International Journal of Electrical and Computer Engineering (IJECE)
Vol. 10, No. 4, August 2020, pp. 4270~4278
ISSN: 2088-8708, DOI: 10.11591/ijece.v10i4.pp4270-4278

A high security and noise immunity of speech based on double chaotic masking

Ehab AbdulRazzaq Hussein[1], Murtadha K. Khashan[2], Ameer K. Jawad[3]
[1,2]Department of Electrical Engineering, Faculty of Engineering, University of Babylon, Iraq
[3]Department of Computer Engineering, Faculty of Engineering, University of Islamic, Iraq

Article Info

Article history:

Received Jul 11, 2019
Revised Feb 25, 2020
Accepted Mar 2, 2020

Keywords:

Chaotic flow systems
Double chaotic masking
communication security
Encryption
Speech quality

ABSTRACT

It is known that increasing the security of the information and reducing the noise effect through public channels are two of the main priorities in developing any communication system. In this article, an efficient, secure communication system with two levels of encryption has been applied to the speech signal. The suggested security approach was implemented by using two different stages of chaotic masking on the signal; one masking was conducted by using Lorenz system and the other masking was built by using Rössler chaotic flow system. The main goal of developing this two-chaotic masking approach is to increase the key space and the security of the information. Also, an immunity technique has been implemented in the suggested approach to reduce the noise effect. For practical application purposes, this system was tested with additive white gaussian noise (AWGN) channel. The simulation results show that the quality of reconstructed speech signal is changeable according to the used signal to noise ratio (SNR); therefore, a proposed technique based on digital processing method (DPM) was applied to the first masked signal by converting the sampled data from the analog to the binary format. The simulation results show that an 22 dB (SNR) is sufficient to recover the speech signal with minimum noise by using the suggested approach.

Corresponding Author:

Ehab AbdulRazzaq Hussein,
Department of Electrical Engineering,
Faculty of Engineering,
University of Babylon, Babylon, Iraq.
Email: dr.ehab@itnet.uobabylon.edu.iq

1. INTRODUCTION

In communication system security is the main goal that must be achieved, in order to keep data away from attacks (an eavesdropper). Information must be encrypted over various techniques, Send encrypted speech or any form of data need to use a general key that should be known by the receiver of communication system. A chaotic system has many properties like, very sensitive to initial condition and parameters, ergodic, unpredictable signal and deterministic system. Due to the important properties of chaotic that mentioned, chaotic can be utilized in secure communication.

Several works and study can be done in the application of chaotic in secure communication. Since 1993 Oppenheim and Cuomo, implemented masking scheme of the Lorenz system in secure communication [1, 2]. In 1996 Milanovice Zaghloul put an improved technique to implement chaotic masking in the communication field [3, 4]. After this chaotic circuit of secure communication based on Lorenz system is implemented in discrete electronics component [5, 6]. In 2009 a secure communication based on a fractional chaotic method was proposed [7]. In 2011, a new 3-dimensional system based on chaos theory was proposed by Li and Ou [8], using the chaotic flow, Lorenz system. Zhang and Zhao have studied a two-stage driver system by employing the pecora and carroll (PC) method on the Lorenz chaos model in

the field of secure communications [9]. In 2018, presented a security of speech based on two encryption stage, the first stage is time scrambling to construct by chaotic map, while the second stage is chaotic masking established by the chaotic flow [10].

Yamada and Fujisaka [11], conducted on the first research on synchronizing, a chaotic system. While pecora carroll [12, 13] achieve that chaotic models can be synchronized when a suitable connection design is found, such as the chaotic time growth of the two- systems become comparable. Chaotic secure communication is presented in three main types: Chaotic modulation, chaotic masking and chaotic shift keying [14, 15]. In this work two levels of chaotic masking are applied to the speech signal.

The outline of this article is as go ahead. In Section 2, we set the description of the proposed system; the aim of the multi chaotic masking; the design of the proposed system with additive white gaussian noise (AWGN) channel has been introduced. In Section 3, we expose the quality measurement of the speech so as to explain the robustness of the model that studied concerning the residual clarity of the ciphered signal and the properties of the received data. In Section 4 the simulation results are obtained include the masking/de-masking process and the results of using the proposed method to reduce the effect of noise. The conclusion is presented in the last section.

2. THE PROPOSED MODEL

The security of the encrypted signal increases proportional to the randomness of the chaotic signal and the size of the key space of the system that be used. In this work double masking to the speech signal based on chaotic signal has been introduced. Each part of the proposed system needs to be synchronized with their identical parts at the receiver side. As a result, self-synchronization (PC) method that proposed by Pecora Carroll has been used in this model, in which two identical systems, one master system (driven) and other slave system (response) can be synchronized, by choosing one of the states of the differential equations of master system as a driven signal to the other side slave system [12]. Lorenz and Rössler consist, the first and the second stages of the proposed model, respectively as clarify in Figure 1. Then the noise effect on the received data has been introduced by applying an AWGN channel to the system, so that a specific method is proposed to reduce noise on the signal by digital processing method to the first chaotic masking. The proposed model components can divided as the following:

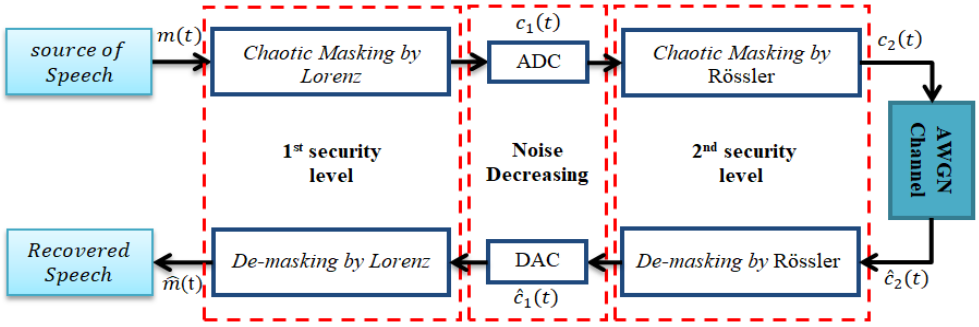


Figure 1. General diagram of proposed model

2.1. Double masking secure communication

There are several applications to the chaotic signal in secure communications such as the parameter chaotic modulation, the chaotic shift keying, the on- off keying, and the chaotic masking [16]. The chaotic masking can be considered the simplest application for the chaotic signal in the secure communications. Also, it can be easily executed in the electronic circuits, so it is used in this proposed system. The schematic of the double masking for the proposed system used in this study is shown in Figure 2.

At transmitter side. In the first block, the Lorenz flow system is used [17], since we have three states in the system $(\dot{x}, \dot{y}, \dot{z})$ and according to self-synchronization, by choice x_{m1} as a chaotic mask to the data, as follow. The Lorenz master system is given by:

$$\begin{aligned} \dot{x}_{m1} &= \sigma(y_{m1} - x_{m1}) \\ \dot{y}_{m1} &= r x_{m1} - y_{m1} - x_{m1} z_{m1} \\ \dot{z}_{m1} &= x_{m1} y_{m1} - b z_{m1} \end{aligned} \quad (1)$$

So, the first masked signal $c_1(t)$ is given by:

$$c_1(t) = m(t) + x_{m1}(t) \quad (2)$$

Where: $m(t)$ is the speech signal.

m & s subscript: is the master and slave systems respectively.

In the second block, the Rössler chaotic system is used and according to self-synchronization, by choosing y_{m2} as the chaotic mask to $c_1(t)$ as follows,

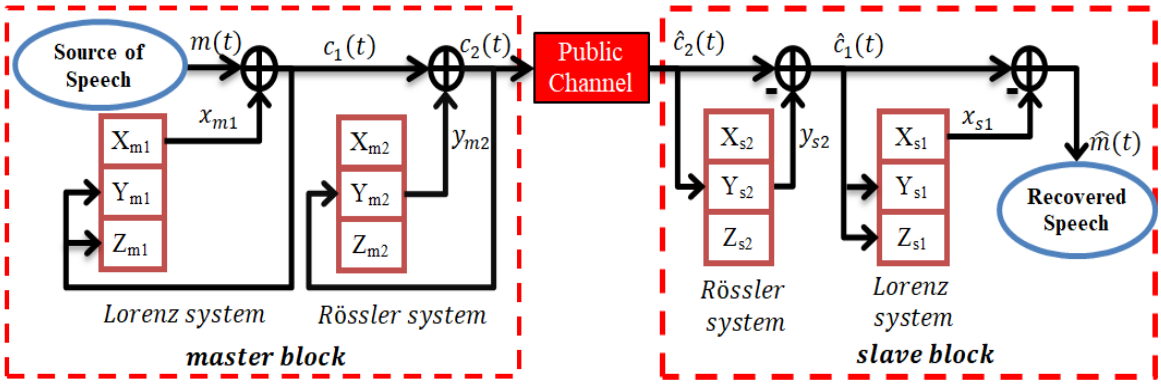


Figure 2. Schematic of double masking proposed system

The Rössler master model is given by:

$$\begin{aligned} \dot{x}_{m2} &= -(y_{m2} + z_{m2}) \\ \dot{y}_{m2} &= x_{m2} + a y_{m2} \\ \dot{z}_{m2} &= b + z_{m2}(x_{m2} - c) \end{aligned} \quad (3)$$

So, the second masked signal $c_2(t)$ which sent to the channel is given by:

$$c_2(t) = c_1(t) + y_{m2}(t) \quad (4)$$

At receiver side. The received signal $\hat{c}_2(t)$ is subtracted from the first block (Rössler slave system) by the chaotic signal y_{s2} to give the recovered signal $\hat{c}_1(t)$ as follows. The Rössler slave system is given by:

$$\begin{aligned} \dot{x}_{s2} &= -(y_{s2} + z_{s2}) \\ \dot{y}_{s2} &= x_{s2} + a y_{s2} \\ \dot{z}_{s2} &= b + z_{s2}(x_{s2} - c) \end{aligned} \quad (5)$$

So, $\hat{c}_1(t)$ is expressed by:

$$\begin{aligned} \hat{c}_1(t) &= c_2(t) - y_{s2} \\ \hat{c}_1(t) &= (c_1(t) + y_{m2}) - y_{s2} \\ &= c_1(t) + e_{r2} \end{aligned} \quad (6)$$

where: $e_{r2} = y_{m2} - y_{s2}$

Finally the recovered information $\hat{m}(t)$is obtained by subtracting $\hat{c}_1(t)$ from the chaotic signal $x_{s1}$of the second block (Lorenz slave system) as follows. The Lorenz slave system is given by:

$$\begin{aligned} \dot{x}_{s1} &= \sigma(y_{s1} - x_{s1}) \\ \dot{y}_{s1} &= r x_{s1} - y_{s1} - x_{s1} z_{s1} \\ \dot{z}_{s1} &= x_{s1} y_{s1} - b z_{s1} \end{aligned} \quad (7)$$

So, $\hat{m}(t)$ is given by:

$$\begin{aligned}\hat{m}(t) &= \hat{c}_1(t) - x_{s1} \\ &= (c_1(t) + e_{r2}) - x_{s1} \\ &= m(t) + e_{l1} + e_{r2}\end{aligned} \quad (8)$$

where: $e_{l1} = x_{m1} - x_{s1}$
The synchronization error between Lorenz drive and response systems is given by:

$$\begin{aligned}e_{l1} &= x_{m1} - x_{s1} \\ e_{l2} &= y_{m1} - y_{s1} \\ e_{l3} &= z_{m1} - z_{s1}\end{aligned} \quad (9)$$

The synchronization error between Rössler drive and response systems is given by:

$$\begin{aligned}e_{r1} &= x_{m2} - x_{s2} \\ e_{r2} &= y_{m2} - y_{s2} \\ e_{r3} &= z_{m2} - z_{s2}\end{aligned} \quad (10)$$

2.2. Double masking secure communication system under the AWGN channel

For practical applications the proposed system was tested and simulated with AWGN channel, so as to study the effect of noise in the reconstructed information and to estimate the amount of power must be added to the signal in order to receive it at good quality. Figure 3 illustrates the proposed double masking secure communication system under the AWGN channel.

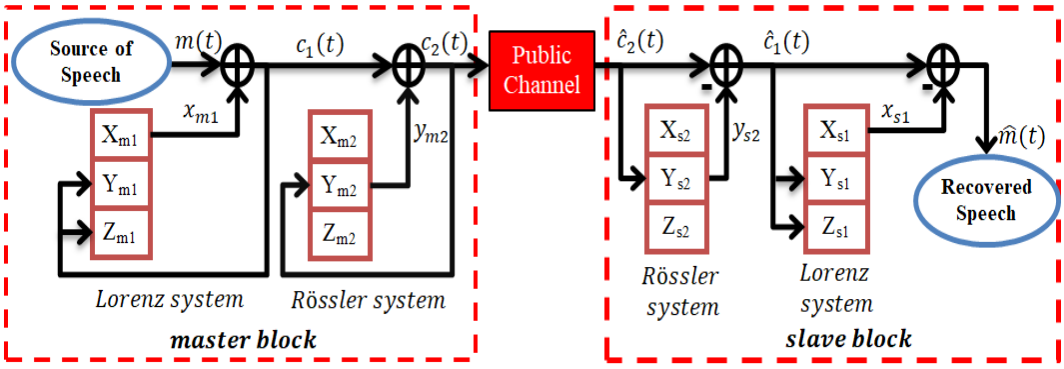


Figure 3. Double masking proposed system under the AWGN channel

The recovered speech signal is affected by noise as follow:

$$s(t) = c_2(t) + n(t) \quad (11)$$

where $\boldsymbol{n}$ $(\boldsymbol{t})$ is Additive White Gaussian Noise (AWGN).
And referred to (7) then

$$\hat{m}(t) = m(t) + e_{l1} + e_{r2} + n(t) \quad (12)$$

2.3. Noise reduction by digital processing method (DPM)

In this method, the first masked signal $c_1(t)$ is transformed from the analog to the digital utilizing (ADC) converter, before make masking with the chaos signal of the second block of the proposed system. At the receiver side, the first recovered signal $\hat{c}_1(t)$ which is binary data form will be changed over back to the analog form by using (DAC) transformer. This conversion of first masked signal to binary form will reduce the impact of noise on the signal. In fact, the samples that converted from the analog to the binary can be acted by (1, 2, 3 or 4.... N_b) bits for each sample [18, 19]. Clear speech is obtained, by increase the number of bits that used. The proposed method is depicted by the subsequent points:

- Make converting to the samples of the first masked signal $c_1(t)$ from analog to the digital form using (ADC).
- Masking the changed over data with the second block chaotic signal.
- Add AWGN channel to the masked signal.
- On the receiver side, and after synchronization of the first block slave system, the binary data was recovered, and then by using (DAC) the sampled data was obtained.

3. QUALITY MEASURMENT OF SPEECH

A numeral of quantities, measurements can be utilized to evaluate the effectiveness of the proposed system concerning security of encrypted signal and the properties of the recovered speech signal. These are signal-to noisy ratio (SNR), (LPC) linear predictive code measure, cepstral distance measure (CD) and mean square error (MSE) [20, 21]. These measurements are defined as follows:

3.1. Segmental spectral signal-to noise ratio

Segmental spectral signal-to noise ratio (SSSNR) is a quantification of noise in a specific signal. It is a collective measurement of the residual clarity of the encrypted speech and the fineness of the reconstructed speech. It is specified by the subsequent equation [22]:

$$\mathrm{SSSNR}\big(\mathrm{s(i)},\mathrm{sn(i)}\big) = 10\log\ \left(\frac{\sum_{\mathrm{i=1}}^{\mathrm{i=l}} \mathrm{s(i)}^2}{\sum_{\mathrm{i=1}}^{\mathrm{i=l}} \big(\mathrm{s(i)}-\mathrm{sn(i)}\big)^2}\right) \quad (13)$$

where l is "number of samples", $\mathrm{s(i)}$ is original signal amplitude and $\mathrm{sn(i)}$ is "the amplitude" of the encrypted or decrypted signal.

3.2. Linear pre-dicative code (LPC)

$$\mathrm{d_{lpc}} = \ln\left(\frac{\mathrm{AVA^T}}{\mathrm{BVB^T}}\right) \quad (14)$$

where: V is the auto-correlation matrix of the actual speech block, vectors A & B contain the LPC coefficient for the pure speech block and the recovered or encrypted speech blocks [23].

3.3. Cpestral distance measure (CD)

$$\mathrm{CD} = 10\log_{10}\left[2\sum_{\mathrm{n=1}}^{\mathrm{p}}\big\{\mathrm{C_x(n)} - \mathrm{C_y(n)}\big\}^2\right]^{\frac{1}{2}} \quad (15)$$

where: $\mathrm{c_y(n)}$ and $\mathrm{c_x(n)}$ are the cepestral coefficients of the original speech and the reconstructed or encrypted speech.

3.4. Mean square error (MSE)

$$\mathrm{MSE} = \frac{\sum(\mathrm{y}-\mathrm{x})^2}{\mathrm{n}} \quad (16)$$

Is the measure of the recovered speech quality, where the smallest value of MSE means good quality of the reconstructed speech signal where (x) is "the original signal", (y) is "the reconstructed signal" and (n) is "the length vector of the signal" [24, 25].

4. SIMULATION RESULTS

In this part, the theoretical analyses and results are presented to explain the effectiveness of the proposed system. The speech file entered through the cool edit96 device, the file with 8 kHz, 8bits per samples, one channel, 42960 samples for 5.3700 second. The simulation results will be presented as follows; double masking implementation of the speech signal from source to destination, the impact of AWGN channel noise on speech data at receiver side includes the results of noise reduction by using digital processing method (DPM), the key space and performance of the proposed model as compared with some encryption systems are presented.

4.1. Simulation results of double chaotic masking

Respect to the process of encryption as explained in section (II.A), the original speech signal entered with 42960 samples, 5.3700 second duration shown in Figure 4(a). Then the masked signal from the first stage of encryption is given in Figure 4(b). Finally the encrypted signal that produced from the two stages of master system is given by Figure 4(c).

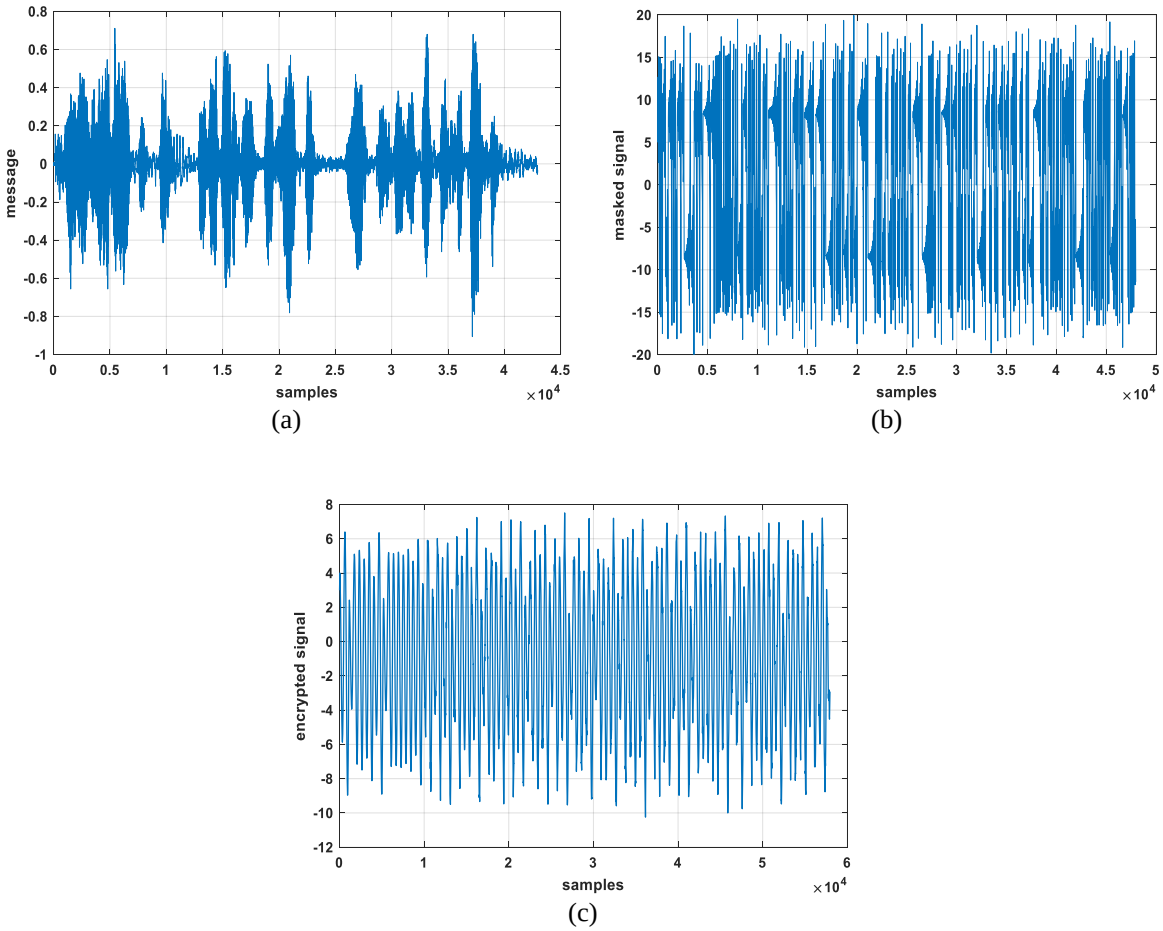


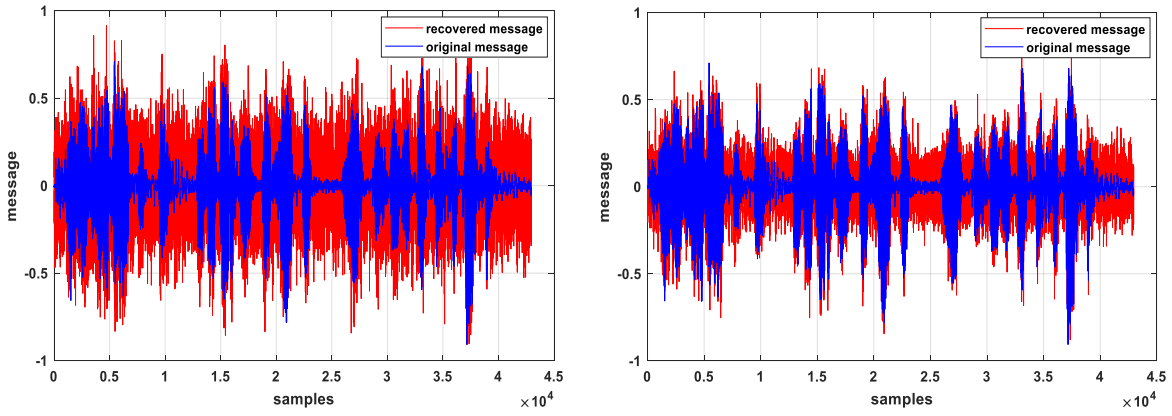
Figure 4. (a) Original speech signal, (b) Masked signal after the first stage of encryption, (c) The encrypted speech

From the above encrypted signal, it is clear that the entire speech data is hidden inside the chaotic signal and this is one of the main requirements to obtain the efficient security. On the slave side, after applying the process of the first and the second de-masking blocks the final recovered speech $\hat{m}(t)$ was obtained which is nearly exact to the original speech data with mean square error (MSE) = $5.2692 * 10^{-6}$.

4.2. Proposed system under AWGN channel

Double mask secure communication system is subjected and tested under the AWGN channel, Table 1 illustrates the effect of noise on recovered speech signal for different SNRs. It is noticeable that the system has poor performance at 32 and 35 dB, while when the SNR is reaching over 37 dB the recovered speech signal becomes clearer (SSSNR have positive value). To clarify this, different SNRs are simulated as in Figure 5.

By using the proposed method DPM, the first masked signal was converted from the analog to the digital form so that the impunity of the change in the masked signal values due to the noise would increase. Table 2 shows the results that obtained by using the proposed scheme at different SNRs. It is seen from this table, in case of 15 and 16 dB, the system has poor execution utilizing the three speech understandability models, from 18 dB and go up, the system execution is enhanced (i.e SSSNR begin to have positive esteem).



(a) (b)

Figure 5. The recovered speech at: (a) SNR=35 dB (b) SNR=39 dB

Table 1. Test the quality of recovered speech for different SNRs

SNR [dB]	LPC	SSSNR [dB]	MSE
29	1.2982	-7.6298	0.0388
32	1.2429	-4.4181	0.0194
35	1.1647	-1.1455	0.0097
37	1.1081	1.0776	0.0061
39	1.0194	3.1674	0.0039
40	0.9980	4.3625	0.0030

Table 2. Test the quality of recovered speech for different SNRs by using (DPM)

SNR [dB]	LPC	SSSNR [dB]	MSE
15	3.4908	-24.5542	2.5657
16	3.1865	-13.0129	0.8723
18	2.5364	19.0608	0.0080
20	1.0246	31.6376	0.0025
21	0.2531	34.2952	$3.7135 * 10^{-6}$
22	0.0993	34.2931	$6.0041 * 10^{-8}$

4.3. Key area

Key area is the overall number of "keys" that can be utilized for the encryption strategy. It should be great enough, to fight the brute force attacker. In our proposed system a high security can be obtained from the secret key is divided on two system Lorenz and Rössler systems as follows:

a) For Lorenz system

The secret key is (σ, r, b_l) a floating point precision of $\Delta = 10^{-2}$ is utilized for the secret keys, therefore the key area is $(10^2)^3 = 10^6$.

b) For Rössler system

The secret key is (a, b_r, c) a floating point precision of $\Delta = 10^{-3}$ is utilized for the secret keys, therefore the key area is $(10^3)^3 = 10^9$. Therefore, the total key space is $(10^6 * 10^9)$ which is a huge key size to resist the common attack.

4.4. Performance comparison of the some encryption systems and double chaotic masking system

For high security the residual intelligibility of encrypted signal should be small as possible to prevent any attacker from reach to encrypted data. For more explained about methods that used for encrypting the self-speech clip considered in this research see [26]. The studied works used are: "Frequency domain scrambling", "Time domain scrambling" also "Two dimensional scrambling" respectively as in Table 3.

Table 3. Proposed model results as compared with some encryption systems

Classical Scrambling	LPC	SSSNR [dB]	CD
Time domain scrambling	0.6532	0.9754	2.4273
Frequency domain scrambling	0.5823	-0.2735	2.5095
Two dimensions scrambling	0.6132	-1.9543	3.2369
	0.9751	-21.5620	3.9661

It is obvious from Table 3 that the studied model is much better than other encryption methods. In public, and after looking to the gained results we observe that the accumulated execution by using doubly chaotic masking utilized, in terms of "SSSNR" is much reduced (from 0.9754 to -21.5620) compared with the time domain method and this indicate of decrease the residual intelligibility of the encrypted data.

5. CONCLUSION

In this paper, an active secure communication system was applied to the information signal based on the double chaotic masking technique. The following conclusions can be drawn from this study: (a) The suggested security approach was implemented by using two different stages of chaotic masking on the signal; one masking was conducted by using Lorenz system and the other masking was built by using Rössler chaotic flow system; (b) A large key space of $(10^6 * 10^9)$ was obtained by using this proposed methodology. The large key space of this model makes the system with a high randomness and more immunity against attacks; (c) By using this double chaotic masking technique, the residual intelligibility of the encrypted data decreased where the SSSNR is much reduced from 0.9754 to -21.5620 which is much lower as compared with some of the previous studies; (d) For usage applications, the proposed system was tested over an AWGN channel and the results showed that the quality of the recovered information begins to be clear at a minimum SNR value of 37 dB with an MSE equal to 0.0061; (e) The digital processing method (DPM) has been combined with this approach to reduce the effect of noise on the recovered information. This combination led to make the proposed approach work properly at SNR of 21 dB with a mean square error $(\text{MSE}) = 3.7135 * 10^{-6}$. Although this combination is very beneficial to improve the quality of the recovered signal, the complication of the system was increased and this will require some increments in the bandwidth of the channel due to the change in the data type from the analog to the binary form.

REFERENCES

[1] Cuomo K.M, Oppenheim A.V, and Strogatz S.H, "Synchronization of lorenz-based chaotic circuits with applications to communications," *IEEE Transactions on circuits and systems II: analog and digital signal processing*, vol. 40, no. 10, pp. 626-633, 1993.

[2] S. Sridharan, E. Dawson, B. Goldburg, "Fast Fourier Transform Based Speech Encryption System," *IEE Proceedings I - Communications, Speech and Vision*, vol. 138, no. 3, pp. 215-223, Jun. 1991.

[3] Milanović V, and Zaghloul M. E, "Improved masking algorithm for chaotic communications systems," *Electronics Letters*, vol. 32, no. 1, pp. 11–12, 1996.

[4] Rupak K., "Design and Implementation of Secure Chaotic Communication Systems," Ph.D. Thesis, University of Northumbria at Newcastle, 2011.

[5] Yu-Min L, Yu-Hong Z, and Jin-Quan Y, "Circuit implementation of secure communication system based on improved chaotic masking algorithm," *Journal of Circuits and Systems*, vol. 14, no. 1, pp. 116–118, 2009.

[6] J. C. Feng, C. K. Tse, "Reconstruction of Chaotic Signals with Applications to Chaos-Based Communications," Tsinghua University Press, 2008.

[7] Arman Kiani-B, *et al*., "A chaotic secure communication scheme using fractional chaotic systems based on an extended fractional kalman filter," *Communications in Nonlinear Science and Numerical Simulation*, vol. 14, no. 3, pp. 863-879, 2009.

[8] X. Li, and Q. Ou, "Dynamical properties and simulation of a new lorenz-like chaotic system," *Nonlinear Dyn*., vol. 65, no. 3, pp. 255-270, 2011.

[9] Y. Zhang, Y, H. Zhao, and L. Zhang, "Synchronization of chaotic system and its application in secure communication, "*In International Conference on Computer Application and System Modeling (ICCASM)*, vol. 14, pp. 94-97, 2010.

[10] Saad S. Hreshee, Hikmat N. Abdullah, and Ameer K. Jawad, "A high security communication system based on chaotic scrambling and chaotic masking," *International Journal on Communications Antenna and Propagation (I.Re.C.A.P.)*, vol. 8, no. 3, 2018.

[11] Fujisaka, H., and Yamada, T, "Stability theory of synchronized motion in coupled-oscillator systems," *Prog. Theor. Phys.*, vol. 69, no. 1, pp. 32-47, 1983

[12] Pecora, L.M., and Carroll, T.L, "Synchronization in chaotic systems," *Phys. Rev. Lett.*, vol. 64, no, 8, pp. 821-824, 1990.

[13] Sivaperumal, S, "Hybrid Synchronization of Identical Chaotic Systems Via Novel Sliding control with Application to Hyperchaotic Vaidyanathan—Volos system," *Int. J. Control Theory Appl*., vol. 9, pp. 261–278, 2016.

[14] Li S, Alvarez G, and Chen G, "Breaking a chaos-based secure communication scheme designed by an improved modulation method," *Chaos, Solitons and Fractals*, vol. 25, no. 1, pp. 109-120, 2005.

[15] Huan Z., Shaofang H., Zuo C., and Xixiang Z., "Dual Key Speech Encryption Algorithm Based Underdetermined BSS," *The Scientific World Journal*, pp. 1-7, 2014.

[16] Nicholas R., "Introduction to Lorenz's System of Equations," Math 6100, Dec. 2003.

[17] B. Sklar, "Digital Communication: Fundamentals and Applications," *Prentice hall publication PTR*, Third Edition, 2011.

[18] Tariq, M.K, "Objective tests of speech signal," M.Sc. Thesis, College of Engineering Al-Mustansiriya University, Department of Electrical Engineering, 2001.

[19] C. Chin Yi, and X. Daolin "Secure digital communication using controlled projective synchronisation of chaos," *Chaos, Solitons and Fractals*, vol. 23, no. 3, pp. 1063-1070, 2005.

[20] Y. Zhang, Y, H. Zhao, L. Zhang, "Synchronization of chaotic system and its application in secure communication," In: *International Conference on Computer Application and System Modeling (ICCASM)*, vol. 14, pp. 94-97, 2010.

[21] Ramin V., "Sequence Synchronization in Chaos-Based Direct Sequence Spread Spectrum Communication Systems," PhD. Thesis, University of Auckland, New Zealand, 2012.
[22] A. V. Prabu, S. Srinivasarao, T. Apparao, M. J. Rao and K. B. Rao, "Audio Encryption in Handsets," *International Journal of Computer Applications*, vol. 40, no. 6, pp. 40-45, 2012.
[23] X. Chen, *et al*., "Adaptive Control of Multiple Chaotic Systems With Unknown Parameters In Two Different Synchronization Modes," *Adv. Differ. Equ*., vol. 231, pp. 1-17, 2016.
[24] Rubak K., K. Busawon, and Z. Ghassemloogy, "Novel Cascade Chaotic Masking For Secure Communication," *In Conference The 9th annual Postgraduate Symposium on the convergence of Telecommunications, Networking & Broadcasting (PGNET 2008)*, At: Liverpool, UK 2008.
[25] A. Abel and W. Schwarz, "Chaos Communications-Principles, Schemes and System Analysis," *Proceedings of The IEEE*, vol. 90, no. 5, pp. 691 –710, 2002.
[26] N. Abdullah, *et al*., "Design of efficient noise reduction scheme for secure speech masked by chaotic signal," *Journal of American Science*, vol. 11, no. 7, pp. 49-55, 2015.

BIOGRAPHIES OF AUTHORS

Ehab AbdulRazzaq Hussein, PhD. MSc. Electrical Engineering was born in Babylon on January 1, 1976. He obtained his BSc degree (1997) in Electrical Engineering at the Faculty of Engineering, University of Babylon and MSc degree (2000), in electrical engineering at the Department of Electrical Engineering, University of Technology and his PhD. Degree from the Department of Electrical Engineering at the Faculty of Engineering, University of Basrah, Currently he works as assistant professor at the Electrical Department at the Faculty of Engineering, University of Babylon. His main interest is signal processing, analysis, information transition, sensors and control system analysis.

Murtadha Khafief Khashan, Electrical Engineer was born in ThiQar, 1991. He obtained his BCs degree (2014) in Electrical Engineering at the Faculty of Engineering, University of Kufa. Currently he is studying for a master's degree in Electrical Engineering at the Faculty of Engineering, University of Babylon. His main interest is communication systems, digital signal processing, measurement and control system analysis.

Ameer K. Jawad was born in Hillah, Iraq, in 1988. He received his BSc degree in Electronic and Communication Engineering from the Electronic and Communication Engineering Department, Al-Hossain University College, Karbala, Iraq, in 2012. He obtained his MSc in Electronic and Communication Engineering from the Electrical Engineering Department, Al-Mostansiria University, Iraq, in 2015. Since 2015, he has been with the staff of the Department of Computer Engineering, Islamic University College, Najaf –Iraq.