الهندسة الكهربائية

جعفر قاسم كاظم
الجامعة المستنصرية / كلية الهندسة
قسم الهندسة الكهربائية

الخلاصة :

يتناول هذا البحث تشفير الكلام باستخدام نظام فوضوي ذي رتب كسرية، وتم استخدامه بسبب الكثير من الخصائص اولا وقبل كل شيء استخدام الرتب الكسرية كمفتاح مما يزيد من سعة المفتاح وهذا يصعب عملية فك التشفير بالنسبة للمتنصت، عشوائية ومشابهة لسلوك الضوضاء، معرفة ضمن مجال الاعداد الحقيقية المستمرة وهذه الخاصية تمكننا من استخدام الكثير من الدوال غير الخطية في عملية التشفير. تم استخدام قناة ارسال واحدة مع طريقة الاخفاء الفوضوي لتشفير اشارة الكلام قليلة السعة. تم حل مشكلة اشارة الكلام قليلة السعة باستخدام قناتي ارسال للاتصال الامن وفي هذه الطريقة تم استخدام احدى قناتي الارسال لارسال اشارة التزامن فقط للحصول على تزامن سريع. استخدمت دوال غير خطية عالية لتشفير اشارة الكلام وتم ارسالها عن طريق القناة الاخرى. أظهرت نتائج المحاكاة ان اشارة الكلام المشفرة غير مفهومة وتمت المحافظة على نطاق الحزمة الترددية والاستجابة الديناميكية لنظام لورينز الفوضوي ذي الرتب الكسرية حساس للغاية لقيم الرتب الكسرية وقيم المعالم، صعوبة التنبؤ بمسار الفوضى، توسعة في المفتاح مع ضمان امنية عالية. اظهرت النتائج الامنية العالية لتشفير الكلام باستخدام نظام فوضوي ذي رتب كسرية مقارنة مع طرائق تشفير الكلام التقليدية. استخدمت بعض المقاييس الامنية لغرض المقارنة.

1. Introduction :

The design of efficient voice security methods demands new challenges which can provide high security to the voice data. To achieve this, a number of voice encryption techniques have been suggested. In general, there are four categories of cryptographic algorithms widely used in speech communication, namely frequency domain, time domain, amplitude scrambling, and two-dimensional mixed scrambling methods [1]. Among them, the chaos-based techniques are considered efficient for dealing with bulky, redundant voice data. This is because that the chaotic systems are characterized with high sensitivity to its initial conditions, ergodicity, random behavior, and long periodicity [2].

Chaos is a typical behavior of nonlinear dynamic systems. It is characterized by extremely sensitive to parameters and initial conditions, mathematically defined as randomness governed by simple deterministic rules [3]. A high dimensional chaotic system like Lorenz system will give a more complex structure, more system variables, and parameters. Then the cryptosystem's key space will be larger for integer orders, and the system variables time sequence will be more erratic and unpredictable than using the low-dimension chaotic system[4]. To increase the security level fractional order chaotic Lorenz system (Non integer orders) can be used. The advantage of using fractional order chaotic systems in communication is that the derivative orders can be used as secret keys as well. The results are increasing the key space and hence enhance the security level of communication.

2. Fractional Order Lorenz System :

The mathematical description of the fractional-order Lorenz system is expressed as [4] :-

$$\begin{aligned} D^{\alpha 1}x &= \sigma(y - x) \\ D^{\alpha 2}y &= -xz + \rho x - y \\ D^{\alpha 3}z &= xy - \beta z \end{aligned} \qquad (1)$$

where (σ, ρ, β) are system parameters , (α_1, α_2 and α_3 determine the fractional orders of the equation and (α_1, α_2, $\alpha_3 > 0$) . When $\alpha_1 = \alpha_2 = \alpha_3 = 1$, Equation (1) becomes the ordinary integer orders Lorenz system, the solution of fractional-order Lorenz system using Fractional Backward Difference Methods can be written as [5-6] :-

$$\begin{aligned} x_m &= h^{\alpha 1} * [\sigma * (y_{m-1} - x_{m-1})] - \sum_{k=1}^{m} w_k x(m - kh) \\ y_m &= h^{\alpha 2} * [-z_{m-1} * x_{m-1} + \rho * x_{m-1} - y_{m-1}] - \sum_{k=1}^{m} w_k y(m - kh) \\ z_m &= h^{\alpha 3} * [x_{m-1} * y_{m-1} - \beta * z_{m-1}] - \sum_{k=1}^{m} w_k z(m - kh) \end{aligned} \qquad (2)$$

where h, is step size parameter and m = 0,1,2,..,N.
The coefficients w_k can be computed in a recursive scheme (with $w_0 = 1$) by

$$w_k = \left(1 - \frac{\alpha+1}{k}\right) w_{k-1} \qquad (3)$$

3. Synchronization in Chaotic Systems :

The concept of using synchronization methods in communication schemes is based on the idea that two similar circuits or state space systems, one at the transmitter and the other at the receiver, can have at any particular time, the same dynamical state.

The earliest and the simplest form of synchronization is a Complete Synchronization[7]. This occurs in coupled identical systems and is also referred to as a conventional synchronization or an identical synchronization. Two continuous-time chaotic systems:

$\dot{x}(t) = F(x(t))$ and $\dot{\hat{x}}(t) = F(\hat{x}(t))$ are said to obtain Complete Synchronization if:

$\lim_{t\to\infty}[\hat{x}(t) - x(t)] = 0$

The fractional Lorenz system (system 1) is given by

$$D^{\alpha 1}x = \sigma(y - x)$$
$$D^{\alpha 2}y = -xz + \rho x - y \qquad \text{system 1}$$
$$D^{\alpha 3}z = xy - \beta z$$

The first signal x (t) of (System 1) is chosen as synchronization signal to drive another Lorenz system (System 2).

$$D^{\alpha 1}x_r = \sigma(y_r - x_r)$$
$$D^{\alpha 2}y_r = -xz_r + \rho x - y_r \qquad \text{system 2}$$
$$D^{\alpha 3}z_r = xy_r - \beta z_r$$

Systems (1) and (2) are called master and slave systems, respectively. The master-slave system is shown in Figure (1). It is noted that the slave system (y_r, z_r) is dependent on the signal x (t).

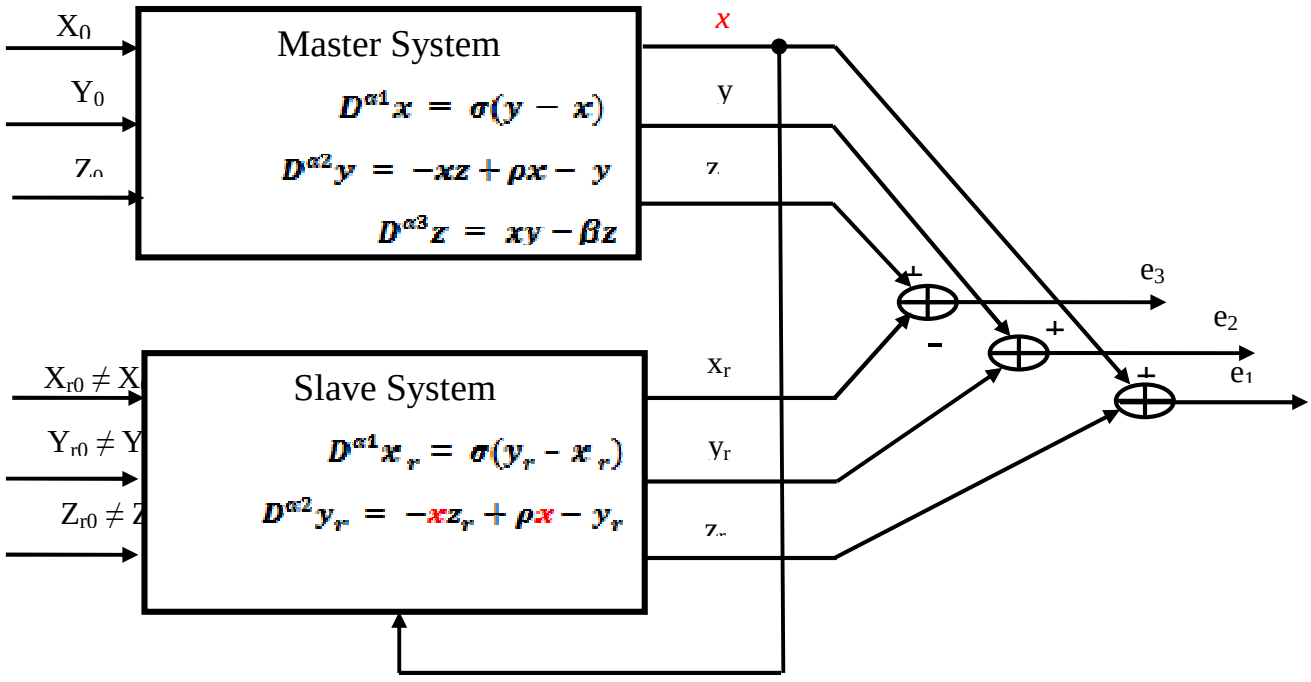

Fig. (1): The Lorenz Three-Dimensional Chaotic Master-Slave System.

Define the state errors between the master and slave system as

$$\begin{aligned} e_1 &= x - x_r \\ e_2 &= y - y_r \\ e_3 &= z - z_r \end{aligned} \tag{4}$$

Subtracting system (2) from system (1) leads to

$$\begin{aligned} D^{\alpha 1} e_1 &= \sigma(e_2 - e_1) \\ D^{\alpha 2} e_2 &= -x e_3 - e_2 \\ D^{\alpha 3} e_3 &= x e_2 - \beta e_3 \end{aligned} \tag{5}$$

By taking Laplace transform of both side of system (5) and rearranged,

$$L[D^{\alpha} e_i] = s^{\alpha} E_i(s) - s^{\alpha-1}\ e_i(0)$$

gets

$$\begin{aligned} E_1(s) &= \frac{\sigma\, E_2(s)}{s^{\alpha 1} + \sigma} + \frac{s^{\alpha 1 - 1} e_1(0)}{s^{\alpha 1} + \sigma} \\ E_2(s) &= \frac{-L[x e_3]}{s^{\alpha 2} + 1} + \frac{s^{\alpha 2 - 1} e_2(0)}{s^{\alpha 2} + 1} \\ E_3(s) &= \frac{L[x e_2]}{s^{\alpha 3} + \beta} + \frac{s^{\alpha 3 - 1} e_3(0)}{s^{\alpha 3} + \beta} \end{aligned} \tag{6}$$

Using the final value theorem of Laplace transform, it follows that

$$\begin{aligned} \lim_{t\to\infty} e_1(t) &= \lim_{s\to 0} s E_1(s) = \lim_{s\to 0} s E_2(s) = \lim_{t\to\infty} e_2(t) \\ \lim_{t\to\infty} e_2(t) &= \lim_{s\to 0} s E_2(s) = -\lim_{s\to 0} s L[x e_3] \\ \lim_{t\to\infty} e_3(t) &= \lim_{s\to 0} s E_3(s) = \frac{1}{\beta} \lim_{s\to 0} s L[x e_2] \end{aligned} \tag{7}$$

Now, owing to the attractiveness of the attractors of master system and slave system, Since $E_1(s)$, $E_2(s)$ and $E_3(s)$ are bounded, then

$$\lim_{t\to\infty} e_1(t) = \lim_{t\to\infty} e_2(t) = \lim_{t\to\infty} e_3(t) = 0 \tag{8}$$

Figure (2) shows the synchronization of master and slave systems. It is shown that the master and slave systems have been synchronized after the initial synchronization time which is about four seconds.

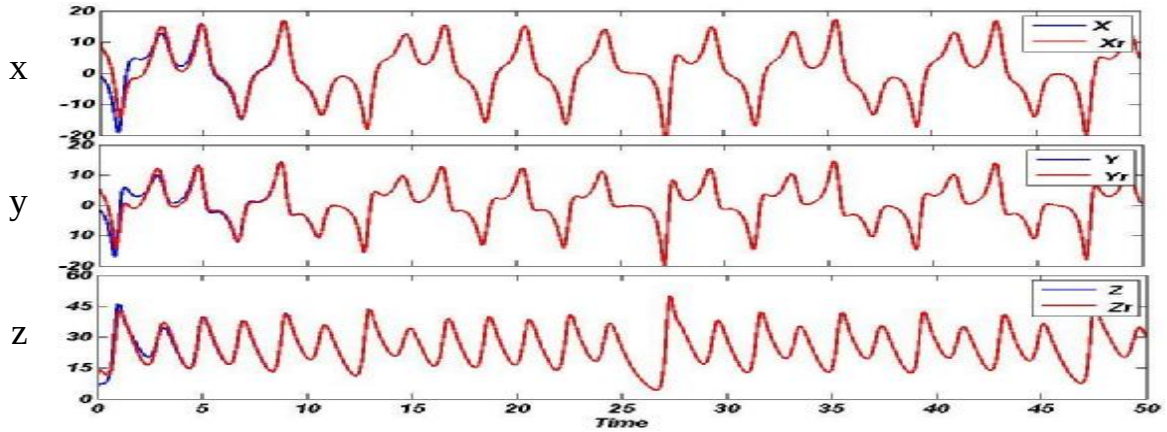

Fig. (2): The Response and Synchronization of the Master and Slave systems.

4. Fractional order chaotic Cryptosystem :

Different methods for implementing chaotic secure communication will be discussed, such as chaotic masking; improved chaotic masking and two-channel secure communication methods since these methods form the foundation of chaotic communication and are very important to understand newer techniques. The fractional order chaotic cryptosystem is mainly composed of two parts: an encrypter and a decrypter. The details of each part are described as follows:-

4.1 Encrypter

The encrypter uses fractional order chaotic Lorenz system as generator, to generate x, y and z sequences and uses a highly nonlinear or linear function to encrypt the original speech depending on the number of channels used. This will be described in Section (5) and Section (6).

The equations of fractional Lorenz system as encrypter are given as:-

$$D^{\alpha 1}x = \sigma(y - x)$$
$$D^{\alpha 2}y = -xz + \rho x - y$$
$$D^{\alpha 3}z = xy - \beta z$$

4.2 Decrypter

The slave system in decrypter is defined by the following equations

$$D^{\alpha 1}x_r = \sigma(y_r - x_r)$$
$$D^{\alpha 2}y_r = -x_r z_r + \rho x_r - y_r$$
$$D^{\alpha 3}z_r = x_r y_r - \beta z_r$$

5. One-Channel Secure Communication :

Most of the chaotic secure communication uses one channel. The advantage of communication with one channel is high efficiency of the channel and the encryption structure is simple. But common shortcoming is that the driving signal is distorted by the information signal. One channel secure communication uses the following techniques:-

5.1 Chaotic Masking

Chaotic masking involves the addition of a message signal *s(t)* to a chaotic carrier signal *x*, before the transmission of the sum of the two signals takes place [8]. The block diagram illustrating the principles of chaotic masking is shown in Figure (3).

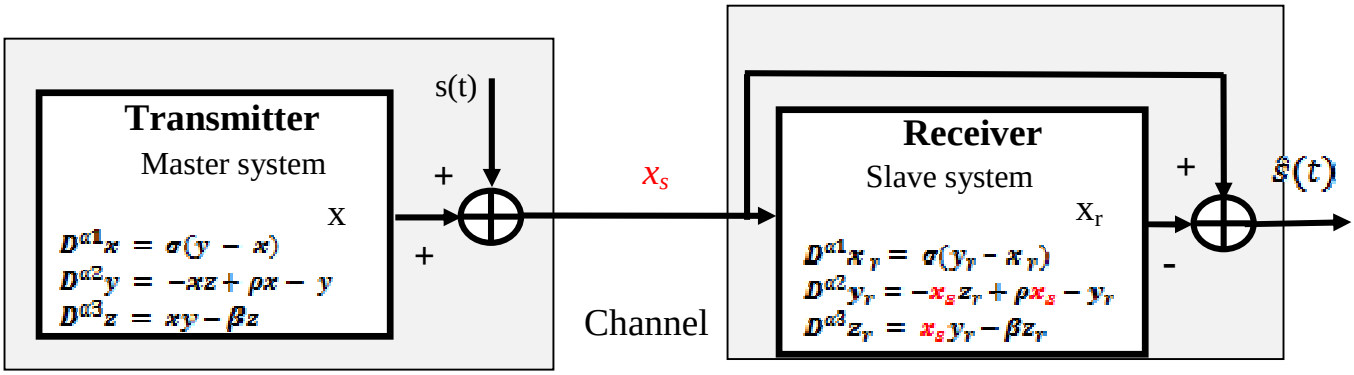

Fig. (3): Block Diagram of the Chaotic Communication System Based on the Chaotic Masking.

The slave system of the receiver generates a signal x_r which is expected to be synchronized with the corresponding master signal *x* of the transmitter. After a sufficient amount of time has passed for *x* and x_r to synchronize, the transmitted message *s(t)* can be recovered in the form of:-

$$\hat{s}(t) = x_s - x_r = \big(x + s(t)\big) - x_r \cong \hat{s}(t) \qquad (9)$$

The requirement of a chaotic masking scheme is that the power of the information signal *s(t)* has to be significantly lower than the power of the chaotic carrier x(t). When the message power is big, the driving signal does not perfectly fit the receiver. On the one hand, the error of synchronization grows rapidly and stability of synchronization decreases as shown in **Figure (4).**

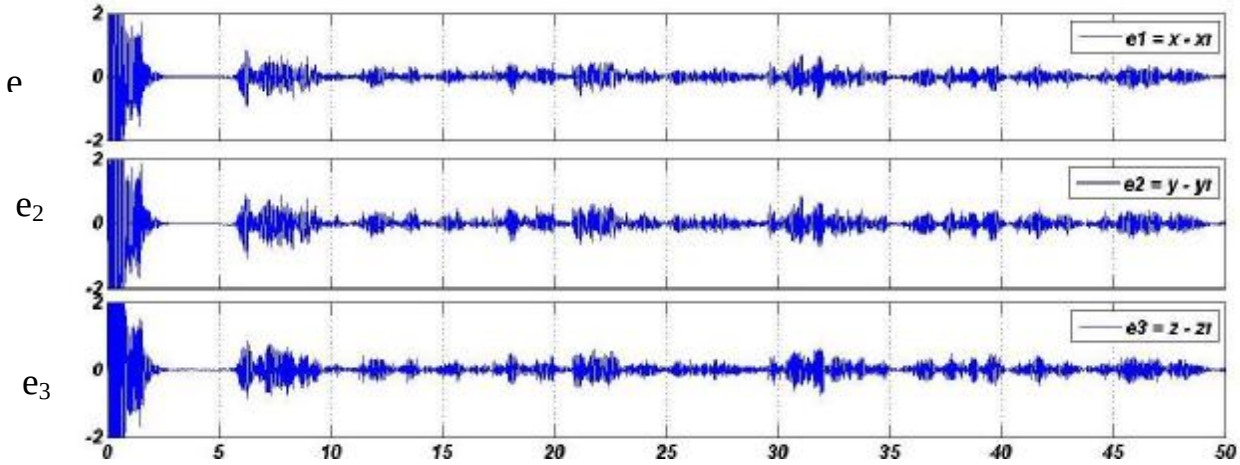

Fig.(4): The Error of Synchronization between Master and Slave Systems in One Channel Chaotic Masking.

5.2 Improvement of Chaotic Masking

To avoid the restriction of the small amplitude of the information signal, a modulation scheme, called Improvement of Chaotic Masking, has been proposed in [9] . As shown in **Figure (5)** in which the Lorenz system is used again as the chaotic generator, the basic idea is to feedback the information signal into the chaotic transmitter in order to have identical input signals for both the chaotic transmitter and the receiver. Specifically, the transmitted signal, consisting of the information signal s(t) and the chaotic signal x(t) is communicated to the receiver which is identical to the chaotic transmitter, as shown in **Figure (6).** Since the reconstructed signal $x_r(t)$ will be identical to x(t) , the information signal s(t) can be decoded from the received signal.

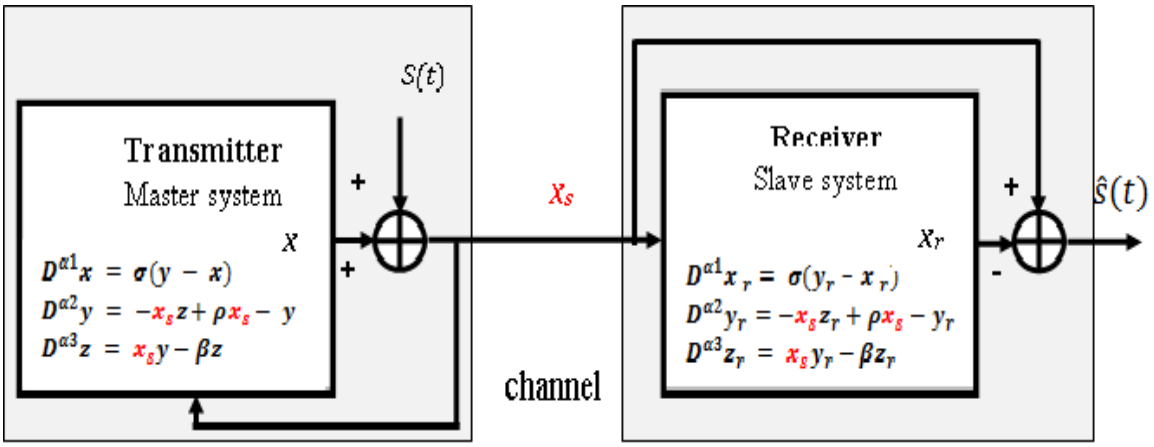

Fig. (5): Block Diagram of Improved Chaotic Masking Communication System.

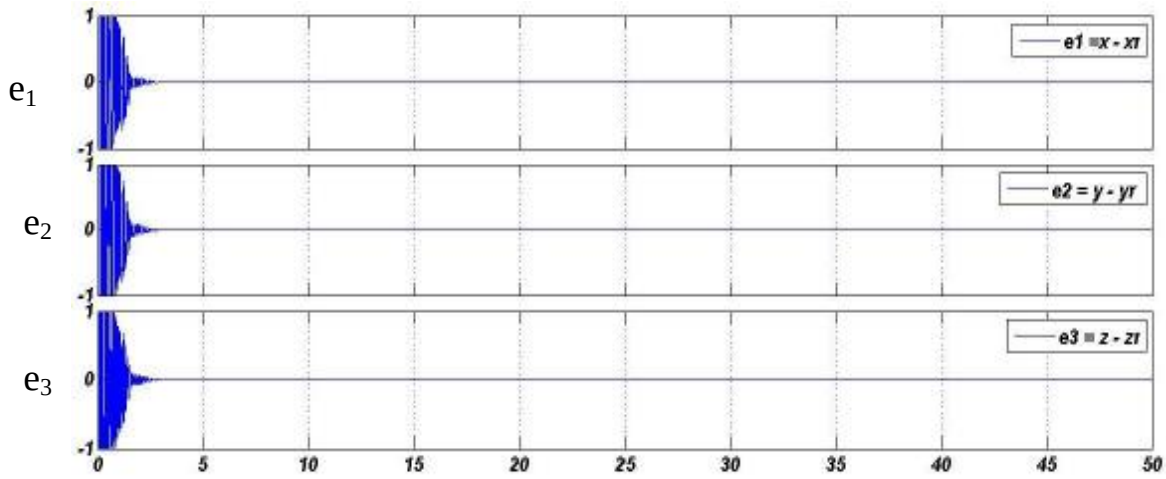

Fig. (6): The Error of Synchronization between Master and Slave Systems in One Channel Improvement Chaotic masking

6. Two-Channel Secure Communication :

Two-channel transmission method is adopted for the purpose of faster synchronization and higher security .One output of the chaotic transmitter is sent for synchronization only in one channel, with no connection with the information signal, so the amplitudes of information signal has nothing to do with synchronization. The other channel transmits the information - bearing signal. So the first channel serves the purpose of efficient synchronization, the second channel is used for complicated encryption and, therefore, improved security [10] . Figure (7) illustrates this idea. The public channel is used to transmit both *x* (the driving signal necessary for synchronization), and *E*, the encrypted secret message.

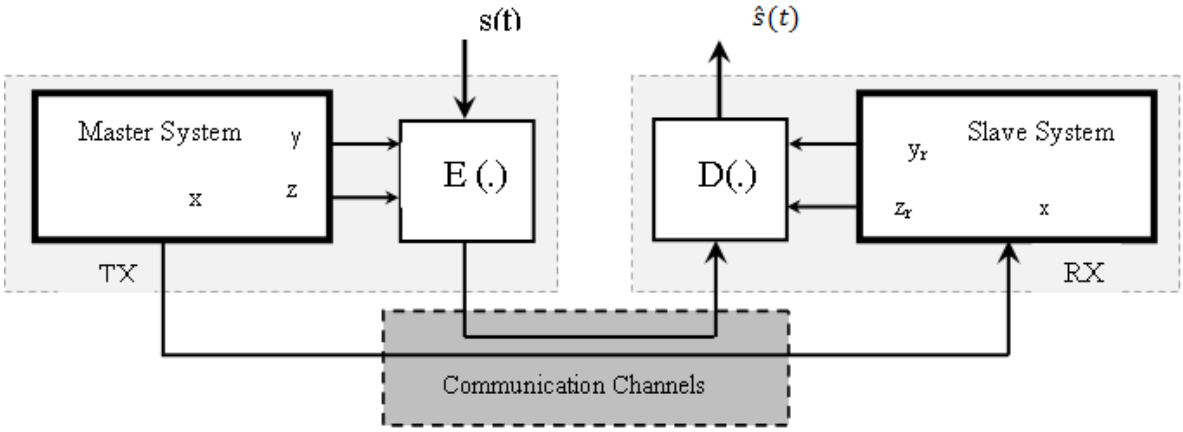

Fig. (7): A Block Diagram Representation of two channels Secure Communication System.

The encrypter uses *y(t)* and *z (t)* of master system to provide the desired key sequence. To further enhance the security of the cryptosystem, an encryption function is introduced such as [11] :-

$$E_1(y,z,s,t) = \frac{y(t) + s(t)}{z(t)} \qquad (10)$$

where $s(t)$ is the original speech. The cipher-speech is sent to the decrypter through the channel.

At the receiver, the recovered speech $\hat{s}(t)$ is derived by the decryption function via

$$\hat{s}(t) = D(E_1, y_r, z_r, t)$$
$$= E_1(y,z,s,t) * z_r(t) - y_r \qquad (11)$$

If the variables $y_r(t)$ and $z_r(t)$ of the slave system can be synchronized with corresponding variables *y(t)* and *z(t)* of the master system , the decrypter can find the same $\hat{s}(t)$, as in the encrypter, *s(t)*.

7. Modification of Two-Channel Chaotic Communication :

A better scrambling of the secret message can be obtained if the encryption function is made to depend on a continuously changing parameter along with the chaotic states of the transmitter. This parameter corresponds to one of the chaotic transmitter parameters and consequently it can accomplish two tasks:

1- To act as a cipher key that makes the scrambling process of the transmitted message more robust.
2- To continuously change the chaotic attractor of the transmitter; thus making it harder for an intruder to break into the communication channel.

Referring to the encryption function in Equation (12), it is noted that it is a simple nonlinear function. To complicate the process of cryptanalyst one may use a more complex nonlinear function resulting in a more robust secure communication system, given by [12] :

$$E = y^2 + (1 + y^2) * s(t) \quad (12)$$

Thus a modified system for the robust secure communication system,
Both the encryption and decryption functions are given in Equations (13) and (14).

$$E_2(y, \mu, s, t) = y^2 + (\mu^2 + y^2) * s(t) \quad (13)$$

$$\hat{s}(t) = D(y, \mu, s, t) = \frac{E_2(\hat{y}, \hat{\mu}, s, t) - \hat{y}^2}{(\hat{\mu}^2 + \hat{y}^2)} \quad (14)$$

Where μ , is the modified parameter.
y and μ are used to construct the nonlinear scrambling. The decryption function should settle very fast to the inverse of the encryption function, once synchronization is achieved.

8. Measures of Quality :

A number of quantitative measures can be used to evaluate the performance of the designed system. These are Segmental Spectral Signal to Noise Ratio (SSSNR), LPC Distance Measure, and Cpestral Distance Measure (CD). These measures are defined as follows:

a. Segmental Spectral Signal to Noise Ratio (SSSNR):

This is given by [13]

$$SSSNR_i = 10log \frac{\sum_{k=1}^{N} |X_i(k)|}{\sum_{k=1}^{N} [|X_i(k)| - |Y_i(k)|]} \quad [dB] \quad (15)$$

Where $X_i(k)$ & $Y_i(k)$ are the DFT of original speech & scrambling speech.

b. Linear Predicative Code Measure (LPC):

This is given by [14]

$$LPC = \ln\left(\frac{AVA^T}{BVB^T}\right) \quad [dB] \quad (16)$$

where *V* is the autocorrelation matrix of the original speech block, vectors *B* & *A* contain the LPC coefficients for the clear speech block and scrambled speech block.

c. Cpestral Distance Measure (CD):

This is given by [15]

$$CD = 10log_{10}\left[2\sum_{n=1}^{p}\{Cx(n) - Cy(n)\}^2\right]^{\frac{1}{2}} \quad [dB] \quad (17)$$

where *Cx(n)* & *Cy(n)* are the cpestral coefficients of the original speech and scrambled speech.

9. Simulation Results :

The simulation uses the following referencein(Arabic) speech file:-

" تطورت الحاسبات الالكترونية سريعا وأصبح استخدامها من الصفات المميزة لعصرنا الحديث "

The translation of is: **The computers have evolved rapidly and became a major characteristics of the modern era**

The speech signal is sampled at 8 kHz and (5.6879 seconds long having 45503 samples) with 16 bits / sample, as shown in Figure (8). In this simulation, the chaotic signal was simulated for 50 seconds with 50000 samples. Due to initial synchronization error shown in Figure (2), the first five seconds of the chaotic signal were neglected in encryption and decryption..

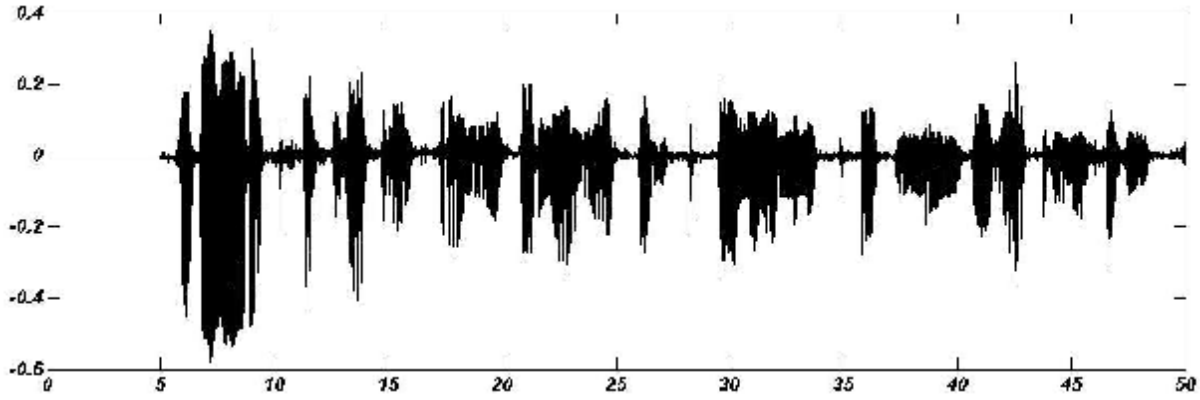

Fig. (8): Original Speech Signal.

9.1 Testing the Secret Keys of Lorenz System.

The secret keys of Lorenz system can be classified into:-

Parameters keys (σ, ρ, β) for integer order Lorenz system, (ii) Fractional orders (α_1 ,α_2 ,α_3). The first one is tested by Lyapunov Exponent methods [16] while the second one is tested by '0-1 Test' algorithm [17] as explained in the following sections.

9.1.1 Testing Parameters of Integer Order Lorenz System.

Chaotic system parameters are chosen carefully with a large positive Lyapunov exponent value. A chaotic system with a large exponent value means that the chaotic system with certain parameter values is sensitive to initial conditions and behavior chaotically. Computing and testing of these parameters (σ, ρ, β) for integer order Lorenz system by Lyapunov Exponent are shown in **Table (1).**

9.1.2 Testing Fractional Order Lorenz System.

The fractional orders (α_1, α_2 , α_3) is chosen arbitrary and the best choice must be closer to unity to achieve the chaotic behavior of system , the '0-1 Test' is used to obtain a results of (K) that is close to unity to get chaotic behavior, as shown in **Table (2).**

Table (1): Testing Parameters of Chaotic Lorenz System use Lyapunov Exponent.

σ	ρ	β	λ_1	λ_2	λ_3
10	28	8/3	1	0	-14.5
16	45.92	4	1.5	0	-22.44
12	37	3	1.14	0	-17.3
17	49.6	5.3	1.723	0	-24.95
20	57	7	2.05218	0	-29.97
26	63	8	2.36	0	-37.2
35	91	11	3.337	0.001	-50.188
51	86	7.6	2.856	0	-61.266
267	595	100	24.2	0.018	-22.4

Table (2): Testing Fractional Orders of Chaotic Lorenz System using "0-1" Test.

α_1	α_2	α_3	K
0.97	0.98	1.1	0.9889
0.95	0.96	1.05	0.9598
1.07	0.95	0.9	0.9617
0.965	1.06	0.88	0.9538
0.65	1.15	0.92	0.9368
1.05	1.08	1.12	0.9397
1.15	0.85	1.17	0.9627
0.95	0.97	0.98	0.9142
0.971	0.981	1.11	0.9572

Table (1) shows the arbitrary chosen values of (β), which must be positive, the values of (σ and ρ) are calculated accordingly, after calculating (λ_1 ,λ_2 ,λ_3) using Lyapunov Exponent the system was chaotic because [($\lambda_1 > 0$), ($\lambda_2 = 0$), ($\lambda_3 < 0$)]. The following choices of fractional derivative orders, parameters, and initial conditions for the master and slave systems are used for simulation.

(α_1 , α_2 , α_3) = (0.97, 0.98, 1.1). (σ , ρ , β) = (16 , 45.92 , 4).
[x(0) , y(0) , z(0)] = [−1,−2, 5]. [$x_r(0)$, $y_r(0)$, $z_r(0)$] = [1 , 2, 1].

9.2 Bandwidth Expansion Consideration:

In order to transmit the scrambling speech signal in an exiting channel with standard bandwidth, it is important that the scrambled speech should be real and should have a B.W essentially the same as that for the original speech. In classical speech scrambling, a trade-off between security and B.W expansion must be considered. In fractional order chaotic speech scrambling if the security is increased, then the B.W is not expanded and remained unchanged, due to the nature of chaotic signal characteristics. Figure (9) shows the B.W of the original speech signal and the B.W of transmitted signals due to fractional order chaotic speech scrambling.

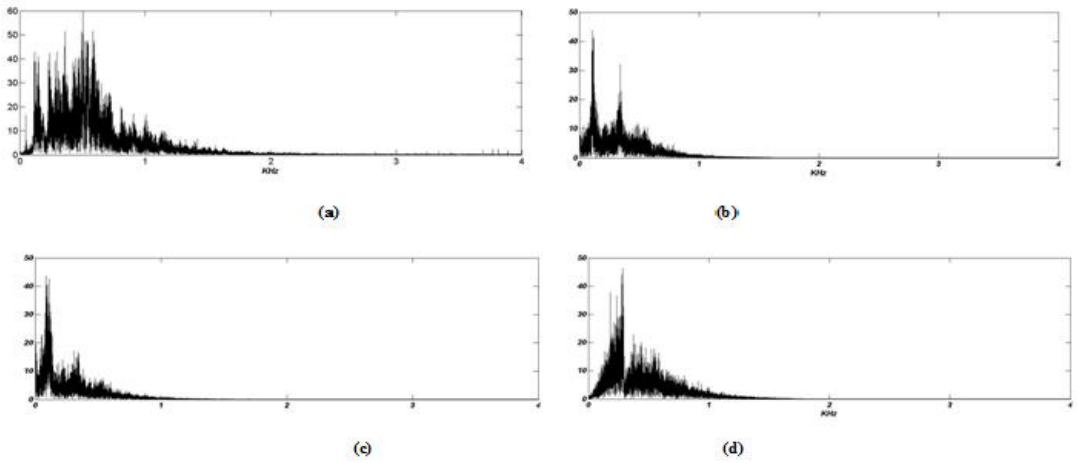

Fig.(9): (a) B.W of Original Speech Signal, (b) BW of Two Channel Secure Communication,(c) B.W of Modified Two Channel Secure Communication , and (d) BW of Fractional order chaotic Masking

9.3 Sensitivity to Fractional Orders

Two identical Lorenz systems (*a* & *b*) are taken with the same parameters and initial conditions but starting from different fractional orders (nearly identical however). The difference in fractional order taken between two Lorenz variables x_a and x_b was chosen to be 10^{-6}. Figure (10) depicts the time series of variables x_a and x_b for two Lorenz systems. After some period, the two variables quickly diverge from each other even though they started from identical fractional order. in particular, $\sigma_a = \sigma_b = 10$, $\rho_a = \rho_b = 28$, $\beta_a = \beta_b = 8/3$, $\alpha_{a1} = \alpha_{b1} = 0.97$, $\alpha_{a2} = 0.98$, $\alpha_{b2} = 0.980001$, $\alpha_{a3} = \alpha_{b3} = 1.1$.

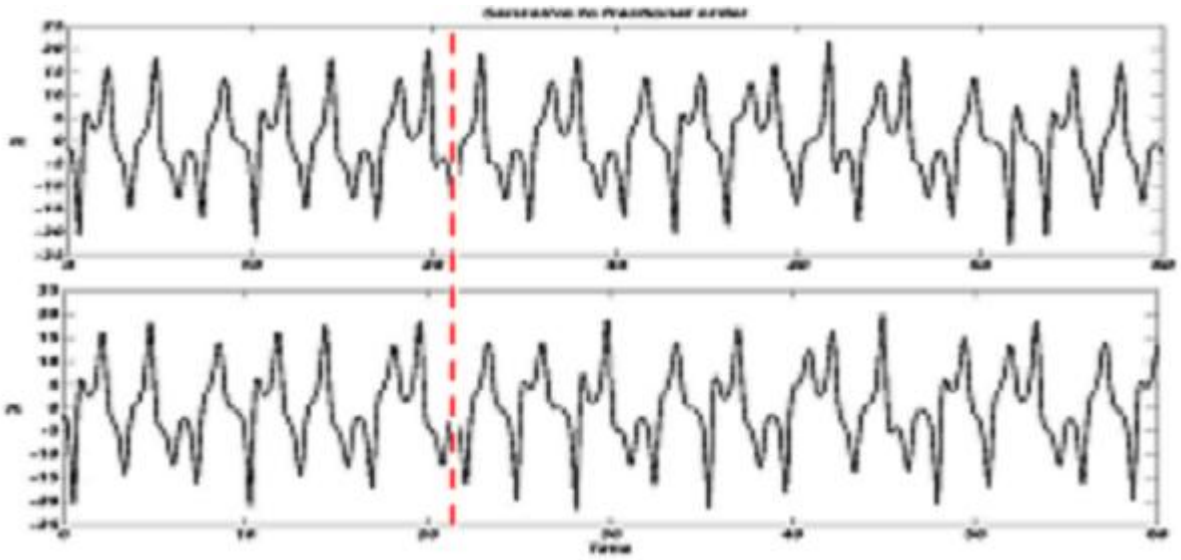

Fig. (10): Two Numerical Solutions of the Lorenz System Showing Sensitivity to fractional order.

9.4 Comparison between Classical Speech Scrambling and Speech Scrambling based Fractional Order Chaotic System.

The scrambled speech is tested by using the three measures discussed in section (8). The encrypter results for classical speech scrambling and speech scrambling based fractional order chaotic systems are depicted in Tables (3) and (4) respectively. Table (3) shows the results for classical speech scrambling; time domain scrambling, frequency domain scrambling and two dimensional scrambling. In all of these cases the analysis takes place at narrow band scrambling. It is noted from Table (3) that the residual intelligibility is increased when using two dimensional scrambling methods.

Table (4) shows the results for chaotic speech scrambling which includes; chaotic masking, improved chaotic masking, two channel secure communication and, modified two channel secure communication.

Table (3): Simulation Results of Classical Speech Scrambling.

Encrypted speech signal			
	LPC	CD	SSSNR [dB]
1-Time domain scrambling	0.6562	2.4373	0.9754
2-Frequency domain scrambling	0.5723	2.5075	-0.2935
3-Two dimensional scrambling	0.6732	3.2269	-1.9443

Table (4): Speech Scrambling based Fractional Order Chaotic System.

Encrypted speech signal			
	LPC	CD	SSSNR [dB]
1- chaotic Masking	0.8367	4.4776	-19.6577
2- Improved Chaotic Masking	0.8535	4.6820	-21.4244
3- Two channel secure communication	0.8676	4.8073	-22.2537
4- Modified Two channel secure communication	1.2294	5.5290	-20.0252

From the simulation results obtained from the given Tables(3) and (4) there is an explanation about the big difference in the results between the classical speech scrambling and speech scrambling -based chaotic system, this is described as follows:-

1- A chaotic system has a random-like noise behavior.
2- Chaos –based encryption schemes can be defined over continuous number fields, which lead to the possibility of using many nonlinear functions in encryption.

10. Cryptanalysis :

This section presents a cryptanalysis study of the fractional order chaotic scrambling. The analysis focuses on the determination of the key space, and the key sensitivity.

10.1 Key Space

In a good encryption scheme, the key space should be large enough. In the present scheme, the encryption sequences, x, y and z, are generated from the fractional Lorenz system with fractional derivative orders $(\alpha_1, \alpha_2, \alpha_3)$ and the parameters (σ, ρ, β). The fractional derivative orders can be used as secret keys as well. Hence, the secret key consists of six numbers $(\alpha_1, \alpha_2, \alpha_3, \sigma, \rho, \beta)$. Since these six numbers are real numbers, the space of the keys will be a 6-dimensional space. Large secret key parameter space is very important to prevent an exhaustive search attack.

10.2 Key Sensitivity

Key sensitivity is an essential property for any good cryptosystem, which ensures the security of the cryptosystem against brute-force attacks. To demonstrate the key sensitivity,

only one parameter of key is changed at a time by a tiny amount, keeping all other parameters of key unchanged and the scheme is applied to recover the speech signal. Key sensitivity can be described in the following cases:

Case 1:-

Consider an intruder intercepts both the ciphertexts and synchronization signals. Assume the intruder gets an approximate estimate of the keys, If the fractional order $\alpha_{r3,}$ is changed to a value [(1± %1) *α_3], then all chaotic techniques are affected, where results shown in **Table (5). Figure (11)** shows the sensitivity of present secure communication scheme to a slight mismatch of keys. It is noted that the recovered speech signal is totally different from the original speech signal.

Case 2:-

If the fractional order $\alpha_{r2,}$ is changed by a value [(1± %1) *α_2], then all the chaotic techniques are affected, the recovered speech signal of all fractional order chaotic speech scrambling is totally different from the original speech signal. The results are shown in **Table (6)**

Table (5): Mismatch fractional order α_{r3} by (±1%).

Encrypted speech signal Recovered speech signal			
	LPC	CD	SSSNR [dB]
1- chaotic Masking	0.7968	4.4160	-18.1685
2- Improved Chaotic Masking	0.8877	3.6963	-12.8760
3- Two channel system	0.7516	4.5238	-17.2380
4- Modified Two channel system	1.1072	4.1787	-9.1470

Table (6): Mismatch fractional order α_{r2} by (1%).

Recovered speech signal			
	LPC	CD	SSSNR [dB]
1- chaotic Masking	0.7497	4.4177	-18.0192
2- Improved Chaotic Masking	0.8305	3.7275	-13.2377
3- Two channel system	0.7953	4.1998	-16.4438
4- Modified Two channel system	0.9811	4.5023	-11.6848

From Tables (5) and(6) ,where the mismatching in the fractional orders (α2 , α3) are (±1%) , the recovered speech signal of all fractional order chaotic speech scrambling suffered a strong distortion due to high sensitivity to fractional order .

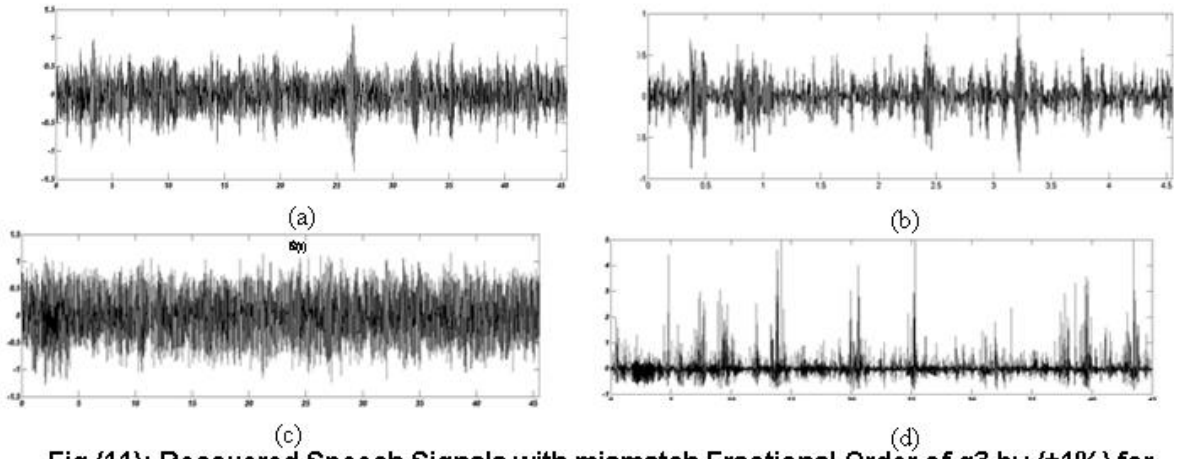

Fig.(11): Recovered Speech Signals with mismatch Fractional Order of α3 by (±1%) for :- (a) Chaotic Masking (b) Improved Chaotic Masking (c) Two Channel Secure Communication (d) Modified Two Channel Secure Communication

Case 3:-

If the parameter $\beta_{r,}$ is changed to a value [(1± %2) *β], then all chaotic technique are affected, the results are shown in Table (7).

Case 4:-

If the parameter $\rho_{r,}$ is changed to a value [(1± %2) *ρ], then only chaotic masking and dynamic feedback modulation are affected. But when $\rho_{r,}$ is changed to a value [(1± %5) *ρ] , then all the chaotic techniques are affected , the results are shown in Table(8).

Table (7): Mismatch parameter β_r by (2%).

Recovered speech signal			
	LPC	CD	SSSNR [dB]
1- chaotic Masking	0.6138	3.3653	-14.2837
2- Improved Chaotic Masking	0.7255	3.9502	-16.0411
3- Two channel system	0.7529	4.2037	-19.6325
4- Modified Two channel system	0.9259	4.3579	-10.4579

Table (8): Mismatch parameter ρ_r by (±5%).

Recovered speech signal			
	LPC	CD	SSSNR [dB]
1- chaotic Masking	0.6138	3.3653	-12.3420
2- Improved Chaotic Masking	0.7255	3.9502	-14.5183
3- Two channel system	0.6451	3.8137	-10.6324
4- Modified Two channel system	0.7332	4.0276	-8.7619

Tables (5), (6), (7) and (8) show that the speech scrambling techniques based-fractional order chaotic Lorenz system are very sensitive to key (parameters & fractional orders). This feature gives robust encryption and the attacker doesn't able to recover the original speech signal.

Conclusion :

In this paper, high dimensional chaotic system like Lorenz is employed to generate more complex and unpredictable three chaotic sequences. The use of speech scrambling

with chaotic techniques decreases the Segmental Spectral Signal to Noise Ratio Measure in the encrypted speech signal by about -16dB and increases Cpestral Distance Measure by about 1.5 dB compared with classical speech scrambling. preserving bandwidth operation, the dynamic response of fractional order chaotic system is highly sensitive to fractional order values and the variation of a parameter, chaotic trajectory is very unpredictable. With the use of fractional derivative order as the keys the key space is expanded and guarantees higher security. This system has a large key sensitivity because a small change in the secret key causes a large change in the encrypted signal.

References

1. **M. J. Orceyre & R. M. Heller "An Approach to Secure Voice Communication Based on the Data Encryption Standard",** ***IEEE Communications Society Magazine,*** **pp. 41–50, 1978.**
2. **Tariq .M.K " Objective Tests of Speech Signal " M.Sc. Thesis, College of Engineering Al-Mustansiriya University, Department of Electrical Engineering, Iraq, Baghdad, October 2001.**
3. **S. H. Strogatz, "Non linear dynamics and chaos" Preseus Books Publishing, LLC, 1994.**
4. **Nicholas R. "Introduction to Lorenz's System of Equations", Math 6100, December 2003,**
5. **Marc W. "Efficient Numerical Methods for Fractional Differential Equations and their Analytical Background". Ph.D. Thesis, Technical University of Braunschweig, Germany, 2005.**
6. **Igor Podlubny "Fractional Differential Equations", Slovak Republic, Academic Press 1999..**
7. **S. Boccaletti & C. S. Zhou, "The synchronization of chaotic systems,"** ***Physics Reports,*** **vol. 366, pp. 1-101, 2002.**
8. **B. Jovic "Synchronization Techniques for Chaotic Communication Systems", Springer-Verlag Berlin Heidelberg. 2011.**
9. **Jiu C. F. "Reconstruction of Chaotic Signals with Applications to Chaos-Based Communications", Tsinghua University Press and World Scientific Publishing Co. Pte. Ltd., 2008.**
10. **Liao Ni-huan "A Hybrid Secure Communication Method Based on Synchronization of Hyper-Chaos Systems", International Conference on Communication Systems and Network Technologies. pp. 289-293. 2012.**
11. **Long J. S. "A speech encryption using fractional chaotic systems" Springer Science & Business Media B.V. pp. 103-108. 2010.**

12. **Long J. S. & Wei C. C.“A Two-Channel Secure Communication Using Fractional Chaotic Systems” World Academy of Science, Engineering and Technology 65 2010.**

13. **S. Sridharan & E. Dawson & B. Goldburg “Fast Fourier transform based speech encryption system” IEE Proc-I, Vol. 138, No. 3, JUNE 199, pp. 215-223, JUNE 1991.**

14. **M. R. Sambur & N. S Jayant “ Speech Encryption by Manipulations of LPC parameters ” Bell System Technical J., Vol. 55, pp. 1373-1389. November 1976.**

15. **A. Matsunaga, K. Koga & M. Ohkawa “An Analog Speech Scrambler Using the FFT Technique with High-Level Security” IEEE J. on selected area in communication, Vol. 7. No.4, pp. 540-547 , May 1989.**

16. **Q.V. Lawande & B. R. Ivan “Chaos Based Cryptography: A New Approach to Secure Communications” , BARC Newsletter 2005**

17. **Sun Ke-Hui & Zhu Cong-Xu “The 0-1 Test algorithm for Chaos and its Applications”, Chinese Physical Society and IOP Publishing Ltd Vol. 19, No. 11 2010.**