

## Chaotic elliptic map for speech encryption

Obaida M. Al-Hazaimeh<sup>1</sup>, Ashraf A. Abu-Ein<sup>2</sup>, Khalid M. Nahar<sup>3</sup>, Isra S. Al-Qasrawi<sup>1</sup>

<sup>1</sup>Department of Computer Science and Information Technology, Al-Balqa Applied University, Jordan

<sup>2</sup>Department of Electrical Engineering, Al-Balqa Applied University, Jordan

<sup>3</sup>Department of Computer Sciences, Yarmouk University, Jordan

### Article Info

#### Article history:

Received Nov 22, 2021

Revised Dec 18, 2021

Accepted Dec 23, 2021

#### Keywords:

Chaos

Cryptanalysis

Encryption

Jacobian elliptic map

NIST test suite

### ABSTRACT

Using a new key management system and Jacobian elliptic map, a new speech encryption scheme has been developed for secure speech communication data. Jacobian elliptic map-based speech encryption has been developed as a novel method to improve the existing speech encryption methods' drawbacks, such as poor quality in decrypted signals, residual intelligibility, high computational complexity, and low-key space. Using the Jacobian elliptic map as a key management solution, a new cryptosystem was created. The proposed scheme's performance is evaluated using spectrogram analysis, histogram analysis, key space analysis, correlation analysis, key sensitivity analysis and randomness test analysis. Using the results, we can conclude that the proposed speech encryption scheme provides a better security system with robust decryption quality.

*This is an open access article under the [CC BY-SA](https://creativecommons.org/licenses/by-sa/4.0/) license.*



### Corresponding Author:

Obaida M. Al-hazaimeh

Department of Computer Science and Information Technology, Al- Balqa' Applied University

Jordan

Email: dr\_obaida@bau.edu.jo

## 1. INTRODUCTION

All of our daily activities, including trade, banking, e-learning, education, politics, and the military all rely on speech communication. In these applications, a substantial volume of sensitive audio data is transmitted through widely shared and open networks (i.e., un-secure). Cryptographic algorithms are needed now more than ever because of the rapid development of data communications and digital audio, which require greater security. In contrast to digital data or text messages, speech information has a larger correlation among samples and a higher level of redundancy [1], [2]. There are two types of speech encryption: analog (i.e., scramble) and digital. In analog speech encryption, the speech stream is scrambled or permuted in the time, frequency, or both domains. While digital speech encryption involves encrypting the speech signal with advanced digital cryptosystems such as data encryption standard (DES) and advanced encryption standard (AES). Analog speech encryption has a number of advantages to digital speech encryption, such as good quality of the recovered speech, low bandwidth, and ease of use, but they are less secure. In contrast, digital speech encryption is more secure, but it requires a considerable amount of bandwidth for transmission and a complicated implementation process [3], [4]. Traditional cryptographic systems may be efficient for text data, but they are inappropriate for providing security for voice data due to bulk data capacity and high redundancy. As a result, efficient algorithms, such as chaos-based algorithms for dealing with redundant speech data are required for speech security. These algorithms offer faster and more secure encryption approaches [5], [6].

Figure 1 shows the tight connection (i.e., relationship) between chaos and cryptography that several academics have discovered [7]-[10]. It is possible to create secure communications using chaotic systems because of their inherent randomness, ergodicity, control parameters, sensitivity to initial conditions, and

other random characteristics [11]-[13]. A number of chaos-based encryption schemes have been presented in the last years. As examples, Sathiyamurthi and Ramakrishnan [14] developed a new method for speech encryption in which incoming speech signals are partitioned into four layers and then shuffled using four different chaotic maps such as logistic maps, quadratic, Bernoulli's, and tent. Then, the chen map is employed to complete the shuffling process. According to Hasan [4], the speech signal is encrypted using a fixed point chaos-based stream cipher (FPC-SC). The suggested approach provides good statistics and encryption measures, according to the results. Wahab and Mahdi [15] modified overlapped block shuffling (MOBS) and a hybrid chaotic system-based technique has been developed. After converting the signal from 1 and 2 dimensions, the speech signal is partitioned into overlapped square blocks using the Arnold cat and Hénon map to obtain ciphered speech data.

Elzaher *et al.* [5] introduced a new method of voice encryption. The samples of the original signal are first permuted using Arnold cat map, and then substituted using Hénon map. In the proposed approach, the decrypted voice signal has a large key space (i.e., enough) and is of good quality. For speech encryption Farsana and Gopakumar [16] used the Zaslavsky and Cat map transforms to developed a new speech encryption scheme. After compressing the original signal using discrete cosine transform technique (DCT), the original signal is encrypted using the Zaslavsky map. The resulting signal is then treated with Arnold cat map in order to confuse the data samples. The analysis demonstrates that the study is simple and computationally efficient. Elshamy *et al.* [1] used Arnold cat map or Baker Map with "double random phase encoding" to encrypt the audio signal. Different quality measures for encryption and decryption demonstrate that the given approach raises the level of voice confidence and security. According to Al-Hazaimah [2], chaotic system and stream cipher technique are employed for developing voice over internet protocol method (VoIP). In this method, a random key is created utilizing chaotic systems to encrypt the speech data. Experiments indicate that this system can provide the lowest possible delay and packet loss in the transferred packet. In Habib *et al.* [17] the original audio signal is partitioned to four blocks, and then each block is confused using various chaotic systems. The outcomes of different experiments prove the security of the presented strategy. Al-Hazaimah [18] designed encryption method based on Hénon map for voice data. The proposed method was applied and tested to prove its applicability and validity. The validation demonstrates that the designed method is simple and computationally efficient.

Based on the literature, a number of chaotic systems such as the logistic map have been widely employed because of their high-level efficiency and simplicity [19], [20]. Although these chaotic cryptosystems have certain advantages, they also have some disadvantages such as a weak security and small key space (i.e., not large enough) [2], [21]-[24]. Therefore, this study proposes a new cryptosystem that overcomes the aforementioned shortcomings. Experimental results and security analysis show that the proposed encryption scheme based on the Jacobian elliptic map is favorable in terms of key space and security level (i.e., high security level, key space enough). In the following section, a brief discussion is introduced for chaotic map namely Jacobian elliptic map which is used in this research.

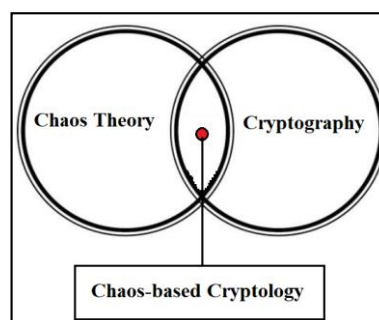


Figure 1. Chaos and cryptography relationship

## 2. JACOBIAN ELLIPTIC MAPS

The ratio of polynomials of degree N can be used to define as "One-parameter families of Jacobian elliptic rational mappings over the interval [0, 1] with an invariant measure" [25]:

$$\phi_N(x, \alpha) = \frac{\alpha^2 F^2}{1 + (\alpha^2 - 1) F^2} \quad (1)$$

where  $F$  is substituted in the elliptic functions for  $sn$ ,  $cn$  and  $dn$ . The function of Jacobian elliptic map is depending on  $k$  modulus and argument  $u$ . Therefore,  $sn(u)$  and  $dn(u)$  are given in the following equations and plotted on Figure 2.

$$u = \int_0^{sn(u)} \frac{dx}{\sqrt{(1-x^2)(1-k^2x^2)}} \tag{2}$$

$$cn(u) = \sqrt{1 - (sn(u))^2} \tag{3}$$

$$dn(u) = \sqrt{1 - k^2(sn(u))^2} \tag{4}$$

To make it clear,  $sn(u)$  and  $dn(u)$  relations can also be represented by (5).

$$sn^2(u) + cn^2(u) = 1, dn^2(u) + k^2sn^2(u) = 1 \tag{5}$$

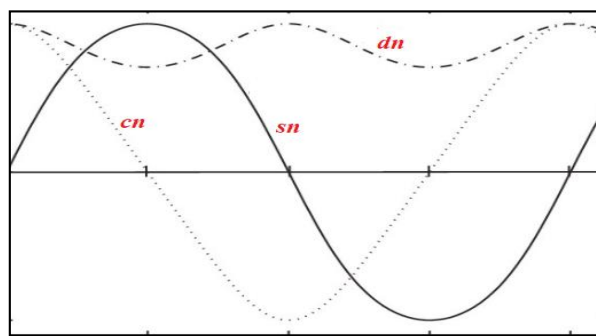


Figure 2. Functions of Jacobi elliptic map

The maps  $\phi_N(\alpha, x)$  are  $(N - 1)$  nodal maps, their critical points in the interval  $[0, 1]$  are  $(N - 1)$  (see Appendix A, for Schwarzian derivation of Jacobian rational) [26]. Figure 3 depicts their ergodic behavior, which is characterized by a single period of stable fixed points. The Lyapunov exponent is defined by [26].

$$\lambda(x_0) = \lim_{t \rightarrow \infty} \frac{1}{t} \sum_{i=0}^{t-1} \ln \left| \frac{d\phi_N(x_i)}{dx} \right| \tag{6}$$

The maps  $\phi_N(x, \alpha)$  have at most  $N + 1$  attractive periodic orbits with only one stable fixed point with a single period, or they are ergodic maps (see Appendix B, for an example of Jacobian maps) [26].

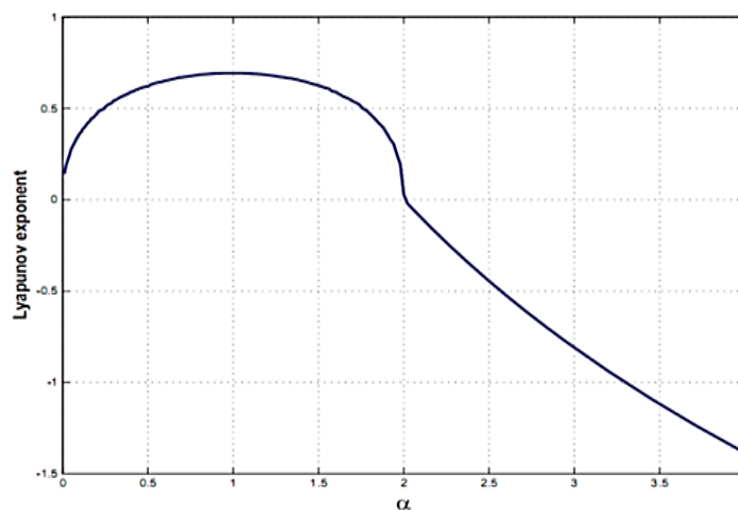


Figure 3. The plot of Lyapunov exponent

### 3. PROPOSED SCHEME

Jacobian elliptic map is chosen from the chaotic maps to be utilized in the encryption and decryption processes. The proposed cryptosystem is a block cipher scheme, which is comprised of the following key steps: Step 1: First the public table ( $P_{m \times n}$ ), the control parameters ( $\alpha, k$ ) and the initial condition ( $x$ ) are input into the algorithm as a key for Jacobian elliptic map.

Step 2: Re-shaped the public table ( $P_{m \times n}$ ) into a one-dimensional array ( $P_{m \times n} \times 1$ )

Step 3: Iterate the Jacobian elliptic map for 1000 times and ignore the result to eliminate the chaotic map's transient effects.

Step 4: Confuse and defuse each element of matrix  $P$  using (7) and put the result into matrix  $C$  which is called private table ( $P_r$ ).

$$\phi_2^{(cn)}(x, \alpha) = \frac{4\alpha^2 x(1-k^2x)(1-x)}{(1-k^2x^2)^2 + 4(\alpha^2-1)x(1-k^2x)(1-x)} \tag{7}$$

Step 5: Generate a secret value ( $K_s$ ) with 1024 bit key length.

Step 6: Re-shaped the plain text into a one-dimensional array ( $P_t$ ).

Step 7: Using a simple operation ( $XoR$ ), the ciphered data is obtained:

$$C_1 = K_s \oplus P_t$$

Step 8: Generate the values of the key positions from the private table ( $P_r$ ).

Step 9: Finally, insert each 8-bit of the secret key ( $K_s$ ) in the ciphered data ( $C_1$ ) depending on the key positions value (i.e., Step 8) and so on till this repeated for all the key to generate a ciphered data with the inserted key ( $C_2$ ).

The proposed encryption scheme's block diagram is shown in Figure 4. To make it clear, the insertion process is carried out in accordance with the key positions. The first 8-bit ( $t$  (1<sup>st</sup> octet) of the key will be inserted into the ciphered data (i.e.,  $C_1$ ) according to the value of the first position value, and the second 8-bit (2<sup>nd</sup> octet) of the key will be inserted according to the value of the second position value, depending on the private table, and so on until this process is repeated for all keys to generate a ciphered data with inserted key (i.e.,  $C_2$ ) as shown in Figure 5. The process of decryption is nearly identical to the process of encryption, with just a few minor differences. Algorithmically speaking, both the encryption and decryption processes are nearly identical in time consumption and complexity [6], [12].

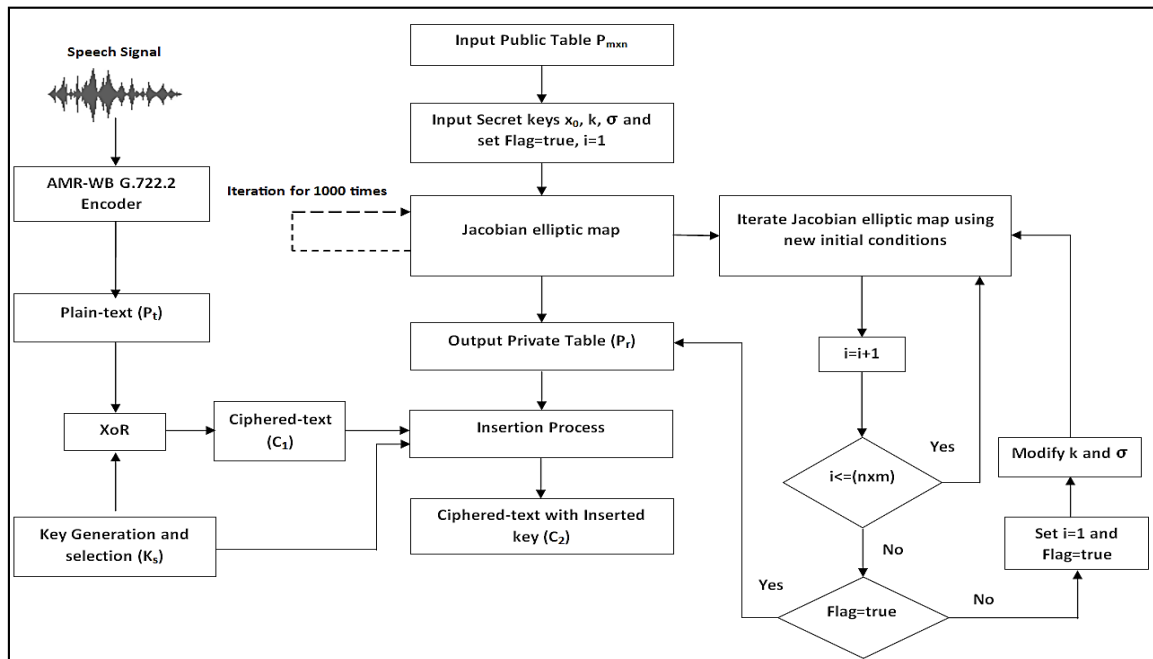


Figure 4. Block diagram of the encryption scheme

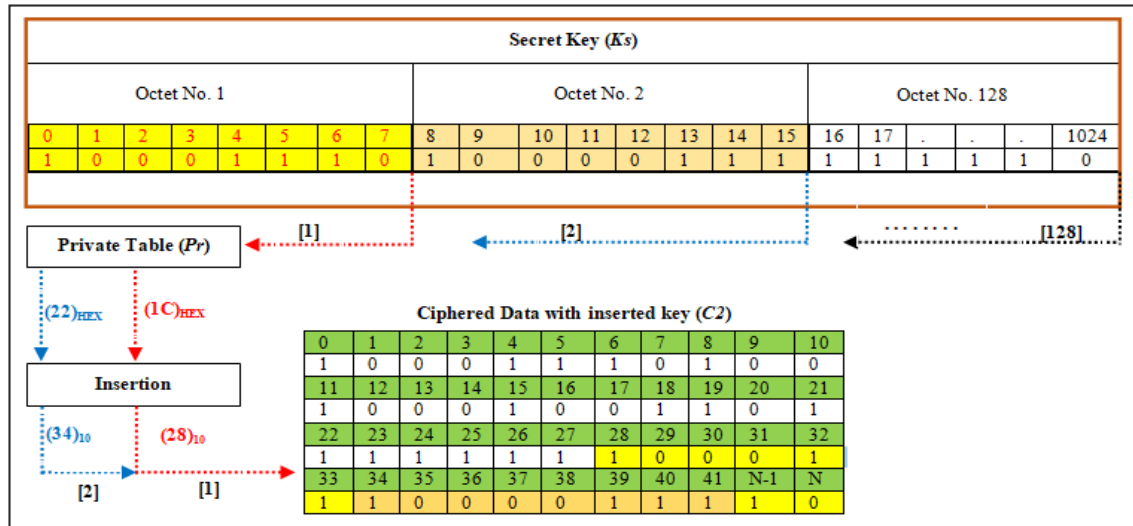


Figure 5. Insertion process

4. SIMULATION RESULTS

To demonstrate the effectiveness of the proposed speech encryption scheme, the following simulation results are provided in this section. The histogram of the plain text (i.e., original speech) is given in Figure 6(a), which encrypted with the proposed scheme and corresponding ciphred data such as ciphred signals and ciphred signals with the inserted key are given in Figure 6(b) and Figure 6(c) respectively. Moreover, the decrypted signal using the proposed scheme is given in Figure 6(d). In addition, the signals spectrograms of the original and ciphred data are also given in Figure 7(a) and Figure 7(b) respectively.

The English language speech database for speaker recognition (ELSDSR) database was used as a standard. The suggested speech encryption scheme is tested using MATLAB software on a core (TM) i5-1.6 GHz, a 2 TB hard drive capacity, and 8 GB RAM. For example, distinct speech samples from audio files with varying sampling rates are selected (i.e., 5000 samples per second).

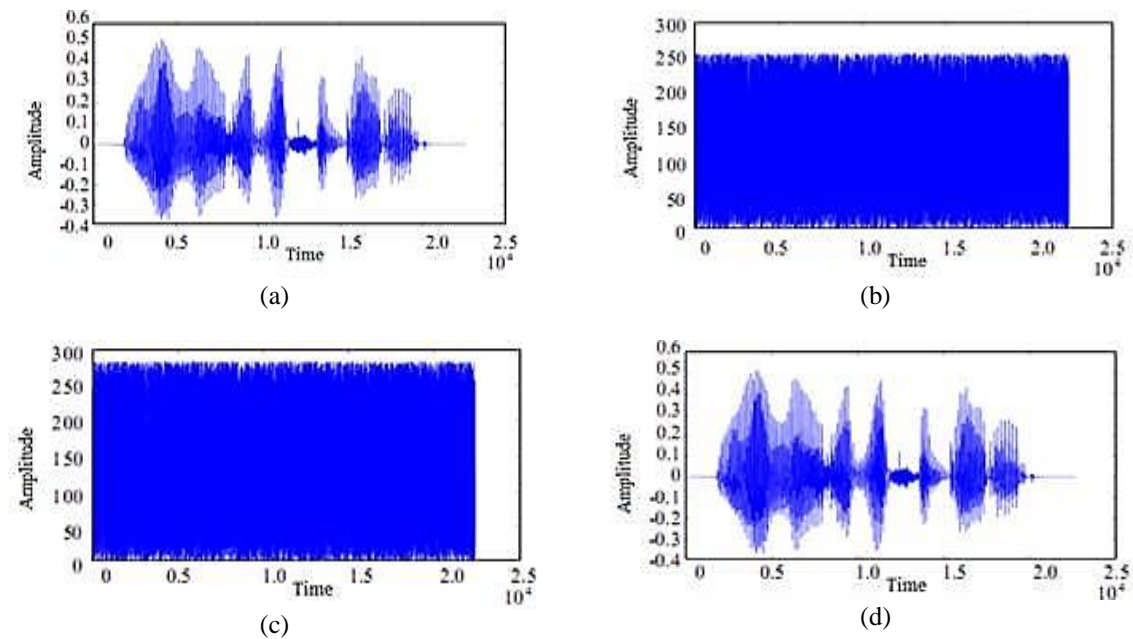


Figure 6. Simulation results of (a) original signal, (b) ciphred signal, (c) ciphred signal with the inserted key (Ks), and (d) decrypted signal

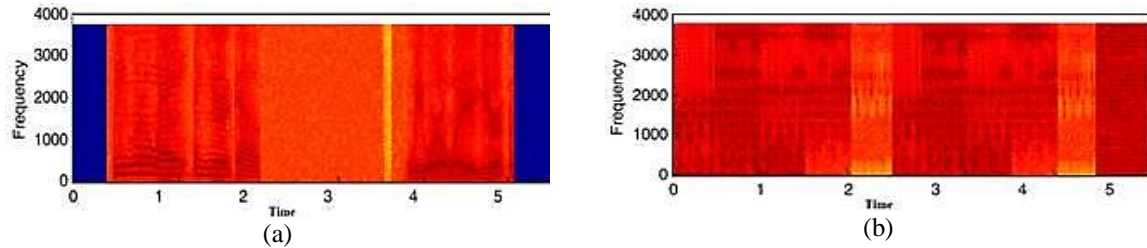


Figure 7. Spectrograms of (a) original signal and (b) encrypted signal with the inserted key ( $K_s$ )

**5. SECURITY ANALYSIS**

When a new cryptosystem is suggested, a certain security evaluations should be included. A secure encryption procedure should be resistant to all forms of assaults from the cryptanalytic, the statistical, and brute-force kind. Various security evaluations, such as key space analysis and statistical analysis, have been performed on the proposed scheme in this section. The new scheme had a high security level, according to the security analysis. A two-phase evaluation of the proposed a scheme's performance and security was carried out: first, key positions were examined, and then, cipher data with the inserted key was examined.

**5.1. Key positions**

In the proposed scheme, there should be a public table available on both ends (i.e., sender and receiver). Since the public table is not secret, it can be made public as shown in Figure 8. A private table was constructed after executing regular confusion and diffusion operations using Jacobian elliptic map as shown in Figure 9, and the values (i.e., HEX) in the private table were used to produce the key positions.

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
1	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	0	1	2	3	4	5	6	7
2	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	0	1	2	3	4	5	6	7	8
3	2	3	4	5	6	7	8	9	A	B	C	D	E	F	0	1	2	3	4	5	6	7	8	9
4	3	4	5	6	7	8	9	A	B	C	D	E	F	0	1	2	3	4	5	6	7	8	9	A
5	4	5	6	7	8	9	A	B	C	D	E	F	0	1	2	3	4	5	6	7	8	9	A	B
6	5	6	7	8	9	A	B	C	D	E	F	0	1	2	3	4	5	6	7	8	9	A	B	C
7	6	7	8	9	A	B	C	D	E	F	0	1	2	3	4	5	6	7	8	9	A	B	C	D
8	7	8	9	A	B	C	D	E	F	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E
9	8	9	A	B	C	D	E	F	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
10	9	A	B	C	D	E	F	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	0
11	A	B	C	D	E	F	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	0	1
12	B	C	D	E	F	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	0	1	2
13	C	D	E	F	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	0	1	2	3
14	D	E	F	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	0	1	2	3	4
15	E	F	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	0	1	2	3	4	5
16	F	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	0	1	2	3	4	5	6
17	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	0	1	2	3	4	5	6	7
18	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	0	1	2	3	4	5	6	7	8
19	2	3	4	5	6	7	8	9	A	B	C	D	E	F	0	1	2	3	4	5	6	7	8	9
20	3	4	5	6	7	8	9	A	B	C	D	E	F	0	1	2	3	4	5	6	7	8	9	A
21	4	5	6	7	8	9	A	B	C	D	E	F	0	1	2	3	4	5	6	7	8	9	A	B
22	5	6	7	8	9	A	B	C	D	E	F	0	1	2	3	4	5	6	7	8	9	A	B	C
23	6	7	8	9	A	B	C	D	E	F	0	1	2	3	4	5	6	7	8	9	A	B	C	D
24	7	8	9	A	B	C	D	E	F	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E

Figure 8. Public table ( $P_{m \times n}$ )

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5
2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6
3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7
4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8
5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9
6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0
7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1
8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2
9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3
10	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4
11	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5
12	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6
13	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7
14	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8
15	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9
16	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0
17	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1
18	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2
19	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3
20	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4
21	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5
22	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6
23	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7
24	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8

Figure 9. Private table ( $P_r$ )

The relationship between the public table and the private table has an impact on the strength of the key positions. In other words, the key positions are strengthened when there is no relation (i.e., connection) between the public and private tables. However, if there is a link between the public and private tables, attackers may be able to re-generate the key positions. Therefore, correlation analysis was used in this research to investigate the relationship between the public table and the private table.

**5.1.1. Correlation analysis**

The following relation is used to determine the correlation coefficients in diagonal, vertical, and horizontal directions for the correlations between the public and private tables [18], [27]:

$$cov(x, y) = \frac{1}{N} \sum_{i=1}^N (x_i - E(x))(y_i - E(y)) , r_{xy} = \frac{cov(x, y)}{\sqrt{D(x)}\sqrt{D(y)}} ,$$

where,

$$E(x) = \frac{1}{N} \sum_{i=1}^N x_i , D(x) = \frac{1}{N} \sum_{i=1}^N (x_i - E(x))^2 \tag{8}$$

$E(x)$  is the mathematical expectation of  $x$ ,  $D(x)$  is the variance of  $x$ , and  $cov(x, y)$  is the covariance between  $x$  and  $y$ . Correlation analysis is performed by selecting random data from the public and private tables. Table 1 contains the correlation coefficients for the public and private tables in vertical, horizontal, and diagonal directions.

	Public Table	Private Table
Vertical	1.0	- 0.069
Horizontal	1.0	0.0501
Diagonal	1.0	- 0.0716

The correlation coefficient, which varies from [-1 to +1], measures the degree of correlation between the public and private tables [28]. Correlation coefficients in Table 1 show that the private table's three-dimensional correlation coefficients are close to zero, whereas public table correlation coefficients for all three dimensions are 1.00. There appears to be a significant gap between the public and private tables. The comparable distributions for public table in the horizontal and vertical directions are illustrated respectively in Figure 10(a) and Figure 10(b) as well as the distributions for private table in the horizontal and vertical directions is respectively illustrated in Figure 10(c) and Figure 10(d). From Figure 10, it can be seen that the Jacobian elliptic map has successfully covered all of the public table characters while also demonstrating good performance.

**5.2. Cipher-text with the inserted key**

There are a number of different statistical tests that can be used to evaluate security level of the ciphered data with the inserted key (i.e., correlation coefficients and NIST) that may be used in this context. The purpose of these tests is to determine the randomness (i.e., unpredictability) of a given sequence [29].

**5.2.1. Correlation coefficients test**

The correlation coefficient between identical segments (i.e., clear and cipher signals) may be used to evaluate the encryption quality of any cryptosystem. In the chaotic system, a powerful encryption mechanism that can be easily detected using the correlation approach was discovered [29]. For the original speech data and ciphered speech data, correlation coefficients are determined and given in Table 2 in this section. Table 2 indicates that the proposed speech encryption scheme is sufficiently efficient since the correlation test has been satisfied, indicating that it is resistant to statistical assaults.

File Name	Original	Ciphered	Ciphered with inserted key
Speech Sample No. 1	0.85139	0.000889	0.000592
Speech Sample No. 2	0.89672	0.000754	0.000649
Speech Sample No. 3	0.96571	0.000896	0.000708

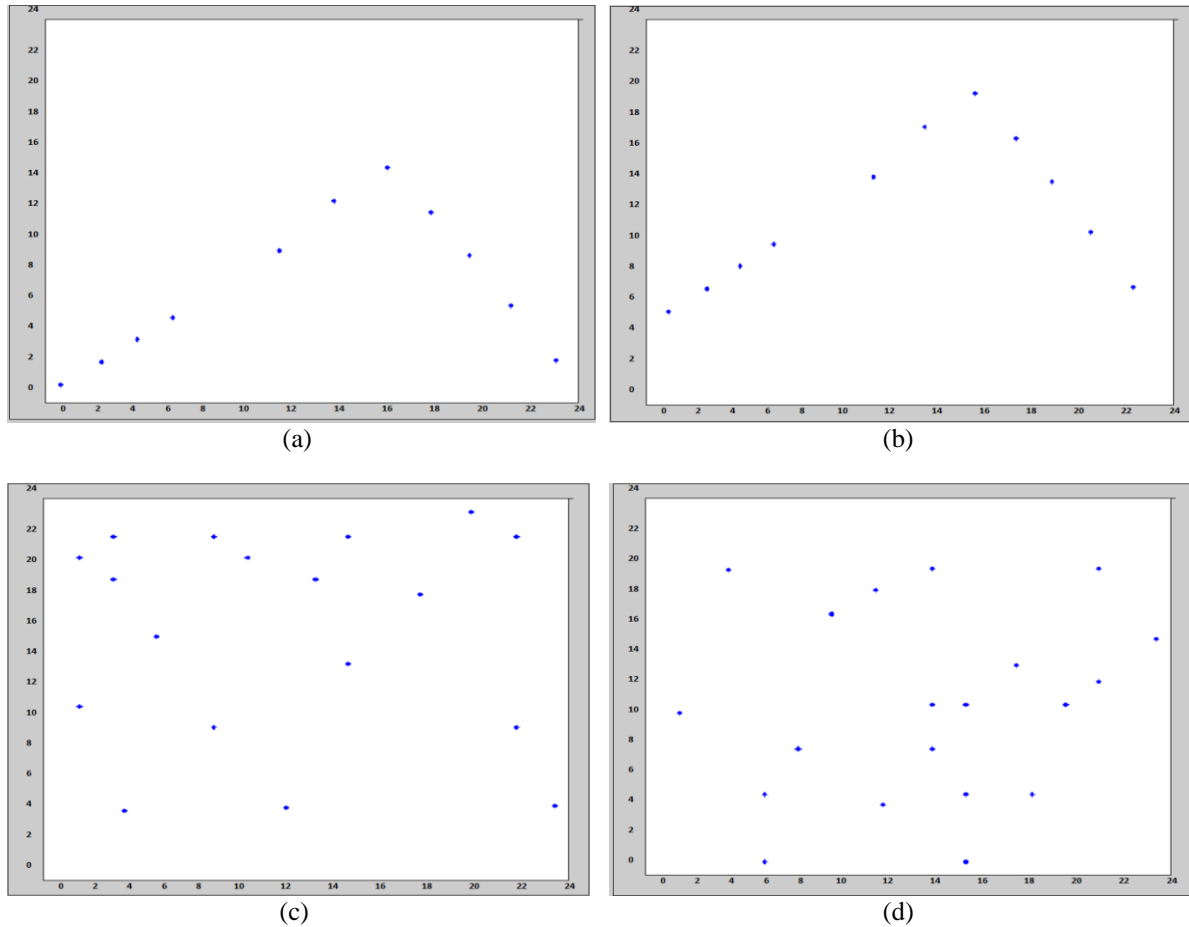


Figure 10. Correlation analysis of (a) public table-horizontal, (b) public table-vertical, (c) private table-horizontal, and (d) private table-vertical

**5.2.2. Randomness tests**

We used a statistical test suite (i.e., 15 tests) known as NIST to assess the strength of ciphered speech frames against cryptanalysis assaults [30], [31]. These suites are primarily used to assess the quality of randomization for a particular sequence. Table 3 (see Appendix) shows that the p-value of each test runs from 0.01 to 0.99, indicating that the ciphered data sequence behavior is random at the 99 percent confidence level. Table 3 shows the NIST test suite findings for the speech sample, and it can be inferred that the ciphered data exhibits extremely unpredictable behavior (i.e., random) since p-value within the success range.

**5.2.3. Key-space analysis**

To ensure the security of a cryptosystem, the key space should be big enough to make brute-force attacks impractical [32]. The secret key for the chaotic Jacobian elliptic map depends on the size of the ciphered blocks. Table 4 lists the number of potential keys based on the size of the key (i.e., Possibility). In the proposed scheme, the secret key size is 1024 bit, the results in a key space size is equal to  $3.17 \times 10^{365}$ , which is very large to prevent brute-force attacks.

Table 4. Key-space analysis

Secret key length	Possibility	Cryptanalysis computation time (Year)
64 -bit	$1 \times 10^{34}$	$3.17 \times 10^{17}$
128-bit	$1 \times 10^{62}$	$3.17 \times 10^{51}$
256-bit	$1 \times 10^{126}$	$3.17 \times 10^{113}$
512-bit	$1 \times 10^{252}$	$3.17 \times 10^{239}$
1024-bit	$1 \times 10^{506}$	$3.17 \times 10^{365}$



**5.2.4. Key sensitivity analysis**

The most significant feature of chaotic encryption is key sensitivity. Key sensitivity implies that if the encryption and decryption keys differ by a little amount, the encrypted speech signal cannot be deciphered accurately [18], [26]. In other words, if a single bit value of the keys were changed in the suggested scheme, the decryption results would be radically different as demonstrated in Figure 11(a). As well as, if a position of the keys were changed, the decryption results would be radically different in the suggested scheme as shown in Figure 11(b).

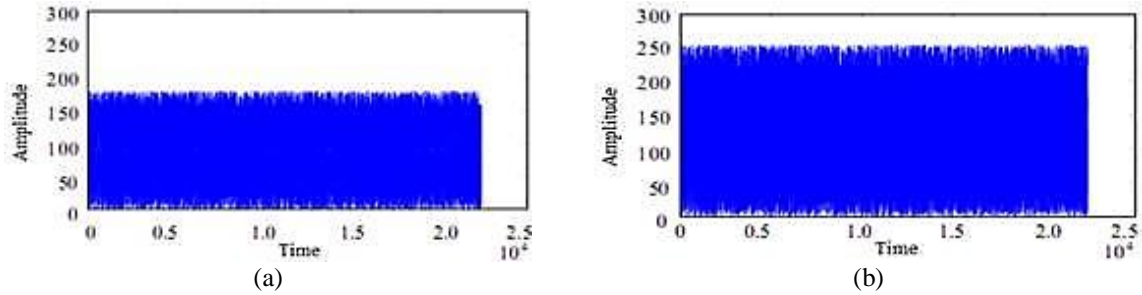


Figure 11. Key sensitivity analysis of (a) decryption with incorrect secret key (Ks) and (b) decryption with incorrect positions

**6. CONCLUSION**

To improve the quality of speech applications, we developed a scheme based on the Jacobian elliptic map and described in this work. The key management, key insertion, and encryption/decryption procedures were all separated into three distinct steps in the proposed scheme. In order to assess the suggested scheme's security level, simulations, implementations, and analyses have been carried out efficiently. Every new packet of speech data is protected against cryptanalysis assaults by employing a multi-key and lengthening the proposed scheme's key length (i.e., 1024 bit). Using the suggested scheme, the findings show that it has a greater level of security with minimum time (i.e., delay), making it an appropriate alternative in practical for voice applications.

**APPENDIX**

**Appendix A. Derivation**

A definition of Jacobian elliptic functions is that they are simply the inversion of Legendre's elliptic integral of the first kind. The Schwarzian derivative of the Jacobian elliptic rational maps (i.e., which is defined on the interval [0, 1]) is given by:

$$S_{\phi}(x, \sigma) = D_x^3 \phi_N(x, \sigma) (D_x \phi_N(x, \sigma))^{-1} \frac{3}{2} \left( \left( D_x^2 \phi_N(x, \sigma) (D_x \phi_N(x, \sigma)) \right)^{-1} \right)^2 \tag{A.1}$$

**Appendix B. An example of Jacobian elliptic maps**

As an example of Jacobian elliptic maps, the following maps can be defined:

$$\phi_N(x, \alpha) = \frac{\alpha^2 F^2}{1 + (\alpha^2 - 1) F^2} \tag{B.1}$$

$$\phi_2^{(cn)}(x, \alpha) = \frac{4\alpha^2 x(1-k^2x)(1-x)}{(1-k^2x^2)^2 + 4(\alpha^2 - 1)x(1-k^2x)(1-x)} \tag{B.2}$$

$$\phi_2^{(dn)}(x, \alpha) = \frac{4\alpha^2 x(1-k^2x)(1-x)}{(1-k^2x^2)^2 + 4(\alpha^2 - 1)x(1-k^2x)(1-x)} \tag{B.3}$$

$$\phi_2^{(sn)}(x, \alpha) = \frac{\alpha^2 ((1-k^2)(2x-1) + k^2x^2)^2}{\left( (1-k^2 + 2k^2x - k^2x^2)^2 + ((\alpha^2 - 1)(1-k^2)(2x-1)k^2x^2) \right)^2} \tag{B.4}$$

Table 3. NIST tests suite

Test	References	Formula	Obtained $p$ -value	Behavior
Cumulative Sums	[30], [32]	$p - \text{value} = 1 - \sum_{k=\left(\frac{-n+1}{4}\right)}^{\left(\frac{n-1}{4}\right)} \left[ \Phi\left(\frac{(4k+1)z}{\sqrt{n}}\right) - \Phi\left(\frac{(4k-1)z}{\sqrt{n}}\right) \right] \\ + \sum_{k=\left(\frac{-n-3}{4}\right)}^{\left(\frac{n-1}{4}\right)} \left[ \Phi\left(\frac{(4k+3)z}{\sqrt{n}}\right) - \Phi\left(\frac{(4k+1)z}{\sqrt{n}}\right) \right]$	0.609925	Random
Discrete Fourier Transform (Spectral)	[9], [31], [33]	$p - \text{value} = \text{erfc}\left(\frac{ d }{\sqrt{2}}\right)$	0.307675	Random
Runs	[29], [31]	$p - \text{value} = \text{erfc}\left(\frac{ V_n(\text{obs}) - 2n\pi(1-\pi) }{2\sqrt{2n\pi}(1-\pi)}\right)$	0.900157	Random
Serial	[29], [30]	$p - \text{value}1 = \text{igamc}(2^{m-2}, \nabla\phi^2 m)$ $p - \text{value}1 = \text{igamc}(2^{m-3}, \nabla^2\phi^2 m)$	0.405180	Random
Binary Matrix Rank	[34]	$p - \text{value} = e^{-x^2(\text{obs})/2}$	0.395881	Random
Frequency Test within a Block	[30]	$p - \text{value} = \text{igamc}\left(\frac{N}{2}, x^2 \frac{(\text{obs})}{2}\right)$	0.621272	Random
Non-overlapping Template Matching	[31]	$p - \text{value} = \text{igamc}\left(\frac{N}{2}, \frac{x^2(\text{obs})}{2}\right)$	0.603819	Random
Overlapping Template Matching	[30]	$p - \text{value} = \text{igamc}\left(\frac{5}{2}, \frac{x^2(\text{obs})}{2}\right)$	0.508530	Random
Maurer's	[2], [34], [35]	$p - \text{value} = \text{erfc}\left(\frac{ f_n - \text{expectedValue}(L) }{\sqrt{2\sigma}}\right)$	0.325102	Random
Linear Complexity	[17], [36]	$p - \text{value} = \text{igamc}\left(\frac{k}{2}, \frac{x^2(\text{obs})}{2}\right)$	0.608537	Random
Longest Run of Ones in a Block	[30], [31]	$p - \text{value} = \text{igamc}\left(\frac{k}{2}, \frac{x^2(\text{obs})}{2}\right)$	0.586710	Random
Approximate Entropy	[29], [37]	$p - \text{value} = \text{igamc}\left(2^{m-1}, \frac{x^2}{2}\right)$	0.480018	Random
Frequency	[4], [29], [30]	$p - \text{value} = \text{erfc}\left(\frac{S_{\text{obs}}}{\sqrt{2}}\right)$	0.599644	Random
Random Excursions	[2], [21], [31]	$p - \text{value} = \text{igamc}\left(\frac{5}{2}, \frac{x^2(\text{obs})}{2}\right)$	0.490669	Random
Random Excursions Variant	[31]	$p - \text{value} = \text{erfc}\left(\frac{ \varepsilon(x) - J }{\sqrt{2J(4 x  - 2)}}\right)$	0.508651	Random





## REFERENCES

- [1] E. M. Elshamy *et al.*, "Efficient audio cryptosystem based on chaotic maps and double random phase encoding," *International Journal of Speech Technology*, vol. 18, pp. 619-631, 2015, doi:10.1007/s10772-015-9279-3.
- [2] O. M. Al-Hazaimeh, "A new dynamic speech encryption algorithm based on Lorenz chaotic map over internet protocol," *International Journal of Electrical and Computer Engineering*, vol. 10, p. 4824, 2020, doi:10.11591/ijece.v10i5.
- [3] S. N. Al Saad and E. Hato, "A speech encryption based on chaotic maps," *International Journal of Computer Applications*, vol. 93, pp. 19-28, 2014, doi: 10.5120/16203-548.
- [4] F. S. Hasan, "Speech Encryption using Fixed Point Chaos based Stream Cipher (FPC-SC)," *Eng. &Tech. Journal*, vol. 34, pp. 2152-2166, 2016.
- [5] M. F. Abd Elzaher, M. Shalaby, and S. H. El Ramly, "Securing modern voice communication systems using multilevel chaotic approach," *International Journal of Computer Applications*, vol. 135, pp. 17-21, 2016, doi:10.5120/ijca2016908497.
- [6] M. A.-H. Obaida, "Combining audio samples and image frames for enhancing video security," *Indian Journal of Science and Technology*, vol. 8, p. 940, 2015, doi: 10.17485/ijst/2015/v8i10/53149.
- [7] R. Brown and L. O. Chua, "Clarifying chaos: Examples and counterexamples," *International Journal of Bifurcation and Chaos*, vol. 6, pp. 219-249, 1996, doi: 10.1142/S0218127496000023.
- [8] J. Fridrich, "Symmetric ciphers based on two-dimensional chaotic maps," *International Journal of Bifurcation and chaos*, vol. 8, pp. 1259-1284, 1998, doi: 10.1142/S021812749800098X.
- [9] O. Al-Hazaimeh, M. Al-Jamal, M. Bawaneh, N. Alhindawi, and B. Hamdoni, "A New Image Encryption Scheme Using Dual Chaotic Map Synchronization," *International Arab Journal Of Information Technology*, vol. 18, pp. 95-102, 2021, doi: 10.34028/iajit/18/1/11.
- [10] N. Tahat, A. Alomari, A. Al-Freedi, O. M. Al-Hazaimeh, and M. F. Al-Jamal, "An Efficient Identity-Based Cryptographic Model for Chebyhev Chaotic Map and Integer Factoring Based Cryptosystem," *Journal of Applied Security Research*, vol. 14, pp. 257-269, 2019, doi: 10.1080/19361610.2019.1621513.
- [11] S. Behnia, A. Akhshani, H. Mahmodi, and A. Akhavan, "A novel algorithm for image encryption based on mixture of chaotic maps," *Chaos, Solitons & Fractals*, vol. 35, pp. 408-419, 2008, doi: 10.1016/J.CHAOS.2006.05.011.




- [12] N. Tahat, A. A. Tahat, M. Abu-Dalu, R. B. Albadarneh, A. E. Abdallah, and O. M. Al-Hazaimah, "A new RSA public key encryption scheme with chaotic maps," *International Journal of Electrical & Computer Engineering (2088-8708)*, vol. 10, 2020, doi: 10.11591/ijece.v10i2.pp1430-1437.
- [13] M. Farah, A. Farah, and T. Farah, "An image encryption scheme based on a new hybrid chaotic map and optimized substitution box," *Nonlinear Dynamics*, vol. 99, pp. 3041-3064, 2020, doi: 10.1007/s11071-019-05413-8.
- [14] 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, pp. 1-11, 2017, doi: 10.1186/S13636-017-0118-0.
- [15] H. B. A. Wahab and S. I. Mahdi, "Modify speech cryptosystem based on shuffling overlapping blocks technique," *International Journal of Emerging Trends & Technology in Computer Science*, vol. 4, pp. 70-75, 2015.
- [16] F. Farsana and K. Gopakumar, "A novel approach for speech encryption: Zaslavsky map as pseudo random number generator," *Procedia computer science*, vol. 93, pp. 816-823, 2016, doi: 10.1016/J.PROCS.2016.07.30.
- [17] Z. Habib, J. S. Khan, J. Ahmad, M. A. Khan, and F. A. Khan, "Secure speech communication algorithm via DCT and TD-ERCS chaotic map," in *2017 4th international conference on electrical and electronic engineering (ICEEE)*, 2017, pp. 246-250, doi: 10.1109/ICEEE2.2017.7935827.
- [18] O. M. Al-hazaimah, "A new speech encryption algorithm based on dual shuffling Hénon chaotic map," *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 11, pp. 2203-2210, 2021, doi: 10.11591/IJECE.V11I3.PP2203-2210.
- [19] S. Elnashaie, M. Abashar, and F. Teymour, "Chaotic behaviour of fluidized-bed catalytic reactors with consecutive exothermic chemical reactions," *Chemical engineering science*, vol. 50, pp. 49-67, 1995, doi: 10.1016/0009-2509(94)00178-T.
- [20] O. M. Al-hazaimah, "A novel encryption scheme for digital image-based on one dimensional logistic map," *Computer and Information Science*, vol. 7, p. 65, 2014, doi: 10.5539/cis.v7n4p65.
- [21] L. Kocarev, "Chaos-based cryptography: a brief overview," *IEEE Circuits and Systems Magazine*, vol. 1, pp. 6-21, 2001, doi: 10.1109/7384.963463.
- [22] V. Ponomarenko and M. Prokhorov, "Extracting information masked by the chaotic signal of a time-delay system," *Physical Review E*, vol. 66, p. 026215, 2002, doi: 10.1103/PHYSREVE.60.320.
- [23] C. Li, S. Li, G. Chen, and W. A. Halang, "Cryptanalysis of an image encryption scheme based on a compound chaotic sequence," *Image and Vision Computing*, vol. 27, pp. 1035-1039, 2009, doi: 10.1016/j.imavis.2008.09.004.
- [24] F. Farsana, V. Devi, and K. Gopakumar, "An audio encryption scheme based on Fast Walsh Hadamard Transform and mixed chaotic keystreams," *Applied Computing and Informatics*, 2020, doi: 10.1016/j.aci.2019.10.001.
- [25] M. Jafarizadeh and S. Behnia, "Hierarchy of one-and many-parameter families of elliptic chaotic maps of cn and sn types," *Physics Letters A*, vol. 310, pp. 168-176, 2003, doi: 10.1016/S0375-9601(03)00343-8.
- [26] R. L. Devaney, *An introduction to chaotic dynamical systems*: Chapman and Hall/CRC, 1989.
- [27] F. Yang, J. Mou, C. Ma, and Y. Cao, "Dynamic analysis of an improper fractional-order laser chaotic system and its image encryption application," *Optics and Lasers in Engineering*, vol. 129, p. 106031, 2020, doi: 10.1016/j.optlaseng.2020.106031.
- [28] S. Tao, W. Ruli, and Y. Yixun, "Perturbance-based algorithm to expand cycle length of chaotic key stream," *Electronics Letters*, vol. 34, pp. 873-874, 1998.
- [29] S.-J. Kim, K. Umeno, and A. Hasegawa, "Corrections of the NIST statistical test suite for randomness," *arXiv preprint nlin/0401040*, 2004.
- [30] C. Georgescu, E. Simion, A.-P. Nita, and A. Toma, "A view on NIST randomness tests (in) dependence," in *2017 9th International Conference on Electronics, Computers and Artificial Intelligence (ECAI)*, 2017, pp. 1-4, doi: 10.1109/ECAI.2017.8166460.
- [31] M. Sys and Z. Řiha, "Faster randomness testing with the NIST statistical test suite," in *International Conference on Security, Privacy, and Applied Cryptography Engineering*, 2014, pp. 272-284.
- [32] O. M. Al-Hazaimah, M. F. Al-Jamal, N. Alhindawi, and A. Omari, "Image encryption algorithm based on Lorenz chaotic map with dynamic secret keys," *Neural Computing and Applications*, vol. 31, pp. 2395-2405, 2019, doi: 10.1007/s00521-017-3195-1.
- [33] G. Gong, S. Ronjom, T. Helleseth, and H. Hu, "Fast discrete Fourier spectra attacks on stream ciphers," *IEEE Transactions on Information Theory*, vol. 57, pp. 5555-5565, 2011, doi: 10.1109/TIT.2011.2158480.
- [34] Q. Din, A. Elsadany, and S. Ibrahim, "Bifurcation analysis and chaos control in a second-order rational difference equation," *International Journal of Nonlinear Sciences and Numerical Simulation*, vol. 19, pp. 53-68, 2018, doi: 10.1515/ijnsns-2017-0077.
- [35] T. Etem and T. Kaya, "A novel true random bit generator design for image encryption," *Physica A: Statistical Mechanics and its Applications*, vol. 540, p. 122750, 2020, doi: 10.1016/j.physa.2019.122750.
- [36] M. Khan and A. Rasheed, "Permutation-based special linear transforms with application in quantum image encryption algorithm," *Quantum Information Processing*, vol. 18, pp. 1-21, 2019, doi: 10.1007/s11128-019-2410-7.
- [37] M. Chen, H. Chen, L. Fan, and D. Feng, "Templates selection in non-overlapping template matching test," *Electronics Letters*, vol. 52, pp. 1533-1535, 2016, doi: 10.1049/EL.2016.0260.

## BIOGRAPHIES OF AUTHORS






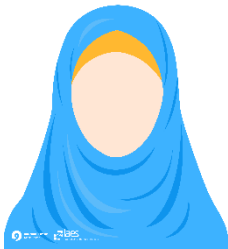
**Obaida M. Al-Hazaimah**     earned a BSc in Computer Science from Jordan's Applied Science University in 2004 and an MSc in Computer Science from Malaysia's University Science Malaysia in 2006. In 2010, he earned a PhD in Network Security (Cryptography) from Malaysia. He is an associate professor at Al-Balqa Applied University's department of computer science and information technology. Cryptology, image processing, machine learning, and chaos theory are among his primary research interests. He has published around 40 papers in international refereed publications as an author or co-author. He can be contacted at email: dr\_obaida@bau.edu.jo.






**Ashraf A. Abu-Ein**    is an Associate Professor in the Department of Electrical Engineering. He has completed his PhD at National Technical University of Ukraine, Computer Engineering. “Computers, Computing Systems and Networks”, 2007. Now, he is a lecturer at Al-Balqa Applied University–Al-huson University College, Jordan. He can be contacted at email: ashraf.abuain@bau.edu.jo.



**Khalid M. Nahar**    is an Associate Professor in the Department of Computer Sciences-Faculty of IT, Yarmouk University, Irbid-Jordan. He received his BS and MS in Computer Sciences from Yarmouk University in Jordan, He was awarded a full scholarship to continue his PhD in Computer Sciences and Engineering from King Fahd University of Petroleum and Minerals (KFUPM), KSA. In 2013, he completed his PhD. For now, he was the dean assistant for quality assurance for one year, and for now, he is the chairman of the training department at the accreditation and quality assurance center. He can be contacted at email: khalids@yu.edu.jo.



**Isra S. Al-Qasrawi**    received the B.S. degree in Computer Science from Al-Balqa Applied University, Jordan in 2004, the MSc in Computer Science from Yarmouk University, Jordan in 2009, Working as instructor in Al-Balqa Applied University/Al-Huson University College-Department of Information Technology. She can be contacted at email: israonnet@bau.edu.jo