International Journal of Information and Communication Sciences
2016; 1(2): 16-21
http://www.sciencepublishinggroup.com/j/ijics
doi: 10.11648/j.ijics.20160102.11

Digital Chaotic Scrambling of Voice Based on Duffing Map

Amina Mahdi[1], Ameer K. Jawad[2], Saad S. Hreshee[1]

[1]Electrical Engineering Department, College of Engineering, University of Babylon, Babylon, Iraq

[2]Computer Engineering Department, Islamic University College, Najaf -Iraq

Email address:
eng.saad.saffah@uobabylon.edu.iq (S. S. Hreshee)

To cite this article:
Amina Mahdi, Ameer K. Jawad, Saad S. Hreshee. Digital Chaotic Scrambling of Voice Based on Duffing Map. *International Journal of Information and Communication Sciences.* Vol. 1, No. 2, 2016, pp. 16-21. doi: 10.11648/j.ijics.20160102.11

Received: June 15, 2016; **Accepted:** June 18, 2016; **Published:** August 26, 2016

Abstract: With the significant development in communication systems especially in the public channels through which our information travels, there are more increasing in the channels problems. The information security is the important one that should be enhanced. This paper presents a chaos-based speech scrambling system. Chaotic maps have been successfully used for large-scale data encryption such as image, audio and video data, due to their good properties such as pseudo-randomness, sensitivity to changes in initial conditions and system parameters and a periodicity. In this paper a security model based on chaotic system has been designed to be used to encrypt voice signal, chaotic duffing map used for digital Scrambling, each samples of the speech are divided into 8 bits. The simulation results show that the Cpestral Distance Measure (CD) in the proposed system is increased by (4.559) by comparing with the time domain scrambling which is about four times that gives from the analog scrambling. In addition, d_{lpc} increased to (4.428) as comparing with time domain. The key space in this proposed is $11.8336 * 10^{64} \times$ range of parameters.

Keywords: Speech, Secure Communication, Scrambling, Chaos, Duffing Map

1. Introduction

Security is the first goal in any communication system. To get secure system the information that transmitted must be pass through different types of encryption techniques. Sending encrypted voice or information, need to send the encrypted signal with a public key that must be known in the other side of the communication system (receiver), but again there is an unreal user (Eavesdropper) attacks the channel to get this information. This is the main problem in the cryptography.

Cryptographic algorithms can be divided into four types widely used in speech communication, these are frequency domain, time domain, amplitude scrambling, and two-dimensional mixed scrambling methods that combines frequency and time domain scrambling [1].

One of the important algorithms for cryptography is based on using chaotic systems that depends on chaos technique. Chaos is a typical concept used to describe deterministic dynamical systems whose of complex behavior, unpredictable and extremely sensitive to initial conditions [2].

The traditional chaos based cryptographic systems are effective for the text data. But they fail in providing the same security level for the voice data due to the high redundancy and bulk data capacity of voice. Therefore, the efficient voice security design will has new challenges. Can the proposed system provides high security to the voice signal? To realize this, a number of voice encryption techniques have been studded [3-16]. From these researches, the chaotic system was regarded as an efficient technique for voice data. They provide high secure techniques. This is because of that the chaotic techniques have a high sensitivity to any change in its initial conditions, in addition to the other properties such as random behavior, ergodicity, and the long periodicity.

In this paper one level of security is used to encrypt the input signal which this level is digital chaotic scrambling in order to increase the key space.

2. The Proposed System Model

In this proposed digital scrambling with the chaotic map used to encrypt the input signal. The encrypted signal will be transmitted through the channel to the receiver. In the receiver side, the signal, which encrypted will be descrambled according to chaotic map in order to recovered

the voice see fig. (1).

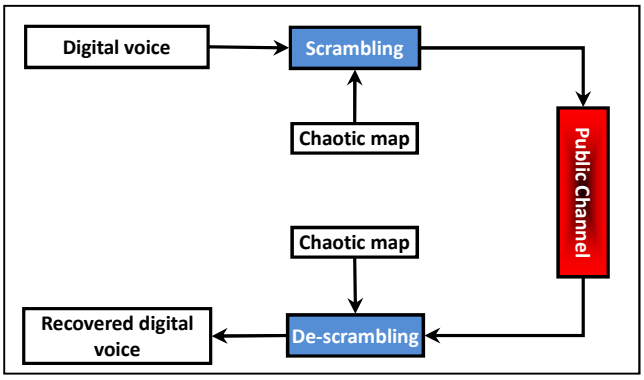

Fig. 1. *The proposed of digital security model based on multi chaotic maps.*

3. Digital Chaotic Scrambling

Returning to fig. 1, the voice messages are first digitized and converted into binary data sequences. These binary sequences are scrambled according to the chaotic scrambling algorithm. Chaotic scrambling algorithm in this design is based on using any type of chaotic maps. In this paper duffing map (Holmes map) is used in this stage. The reason of using chaotic map instead of chaotic flow as mentioned above is the discrete time system.

Duffing map is one of the chaotic functions, which is expressed as [6]:

$$\left.\begin{aligned} x_{n+1} &= y_n \\ y_{n+1} &= -bx_n + ay_n - {y_n}^3 \end{aligned}\right\} \quad (1)$$

where $b = 0.15\ and\ a = 2.75$

The digital chaotic scrambling algorithm is:

Step 1: The voice will be converted to digital, this voice has a number of samples FS (frequency sampling) and each sample has N bits (8-bits) in this paper, which will be scrambled according to Duffing map. For example if a sample has the value 0.6139 in decimal. To convert to binary (8-bit), first, the number multiplied by 256 or (2^8). In this case 0.6139 will be $(116)_{10}$ and that equal to $(0\ 1\ 1\ 1\ 0\ 1\ 0\ 0)_2$ in binary numbers. These bits then scrambled according to the chaotic scrambled algorithm explained below.

Step 2: at the transmitter, chaotic map will be generated with length equal to voice length. For example for N=8, and Duffing map given by equations (1) with initial condition:

$x(1) = 0.11\ \&\ y(1) = -0.5$, as shown in table (1):

Table 1. *The generated sequence Duffing map.*

n	1	2	3	4	5	6	7	8
x_n	0.11	-0.5	-1.2665	-1.3736	-0.9876	-1.5461	-0.4074	-0.8209
Data	0	1	1	1	0	1	0	0

Step 3: The results of the chaotic vector will be sorted ascedingly as shown in table (2):

Table 2. *The resorted the chaotic vector.*

n	6	4	3	5	8	2	7	1
x_n	-1.5461	-1.3736	-1.2665	-0.9876	-0.8209	-0.5	-0.4074	0.1100

According to that sorting the index of the values will be changed, these indices are the interleaving look up table for both transmitter and the receiver, For N=8 the LUT is shown in table (3):

Table 3. *The interleaving look up table for the sorted indices for both transmitter and the receiver*

input index	1	2	3	4	5	6	7	8
output index	6	4	3	5	8	2	7	1
1st stage (hashed data)	1	1	1	0	0	1	0	0

Step 4: After the scrambling stage, the bits will be $(1\ 1\ 1\ 0\ 0\ 1\ 0\ 0)_2$ which is equal $(228)_{10}$ which is began with $(116)_{10}$, which will be transmitted to the second stage of encryption.

4. Measuring the Performance of the System

The performance of the system must be studded in two important features:

a). Sensitivity of the chaos system for any very small change in the initial condition can be achieved by Lypunov Exponents.

b). Measuring the quality of the speech by computing the performance of the designed system concerning the security in channel. The most familiar technique to evaluate the quality are Segmental Spectral Signal to Noise Ratio (SSSNR), LPC Distance Measure, and Cpestral Distance Measure (CD).

4.1. Lyapunov Exponents (Key Sensitivity)

Lyapunov characteristic exponent of a system is a measurement for all the elements of chaos and sensitivity dependence on their initial states. Lyapunov characteristic exponents are a measurement of the separation of two close

trajectories in terms of initial conditions. The separation δ(t) of such two trajectories occurs very faster as time progresses [17].

Consider two points, $x_n(t)$ and $x_n(t) + \Delta x_n(t)$, are on the attractor at time t, so exploiting this property of chaos by making each number of this high sensitivity a key space so we will have a very high key space. For duffing map when changing the initial condition by (10^{-16}) from (0.1) to (0.1000000000000001) the behavior is shown in Fig. (2).

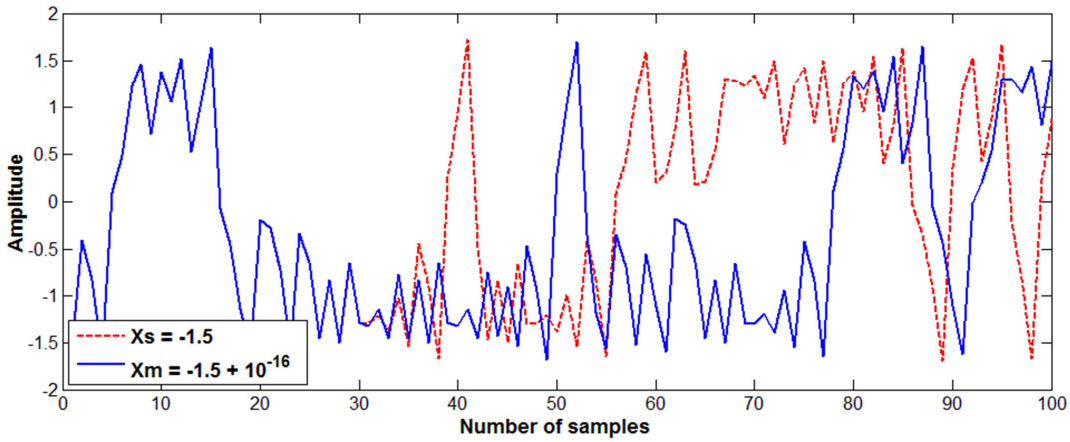

Fig. 2. *Duffing map, with slightly change in of about 10^{-16} between x_m and x_s.*

Fig. 2 illustrates that any small change $\Delta = (10^{-16})$ in the initial conditions will give another path that cannot be predicted. Therefore, it is explaining that chaotic systems are high sensitivity for the initial condition. The sensitivity proportional to the key space $K_i = \frac{1}{S_i} * R_i$ where R_i is rang of function for each dimension of any key which is the distance between the maximum and minimum value of the chaotic map and $S_i = 10^{-16}$ is a sensitivity in each dimension.

4.2. Quality of Speech

A number of quantitative measures can be used to evaluate the performance of the designed system concerning the security in channel. These three measurements are Segmental Spectral Signal to Noise Ratio (SSSNR), LPC Distance Measure, and Cpestral Distance Measure (CD). These measures are defined as follows [5, 18]:

4.2.1. Segmental Spectral Signal to Noise Ratio (SSSNR)

$$SSSNR_i)_{dB} = 10log \frac{\sum_{k=1}^{N}|X_i(k)|}{\sum_{k=1}^{N}[|X_i(k)|-|Y_i(k)|]} \quad (2)$$

where $X_i(k)$ & $Y_i(k)$ are the DFT of original signal & recovered signal respectively [5, 18, 19].

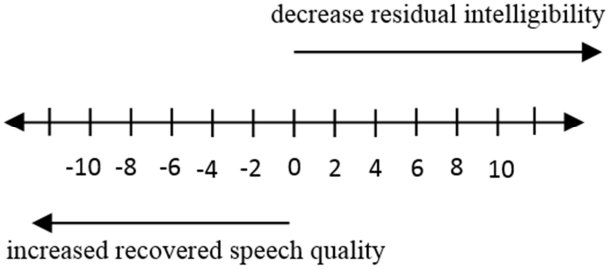

Fig. 3. *SSSNR Measure [5].*

4.2.2. Linear Predicative Code Measure (LPC)

$$d_{lpc} = \ln\left(\frac{AVA^T}{BVB^T}\right) \quad (3)$$

where *V* is the autocorrelation matrix of the original speech block, vectors A&B contain the LPC coefficients for the clear speech block and recovered or encrypted speech block respectively [20].

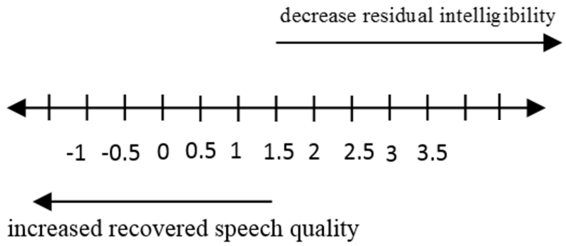

Fig. 4. *LPC Distance Measure [5].*

4.2.3. Cpestral Distance Measure (CD)

$$CD = 10log_{10}\left[2\sum_{n=1}^{p}\{C_x(n) - C_y(n)\}^2\right]^{\frac{1}{2}} \quad (4)$$

where $C_x(n)$ & $C_y(n)$ are the cpestral coefficients of the original signal and recovered or encrypted signal respectively[21].

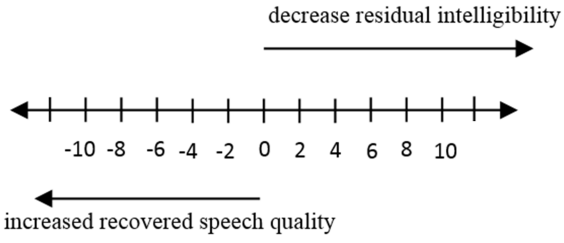

Fig. 5. *Cepstral Distance Measure [5].*

5. Simulation Results

A simulation model based on block the system shown in fig.1 has been implemented using MATLAB. The performance of the proposed systems are shown and discussed. The voice used in this test has 8 KHz sampling frequency and 5 seconds length (40000 samples) each sample has 8-bits.

5.1. Speech Residual Unintelligibility (Security)

Unintelligibility of speech is an important factor, which it can be tested by using the three measurements, which decrypted in the section 3.2. In this system, voice will be recovered by three receive types:

1. Eavesdropper who is any person (any R_X) does not has any key (just convert encrypted bits to voice).
2. Attacker who is a person has a key with extremely small difference with the original key in any dimensions of keys.
3. Goal receiver who is a person (original receiver) who has the exact keys in all dimensions.

5.2. Residual Unintelligibility for the Proposed System Digital Chaotic Scrambling

The corresponding results for the Digital chaotic scrambling appear the unintelligibility of speech to the Attacker and Eavesdropper shown in Table (4).

From table (1) we show that By changing one of the initial condition of the duffing map the difference between the Eavesdropper and the Attacker (0.097) in d_{lpc} and (0.005) in CD. While the difference between the Attacker and goal receiver (4.955) in d_{lpc} and (10.494) in CD. This calculation give indication that the Attacker will be closer to the Eavesdropper and remote then the goal receiver which that we need. Also, it is worth mentioning that the $SSSNR_{dB}$ in the receiver is (31.44dB) that due to converting the voice from analog to digital.

Table 4. *Digital chaotic scrambling using one sample converted to 8bits.*

R_x	Difference in any initials	d_{Lpc}	$SSSNR_{dB}$	CD
Eavesdropper	Any value	5.082	0.5013	6.996
Attacker known all initials	$\Delta(all) = 0$	0.0297	31.44	-3.503
	$\Delta(x) = 10^{-16}$	4.985	0.496	6.896
	$\Delta(y) = 10^{-16}$	4.959	0.4774	6.885
	$\Delta(a) = 10^{-16}$	4.988	0.476	6.991
	$\Delta(b) = 10^{-16}$	4.972	0.436	6.898
Goal Receiver	0	0.0297	31.44	-3.503

The Attacker will be closer to the value of Eavesdropper and remote to the value of the receiver this resist the Attacker to recover the original voice such as discussed in the previews sections. To display that Duffing map used in digital chaotic scrambling equation (1) where $x_m = 0.5$ and $y_m = 0.1$. Slight change in initial condition either x_m or y_m will result in inability of recovering the original speech, as shown in Fig. 6.

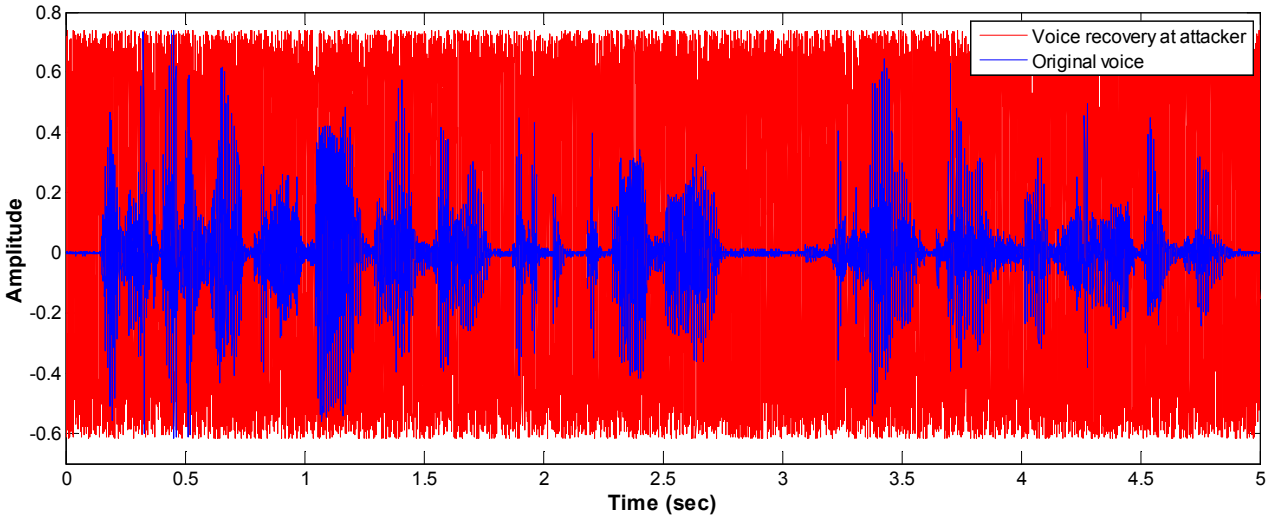

Fig. 6. *Digital chaotic scrambling, (a) original speech with* $x_m = 0.5$ *and* $y_m = 0.1$ *(b) red line recovered speech with* $x_s = 0.5$ & $y_s = 0.1 + 10^{-16}$.

Fig. (6) show that any small change in the initial condition will due to impossibility to recover the original information, this is due to the high sensitivity of chaotic map, which discussed in details in Lyapunov exponents.

6. Cryptanalysis (Testing the Secret Keys and Sensitivity)

Key space analysis is one of the important criteria of the performance analysis of encryption system. A good encryption algorithm should have a large key space, and should be sensitive to the key value. The key space of the encryption system should be large enough to resist the Attacker. Key sensitivity means that the encrypted signal cannot be decrypted correctly if there is any change between encryption and decryption keys. Large key sensitivity is required by all secure cryptosystems [22, 23]. In another word to display the key sensitivity, only one factor of key, initial condition of x_m or y_m is changed by a tiny amount;

this simple change cannot retrieve information by the Attacker [24].

The key space in one dimension:

$$\mathrm{K} = \frac{1}{\mathrm{S}} * \mathrm{R} \tag{5}$$

where K is a key for each dimension, $S = 10^{-16}$ is the sensitivity in each dimension, R is rang of function for each dimension of any key which is the distance between the maximum and minimum value of the chaotic map. So that:

$$K = 10^{16} * R$$

The key space for d dimension

$$K_d = \prod_{i=1}^{d} K_i = \prod_{i=1}^{d} [(10^{16}) * R_i] \tag{6}$$

Then

$$K_d = (10^{16})^d \prod_{i=1}^{d} [R_i] \tag{7}$$

The key space in chaotic scrambling based on duffing map, and this map has 2 vectors and 2 parameters, therefore the key space have 4 dimensions:

$$\mathrm{K_d} = (10^{16})^4 \prod_{\mathrm{i=1}}^{4} [\mathrm{R_i}]$$

$$K_d = (10^{16})^4 (3.44)^2 * R_a * R_b = 11.8336 * 10^{64} * R_a R_b$$

where $\mathrm{R_a} * \mathrm{R_b}$ is the range of parameters depends on the bifurcation theorem [17] for each function of chaotic maps.

7. Comparison of the Proposed System with Traditional Encryption Systems

In order to compute the performance of the proposed by computing the ability of this system to encryption, in other word computing the key space of this proposed system, So it should be compared with the other traditional systems used in speech encryption. The traditional methods considered are time domain scrambling, frequency domain scrambling and, two-dimensional scrambling, chaotic scrambling (analog), our proposed method is digital chaotic scrambling. Table (5) illustrates the comparison between traditional methods that used for encryption in the voice clip that have been studied in [5, 18] and our method.

Table 5. *Illustrates the comparison between traditional methods and proposed methods.*

Classical Scrambling	d_{Lpc}	$SSSNR_{dB}$	CD
Time Scrambling	0.6532	0.9754	2.4373
Frequency Scrambling	0.5723	-0.2935	2.5075
Two Dimensional Scrambling	0.6732	-1.9443	3.2269
Analog Chaotic Scrambling	0.6087	-4.2272	3.4406
Digital Chaotic scrambling	5.082	0.5013	6.996

This table above shows that the traditional methods, which is used, for encryption have very low ability as compared with the chaos system encryption, the proposed system gives very strength ability for encryption. The CD in the analog chaotic scrambling is increased by (1.003) from (2.4373 to 3.4406) by comparing with the time scrambling while in this stage (Digital chaotic scrambling) increased by (4.559) from (2.4373 to 6.996) in comparing with the time domain which is about four times that gives from the analog scrambling. By comparing the results with the d_{lpc} also we show that in the analog scrambling the d_{lpc} decreased to (-0.044) from (0.6532 to 0.6087) in comparing with the time domain while d_{lpc} increased to (4.428) from (0.6532 to 5.082) as comparing the proposed with time domain. The key space will be high greater than used in traditional methods because the key space depend on the dimensions the key space over all system is have 4 dimensions.

$$\mathrm{K_4} = (10^{16})^4 (3.44)^2 \mathrm{R_a R_b}$$

$$\mathrm{K_4} = 11.8336 * 10^{64} \mathrm{R_a R_b}$$

8. Conclusions

In this paper, a high-efficient secure communication system based on digital chaotic scrambling was designed. Using the chaos techniques in any communication system result in high encryption level because any slight change in any parameter or initial condition in the chaotic map, will give another path that can't be predicted. This is a great strength of the encryption.

In addition, chaotic map has more than one dimension, each dimension gives high key space so for this system its gives very high key space due to the two dimensions in the duffing map used in this paper.

The encryption strength with chaotic masking show better behavior when compared with the classical methods, in addition to the comparison with analog scrambling methods and at the same time, it does not affect the bandwidth of the information.

Finally, it must be noted that the scrambling cannot combine the three advantages (security, real time and bandwidth) at the same time.

References

[1] R. Gnanajeyaraman, K. Prasadh, Dr. Ramar, "Audio Encryption Using Higher Dimensional Chaotic Map", International Journal of Recent Trends in Engineering, Vol. 1, No. 2, PP. 103 -107, May 2009.

[2] H. Bai-Lin, "Chaos", World Scientic, Singapore Vol. I (1984) and Vol. II (1989).

[3] Maher K. M. Al-Azawi, Jaafar Qassim Kadhim, "Speech Scrambling Employing Lorenz Fractional Order Chaotic System", Journal of Engineering and Development, Vol. 17, No. 4, PP. 195-211, ISSN 1813- 7822, October 2013.

[4] Q. H. Lin, F. L. Yin, T. M. Mei and H. Liang, (2006) "A Blind Source Separation Based Method for Speech Encryption", IEEE Transaction on circuits and systems-I, Vol. 53, No. 6, pp. 1320–1328.

[5] Hikmat N. Abdullah, Saad S. Hreshee, Ameer K. Jawad, "Design Of Efficient Noise Reduction Scheme For Secure Speech Masked By Chaotic Signals", Journal of American Science 2015; Vol. 11, Issue 7, pp. 49-55.

[6] J. I. Guo, J. C. Yen and H. F. Pai, (2002) "New Voice over Internet Protocol technique with Hierarchical Data Security Protection", IEE Proceedings Vision, Image & Signal Processing, Vol. 149, No. 4, pp. 237–243.

[7] K. W. Wong, K. P. Man, S. Li and X. Liao, (2005) "A more Secure Chaotic Cryptographic scheme based on Dynamic Look-up table", Circuits, Systems and Signal Processing, Vol. 24, No. 5, pp. 571–584.

[8] K. W. Tang, and W. K. S. Tang, (2005) "A Chaos-based Secure Voice Communication System", International Conference on Industrial Technology, pp. 571–576.

[9] K. P. Man, K. W. Wong and K. F. Man, (2006) "Security Enhancement on VoIP using Chaotic Cryptography", International Conference on Industrial Electronics, pp. 3703–3708.

[10] H. F. Qi, X. H. Yang, R. Jiang, B. Liang, and S. J. Zhou, (2008) "Novel End-to-End Voice Encryption Method in GSM System", International Conference on Networking, Sensing and Control, 217–220.

[11] Hikmat N. Abdullah and Sarab K. Mahmood, "Performance Evaluation of Non-redundant Error Correcting Scheme Using Logistic Chaotic Map", Wireless Personal Communications, An International Journal, Volume 86, Issue 3, pp 1169-1181, February 2016.

[12] Liu J. & Ma H. "A Speech Chaotic Encryption Algorithm based on Network", Proceedings of IIHMSP, IEEE press, Harbin, China, pp. 283–286, 2008.

[13] Rahul Ekhande and Sanjay Deshmukh, "Chaotic Signal for Signal Masking in Digital Communications", International organization of Scientific Research (IOSR), PP. 29-33, Vol. 04, February. 2014.

[14] F. Palmieri, and U. Fiore, (2009) "Providing true end-to-end security in converged voice over IP infrastructures", Computers & Security, Vol. 28, No. 6, pp. 433–449.

[15] M. Ahmad and Izharuddin, (2010) "Randomness Evaluation of Stream Cipher for Secure Mobile Communication", International Conference on Parallel, Distributed and Grid Computing, pp. 165–168.

[16] S. Mukhopadhyay and P. Sarkar, (2006) "Application of LFSRs for Parallel Sequence Generation in Cryptologic Algorithms", Applied Cryptography and Information Security, LNCS, Vol. 3982, pp. 426–435.

[17] Rahul Ekhande, Sanjay Deshmukh, "Chaotic Signal for Signal Masking in Digital Communications", International organization of Scientific Research Journal of Engineering, Vol. 4, Issue. 2, PP. 29-33, February, 2014.

[18] Jaafar Q. K., "Speech Scrambling Employing Lorenz Fractional Order Chaotic System", M.Sc. Thesis, AL-Mustansiriya University, Electrical Engineering Department, 2013.

[19] Mahmoud. M. "Analysis and Design Security Primitives Based on Chaotic Systems for ecommerce", Ph.D. Thesis, School of Engineering and Computing Sciences, Durham University, United Kingdom, 2012.

[20] S. H. Strogatz, "Nonlinear dynamics and chaos" preseus Books publishing, LLC, 1994.

[21] 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.

[22] S. Sridharan & E. Dawson & B. Goldburg "Fast Fourier Transform Based Speech Encryption System" IEE Proc-I, Vol. 138, No. 3, pp. 215-223 JUNE 1991.

[23] Chuan p., Yuanxiang L., "A new algorithm for image encryption based on couple chaotic system and cellular automata", Mechatronic Sciences, Electric Engineering and Computer (MEC), Proceedings 2013 International Conference on IEEE, PP. 1645 - 1648.

[24] G. Heidari-Bateni and C. D. Mc Gillem, "A chaotic direct-sequence spread-spectrum communication system" IEEE Transactions on Communications, Vol. 42, Issue, 234, PP. 1524 - 1527, 1994.