International Journal of Electrical and Computer Engineering (IJECE)
Vol. 10, No. 5, October 2020, pp. 4824~4834
ISSN: 2088-8708, DOI: 10.11591/ijece.v10i5.pp4824-4834

A new dynamic speech encryption algorithm based on Lorenz chaotic map over internet protocol

Obaida M. Al-Hazaimeh
Department of Computer Science and Information Technology, Al- Balqa' Applied University, Jordan

Article Info

Article history:

Received Feb 3, 2020
Revised Mar 13, 2020
Accepted Mar 24, 2020

Keywords:

AMR-WB-G.722.2
Chaos-theory
Cryptography
IP telephony
Lorenz map

ABSTRACT

This paper introduces a dynamic speech encryption algorithm based on Lorenz chaotic map over internet protocol to enhance the services of the real-time applications such as increases the security level and reduces latency. The proposed algorithm was divided into two processes: dynamic key generation process using 128-bit hash value to dynamically alter the initial secret keys, and encryption and decryption process using Lorenz system. In the proposed algorithm, the performance evaluation is carried out through efficient simulations and implementations and statistical analysis. In addition, the average time delay in the proposed algorithm and some of the existing algorithms such as AES is compared. The obtained results concluded that, the proposed dynamic speech encryption algorithm is effectually secured against various cryptanalysis attacks and has useful cryptographic properties such as confusion and diffusion for better voice communication in the voice applications field in the Internet.

Corresponding Author:

Obaida M. Al-hazaimeh,
Department of Computer Science and Information Technology,
Al- Balqa' Applied University,
21163, Jordan.
Email: dr_obaida@bau.edu.jo

1. INTRODUCTION

Voice application over Internet protocol (i.e., VoIP) is a IP telephony technology that allows the voice data as human voice to transfers in real-time over Internet Protocol (i.e., IP) in a manner that emulates the traditional telephone service (i.e., PSTN) [1, 2]. In general, the voice application over internet protocol only requires an program on the end-point computer (i.e., sender, or receiver) capable of encoding and decoding transmitting speech and Internet access [3, 4].

Voice application over internet protocol technology provides more advantages when it is compared to the traditional telephone service. IP telephony technology is cheaper, can be integrated with other media services, portable, and allows for more efficient bandwidth utilization. Therefore, the service providers prefer the IP telephony technology as a method to reduce the cost over existing multimedia services. Moreover, the infrastructure of the IP telephony is considered as a solid economical ground in building the more recent revenue-generating services. Markedly, the deployment of IP telephony technology is becoming more popular and is considered as an integral part of a global competitive landscape [5, 6]. Despite of all these positive features, the IP telephony technology is facing some difficulties and challenges such as security, packet loss, and latency. Consequently, more advanced techniques or strategies are warranted to competently manage these difficulties, which are expected to ensure the quality of the IP telephony technology services (i.e., QoS) [3, 7]. For example, the threat of the intruders over IP networks is the greatest security challenge in IP telephony technology. The later will be a great concern since these offenders utilize various sniffing tools to compromise the conversation of the IP telephony. To managing the security challenges, cryptography serves as a valuable tool to maintain data secrecy [8, 9].

The science of cryptology consists of two major parts: cryptography and cryptanalysis. The science of cryptology and its cryptographic primitives are categorized as illustrated in Figure 1. While cryptography is the art of maintaining data secrecy against unauthorized access (i.e., intruders), on the other sided, cryptanalysis is about analyzing and handling infringement of secure communication [10, 11].

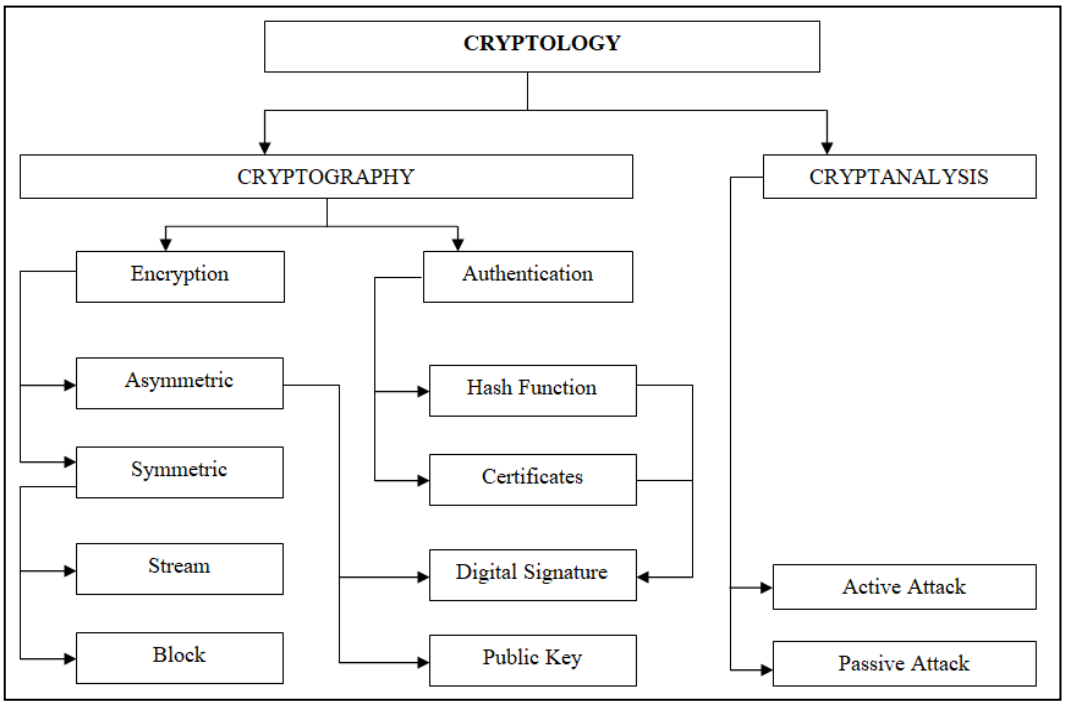

Figure 1. Taxonomy of cryptology

To maintain data secrecy against unauthorized access over IP networks the cryptography is widely used. However, most of the existing cryptographic algorithms are built to maintain text data secrecy. Therefore, these existing algorithms are not suitable for voice applications over internet protocol because it involves extensive computation and consumed a large amount of time (i.e., delay) [5, 12]. The following four performance factors: encryption delay, the security level, message delay, and processing power are mainly used to measure the VoIP security. The security level (i.e., complexity) of the security algorithm seems to have an impact on these measurement factors [8, 13, 14]. Constructing new speech encryption algorithms based on chaos theory to increase the security level has drawn for many scientists and researchers attention [15-21], but unfortunately some of these constructed algorithms have a number of practical problems in terms of cryptanalysis attacks [22, 23]. In this paper, a new dynamic speech encryption algorithm using Lorenz chaotic map over IP network is proposed. While generating a chaotic key stream, the system parameters and 128-bit hash value of the plain-speech are included in the proposed algorithm to obtain a highest security level.

The rest of this paper is organized into 5 sections including the introduction as follows: section 2 has described the proposed algorithm based on Lorenz system. Section 3 describes simulation result and security analysis, and explains the procedures used to test the proposed algorithm. In section 4, a comparison with existing work is given and finally conclusion is presented in sections 5.

2. PROPOSED ALGORITHM

In practical, Lorenz chaotic map has useful cryptographic properties such as confusion and diffusion, sensitivity to initial conditions and parameters, and un-predictability [20]. Therefore, Lorenz chaotic map is used in this paper to propose a new symmetric speech encryption algorithm. It consists of two major parts: keys generation using 128-bit hash value of plain speech frame and the logistic, and encrypting the speech frame using chaotic sequences which are generated by Lorenz system. The overall block diagram of the proposed algorithm architecture can be illustrated by Figure 2.

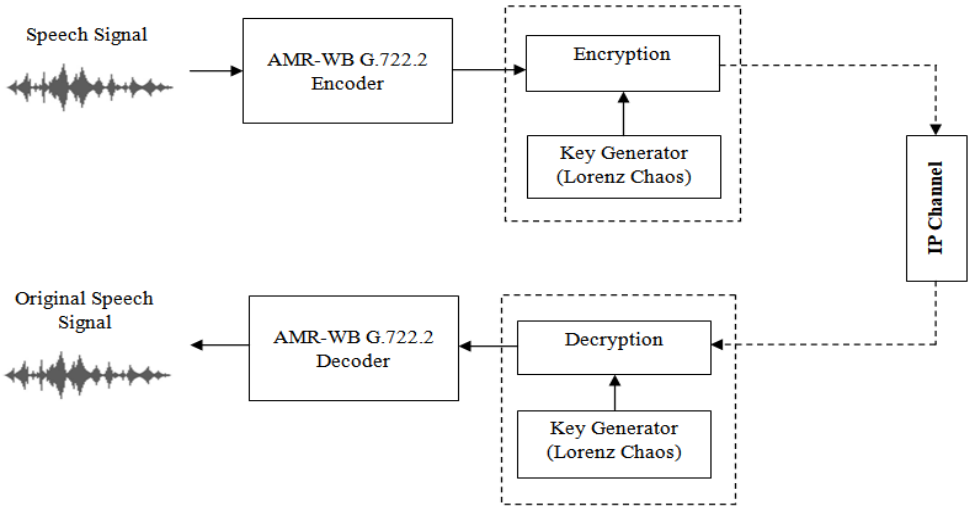

Figure 2. Block diagram

Below, we will provide an introductory definition of the Lorenz system and analyze its main positive features regarding to cryptography. Then, the steps to implement such a process of the encryption parts will be discuss. The decryption steps for completeness will also be illustrated.

2.1. Lorenz chaotic system

Lorenz system is a dynamical system which was studied first by Edward Norton Lorenz around 1960 [24], This chaotic system is described by non-linear system of ordinary differential equations (i.e., ODEs) as given in (1).

$$\begin{aligned} \dot{x} &= a(y - x), \\ \dot{y} &= (\sigma - z)x - y, \\ \dot{z} &= xy - bz. \end{aligned} \tag{1}$$

The real numbers a, σ, b are called the control parameters, where x, y, z are variables called the state variables, and $\dot{x}$, $\dot{y}$, and $\dot{z}$ are the time derivatives of x, y, and z. Usually, the Lorenz system (1) is commonly solved numerically using RK45 (Runge-Kutta methods) for given control parameters, and initial values of the state variables (i.e., x_0, y_0, z_0). In Figure 3 a chaotic attractor (i.e., Lorenz butterfly) of the dynamical Lorenz system (1) is presented.

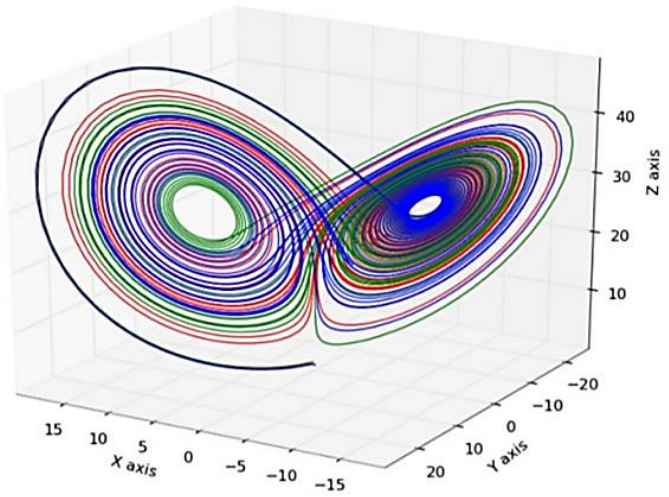

Figure 3. Chaotic attractor

For different values of parameter σ the dynamical system (1) exhibits chaos. By having positive Lyapunov exponents (i.e., sensitivity to initial conditions), chaos can be recognized for many dynamical systems, and in particular (1). In Figure 4, the maximum Lyapunov exponent of (1) versus values of σ are plotted. In this paper, we have fixed a and b to be $a = 10$, $b = 8/3$, and allow value of σ to dynamically vary in the interval $[28, 90]$ to provide a large enough key-space to resist brute-force attacks. Moreover, this will guarantee that (1) has dense (chaotic) attractors, which is important in terms of cryptography; any change in initial conditions will cause trajectories to remain in the same attractor set, thus making it difficult to predict any outcome without knowing the exact initial conditions of the system as well as the iteration counts in the numerical solution.

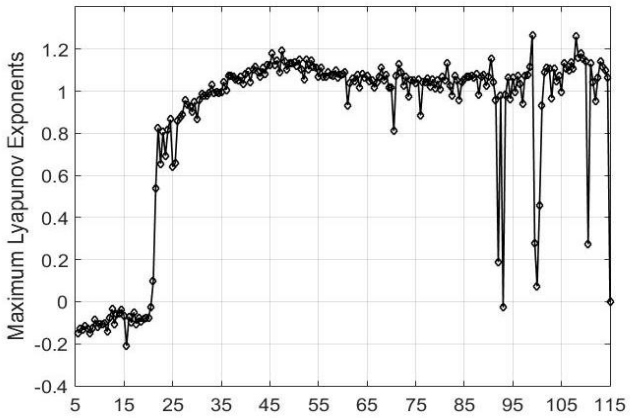

Figure 4. Maximum lyapunov exponents

2.2. Generation process for the initial values and parameters

In the generation process, we utilize the 128-bit hash value of the plain-speech frame generated by MD5 hash function to dynamically change the initial secret keysx_0, y_0, $z_0$and σ_0. In the following steps, the generation process is described in the details.

Algorithm 1: Generation process

Compute a 128-bit hash value K from the plain speech frame B_j, and then compute four 26-bit sequences as the following:

Step 1:
$x_n = \text{digits}(x_0 - \text{floor}(x_0), 26)$
$y_n = \text{digits}(y_0 - \text{floor}(y_0), 26)$
$z_n = \text{digits}(z_0 - \text{floor}(z_0), 26)$
$\sigma_n = \text{digits}(\sigma_0 - \text{floor}(\sigma_0), 26)$

Step 2: Set $r = \text{mod}(\text{count}(\sigma_n, 1), 13)$.

Step 3: Set $s = x_n, y_n, z_n, 1_{100}$ to construct the 128-bit string.

Step 4: Compute a new 128-bit hash-value by $H_N = \text{rot}_L(s \text{ XOR } K, r)$, then divide 128-bit hash value into four 32-bit vectors: $H_N = k_1, k_2, k_3, k_4$.

Step 5: Normalize the initial secret key to the interval $(0, 1)$ using $f(t) = (\arctan(t) + \pi/2)/\pi$ as the following:
$x_N = f(x_0)$, $y_N = f(y_0)$, $z_N = f(z_0)$, $\sigma_N = f(\sigma_0)$.

Step 6: Set $n_i = 100 + \text{count}(k_i, 1)$, $i = 1, 2, 3, 4$ to construct a four chaotic numbers l_1, l_2, l_3, $l_4 \in (0, 1)$ by iterating the logistic map n_1, n_2, n_3, and n_4 times using the initial-values x_N, y_N, z_N, σ_N, respectively.

Step 7: Finally, the following formula is used to compute the new four chaotic keys $\bar{x}$, $\bar{y}$, $\bar{z}$, and $\bar{\sigma}$:
$[\bar{x}\bar{y}\bar{z}] = [x_0 y_0 z_0] + [l_1 l_2 l_3] + 2^{-32} \times [k_1 k_2 k_3], \bar{\sigma} = 14 + 15 \times (l_4 + 2^{-32} k_4)$.

2.3. Encryption process

In the encryption process, a several iterations over the plain speech frame that involves a set of operation such as substitutions, permutations, transformations, and transpositions are performed to complicate the process of decrypting cipher speech frame by cyber-intruders (i.e., unauthorized access) [25, 26]. In Figure 5 the block diagram of the proposed decryption process is presented. The speech encryption algorithm proposed in this paper consists of the following sequential steps:

Algorithm 2: Encryption process

Step 1: Arrange the 20-ms speech frame in $\mathbf{B} = \{B_1, B_2, \dots, B_j\}$ of length $j = 132$, each element is the 8-bit representation of the bit 0 (BIT-0: FF81) or the bit 1 (BIT-1: 007F) of the coder parameters which is codified on 8 bits.

Step 2: Set $\bar{d} = \text{floor}(d/13)$, then iterate the Lorenz system (1)using RK-45 method for $(\bar{d} + 1)$ times using the new initial-values $x(0) = \bar{x}$, $y(0) = \bar{y}$, and $z(0) = \bar{z}$, and new control parameter $\sigma = \bar{\sigma}$, to get three chaotic sequences X, Y, and Z. Then compute the following three sequences:
$X_N = \{x_1, x_2, \dots, x_{\bar{d}+1}\}$, $Y_N = \{y_1, y_2, \dots, y_{\bar{d}+1}\}$, $Z_N = \{z_1, z_2, \dots, z_{\bar{d}+1}\}$
for $i = 1, 2, \dots, \bar{d} + 1$:
$x_i = \text{digits}(X_i - \text{floor}(X_i), 26)$,
$y_i = \text{digits}(Y_i - \text{floor}(Y_i), 26)$,
$z_i = \text{digits}(Z_i - \text{floor}(Z_i), 26)$.

Step 3: Set $\tilde{d} = \bar{d}$ if $(d/13)$ is an integer. Otherwise, $\tilde{d} = \bar{d} + 1$, . Then, partitioning the array $\boldsymbol{P}$ into $\tilde{d}$ vectors as $\boldsymbol{P} = P_1, P_2, \dots, P_{\tilde{d}}$
where,
$P_i = p_{13(i-1)+1}, \dots, p_{13i}$, $P_{\tilde{d}} = p_{13\bar{d}+1}, \dots, p_d$, $i = 1,2, \dots, \bar{d}$

Step 4: Construct the sequence $U = U_1, U_2, \dots, U_{\tilde{d}}$ with$U_i = B_i$, for $i = 1, 2, \dots, \bar{d}$, and $U_{\tilde{d}} = \text{digits}(B_{\tilde{d}}, \text{length}(P_{\tilde{d}}))$. Observe that $\text{length}(U_i) = 28 + 28 = 56\text{bit} = 7 \times 8\text{bit}$, and $\text{length}(P_{\tilde{d}}) = (d - 13\bar{d}) \times 8\text{bit}$.

Step 5: Construct rotations$r_i = \text{count}(z_i, 1)$, $i = 1, 2, \dots, \tilde{d}$.

Step 6: Finally, the cipher speech frame $\mathbf{C}$ is obtained using the formula:
$C_i = \text{rot}_L(U_i \; XOR \; P_i, r_i)$, $i = 1,2, \dots, \tilde{d}$.

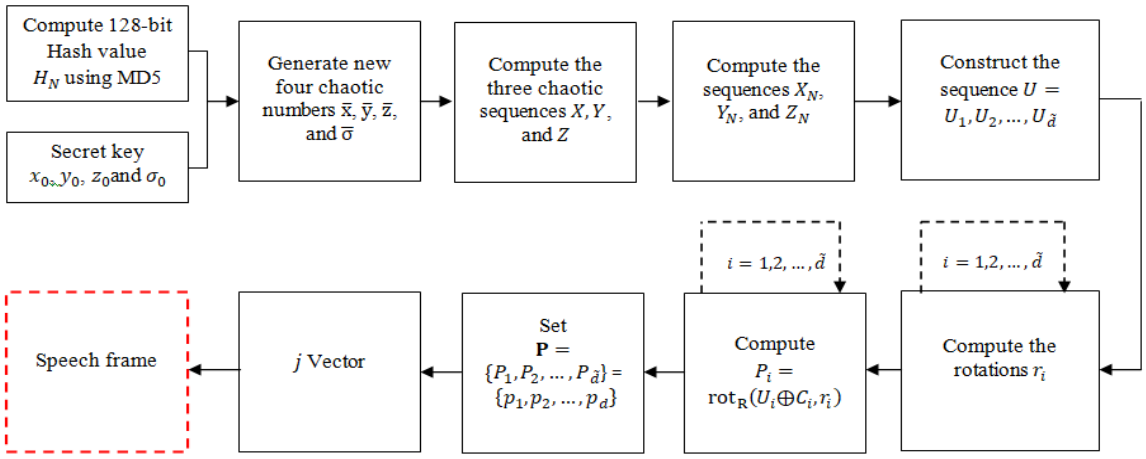

Figure 5. Decryption algorithm

3. SIMULATION RESULT AND SECURITY ANALYSIS

This section discusses the proposed speech encryption algorithm, which simulated on a 1.6 GHz core (TM) i5, 1-TB hard disk capacities and 4-GB memory with MATLAB software. In this section, as an example, different speech samples of audio files are selected with different sampling rate (i.e., 5000 samples per second). The simulation result was validated by applying the statistical tests such as histogram analysis, correlation, randomness, and sensitivity to prove the performance metrics [22]. Below, standardized tests are given.

3.1. Histogram analysis test

To evaluate the quality of encrypted speech signals, this analysis is the most accurate test. Practically, the proposed algorithm is likely to encrypt the plain speech signals in a random manner (i.e., noisy signals). Histogram of the input speech signals are illustrated in Figure 6(a) and Figure 6(d). The corresponding histogram of the encrypted speech signals using the secret keys: x_0, y_0, z_0, σ_0, and 128-bit hash value of the speech signals are illustrated in Figure 6(b) and Figure 6(e). The results in Figure 6 shows that the histograms of the encrypted speech signals are fairly uniform distributed and totally different from the plain speech signals. In addition, the result indicates that the proposed algorithm can be decrypted correctly with the correct keys as illustrated in Figure 6(c) and Figure 6(f).

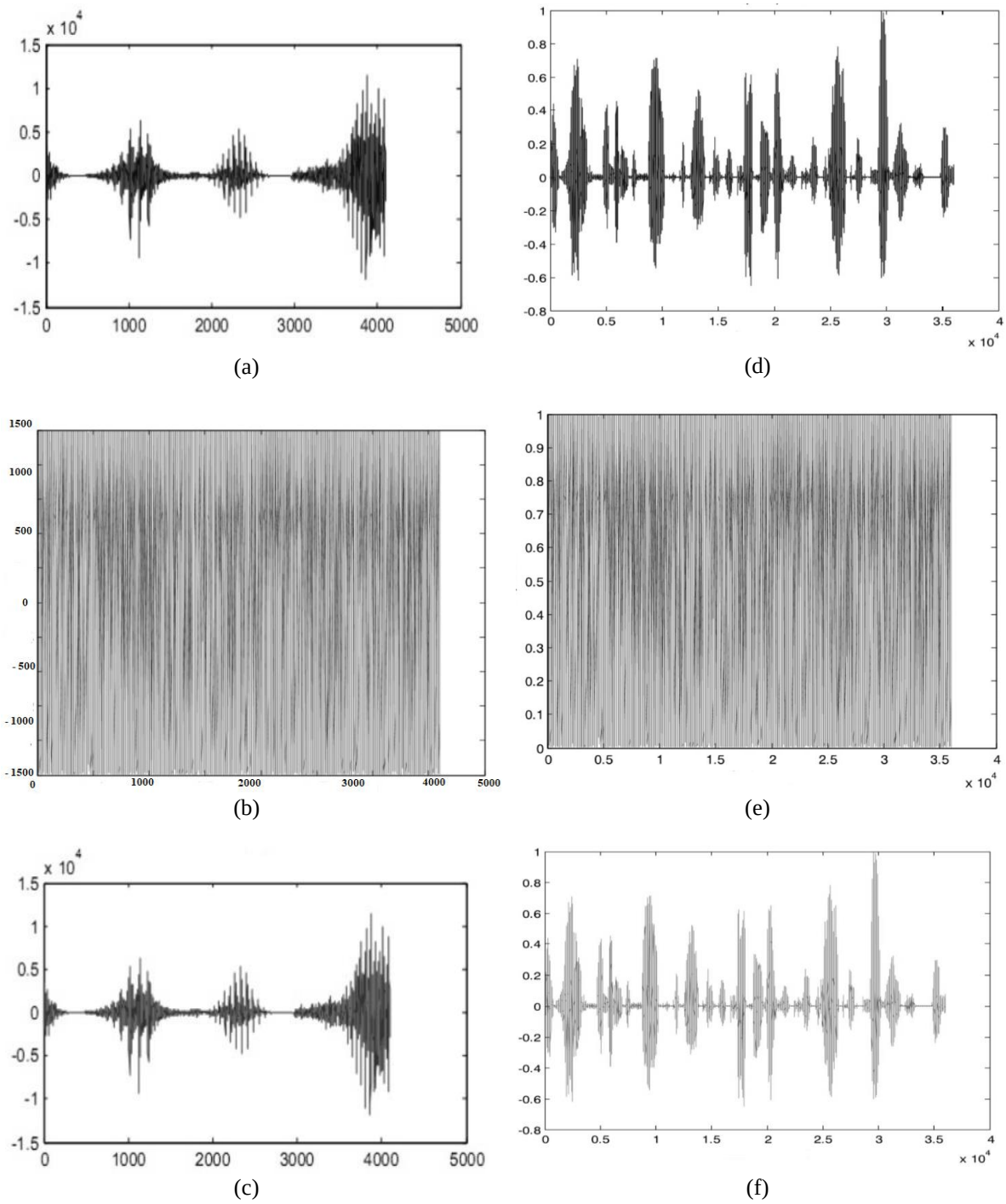

Figure 6. Histogram analysis, (a) Input speech signal_1, (b) Encrypted speech signal_1, (c) Decrypted speech signal_1, (d) Input speech signal_2, (e) Encrypted speech signal_2, (f) Decrypted speech signal_2

3.2. Correlation test

The chaotic system was found to produce a strong encryption method, which can be efficiently identified by correlation method [23]. The correlation method is computed as (2).

$$r_{xy} = \frac{\text{cov}(x,y)}{\sqrt{D(x)\sqrt{D(y)}}} \quad (2)$$

where

$$\text{cov}(x,y) = \frac{1}{N}\sum_{i=1}^{N}\big(x_i - E(x)\big)\big(yi - E(y)\big),\ \ E(x) = \frac{1}{N}\sum_{i=1}^{N} x_i,\ \ D(x) = \frac{1}{N}\sum_{i=1}^{N}(x_i - E(x))^2,$$

where N is the number of speech samples. In proposed algorithm, the correlation coefficient $\text{cov}(x,y)$ between the plain and the ciphered speech samples are tabulated in Table 1. The result in Table 1 shows that the proposed speech encryption algorithm is efficient enough, because the correlation test has been satisfied that would resist statistical attacks.

Table 1. Correlation test

File Name	Original	Encrypted
Sample_1.wav	0.98153	0.000992
Sample_2.wav	0.98726	0.000642
Sample_3.wav	0.99114	0.001765
Sample_4.wav	0.96241	0.001357

3.3. Randomness tests

To measure the strength of the encrypted speech frames against cryptanalysis attacks, we have performed a different suite of statistical tests in this section known as DIEHARD (i.e., 18-tests) and NIST (i.e., 15-tests) test suite [23, 27]. For given sequence, these suites are designed mainly to measure the quality of the randomness. As can be seen from Table 2 and Table 3, the *p*-value of each test ranges from 0.01 to 0.99 (i.e., success range), which means the encrypted sequence is random at the 99% of confidence level.

Table 2. DIEHARD tests suite

Test No.	*p*-value	Result
1	0.508955	Testing passed
2	0.352178	Testing passed
3	0.985131	Testing passed
4	0.432234	Testing passed
5	0.577165	Testing passed
6	0.531168	Testing passed
7	0.579962	Testing passed
8	0.461181	Testing passed
9	0.534275	Testing passed
10	0.440085	Testing passed
11	0.537715	Testing passed
12	0.698621	Testing passed
13	0.700913	Testing passed
14	0.385725	Testing passed
15	0.700982	Testing passed
16	0.672727	Testing passed
17	0.700116	Testing passed
18	0.071163	Testing passed

Table 3. NIST tests suite

Test No.	*p*-value	Result
1	0.644569	Testing passed
2	0.537212	Testing passed
3	0.822953	Testing passed
4	0.691672	Testing passed
5	0.287185	Testing passed
6	0.279095	Testing passed
7	0.513448	Testing passed
8	0.436158	Testing passed
9	0.214367	Testing passed
10	0.433041	Testing passed
11	0.207415	Testing passed
12	0.387142	Testing passed
13	0.597824	Testing passed
14	0.509732	Testing passed
15	0.484727	Testing passed

3.4. Information entropy

Information entropy is used usually as a measure of disorder, or randomness in encrypted speech signal [28]. The entropy function $H(s)$of a source *s* can be computed as (3).

$$H(s) = \sum_{i=1}^{2N-1} P(s_i) \log_2 \frac{1}{P(s_i)} \quad (3)$$

where P(Si) represents Si probability. The entropy value for the encrypted speech signals should ideally be 8. In other words, if the entropy value of the encrypted speech signals is less than 8, then the predictability threats to the encrypted speech signals are exists. In this paper, ENT test suite is used to calculate the information entropy value. Practically, ENT is a suite composed of the following three tests: entropy, serial correlation, and chi-square coefficient as shown in Table 4. From these results, the obtained values are evaluated to be almost as the theoretical value, which means that the proposed speech encryption algorithm is efficient enough (i.e., secure) upon the cryptanalysis attacks (i.e., entropy).

Table 4. ENT test suite

No.	ENT test suite	Theoretical value	Obtained value
1	Entropy	Close to 8	7.999986
2	Serial correlation	Close to 0	0.000381
3	Chi-square coefficient	Close to 127.5	127.5019

3.5. Key sensitivity test

To ensure the security against brute-force attacks, the excellent encrypted speech quality must be sensitive in extreme way with respect to the secret keys [24, 29]. In the proposed algorithm, any slightly change (i.e., bit flip) on the following sensitivity factors: hash values, keys, and other encryption keys such as parameters that would generate a completely different decryption results as shown in Figure 7.

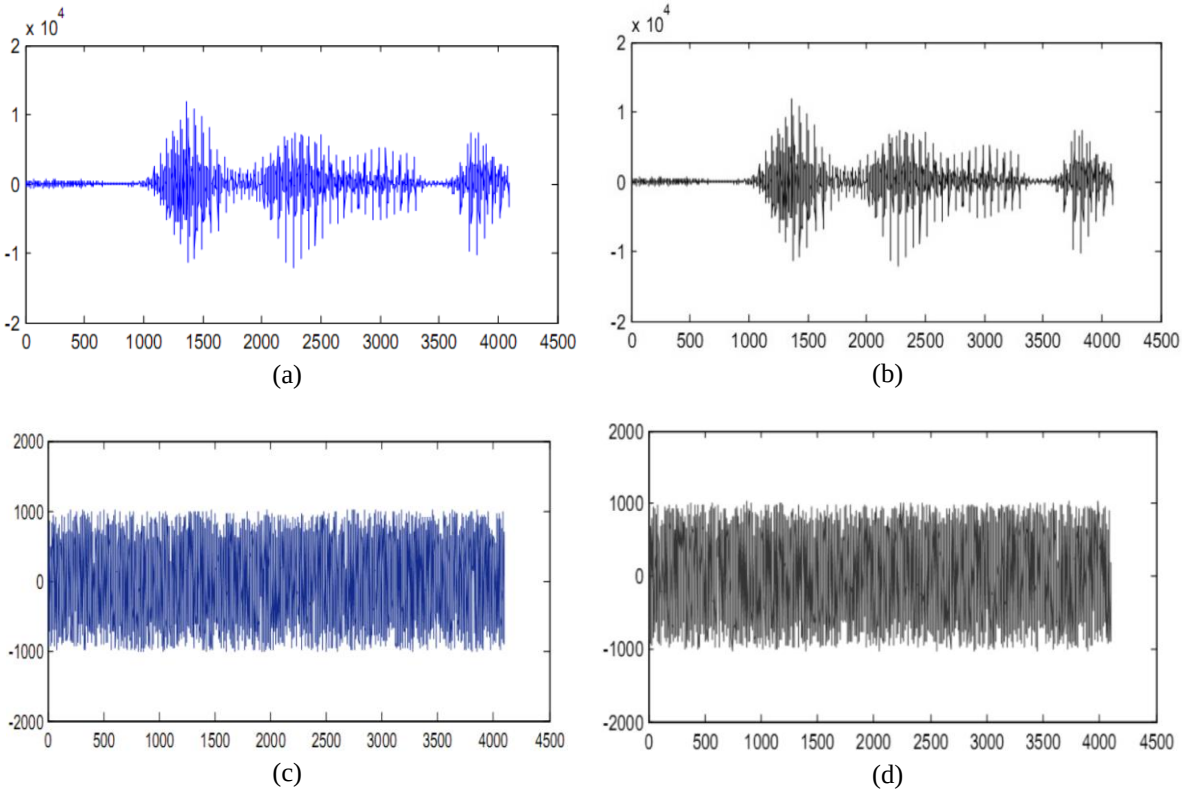

Figure 7. Key sensitivity, (a) Input speech signal, (b) Decrypted speech signal with correct key, (c) Decrypted speech signal with incorrect key hash value, (d) Decrypted speech signal with incorrect x_0

4. COMPARISON WITH EXISTING WORKS

There are several types of delay in the current IP telephony networks such as processing (i.e., coder, decoder, digital signal processing), serialization, queuing, propagation, and network delay as shown in Figure 8. Some of them are fixed while others are variable as illustrated in Table 5. IP telephony applications are delay sensitive. Therefore, the ITU-T has recommended that the maximum threshold of the delay time (i.e., ∑delay sources) is 150 ms [2, 5, 6]. The adaptive multi-rate wideband (AMR-WB G.722.2) speech codec is used in this paper to collect *N* speech samples as one frame because it supports the GSM features such as discontinuous transmission, comfort noise generation, and voice activity detection [30].

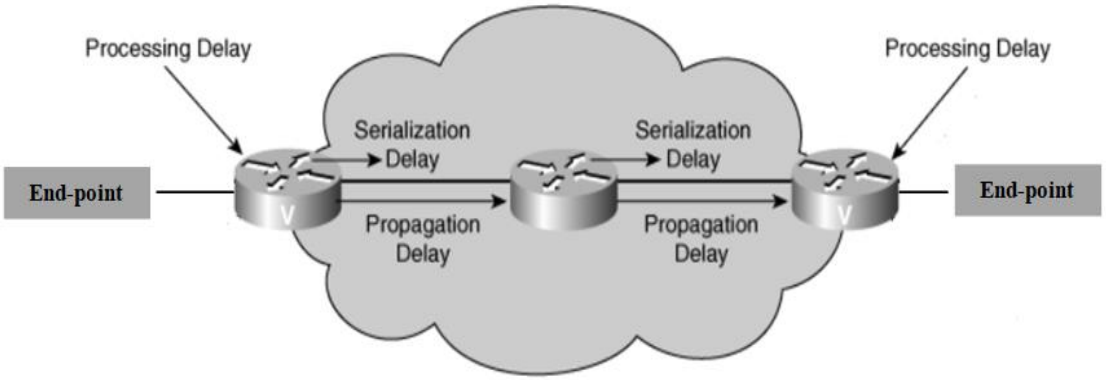

Figure 8. Packet flow

Table 5. Delay source

Delay source	Formula	Description	Delay type
Coder	$C_D = (2N + 1) * Frame\ Size + Look\ ahead\ time$	Collect the speech samples as frames.	Fixed
Decoder	$D_D = \frac{C_D}{2}$	Playback of the coder process.	Fixed
Serialization	$S_D = \frac{Frame\ Size}{Interface\ Clocking\ Rate}$	Time to clock a speech frame onto a network interface.	Fixed
Queuing	$Q_D = \frac{(Voice\ Frame\ Size + 5120)}{Line\ Speed}$	Time the voice packet spends in router.	Variable
Network	$N_D = Number\ of\ Routers * (Q_D + S_D)$	Time the voice packet spends to go from one point to another.	Variable
Propagation	Caused by the light speed in copper-based networks (i.e., 125,000 miles per second), or in fiber (i.e., 186,000 miles per second)		Fixed
Security	Caused by the encryption and decryption processes.		Fixed

A practical comparison on the average time delay between advanced encryption standard algorithm and proposed algorithm in the same environment and conditions is made in this section. In end-to-end delay, the implementation result shows that the average time delay to encrypt the speech data using the proposed algorithm is 2.287701494 ms and the average time delay to encrypt the speech data using AES is 2.7832762824 ms as illustrated in Table 6 and Table 7 respectively. In other words, a column chart showing the AES algorithm is slower than the proposed speech encryption algorithm is presented in Figure 9.

Table 6. End-to-end delay time for fast Ethernet using the proposed speech encryption algorithm

Speech Coder		Fixed					Variable		Total (ms)
Codec	Reference	Coder	Decoder	Security (proposed algorithm)	Serialization	Propagation	Queuing	Network	
				Trial No. (ms)					
				1 0.58438227					
				2 0.57427116					
AMR-WB	G.722.2	0.9375	0.46875	3 0.57707780	0.07303	0.006	0.228121	0	
				4 0.57752808					
				5 0.55824316					
Average (ms)		0.9375	0.46875	0.574300494	0.07303	0.006	0.228121	0	2.287701494

Table 7. End-to-end delay time for fast ethernet using AES algorithm

Speech Coder				Fixed			Variable		Total (ms)
Codec	Reference	Coder	Decoder	Security (AES)	Serialization	Propagation	Queuing	Network	
				Trial No. (ms)					
AMR-WB	G.722.2	0.9375	0.46875	1 1.083813452 2 1.047655243 3 1.088726224 4 1.038455265 5 1.090726228	0.07303	0.006	0.228121	0	
Average (ms)		0.9375	0.46875	1.0698752824	0.07303	0.006	0.228121	0	2.7832762824

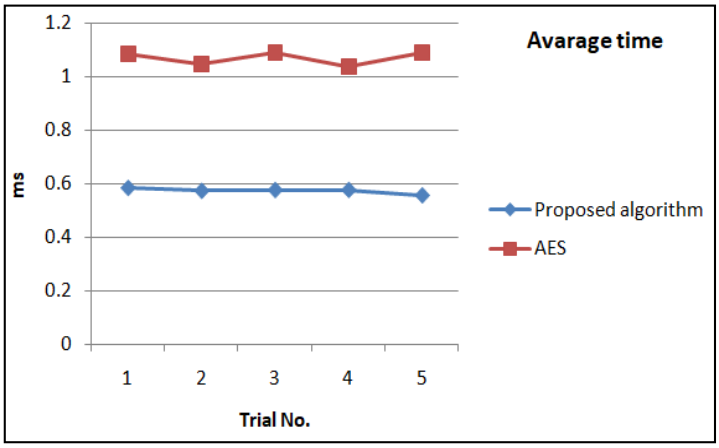

Figure 9. Average delay time

5. CONCLUSION

In this paper we have achieved our objective of designing a dynamic speech encryption algorithm based on Lorenz chaotic map over internet protocol to enhance the real-time services. The proposed algorithm was divided into two processes: key generation process using 128-bit hash value, and encryption and decryption process using Lorenz system. To evaluate the security level of the proposed algorithm, efficient simulations and implementations and analysis have been conducted. The security level is increased by using a multi key with every new speech packet and increasing a key length which protects the proposed algorithm against various cryptanalysis attacks. In addition, a comparison between the average time delay in the proposed algorithm and some of the existing encryption algorithms is made. The results endorse that the proposed algorithm achieved a higher security level with a lowest average delay time and it is an excellent choice for voice communication in practical applications in the Internet.

REFERENCES

[1] B. Goode, "Voice over internet protocol (VoIP)," *Proceedings of the IEEE*, vol. 90, no. 9, pp. 1495-1517, 2002.
[2] H. Oouch, *et al*., "Study on appropriate voice data length of IP packets for VoIP network adjustment," in *Global Telecommunications Conference, 2002. GLOBECOM'02. IEEE*, vol. 2, pp. 1618-1622, 2002.
[3] R. Dantu, *et al*., "Issues and challenges in securing VoIP," *Computers & Security*, vol. 28, no. 8, pp. 743-753, 2009.
[4] O. M. Al-Hazaimeh, "Increase the security level for real-time application using new key management solution," *International Journal of Computer Science Issues (IJCSI)*, vol. 9, no. 3, pp. 240-246, 2012.
[5] S. Na and S. Yoo, "Allowable propagation delay for VoIP calls of acceptable quality," in *Proceedings of the First International Workshop on Advanced Internet Services and Applications*, pp. 47-56, 2002.
[6] O. M. Al-Hazaimeh, "New cryptographic algorithms for enhancing security of voice data," Thesis, Universiti Utara Malaysia, 2010.
[7] M. Zandi, *et al*., "Overview of security issues of VoIP," in *Proceedings of the Third IASTED European Conference on Internet and Multimedia Systems and Applications*, pp. 254-259, 2007.
[8] J. Seedorf, "Security challenges for peer-to-peer SIP," *IEEE Network*, vol. 20, no. 5, pp. 38-45, 2006.
[9] O. M. Al-Hazaimeh, "Combining audio samples and image frames for enhancing video security," *Indian Journal of Science and Technology*, vol. 8, no. 10, p. 940, 2015.
[10] E. Schaefer, "An introduction to cryptography and Cryptanalysis," California's Silicon Valley: Santa Clara University, pp. 4-5, 2009.
[11] M. Mishra and V. H. Mankar, "Review on chaotic sequences based cryptography and cryptanalysis," *International Journal of Electronics Engineering*, vol. 3, no. 2, pp. 189-194, 2011.

[12] O. M. Al-Hazaimeh, *et al*., "A novel video encryption algorithm-based on speaker voice as the public key," in *2014 IEEE International Conference on Control Science and Systems Engineering*, pp. 180-184, 2014.
[13] C. T. Elrod, "VoIP security," Google Patents, US8295188B2, 2012.
[14] M. Šalamon, "Chaotic electronic circuits in cryptography," in *Applied cryptography and network security*, pp. 295-320, 2012.
[15] E. Mosa, *et al*., "Chaotic encryption of speech signals," *International Journal of Speech Technology*, vol. 14, no. 4, pp. 285-26, 2011.
[16] L. J. Sheu, "A speech encryption using fractional chaotic systems," *Nonlinear dynamics*, vol. 65, no. 1, pp. 103-108, 2011.
[17] P. Sathiyamurthi and S. Ramakrishnan, "Speech encryption using chaotic shift keying for secured speech communication," *EURASIP Journal on Audio, Speech, and Music Processing*, vol. 2017, no. 1, pp. 20-30, 2017.
[18] H. T. Yau, *et al*., "Application of a chaotic synchronization system to secure communication," *Information technology and control*, vol. 41, no. 3, pp. 274-282, 2012.
[19] M. S. Azzaz, *et al*., "Synchronized hybrid chaotic generators: Application to real-time wireless speech encryption," *Communications in Nonlinear Science and Numerical Simulation*, vol. 18, no. 8, pp. 2035-2047, 2013.
[20] F. J. Farsana, *et al*., "An audio encryption scheme based on Fast Walsh Hadamard Transform and mixed chaotic keystreams," *Applied Computing and Informatics*, 2019.
[21] K. Kordov, "A Novel Audio Encryption Algorithm with Permutation-Substitution Architecture," *Electronics*, vol. 8, pp. 530-544, 2019.
[22] C. E. Shannon, "Communication theory of secrecy systems," *The Bell system technical journal*, vol. 28, no. 4, pp. 656-715, 1949.
[23] W. Chang, *et al*., "Randomness testing of compressed data," *arXiv preprint arXiv:1001.3485*, 2010.
[24] O. M. Al-Hazaimeh, *et al*., "Image encryption algorithm based on Lorenz chaotic map with dynamic secret keys," *Neural Computing and Applications*, pp. 1-11, 2017.
[25] R. S. Mohammed and S. B. Sadkhan, "Speech scrambler based on proposed random chaotic maps," in *2016 Al-Sadeq International Conference on Multidisciplinary in IT and Communication Science and Applications (AIC-MITCSA)*, pp. 1-6, 2016.
[26] A. K. Mittal, *et al*., "Secure communication based on chaotic switching and rapid synchronization using parameter adaptation," *International Journal of Innovative Computing, Information and Control*, vol. 11, no. 2, pp. 569-585, Apr 2015.
[27] J. Soto, "Statistical testing of random number generators," in *Proceedings of the 22nd national information systems security conference*, 1999.
[28] X. Zhang and Z. Zhao, "Chaos-based image encryption with total shuffling and bidirectional diffusion," *Nonlinear Dynamics*, vol. 75, no. 1-2, pp. 319-330, 2014.
[29] J. Fridrich, "Symmetric ciphers based on two-dimensional chaotic maps," *International Journal of Bifurcation and chaos*, vol. 8, no. 6, pp. 1259-1284, 1998.
[30] M. Boumaraf and F. Merazka, "Speech Coding Combining Chaos Encryption and Error Recovery for G. 722.2 Codec," in *Proceedings of the 3rd International Conference on Natural Language and Speech Processing*, pp. 128-134, 2019.

BIOGRAPHY OF AUTHOR

Obaida M. Al-Hazaimeh received his BSc in Computer Science from Applied Science University, Jordan in 2004 and MSc in Computer science from University Science Malaysia, Malaysia, in 2006. He received his PhD degree in Network Security (Cryptography) from Malaysia in 2010. He is an associate professor at department of computer science and information technology, Al-Balqa' Applied University, Jordan. His main research interests are Cryptology, image processing, machine learning, and chaos theory. He has published more than 34 Papers as author and Co-author in international refereed journals.