SECURE SPEECH TRANSMISSION USING CHAOTIC SYSTEM

Hamsa A. ABDULLAH[1]

One of the most important methods in the secure communication based on the chaotic systems is chaotic masking. The transmitter and the receiver synchronization have a significant role in chaotic masking systems. The received signal affected by the noise through wireless communication channel leads to a mismatch of the synchronization and reduces the performance of the system. In this paper, an enhanced chaotic system is presented with the hyperchaotic characteristics that increase the masking system strength and robustness. The proposed system offers a wide area of initial key size 2^{416} and that increases the security level of the system. The simulation results illustrate that the proposed system has good performance in the AWGN channel where the signal recovered at 40 dB. The sensitivity of the chaotic system to initial value make the proposed system more secure and robust since the small changes in the initial value (10^{-10}) at the receiver side make it impossible to recover the speech signal.

Keywords: Secure communication, Speech signal, Chaotic, AWGN, Synchronization, Masking

1. Introduction

Recently, with the growth of signal processing methods and communication technology has become feasible to secure speech transfer over the communication channel [1]. Chaotic systems have been utilized in many implementations such as signal detection, analog to digital converters, wireless communication, and encryption [2]. In communication systems, chaotic signals can be used as carriers. The basic concept in a chaotic system is high sensitivity to the initial values. Other feature of a chaotic signal generator is its simplicity. The synchronization of chaotic systems is an important feature of communication systems based on chaotic dynamics.

In [3] noise reduction method for masking speech based chaotic system is presented. In this paper, a communication system with high security level and resistance to noise is proposed. In [4], speech scrambling based on a chaotic system is presented. In this paper, Duffing chaotic system used for scrambling and an encrypting the voice signal. In [2], the investigation of two communication schemes of masking based on Sprott94 Case A chaotic system is presented.

[1] College of Information Engineering, Al-Nahrain University, Baghdad, Iraq, e-mail: hamsa.abdulkareem@coie-nahrain.edu.iq

In this work, an enhanced chaotic system is proposed. The advantage of the enhanced system is the capability to run in a lower frequency and higher amplitude with low synchronization error. The enhanced system used to provide secure and robust system to transmission speech signal over Additive White Gaussian Noise (AWGN) channel. The paper divided in to five sections. Section 2 contains a description of the developed system, section 3 consists of the performance evaluation of the proposed system. Section 4 contains the proposed chaotic masking and synchronization system. Finally, section 5 conclude the whole paper.

1. Developed Duffing system

In this paper, the focus of developing a new hyperchaotic system is the main contribution in order to increase the level of security in masking and transmission of speech signal. The Duffing's map has two variables (X_{dn}, Y_{dn}) [5]:

$$\begin{aligned} X_{d(n+1)} &= Y_{dn} \\ Y_{d(n+1)} &= -b_d X_{dn} + a_d Y_{dn} - Y_{dn}^3 \end{aligned} \tag{1}$$

The Duffing map be determined by the two parameters $a_d = 2.75$ and $b_d = 0.2$. The proposed enhanced system is:

$$\begin{aligned} X_{(n+1)} &= -aY_n + bX_n - X_n^3 \\ Y_{(n+1)} &= cX_n - dY_n \\ Z_{(n+1)} &= X_n - eZ_n \end{aligned} \tag{2}$$

The enhanced system depends on the five parameters $a, b, c, d, and\ e$. These are usually set to a= $0.1, b = 2.65,\ c = 0.7, d = 0.2, and\ e = 0.5$ to produce chaotic behavior. The phase portrait of the suggested system is illustrated in Fig. 1. The number of keys in the proposed system is 8 (a, b, c, d, e, X(0), Y(0), Z(0)). In accordance with IEEE floating-point standard, the 64-bit double-precision number computational accuracy is about 2^{-52}. So, the proposed system keys size is $(2^{52})^8=2^{416}$ and which is greater than the basic size (2^{100}) and that ensure the high security level to the proposed system.

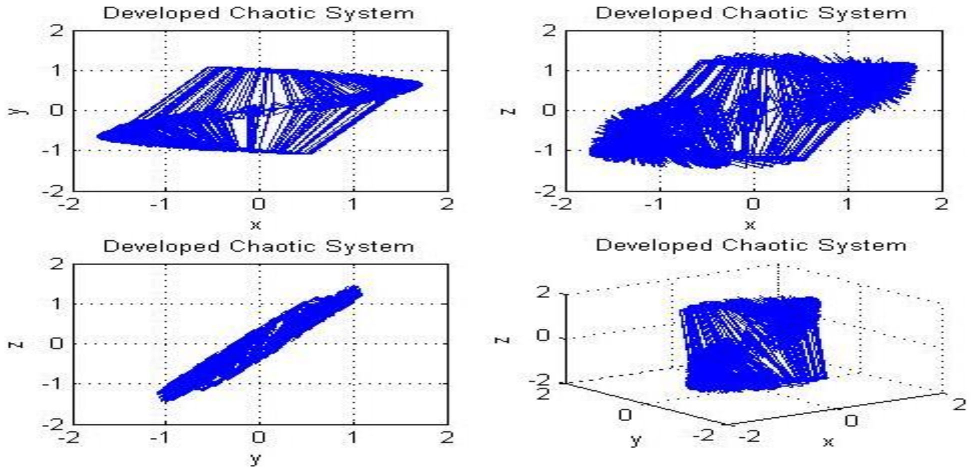


Fig. 1: The Proposed System Phase Portrait

Fig. 2 illustrates that the proposed system produces three signals (X, Y, and Z) at a time with different values and behavior which can be used in different areas such as secure transmission and encryption.

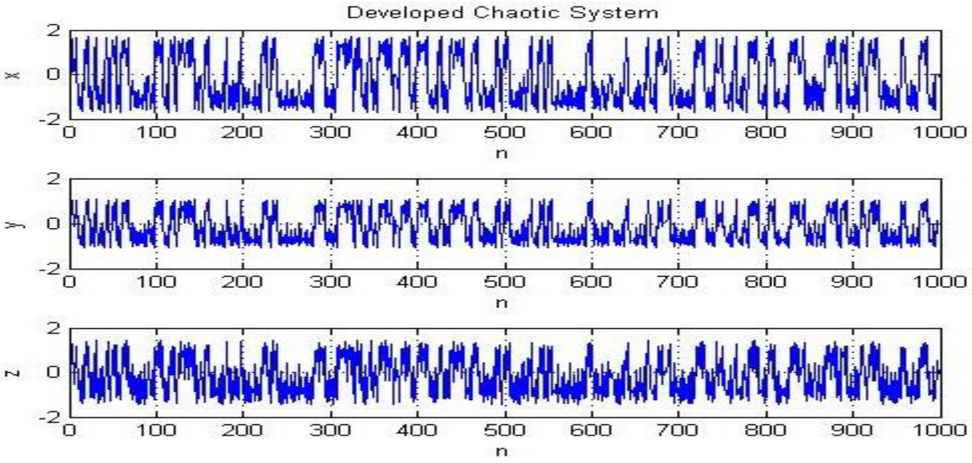


Fig. 2: The proposed system waveforms

2. Performance measurement

To approve the randomness and chaotic behavior of the enhanced system, a set of measurements are applied.

2.1 Chaotic Behavior Tests

Zero- one (0-1) and Lyapunov exponent (LE) tests are applied to determine the developed system is chaotic or regular.

3.1.1. Chaotic Behavior Test:

1. Zero-One Test

The Zero-One test is used to recognize between chaotic dynamics and regular in deterministic dynamical systems. The data of this test is a 1-D vector $\varphi(n)$ where n = 1, 2, 3... The data $\varphi(n)$ is used to determine the 2-D system [6].

$$N(n+1) = N(n) + \varphi(n)\cos cn \tag{3}$$

$$M(n+1) = M(n) + \varphi(n)\sin cn \tag{4}$$

where c ∈ (0,2π) is constant. The mean square displacement MSD is determined by:

$$MSD(n) = \lim_{N\to\infty} \frac{1}{N} \sum_{j=1}^{n} [N(j+n) - N(j)]^2 + [M(j+n) - M(j)]^2 \tag{5}$$

The approximate growth rate is:

$$K_c = \frac{\log MSD(n)}{\log\ n} \tag{6}$$

$$K = Median\ (K_c) \tag{7}$$

$$Decision = \begin{cases} \mathrm{K} \approx 0 & \text{The system is Regular} \\ \mathrm{K} \approx 1 & \text{The system is Chaotic} \end{cases} \tag{8}$$

The K values of enhanced system variables $(X, Y, and\ Z)$ were achieved: $Kx = 0.9975, Ky = 0.9972, Kz = 0.9977$. According to these results, since all values were computed of K are close to 1, the enhanced system is a chaotic system.

3.1.2. Lyapunov Exponent

Lyapunov exponents (λ) are a measure of the system's sensitivity to variation in initial parameters [7]. It describes two adjacent curves convergence in the state-space [8, 9, 10]:

$$\lambda = \lim_{N\to\infty} \frac{1}{N} \sum_{n=1}^{N} \log_2 \frac{Xn}{X0} \tag{9}$$

X_0 is the primary value and X_n is consistent trajectory (N=1, 2, 3…). The system is considered as chaotic when one of the λ is plus, [9]. The system is considered as periodic when the value of λ is minus. The divergence arises when the value of λ is zero. The system is further chaotic when the λ is plus [11]. The system is considered as hyperchaotic when two or more values of λ becomes plus [12]. After calculating λ for developed system, the following outcomes are found:

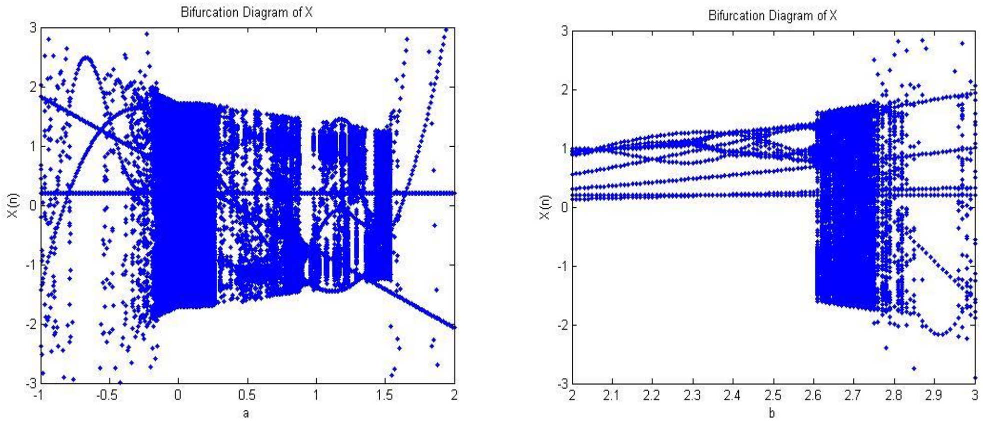
$\lambda 1 = -1.7927$, $\lambda 2 = 1.6041$, $\lambda 3 = 2.2504$. The results of this test show that there are two values of λ are plus, so the enhanced system is a hyperchaotic.

3.1.3. Bifurcation Graph

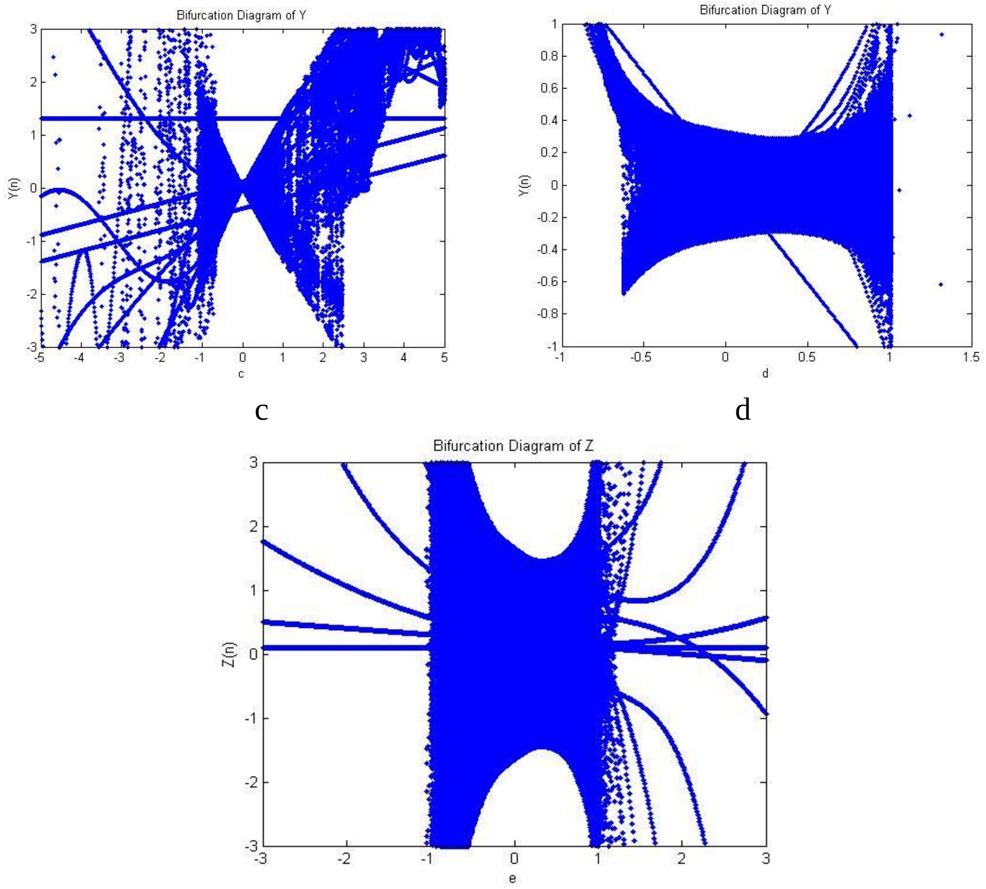
The bifurcation area of the proposed system can readily be noticed by looking to graphs of X with each of the control parameters a and b if the Y and Z are fixed. Fig. 3 show the bifurcation diagram of the proposed system. Fig. 3 (a and b) shows that, when the value of ***a*** is less than -0.120 and ***b*** is less than 2.59, the proposed system performance is periodic. When the parameter ***a*** is within the range [-0.119; 1.49998] and parameter ***b*** is within the range [2.6; 2.84], the proposed system performance is chaotic.

The bifurcation area for variable Y can be noticed by looking to graphs with each of the control parameters ***c*** and ***d*** if we fix the X and Z. Fig. 3 (c and d) shows that, when the value of ***c*** is less than -1.11 and value of ***d*** is less than -0.6, the proposed system performance is periodic. When the parameter ***c*** is within the range [-1.1; 5] and parameter ***d*** values [-0.6; 1.1] the proposed system performance is chaotic.

The bifurcation area for variable Z can be noticed by looking to graphs with each of the control parameter c if we fix the X and Y. Fig. 3.e shows that, when the value of ***e*** is less than -0.83, the proposed system performance is periodic. When the parameter ***e*** is within [-0.82; 1], the proposed system performance is chaotic.



a b



c d

e

Fig. 3: Bifurcation diagram of the suggested system a. Parameter a with $X(n)$ b. Parameter b with $X(n)$ c. Parameter c with $Y(n)$ d. Parameter d with $Y(n)$ e. Parameter e with $Z(n)$.

3.1.4. The Results of the Randomness Analyses

The randomness analyses are applied to confirm the unpredictability of the bits stream that are generated based on a chaotic system. This paper introduces the details of the realization method that transforms the chaotic signals into binary. The transformation is based on comparing two chaotic systems running concurrently with the same parameters $(a, b, c, d, e) = (2.75,0.2,0.5, 0.2, 0.7)$ and with dissimilar initial values according to (10) - (12). The first system initial conditions are $(X_1(0), Y_1(0), Z_1(0)) = (1.3, 0.2, 0.1)$ whereas the second system initial conditions are $(X_2(0), Y_2(0), Z_2(0)) = (0.1, -0.2\ , 0.5)$.

$$G1(X_1, X_2) = \begin{Bmatrix} 1\ if\ X_1 > X_2 \\ 0\ if\ X_1 \leq X_2 \end{Bmatrix}\ where\ X_1(0) \neq X_2(0) \tag{10}$$

$$G2(Y_1,Y_2) = \begin{Bmatrix} 1 \; if \;\; Y_1 > Y_2 \\ 0 \; if \;\; Y_1 \leq Y_2 \end{Bmatrix} \; where \; Y_1(0) \neq Y_2(0) \tag{11}$$

$$G3(Z_1,Z_2) = \begin{Bmatrix} 1 \; if \; Z_1 > Z_2 \\ 0 \; if \; Z_1 \leq Z_2 \end{Bmatrix} \; where \; Z_1(0) \neq Z_2(0) \tag{12}$$

The size of the bit sequences that are used in the tests is 15,000 bits of each system. The analyses results are shown in Table 2. All the tested binary series P-value greater than 0.001 and that shows the suggested system has random performance.

Table 1:

The Randomness Analyses Results

No	Test type	X	Y	Z	*P-value ≥ (0.001)*
1	Frequency	0.2950	0.3353	0.3192	Accepted
2	Frequency Block	0.3078	0.3474	0.3312	Accepted
3	Run	0.3329	0.0017	0.0909	Accepted
4	Longest Run	0.3019	0.3409	0.2763	Accepted
5	Binary Matrix Rank	0.5317	0.4980	0.5732	Accepted
6	DFT	0.5858	0.4980	0.5732	Accepted
7	Maurer's	0.9800	0.8817	0.9622	Accepted
8	Approximate Entropy	0.0253	0.0253	0.0253	Accepted
9	Cumulative Sum	1	1	1	Accepted
10	Random Excursions (RE)	0.3840	0.0203	0.7717	Accepted
11	RE Variant	0.2915	0.7746	0.9053	Accepted

3. Proposed chaotic masking and synchronization system

The suggested chaotic masking system block diagram is shown in Fig.5. The original speech signal $M(t)$ is masked by the proposed chaotic signal $Y(t)$ through the addition process. The exact $\widehat{M}(t)$ is reconstructed at the receiver side by the subtraction of received signal from the chaotic signal that generated in slave chaotic system. The masked signal can be described as:

$$R(t) = Y(t) + M(t) \tag{13}$$

The transmitted speech signal affected by noise is:

$$R(t) + N(t) = Y(t) + M(t) + N(t) \tag{14}$$
$$\widehat{M}(t) = R(t) + N(t) - \hat{Y}(t)$$
$$\widehat{M}(t) = M(t) + N(t) + [Y(t) - \hat{Y}(t)]$$

So, the received speech signal is:

$$\widehat{M}(t) = M(t) + N(t) \tag{15}$$

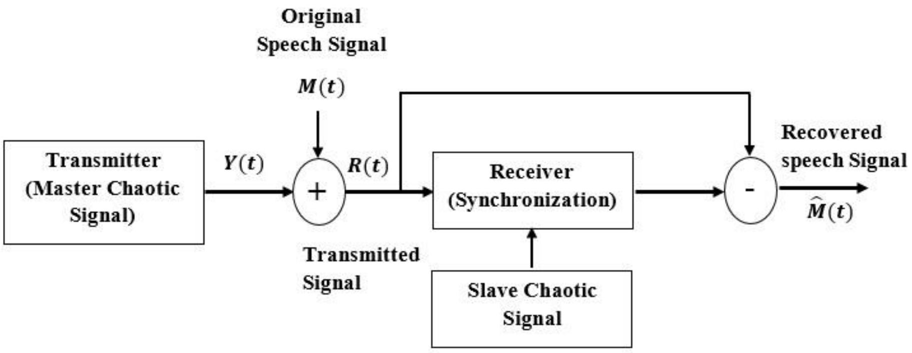


Fig. 4: Block Diagram of the Proposed Masking System

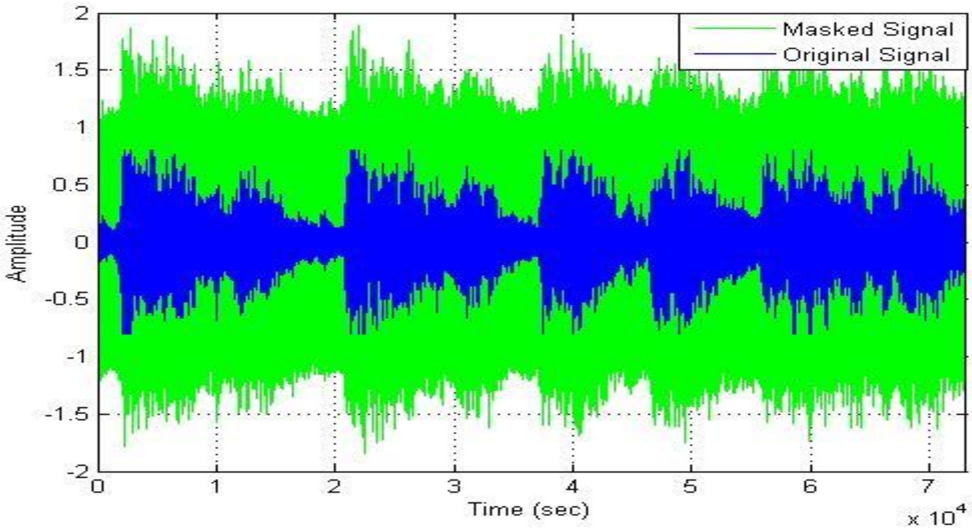


Fig. 5: The Transmission Speech Signal over AWGN Channel

In order to successfully remove the mask, the suggested chaotic signals on both transmitter and receiver system have to synchronize. The nonlinear control law synchronization schemes are used to achieve synchronization. The proposed chaotic system synchronization capability given in (2) is tested using laws of nonlinear control. The receiver system is:

$$\widehat{X}_{(n+1)} = -a\widehat{Y}_n + b\widehat{X}_{dn} - \widehat{X}_n^3 + u_{1n}$$

$$\widehat{Y}_{(n+1)} = c\widehat{X}_n - d\widehat{Y}_n + u_{2n} \tag{16}$$

$$\hat{Z}_{(n+1)} = \hat{X}_n - \mathrm{e}\hat{Z}_n + u_{3n}$$

The error is defined by:

$$\begin{gathered} e_{1(n+1)} = \hat{\mathrm{X}}_{(n+1)} - \mathrm{X}_{(n+1)} \\ \mathrm{e}_{2(n+1)} = \hat{\mathrm{Y}}_{(n+1)} - \mathrm{Y}_{(n+1)} \\ \mathrm{e}_{3(n+1)} = \hat{\mathrm{Z}}_{(n+1)} - \mathrm{Z}_{(n+1)} \end{gathered} \tag{17}$$

where $X_{(n+1)}, Y_{(n+1)}, and\ Z_{(n+1)}$ are the variable of transmitter system whereas $\hat{X}_{(n+1)}, \hat{Y}_{(n+1)}$ and $\hat{Z}_{(n+1)}$ are the variable of receiver system. The errors e_{1n}, e_{2n},and e_{3n} can be obtained by representing (1) and (16) in (17):

$$\begin{gathered} e_{1(n+1)} = -a\hat{Y}_n + b\hat{X}_{dn} - \hat{X}_n^3 + u_{1n} + aY_n - bX_n + X_n^3 \\ \mathrm{e}_{2(n+1)} = c\hat{X}_n - d\hat{Y}_n + u_{2n} - cX_n + dY_n \\ e_{3(n+1)} = \hat{X}_n - \mathrm{e}\hat{Z}_n + u_{3n} - X_n + eZ_n \end{gathered}$$

The identification of equations in [13] is used to simplify the equations, which become:

$$\hat{X}^2 - X^2 = \hat{X}e_1 + Xe_1 \tag{18}$$

$$-\hat{Y}^2 + Y^2 = -\hat{Y}e_2 - Ye_2 \tag{19}$$

$$\hat{X}\hat{Y} - XY = Ye_1 + Xe_2 \tag{20}$$

$$-\hat{X}^3 + X^3 = -e_1^3 - 3X\hat{X}e_1 \tag{21}$$

According to (18) - (21) the error can also be denoted by:

$$\begin{gathered} e_{1(n+1)} = -a(\hat{Y}_n - Y_n) + b(\hat{X}_n - X_n) - \hat{X}_n^3 + X_n^3 + u_{1n} \\ 0 = -ae_{2n} + be_{1n} - e_{1n}{}^3 - 3X_n\hat{X}_n e_{1n} + u_{1n} \end{gathered}$$

The laws of control u_{1n}:

$$u_{1n} = ae_{2n} - be_{1n} + e_{1n}{}^3 + 3X_n\hat{X}_n e_{1n} \tag{22}$$

The error e_{2n} can then be denoted by:

$0 = c(\hat{X}_n - X_n) - d(Y_n - \hat{Y}_n) + u_{2n}$

The laws of control u_{2n}:

$$u_{2n} = -ce_{1n} + de_{2n} \tag{23}$$

The error e_{3n} can then be denoted by:

$$\begin{gathered} 0 = \hat{X}_n - X_n - e(\hat{Z}_n - Z_n) + u_{3n} \\ 0 = e_{1n} - ee_{3n} + u_{3n} \end{gathered}$$

The laws of control u_{3n}:

$$u_{3n} = -e_{1n} + ee_{3n} \tag{24}$$

After passing through an AWGN channel, the signal is distorted by additive noise $(M(t) + N(t))$. Fig. 6 shows that when Signal to Noise Ratio (SNR) = 20 dB and has greater values, the system performance is getting better. When the SNR is over 40 dB, the reconstructed speech signal becomes clear.

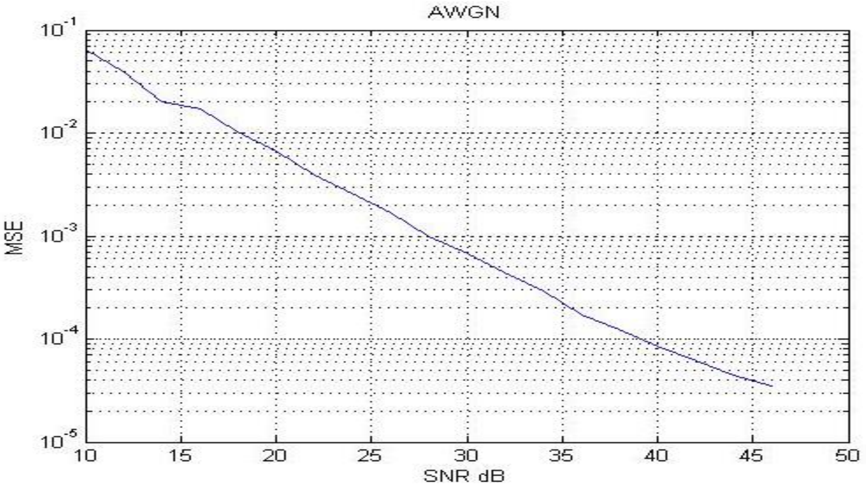


Fig. 6: Mean Square Error (MSE) of the proposed system

The security level that is provided by chaotic masking appeared in Fig. 7, where small changes in the initial value $X(0)$ make impossible to retrieve the original speech signal because of the chaotic system high sensitivity to initial values and parameters.

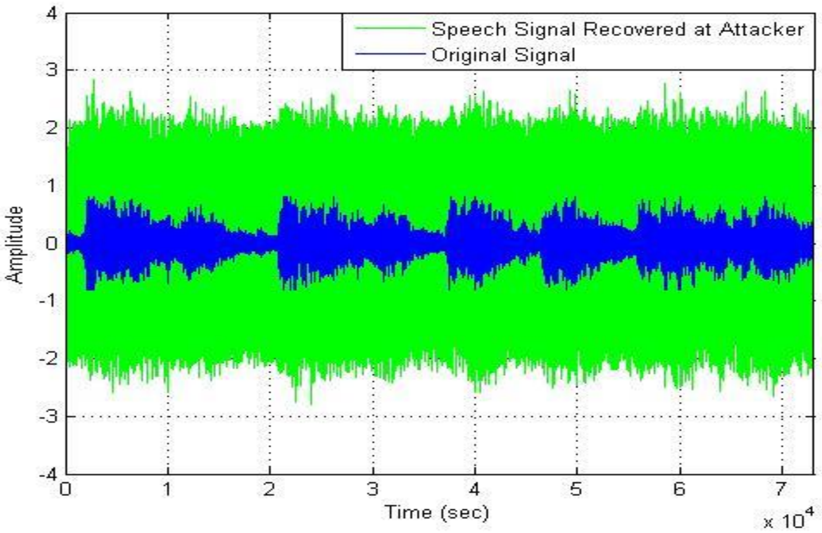


Fig. 7: Recovered Speech Signal (a) Blue recovered signal with $X(0) = 0.3$ (b) Green recovered signal with $X(0) = 0.3 + 10^{-11}$

Table 2 shows the comparison of the performance measurements between the proposed system and [14] in terms of correlation of encryption and decryption, SNR and Peak Signal to Noise Ratio (PSNR). The proposed system shows that the correlation between the masked signal and the original signal is very low (0.04128) while the correlation of the recovered signal is close to 1. The table shows that the proposed system has better performance than the [14] in terms of SNR and PSNR where the signal recovered at 30 dB in the proposed system while in [14] recovered at 33.7 dB. Table 3 shows the comparison of the chaotic signal that is used in this work and in [15]. The table shows that the chaotic behavior that used in this work much better that that used in [15] in terms the key size and type of chaotic. So the proposed chaotic system is more secure, robust and provides another level of security.

Table 2:

Comparison of the Performance Measurements

	Correlation Encryption	**Correlation Decryption**	**SNR**	**PSNR**
Proposed Method	0.04128	0.9999	30	79.9985
Ref [14]	0.0233	0.9999	33.7464	59.7989

Table 3:

Comparison of Chaotic System

	Dimension	Number of Parameters	Key size	Type of chaotic
Proposed Method	3	5	2^{416}	hyperchaotic
Ref [15]	2	3	2^{260}	chaotic

4. Conclusion

In this paper, a developed chaotic system was introduced. The results show that the proposed system has hyperchaotic behavior, so the system provides another security level. The developed chaotic system was used to produce a high security level for speech signal transmission over AWGN channel based on Chaotic Masking model. The developed chaotic system has three values and five parameters, so the key space that is produced by the developed system is equal to 2^{416} and which is greater than the basic size (2^{100}) that ensures the proposed system has high security level. The sensitivity to initial values and parameters of the chaotic system make the proposed system more secure and robust. The results show that the chaotic behavior that is used in this work is much better that two other such works in terms of the key size and chaotic type. So the proposed chaotic system more secure, robust and provide another level of security.

REFERENCES

[1] M. Boumaraf and F. Merazka, "Speech Coding Combining Chaos Encryption and Er Recovery for G.722.2 Codec," in *Proceedings of the 3rd International Conference on Natu Language and Speech Processing*, Trento, Italy, 2019.

[2] M. Mobini, M. Zahabi, "Masking Communication Using Sprott94 Case A Chaotic System AWGN Channel," *Journal of World's Electrical Engineering and Technology,* vol. 7, no. 2, 9-16, 2018.

[3] H. N. Abdullah, S. Hreshee, A. Jawad, "Design of Efficient Noise Reduction Scheme for Sec Speech Masked by Chaotic Signals," *Journal of American Science,* vol. 11, no. 7, pp. 49- 2015.

[4] A. Mahdi, A. Jawad, S. Hreshee, "Digital Chaotic Scrambling of Voice Based on Duffing Ma *International Journal of Information and Communication Sciences,* vol. 1, no. 2, pp. 16- 2016.

[5] L. Longsuo, "Suppressing Chaos of Duffing-Holmes System Using Random Phas *Mathematical Problems in Engineering, Hindawi Publishing Corporation,* vol. 2011, p. 8, 201

[6] H. A. Abdullah, H. N. Abdullah, "A New Chaotic Map for Secure Transmissior *TELKOMNIKA,* vol. 16, no. 3, p. 1135~1142, 2018.

[7] M. Rüdisüli, T.J. Schildhauer, S. Biollaz, J. Ommen, "Measurement, monitoring and control fluidized bed combustion and gasification," in *Fluidized Bed Technologies for near-Ze Emission Combustion and Gasification,* Woodhead Publishing, 2013, pp. 813-864.

[8] M. B. Tayel., E. I. AlSaba,, "Robust and Sensitive Method of Lyapunov Exponent for Heart R Variability," *International Journal of Biomedical Engineering and Science (IJBES),* vol. 2, no pp. 31-48, 2015.

[9] A. Wolf, J. B. Swift, H. L. Swinney, J. A. Vastano,, "Determining Lyapunov Exponents From Time Series," *Physica 16D, Elsevier Science Publishers,* vol. 16, no. 3, pp. 285-317, 1985.

[10] R. Kriz, "Finding Chaos in Finnish GDP," *International Journal of Automation and Computi* vol. 11, no. 3, pp. 231-240, 2014.

[11] Michael, V. Opstall, "Quantifying chaos in Dynamical Systems with Lyapunov Exponent *Electronic Journal of Undergraduate Mathmatics,* vol. 4, 1998.

[12] K. Rajagopal, L. Guessas, S. Vaidyanathan, A. Karthikeyan, A. Srinivasan, "Dynami Analysis and FPGA Implementation of a Novel Hyperchaotic System and Its Synchronizati Using Adaptive Sliding Mode Control and Genetically Optimized PID Control," *Mathemati Problems in Engineering,* vol. 2017, p. 14, 2017.

[13] B. Jovic, "Chaotic Signals and Their Use in Secure Communication," in *Synchronizati Techniques for Chaotic Communication Systems,* New Zealand, Springer, 2011, pp. 31-47.

[14] P. Sathiyamurthi, S. Ramakrishnan, "Speech encryption using chaotic shift keying for secu speech communication," *EURASIP Journal on Audio, Speech, and Music Processing,* vol. 20, 11, 2017.

[15] F J. Farsana, K. Gopakumar, "A Novel Approach for Speech Encryption: Zaslavsky Map Pseudo Random Number Generator," *Procedia Computer Science,* vol. 93, p. 816 – 823, 2016