Hindawi
Mathematical Problems in Engineering
Volume 2021, Article ID 5554707, 15 pages
https://doi.org/10.1155/2021/5554707

Research Article

A Noise-Tolerant Audio Encryption Framework Designed by the Application of S_8 Symmetric Group and Chaotic Systems

Haris Aziz,[1,2] **Syed Mushhad Mustuzhar Gilani**,[1] **Iqtadar Hussain**,[3] **Abdul Kashif Janjua**,[2] **and Shahzada Khurram**[4]

[1]*University Institute of Information Technology, Pir Mehr Ali Shah Arid Agriculture University, Rawalpindi, Pakistan*
[2]*U.S.-Pakistan Center for Advanced Studies in Energy (USPCAS-E), National University of Sciences and Technology (NUST), H-12, Islamabad 44000, Pakistan*
[3]*Department of Mathematics, Statistics and Physics, Qatar University, Doha 2713, Qatar*
[4]*Department of Information Security, The Islamia University of Bahawalpur, Bahawalpur, Pakistan*

Correspondence should be addressed to Syed Mushhad Mustuzhar Gilani; mushhad@uaar.edu.pk

Received 18 February 2021; Revised 24 March 2021; Accepted 31 March 2021; Published 14 April 2021

Academic Editor: Taha Aziz

The recent decade has witnessed an exponential surge of digital content, especially multimedia and its applications. The security requirements of these innovative platforms necessitate the significance of enhancing advanced encryption schemes. In this paper, a novel encryption scheme is presented for real-time audio applications. The framework of the proposed scheme is grounded on the principles of confusion and diffusion. The confusion incorporates nonlinearity by the application of Mordell elliptic curves (MEC) and a symmetric group of permutations S_8. The endurance of the proposed scheme is further enriched through the application of chaotic maps. The proposed scheme is intended to cater requirements of real-time voice communications in defense applications particularly warzones. The adoption of a modular design and fusion of chaotic maps makes the algorithm viable for numerous real-time audio applications. The security can further be enriched by incorporating additional rounds and number of S-boxes in the algorithm. The security and resistance of the algorithm against various attacks are gaged through performance evaluation and security measurements. The audio encryption scheme has the ability to tolerate noise triggered by a channel or induced by an invader. The decryption was successful and the resultant output was audible for noisy data. The overall results depict that the proposed audio encryption scheme contains an excellent cryptographic forte with the minimum computational load. These characteristics allow the algorithm to be a hotspot for modern robust applications.

1. Introduction

The recent decade has witnessed an unprecedented growth of multimedia and its applications. Multimedia data are the majority of data exchanged on modern open communication systems. Therefore, multimedia systems are highly prone to attacks and face significant security challenges. Keeping in view, its deemed necessary to develop secure, fast, and stable security frameworks to ensure confidentiality, privacy, and authentication of multimedia applications. Encryption is a fundamental tool to achieve security and researchers across the world are acquainted with modern and innovative assaults for the security of these platforms. The ability to cope with the security requirements of these modern multimedia platforms is an eminent research domain [1]. The audio data applications hold utmost importance and prevalence in multimedia systems [2, 3]. Digital audio communications are witnessing a tremendous surge and prominence in various areas, such as military, telephone banking, education, and confidential voice conferencing. The laps in audio data security will significantly impact the security and resiliency of those applications. The audio signals in contrast to images possess a large size and strong correlation among data samples and further involve real-time processing. Moreover, modern audio or voice applications also require low power consumption and less

computation time. Despite cryptographic forte, the conventional encryption algorithms like AES [4], DES [5], and RSA [6] are not feasible with the latest low-profile audio applications due to high computational complexity. Therefore, the development of audio encryption algorithms with low power consumption, high presence for real-time systems, and fast multimedia processing is a significant area in the current research arena [7–13].

Shannon [14] presents an idea of substitution permutation network (SPN) that becomes the forefront of all modern cryptosystems. SPN is considered a key design element to yield resilient and secure symmetric encryption algorithms [15]. This elementary concept is grounded on two key principles, that is, confusion and diffusion. These key parameters eliminate local correlation among adjacent data samples and alter them by substituting pseudorandom values. The confusion is attained through the application of a sole nonlinear component called substitution box or S-box. It is like a nucleus for topnotch symmetric cryptosystems and their endurance counts on the strength of deployed S-boxes. This work does not demand to review the extensive literature on S-box's algebraic properties but readers can be referred to [16–18] for understanding. Numerous frameworks are rendered to seed novel and resilient S-boxes such as algebraic structures, chaos theory, analytical methods, the theory of automata, and control mapping. In modern applications, elliptic curve (EC) cryptography is in the limelight due to its resilience and acts as the backbone of blockchain applications. Recently, Hayat et al. [19, 20] devised a framework using EC to yields 8×8 S-boxes. The cryptosystems based on ECs are robust and secure in comparison to conventional schemes. Considering the importance of Mordell elliptic curves (MEC) on a finite field, MEC along withS8 symmetric group is employed to synthesize a collection of S-boxes. In this work, an SPN-based audio encryption scheme is proposed and a cryptographically potent S-box is designed and deployed to ensure the resiliency of the algorithm.

In recent years, the discipline of nonlinear dynamical systems particularly chaos has hailed substantial advancements. The chaotic solutions possess unique peculiarities including hypersensitive dependence, ergodicity, and pseudorandomness, which adds extensive unpredictability in deterministic nonlinear systems. The predominant applications of chaos are multimedia encryption applications. Chaotic maps were extensively deployed in various image encryption schemes [21–28]. In particular, chaos-oriented audio encryption algorithms are in limelight due to excellent cryptographic attributes. These algorithms handle redundant and bulky audio files and lead to a high level of security. Roy and Misra [29] employed an audio encryption scheme using chaotic Hénon map and lifting wavelet transforms. The lifting wavelet is used to transform audio signal to data signal and then encrypted via the chaotic map. The transformation adds additional processing overhead and makes it hard to comment on its employment in low-profile applications. Liu et al. [30] offered a cryptosystem through the application of a multiscroll chaotic to generate confusion and diffusion in audio data. Kordov [31] deployed an SPN structure with chaotic maps to design an audio encryption algorithm. Recently, Shah et al. [32] proposed another audio encryption scheme by the application of SPN. The algorithm attained confusion through Mobius transformation and diffusion via chaotic Hénon map. Abdelfatah [33] proposed a novel audio encryption scheme through the combination of four methods self-adaptive scrambling, multiple chaotic maps, cipher feedback, and DNA encoding. The proposed scheme tends to enhance keyspace and provide strength against brute force attacks. Naskar et al. [34] presented a novel audio encryption technique that adopts block ciphering via DNA encoding and logistic chaotic map. The channel shuffling is further introduced to secure against cryptanalysis. To cater to demands of real-time low-profile audio applications in constricted environments. Peng et al. [35] proposed an ultra-lightweight secure architecture for underwater acoustic networks. The algorithm is based on chaotic maps and Feistel structure to cater to demands of low bandwidth with limited overhead. Adeel et al. [36] introduced a novel lightweight chaotic encryption algorithm for next-generation audio-visual hearing equipment. Nagakrishan and Revathi [37] offered a speech authentication system by the applications of chaotic maps and DNA.

Lightweight ciphers have the drawback that they are prone to channel noise. Therefore, the researchers have focused on developing noise-tolerant ciphers for multimedia applications. The noise-tolerant ciphers on the other hand possess processing load and inadequate for systems that require constrained computing power. Recently, chaos has been employed in several noise-tolerant image encryption schemes. Ahmad et al. [38] utilized properties of orthogonal matrices and proposed a chaotic image encryption scheme with the ability to handle channel noise. Elashry [39] proposed another noise-tolerant image encryption design through baker chaotic using three modes of operation. In another method, Patro et al. [40] implemented a noise-resistant image encryption algorithm utilizing hyperchaos with DNA shuffling. There are no substantial and comprehensive implementations of chaos targeting noise tolerance in audio applications. Hussein et al. [41] employed double chaotic masking on the audio signal to increase keyspace and achieve higher security. The immunity technique is further implanted to reduce the effect of noise. However, a thorough security review is lacking to ascertain the resilience of the algorithm against attacks. Michel-Macarty et al. [42] proposed a multiuser communication scheme for applications related to telemedicine. The scheme utilizes a chaotic Hénon map with code division multiple access (CDMA) technique to ensure privacy and shows robustness against noise. Sheela et al. [43] came with a new audio encryption algorithm based on chaotic maps and DNA encoding. The algorithm offers reasonable security and achieves a prominent signal-to-noise ratio (SNR). In [44] through 5G and IoT, chaos drove secure real-time next-generation audio-video hearing aid framework is proposed. The system has the potential for the acquisition of high-quality speech restoration in noisy environments.

The aforementioned survey of current literature depicts that no major study is available for current real-time low-profile audio applications with the ability to handle noise,

especially to address the security concerns related to military voice communications in warzones. Moreover, the chaos-based audio encryption schemes largely lack cryptanalysis and inadequate security evaluations were performed to verify the stability of these cryptosystems against attacks. In this paper, an SPN-based structure is proposed by the application of three secure chaotic maps to develop an audio encryption application. The proposed scheme is explicitly intended to protect military communications focused on security. Detailed evaluations of the cryptosystem demonstrate the endurance of the system.

There are a number of integral outcomes achieved through this work. A highly nonlinear S-box is designed and yielded through the application of MEC on a finite field and symmetric group of permutations S_8. Moreover, a real-time secure chaotic audio encryption scheme is presented through the SPN paradigm for modern communication platforms particularly targeting military communications. The scheme employs chaotic maps along with proposed S-boxes, permutation, and cyclic shift operation. The proposed audio encryption scheme is resistant to noise induced in audio signals either through channel disturbance or deliberately by an eavesdropper. The strength of the scheme is evaluated against noise through experiments and the result yields a promising output. The eminent performance of the proposed scheme is depicted through the execution of series of analyses and equating them with modern renowned schemes.

2. Problem Statement

In the modern era, the electronic revolution and communication technologies witnessed a staggering rise in multimedia systems. Particularly, secure transmission and multimedia processing is a challenging research area to convey with the requirements of modern innovative applications. Therefore, multimedia data security poses significant concerns and confronts various forms of attacks. The audio data signals constitute a crucial role and prominence in multimedia systems. Digital audio communications are critical for military and defense and their security is of prime significance. Modern forms of warfare revolve around military communications. To ensure that all aspects of command and control (C2) are successfully shared, military forces require a broad spectrum of real-time voice communications capability. Secure voice messaging with high availability is the lifeline on the battlefield and border areas. The main threats to voice or audio communications in a military environment are eavesdropping, impersonation, and illegal access to the medium. Therefore, the encryption of audio is highly desirable and critical from a security perspective. Unlike images and text, the encryption of audio requires a unique transformation of maps and strong security. The adjacent audio data samples possess a strong correlation and slow time varying and is substantially large.

Eavesdropping is not the only problem encountered during audio messaging in the military environment. The enemies intentionally add noise to corrupt encrypted audio signals. In cases, the whole channel is chocked with noise to deprive the opposition of the means to communicate, whereas conventional radio military apparatus also induces noise over communication channels. Due to the intrinsic nature of these audio applications, conventional encryption schemes such as DES, AES, and RSA are not appropriate for achieving the desired results. These traditional encryption schemes are also not resistant to noise through the channel and or added deliberately by opponents. The advanced warfare communication technologies drive through the competition between electronic countermeasures (ECM) and electronic counter-countermeasures (ECCM) [45]. Frequency hopping is a modern and promising technique employed by the military, where the transmitter rapidly switches the carrier wave frequency [45]. The frequency hopping is used in line with digital encryption to make the communication secure and reliable. At the same time, the frequency hopping inherently adds noise to the transmission. Considering the ECM and ECCM, developing a robust noise-resistant audio encryption algorithm with low computational complexity is a challenge, especially in battlegrounds, where secure real-time point-to-point audio messaging is of prime significance. These technological mandates, security concerns, integration, and interoperability requirements provide a catalyst to develop next-generation secure encryption algorithms.

2.1. Chaotic Maps for Proposed Cryptosystem. This section briefly presents chaotic maps deployed for our proposed audio encryption scheme. Three different maps, that is, Chebyshev, Tangent Delay Ellipse Reflecting Cavity Map System (TD-ERCS), and circle chaotic maps, are deployed for our proposed encryption scheme, while engaging three distinct chaotic maps escalates the randomness of the proposed scheme and has a larger keyspace than a single chaotic system.

It is well known that Chebyshev polynomial exhibits chaotic behavior and is significantly deployed in secure communication. In [46], a modified version of Chebyshev chaotic map was employed to encrypt thermal images and achieved promising output. Proposed scheme implements modified Chebyshev chaotic map and is mathematically expressed as

$$x(i+1) = \mathrm{mod}\left(\mathrm{floor}\left(x(i) \times 1000 \times n\right)\right)256 + 1. \quad (1)$$

Here, n is an integer and x has a range $[-1\ 1]$.

TD-ERCS chaotic map yields two chaotic sequences and is represented in the following equation [47]:

$$\begin{cases} x_n = -\dfrac{2k_{n-1}y_{n-1} + x_{n-1}\left(\mu^2 - k_{n-1}^2\right)}{\mu^2 + k_{n-1}^2}, \\ k_n = \dfrac{2k_{n-m}^{'} - k_{n-1} + k_{n-1}k_{n-m}^{'2}}{1 + 2k_{n-1}k_{n-m}^{'} - k_{n-m}^{'2}} \end{cases} \quad (2)$$

where

$$k_n' = \frac{x_n}{x_n}\mu^2, \tag{3}$$

$$y_n = k_{n-1}\left(x_n - x_{n-1}\right) + y_{n-1}, \tag{4}$$

$$k_{n-m} = \begin{cases} \dfrac{x_{n-1}}{y_{n-1}}\,\mu^2, & \text{if } n < m, \\ \dfrac{x_{n-m}}{y_{n-m}}\mu^2, & \text{if } n \geq m, \end{cases} \tag{5}$$

where (μ, x_0, φ, m) represents initial parameters with $x_0 \in [-1\ 1]$, $\tan\varphi \in (-\infty, \infty)$, $\mu \in (0.05, 1)$, and $m = 2, 3, \ldots, n$; now,

$$y_0 = \mu\sqrt{1 - x_0^2}, \tag{6}$$

$$k_0' = \frac{x_0}{y_0}\mu^2, \tag{7}$$

$$k_0 = \frac{\tan\,\varphi + k_0'}{1 - k_0'\,\tan\,\varphi}. \tag{8}$$

The third map employed in the proposed scheme is a one-dimensional circle chaotic map. Circle map shows good chaotic behavior when applied to any data and its mathematical form is given as

$$x_{n+1} = \mathrm{mod}\left(x_n + \Omega - \frac{k}{2\Pi}\,2\Pi\,(x_n), 1\right), \tag{9}$$

where $x_n = 0.4$, $\Omega = 0.5$, $x_n + 1$ is computed as mod 1, and k is constant.

The chaotic ranges of all three maps are thoroughly examined and only those ranges are considered where maps show chaotic behavior. The chaotic sequences are then selected from the application of these three chaotic maps. The initial values of those sequences will serve as an encryption key in the proposed cryptographic scheme.

2.2. S_8 MEC S-Box. In recent years, EC cryptography has been widely adopted to develop powerful and exceptionally secure cryptosystems. The key offerings of these elliptical curve cryptosystems are their efficiency and tolerance against modern cryptanalysis. Ullah et al. [48] proposed a pseudorandom number generator (PRNG) through the application of ordered MEC to seed distinct and mutually uncorrelated S-boxes. Now, the S-boxes are further employed as a seed to yield new S_8 MEC S-boxes. Hussain et al. [49] devised an approach to yield highly nonlinear S-boxes through the action of the symmetric group S_8. The design structure of this algorithm relies upon symmetric group S_8 that is the permutations group of order 40328. These permutations are incorporated in the algebraic structure of the resultant S-boxes. In this paper, we engage the action of S_8 symmetric group on the MEC S-box to construct a collection of 40320 unique S_8 MEC S-boxes of identical strength and features. The sample 8×8 S-box is depicted in Figure 1.

The cryptosystem designed by applying a single S-box lacks adequate stability and reliability to address the security requirements of modern applications. In particular, multimedia applications such as audio files possess highly correlated data. Therefore, the cryptosystems designed through the applications of multiple S-boxes are more resilient and achieve high confusion and diffusion. The collection of multiple S_8 MEC S-boxes is extremely pertinent to the scenario of the current target application and improves the security of the proposed scheme. The scenario is explained in Figure 2 where 8 identical pixel values are transformed through single as well as with 8 different S-boxes. The figure reveals that transformation with one S-box has no effect on correlation though multiple S-box transformations that give unique values and enhanced correlation. The transformation effect via multiple S-boxes will optimize the cryptosystem and achieve desired security using fewer rounds.

3. Proposed Audio Encryption Algorithm

It is evident through results that S_8 permutation will totally alter the values and yield unique S-boxes after application. The algebraic characteristics acquired by new S-boxes are identical to the parent S-box and play a significant to establish a resilient cryptosystem. In this section, the architecture of the proposed audio encryption scheme is presented. The scheme is based on the SPN framework and contains three main steps cyclic shift, substitution, and permutation repeated for a set of four rounds. The overall idea is depicted in Figure 3 where an audio file of size M is served as an input to the encryption scheme. The audio input is divided into samples with digital values. The values in the original audio were in the range [−1 1]. To make input coherent with the proposed scheme, a preprocessing step was taken first. A positive shift of 128 was applied and further rescaled 128 times, resulting in a sequence of values between 0 and 256. The sequence was further separated into a range of length 65535 and then translated into a matrix of size 256×256. Each element of the matrix has a range [0 256] and can be addressed in 8 bits. The element of the matrix is represented as $A\ (u, v, m)$ or simply $A\ (u, v)$ where u and v represent row and column and m denotes the frame number. The schemes comprise three steps and each step takes unique keys as input.

The first chaotic sequence utilized in the proposed scheme is derived from Chebyshev chaotic map denoted as x. Moreover, x_o and P are the preliminary chaotic values acquired from its range. These preliminary values are considered as the initial two encryption keys for the proposed scheme; that is, $x_o = k_1$ and $P = k_2$. The length of this Chebyshev chaotic sequence is $(d * e * f)$ with an initial range that lies within [−1 1]. In order to employ the proposed scheme, the range of chaotic sequence is amplified by multiplying with 100 and then applying modulo 8 to restrict value within 255. The value $A(u, v)$ is now converted into an 8-bit binary denoted as $A_b(u,v)$. The left cyclic shift operation of x_q bits is further performed and cyclic shifted value is termed as $A_c(u,v)$, where $x = 1,2,3, \ldots..\mathrm{d}\ ^*\ \mathrm{e}\ ^*\ \mathrm{f}$. This cyclic shift is understood with the help of an example; that is, suppose $A_b(u,v) = 11011001$ and $x_q = 3$; then $A_c(u,v) = 10111001$.

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	98	201	74	194	234	164	106	3	139	134	195	58	226	122	116	81
1	184	133	186	51	67	37	177	157	11	76	1	230	44	200	55	47
2	245	166	38	114	244	31	151	93	42	242	192	19	53	35	87	246
3	209	176	0	160	80	212	13	64	211	218	173	130	22	243	136	146
4	5	170	10	59	82	180	236	102	69	217	57	158	119	202	8	228
5	153	147	112	15	2	7	138	85	23	156	128	89	101	190	50	68
6	70	4	168	117	16	78	137	113	111	237	174	77	155	88	46	107
7	71	90	18	135	250	181	34	120	94	235	49	79	249	95	54	124
8	27	73	251	240	145	167	179	221	110	152	63	62	193	222	140	41
9	96	208	24	198	220	159	36	183	109	118	255	131	144	227	219	65
10	189	48	252	60	103	105	163	154	17	197	215	26	248	254	28	100
11	30	223	40	182	121	142	196	175	104	12	149	191	29	84	9	32
12	33	83	127	91	241	205	247	108	20	148	72	161	185	99	6	39
13	233	199	43	129	187	125	75	224	188	132	56	239	210	232	45	162
14	97	52	141	238	21	61	123	115	143	207	14	126	25	213	171	231
15	165	178	216	203	92	66	204	225	206	150	214	229	86	169	253	172

Figure 1: S_8 MEC S-box for proposed cryptosystem.

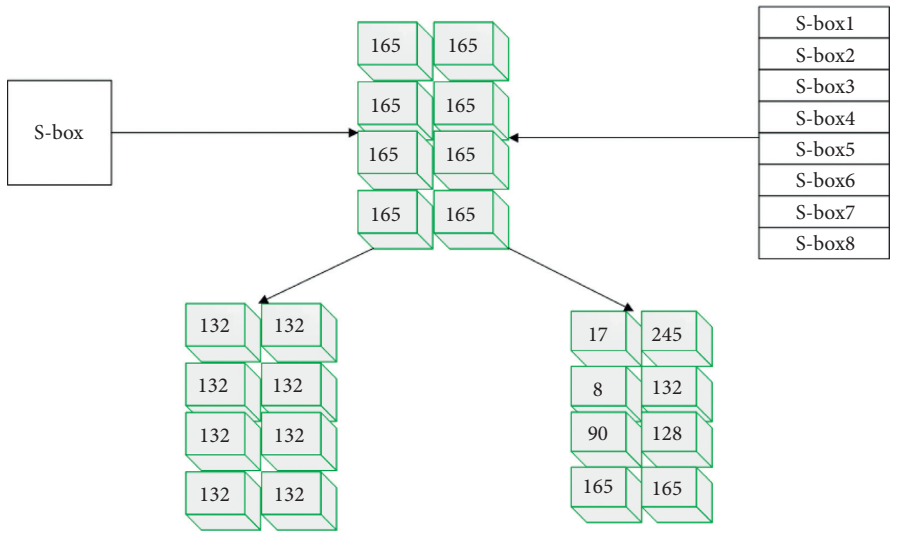

Figure 2: Transformation effect through S-box.

Consider that TD-ERCS chaotic map and two chaotic sequences o and t are considered with initial values as x_0, tan φ, μ, and n. The next secret keys k_3, k_4, k_5, and k_6 are considered from these initial chaotic values. The chaotic sequence o is further considered as the algorithm requires only one chaotic sequence. The o has range [1, max (d,e)] and max(d,e) is the length of o. Here, [−1 1] is the preliminary range of chaotic sequence and stretched to [0, 2] and amplified by multiplying sequence with 100 * max (d,e) and also limiting in range [1, max(m,n)]. Vector o only has unique values from 1 to max (m, n). The cyclic shifted value $A_c(i,j)$ is concurrently altered to decimal and denoted as $A_d(u,v)$. The diffusion operation is done through the permutation of rows and columns of $A_d(u, v)$ and permuted value is denoted as A_p. Suppose (23, 56, 12) are initial values of chaotic sequence o; then, the first three rows of A_d will be positioned at (23, 56, 12) rows of A_p. The permuted value A_p is acquired by row and column permutation on A_d.

$$\begin{cases} A_p(:, o(u)) = A_d(:, u), \ \forall u \in d, \\ A_p(y(u), :) = A_{p_1}(v, :), \ \forall v \in e. \end{cases} \tag{10}$$

The circle map is the third chaotic map deployed in the proposed scheme. Consider chaotic sequence t derived from

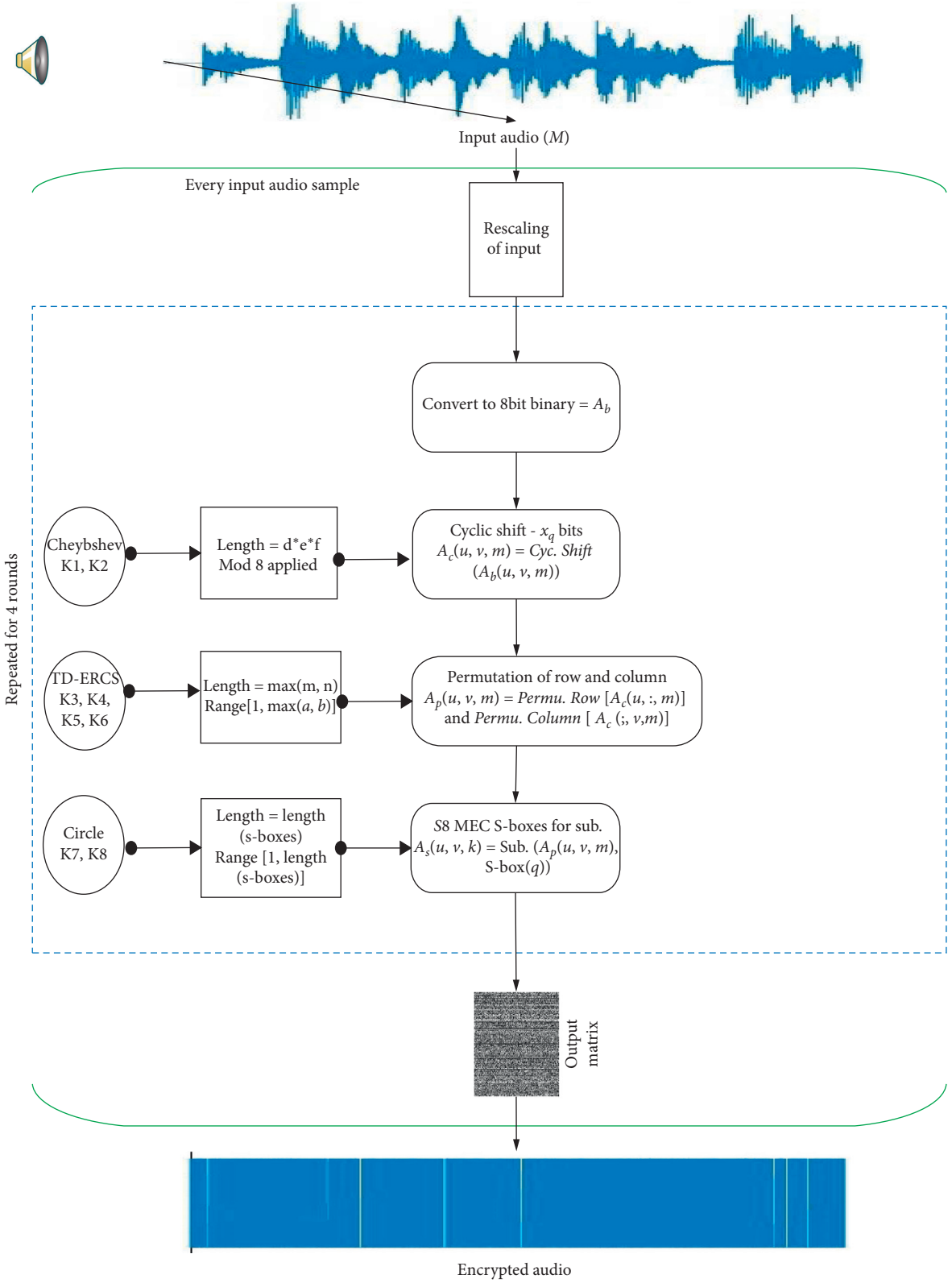

Figure 3: Flow diagram of proposed audio encryption scheme with unique keys.

circle chaotic map with x_0 and Ω as its initial conditions. The final two secret keys k_7 and k_8 are the initial value of these two chaotic maps. Chaotic sequence t has a length $d^* e^* f$ with modulo η, where η is the overall S-boxes deployed in the proposed scheme. Following on similar lines, range [0 1] of the chaotic sequence t is amplified with $100^* \eta$ and then

limiting within modulo η.boxes yielded through the application of a symmetric group of permutation S_8 is denoted as S_p. A large collection of S-boxes is constituted via the proposed S-box construction methodology. However, the number of S-boxes engaged in the proposed algorithm will purely rely on application and computational resources. The proposed algorithm is intended for military audio communications, so 256 unique S-boxes are employed in the proposed approach. To meet the security requirements of low-profile applications, total number of active S-boxes can be reduced to 128. However, incorporating additional S-boxes enhances the computational complexity of the system. During the third step of the proposed scheme, substitution is done on A_p with one of the S-boxes.

$$A_s(u,v) = s\text{box}\left(A_p(u,v),\, S_{t(q)}\right), \quad \forall u \in d, \forall v \in e,\, \forall q \in (1,2,\ldots d*e*f). \tag{11}$$

To enhance the resiliency of the proposed scheme, no active S-boxes can be chosen through the chaotic sequence t. The results obtained through this substitution are denoted as A_s. The above steps are now repeated in a cycle of four rounds till a subsequent encrypted matrix is acquired. The size of the resultant encrypted matrix is identical to the original input and is further rescaled in the range [−1, 1] to obtain an encrypted audio file.

Now, in order to decrypt the audio signal via the proposed scheme, the steps must be followed in reverse order as shown in Figure 3. In the case of decryption, the encrypted matrix of size $d*e*f$ is fed to the algorithm as input, whereas the same set of keys are used for decryption and operations of substitution, permutation, and cyclic shift are performed inversely.

In the first step, inverse S-box is used to substitute encrypted matrix C. Inverse substitution on matrix C is given as

$$A_{\text{is}}(u,v) = \text{inv\_}s\text{box}\left(C(u,v),\, S_{t(q)}\right), \quad \forall u \in d,\, \forall v \in e,\, \forall q \in (1,2,\ldots d*e*f). \tag{12}$$

The inverse of the S-box, that is, Inv-S_8 MEC S-box, takes two parameters and performs inverse substitution. Similarly, an inverse permutation is applied on permuted matrix A_{i8} with reference to chaotic sequence o. TD-ERCS map generates chaotic sequence r and matrix A_{ip} is obtained by the action of inverse permutation.

$$\begin{cases} A_{\text{up1}}(:,u) = A_{u8}(:, y(u)), & \forall u \in d, \\ A_{\text{up}}(v,:) = A_{\text{up}_1}(y(u),:), & \forall v \in e. \end{cases} \tag{13}$$

Finally, during the last step, values A_{ip} are transformed from decimal to 8-bit binary denoted as $A_{ip}(i,j)$. In this case, a right cyclic shift of x_q bits is executed with an outcome denoted as $A_{ic}(i,j)$, where $q = 1, 2, \ldots, a * b * c$ and x is chaotic sequence obtained from Chebyshev chaotic map having identical initial values. The same steps are followed for all four rounds to get the final input matrix. The matrix is again rescaled and transformed into an original audio file denoted as D.

4. Results and Discussion

In order to perform simulation analyses, an "audio1.wav" is nourished as a carrier input to the proposed scheme. The secret keys deployed in the algorithm are generated via chaotic maps and outlined in Table 1. Figures 4(a) and 4(b) represent the original audio file and its histogram before encryption. The audio sample 1 is fed as input to the proposed scheme and Figures 4(c) and 4(d) represent the output encrypted matrix and its histogram. Finally, Figure 4(e) reveals the encrypted audio file using the intended scheme and results show that outcomes are remarkably strong as compared with the original input.

This can also be visually elaborated through waveform plotting of original and encrypted audio files. The resiliency of the proposed scheme is further verified using "audio2.wav" as shown in Figure 5. The input and decrypted output audio are mapped together in Figure 5(d) and identical output proves that audio is recovered successfully. The outcomes divulge that the encrypted scheme is resilient and alters output in few rounds. The results are also substantiated from the outcomes of the next section.

4.1. Cryptographic Security and Performance Analysis. These analyses gage the resiliency, performance, and strength of our audio encryption scheme. Security and performance analysis is not appropriately performed on audio encryption schemes presented in recent literature. Therefore, it is extremely difficult to evaluate and comment on the practical applications of these algorithms. The statistical analysis is also presented in this section to sort the working mechanism and determine the strength of the proposed scheme. These analyses are executed and a comparison of results is done with the current state-of-the-art literature. This analysis aids superior performance of the proposed scheme.

4.1.1. Correlation. This analysis is a statistical metric to determine the strength of an encryption scheme. Correlation is tremendously beneficial for multimedia applications and

Table 1: Encryption keys of the proposed algorithm yielded by the application of chaotic maps.

Parameters						
Chaotic maps	x_0	$\tan \varphi$	μ	N	Ω	P
Chebyshev chaotic map	0.5					3.5
TD-ERCS chaotic map	0.5	1	0.4	50		
Circle chaotic map	0.4				0.5	

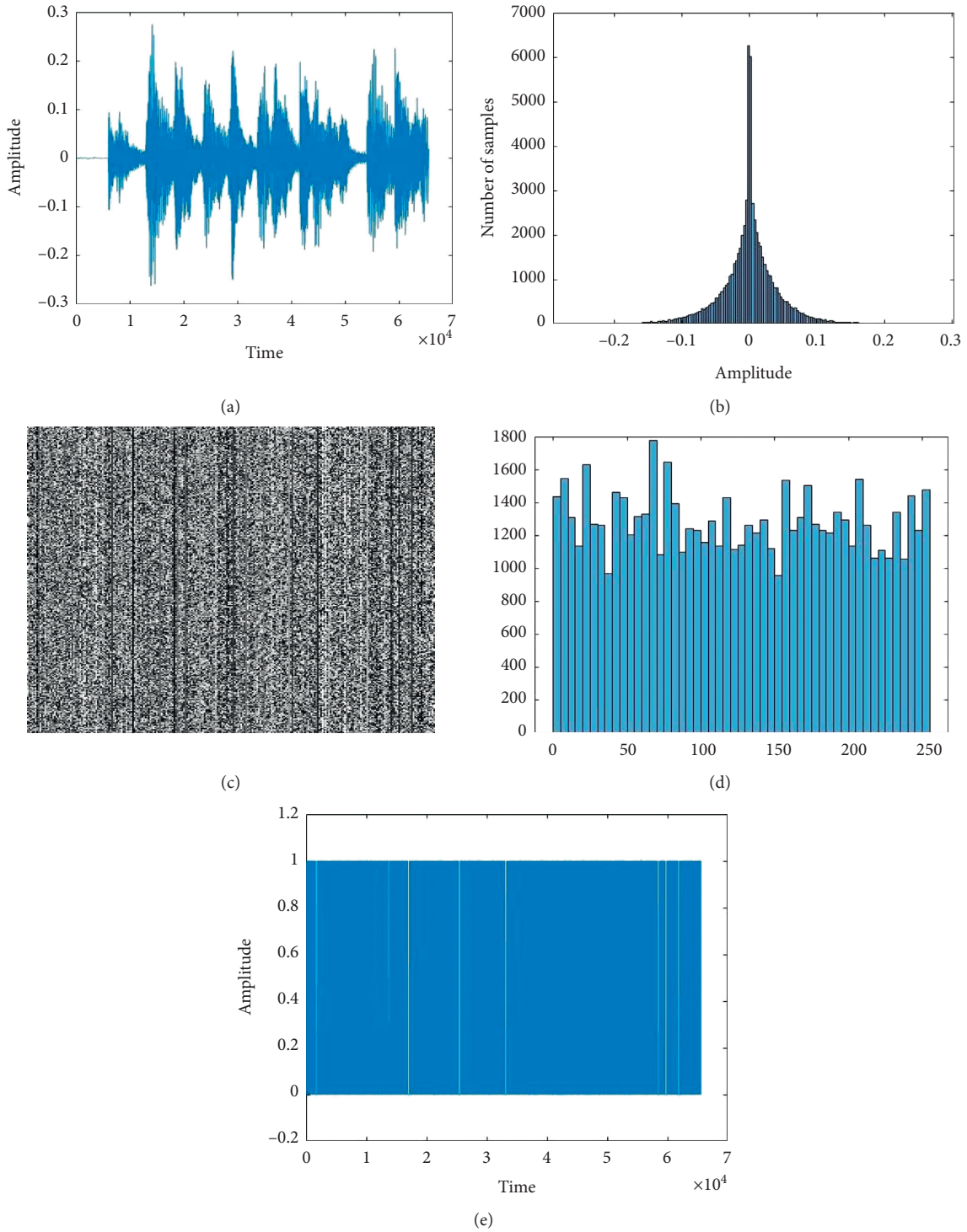

Figure 4: Results of encryption scheme with histograms on audio1.wav.

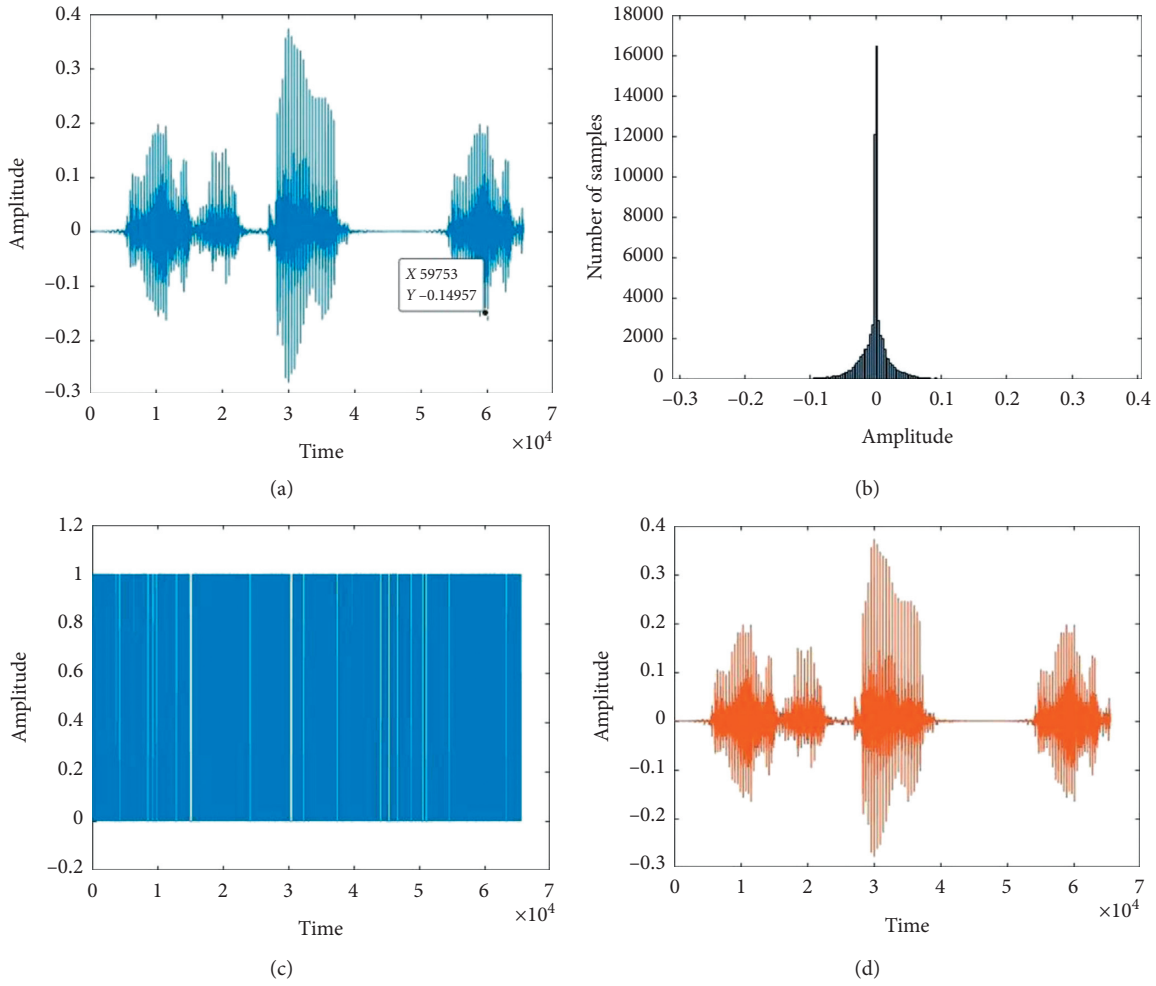

Figure 5: Results of simulation for the proposed scheme on audio2.wav.

audio; this analysis is done in the horizontal direction. Correlation computes the mutual relationship between identical segments in original and encryption audio samples. A resilient cryptosystem alters audio samples into a random noise signal with a low correlation coefficient. The equation presents the correlation coefficient:

$$\mathrm{Corr}_{ij} = \frac{\mathrm{Cov}(i,j)}{\sigma_i \sigma_j} = \frac{(1/N_s)\sum_{x=1}^{N_s}(i_x - E(i))\left(j_y - E(j)\right)}{\sqrt{(1/N_s)\sum_{x=1}^{N_s}(i_x - E(i))2}\sqrt{(1/N_s)\sum_{x=1}^{N_s}(j_x - E(j))2}}. \tag{14}$$

Here, N_s represent the total number of samples and i_x and j_x are sample values of encrypted audio. $E(i)$, $E(j)$, σ_i, and σ_j represent the mean and standard deviation of an original and encrypted audio file. Cov(i,j) is the covariance among both files. The analysis ascertains perfect result as shown in Table 2, and correlation coefficient values are edging towards zero.This means no similarity exist among two files and shows randomness of the encrypted sample.

4.1.2. Entropy. It is a metric to evaluate the degree of uncertainty in encrypted audio data. The entropy analysis determines the randomness as shown in Table 3 and its higher value depicts randomness.

4.1.3. Contrast. The contrast level determines dissimilarity in the audio signals. It is a metric to verify the effectiveness of encryption and determines that encryption creates required diffusion.

$$\mathrm{Contrast} = \sum_{i,j} |i-j|^2 P(i,j), \tag{15}$$

where i and j represent the position of a specific element of audio data. P(i, j) indicates the order of the cooccurrence matrix.

4.1.4. Homogeneity. The audio data are usually distributed depending on the nature of the audio file. To gauge

Table 2: Comparison of correlation analysis with related work.

Reference [32]	Reference [34]	Reference [33]	Reference [50]	Reference [51]	Proposed (Audio 1)	Proposed (Audio 1)	Proposed (Audio 3)
0.0038	0.00108	0.0052	0.0119	0.0021	0.0031	−0.0164	−0.0067

Table 3: Evaluation of statistical analysis and comparison on encrypted audio files.

Statistical analysis	Reference [32]	Proposed scheme (Audio 1)	Proposed scheme (Audio 2)	Proposed scheme (Audio 3)
Entropy	7.9974	7.9471	7.9473	7.9371
Contrast	10.463	10.5931	10.4042	10.6186
Energy	0.0156	0.0158	0.0156	0.0157
Homogeneity	0.3896	0.3878	0.3887	0.3890

characteristics of distribution, homogeneity analysis is applied to measure the spread of components in gray-level cooccurrence matrix (GLCM). Mathematically, it is expressed as

$$\text{Homogeneity} = \sum_{i,j} \frac{P(i,j)}{1+|i-j|}, \tag{16}$$

where i and j represent the position of a specific element of audio data. $P(i,j)$ indicates the order of the cooccurrence matrix.

4.1.5. Energy.

$$\text{Energy} = \sum_{i,j} P(i,j)^2, \tag{17}$$

where i and j represent positions of a particular element of audio data.

This analysis computes the energy and determines the sum of squared elements of gray values in GLCM. It is mathematically given as

All these four analyses are performed on an audio encryption scheme using different data samples and compared with relevant approaches as given in Table 3. The outcomes point towards the substantial performance of the algorithm.

4.1.6. Keyspace Analysis. The keyspace represents all possible values that can be deployed as a secret key in the encryption algorithm. The proposed algorithm incorporates three chaotic maps to yield eight secret keys derived from their initial values. Their ranges are considerably large to resist brute force attacks. Assume the average range of keys is 10^{10} and for all the eight secret keys, there are about 10^{80} possible keys. It is almost equivalent to 256 binary bits. A modern computer would require around 10^{15} years to check the keyspace of this size.

4.1.7. Key Sensitivity Analysis. Keyspace on its own is not sufficient to ensure stability, and a resilient cryptosystem should therefore have to attain key sensitivity. Key sensitivity is related to the decryption and a tiny change in key-value results in failure of decryption and yields different output. In this scheme, the input audio is encrypted via secret keys presented in Table 1. Three separate scenarios are considered in order to illustrate the key sensitivity of the proposed scheme. Firstly, we alter $k_1 = q_0 = 0.5$ to $k_1' = q_0 = 0.500000001$ and the remaining keys remain the same. In Figure 6(a), the difference with blue color represents decrypted audio and red color shows the original file. Now, for the second case, key k_5 is changed from $k_5 = \mu = 0.4$ to $k_5' = \mu = 0.4000000001$ and similarly $k_8 = \Omega$ to $k_8' = \Omega = 0.500000001$. The decrypted audio outputs are represented in Figures 6(b) and 6(c). It is clear that decryption of audio is failed with only a slight change in the encryption key and the algorithm shows formidable results.

4.1.8. Number of Sample Change Rates (NSCR) and Unified Average Changing Intensity (UACI) Analysis. NSCR and UACI are robustness tests for investigating the performance of the encryption scheme. NSCR and UACI are mathematically represented as

$$\text{NSCR} = \frac{\sum_{i=1}^{N} D_i}{N} \times 100\%, \tag{18}$$

$$\text{UACI} = \frac{1}{N_s}\left[\frac{\sum_i x_i - x_i'}{255}\right] \times 100\%, \tag{19}$$

where x_i and x_i' are the representation of encrypted audio samples at *ith* position. N_s is the length of the audio segment. D_i can be defined as

$$D_i = \begin{cases} 1, & x_i \neq x_i', \\ 0, & \text{otherwise.} \end{cases} \tag{20}$$

Table 4 shows the result of NSCR and UACI and comparisons have been done with modern schemes that depicted excellent performance and better resistance against differential attacks.

4.1.9. Encryption Quality. These metrics are applied to estimate the performance of the audio encryption framework. The analyses performed are mean square error (MSE), peak signal-to-noise ratio (PSNR), and structural similarity index (SSIM). The MSE measures the similarity between the original and the encryption file. SSIM gages the difference between the two audio samples. PSNR is a measure of the ratio between the original and encrypted audio file and

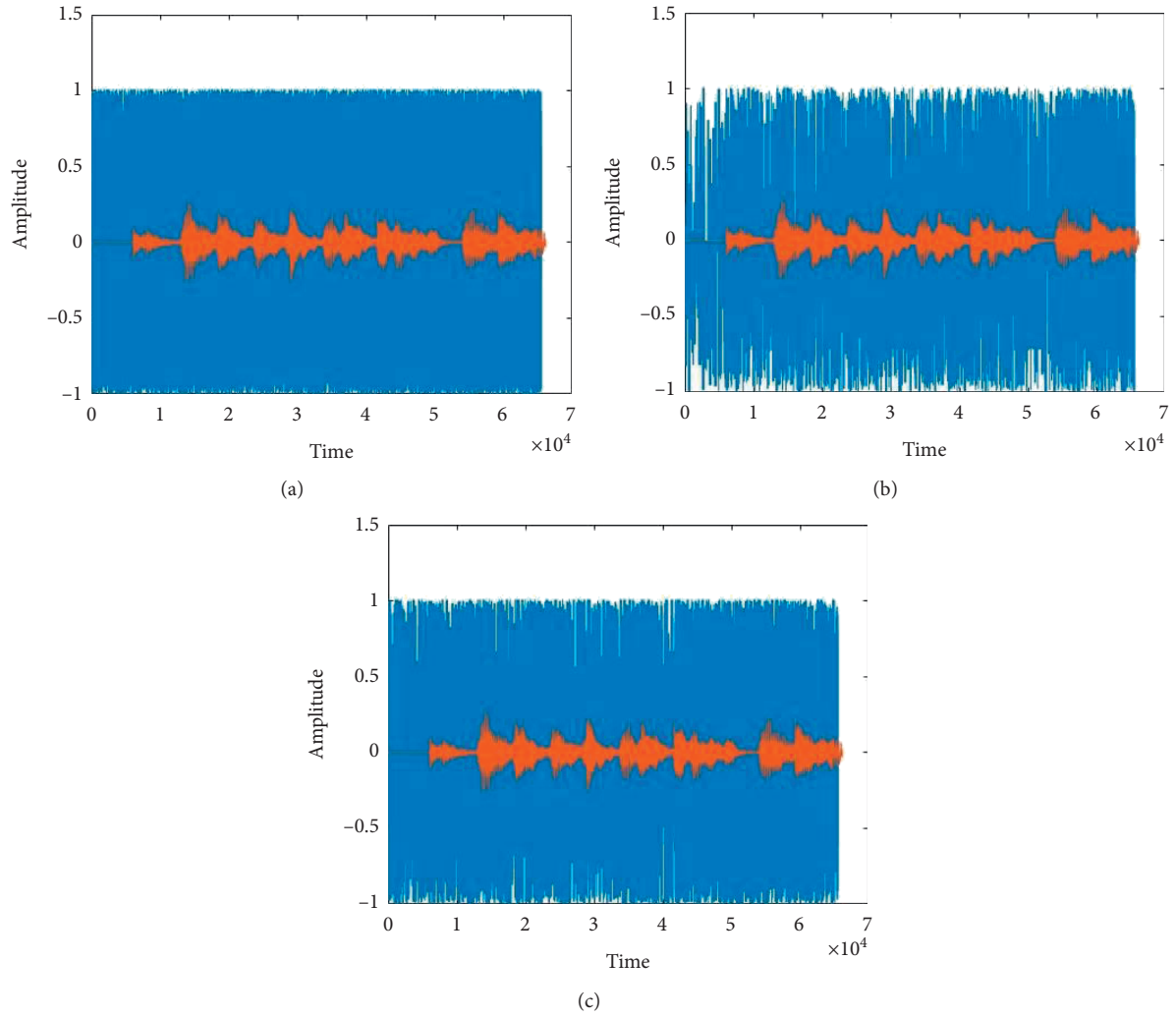

Figure 6: Analysis of key sensitivity having slight modification in encryption key on Audio 1.

Table 4: Comparison of NSCR and UACI with recent approaches.

Analysis	Reference [32]	Reference [33]	Reference [51]	Proposed (Audio 1)	Proposed (Audio 2)	Proposed (Audio 3)
NPCR (%)	99.9979	99.97	99.9961	99.5316	99.5987	99.6201
UACI (%)	25.5092	35.52	33.1858	25.7984	25.1824	25.7742

determines the power of a clean signal in contrast to the power of noise. These are calculated as

$$\text{MSE} = \frac{1}{N}\sum_{i=1}^{N}(x_i - y_i)^2, \tag{21}$$

$$\text{PSNR} = 20\log_{10}\left(\frac{255}{\sqrt{\text{MSE}}}\right), \tag{22}$$

where N is total samples and x_i and y_i are sample values of plain and encrypted audio.

$$\text{SSIM} = \frac{(2\overline{AC} + B_1)(2\sigma_{AC} + B_2)}{(A^2 + C^2 + B_1)(\sigma_A^2 + \sigma_C^2 + B_2)}, \sigma_C. \tag{23}$$

Here, $\overline{A}, \overline{C}$ is the mean and σ_A and σ_C are the standard deviation. Further, σ_{AC} indicates cross correlation, $B_1 = (K_1Q)^2$, and $B_2 = (K_2Q)^2$, where Q is dynamic range and $K_1 = 0.02$ *and* $K_2 = 0.03$. It is apparent from the results as shown via Table 5 that the proposed scheme coheres excellent encryption effect.

4.1.10. Crest Factor (CF) and Root Mean Square (RMS) Analysis. CF is a metric that determines the ratio of the peak value and its effectiveness in a waveform. If its value is zero, this means no peak and a higher value means a higher peak. RMS is calculated via the average amplitude level of an audio signal. These are mathematically expressed as

Table 5: Outcomes of encryption quality metrics and comparison with recent approaches.

Analysis	Proposed (Audio 1)	Proposed (Audio 2)	Proposed (Audio 3)	Reference [50]	Reference [52]	Reference [37]	Reference [33]
PSNR	10.7163	10.8230	10.6707	59.7989	48.0219	6.1235	4.426
MSE	37.4487	37.3420	37.4943	—	—	—	—
SSIM	0.0002917	0.00048188	−0.0016	—	—	—	—

$$\mathrm{CF} = 20 \log 10 = \frac{|V_{\mathrm{Peak}}|}{V_{\mathrm{RMS}}}, \tag{24}$$

$$\mathrm{RMS} = \sqrt{\frac{1}{N}\sum_{i=1}^{N}|A_i^2|}. \tag{25}$$

With reference to results obtained from Table 6, no statistical relation was found among original and audio files.

4.1.11. Spectrogram Analysis. A spectrogram is a two-dimensional illustration of an audio signal. The third dimension is represented with different colors and can be obtained via Fourier transform. The colors indicate the loudness of a specific frequency at a certain time. Figure 7 represents the spectrogram of original and encrypted audio files. It is clearly evident from results that encrypted audios are uniform and no similarities exist between original and encrypted audio files.

4.1.12. Computational Time. Modern encryption schemes necessitate low computational requirements to synchronize with modern real-time audio applications. The robust design and SPN framework ensure superior performance of the encryption scheme. One elementary reason is four encryption rounds to attain desired security in contrast to other schemes that require a minimum of 12 rounds.

4.1.13. Noise-Resistant Analysis. The forefront characteristic of the proposed audio encryption scheme is its ability to withstand noise. It is a proven fact that audio or voice conversations possibly suffer the effect of channel noise. The noise is purposely added by an unauthorized user or as a result of channel disturbance. All foremost encryptions schemes are inherently designed in such a way that slight modifications in cipher data fail successful decryption. Error detection and error correction measures are taken into account to address these issues but at the cost of additional computational load, whereas the real-time low-profile audio applications demand swift processing in contrast to security. Currently, no major approach is available to cater noise resistance in audio encryption applications.

The proposed audio scheme successfully decrypts the noisy cipher audio. Several experiments have been conducted by adding noise to a large number of audio files. The audio files of varying sizes, formats, and frequencies are fed to the proposed scheme. "Salt and pepper" noise of density 0.1, 0.2, and so on is further induced in cipher audio. It is evident through experimental results that decrypted files are audible and proves noise tolerance of the proposed encryption scheme. The outcomes depict that the proposed scheme addresses our target problem of military warfare communication with high effectiveness.

5. Cryptanalysis

Linear and differential cryptanalysis are the major approaches to determine the strength of the cryptosystem. The proposed audio encryption scheme is secure against both attacks. The linear approximation probability $LProb_{max} = 2^{-4.21}$ tests the imbalance of an event. The proposed approach employs 256 S-boxes in four rounds of the encryption scheme. Therefore, $LinearProb._{max}^{4r} = 2^{-4.21 \times 256} = 2^{-1077..76}$ and shows that differentiating a random permutation for cryptanalyst is highly challenging. Similarly, the differential probability is $DifferentialProb._{max}^{4r} = 2^{-4.05 \times 256} = 2^{-1036.8}$ and S-boxes have a uniform mapping and audio encryption is resistant to differential cryptanalysis. The proposed scheme should also avoid several other attacks model of cryptanalysis. The most prominent of these are cipher-text only and known-plaintext and chosen-plaintext attacks. The proposed audio encryption algorithm has an exceptional confusion and diffusion framework. Moreover, the results of key sensitivity, keyspace, and other security analyses make algorithms prone to these attacks.

The security and strength of the proposed audio encryption scheme are evaluated through a variety of security and performance metrics. The outcomes are further equated with the recent state-of-the-art approaches and yield exemplary performance. The results indicate that the audio encryption scheme is resilient and feasible for real-time applications. The performance metrics prove that the scheme has moderate computational requirements and noise-resistant characteristics. The robust design and inherent characteristics of the scheme make it practically feasible to use it in modern military communications. The proposed scheme as a whole tends to

Table 6: Results of CF and RMS.

Analysis	Proposed (Audio 1)	Proposed (Audio 2)	Proposed (Audio 3)
CF	49.3 dB	49.2313 dB	49.4125 dB
RMS	0.0034277	0.0034549	0.0033836

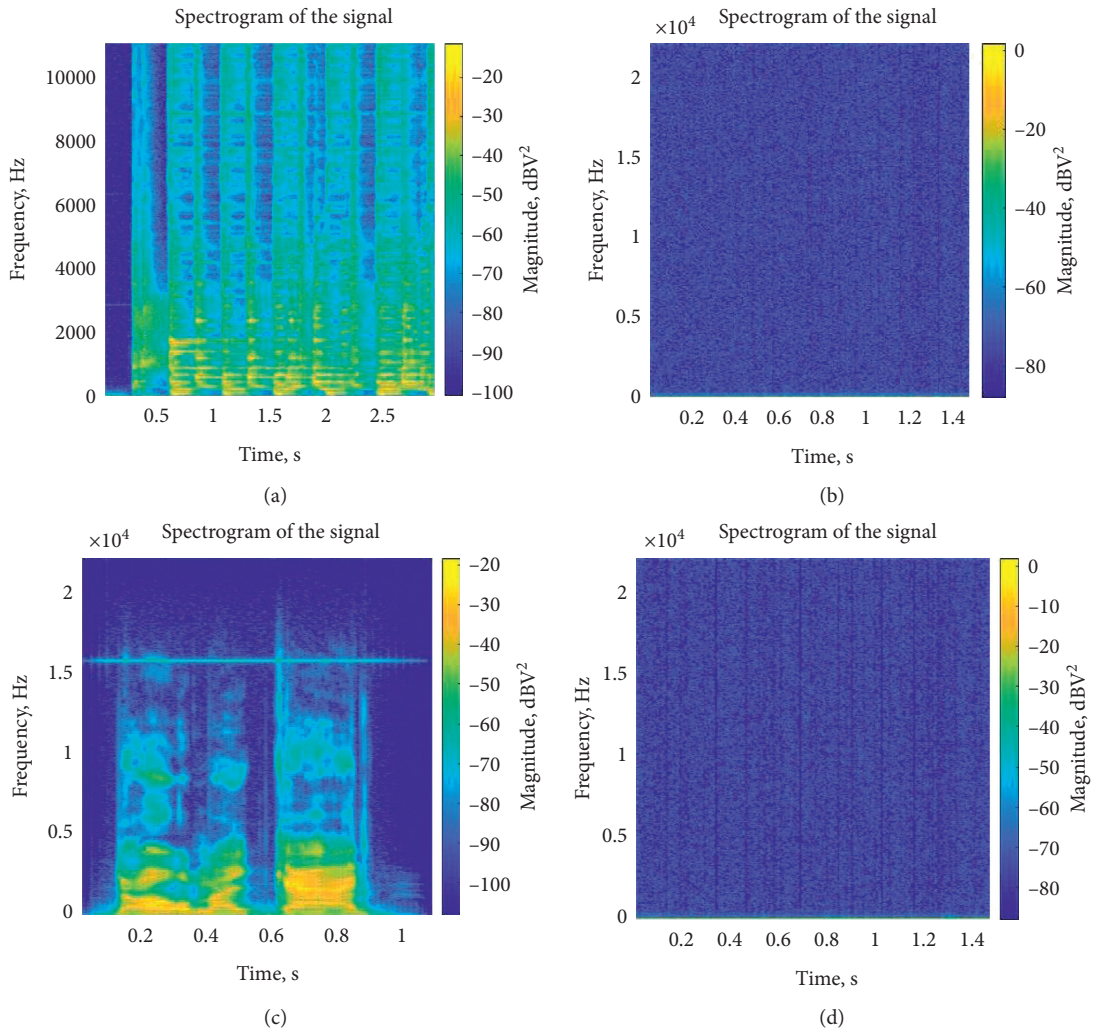

Figure 7: Spectrogram of original Audio 1 and Audio 2 and encrypted Audio 1 and Audio 2. (a) Audio 1, (b) encrypted Audio 1, (c) Audio 2, and (d) encrypted Audio 1.

target noise-resistant and low-profile modern multimedia applications.

6. Conclusion

In the present research, an encryption framework is proposed to ensure the security of real-time multimedia applications. The design framework encrypts audio applications and is primarily developed to ensure the integrity of military voice communications. Three chaotic maps are further incorporated in the proposed scheme to enhance resiliency. The prescribed approach incorporates the action of three recurring steps cyclic shift, permutation, and substitution of bits repeated for four rounds. The proposed design exploits MEC and S_8 symmetric group to synthesize confusion components. Each component of the algorithm has an input yielded by a distinctive chaotic sequence.

The security and performance analysis depicted that the proposed scheme resists all modern attacks. Moreover, the simulation results manifest that the encryption scheme is robust and resistant to noise perturbation. The unique characteristics of noise resistance make the algorithm a unique choice in critical applications. Moreover, the algorithm is flexible and adaptive towards changes. The modular design adopted via the SPN framework along with the fusion of chaotic maps renders the scheme feasible to a variety of low-profile modern applications. The inherent characteristics and evaluation results make the scheme an ideal candidate for modern

warfare communication. The most sublime feature of the proposed scheme is its noise-resistant characteristic that suits ideally to target problem area of real-time audio communication in warzones. The resiliency of the scheme is enhanced by employing additional S-boxes and increasing rounds of encryption. This will surely be subjected to the target application and also increases computational requirements. The proposed paradigm is ideally suited to real-time audio applications and also incorporates digital video with minor alterations. In forthcoming work, we intend to develop a cryptosystem for the security of remote sensing big data. The current scheme will also be fused with a machine learning approach. As a new proposal, it is suggested to analyze this framework before deployment.

Data Availability

The data used to support the findings of this study are included within the article.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

References

[1] M. Ghadi, L. Laouamer, and T. Moulahi, "Securing data exchange in wireless multimedia sensor networks: perspectives and challenges," *Multimedia Tools and Applications*, vol. 75, no. 6, pp. 3425–3451, 2016.

[2] A. Kaur and M. K. Dutta, "An optimized high payload audio watermarking algorithm based on LU-factorization," *Multimedia Systems*, vol. 24, no. 3, pp. 341–353, 2018.

[3] Z. Liu, J. Huang, X. Sun, and C. Qi, "A security watermark scheme used for digital speech forensics," *Multimedia Tools and Applications*, vol. 76, no. 7, pp. 9297–9317, 2017.

[4] J. Daemen and V. Rijmen, *The Design of Rijndael AES-The Advanced Encryption Standard*, Springer-Verlag, Berlin, Germany, 2001.

[5] M. Faheem, S. Jamel, A. Hassan, N. Shafinaz, and M. Mat, "A survey on the cryptographic encryption algorithms," *International Journal of Advanced Computer Science and Applications*, vol. 8, no. 11, pp. 333–344, 2017.

[6] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Communications of the ACM*, vol. 21, no. 2, pp. 120–126, 1978.

[7] A. Ghasemzadeh and E. Esmaeili, "A novel method in audio message encryption based on a mixture of chaos function," *International Journal of Speech Technology*, vol. 20, no. 4, pp. 829–837, 2017.

[8] S. F. El-Zoghdy, H. S. El-Sayed, and O. S. Faragallah, "Transmission of chaotic-based encrypted audio through OFDM," *Wireless Personal Communications*, vol. 113, no. 1, pp. 241–261, 2020.

[9] Z. N. Al-kateeb and S. J. Mohammed, "A novel approach for audio file encryption using hand geometry," *Multimedia Tools and Applications*, vol. 79, no. 27-28, pp. 19615–19628, 2020.

[10] H. Dutta, R. K. Das, S. Nandi, and S. R. M. Prasanna, "An overview of digital audio steganography," *IETE Technical Review (Institution of Electronics and Telecommunication Engineers, India)*, vol. 19, 2019.

[11] P. Sathiyamurthi and S. Ramakrishnan, "Speech encryption algorithm using FFT and 3D-Lorenz-logistic chaotic map," *Multimedia Tools and Applications*, vol. 79, no. 25-26, pp. 17817–17835, 2020.

[12] S. F. Yousif, "Speech encryption based on zaslavsky map," *Journal of Engineering and Applied Science*, vol. 14, no. 17, pp. 6392–6399, 2019.

[13] H. B. Abdalla, A. M. Ahmed, and M. A. Al Sibahee, "Optimization driven mapreduce framework for indexing and retrieval of big data," *KSII Transactions on Internet and Information Systems*, vol. 14, no. 5, pp. 1886–1908, 2020.

[14] C. E. Shannon, "Communication theory of secrecy systems. 1945," *MD Computers*, vol. 15, no. 1, pp. 57–64, 1949.

[15] C. Li, Y. Zhang, and E. Y. Xie, "When an attacker meets a cipher-image in 2018: a year in review," *Journal of Information Security and Applications*, vol. 48, Article ID 102361, 2019.

[16] N. Ferguson, R. Schroeppel, and D. Whiting, "A simple algebraic representation of rijndael," in *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, pp. 103–111, Springer, Berlin, Germany, 2001.

[17] J. Fuller, W. Millan, and E. Dawson, "Multi-objective optimisation of bijective S-boxes," *New Generation Computing*, vol. 23, no. 3, pp. 201–218, 2005.

[18] L. Jing-Mei, W. Bao-Dian, C. Xiang-Guo, and W. Xin-Mei, "Cryptanalysis of rijndael S-box and improvement," *Applied Mathematics and Computation*, vol. 170, no. 2, pp. 958–975, 2005.

[19] U. Hayat, N. A. Azam, and M. Asif, "A method of generating 8 × 8 substitution boxes based on elliptic curves," *Wireless Personal Communications*, vol. 101, no. 1, pp. 439–451, 2018.

[20] U. Hayat and N. A. Azam, "A novel image encryption scheme based on an elliptic curve," *Signal Processing*, vol. 155, pp. 391–402, 2019.

[21] G. Cheng, C. Wang, and C. Xu, "A novel hyper-chaotic image encryption scheme based on quantum genetic algorithm and compressive sensing," *Multimedia Tools and Applications*, vol. 79, no. 39-40, pp. 29243–29263, 2020.

[22] H. Natiq, N. M. G. Al-Saidi, M. R. M. Said, and A. Kilicman, "A new hyperchaotic map and its application for image encryption," *The European Physical Journal Plus*, vol. 133, no. 1, 2018.

[23] X. Wang and Y. Su, "Color image encryption based on chaotic compressed sensing and two-dimensional fractional Fourier transform," *Science Reports*, vol. 10, no. 1, pp. 1–19, 2020.

[24] A. Qayyum, J. Ahmad, W. Boulila et al., "Chaos-based confusion and diffusion of image pixels using dynamic substitution," *IEEE Access*, vol. 8, pp. 140876–140895, 2020.

[25] N. Sasikaladevi, K. Geetha, K. Sriharshini, and M. Durga Aruna, "H3-hybrid multilayered hyper chaotic hyper elliptic curve based image encryption system," *Optics & Laser Technology*, vol. 127, 2020.

[26] Y. Liu and J. Zhang, "A multidimensional chaotic image encryption algorithm based on DNA coding," *Multimedia Tools and Applications*, vol. 79, no. 29-30, pp. 21579–21601, 2020.

[27] Q. Lu, C. Zhu, and X. Deng, "An efficient image encryption scheme based on the LSS chaotic map and single S-box," *IEEE Access*, vol. 8, pp. 25664–25678, 2020.

[28] H. Aziz, S. M. M. Gilani, I. Hussain, and M. A. Abbas, "A novel symmetric image cryptosystem resistant to noise perturbation based on S8 elliptic curve S-boxes and chaotic maps," *The European Physical Journal Plus*, vol. 135, no. 11, pp. 1–42, 2020.

[29] A. Roy and A. P. Misra, "Audio signal encryption using chaotic Hénon map and lifting wavelet transforms," *The European Physical Journal Plus*, vol. 132, no. 12, pp. 1–10, 2017.

[30] H. Liu, A. Kadir, and Y. Li, "Audio encryption scheme by confusion and diffusion based on multi-scroll chaotic system and one-time keys," *Optik*, vol. 127, no. 19, pp. 7431–7438, 2016.

[31] K. Kordov, "A novel audio encryption algorithm with permutation-substitution architecture," *Electron.*vol. 8, no. 5, 2019.

[32] D. Shah, T. Shah, and S. S. Jamal, "Digital audio signals encryption by Mobius transformation and Hénon map," *Multimedia Systems*, vol. 26, no. 2, pp. 235–245, 2020.

[33] R. I. Abdelfatah, "Audio encryption scheme using self-adaptive bit scrambling and two multi chaotic-based dynamic DNA computations," *IEEE Access*, vol. 8, pp. 69894–69907, 2020.

[34] P. K. Naskar, S. Paul, D. Nandy, and A. Chaudhuri, "DNA encoding and channel shuffling for secured encryption of audio data," *Multimedia Tools and Applications*, vol. 78, no. 17, pp. 25019–25042, 2019.

[35] C. Peng, X. Du, K. Li, and M. Li, "An ultra-lightweight encryption scheme in underwater acoustic networks," *Journal of Sensors*, vol. 2016, no. 3, 2016.

[36] A. Adeel, J. Ahmad, H. Larijani, and A. Hussain, "A novel real-time, lightweight chaotic-encryption scheme for next-generation audio-visual hearing aids," *Cognitive Computation*, vol. 12, no. 3, pp. 589–601, 2020.

[37] R. Nagakrishnan and A. Revathi, "A robust cryptosystem to enhance the security in speech based person authentication," *Multimedia Tools and Applications*, vol. 79, no. 29-30, pp. 20795–20819, 2020.

[38] J. Ahmad, M. A. Khan, S. O. Hwang, and J. S. Khan, "A compression sensing and noise-tolerant image encryption scheme based on chaotic maps and orthogonal matrices," *Neural Computing and Applications*, vol. 28, no. s1, pp. 953–967, 2017.

[39] I. F. Elashry, W. El-Shafai, E. S. Hasan et al., "Efficient chaotic-based image cryptosystem with different modes of operation," *Multimedia Tools and Applications*, vol. 79, no. 29-30, pp. 20665–20687, 2020.

[40] K. A. K. Patro, B. Acharya, and V. Nath, "Secure, lossless, and noise-resistive image encryption using chaos, hyper-chaos, and DNA sequence operation," *IETE Technical Review*, vol. 37, no. 3, pp. 223–245, 2020.

[41] E. A. Hussein, M. K. Khashan, and A. K. Jawad, "A high security and noise immunity of speech based on double chaotic masking," *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 10, no. 4, pp. 4270–4278, 2020.

[42] J. A. Michel-Macarty, M. A. Murillo-Escobar, R. M. López-Gutiérrez, C. Cruz-Hernández, and L. Cardoza-Avendaño, "Multiuser communication scheme based on binary phase-shift keying and chaos for telemedicine," *Computer Methods and Programs in Biomedicine*, vol. 162, pp. 165–175, 2018.

[43] S. J. Sheela, K. V. Suresh, and D. Tandur, "A novel audio cryptosystem using chaotic maps and DNA encoding," *Journal of Computer Networks and Communications*, vol. 2017, 2017.

[44] A. Adeel, J. Ahmad, and A. Hussain, "Real-time lightweight chaotic encryption for 5g iot enabled lip-reading driven secure hearing-aid," 2018, https://arxiv.org/abs/1809.04966.

[45] B. Zohuri and B. Zohuri, "Electronic countermeasure and electronic counter-countermeasure," in *Radar Energy Warfare and the Challenges of Stealth Technology*, pp. 111–145, Springer International Publishing, New York, NY, USA, 2020.

[46] I. Hussain, A. Anees, and A. Algarni, "A novel algorithm for thermal image encryption," *Journal of Integrative Neuroscience*, vol. 17, no. 3-4, pp. 447–461, 2018.

[47] L. Y. Sheng, L. L. Cao, K. H. Sun, and J. Wen, "Pseudo-random number generator based on TD-ERCS chaos and its statistic characteristics analysis," *Wuli Xuebao/Acta Physica Sinica*, vol. 54, no. 9, pp. 4031–4037, 2005.

[48] I. Ullah, N. A. Azam, and U. Hayat, "Efficient and secure substitution box and random number generators over Mordell elliptic curves," *Journal of Information Security and Applications*, vol. 56, Article ID 102619, 2021.

[49] I. Hussain, T. Shah, and H. Mahmood, "A new algorithm to construct secure keys for AES," *International Journal of Contemporary Mathematical Sciences*, vol. 5, no. 26, pp. 1263–1270, 2010.

[50] 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, 2017.

[51] J. B. Lima and E. F. Da Silva Neto, "Audio encryption based on the cosine number transform," *Multimedia Tools and Applications*, vol. 75, no. 14, pp. 8403–8418, 2016.

[52] A. Belmeguenai, Z. Ahmida, S. Ouchtati, and R. Djemii, "A novel approach based on stream cipher for selective speech encryption," *International Journal of Speech Technology*, vol. 20, no. 3, pp. 685–698, 2017.