A Speech Cryptosystem Based on Chaotic Modulation Technique

Mahmoud F. Abd Elzaher[*1], Mohamed Shalaby[**2], Yasser Kamal[**3], Salwa El Ramly[*4]

[*]*Department of Electronics and Electrical Communications, Faculty of Engineering,*

Ain Shams University, Cairo, Egypt

[1]8273@eng.asu.edu.eg

[4]Salwa_elramly@eng.asu.edu.eg

[**]*Department of Computer Science, Arab Academy for Science, Technology*

& Maritime Transport, Cairo, Egypt

[2]myousef73@hotmail.com

[3]dr_yasser_omar@yahoo.com

Abstract: ***In this paper, an encryption approach for Speech communication based on direct chaotic modulation (non-autonomous modulation) is presented, in which speech signal is injected into one variable of the master system (using Lorenz system) without changing the value of any control parameter. This approach is based on the change of chaotic signal by injecting Speech samples into one variable in chaotic system and hence generating a new chaotic signal. The Speech signal is then extracted from the chaotic signal on the receiver side. Furthermore, a high dimension chaotic system is used, which increases the security of the encrypted signal. Non-autonomous modulation technique is suitable for securing real-time applications. A comparative study of approach and Speech masking technique is also presented. Experimental results show that non-autonomous methods give better performance than their chaotic masking counterparts when they are analyzed against Signal-to-Noise-Ratio (-38.55 dB vs. -35.51 dB), Segmental signal-to-Noise-Ratio (-38.91 dB vs. -35.84 dB), Log-Likelihood Ratio (0.89 vs. 0.80), and Correlation Coefficient Analysis (0.0345 vs. 0.021). Non-autonomous techniques overcome the chaotic masking break and considered more secure.***

Keywords: ***Encryption; Speech encryption; Chaotic Modulation; Non-autonomous modulation; Lorenz system.***

1 INTRODUCTION

Speech communication is in close relation with daily life, such as education, commerce, politics, e-learning and news telecasting. With the advancement of modern telecommunication and multimedia technologies, Modern Speech communication systems demand a huge amount of information to be exchanged across Social Networks and the Internet every day so the need for encryption and security has increased. The conventional cryptographic techniques may be efficient for the text data; however, they are unsuitable to the bulk data capacity. One of the techniques that provide fast and highly secure encryption methods is chaos-based techniques. Continuous cryptographic systems have been developed which use the synchronization between the transmitter and receiver to retrieve data transmitted through an insecure medium.

The first generation of these systems is masking. A Speech masking technique based on Lorenz System is presented in [1, 2] which uses Lorenz equation to generate Chaotic Signals, these signals are used as a base carrier signal on which the information signal is modulated at the transmitter side. The information signal is then recovered at the receiver side. The method of masking has been shown to be insecure as there are various cryptanalysis methods [3] that make it possible to estimate the sender dynamics and decoding of the message signal.

The second generation is the parameter and non-autonomous modulation techniques. Non-autonomous techniques were developed to overcome the chaotic parameter modulation break, which includes the return map, and adaptive observer [4]. Non-autonomous modulation is considered to be more secure than parameter modulation.

The main goal of this paper is proposing a Speech encryption system that provides users with a high degree of confidence and key sensitivity, and preserving a good quality of the reconstructed speech signal by chaotic systems. In section 2, Chaos-based cryptography systems are discussed. In Section 3, a speech masking technique based on Lorenz System is presented. In Section 4, the proposed

encryption approach is presented. The results of applying our proposed approach are shown in Section 5. Finally, our work is concluded in section 6.

2 CHAOTIC SYSTEM

Chaos theory was originally developed by mathematicians and physicists. The theory deals with the behaviors of nonlinear dynamic systems. Chaos theory has desirable features, such as deterministic, nonlinear, irregular, long-term prediction, and sensitivity to initial conditions. Therefore, and based on chaos theory features, the security research community adopts chaos theory in modern cryptography. A function that possesses a kind of chaotic behavior is defined as a chaotic flow or map. In the following subsections, we discuss one type of chaotic systems (which we used to implement our proposed system), namely, Lorenz system.

Lorenz system can be described with three dimensions as shown in equations (1, 2 and 3).

$$\dot{X}(t) = \sigma(Y(t) - X(t)) \quad (1)$$

$$\dot{Y}(t) = rX(t) - X(t)Z(t) - Y(t) \quad (2)$$

$$\dot{Z}(t) = X(t)Y(t) - pZ(t) \quad (3)$$

where $X(t), Y(t), Z(t)$ are the Lorenz chaotic variables, $X(0), Y(0), Z(0)$ are initial conditions, and σ, r and p are positive constants with $r \geq 24.74$. Figure 1 shows a 3D figure of Lorenz chaotic system.

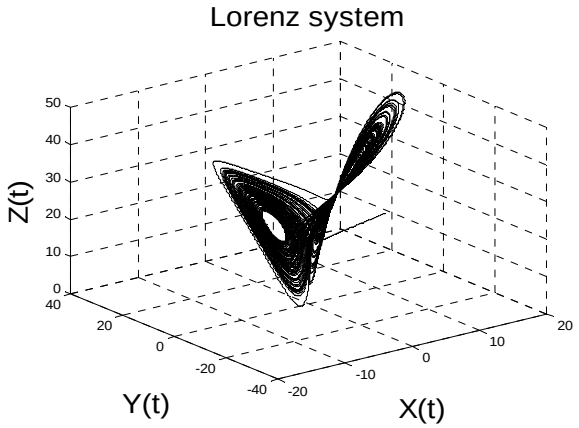


Figure 1: The 3D figure of Lorenz chaotic system

3 A SPEECH MASKING TECHNIQUE BASED ON LORENZ SYSTEM

The block diagram of the designed chaotic masking scheme is shown in Figure 2. The speech signal S_n is added to the Lorenz chaotic generator signal X_m which also acts as a driving signal for synchronization as will be explained later (Pecora-Carroll Synchronization). The speech signal is precisely recovered at the receiver by the subtraction of the receiver's regenerated drive signal from the received signal [1, 2].

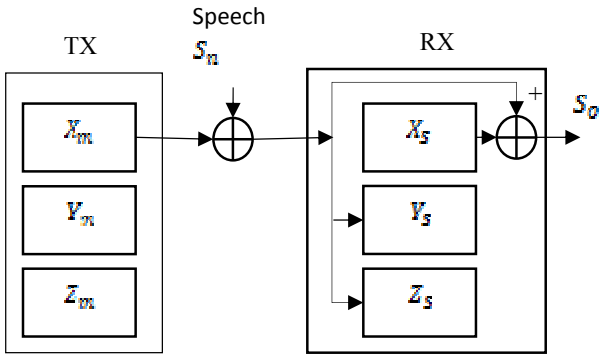


Figure 2: Chaotic masking and recovery information based on Lorenz system.

Here, we implement the master subsystem using equations (4, 5, and 6) related to Lorenz equations (1, 2, and 3). We note that S_n is the input Speech sample.

$$\dot{X}_m = F(X_M, Y_M, Z_M) + S_n \quad (4)$$

$$\dot{Y}_m = G(X_M, Y_M, Z_M) \quad (5)$$
$$\dot{Z}_m = W(X_M, Y_M, Z_M) \quad (6)$$

The slave subsystem uses Lorenz equations (7, 8, 9, and 10) to decrypt the encrypted signal.

$$\dot{X}_s = F(X_s, Y_s, Z_s) \quad (7)$$
$$\dot{Y}_s = G(X_M, Y_s, Z_s) \quad (8)$$
$$\dot{Z}_s = W(X_M, Y_s, Z_s) \quad (9)$$
$$S_O = X_M - X_s \quad (10)$$

4 THE PROPOSED CRYPTOSYSTEM

The proposed cryptosystem is shown in Figure 3. The samples of Speech signal S_n are injected into the chaotic generator (master system) which also acts as a driving signal for synchronization. The Speech signal is precisely recovered at the receiver side (slave system) by the subtraction of the receiver's regenerated drive signal from the received signal [4]. We implement our proposed system using Lorenz system.

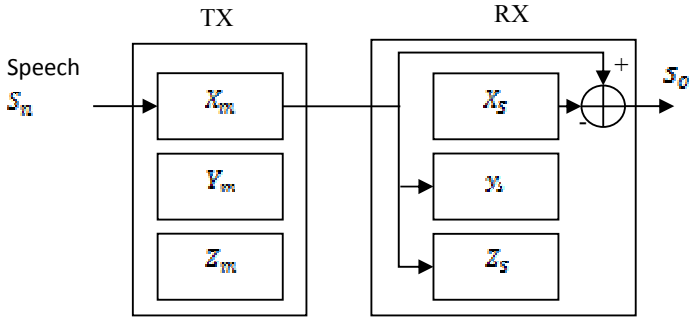


Figure 3: THE PROPOSED CRYPTOSYSTEM

Here, the master subsystem is implemented using equations (11, 12, and 13) related to Lorenz equations (1, 2, and 3). It is to be noted that $S_n$is the input Speech sample, it is clear that S_n is now a parameter of function F.

$$\dot{X}_m = F((X_M + S_n), Y_M, Z_M) \quad (11)$$
$$\dot{Y}_m = G(X_M, Y_M, Z_M) \quad (12)$$
$$\dot{Z}_m = W(X_M, Y_M, Z_M) \quad (13)$$

The slave subsystem uses Lorenz equations (14, 15, 16, and 17) to decrypt the encrypted signal.

$$\dot{X}_s = F(X_s, Y_s, Z_s) \quad (14)$$
$$\dot{Y}_s = G(X_M, Y_s, Z_s) \quad (15)$$
$$\dot{Z}_s = W(X_M, Y_s, Z_s) \quad (16)$$
$$S_O = X_M - X_s \quad (17)$$

- *Pecora-Carroll (PC) Synchronization*

In order to receive the Speech signal sample successfully, chaotic signals on both Transmitter (Master) and Receiver (Slave) must be synchronized, one of the efficient synchronization schemes that can be used is Pecora-Carroll (PC) Synchronization [5]. In this scheme, a driving signal is sent from the chaotic generator at the transmitter, to the chaotic generator at the receiver. At the receiver, state error vectors which describe the difference between the encryption and decryption state variables are constructed (equations 18, 19, 20). Figure 4 shows the block diagram of the mechanism of PC synchronization of Lorenz system.

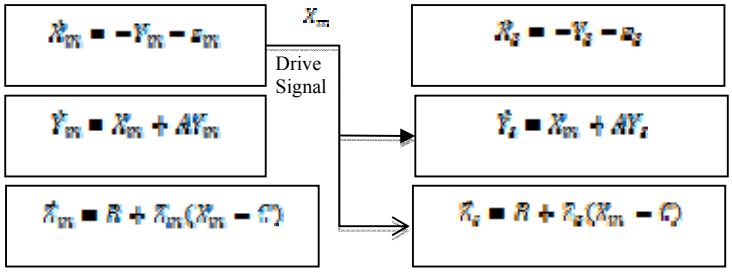


Figure 4: PC synchronization of Lorenz system

State error vectors (synchronization error) which describe the difference between the master and slave state variables are constructed. Equations (24, 25 and 26) show that the variables e_x, e_y, and e_z represent the synchronization error of X, Y, and Z, respectively, in our proposed system using Lorenz equations. Figure 5 shows this synchronization error.

$$e_x = X_M - X_S \quad (18)$$

$$e_y = Y_M - Y_S \quad (19)$$

$$e_z = Z_M - Z_S \quad (20)$$

It has been shown that with the aid of the driving signal these states errors can be reduced to zero after a certain amount of time as shown in Figure 5.

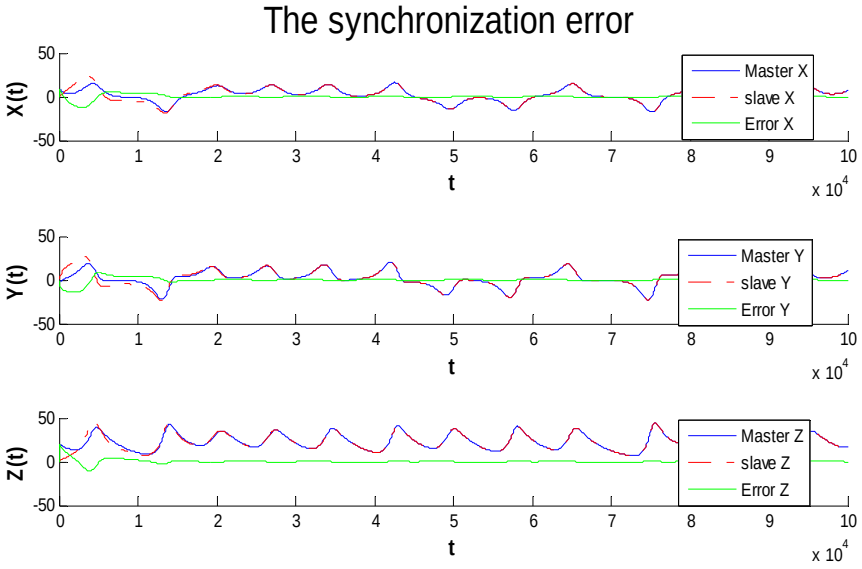
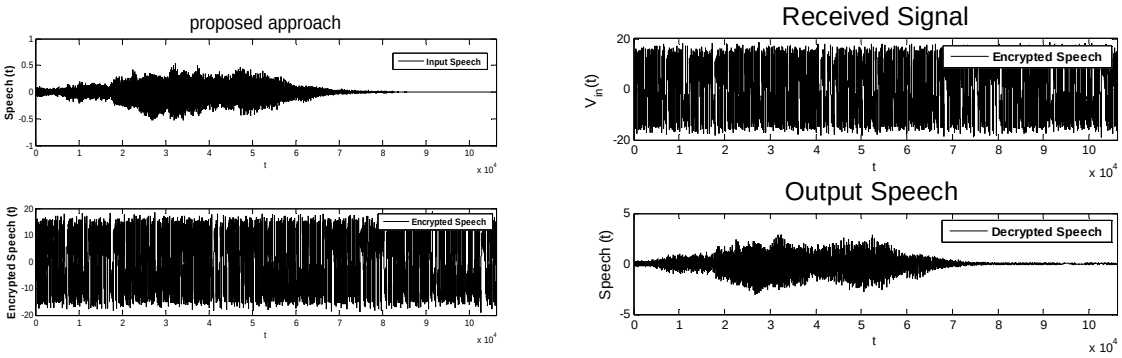


Figure 5: The synchronization error of (X,Y and Z) in the proposed system using Lorenz system

5 EXPERIMENTAL RESULTS AND ANALYSIS

In section 4, we presented our proposed system, which is implemented using Lorenz system, and the Speech samples, which are embedded in the chaotic signal to generate a new chaotic signal. The Speech signal is then extracted from the chaotic signal at the receiver side. Figure 6(a) shows the waveform of the original signal and the waveform of the encrypted signal for the proposed approach. Figure 6(b) shows the waveform of the received signal and the waveform of the decrypted signal for the proposed approach. Figure 7 shows the autocorrelation of the proposed approach transmitted signal. The autocorrelation function used to measure randomness, an ideal random sequence should be uncorrelated.



(a) **(b)**

Figure 6. Proposed approach (encrypted signal - decrypted signal)

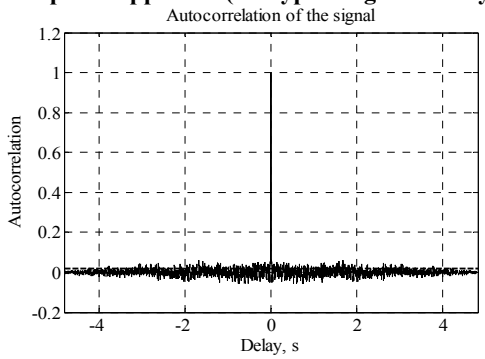


Figure 7: Proposed approach (autocorrelation of the transmitted signal)

Figure 8 shows that, unlike masking $x(t)$ using Lorenz system to the original signal, which makes slight change to the original signal, embedding voice samples to $x(t)$ using Lorenz system (direct modulation) makes significant changes to the original signal.

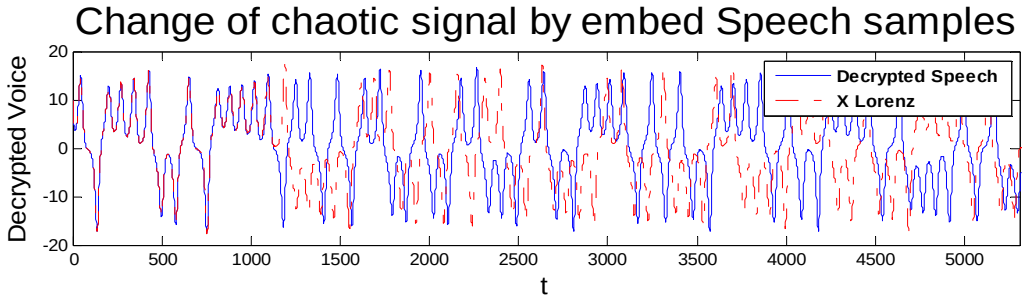


Figure 8: The effect of injecting Speech samples to Lorenz system

Figure 9 shows the effect of masking Speech samples to $x(t)$ of Lorenz system.

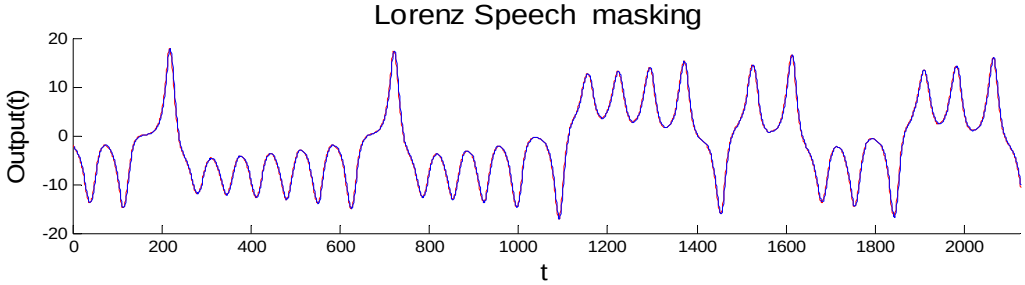


Figure 9. The effect of masking Speech samples to Lorenz system

In the following subsections, we analyze the results of applying the proposed approach according to different perspectives. In section (A), we present a comparative study between our proposed Non-autonomous approach and its chaotic masking counterpart because the results are not similar. In sections (B) and (C) there is no significant difference

between the results of our proposed Non-autonomous approach and its chaotic masking counterpart, therefore we limit our self to show the results of our proposed Non-autonomous approach.

A. Statistical Analyses

To statistically analyze our results, four different measures [6] are used, Signal-to-Noise-Ratio (SNR), Segmental signal-to-Noise-Ratio (SNRseg), Log-Likelihood Ratio (LLR), and Correlation Coefficient Analysis (CCA). Tables 1, and 2 show the average result of these measures and chaotic masking based on Lorenz system.

TABLE 1

STATISTICAL ANALYSES OF SNR, SNRSEG, LLR, AND CCA FOR ENCRYPTED SIGNAL

Approach	**SNR**	**SNRseg**	**LLR**	**CCA**
Proposed approach	-38.55 dB	-38.91 dB	0.89	0.0345
Masking using Lorenz system	-35.51 dB	-35.84 dB	0.80	0.012

TABLE 2

STATISTICAL ANALYSES OF SNR, SNRSEG, LLR, AND CCA FOR DECRYPTED SIGNAL

Approach	**SNR**	**SNRseg**	**LLR**	**CCA**
Proposed approach	5.01dB	4.99 dB	0.213	0.82
Masking using Lorenz system	2.75 dB	2.50 dB	0.1	0.8519

B. Spectrogram Analyses

A spectrogram is a powerful tool that divides the Speech sample into multiple “blocks" (in the time domain) then plotting the Fast Fourier Transform (FFT) of each block and displaying all of them in the same graph [7, 8]. Figure 10 shows the spectrogram of the original signal frequency versus time and the spectrogram of the encrypted signal frequency versus time (proposed approach).

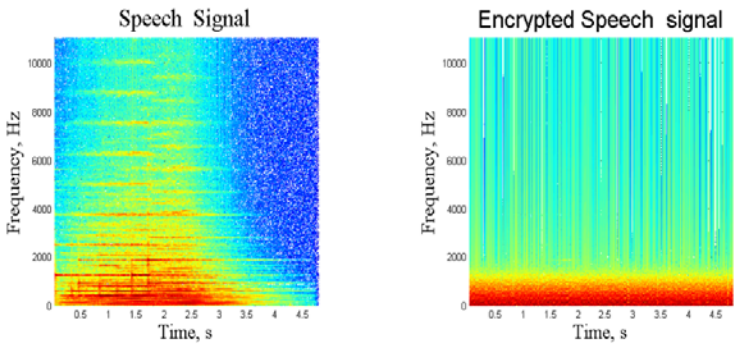


Figure 10: Proposed approach spectrogram (Original signal - encrypted signal)

C. Histogram analysis

Distributions of data values in a system comprise the histogram. Histogram analysis can be made by examining data distributions in many different fields [9]. In encryption practices, if the distributions of numbers that represent encrypted data are close, this means that encryption is performing well. The closer the encrypted data distributions are, the higher their encryption levels. Figure 11 shows the distribution versus sample value (for proposed approach).

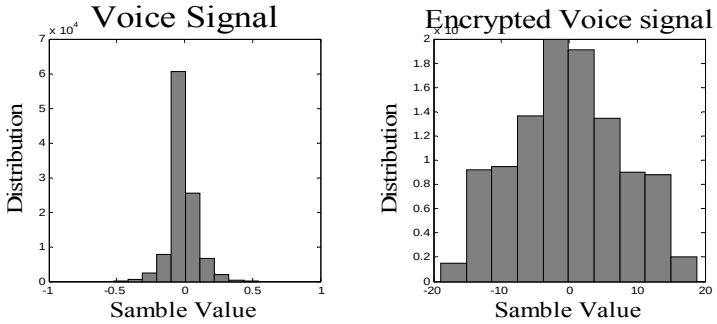


Figure 11: First proposed approach Histogram (Original signal - encrypted signal)

D. Key Sensitivity and Key Space

Key sensitivity analysis is the most important criteria of the performance analysis of the encryption system. A good encryption algorithm should be sensitive to the initial condition and key value. Lyapunov exponent (LE) [4] can be used to evaluate the chaotic system sensitivity to the initial condition. The larger value of Lyapunov exponent values the chaotic system has the more sensitivity of this system to the initial condition. Figure 12 shows dynamics of Lyapunov of Lorenz system.

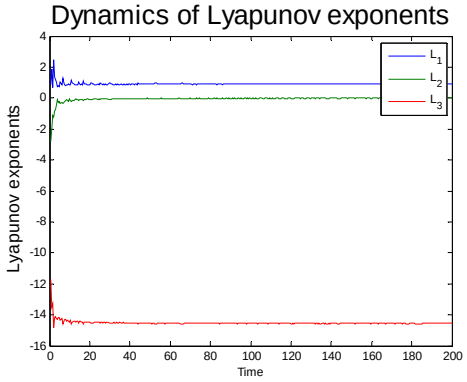


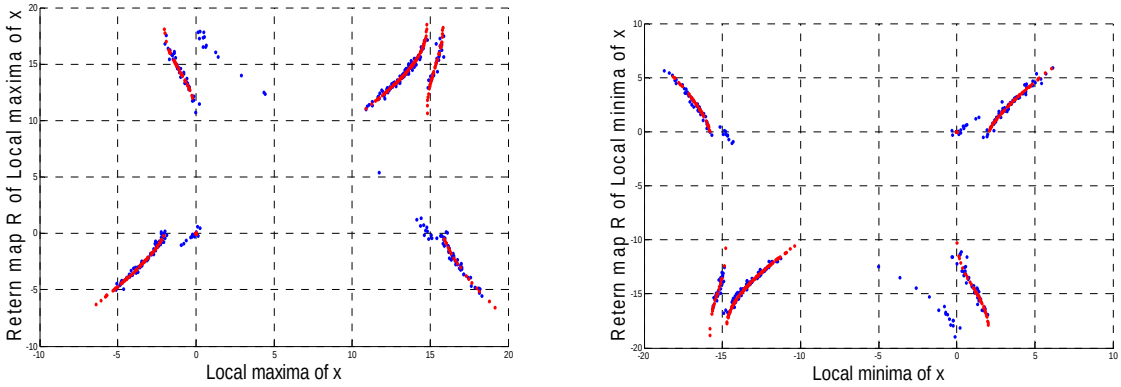
Figure 12: Dynamics of Lyapunov exponents of Lorenz system

It is well demonstrated that the Lorenz system has two positive Lyapunov exponents and a small negative Lyapunov exponent [10], that is, the leading positive LE l_1 of the Lorenz system is equal to 0.9051 and the second positive LE l_2 has a value of 8.12*10^{-4}, the negative Lyapunov exponent positive LE l_3 of the Lorenz system is equal to -14.5718. The Lyapunov exponents provide a good indication of how chaotic the Lorenz systems are. Hence, this explains why the system is very sensitive to initial conditions and more unpredictable than other systems. In our approaches a small change in parameters leads to different results during the decryption, the data cannot be decrypted without knowing all parameters because the decryption does not happen in the correct order. The size of the key space defines the total number of different keys that are used for the encryption / decryption algorithm. It should be large enough to resist the attack. The key space depends on the initial conditions and the control parameters of chaotic system. In Lorenz system, we use three initial conditions and three control parameters.

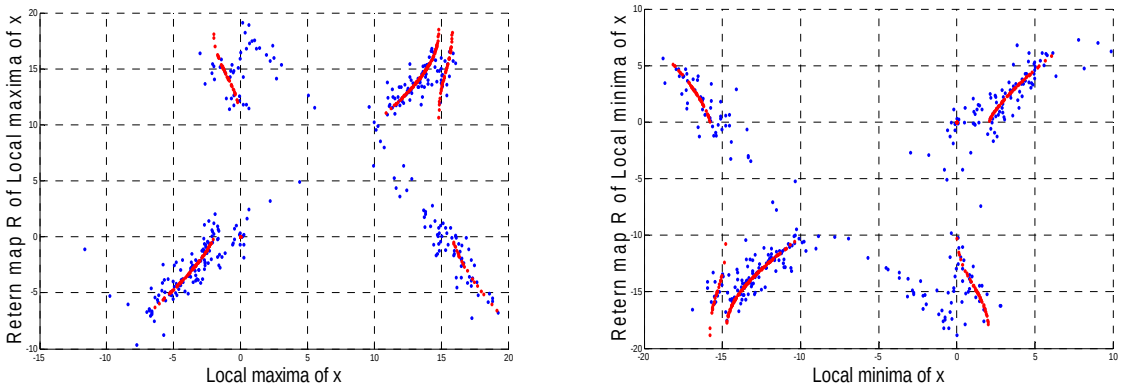
6 THE CONCRETE ADVANTAGES OVER THE CHAOTIC MASKING TECHNIQUE

There are different cryptanalysis techniques (return map) that make the methods of masking insecure, as these techniques can estimate the sender parameters and hence decrypt the message signal correctly. Non-autonomous techniques were developed to overcome the chaotic masking and chaotic parameter modulation break and considered more secure. A voice masking technique based on Lorenz chaotic flow is presented in [1, 2]. We also presented a comparative study between our approach (non-autonomous modulation using Lorenz chaotic flow) as well as the conventional chaotic masking methods using Lorenz chaotic flow. Experimental results show that the non-autonomous methods give similar results of spectrogram, histogram, key sensitivity and key space

analysis compared with their chaotic masking counterparts and better performance than their chaotic masking counterparts when they are analyzed against SNR (-38.55 dB vs. -35.51 dB), SNRseg (-38.91 dB vs. -35.84 dB), LLR (0.89 vs. 0.80) and CCA (0.0345 vs. 0.021). Figure 13 shows the return map of the proposed algorithm. In figure 13 (a), the red dots represent the return map of the Lorenz system, and the blue dots represent the return map using masking techniques. This indicates that the return map of the proposed system is blurred by the signal from the permutation generator. Figure 13 (b) shows the effect of the injected data on the return map. Clearly, the data signal increases the blurriness of the return map, which is desirable.



(a)



(b)

Figure 13: The return map of the proposed approach vs. their chaotic masking counterpart

7 CONCLUSIONS

We proposed a new chaotic-based crypto system; this system depends on the change of chaotic signal by injecting Speech samples into one variable of the master system to generate a new chaotic signal. The dynamics and decoding of this new chaotic signal is very hard to be estimated, and hence, the proposed system overcomes the disadvantages of Chaotic Masking and parameter modulation techniques. Non-autonomous modulation approaches were used to implement the proposed system using Lorenz system. Although Non-autonomous approaches give similar results of spectrogram, histogram, key sensitivity and key space analysis compared with their chaotic masking counterpart, experimental results show that Non-autonomous approaches give better performance than their chaotic masking counterpart when they are analysed against Signal-to-Noise-Ratio, Segmental signal-to-Noise-Ratio, Log-Likelihood Ratio, and Correlation Coefficient Analysis. The proposed Non-autonomous modulation approach is sensitive to the initial conditions and control

parameters, which means it is difficult to decrypt the encrypted signal correctly if there is a very small change between encryption and decryption keys.

REFERENCES

[1] Rahul Ekhande, Sanjay Deshmukh, "Chaotic Signal for Signal Masking in Digital Communications", *IOSR Journal of Engineering ISSN* (e): 2250-3021, ISSN: 2278-8719 Vol. 04, Issue 02, pp. 29-33, February. 2014.

[2] Hikmat N, Saad S.," Design of Efficient Noise Reduction Scheme for Secure Speech Masked by Chaotic Signals", *Journal of American Science,* Vol. 11, No.7 , pp.49-55, Nov. 2015.

[3] Kevin M. Short, "Steps toward unmasking secure communications", *International Journal of Bifurcation and Chaos*, Vol. 4, pp. 959-977, 1994.

[4] M. Haroun, T. A. Gulliver, "Real-Time Image Encryption Using a 3D Discrete Dual Chaotic Cipher", *International Journal of Electrical, Computer, Energetic, Electronic and Communication Engineering* Vol. 9, No: 3, pp. 415-422 2015.

[5] Rahul Ek., Sanjay De., "Chaotic Synchronization in Digital Communication", *International Journal of Engineering Research*, Volume 3, Issue No.7, pp. 458-461, July 2014.

[6] Santo Banerjee, Politecnico Di, "*Chaos Synchronization and Cryptography for Secure Communications Applications for Encryption*". Information Science Reference, 2011.

[7] Branislav Jovic, *Synchronization Techniques for Chaotic Communication Systems*, Signals and Communication Technology, ISBN: 978-3-642-21848-4, 2011.

[8] Dennis luke owuor "Chaos-based secure communication and systems design "master thesis, faculty of engineering and the built environment, Tshwane University of technology, 2012.

[9] Hala B., Sundus I. Mahdi, "Modify Speech Cryptosystem Based on Shuffling Overlapping Blocks Technique", *International Journal of Emerging Trends & Technology in Computer Science* Volume 4, Issue 2, pp. 70-75, 2015.

[10] E. Mosa, O. Zahran, "Chaotic encryption of speech signals", *International Journal of Speech Technology* Volume 14, Issue 4, pp. 285-296 , December 2011.

[11] M. Ashtiyani, P. Moradi Birgani, S. Karimi Madahi, "Speech Signal Encryption Using Chaotic Symmetric Cryptography", *Journal of Basic and Applied Scientific Research*, Vol. 2, No. 2, pp. 1678-1684, 2012.

[12] Osama Faragallah, Elsayed Elshamy, Sayed El-Rabaie, "Speech Encryption Based on Arnold Cat Cap and Double Random Phase Encoding", *International Journal of Speech Technology*, Vol. 21, No. 5, pp. 14-24, 2013.

[13] Meador, Clyde-Emmanuel Estorninho, "Numerical Calculation of Lyapunov Exponents for Three-Dimensional Systems of Ordinary Differential Equations" Theses, Theoretical Physics Project, Semantic Scholar, 2011.

[14] Jo Bovy, "Lyapunov Exponents and Strange Attractors in Discrete and Continuous Dynamical Systems". Theoretical Physics Project, Marshall Digital scholar, Marshall University, 2014.

BIOGRAPHY

Mahmoud Fawzy, BSc in Electrical Engineering, Alexandria University. Currently works with the Air Force Defense. Fields of interest: electrical engineering and communication systems.

Mohamed Shalaby, PhD in Computer Science, University of Bradford, United Kingdom. Currently works with the Arab Academy for Science, Technology & Maritime Transport and Air Force Defense. Fields of interest: Computer Science.

Yasser Kamal, PhD in Computer Science. Currently works with the Arab Academy for Science, Technology & Maritime Transport. Fields of interest: Computer Science.
.

Salwa El Ramly, PhD in Electrical Engineering from Nancy University, France. Professor in the Electronics and Communication Engineering Department, Faculty of Engineering, Ain Shams University. Fields of interest: Communication systems & Signal Processing

نظام تأمين للكلام مبنى على تقنية التعديل الفوضوى المباشر

محمود فوزى[1]*، محمد شلبى[2]**، ياسر كمال[3]**، سلوى الرملى[4]*
كلية الهندسة، جامعة عين شمس
**كلية الهندسة والتكنولوجيا، الاكاديمية العربية للعلوم والتكنولوجيا و النقل البحرى
[1]8273@eng.asu.edu.eg
[2]myousef73@hotmail.com
[3]dr_yasser_omar@yahoo.com
[4]Salwa_elramly@eng.asu.edu.eg

ملخص
نقدم تقنية لتشفيرنظم التخاطب عبر وسائل الإتصال مبنيا على التعديل الفوضوى المباشر حيث يتم تضمين أو حقن إشارات المحادثة الصوتية داخل متغير واحد من النظام الفوضوى الرئيسي (بإستخدام نظام لورينز) دون تغيير قيم الخصائص المسيطرة على النظام الفوضوى. ويستند هذا النهج على تغيير الإشارة المولدة من النظام الفوضوى عن طريق حقن الإشارات لمتغير واحد في نظام الفوضوى وينتج عن ذلك توليد إشارة فوضويه جديدة. ثم يتم إستخراج إشارات المحادثة الصوتية من الإشارة الفوضوية بواسطة النظام الفوضوى المستقبل. وعلاوة على ذلك، يتم إستخدام نظام الفوضوى متعدد الابعاد ليزيد من تأمين الإشارة المشفرة. تقنية التعديل الفوضوى المباشره مناسبة لتأمين التطبيقات في الوقت الحقيقي. ونقدم أيضا دراسة مقارنة بين هذه التقنية و تقنية الإخفاء الفوضوى لإشارات التخاطب. وقد أظهرت النتائج أن التعديل الفوضوى المباشر يزيد من أمن نظام التشفير.