Design of Efficient Noise Reduction Scheme for Secure Speech Masked by Chaotic Signals

Hikmat N. Abdullah [1], Saad S. Hreshee [2], Ameer K. Jawad [3]

[1.] College of Information Engineering, AL-Nahrain University, Baghdad-Iraq
[2.] Department of Electrical Engineering, Babylon University, Babylon-Iraq
[3.] Department of Electrical Engineering, AL-Mustansiryah University, Baghdad-Iraq
E-mail: dr.h.abdullah@ieee.org

Abstract: To achieve efficient transmission through public channels, the communication system should have ability to overcome many problems. Among these problems, the security and the noise are the most challenging ones. In this paper, an efficient communication system with high security and high immunity against noise based on sample repetitions has been proposed. From security perspective, the simulation results show that the Segmental Spectral Signal to Noise Ratio **(**SSSNR) of Lorenz chaotic masking is reduced by 20.679 dB in comparison with time domain scrambling. Concerning the immunity against noise, the proposed system is based on conversion of information from analog to digital format before doing the masking. The simulation results of this method show that the mean square error (MSE) is reduced and this reduction increases as signal to noise ratio (SNR) increase. For instance when, SNR=10dB, MSE is reduced from 0.1 to 0.02 while it reduced from $5*10^{-3}$ to 10^{-6} when SNR=22dB.
[Abdullah H, Hreshee S, Jawad A. **Design of Efficient Noise Reduction Scheme for Secure Speech Masked by Chaotic Signals.** *J Am Sci* 2015;11(7):49-55]. (ISSN: 1545-1003). http://www.jofamericanscience.org. 7

Keywords: Key words: chaotic encryption, chaotic masking, speech quality, and Communication security

1. Introduction

Communications today are becoming more widespread and accessible, which brings about many advantages and unfortunately some restrictions that may be considered as disadvantages. The positive aspect is that more and more people can now communicate easily at any time. However, more traffic brings about problems with cross-talk, speech privacy, etc (Liu J. and Ma H., 2008, Gnanajeyaraman R. *et al*, 2009). These applications are critical with respect to integrity protection of speech data and privacy protection of authorized users. Hence, the need of high level security system of speech encryption is pre-requisite of any secure speech communication system to forestall these attacks.

One of the likely solutions that have association with the growth of a nonlinear communication system is chaos. Chaos is irregular behavior occurring over a long period of time in a deterministic system dependence on parameters and initial conditions, founded by Lorenz (Sprott, 2015). The communication security using chaos had been studied by many researchers. In 2012, Kohad *et al* (Kohad *et al*, 2012) designed a large set of Kasami sequence are generating from the polynomial by using chaotic map to speech encryption. In 2013, M. Al-Azawi and Kadhim J. (Al-Azawi and Kadhim, 2013) presented techniques of speech masking with chaotic signal based-fractional order to increase the key space. In 2014, Ekhande R. and Deshmukh S. (Ekhande and Deshmukh, 2014) presented work, uses Lorenz equation generated chaotic signals are used as a base carrier signal for information signal modulation in the T_X and R_X. However, all the works mentioned above did not consider the effect of additive noise.

This paper presents a proposed method to reduce the effect of noise on the speech signal that are masked by Lorenz chaotic signal using the principle of digital processing of speech signal. This method is abbreviated as DPCM which stands for Digital Processing Chaotic Masking.

2. The Proposed System Model

The proposed system model is shown in Figure 1. In this model, first the analog speech signal is converted to digital using ADC. Then the digital symbols are masked by chaotic signal generated from Lorenz chaotic system.

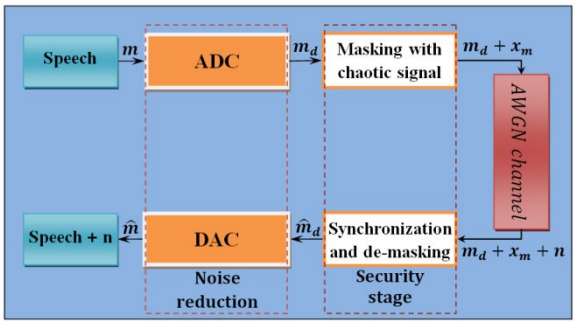

Figure 1: The block diagram of the proposed secure and noise reduction system using DPCM method

At the receiver side, the received masked signal plus AWGN noise is collected from the transmission channel. The mask is first removed using a

synchronized version of the chaotic signal available at the receiver. Then the binary data converted back to analog speech signal. This process will reduce the noise effect on the recovered speech as provide by the results presented in section IV.

A. Chaotic Masking

The block diagram of the designed chaotic masking scheme is shown in Figure 2. The speech signal $m(t)$is added to the Lorenz chaotic generator signal $X_m(t)$. which also acts as driving signal for synchronization purpose as will de explained later. the speech signal is precisely recovered at the receiver by the subtraction of the receiver's regenerated drive signal from the received signal (Rupak, 2011, Ekhande and Deshmukh, 2014).

In order to remove the mask successfully, chaotic signals on both Tx & Rx must be synchronized, one of the efficient synchronization schemes can be used to achieve this is Pecora-Carroll (PC) Synchronization (Pecora and Carroll, 1990, Jovic, 1996). In this scheme, a driving signal is sent from the chaotic generator at Tx, called master, to the chaotic generator at Rx, called slave. At the receiver, state error vectors which describe the difference between the master and slave state variables are constructed. Figure 3 shows the block diagram of PC synchronization scheme when Lorenz chaotic generator given in equation 1 is used.

$$\begin{aligned} \dot{x} &= \sigma(y - x) \\ \dot{y} &= rx - y - xz \\ \dot{z} &= xy - bz \end{aligned} \qquad (1)$$

where the $\dot{x}, \dot{y}$ *and* $\dot{z}$ are the states vector of Lorenz system and σ, r *and* b are the control parameters of Lorenz equations. The states errors are e_x, e_y, e_z are given by:

$$\begin{aligned} e_x &= x_m - x_s \\ e_y &= y_m - y_s \\ e_z &= z_m - z_s \end{aligned} \qquad (2)$$

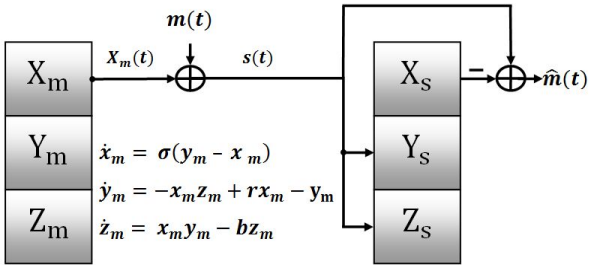

Figure 2: Chaotic masking and recovery information based on Lorenz system.

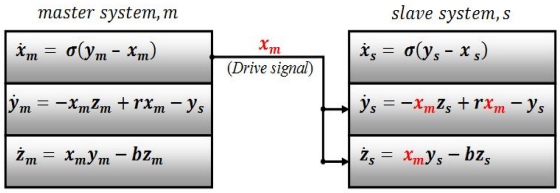

Figure 3: Mechanism of PC synchronization of Lorenz system**.**

It have been shown that with aid of the driving signal these states errors can be reduced to zero after a certain amount of time as shown in Figure 4.

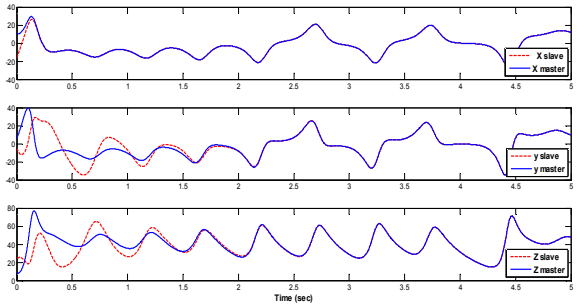

Figure 4: The synchronization error of $(x, y \text{ and } z)$ in the master and slave Lorenz systems.

Coming back to Figure 3, the received signal is

$$s(t) = x_m(t) + m(t) \qquad (3)$$

and recovered speech signal is:

$$\begin{aligned} \hat{m}(t) = s(t) - x_s(t) &= [m(t) + x_m(t)] - x_s(t) \\ &= m(t) + e(t) \end{aligned} \qquad (4)$$

$$where \quad e_x(t) = x_m(t) - x_s(t)$$

Figure 5 illustrates the original speech signal $m(t)$, chaotic signal $x_m(t)$, masked information with chaotic masking $s(t)$ and reassembled speech $\hat{m}(t)$. $e_x(t)$ is produced due to the fact that the presence of information signal makes the driving signal $x_m(t)$ does not perfectly have the same replica at the receiver $(x_m(t) + m(t))$. Hence $m(t)$ causes a disturbance on the synchronization process.

To neglect the effect of signal information sent on the synchronization process in the receiver, the information signal is feedback into the chaotic transmitter (Milanovic and Zaghloul, 1996) as shown in Figure 6. Figure 7 illustrates the synchronization error between the transmitter and the receiver during chaotic masking with and without feedback.

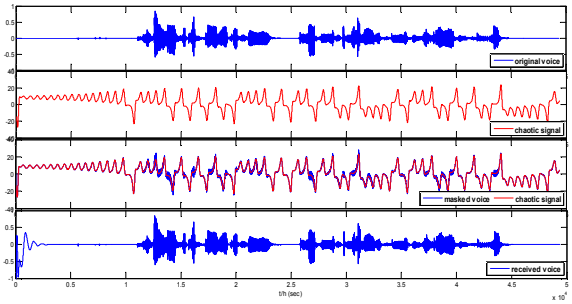

Figure 5: Chaotic Masking, (a) The original speech signal (b) Chaotic Lorenz signal, (c) Transmitted signal in channel and (d) The reconstructed speech signal.

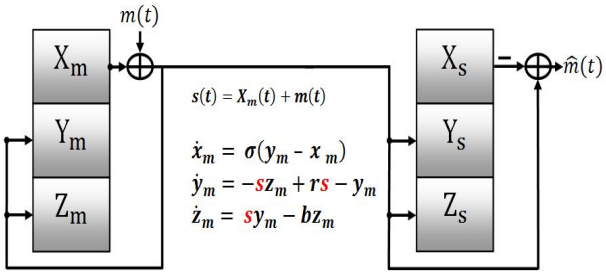

Figure 6: Chaotic masking with feedback and recovery information using Lorenz system.

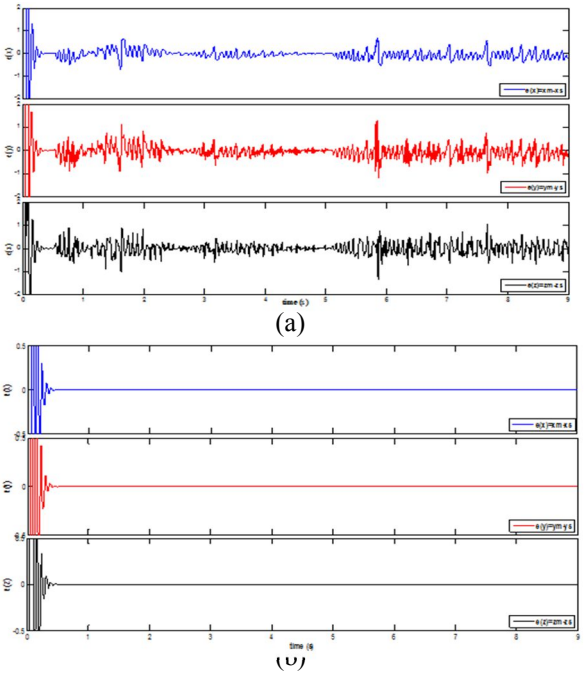

Figure 7: The error of synchronization between the transmitter and the receiver systems in chaotic masking (a) without feedback, (b) with feedback.

B. Chaotic Masking over AWGN Channel

In practical applications and to achieve good recovered signals quality, we need to work with at least SNR = 30 dB or above (Rupak, 2011), (Kevin, 1994). In fact it is very high SNR and difficult to be achieved because the speech signals that will be obtained after de-masking is corrupted by noise. i.e the de-masking will not remove the noise collected from the channel as shown in Figure 8.

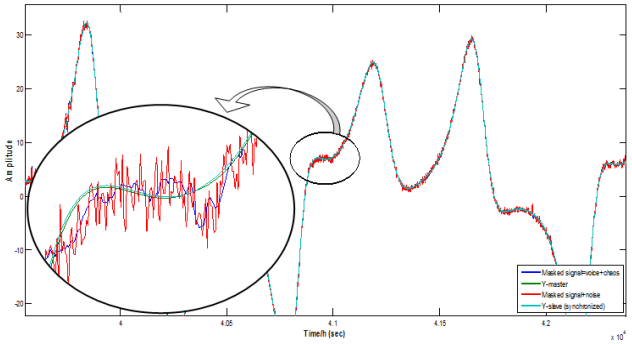

Figure 8: Feedback chaotic masking and information recovery using Lorenz system over AWGN channel**.**

The recovered speech signal infected by noise is:

$$s(t) + n(t) = x_m(t) + m(t) + n(t) \qquad (5)$$

$$\hat{m}(t) = s(t) + n(t) - x_s(t)$$

$$= m(t) + [x_m(t) - x_s(t)] + n(t)$$

Thus the recovered signal will be

$$\hat{m}(t) = m(t) + n(t) \qquad (6)$$

Figure 9 shows the drive chaotic signal $x_m(t)$, the masked signal $s(t)$, the masked signal plus noise and the slave chaotic signal $x_s(t)$. The signal to noise ratio must be high enough to reduce the effect of noise on the information recovery.

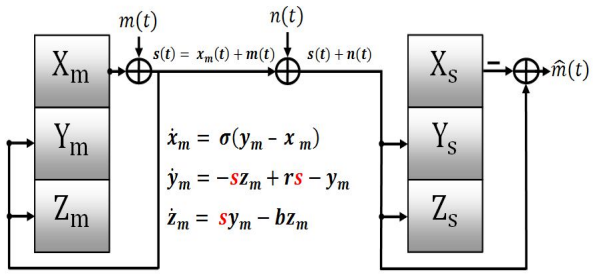

Figure 9: Chaotic masking based on Lorenz system over AWGN channel at SNR = 25 dB. where: ***Green-line*** "drive signal", ***Blue-line*** "masked signal", ***Red-line*** "masked signal + noise" ***and Sky blue-line***"

Figure 10 shows that the speech recovery when SNR = 25 dB. It is can be seen from this figure that the speech signal will suffer from huge amount of noise, so there is a real need to develop an efficient noise reduction scheme to improve the recovery process.

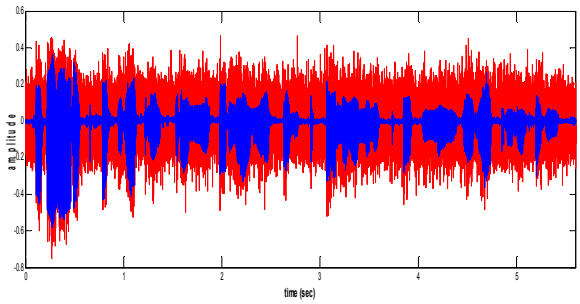

Figure 10: Recovery of speech signal in present of AWGN channel at SNR = 25 dB. *Blue line* and *red line* represents the original and recovered speech respectively.

C. Noise Reduction using Proposed Digital Processing Method (DPCM)

In this method, the speech or any information signal is converted from analog to digital using ADC converter (Sklar, 2011) before masking with the chaotic signal. At the receiver, the received binary data will be converted back to analog form using DAC converter. This conversion of speech signal to binary will reduce the effect of noise since the signal levels are either 0 or 1. In fact, the sample converted from analog to digital can be represented by either 1, 2 or 3.... N_b bits. The greater the number of bits used, the clearer the speech obtained. The steps of this method are described, as follows:

Step1: Converting the samples of speech from analog to digital using ADC. For instant, assume the data to be sent, after conversions are 10010101.

Step2: Masking the converted data with Lorenz chaotic signal.

Step3: Adding AWGN to the masked signal. For numerical illustration, assume that SNR = 20 dB in the transmission channel.

Step4: At the receiver, and after synchronization occurrence, the data are recovered. For our example the result is as follows:

0.735, 0.325, -0.235, 1.27, 0.4125, 0.9652, -0.125, 1.2435,

Step5: After applying a threshold of 0.5, for the recovered data. The result for our example will be 10010101. By doing so, the impact of noise is eliminated clearly.

III. Measuring the Quality of Speech

A number of quantitative measures can be used to evaluate the performance of the designed system concerning the security in channel and the reduction of noise effect on the information at the receiver. These are Segmental Spectral Signal to Noise Ratio (SSSNR), LPC Distance Measure, and Cpestral Distance Measure (CD). These measures are defined as follows (Mustafa, 2011):

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

$$(SSSNR_i)_{dB} = 10log\frac{\sum_{k=1}^{N}|X_i(k)|}{\sum_{k=1}^{N}[|X_i(k)| - |Y_i(k)|]} \quad (9)$$

Where $X_i(k)$ & $Y_i(k)$ are the DFT of original speech & recovered or encrypted speech.

b. Linear Predicative Code Measure (LPC):

$$d_{lpc} = \ln\left(\frac{AVA^T}{BVB^T}\right) \quad (10)$$

Where V is the autocorrelation matrix of the original speech block, vectors B & A contain the LPC coefficients for the clear speech block and recovered or encrypted speech block.

c. Cpestral Distance Measure (CD):

$$CD = 10log_{10}\left[2\sum_{n=1}^{p}\{C_x(n) - C_y(n)\}^2\right]^{\frac{1}{2}} \quad (11)$$

where $C_x(n)$ & $C_y(n)$ are the cpestral coefficients of the original speech and recovered or encrypted speech.

IV. Simulation Results

A simulation model based on block diagram given in Figure 1 has been designed using MATLAB. The parameters used in simulation were as follows: for chaotic masking: Lorenz flow is used with $\sigma = 10$, $r = 28$ *and* $b = 8/3$. The speech clip used for testing purpose has 8 KHz sampling frequency and 05:58 seconds length (45530 samples). The simulation results are presented as follows: first the strength of chaotic masking encryption and comparisons with traditional methods are given. Second the effect of AWGN channel noise on recovered speech at receiver side and the results of the noise reduction by using DPCM method are presented.

i. security in Chaotic Masking

In this process of encryption, three factors are examined to ensure the security of the system.

A. Testing the secret parameters of Lorenz system.
B. Testing the secure speech unintelligibility
C. Cryptanalysis.
D. Comparison with traditional methods.

A. Testing Secret Parameters of Lorenz System

Chaotic system parameters are chosen carefully with at least one positive Lyapunov exponent value. A system with a large Lyapunov exponent value has very sensitive to the initial condition and it is behaving chaotically. Table (1) shows the testing the Lyapunov

exponents of Lorenz system considered (given by equation 1) for some selections of system parameters values (σ, r and b). The computed values of Lyapunov exponents λ_1, λ_2 and λ_3 show that the system is chaotic since at least one of these exponents are positive (λ_1).

Table (1): Testing Parameters of the Chaotic Lorenz System through Lyapunov exponents.

σ	r	b	λ_1	λ_2	λ_3
10	28	8/3	1	0	-14.5
16	45.92	4	1.5	0	-22.44
20	57	7	2.0522	0	-29.95
35	91	11	3.337	0.001	-50.188
51	86	7.6	2.856	0	-60.266

B. Testing the Unintelligibility of the Masked Speech with Chaos

Here, the selection of encrypted speech is done by masking with chaos in methods mentioned section 2.A namely: Chaotic Masking and feedback chaotic masking. Table (2) is shows the residual intelligibility results. In this table, it is clear that the feedback does not affects dramatically the strength of information encryption and this is logically true because the purpose of feedback is not to improve the encryption but to eliminate the effect of the information on the synchronization process.

Table (2): The encrypted speech masked with chaos.

Type of Masking	d_{Lpc}	SSSNR[dB]	CD
Chaotic Masking	0.9702	-19.7036	3.8279
Feedback Chaotic Masking	0.9725	-19.7016	3.9531

C. Cryptanalysis of Chaotic Masking:

The cryptanalysis has two meanings, which are the determination of the key space, and the key sensitivity. In the good encryption system, the key space must be big enough. In the current scheme, the speech encryption is carried out using chaotic map, which mainly relies on the parameters of chaotic system. From other hand key sensitivity is one of the most important property for the calculation of encryption strength of any system, in order to protect the system from any attack. In another word, to demonstrate the key sensitivity, only one factor of key, either initial condition or parameter is changed at a time by a tiny amount; this simple change cannot retrieve information by third party. Here**,** one of states (x, y, z) generated by the Lorenz has been used in the masking process. In Lorenz, there are three parameters (σ, r and b) and each one of these parameters can be a part of the key space. Therefore, three-dimensional key is obtained.

The key sensitivity of designed system is tested through the following cases:

Case 1: When the value of the parameter (σ) is changed by 5%, $\sigma = \sigma[1 \mp 0.05]$ at the receiver and without changing the other parameters, the residual intelligibility results of the recovered information are shown for each of the masking schemes in Table (3).

Case 2: When the value of the parameter (r) is changed by 5%, $r = r[1 \mp 0.05]$, the recovered information are shown in Table (4)**.**

Case 3: When the value of the parameter (b) is changed by 5%, $b = b[1 \mp 0.05]$, the recovered information are shown in Table (5).

Table (3): The effect of changing the parameter σ by 5% on residual intelligibility.

Type of Masking	d_{Lpc}	SSSNR[dB]	CD
Chaotic Masking	0.5268	-15.9484	3.6961
Feedback Chaotic Masking	0.5324	-16.2542	3.7294

Table (4): The effect of changing the parameter r by 5% on residual intelligibility.

Type of Masking	d_{Lpc}	SSSNR[dB]	CD
Chaotic Masking	0.7378	-24.3512	4.6682
Feedback chaotic masking	0.7310	-24.2821	4.7352

Table (5): the effect of changing the parameter b by 5% on residual intelligibility.

Type of Masking	dLpc	SSSNR[dB]	CD
Chaotic Masking	0.5160	-16.0730	2.2819
Feedback Chaotic Masking	0.5026	-15.8379	2.4236

From the results in Tables $(3-5)$, we notice that any slight change in any parameters of Lorenz system (σ, r, b) would not allow the recovery of the original speech by any 3rd parity because this sensitivity. This is a great strength of the encryption in

terms of the key sensitivity. As the results shawed, since the valid theoretical values of parameters in the proposed scheme are infinite, this makes the scheme totally robust.

D. Performance Comparison of the Classical Encryption Systems and Chaotic Masking Encryption System

The residual intelligibility of traditional methods used for encrypting the same speech clip considered in our work that have been studied in [5]. The traditional methods used are: Time domain scrambling, frequency domain scrambling and, two dimensional scrambling and chaotic masking respectively in Table (6)

Table 6: Results the Classical speech scrambling and chaotic masking

Classical scrambling	d_{Lpc}	SSSNR[dB]	CD
Time domain scrambling	0.6532	0.97540	2.4373
Frequency domain scrambling	0.5723	-0.2935	2.5075
Two dimensional scrambling	0.6732	-1.9443	3.2269
Chaotic masking	0.9702	-19.7036	3.8279
Feedback chaotic masking	0.9725	-19.7017	3.9531

From Table (6), it is clear that the encryption method using the chaos is much better than the Classical methods. In general and after overlooking the obtained results we observed that the accumulated performance of using encryption by chaotic masking used in terms of SSSNR is reduced by -20.679 dB (from 0.9754 to -19.7036) compared with time domain scrambling. Furthermore, the key space would be much greater if each method is used alone. This is because it has three-dimensional encryption possibility (σ, r, b), and this is considered another advantage of the presence of masking encryption by chaotic Lorenz signal.

ii. Recovering Speech in the Presence of Noise using DPCM Method

After passing AWGN channel, the signal is corrupted by additive noise $(m(t) + n(t))$. Table (7) shows the effect of the noise on the recovered information for different SNRs. When the SNR is over 30 dB, the recovered speech becomes more clearer (SSSNR have positive value). Using the proposed method and when the speech converted from analog to digital form, its immunity to value change due to additive noise is increased. Table (8) shows the results obtained when the proposed scheme is used.

Table (7): The recovered speech for different SNRs

SNR[dB]	d_{Lpc}	$SSSNR_{dB}$	CD
24	1.9581	-4.9001	5.7207
26	1.7923	-2.8107	5.3875
28	1.6130	-0.7236	5.0493
30	1.4656	1.4697	4.6768
32	1.2844	3.5103	4.2984
34	1.1308	5.7529	3.9002
36	0.9706	7.9799	3.4543

Table (8): The simulation results of DPCM method

SNR[dB]	d_{Lpc}	SSSNR[dB]	CD
10	2.8751	-12.8221	7.1254
12	2.3199	-10.2135	6.8873
14	2.1709	-9.09266	6.7573
16	1.3987	0.53334	5.6297
18	0.3841	16.5787	4.2537
20	0.0559	31.5003	-0.2728
22	0.0297	32.8333	-1.6526
24	0.0297	32.8333	-1.6526

It can be observed from this table that, in cases of 10 dB & 12 dB SNR values, the system has poor performance using the three speech intelligibility standards. When SNR= 16 dB and go up, the system performance is improved (i.e SSSNR start to have positive value). To verify the improvement gained by the proposed scheme, MSE is plot versus SNR and camped with the classical method (without digital conversion) when the number of bits per sample is 8 as shown in Figure 11.

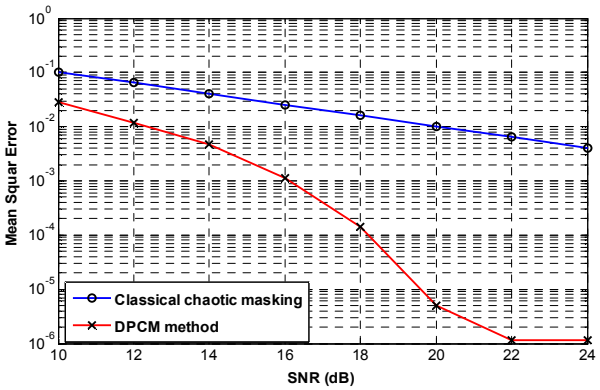

Figure 11: The comparison between the classical and DPCM methods.

In this figure, the improvement in MSE is increased dramatically. When SNR = 10 dB the value of MSE is reduced from 0.1 in the classical chaotic masking method to $2*10^{-2}$ in the DPCM method. When SNR = 14 dB, the MSE is reduced from $3*10^{-2}$ the classical chaotic masking method to $4*10^{-3}$ for DPCM method. The huge improvement in MSE is achieved when SNR = 22 dB, where MSE is reduced from $5*10^{-3}$ in classical chaotic masking method to 10^{-6} in the DPCM method, the system performance stays constant when SNR > 22 dB at MSE = 10^{-6}. This stable minimum error is due to the difference of conversion from analog to digital. This means that the gain in SNR is increased as MSE is decreased. When MSE =10^{-2}, the gain is 6.7 dB and when MSE = 10^{-3} the gain is 14 dB. This is amazing result achieved by the DPCM method.

V. Conclusions

In this paper, an efficient noise reduction scheme based on digital processing is proposed for speech signals masked by Lorenz chaotic system. The results obtained showed that the proposed scheme offers a huge reduction in MSE reaches to its maximum when SNR = 22 dB. with no further reduction beyond this SNR values. As a number of bits represent the digital speech signal increases, the amount of improvement increases but on a penalty of increased complexity and bandwidth. However, the increase in bandwidth does not represent a serious disadvantage since the transmitted signal already have wide bandwidth due to spreading nature of chaotic signal spectrum. It is also proved that the usage of Lorenz chaotic system increases the security of speech transmission as compared with classical encryption schemes due to high key space provided by that system.

Corresponding Author:
Dr. Hikmat N. Abdullah
College of Information Engineering
Al-Nahrain University
Baghdad 64005, Iraq
E-mail: dr.h.abdullah@ieee.org

References

1. Liu J. and Ma H. A Speech Chaotic Encryption Algorithm based on Network. Proceedings of IIHMSP, IEEE press, Harbin, China, 2008: 1(1): 283–286.
2. Gnanajeyaraman R, Prasadh K, and Ramar D. Audio Encryption Using Higher Dimensional Chaotic Map. International Journal of Recent Trends in Engineering, 2009: 1(2):103 -107.
3. Sprott J. New Chaotic Regimes in the Lorenz and Chen Systems. International Journal of Bifurcation and Chaos, 2015: 25(2):1-7.
4. Kohad H, Ingle V, and Gaikwad M. Security Level Enhancement In Speech Encryption Using Kasami Sequence. International Journal of Engineering Research and Applications, 2012: 2(4):1518-1523.
5. Al-Azawi M, and Kadhim J. Speech Scrambling Employing Lorenz Fractional Order Chaotic System. Journal of Engineering and Development, 2013: 17(4): 195-211.
6. Ekhande R and Deshmukh S. Chaotic Signal for Signal Masking in Digital Communications. International organization of Scientific Research Journal of Engineering, 2014: 4(2): 29-33.
7. Rupak K. Design and Implementation of Secure Chaotic Communication Systems. Ph.D. Thesis, University of Northumbria, 2011.
8. Pecora L and Carroll T. Synchronization in Chaotic Systems. Physics Review Litters, 1990: 64(1): 821-824.
9. Jovic B. Synchronization Techniques for Chaotic Communication Systems. First edition, Springer, 2011.
10. Milanovic V. and Zaghloul M. Improved Masking Algorithm for Chaotic Communications Systems. IEE Electronics Letters, 1996: 32(1): 11 – 12.
11. Cuomo K. Analysis and Synthesis of Self-Synchronizing Chaotic Systems. Ph.D. Thesis, Research Laboratory of Electronics. Massachusetts Institute of Technology Cambridge, 1994.
12. Sklar B. Digital Communication: Fundamentals and Applications. Prentice hall publication, Third Edition, 2011.
13. Mustafa T. Objective Tests of Speech Signal. M.Sc. Thesis, Al-Mustansiryah University, Department of Electrical Engineering, Baghdad Iraq, 2001.

5/22/2015