Digital Audio Signal Encryption Using a Chaotic Logistic Map and Variable-length Private Key

Sara Al-Omari *, Zayed Huneiti, and Ahmed Abu-Khadrah
Department of Electrical Engineering, Al-Balqa Applied University, Amman, Jordan
Email: sara.omari@bau.edu.jo (S.A.-O.); zayedhuneiti@bau.edu.jo (Z.H.); a.abukhadrah@bau.edu.jo (A.A.-K.)

Manuscript received May 6, 2026; revised June 8, 2026; accepted June 21, 2026; published September 22, 2026
*Corresponding author

***Abstract*—With the accelerated growth of the global requirements in digital communication and multimedia applications, the need to secure audio data has become progressively important. Digital Audio Signals (DASs) are widely used in broadcasting, voice communication, and several other applications, and they may carry sensitive or private information. For this reason, secure encryption methods are required to protect audio data, especially during propagation. In this paper, a fast and secure cryptographic method for DASs is proposed. The method uses a variable number of encryption and decryption rounds, a variable-length Private Key (PK), and variable-size audio blocking to balance security strength and computational efficiency. The proposed method employs a simple encryption-decryption function, which enhances processing speed compared to existing methods. The PK length increases as the number of rounds is increased, reaching 544 bits when four rounds are utilized, thereby providing a large key space. Test results show that when the number of rounds is increased from 1 to 4, the mean squared error increases from 0.4755 to 6.7589, whereas the peak signal-to-noise ratio and correlation coefficient values decrease from 12.6134 to 8.3193 and from 0.2010 to 0.1036, respectively. Furthermore, the encryption-decryption speed stays quite high, decreasing from 3.8499 M Samples/s to 1.1507 M Samples/s. The results confirmed that the proposed method provides acceptable reconstructed-signal quality, a good level of security, and a competitive processing speed that is less than 1 M Samples/s, making it a promising solution for secure, fast, and efficient audio transmission in modern digital systems.**

***Index Terms*—audio encryption, chaotic logistic map, cryptography, digital audio signals, encryption speed, key space, private key, signal quality**

I. Introduction

With the considerable evolution of multimedia technologies and digital communication systems, the transmission of digital data over private and public networks has expanded considerably in recent years. Multimedia data now plays an important role in contemporary life, including online voice communication, broadcasting, music streaming, healthcare systems, cloud storage platforms, and remote learning. Among the varieties of multimedia, Digital Audio Signals (DASs) represent a widely used and important category because they are directly involved in many daily technical uses. Since audio signals may contain sensitive, confidential, or private information, securing them during transmission and storage has become a very important requirement in modern digital systems.

In general, data security can be attained using multiple methods such as encryption, watermarking, and data hiding. Among these methods, encryption is regarded as one of the most immediate and effective techniques because it converts the original significant signal into an incomprehensible form that cannot be recognized without the precise secret key. This idea is highlighted throughout the multimedia-encryption publications, particularly in image-encryption publications, where encryption is employed to transform original significant content into corrupted data and recover the original content only with the precise key [1, 2]. These studies also record that multimedia signals have features such as redundancy, strong interaction between adjacent elements, and large data size, which make their protection more difficult than common text data.

Conventional cryptographic methods such as Advanced Encryption Standard (AES), Data Encryption Standard (DES), Rivest-Shamir-Adleman (RSA), Elliptic Curve Cryptography (ECC), and International Data Encryption Algorithm (IDEA) provide a high security level in many communication applications [1, 2]. However, multimedia data often calls for encryption methods that can provide not only a high security level but also good computational efficiency. These conditions become more necessary when the secured data is large and continuously generated, or employed in applications that need fast handling. Several studies in the published literature indicate that traditional methods are not always the most proper choice for multimedia signals because multimedia data and images contain strong local correlation and high redundancy. For this reason, many recent publications have focused on modeling specialized encryption methods for multimedia applications rather than relying only on general-purpose cryptographic methods [3–5].

One of the most commonly used approaches in multimedia security publications is chaos-based encryption. Chaos theory has received significant attention in cryptographic applications because chaotic systems have multiple useful features, such as unpredictability, sensitivity to initial conditions, ergodicity, and pseudo-randomness [6–8]. These features make chaotic systems convenient for creating complex sequences that

can be employed in encryption processes. A general principle in chaos-based multimedia encryption is the confusion-diffusion configuration. In the confusion step, the locations of data elements are altered to cover their original sequence, while in the diffusion step, the values of these data elements are modified so that a minor change in the original signal spreads throughout the encrypted output. This principle has been extensively employed in image-encryption algorithms because it assists in reducing statistical correlation and destroying the substantial correlation between adjacent pixels [9, 10].

Several current studies have proposed progressive chaos-based algorithms to enhance both efficiency and security. For example, some of them suggest new chaotic structures to produce maps with more complicated dynamical behavior, aiming to overcome the weaknesses of conventional or simple chaotic maps [11, 12]. Other studies focused on upgrading diffusion processes and scrambling through random substitution, bit-plane processing, Deoxyribonucleic Acid (DNA)-based operations, super pixel representation, and multi-image encryption strategies [13]. These methods are commonly analyzed using criteria such as key sensitivity, key space, histogram analysis, entropy, resistance to differential attacks, execution speed, and correlation analysis [14, 15]. These measures are important because a robust encryption method should present a low correlation in the encrypted output, a sufficiently large key space, high sensitivity to secret-key changes, and acceptable computational cost.

At the same time, researchers have shown that there is always a trade-off between processing efficiency and security strength [16]. Some techniques improve encryption quality and defense against attacks, but they may need more computational stages, more complicated procedures, or even more time for execution. Other techniques focus on simplicity and speed, but they may be less secure if the internal structure or key space is weak. One published study states clearly that, although its published method has robust cryptanalytic properties, it is not appropriate for real-time applications like streaming video encryption [10]. This observation highlights an important challenge in multimedia cryptography, since an encryption method must not only be efficient enough for practical implementation but also be secure enough to resist attacks.

Although most of the published research papers mainly focus on image and multiple-image encryption, they provide functional design ideas that can influence the improvement of digital audio-encryption techniques [17, 18]. However, DASs are different from images in both practical requirements and structure. An image is typically arranged in a two-dimensional sequence, while the audio signal is a one-dimensional time-varying form. In addition, many audio usages require conserving satisfactory reconstructed-signal quality after decryption while still preserving fast processing speed. Therefore, directly employing image-encryption methods to digital audio data may not always be suitable without adjustment. This creates an evident necessity for encryption methods that are especially intended for DASs while still taking advantage of the main ideas of current multimedia-encryption research.

Inspired by this need, this paper suggests a simple and efficient cryptographic technique for DASs. The proposed method is intended to achieve a balance between security strength and execution cost. Rather than using a fixed encryption frame only, the method applies a variable number of encryption and decryption rounds, allowing the operator to control and handle the trade-off between security level and speed according to the needs of the usage. As the number of rounds rises, the encrypted signal becomes more distorted, and the security level becomes stronger, but the handling time also increases. This flexibility is significant because various applications may need different performance constraints and different levels of security. The general block diagram of the proposed DAS cryptographic method is shown in Fig. 1.

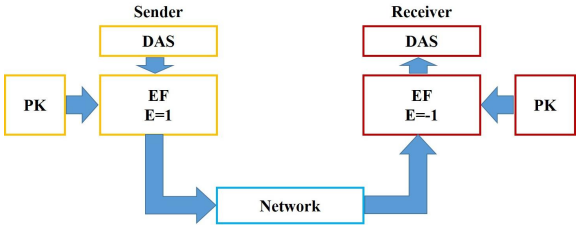

Fig. 1. DAS cryptographic process block diagram.

Another important feature of the proposed method is the employment of a variable-length Private Key (PK). A large and elastic key space is a very important requirement in any safe cryptographic system because it improves resistance to brute-force attacks and unauthorized access attempts [19]. Multimedia-encryption publications regularly emphasize the need for large key spaces and high key sensitivity, since even a very small variation in the key must produce a different encrypted output or forbid successful decryption [20]. Based on this principle, the proposed technique takes on a variable-length PK to support security and enhance resistance against hacking attempts.

In addition, the proposed method uses variable-size blocking of the DAS to improve computational efficiency and to decrease the time needed for key generation. This criterion aims to streamline implementation and improve processing speed compared with more involved speech-cryptography methods [21–23]. In this way, the proposed method provides three important design specifications: a variable number of rounds, a variable PK length, and a variable signal blocking size. These features are planned to make the method suitable for practical audio-encryption applications where both security and efficiency are essential [24].

Recent studies have validated the continuing attention to secure DAS. A byte-level audio-encryption method based on direct audio-domain processing and multiple chaotic systems [25]. Also, a Field Programmable Gate Array (FPGA) based execution of a secure audio-encryption system using a chameleon chaotic algorithm was introduced, by which the practical importance of hardware-oriented recognition was

demonstrated [26]. In addition, an audio-encryption and decryption method predicated on Elliptic Curve Cryptography (ECC) and DNA-related processing was announced, through which hybrid cryptographic methods were shown to be an active direction in recent audio-encryption research [27]. This recent research is directed toward improving implementation efficiency, practical applicability, and security strength in modern audio cryptography.

To evaluate the proposed method, several DASs are used in the testing phase. The performance is tested in terms of level of security, decrypted signal quality, and execution time. These testing factors are determined because a successful audio-encryption process should not only hide the original signal efficiently, but also should allow proper restoration after decryption and operate within a satisfactory processing time. In multimedia-encryption research studies, performance measurements often include measures such as key space, attack resistance, entropy, and correlation, which further support the significance of evaluating both security and efficiency.

Hence, as stated earlier, this paper proposes and tests a simple and efficient encryption method for DASs. The method uses a variable number of rounds, a variable-length PK, and variable-size signal blocking to strike a fine balance between security and computational efficiency. Its performance is proven in terms of level of security, quality of the reconstructed signal, and time of execution.

The proposed work presents a simple and computationally efficient chaos-based DAS encryption method based on a variable number of encryption rounds to provide flexibility between processing efficiency and security level. A variable-length PK generation mechanism was implemented, where the PK length increases according to the selected number of encryption rounds. Also, it utilizes variable-size signal blocking and a one-dimensional chaotic logistic map to achieve efficient DAS encryption and decryption without requiring complex data-conversion operations. Furthermore, security analyses, including entropy analysis, histogram analysis, and Number of Pixels Change Rate/Unified Average Changing Intensity (NPCR/UACI) evaluations, were performed to validate the statistical and differential security characteristics of the proposed DAS encryption method.

II. Related Works

Multimedia encryption has been the focus of many researchers over the years because the safe and efficient protection of digital data, such as images, audio, and video, is vital, particularly during transmission and storage.

In 2019, a cosine-transform-based chaotic system was introduced for image digital data encryption [6]. A common chaotic structure that is capable of generating new chaotic maps with more complicated dynamical behavior than many traditional maps was proposed. The main strength of this work is established based on the development of chaotic-map complication, by which encryption efficiency was improved. However, a restriction in relation to the study is that the method was improved for image encryption and assessed on two-dimensional image data. The main idea of using a stronger chaotic generator can be applied to digital audio encryption, since pseudo-random arrangements are also needed in audio signals for confusion and diffusion tasks. This may be a helpful motivation for constructing a secure audio-encryption method that can be derived from chaotic-system design.

An image-encryption method predicated on polynomial combinations of chaotic maps and kinetic function creation was introduced in [10]. Strong statistical and cryptanalytic properties were highlighted, and a high level of security performance with robust resistance to multiple common analyses was stated. A valuable contribution of this paper depends on the development of chaotic design, through which simple chaotic deficiency maps were handled. However, it was also recorded in the paper that the technique is not convenient for streaming video encryption as a real-time application, which shows a relatively high computational cost. This limitation is significant when audio applications are employed, since fast processing is required. Nevertheless, the method used can still be adapted to audio signals, particularly dynamic-function-based encryption and polynomial chaotic-map generation, to improve the safety, under the condition that the produced method is simplified to satisfy practical speed needs.

In Ref. [17], a multiple-image encryption technique predicated on chaotic systems and DNA encoding was introduced. Several simple images were first embedded into one large image, after which DNA encoding, decoding operations, diffusion, and chaotic scrambling were applied. High security, strong performance, and strong encryption performance according to standards such as statistical analysis, entropy, and key space were reported. The main advantage of this work lies in the integration of chaotic systems with DNA computing concepts, by which multimedia-encryption security was enhanced. However, the approach was developed to include several processing stages and multiple-image encryption, such as DNA encoding and decoding, by which algorithmic complexity was increased. For DASs, such a complication may decrease processing productivity. Even so, the fundamental method of blending chaotic sequences with DNA-inspired methods can be applied to an audio-encryption scheme, particularly when improvement of resistance to attacks, key sensitivity, and randomness is required.

In Ref. [18], a multiple-image encryption method based on chaotic maps and bit-plane decomposition was proposed. Diffusion and scrambling processes were applied in the bit-plane domain, and acceptable efficiency with good security for multiple-image security was shown. The significant investment of this work is that it displayed how encryption performance can be enhanced through bit-level processing while high security features are conserved. The main limitation of the study is that it depends on image-specific bit-plane decomposition and concentrates on multiple-image data. Therefore, the method cannot be immediately implemented on one-dimensional audio signals without adjustment. However,

the outline of bit-level control joined with chaotic handling can be applied to digital audio encryption, since audio models can also be processed and represented at the bit level. Therefore, this approach may be considered as a transferable encryption strategy rather than a suitable audio method.

Recent works have also extended the scope of audio encryption. In 2026, a byte-level audio-encryption method based on multiple chaotic systems was shown, in which direct handling in the audio domain was introduced to improve encryption efficiency. Using direct byte-level processing makes the encryption operation closer to the original audio data. However using multiple chaotic systems increases the structural complexity of the process [25]. In reference [26], an FPGA-based implementation of a protected audio-encryption system employing a chameleon chaotic algorithm was shown, through which the practical importance of hardware recognition was demonstrated. A significant benefit of this work is that its suitability for hardware-oriented protected audio systems was obviously shown. However, the method was primarily focused on implementation at the hardware level, which may restrict its simplicity and flexibility in software applications. In Ref. [27], an audio-encryption and decryption method based on Elliptic Curve Cryptography (ECC) and DNA-related processing was stated, showing that hybrid cryptographic models continue to draw attention. The strength of this work is based on combining ECC with DNA-related processing, by which both hybrid design ability and security were emphasized. However, the embedding of multiple cryptographic components increases the overall design complexity. Therefore, although useful improvements in protection and implementation strategies were supplied by these methods, relatively high implementation complexity was still involved in them.

From the above studies, it can be noted that these studies provide important methods in dynamic function generation, chaotic-map construction, bit-level encryption, and DNA-based processing. Although these studies were particularly implemented for multiple-image and image encryption, their key systems can be employed for DASs because both audio and image encryption aim to increase randomness, reduce data correlation, strengthen resistance against attacks, and enlarge key space. However, these techniques were not significantly prepared for the time-varying nature and the one-dimensional nature of DASs, and some of them also include relatively higher computational complexity. Therefore, the proposed method in this paper aims to gain from these techniques while delivering a more efficient and simpler encryption structure for DASs. The operation of the method is assessed in terms of reconstructed-signal quality, execution time, and security level, and the results show that it provides satisfactory security, adequate quality of the reconstructed signal, and competitive execution speed.

III. Proposed Method

A. Chaotic Logistic Data Set Generation

The Chaotic Logistic Data Set (CLDS) is a set of partial numbers produced using a Chaotic Logistic Map Model (CLMM). This data set is made by using the initial value x, the control parameter r, and the required set size L. According to these values, the chaotic logistic formula is employed to calculate each element of the set, as illustrated in Fig. 2, which shows an example of using the CLMM to produce a ten-element CLDS.

$$x_{i+1} = rx_i(1 - x_i), \qquad 0 < x_i < 1, 0 < r \leq 4$$

where x_i is the current value, r is the control parameter, and L is the number of generated elements.

The produced CLDS can then be written as

$$\text{CLDS} = \{x_1, x_2, \ldots, x_L\}$$

r=3.76
x_0=0.11
L=10

CLDS =

0.3681	**0.8746**	**0.4124**	**0.9112**	**0.3044**
0.7961	**0.6103**	**0.8943**	**0.3555**	**0.8615**

Fig. 2. Example of generated CLDS values using one-dimensional CLMM.

The generated CLDS is highly sensitive to the control parameter r and the initial value x. A very small variation in either of these values produces a significant difference in the generated CLDS, as shown in Fig. 3. This sensitivity is an important chaotic property, since it increases randomness and improves the security of the encryption process.

r=3.76;x=0.11	r=3.66;x=0.11	r=3.76;x=0.12	r=3.66;x=0.10
0.3681	0.3583	0.3971	0.3294
0.8746	0.8415	0.9002	0.8085
0.4124	0.4881	0.3379	0.5667
0.9112	0.9145	0.8412	0.8987
0.3044	0.2862	0.5021	0.3332
0.7961	0.7477	0.9400	0.8131
0.6103	0.6904	0.2121	0.5561
0.8943	0.7824	0.6284	0.9035
0.3555	0.6232	0.8780	0.3192
0.8615	0.8595	0.4027	0.7953

Fig. 3. Effect of varying r and x on the generated CLDS.

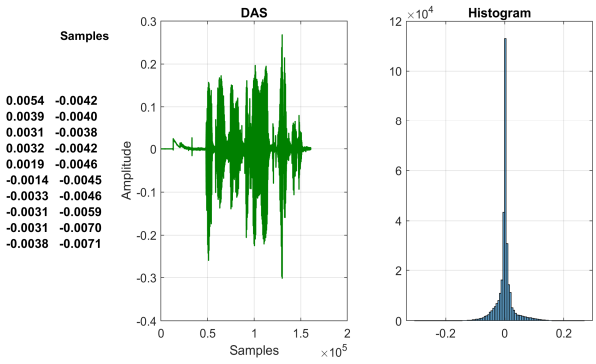

Fig. 4. DAS representation in terms of samples, waveform, and histogram distribution.

The CLDS can be utilized as a noise-like signal in the introduced cryptographic method. It can be added to the DAS to make an encrypted DAS, and it can be subtracted

from the encrypted DAS to rebuild the decrypted DAS. In this suggested method, the values of r, x, and L can be utilized as a component of the PK.

Digital Audio Signal (DAS) is a set of sample values arranged in a one or two-column matrix as shown in Fig. 4. The sample values are usually fractional in the range from −1 to +1. DAS can be represented by the signal plot, the matrix of samples, and the histogram, which points to the counts of sample values, as shown in Fig. 4.

During the encryption and decryption processes, the generated CLDS were applied, keeping the amplitude values within the allowable floating-point range to avoid clipping distortion and overflow.

B. Enhanced Features of the Proposed Method

The proposed method is described by multiple improved features. It is executed as a multiple-round system in which at least one round is needed, and the remaining rounds are independent of each other. A variable-length PK is utilized, where the key length is defined by the selected number of rounds. Because every round needs 136 bits from the PK, a four-round implementation requires a total key length of 544 bits. Moreover, data blocking is employed with a variable Block Size (BS), where the BS may change from 1 to the full size of the DAS. Through these functionalities, adaptability is supplied in adjusting the level of security, size of key-space, and the proposed cryptographic process computational efficiency.

The standard one-dimensional chaotic logistic map was selected due to its simple implementation, fast sequence-generation capability, and low computational complexity, which makes it suitable for real-time DAS encryption applications. In addition, the generated CLS length was selected according to the selected block size to improve sequence variability and reduce the impact of periodic behavior associated with one-dimensional chaotic systems.

C. Encryption and Decryption Procedures

The proposed PK is dynamically created according to the selected number of encryption rounds, under a certain bit allocation presented in Table I. In each round, the parameter set *r, x,* and Block Number Parameter (NB) is extracted from the PK as shown in Fig. 5, and it is used to initialize the one-dimensional chaotic logistic sequence; this sequence was used as noise to be added or subtracted from the DAS. Accordingly, the total PK length increases proportionally with the number of encryption rounds. For example, using four encryption rounds results in a total PK length of 544 bits (4×136), producing a key space of approximately 2^{544}.

```
r1=3.79,  x1=0.10
r2=3.64,  x2=0.18
r3=3.88,  x3=0.21
r4=3.59,  x4=0.15

NB1=100
NB2=120
NB3=130
NB4=140

E=1
```

Fig. 5. Example of the proposed PK parameter configuration.

TABLE I: PK BIT ALLOCATION

Parameter	Description	Bit Length
r	Logistic-map control parameter	64 bits
x	Initial condition parameter	64 bits
NB	Block number parameter	8 bits
Total	PK length per round	136 bits

The proposed method is based on a simple encryption-decryption procedure. The encryption-decryption function uses the DAS signal, block number NB, operation flag E, and the chaotic pair r and x as inputs, where $E = 1$ represents encryption and $E = -1$ represents decryption. Initially, the DAS is converted into a single-row vector and partitioned into blocks according to the selected block size. The CLMM is then utilized to generate the CLDS, which is added to or subtracted from the DAS depending on the selected operation. Finally, the DAS is reconstructed to its original dimensions.

Algorithm 1. DAS Encryption-Decryption Procedure

Input:
DAS signal, control parameter r, initial condition x, block number NB, operation flag E.

Output:
Processed DAS signal

1. Convert the DAS matrix into a single-row vector.
2. Determine the block size BS according to the selected value of NB.
3. Initialize the chaotic logistic map using r and x.
4. Generate the Chaotic Logistic Sequence (CLS) using the one-dimensional logistic equation.
5. Partition the DAS vector into NB blocks.
6. For each block:
   a. Generate the corresponding CLS values.
   b. Add the CLS to the DAS block if $E = 1$ (encryption).
   c. Subtract the CLS from the DAS block if $E = -1$ (decryption).
7. Reconstruct the processed DAS to its original dimensions.
8. Return the processed DAS signal.

IV. RESULTS

The proposed approach was implemented using multiple DASs, and it was observed that the distortion level of the encrypted DAS is increased as the number of rounds is increased, as shown in Fig. 6 and Fig. 7. Multiple DAS samples were chosen and processed to assess the suggested method. The encrypted signal quality parameters, which are the Mean Squared Error (MSE), Peak Signal-to-Noise Ratio (PSNR), and Correlation Coefficient (CC) values, were calculated for multiple rounds, and the obtained results are illustrated in Table II.

As shown in Table II, a similar general direction was produced for all verified DAS sizes. In every case, increasing the number of rounds produced higher MSE values and lower values of CC and PSNR. This confirms that the technique provides a uniform encryption impact for different DAS sizes, where a higher number of rounds leads to lower similarity and greater distortion between the source and encrypted signals.

As illustrated in Figs. 8–10, advancing the number of rounds leads to raising the level of distortion of the

encrypted DAS and decreases its similarity to the source DAS. This is proved by the increment of MSE and the reductions in PSNR and CC values when the number of rounds is varied from one to four. On the other hand, the decrypted DAS remains similar to the source DAS, as indicated by $\mathrm{MSE} = 0$, $\mathrm{CC} = 1$, and $\mathrm{PSNR} = \infty$. These results show that the method gives powerful encryption by increasing rounds while maintaining correct signal recovery after decryption.

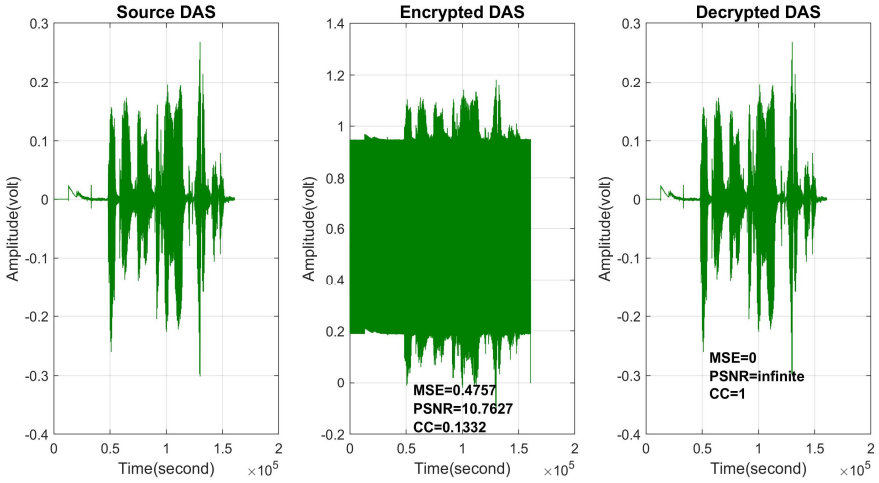

Fig. 6. Original, encrypted, and decrypted DAS signals obtained using one encryption round.

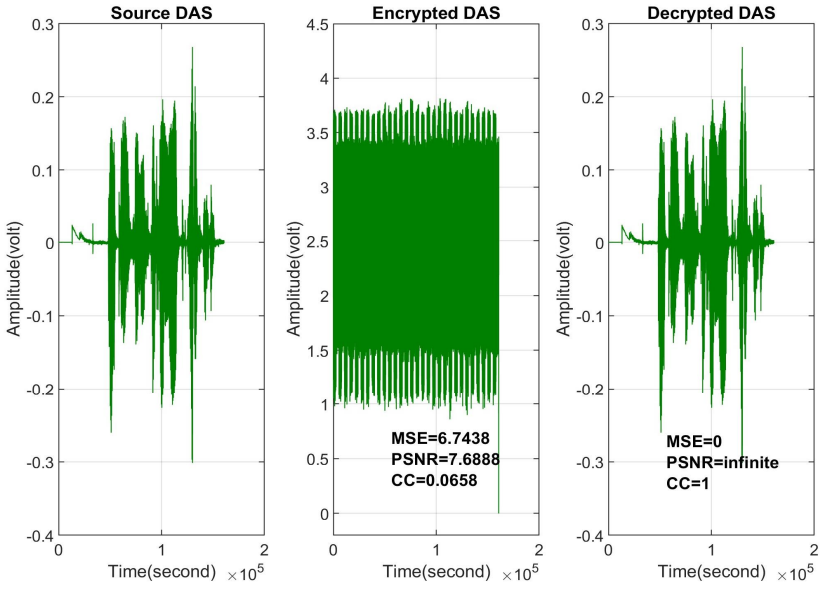

Fig. 7. Original, encrypted, and decrypted DAS signals obtained using four encryption rounds.

TABLE II: QUALITY METRICS OF THE ENCRYPTED DAS FOR DIFFERENT NUMBERS OF ENCRYPTION ROUNDS

DAS Size	**MSE**	**PSNR**	**CC**	**MSE**	**PSNR**	**CC**	**MSE**	**PSNR**	**CC**	**MSE**	**PSNR**	**CC**
(***K* Samples**)	Rounds=1			Rounds=2			Rounds=3			Rounds=4		
196	0.4750	10.8171	0.1028	1.7904	8.7450	0.0767	3.8134	8.5537	0.0555	6.7392	7.9020	0.0494
222	0.4751	10.7823	0.1119	1.7910	8.6184	0.0834	3.8041	8.6733	0.0609	6.7265	7.8671	0.0543
314	0.4757	10.7627	0.1332	1.7927	8.5670	0.0991	3.8164	8.1897	0.0739	6.7438	7.6888	0.0658
420	0.4760	11.2775	0.1287	1.7955	8.8290	0.0951	3.8230	8.7724	0.0702	6.8382	7.7923	0.0538
523.9004	0.4759	19.4275	0.5282	1.7949	14.0680	0.4187	3.8185	11.8832	0.3273	6.7470	10.3465	0.2947
Average	0.4755	12.6134	0.2010	1.7929	9.7655	0.1546	3.8151	9.2145	0.1176	6.7589	8.3193	0.1036

Particularly, when the number of rounds was incremented from 1 to 4, the MSE value increased from 0.4755 to 6.7589, as shown in Fig. 8. Simultaneously, the CC value decreased from 0.2010 to 0.103, as shown in Fig. 9, and the PSNR value decreased from 12.6134 to 8.3193, as illustrated in Fig. 10.

Figs. 8–10 show that, even though the encrypted DAS distortion level increased with increasing the number of rounds, the decryption process stayed accurate. This denotes that the method can improve the encryption strength via additional rounds while maintaining accurate recovery of the original DAS.

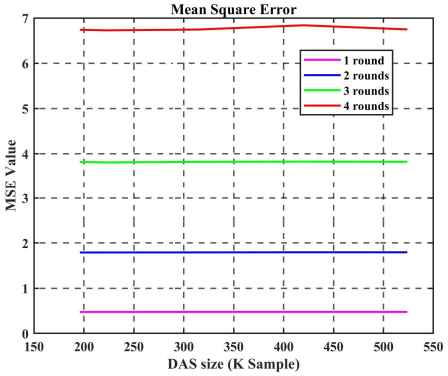

Fig. 8. Effect of the number of encryption rounds on the MSE values for different DAS sizes.

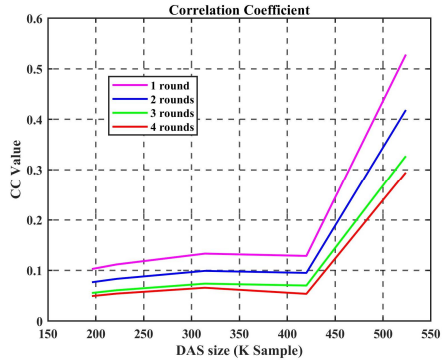

Fig. 9. Effect of the number of encryption rounds on the Correlation Coefficient (CC) for different DAS sizes.

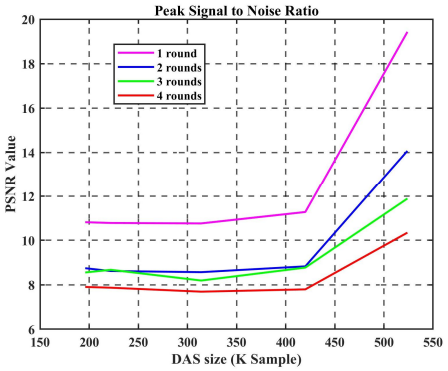

Fig. 10. Effect of the number of encryption rounds on the PSNR values for different DAS sizes.

The selected DASs were employed again, and the encryption-decryption time and speed were measured; the obtained speed results are shown in Table III:

As shown in Table III, increasing the number of rounds increased the encryption-decryption time; Nevertheless, the increment remained relatively small. For example, when the number of rounds increased from one to four, the encryption-decryption time increased from 0.0834 to 0.2766 seconds, as shown in Fig. 11.

In Fig. 12, the encryption-decryption speed declined as the number of rounds increased; however, it relatively stayed high. Particularly, when the number of rounds was incremented from one to four, the encryption-decryption speed decreased from 3.8499 M Samples/s to 1.1507 M Samples/s.

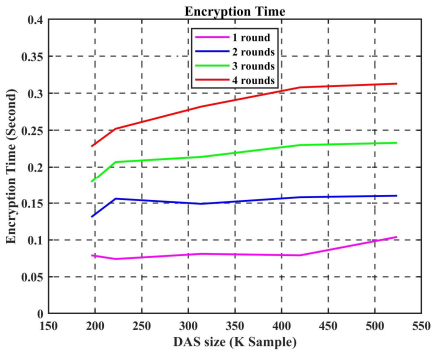

Fig. 11. Effect of the number of encryption rounds on the encryption time for different DAS sizes.

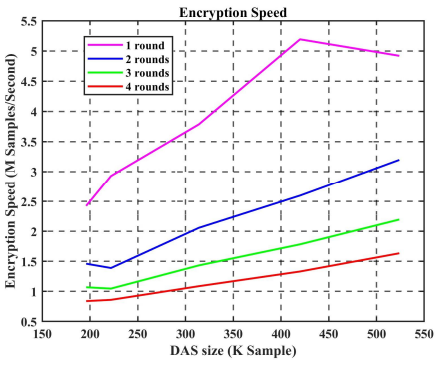

Fig. 12. Effect of the number of encryption rounds on the encryption speed for different DAS sizes.

TABLE III: ENCRYPTION TIME AND SPEED PERFORMANCE FOR DIFFERENT NUMBERS OF ENCRYPTION ROUNDS

DAS Size (*K* Samples)	Encryption Time (Second)	Encryption Speed (M Samples/ s)	Encryption Time (Second)	Encryption Speed (M Samples/ s)	Encryption Time (Second)	Encryption Speed (M Samples/ s)	Encryption Time (Second)	Encryption Speed (M Samples/ s)
	Rounds=1		Rounds=2		Rounds=3		Rounds=4	
196	0.0790	2.4229	0.1310	1.4611	0.1790	1.0693	0.2280	0.8395
222	0.0740	2.9297	0.1560	1.3897	0.2070	1.0473	0.2520	0.8603
314	0.0810	3.7857	0.1490	2.0580	0.2140	1.4329	0.2820	1.0874
420	0.0790	5.1919	0.1580	2.5959	0.2300	1.7833	0.3080	1.3317
523.9004	0.1040	4.9194	0.1600	3.1976	0.2330	2.1958	0.3130	1.6346
Average	0.0834	3.8499	0.1508	2.1405	0.2126	1.5057	0.2766	1.1507

An enhancement in the speed of DAS cryptography was attained by this method. When the performance of the proposed method using four rounds was compared with the existing chaotic and standard methods, the generated results illustrate that a substantial speedup was provided, as presented in Table IV.

TABLE IV: SPEED PERFORMANCE COMPARISON BETWEEN THE PROPOSED METHOD AND EXISTING ENCRYPTION METHODS

Encryption Method Category	Method	Speed (*K* Samples/s)	Proposed Method Speed Up
Classical Standard Methods	Proposed*	106.0864	1.0000
	DES	10.8	9.8228
	3DES	9.3	11.4071
	AES	11.3	9.3882
	RC2	7.7	13.7775
	RC6	19.4	5.4684
	BF	70	1.5155
Chaotic and Hybrid Methods	Proposed (using 1 round)	3942.3	1.0000
	Chaotic [6]	141.2305	27.9139
	Hyper chaotic [6]	636.3379	6.1953
	Introduced in [10]	888.8867	4.4351
	Introduced in [17]	911.0352	4.3273
	Introduced in [18]	638.4082	6.1752

*: Using 4 rounds

TABLE V: ENTROPY VALUES FOR ORIGINAL AND ENCRYPTED DAS

DAS	Entropy
Source DAS	4.9695
Encrypted DAS	7.0577

In addition to the previously obtained distortion and computational-efficiency results, several security analyses were performed to evaluate the robustness of the proposed DAS encryption method against statistical and differential attacks.

Using four encryption rounds produces a total PK length of 544 bits, resulting in a key space of approximately 2^{544}. Such a large key space significantly increases resistance against exhaustive brute-force attacks and improves the overall security strength of the proposed encryption method.

Information entropy analysis was performed to evaluate the randomness characteristics of the encrypted DAS compared with the source signal, as represented in Table V. The original DAS produced an entropy value of 4.9695, while the encrypted DAS achieved an entropy value of 7.0577. The higher entropy value of the encrypted DAS indicates improved randomness and reduced statistical predictability compared with the original DAS, which enhances resistance against statistical analysis attacks.

Histogram analysis was performed to evaluate the statistical distribution characteristics of the original, encrypted, and decrypted DAS signals.

The histogram of the original DAS exhibited a concentrated distribution due to the natural correlation between adjacent audio samples, as shown in Fig. 13. After encryption, the encrypted DAS demonstrated a significantly altered statistical distribution with improved randomness characteristics compared with the original DAS.

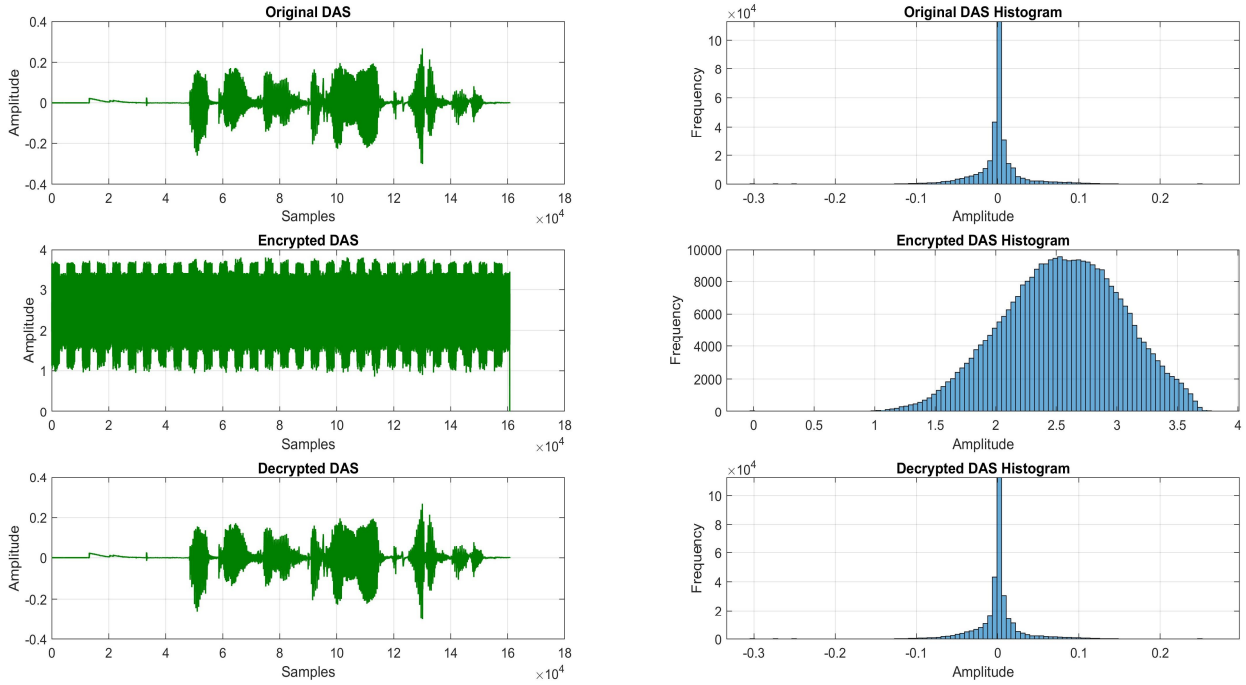

Fig. 13. Histogram analysis of original, encrypted, and decrypted DAS.

This clearly shows that the proposed encryption method effectively reduced the statistical correlation of the original DAS samples and increased the random behavior of the encrypted signal, which improves resistance against statistical analysis attacks. In addition, the decrypted DAS restored a histogram distribution similar to that of the

original DAS, confirming successful signal reconstruction after decryption.

NPCR and UACI analyses were performed to evaluate the resistance of the proposed DAS encryption method against differential attacks, and the results are shown in Table VI. These tests measure the sensitivity of the encrypted signal to small changes in the input data. Higher NPCR values and stable UACI values indicate stronger resistance against differential cryptanalysis.

TABLE VI: NPCR AND UACI RESULTS FOR DIFFERENT DAS SIZES

DAS size (*K* samples)	UACI	NPCR
196	31.7168	99.8461
222	32.1329	99.7212
314	31.4667	99.6018
420	31.5699	99.8422

The obtained NPCR values ranged from 99.6018% to 99.8461%, while the UACI values ranged from 31.4667% to 32.1329%. These results indicate that the proposed method provides high sensitivity to changes in the input DAS and demonstrates satisfactory resistance against differential attacks.

The proposed PK provides a large key space due to the utilization of multiple encryption rounds and variable-length PK construction.

A high sensitivity to the chosen PK is shown by the proposed method. The decryption section must employ the same PK that was employed during encryption. Any variation in the PK during decryption leads to the production of a damaged decrypted DAS, showing robust key sensitivity. To evaluate this property, a DAS was selected and then encrypted utilizing the PK shown in Fig. 14, after which decryption was executed using multiple key values.

r1=3.79, x1=0.10
r2=3.64, x2=0.18
r3=3.88, x3=0.21
r4=3.59, x4=0.15

NB1=100
NB2=120
NB3=130
NB4=140

Fig. 14. Example of the PK parameters used for DAS encryption.

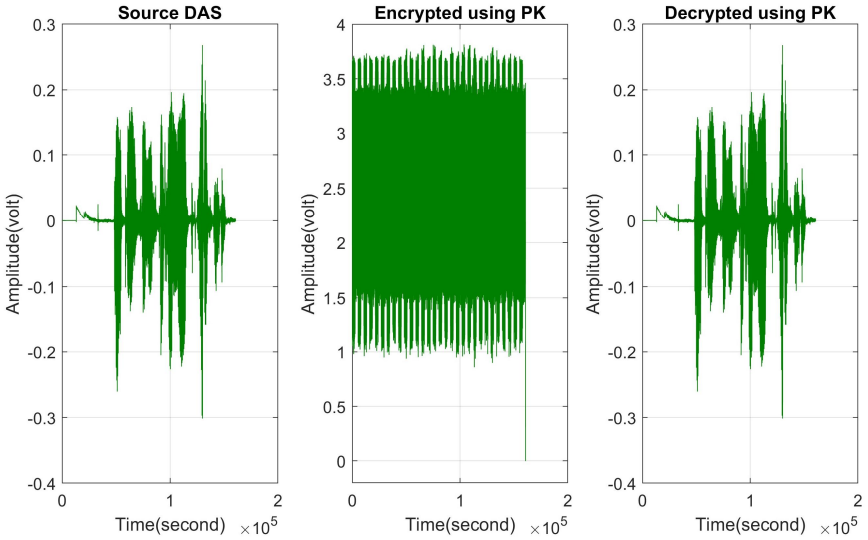

Fig. 15. Original, encrypted, and correctly decrypted DAS signals using the proposed PK parameters.

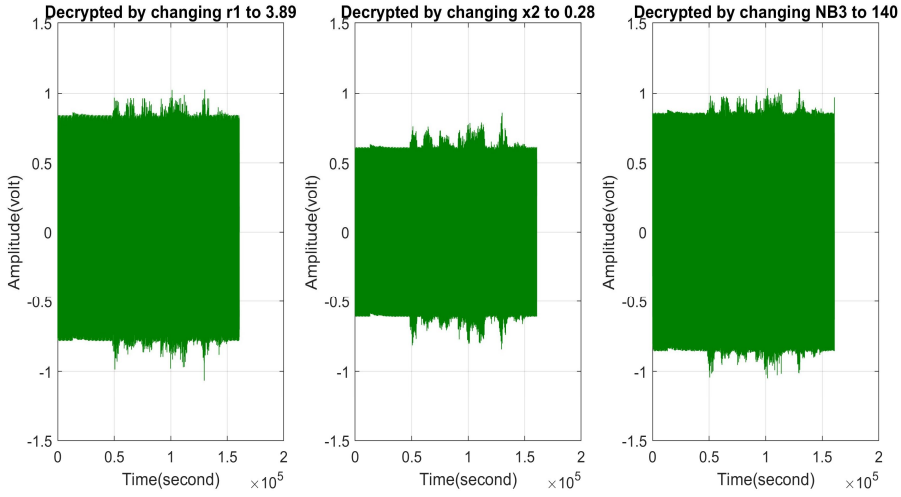

Fig. 16. Decrypted DAS signals obtained using modified PK parameters, demonstrating the sensitivity of the proposed method to PK variations.

As shown in Fig. 15 and Fig. 16, modifying the PK parameters during decryption produced incorrectly reconstructed DAS signals, confirming the high sensitivity of the proposed method to PK variations.

Moreover, Fig. 16 displays that minor adjustments in the PK parameters yield a severely distorted decrypted DAS. This verifies the high key sensitivity of this method and denotes that the right decryption can only be realized when an accurate PK is utilized.

V. Conclusion

A multiple variable number of rounds round-based cryptographic method for DASs was submitted. The method was implemented using one to four independent encryption rounds; every round was executed via a simple encryption-decryption function without requiring data-conversion functions. A chaotic sequence was executed using a simple logistic map model and was added to or subtracted from the source or encrypted DAS to accomplish encryption and decryption. The results obtained showed that increasing the number of rounds from 1 to 4 increases the distortion level of the encrypted DAS, while increasing the MSE from 0.4755 to 6.7589, and the PSNR and CC values decreased from 12.6134 to 8.3193 and from 0.2010 to 0.1036, respectively. Moreover, a variable-length PK was utilized, and its length increased with the number of rounds, attaining 544 bits when four rounds were utilized. This key length supplied a large key space, which is effective against brute-force and unauthorized access attacks. The method also used variable-size data blocking, where the BS was contained in the PK. Although the proposed method has proved satisfactory security and computational efficiency, increasing the number of encryption rounds may increase the overall processing time. The future of DAS encryption is moving toward AI-assisted methods, lightweight cryptographic techniques for IoT applications, and chaos-based security combined with steganography. Current research efforts focus on achieving a balance between strong security, low computational latency, and preservation of audio-signal quality in noisy real-world communication environments. The obtained results demonstrate that the proposed method provides a practical trade-off between computational efficiency and cryptographic security for modern DAS applications.

Conflict of Interest

The authors declare no conflict of interest.

Author Contributions

Sara Al-Omari designed the idea of this study, implemented the method, carried out the experiments, obtained the results, and wrote the manuscript. Zayed Huneiti contributed to the assessment of the idea, revised the manuscript step by step, and presented major comments that improved the discussion and presentation of the results. Ahmed Abu-Khadrah reviewed the methodology and programming code, provided the manuscript structure specifications, advised on the preparation of each section, and contributed to the overall manuscript organization. All authors reviewed the manuscript, provided comments, and approved the final version.

Acknowledgment

The authors wish to thank the Faculty of Engineering Technology at Al-Balqa Applied University.

References

[1] D. Das, S. Roy, K. Gupta, and B. Sahoo, "Performance evaluation of symmetric encryption algorithms using MCDM methods," in *Proc. 2022 IEEE 2nd International Symposium on Sustainable Energy, Signal Processing and Cyber Security (iSSSC)*, 2022. doi: 10.1109/isssc56467.2022.10051594

[2] W. Dai, X. Xu, X. Song, and G. Li, "Audio encryption algorithm based on chen memristor chaotic system," *Symmetry*, vol. 14, no. 1, 17, 2022. doi: 10.3390/sym14010017

[3] A. Taqi and S. M. Hameed, "A secure audio encryption method using tent-controlled permutation and logistic map-based key generation," *Computers, Materials & Continua*, vol. 85, no. 1, pp. 1653–1674, 2025. doi: 10.32604/cmc.2025.067524

[4] A. K. Raghunath, D. Bharadwaj, M. Prabhuram, and A. D, "Designing a secured audio-based key generator for cryptographic symmetric key algorithms," *Computer Science and Information Technologies*, vol. 2, no. 2, pp. 87–94, 2021.

[5] S. A. Gebereselassie, S. Sahoo, A. Tiwari, R. Nathasarma, and B. K. Roy, "A secured audio encryption algorithm based on Gauss and Henon chaotic maps," in *Proc. 2023 Int. Conf. on Computer, Electronics & Electrical Engineering & their Applications (IC2E3)*, 2023. doi: 10.1109/IC2E357697.2023.10262456

[6] Z. Hua, Y. Zhou, and H. Huang, "Cosine-transform-based chaotic system for image encryption," *Information Sciences*, vol. 480, pp. 403–419, 2019. doi: 10.1016/j.ins.2018.12.048

[7] E. A. Albahrani, "A new audio encryption algorithm based on chaotic block cipher," in *Proc. 2017 Annual Conference on New Trends in Information & Communications Technology Applications (NTICT)*, 2017, pp. 22–27. doi: 10.1109/NTICT.2017.7976129

[8] S. Reddy, D. N. Achar, M. S. Mol, and N. Panda, "Audio encryption using AES and cellular automata," in *Proc. 2024 15th International Conference on Computing Communication and Networking Technologies*, 2024. doi: 10.1109/icccnt61001.2024.10724851

[9] M. Demirtas, "A sound encryption method based on feature extraction and a novel chaotic map," in *Proc. 2024 10th International Conference on Computer Technology Applications (ICCTA)*, 2024, pp. 303–309. doi: 10.1145/3674558.3674602

[10] M. Asgari-Chenaghlu, M.-A. Balafar, and M.-R. Feizi-Derakhshi, "A novel image encryption algorithm based on polynomial combination of chaotic maps and dynamic function generation," *Signal Processing*, vol. 157, pp. 1–13, 2019. doi: 10.1016/j.sigpro.2018.11.010

[11] A. Shumran and A.-B. A. Al-Hussein, "Study of chaotic-based audio encryption algorithms: A review," *Iraqi Journal for Electrical and Electronic Engineering*, vol. 20, no. 2, pp. 85–103, 2024. doi: 10.37917/ijeee.20.2.8

[12] E. A. Albahrani, T. K. Alshekly, and S. H. Lafta, "A review on audio encryption algorithms using chaos maps-based techniques," *Journal of Cyber Security and Mobility*, vol. 11, no. 1, pp. 53–82, 2021. doi: 10.13052/jcsm2245-1439.1113

[13] T. Haridas, M. S. Krishnan, and S. S. Muni *et al*., "Chaos-based audio encryption: Efficacy of 2D and 3D hyperchaotic systems," *Franklin Open*, vol. 8, 100158, 2024. doi: 10.1016/j.fraope.2024.100158

[14] X. Wang and Y. Su, "An audio encryption algorithm based on DNA coding and chaotic system," *IEEE Access*, vol. 8, pp. 9260–9270, 2020. doi: 10.1109/access.2019.2963329

[15] A. Shumran and A.-B. A. Al-Hussein, "Chameleon chaotic system-based audio encryption algorithm and FPGA implementation," *Iraqi Journal for Electrical and Electronic Engineering*, vol. 21, no. 1, pp. 232–250, 2025. doi: 10.37917/ijeee.21.1.23

[16] J. Ayad, N. Qaddoori, and H. Maytham, "Enhanced audio encryption scheme: Integrating Blowfish, HMAC-SHA256, and

MD5 for secure communication," *Mesopotamian Journal of CyberSecurity*, vol. 5, no. 1, pp. 178–186, 2025.
[17] X. Zhang and X. Wang, "Multiple-image encryption algorithm based on DNA encoding and chaotic system," *Multimedia Tools and Applications*, vol. 78, no. 6, pp. 7841–7869, 2018.
[18] Z. Tang, J. Song, X. Zhang, and R. Sun, "Multiple-image encryption with bit-plane decomposition and chaotic maps," *Optics and Lasers in Engineering*, vol. 80, pp. 1–11, 2016. doi: 10.1016/j.optlaseng.2015.12.004
[19] M. E. Smid, "Development of the advanced encryption standard," *Journal of Research of the National Institute of Standards and Technology*, vol. 126, 2021. doi: 10.6028/jres.126.024
[20] A. K. Jawad, G. Karimi, and M. Radmelkshahi, "A novel digital audio encryption algorithm using three hyperchaotic rabinovich system generators," *ARO: The Scientific Journal of Koya University*, vol. 12, no. 2, pp. 234–245, 2024.
[21] S. Mokhnache, M. E. H. Daachi, T. Bekkouche, and N. Diffellah, "A combined chaotic system for speech encryption," *Engineering, Technology & Applied Science Research*, vol. 12, no. 3, pp. 8578–8583, 2022. doi: 10.48084/etasr.4912
[22] H. A. Abdallah and S. Meshoul, "A multilayered audio signal encryption approach for secure voice communication," *Electronics*, vol. 12, no. 1, art. no. 2, 2022.
[23] M. Helmy and H. Torkey, "Secured audio framework based on chaotic-steganography algorithm for internet of things systems," *Computers*, vol. 14, no. 6, 207, 2025.
[24] M. Roy, S. Chakraborty, and K. Mali, "Audio encryption framework based on chaotic map and DNA encoding," *Applied Acoustics*, vol. 224, 110152, 2024.
[25] N. M. Abd Ali and T. Z. Ismaeel, "Audio encryption using chaotic systems with direct byte-level processing," *Journal of Engineering*, vol. 32, no. 4, pp. 106–122, 2026.
[26] A. Shumran, A.-B. A. Al-Hussein, and others, "FPGA implementation of a secure audio encryption system based on chameleon chaotic algorithm," *Dynamics*, vol. 6, no. 1, 2026. doi: 10.3390/dynamics6010009
[27] Md. I. Islam, S. N. Khandakar, N. A. Ritu, Md. M. Bhuiyan, and S. Jahan, "Audio encryption and decryption under elliptic curve cryptography and DNA algorithm," *Journal of Communications Software and Systems*, vol. 22, no. 1, pp. 49–60, 2026.

Sara Al-Omari was born in Jordan in 1992. She received her B.Sc. and M.Sc. degrees in electrical engineering from the Jordan University of Science and Technology in Jordan in 2015 and 2019, respectively. She is currently a lecturer in the Department of Electrical Engineering at the College of Engineering Technology, Al-Balqa Applied University, Amman, Jordan. Before starting her academic career, she worked for five years in industrial control schematic design, one year as a research assistant, and one year as a teaching assistant at the Jordan University of Science and Technology. Her research interests include power systems, communication systems, cryptography, and signal security.

Zayed Huneiti is an associate professor of electrical engineering at the College of Engineering Technology, Al-Balqa Applied University, Amman, Jordan. He received his B.Sc., M.Sc., and PhD degrees in electrical and electronics engineering from the United Kingdom. Before his academic career, he spent seven years in the British electronics industry. Since joining academia in 1991, Dr Huneiti has held senior academic positions at several universities in the United Kingdom and the Middle East. His work encompasses teaching at both undergraduate and postgraduate levels, alongside active engagement in research and graduate supervision. Dr Huneiti's research spans multiple areas within electrical engineering, and he has authored or co-authored more than 90 technical publications. He has supervised numerous B.Sc., M.Sc., and PhD students and served on PhD and M.Sc. examining committees in both Jordan and the United Kingdom. He also regularly serves as a reviewer for leading international journals and conferences.

Ahmed Abu-Khadrah was born in the United Arab Emirates in 1981. He received a bachelor of engineering in computer engineering from Al-Balqa Applied University in 2003. He received a master's degree in electronic engineering (computer engineering) from Universiti Teknikal Malaysia Melaka (UTeM) in 2013, and a PhD in computer engineering and communications from UTeM in 2017. He is currently an assistant professor in the Department of Electrical Engineering at the College of Engineering Technology, Al-Balqa Applied University, Amman. His research interests include wireless network protocols, networking and communications, wireless mathematical models, network security, optimization algorithms, machine learning, and multimedia services over networks.