Multimedia Tools and Applications (2021) 80:22251–22273
https://doi.org/10.1007/s11042-021-10697-3

A three-dimensional chaotic map and their applications to digital audio security

Dawood Shah[1] · Tariq Shah[1] · Imtiaz Ahamad[2] · Muhammad Imran Haider[1] · Ijaz Khalid[1]

Received: 14 July 2020 / Revised: 30 November 2020 / Accepted: 10 February 2021/
Published online: 26 March 2021

Abstract
In nonlinear dynamical systems, chaotic behavior is an attractive characteristic that has been broadly examined and researched over the most recent few decades. The chaotic systems are widely used in artificial intelligence and cryptology. Especially, these are considered efficient for multimedia data security. This manuscript has introduced a novel three dimensional (3-D) chaotic systems. The proposed maps are investigated through bifurcation diagrams and phase plots. The resulting diagrams demonstrates the chaotic attractor characteristic and the dynamic behavior of the suggested maps. Furthermore, a lossless audio encryption scheme is introduced utilizing the proposed chaotic maps. In the suggested scheme, the suggested 3-D chaotic sequences are utilized to shuffle the audio data points to achieve the diffusion property. In the confusion module, initially, the sequence of the audio data is divided into 8-bit and 7-bit sequences. Subsequently, the separated sequences are then substituted with different good quality substitution boxes, which are generated through a Mobius transformation over Galois fields. The suggested encryption algorithm is applied to the different audio files of various sizes and characters. The experimental results have revealed that the proposed scheme is capable to secure all kinds of audio files. The security analysis shows that the suggested scheme is capable to withstand differential and statistical attacks.

Keywords Chaotic map · Galois field · Symmetric key cryptography · Audio encryption

✉ Dawood Shah
Dawoodshah254@gmail.com

[1] Department of Mathematics, Quaid-i-Azam University, Islamabad, Pakistan

[2] Department of Mathematics, University of Swabi, Khyber Pakhtunkhwa, Pakistan

1 Introduction

In the current decade, communication technology, multimedia data technology, internet, and internet protocol, the exchange of communication through wireless networks is growing exponentially. The wireless network such as the internet is an open network, so the transmission of sensitive information through the internet is a security risk. Therefore, the development of the new method is essential, which ensures the confidentiality of sensitive information over the open network. For the last several years, researchers have developed classical encryption schemes such as International Encryption Standard (IDES), Data Encryption Standard (DES), RSA, Rivest Cipher 4 (RC4), and Advanced Encryption Standard (AES) [4, 24, 32, 41]. These schemes are depending on mathematical operations and iterated processes, so considered well secure for confidential communication. Since, multimedia data consists of large amount of data and having other distinguishing features such as strong pixels correlation, bulk data capacity, and high redundancy between the rare pixels. Therefore, classical encryption sachem, for example, DES and AES are not appropriated for multimedia data encryption. In literature, several cryptographic schemes are presented using different approaches for multimedia data encryption [1, 2, 22, 30, 37, 38]. Cryptographic algorithms suggested by researchers for digital image encryption is given in [2, 11, 12, 15, 31, 36]. In 1970, Fredrich introduced the notion of chaos-based cryptography and suggested a technique for image encryption based on a chaotic map. Afterward, the researchers have observed that the distinguishing features of the chaotic systems such as their property of dependence on the initial conditions and the high sensitivity property to the parameter and initial condition, randomness, and ergodicity make the theory of chaos suitable for the data security application, in particular for multimedia data encryption. In literature, numerous encryption schemes exist based on chaotic systems for digital images [34]. The existing schemes are based on one dimensional or multidimensional chaotic maps. However, due to a small set of parameters of the one-dimensional chaotic maps, the encryptions schemes that are based on the one-dimensional chaotic maps are proven to not secure against cryptanalysis attacks.

1.1 Related work

In literature, numerous numbers of algorithms are presented for the encryption and decryption of digital audio. However, there does not exist a single scheme that applies to all audio formats. De Martin and Serveti introduced a technique for the partial encryption of telephone speech in 2002 [27], in which the authors have suggested two different methods for partial encryption. The first method was designated as having a high bit rate but low-security strength. However, the second method was designed to encrypt more and more bit data streams and provide strong security. In the same year, Thorwirth et al. had presented the selection encryption method that relied on the standard compression for perceptual audio coding [33]. In the suggested work the authors mostly focused on the analyses of the encrypted MP3 encoded files. Then Serveti et al. presented another MP3 audio encryption scheme in 2003 [28]. The presented algorithm was a partial encryption scheme with low time complexity, which preserved the content of the information nevertheless alter the quality of the original audio. Afterward, Bhargava et al. introduced four encryption schemes for digital video applicable for MPEG format [3]. In the suggested scheme a shared secret key was utilized to randomly modify the coefficient of Discrete Cosine Transform. Subsequently, Grangetto et al. presented a new multimedia data security framework based on arithmetic coding [8]. In the proposed work, the goal of

multimedia data encryption was accomplished by inserting randomization in the procedure of arithmetic coding. In 2008 Yan et al. proposed the procedure of scrambling digital audio data in the compressed domain [39]. The suggested scheme worked to scramble the secret audio data utilizing the key before transmission. However, this work was then proved defenseless against the brute force attack [40]. Neto and Lima suggested an audio encryption scheme using the cosine number transform [18]. The anticipated mechanism was applicable to encrypt the blocks of the audio data. The selection of the block was based on a sample overlapping rule that produced confusion and diffusion in the ciphered data. The theory of chaos was extensively used for multimedia data encryption, presented in the literature. The encryption techniques depend on chaotic maps for the encryptions of static multimedia data such as digital images are given in [5, 14, 35]. Besides, these are widely utilized for dynamic multimedia data like audio and video. Mosa et al. proposed an audio encryption scheme based on the Bakar map in 2011 [21]. In the presented scheme, the Bakar chaotic map is used for the permutation of audio segments and achieves the goal of permutation using masking in the transform and time domain. The speech encryption scheme based on the chaotic shift key was proposed by Sathiyamurthi et al. [25]. In the suggested scheme the goal of the high-security level is achieved by multiple times permutating the sample of the data. Next, Madian et al. introduced audio scrambling to break the correlation between the audio data based on two-dimensional cellular automata [19]. Subsequently, Liu et al. presented an innovative mechanism for the encryption of digital audio, in which a multi-scroll chaotic map was deployed for the confusion and the diffusion of the data. The audio encryption scheme relying on a fuzzy cellular network. The delayed uncertainty of hybrid bidirectional associative memory was proposed by Kalpana et al. in 2018 [13].

1.2 Our contribution

In this paper, we have introduced a novel three-dimensional discrete chaotic map. The structure of the new three-dimensional chaotic map is inspired by the map given in [20]. The map has been extended and includes more control parameters while remaining their dimension the same. The performance analysis demonstrates that the new chaotic map shows better chaotic behavior and enlarge interval of control perimeters than the existing map. Besides, we have presented| a novel lossless audio encryption scheme based on the suggested chaotic maps. The initial conditions and control parameters are used as a secret key to generate chaotic sequences. The generated sequences are then used in diffusion confusion operations. The result of the security analysis and simulations demonstrate that the suggested encryption scheme is more efficient to resist various cryptanalysis attacks.

The remaining part of the manuscript is organized as follows: Section 2, presents a novel chaotic map and their evaluation results. The proposed audio encryption scheme is introduced in Section 3. Section 4 is devoted to the construction and analysis of the seven-bit S-box. In Section 5, we have discussed the simulation results and their comparison with the existing scheme. In the last, Section 6, the discussion has been concluded.

2 Preliminaries

This section is concerned to recall some fundamental definitions and theorems, which are used in the proposed encryption scheme.

Definition2.1. Let X and Y be any two systems, such that

$$X(i+1) = G(X(i)) \tag{1}$$

$$Y(i+1) = F(X(i), Y(i)) \tag{2}$$

$$X(i) = (x_1(i), x_2(i), \ldots, x_{m-1}(i), x_m(i))^T \tag{3}$$

$$Y(i) = (y_1(i), y_2(i), \ldots, y_{m-1}(i), y_n(i))^T \quad n \leq m \tag{4}$$

$$G(X(i)) = (g(x_1(i)), g(x_2(i)), \ldots, g(x_{m-1}(i)), g(x_m(i)))^T \tag{5}$$

$$F(X(i), Y(i)) = (f_1(X(i), Y(i)), f_2(X(i), Y(i)), \ldots., f_m(X(i), Y(i)))^T \tag{6}$$

In the systems, the system in (1) is said to the driving system and the system in (2) is called a driven system. If there exists a transformation$H$, such that

$$H : \mathbb{R}^m \rightarrow \mathbb{R}^n$$

$$H(X(i)) = (h_1(i), h_2(i), \ldots, h_n(i))^T \tag{7}$$

The system of the equations given in (1) and (2) is said to be generalization synchronization. If for a subset $S = S_X \times S_Y \subset \mathbb{R}^m \times \mathbb{R}^n$ and the entire trajectory that is given in Eqs. (1) and (2) with the initial condition in Ssatisfy the following equation.

$$\lim_{i \rightarrow +\infty} \| H(X(i) - Y(i)) \| = 0 \tag{8}$$

Theorem 2.2 Let X, F(X), X_n and F(Y, X) be the systems which are defined in the preliminaries sections and X_n is defined as

$$X_n = (x_1(i), x_2(i), \ldots . x_n(i)) \tag{9}$$

Let T be the invertible transformation defined as follows

$$T : \mathbb{R}^n \rightarrow \mathbb{R}^n$$

$$T(x_1, x_2, \ldots, x_{n-1}, x_n) = (y_1, y_2, \ldots, y_{n-1}, y_n) \tag{10}$$

If the systems that are given in the Eqs. (1) and (2) are generalized synchronization by the transformation $Y = T(X_n)$. Then the functions F(Y, X) given in the equation satisfies the following properties

$$F(Y,X) = T(G_m(x) - r(X_n, Y)) \tag{11}$$

$$G_m(x) = (g_1(x), g_2(x), \ldots, g_m(x))^T \tag{12}$$

The function r that is defined as

$$r(X_n, Y) = (r_1(X_n, Y), r_2(X_n, Y), r_3(X_n, Y), \ldots, r_n(X_n, Y)) \tag{13}$$

guarantee the stability of the zero solution of the following error equation.

$$e(i+1) = T(X_n(i+1)) - Y(i+1) = r(X_n, Y) \tag{14}$$

2.1 Proposed chaotic map

This section is devoted to the introduction of the proposed Chaotic map and to the detailed discussion of their properties which are given as follows

$$x_{i+1} = y_i + \alpha \sin(x_i) + \gamma \cos(z_i) \tag{15}$$

$$y_{i+1} = x_i + \sin(x_i)\cos(y_i) + \tan(z_i) \tag{16}$$

$$z_{i+1} = x_i \sin(i) + y_i \cos(i) + \beta \tan^{-1}(z_i) - \delta \tag{17}$$

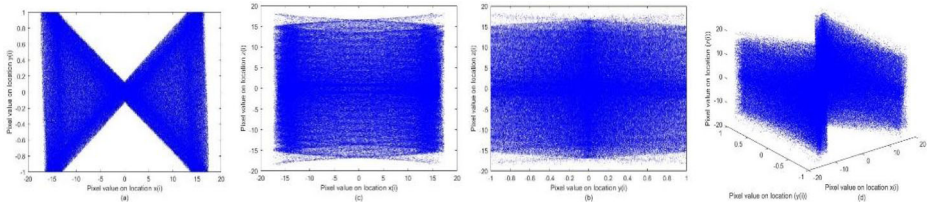
In the above chaotic system of equation, for any $\alpha \in [5, \infty)$, $\beta \in [-10, 10]$and $\{\gamma, \delta\} \subseteq [-1, \ 1]$, and for the initial condition $(x_0, y_0, z_0) = (.0705, 00001, 0038)$, the chaotic orbit of the system of equationsx_i, $y_i z_i$ for the first fifty thousand iterations is visualized in Fig. 1(a-d).

Afterward, defined an invertible matrix M and defined a transformation given as follows:

$$T : \mathbb{R}^3 \rightarrow \mathbb{R}^3$$

Defined by

$$T(x_i, y_i, z_i) = \begin{pmatrix} 3 & -2 & -3 \\ 3 & 0 & -1 \\ -3 & 2 & 3 \end{pmatrix} \begin{bmatrix} x_i \\ y_i \\ z_i \end{bmatrix} \tag{18}$$



(a) (b) (c) (d)

Fig. 1 Chaotic trajectories of variables (**a**) $x_i - y_i$ (**b**) $y_i - z_i$ (**c**) $x_i - z_i$ (**d**) $x_i - y_i - z_i$

Let

$$r(X, Y) = -0.5(TX - Y) \tag{19}$$

Then $r(X, Y)$build an asymptotically stable error equation. Then by using theorem (1) the obtain system is in the form of:

$$Y(i+1) = M(G(X(k)) - r(X, Y)) \tag{20}$$

Choose the initial condition $Y(0) = T(x_0, y_0, z_0)$. The first fifty thousand iterations of the system given are shown in Fig. 2. It can be seen that the chaotic behavior of the systems given in (15), (16), and (17) are completely different, accordingly both the systems are not generalization synchronization related. Besides, its chaotic behavior is better than the system given in [20].

3 Proposed algorithm

We discussed the proposed audio encryption scheme in this section. The proposed scheme is designed to secure digital audio in a wav format before transmitting it over an insecure channel. Initially, the scheme read the audio file in the class signed sixteen-bit integers, whose range value laid in the interval $[-2^{15},\ 2^{15}]$. We denote the matrix of the original audio data by $\mathcal{K}$ having dimension $M \times N$, where M denotes the number of rows and N denotes the number of columns. The step-by-step procedure of the encryption scheme is given as follows;

Step 1. Since, initially, the scheme read the audio file in the class signed bit integers, which contains negative integers, therefore initially the scheme generates binary matrix consist of 0 and 1 to recognize the position of the non-negative and negative integers. The mathematical formulation is given as follows;

$$\mathcal{B}_{i,j} = \begin{cases} 0 & if \quad k_{i,j} < 0 \\ 1 & if \quad k_{i,j} \geq 0 \end{cases} \tag{21}$$

Where $\mathcal{B}_{i,j}$denoted the $(i,j)_{th}$ element of the binary matrix and $k_{i,j}$ denote the element of the data matrix $\mathcal{K}$ at position(i,j). Consequently, get a binary matrix $\mathcal{B}$ of dimension $M \times N$.

Step 2. In the next step, transform the audio data from the set $[-2^{15},\ 2^{15}-1]$ to the set $[-2^{15}-1,\ 2^{15}-1]$ using the following equation;

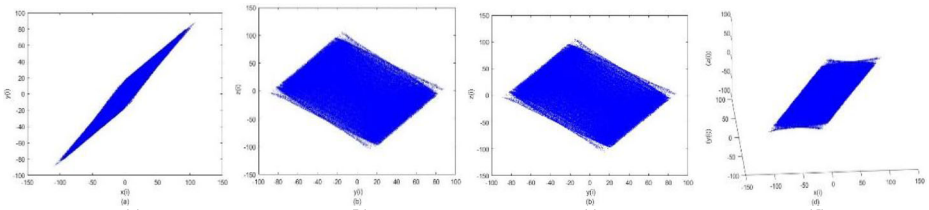


Fig. 2 Chaotic trajectories of variables (**a**) $T(x_i - y_i)$ (**b**) $T(y_i - z_i)$ (**c**) $T(x_i - z_i)$ (**d**) $T(x_i - y_i - z_i)$

$$k_{ij} = \begin{cases} k_{ij} & if \quad k_{ij} > -2^{15} \\ k_{ij} - 1 & if \quad k_{ij} = -2^{15} \end{cases} \tag{22}$$

As resultant get a new matrix$\mathcal{K}^{'}$ having entries between the range $-2^{15}-1$ and $2^{15}-1$, aim to convert the data into 15-bit integer values.

Step 3. Afterward**,** the scheme uses the absolute function and transform the data of the matrix $\mathcal{K}^{'}$ from the set $\{-2^{15}-1,\ldots,2^{15}-1\}$ to the set $\{0,\ldots,2^{15}-1\}$ and get a new matrix $\mathcal{K}^{''}$whose entries consist of 15-bit positive integers.

Step 4. Then the scheme generates the random sequences x_{R_i}, y_{R_i} and $z_{R_i}$by using the following modular equations,

$$x_{R_i} = floor\left(x_i \times 10^5\right) mod\ M \tag{23}$$

$$y_{R_i} = floor\left(y_i \times 10^5\right) mod\ N \tag{24}$$

$$z_{R_i} = floor\left(z_i \times 10^5\right) mod\ L \tag{25}$$

Where x_i, y_i and z_i are the sequences defined in the Eqs. (15–17) and L denote an integer greater than $M \times N$. The random sequences are tested through a statistical test suite from random numbers and pseudorandom numbers generator for cryptographic applications, the result is given in Tab. 4.

Step 5. Since multimedia data exist a strong correlation among the adjacent integers, therefore efficient multimedia data schemes include several features to break the strong correlation among the adjacent values. Accordingly, in this step, the proposed algorithm utilizes the generated sequences given in step 4 and shuffle the matrix $\mathcal{K}^{''}$. We can write it in mathematical form given as follows;

$$\mathcal{K}^{p}(i,j) = \mathcal{K}^{''}(x_R(i), y_R(j)) \tag{26}$$

Where (i,j) denote the integer position in the shuffled matrix $\mathcal{K}^{p}$. The correlation analysis graphs are illustrated in Fig. 7. The figures show that the permutation step successfully break the correlation among the adject pixels.

Step 4. The confusion phase is an essential part of any cryptosystem. In this step, we used the substitution procedure to produced confusion in the ciphered data. Since the data in

the permuted block are 15-bit integers, so it will be might computationally complex to substitute the whole block containing 15-bit integers, therefore we dived the block into two subblocks, containing 8-bit integers and 7-bit integers respectively by using the following maps;

$$\psi_1 : \mathbb{Z}_2{}^{15} \longrightarrow \mathbb{Z}_2{}^{8} \text{ and } \psi_2 : \mathbb{Z}_2{}^{15} \longrightarrow \mathbb{Z}_2{}^{7.}$$

Defined by

$$\psi_1(a_1, a_2, \ldots, a_{15}) = (a_1, a_2, \ldots, a_8, 0, 0, \ldots, 0) \tag{27}$$

$$\psi_2(a_1, a_2, \ldots, a_{15}) = (0, 0, \ldots, 0, a_9, a_{10}, \ldots, a_{15}) \tag{28}$$

Consequently, get two subblocks $\mathcal{K}^p{}_7$ and $\mathcal{K}^p{}_8$ consist of seven-bit and eight-bit elements respectively.

Step 5. Generate two 8×8 S-box and 7×7 S-box by using Möbius transformation over Galois field $GF(2^8)$ and $GF(2^7)$. The procedure of generating 8×8 S-box and their security analyses is given in the literature [16]. Since 7×7 S-box has never been used and analyzed before, therefore in this paper, we briefly discussed the construction procedure of 7×7 S-box and their performance analysis in Section 4.

Step 6. In this step, substitute the subblock $\mathcal{K}^p{}_8$ with 8×8 S-box, the substitution process is same as AES substitution. Since the 7×7 S-box is the 8×16 lookup table as shown in the Table 1, therefore the substitution process is somehow unique. Initially, convert the decimal representation of the elements of the subblock $\mathcal{K}^p{}_7$ into binary representations. Then split the seven bits elements into three and four bits, and convert the three-bits string and the four-bits string elements into decimal representation, and substitute the elements with the elements of the S-box place at the position (i, j), where i denote the decimal representation of the three-bit elements and $j$denote the decimal representation at of the four-bit elements. For better understanding read Example 4.1.

Step 7. After the substitution process, one can get new subblocks $\mathcal{K}^S{}_8$and $\mathcal{K}^S{}_7$. Eventually, used the xor operation and xor the obtained blocks $\mathcal{K}^S{}_8$and $\mathcal{K}^S{}_7$ with the sequence z_{R_i} *mod* 256 and z_{R_i} *mod* 128 and get new blocks $\mathcal{K}^E{}_8$and $\mathcal{K}^E{}_7$.

Step 8. Convert the seven-bit block $\mathcal{K}^E{}_7$ and the eight-bit block $\mathcal{K}^E{}_8$ into a single fifteen-bit block by using the following maps;

$$\psi^{-1} : \mathbb{Z}_2{}^{8} \times \mathbb{Z}_2{}^{7} \rightarrow \mathbb{Z}_2{}^{15}$$

$$\psi^{-1}((a_1, a_2, \ldots, a_8), (a_1, a_2, \ldots, a_7)) = (a_1, a_2, \ldots, a_8, a_1, a_2, \ldots, a_7) \tag{29}$$

Table 1 Proposed **7 × 7** S-box

49	9	118	108	31	13	92	109	41	113	51	103	105	116	112	18
19	22	37	8	81	26	25	87	40	36	29	70	38	46	3	28
72	120	17	57	20	4	107	127	21	30	16	111	48	91	94	88
119	75	64	83	98	47	95	59	54	117	52	125	32	12	67	6
123	101	66	99	44	84	68	61	74	96	23	100	62	121	78	50
10	124	34	58	35	115	90	33	73	122	114	27	106	24	102	63
15	11	104	39	110	0	80	42	71	77	82	7	69	126	56	79
93	55	97	43	45	65	85	76	1	53	14	60	2	5	86	89

Where $a_i \in \{0, 1\}$. As the result of the above map get $M \times N$ block $\mathcal{K}^S{}_{15}$ containing fifteen bits elements.

Step 9. At the final step, map the elements of the matrix $\mathcal{K}^S{}_{15}$from the $\{0, 1, 2, \ldots 2^{15} - 1\}$ to the set $\{-2^{15} - 1,\ 2^{15} - 1\}$ using the binary matrix $\mathcal{B}$. The mathematical formula is given as follows;

$$\mathcal{K}^E(i,j) = \begin{cases} \mathcal{K}^S{}_{15}(i,j) & if\ \ \mathcal{B}(i,j) = 1 \\ -\mathcal{K}^S{}_{15}(i,j) & if\ \ \mathcal{B}(i,j) = 0 \end{cases} \tag{30}$$

The obtained matrix $\mathcal{K}^E$is then converts into the Audio file which is required ciphered audio. Further detail of the proposed scheme is illustrated in the flow chart of the scheme, shown in Fig. 3. To test the security strength of the proposed scheme, we have encrypted various audio files of different characters and different sizes. The result analyses are shown in the following section.

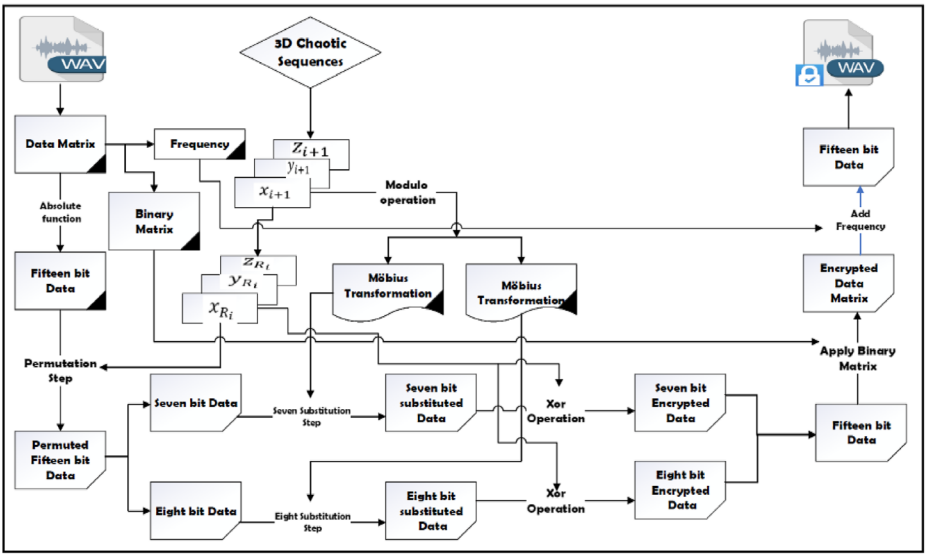


Fig. 3 Flow chart of the propose encryption scheme

Algorithm 1

Audio Encryption	**Audio Decryption**
1. **Start**	1. **Start**
2. **Input:** Audio.wav	2. **Input:** Audio.wav
3. Key: []	3. Key: []
4. **Output:** Encrypted Audio.wav	4. **Output:** Encrypted Audio.wav
5. Data=D	47. [D, F] ←audioread('Input,'native');
6. Frequency=F	5. [row, column]←size (D)
7. [D, F] ←audioread('Input,'native');	6. L ← gmultiply (row, column)
8. [row, column]←size (Data)	7. **for** j=1 to L **do**
9. L ← gmultiply (row, column)	8. $x_{i+1} \leftarrow x_i$
10. **for** j=1 to L **do**	9. $y_{i+1} \leftarrow y_i$
11. $x_{i+1} \leftarrow x_i$	10. $y_{i+1} \leftarrow x_i$
12. $y_{i+1} \leftarrow y_i$	11. **end**
13. $y_{i+1} \leftarrow x_i$	12. K_C=D
14. **end**	13. **for** i=1 to row **do**
15. K=Data	14. **for** j=1 to column **do**
16. **for** i=1 to row **do**	15. B(i,j)=1
17. **for** j=1 to column **do**	16. **if** K_C(i,j)≥0
18. B(i,j)=1	17. **else** B(i,j)=0
19. **if** K(i,j)≥0	18. **end**
20. **else** B(i,j)=0	19. **end**
21. **end**	20. K_o = absolute(K)
22. **end**	21. K_{7E} = K_p-bitshift(bitshift (K_C,-7), 7)
23. K_o = absolute(K)	22. K_{8E} = bitshift(bitshift (K_C,-8), 8)
24. **for i=**1to column	23. K_{7s} = bitxor ($K_{7E,}$ mod (Z_{i+1}, 128))
25. **for j=**1 to row	24. K_{8s} = bitxor ($K_{8E,}$ mod (Z_{i+1}, 256))
26. K_p(i,j)= K_o(x_i, y_i)	25. Inverse_S-box_1=LFT_128 (d, b, c, a)
27. **end**	26. Inverse_S-box_2=LFT_256(d_1, b_1, c_1, a_1)
28. **e**	27. K_7=substitute ($K_{7s,}$ Inverse_S-box_1)
29. S-box_1=LFT_128 (a, b, c, d)	28. K_8=substitute ($K_{8s,}$ Inverse_S-box_2)
30. S-box_2=LFT_256(a_1, b_1, c_1, d_1)	29. K_p= K_8+ K_7
31. K_7 = K_p-bitshift(bitshift (K_p,-7), 7)	30. x_i'=inverse (x_i)
32. K_8 = bitshift(bitshift (K_p,-8), 8)	31. y_i'=inverse (y_i)
33. K_{7s}=substitute ($K_{7,}$ S-box_1)	32. **for i=**1to column
34. K_{8s}=substitute ($K_{8,}$ S-box_2)	33. **for j=**1 to row
35. K_{7E} = bitxor ($K_{7s,}$ mod (Z_{i+1}, 128))	34. K_o(i,j)=K_p(x_i',y_i')
36. K_{8E} = bitxor ($K_{8s,}$ mod (Z_{i+1}, 256))	35. **end**
37. K_E= K_{8E}+ K_{7E}	36. **end**
38. **for** i=1 to row **do**	37. **for** i=1 to row **do**
39. **for** j=1 to column **do**	38. **for** j=1 to column **do**
40. K_C (i,j)= K_E (i,j)	39. K (i,j)= K_o (i,j)
41. **if** B(i,j)≥0	40. **if** B(i,j)≥0
42. **else** K_C (i,j)= -K_C (i,j)	41. **else** K (i,j)= -K_o (i,j)
43. **end**	42. **end**
44. **end**	43. **end**
45. **end**	44. **end**
46. audiowrite('Encrypted Audio.wav', K_C, F)	45. audiowrite('Encrypted Audio.wav', K_C, F)

4 Construction of 7 × 7 S-box and their performance analysis

Since 7 × 7 S-box has never been used before, therefore a brief discussion is given in this section about the construction procedure of the 7 × 7 S-box and their performance analyses. The S-box used to substitute the subblock consist of seven-bit integers is

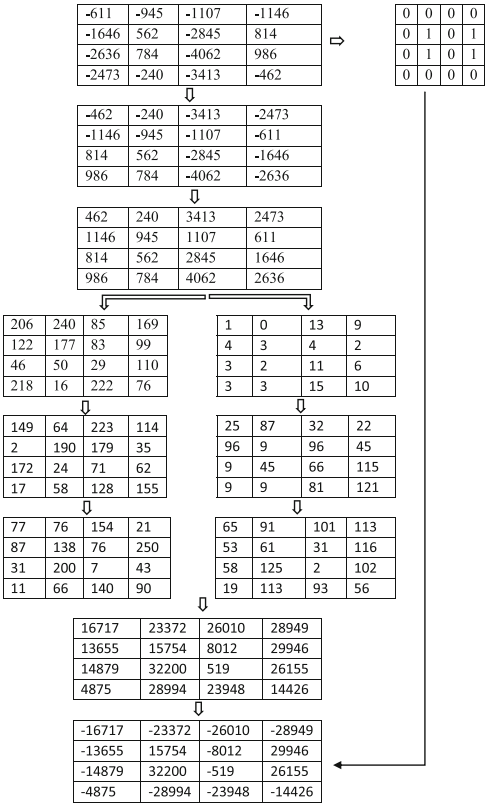
based on the action of general linear group $GL(2, \mathbb{F}_{2^7})$ on the binary Galois field extension $\mathbb{F}_{2^7}$ of order 128 [29], the mathematical representation is defined as follows:

$$\begin{aligned} &S\colon GL(2, \mathbb{F}_{2^7}) \times \mathbb{F}_{2^7} \to \mathbb{F}_{2^7} \\ &S(M, y) = \mathcal{f}_M(y) \end{aligned} \tag{31}$$

Where $\mathcal{f}_M(y)=u(y) + v/w(y) + z$ and u, v, w, and z are the elements of the extension field $\mathbb{F}_{2^7}$, which satisfied the condition $u \times z + v \times z \neq 0$, where the operations × and + are the extension field $\mathbb{F}_{2^7}$ operations field multiplication and addition. $\mathcal{f}_{\mathcal{M}}$ is a discontinues bijective map over the extension filed $\mathbb{F}_{2^7}$.The images of $\mathcal{F}_{\mathcal{M}}$ are then transmute into an 8 × 16 lookup table. In this study, we construct a 7 × 7 S-box by using the parameters $u = 53$, $v = 46$, $w = 33$ and $z = 34$ and primitive irreducible polynomial $p(x) = x^7 + x + 1$. The S-box is shown in Table 1, in the next subsection we analyzed the performance analyses of the constructed S-box.

Example 4.1 Le $I = (0101101)_x$ be the input of the S-box, then the MSB $010_x = 2$ indicates the second row, the numbering starts from 0, and the column $1101_x = 13$. If the input I is substitute with the S-box given in Table 1, then the output of the S-box is$S_1(45 = (101101)_x) = 1$.

Example 4. 2 The following tables demonstrate the step-by-step procedure of proposed encryption scheme.



4.1 Security analysis of the 7 × 7 S-box

In this subsection, we presented some statistical and algebraic analysis of the proposed S-box given in Table 1. followed [18]. The suggested S-box is examined over diverse analyses, for instance, Nonlinearity, Differential approximation probability (DP), Bit independent criterion (BIC), Strict avalanche criterion (SAC), and Linear approximation probability (LP). The nonlinearity of an S-box demonstrates the distance between the Boolean functions of the S-box and the set all affine functions. The upper bound of a Boolean vector function is calculated by the formula $2^{x-1}-2^{\frac{(x-1)}{2}-1}$. Thus for $x=7$ the optimum nonlinearity value is 60. The average nonlinearity value of the proposed is 52.8571 shown in Table 2, which is near the optimum value. Similarly, the results of the other analyses are appeared in a similar table, which demonstrates that the proposed S-box is secure against all kinds of attacks.

5 Security analysis

A well-organized multimedia data encryption scheme should be able to resist all kinds of attacks such as statistical, brute force, and other cryptanalytic attacks. In this section, we analyze the robustness of the suggested encryption algorithm against multiple attacks. The test simulations are carried out by Matlab 2019(b) on a portable personal computer. To investigate the proposed encryption scheme, we have chosen multiple audio samples with different characters such as speech, music, etc., and encrypt these samples via the proposed scheme using different keys. Figure 4 shows the waveforms of the original and the encrypted audio files. From the Figures, it can be seen that the amplitude plotted in the waveform of the encrypted audios is uniform and have no similarity with the amplitude of the original audio, thus the audio is successfully encrypted. In the next subsection, we examine the scheme against various analyses, for example, spectrogram, histogram analysis, entropy and Correlation.

5.1 Spectrogram analysis

The Spectrogram analysis of the audio is widely used for sound analysis. It is the basic tool to analyze the sound in spectral analysis. The spectrogram of audio is defined as two-dimensional graphs with the third dimension represented via different colors. It is the visual representation of the frequency that is varies with time. However, the color in the third dimension represents the amplitude or loudness of the sound at a specific time, whereas the red and blue colors specify the low amplitude and the bright color up means

Table 2 Performance analyses of the **7 × 7** S-box

7×7 S-boxes	Non-linearity	SAC	BIC	BIC-SAC	DP	LP
Proposed S-box	52.8571	.0.4978	52.851	0.504	0.0156	0.09375
Ref. [6] **8×8** S-box	108	0.4988	102.8	0.4988	–	–
Ref. [10] **8×8** S-box	107	0.499023	–	0.50635	.12500	0.0390620

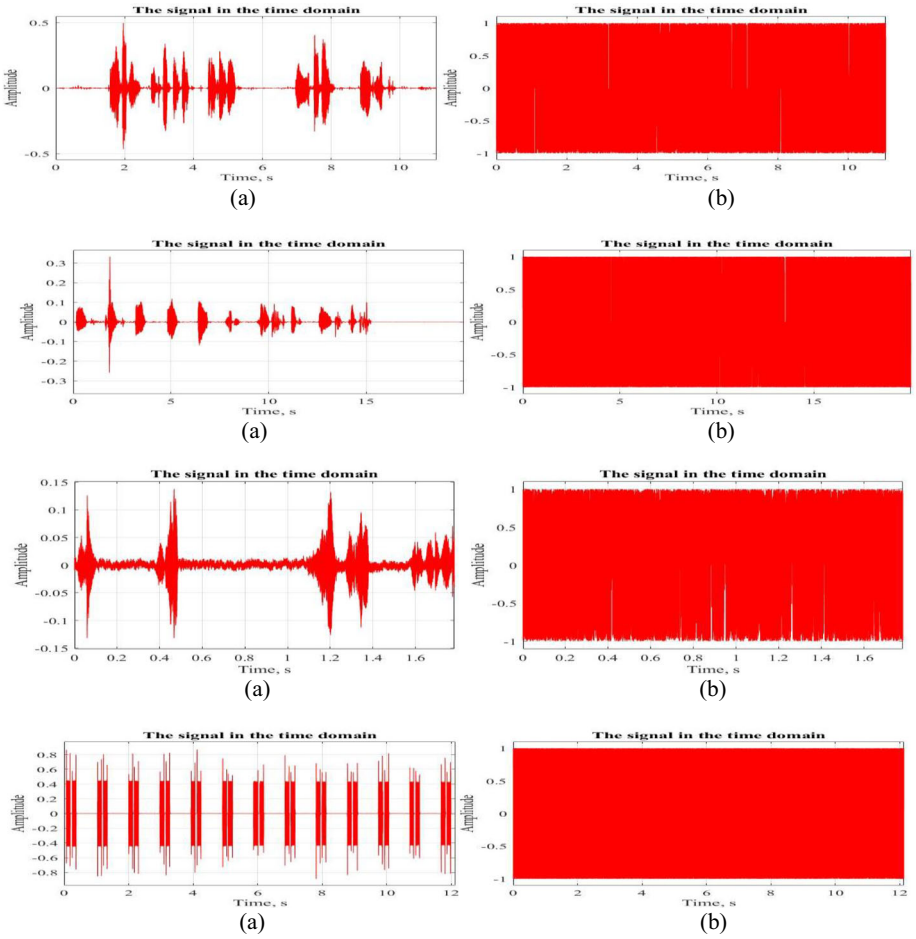


Fig. 4 Waveforms of the man, female, bird and alarm audio (**b**) original audio file (**b**) encrypted audio file

the stronger amplitude. We analyzed the proposed encryption scheme through spectrogram analysis, the result is shown in Fig. 5. Figure 5 (a) displays the spectrogram graph of the original audio file, while the spectrogram of the encrypted audio file is shown in Fig. 5(b). In the figures one can noticed that the spectrogram of the encrypted audio is uniform, have strong amplitude, and completely different from the spectrogram of the original audio, Thus the audio is successfully encrypted.

5.2 Histogram analysis

The histogram analysis is the prominent method, used to examine the encryption quality of the cryptosystem against statistical attacks. Since the cryptosystem is likely to transform the original data into noise and produce randomness in the data. Thus, the well-organized cryptosystem should convert the original data with similarly probable values, so that the encrypted data provides no info that helps the attacker to decrypt the data without information of the secret key. We scrutinize the proposed encryption scheme with histogram analysis, the

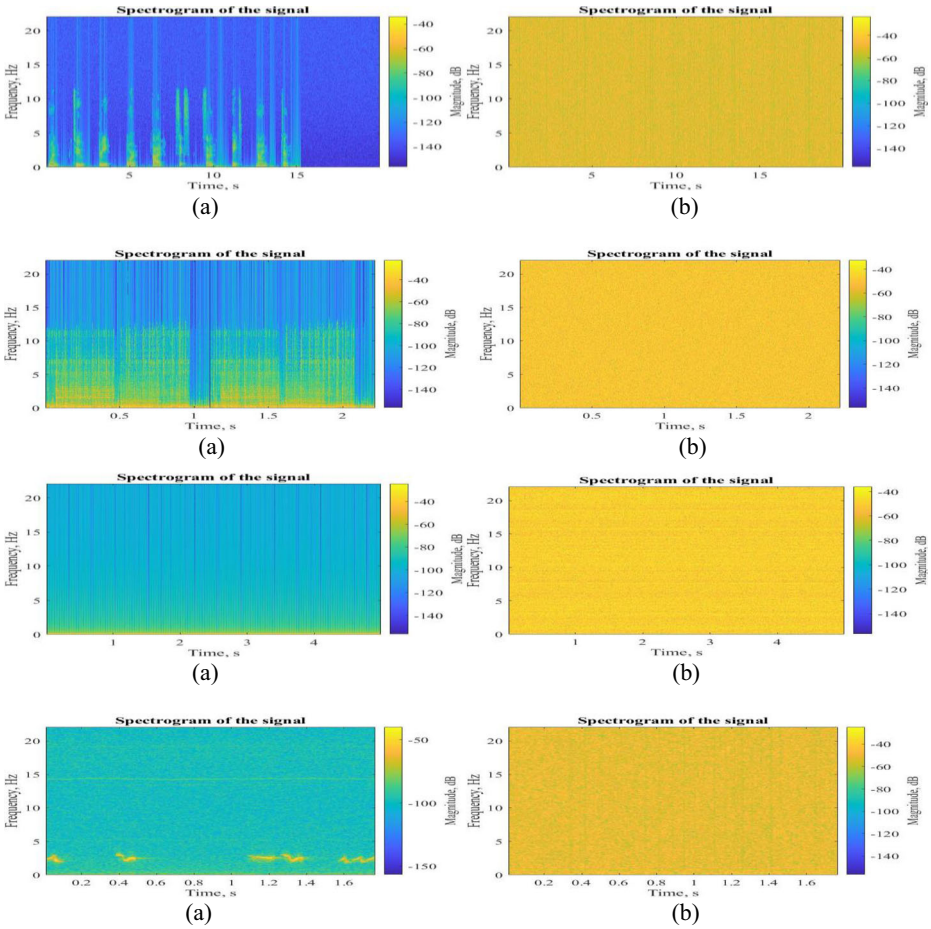


Fig. 5 Spectrogram graph of man sound, female sound, birds sound and alarm (**a**) original audio (**b**) encrypted audio

result is illustrated in Fig. 6. Figure 6(a) displays the histogram of the original audio, while the histogram of the encrypted audio file is shown in Fig. 3(b). It can be seen that the histogram of the original audio signal random and converging to a single point, however, the histograms of all encrypted audio files are almost uniform. Accordingly, the proposed scheme is highly secure against any statistical attack and the eavesdroppers are be unable to extract information from the encrypted data.

5.3 Correlation

The correlation coefficient is a statistical test used to scrutinize the strength of the cryptosystem against several statistical attacks. Since in multimedia data the segments of the data are strongly correlated. Therefor a well-secure cryptosystem should interrupt the correlation among the segment of the data. The Correlation analyses examine the correlation between the similar segments in the data. The mathematical representation of the correlation coefficient is given as follows:

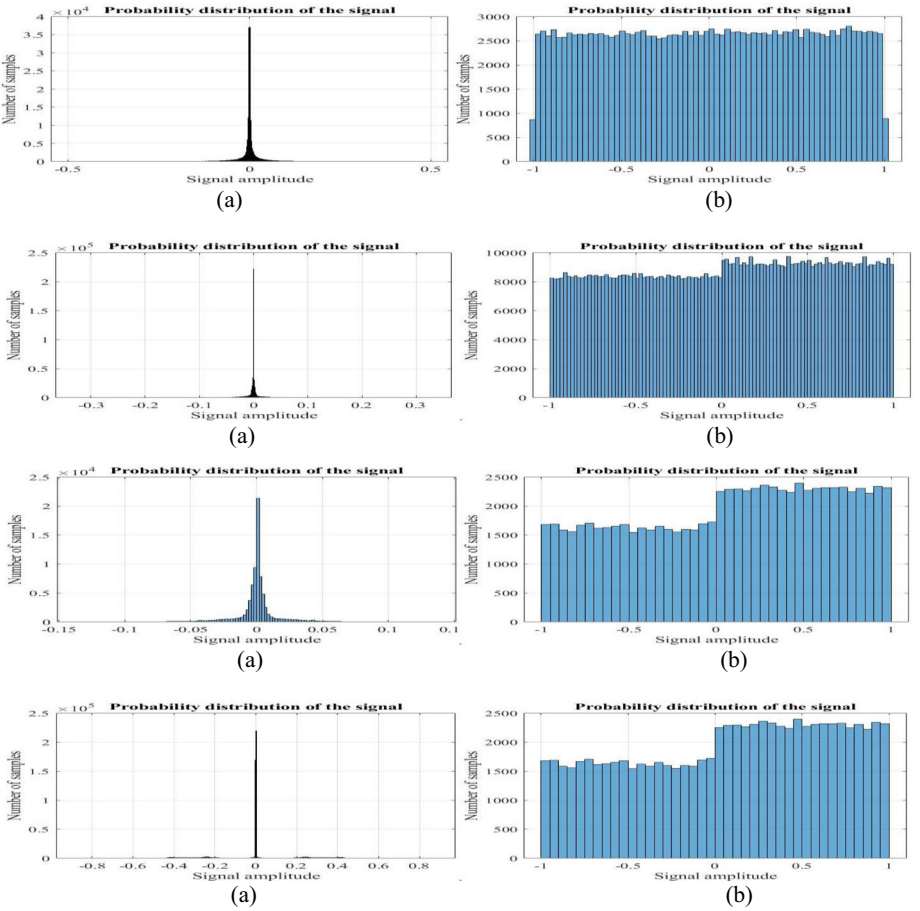


Fig. 6 Histogram analysis of men, female, birds and alarm audio (**a**) histogram of the original audio. (**b**) Histogram of the corresponding encrypted audio

$$\gamma_{uv} = \frac{cov(p,q)}{\sqrt{\mathcal{D}(p)\mathcal{D}(q)}} \tag{32}$$

Where

$$cov(p,q) = \frac{1}{\mathcal{P}} \sum_{i=1}^{\mathcal{P}} p_i - \mathcal{E}(p)(q_i - \mathcal{E}(q)) \tag{33}$$

$$\mathcal{D}(p) = \frac{1}{\mathcal{P}} \sum_{i=}^{\mathcal{P}} (p_i - \mathcal{E}(p))^2 \tag{34}$$

And

$$\mathcal{E}(p) = \frac{1}{\mathcal{P}} \sum_{i=1}^{\mathcal{P}} p_i \tag{35}$$

Table 3 Correlation analysis of different audio

No	Audio	Plain audio	Ciphered audio	Size
1	Animal sound.wav	0.9945	0.0050	530/Kilobyte
2	Alarm sound.wav	0.7317	−0.0060	24,000 / Kilobyte
3	Applause sound. Wav	0.8368	−0.0059	783/ Kilobyte
4	Bells sound. Wav	0.9962	0.0021	32,000/ Kilobyte
5	Birds sound.wav	0.9924	−0.0041	307/ Kilobyte
6	Female sound.wav	0.9933	−0.0019	32/ Kilobyte
7	44,100 Hz tone.wav	0.9886	0.0015	434/Kilobytes
8	Male sound.wav	0.9464	0.0019	345/Kilobytes
9	Machine sound.wav	0.9523	−0.0020	26,000 /Kilobyte
10	Music sound.wav	0.9935	0.0010	11,000/Kilobyte
11	New intro sound.wav	0.9847	−0.0026	900 /Kilobyte
12	Ref. [26]		0.001699	98.6/k
13	Ref. [17]		0.0119	138/k
14	Ref. [23]		0.000207	138/k
15	Ref. [7]		0.009	

In the above equation p_i denote the selected sample at i_{th} position and q_i denote the corresponding adjacent sample. We examine the proposed scheme over correlation coefficient analysis. Mostly correlation analyses of the data are measured in multiple directions such as vertical horizontal and diagonal direction. Since in the audio the data are distributed in a single string, so we analyzed the correlation analysis of the proposed scheme in the horizontal direction, the result is listed in Table 3. From the table it is observed that the value of the correlation analysis of the original audio is equal to 1, it means the segments in the audio data are strongly correlated. However, the value of the correlation analysis of the ciphered audio is approximately equal to 0, i.e., the proposed scheme systematically interrupts the correlation of the audio segment. Besides, the correlation analysis of the original and the encrypted audio file is shown in Fig. 7. Fig demonstrates that the proposed scheme steadily reduced the intercorrelation of the audio file. Thus, the proposed scheme is well secure against the statistical attacks.

5.4 Information entropy

The information entropy analysis is utilized to measure the rate of uncertainty in the ciphered data. The rate of uncertainty is directly proportional to the value of the entropy; the higher value of entropy reflects the higher uncertainty in the encrypted audio file. The mathematical form of the information entropy analysis is given as follows.

$$H = -\sum_{k=0}^{\mathcal{L}} \mathcal{P}(k) log_2 \mathcal{P}(k) \tag{36}$$

Where $\mathcal{L}$ indicates the grayscale of the audio file and $\mathcal{P}(k)$ signifies the probability of the appearance of the grey-value k. In this case, the theoretical value H corresponding to the audio file is 16. So, the cryptosystem considered to be well-secured if the information entropy value of the ciphered file is 16. We inspect the proposed scheme through information entropy analysis; the results are tabulated in Table 4. From the table one can notice that the information value of the proposed scheme is much closed 16 for all ciphered audio, thus the produced optimum uncertainty in the audio file, therefore the proposed algorithm is capable to resist entropy attack.

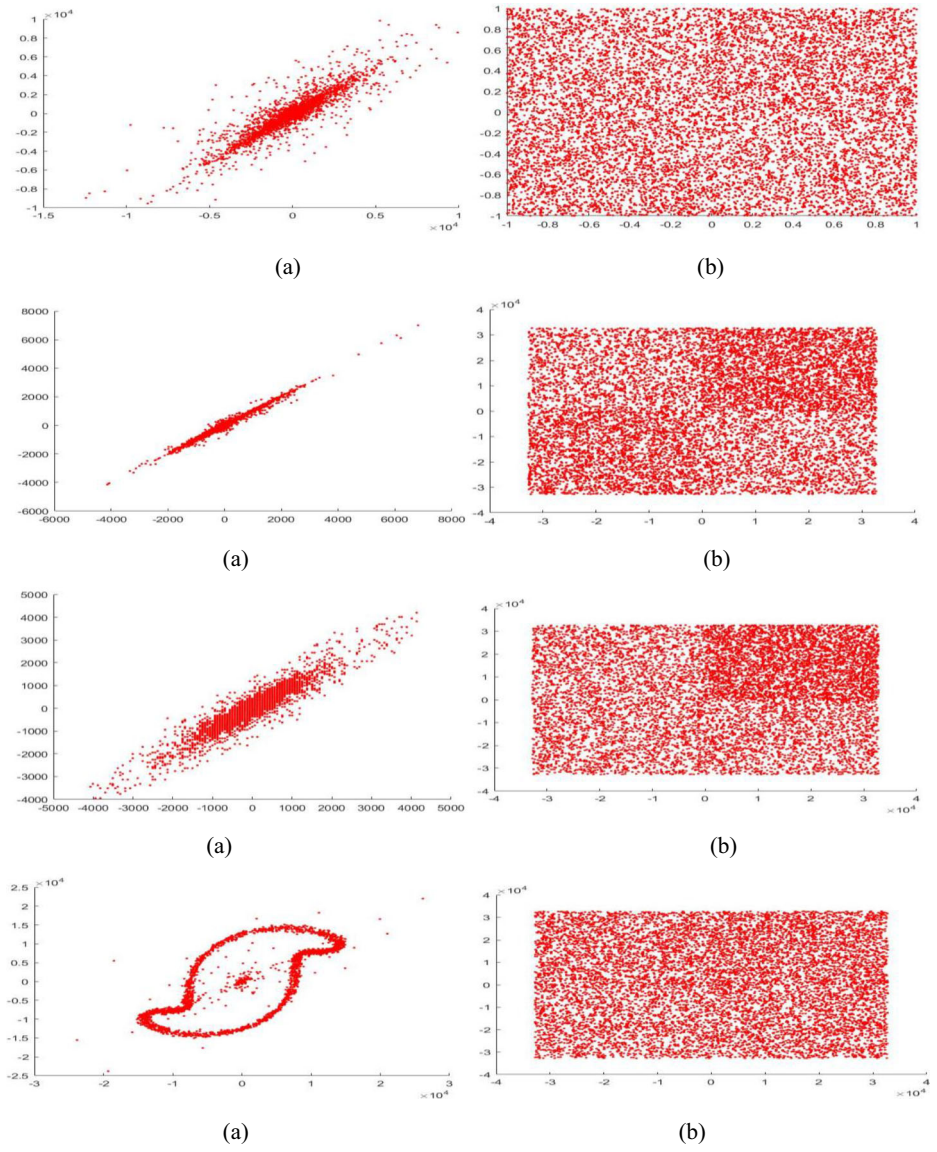


Fig. 7 Correlation analysis of man, female, birds and alarm sound (**a**) Correlation analysis of original audios (**b**) Correlation analysis of their corresponding encrypted audios

5.5 Differential attacks

The differential attacks consist of two analyses, the number of pixel change rates (NPCR) and Unified Average Changing Intensity (UACI) that are used to securitize the sensitivity of the cryptosystem. A proficient cryptographic algorithm should be sensitive so that the slight change in the plain data yields an enormous change in the cipher data. The NPCR and UACI

Table 4 Entropy analysis

No	Audio	Plain audio	Ciphered audio	Size
1	Animal sound.wav	8.0065	15.5010	530/Kilobyte
2	Alarm sound.wav	9.8183	15.6082	24,000 / Kilobyte
3	Applause sound. Wav	13.4401	15.8394	783/ Kilobyte
4	Bells sound. Wav	13.4216	15.9282	32,000/ Kilobyte
5	Birds sound.wav	4.5625	13.9179	307/ Kilobyte
6	Female sound.wav	8.5125	15.0125	32/ Kilobyte
7	44,100 Hz tone.wav	9.8134	15.7416	434/Kilobytes
8	Male sound.wav	10.6914	15.8720	345/Kilobytes
9	Machine sound.wav	14.1688	15.9891	26,000 /Kilobyte
10	Music sound.wav	14.8475	15.9981	11,000/Kilobyte
11	New intro sound.wav	14.8549	15.9877	900/Kilobyte

analysis are used to evaluate the sensitivity of the cryptosystem. The mathematical representation of NPCR and UACI is given as follows.

$$NPCR = \frac{\sum_{u,v} \mathcal{B}(u,v)}{K} \times 100 \tag{37}$$

In the equation () K symbolize the cardinality of the audio data set

$$\mathcal{B}(u,v) = \begin{cases} 1 & \text{if } \mathcal{A}_1(u,v) = \mathcal{A}_2(u,v) \\ 0 & \text{if } \mathcal{A}_1(u,v) \neq \mathcal{A}_2(u,v) \end{cases} \tag{38}$$

The mathematical equation of the UACI is given as follows:

$$UACI = \frac{1}{K} \sum_{u,v} \frac{|\mathcal{A}_1(u,v) - \mathcal{A}_2(u,v)|}{2^K - 1} \times 100 \tag{39}$$

In Eq. (28), the 2^K indicates the order of bit in the audio data set. An algorithm considered to be well-secured against different attacks, if the NPCR and UACI rate of the algorithm is approximately equal 100 and 33.3333 respectively. We evaluate the proposed audio encryption scheme over NPCR and UACI analysis, the resultant values are given in Table 5. The results of both analyses reveal that the proposed scheme is capable to resist the diverse attacks.

5.6 Asymptotic complexity and execution time

The asymptotic time complexity analysis of an algorithm theoretically estimates the running time of the algorithm to complete the execution. Usually, it is denoted by big oh $\mathcal{O}$. In this subsection, we discussed the asymptotic time complexity of the suggested encryption scheme. Since the first step of the scheme permute the audio data according to the random numbers, generated through chaotic maps. The permutation of each element requires constant time $\mathcal{O}(1)$, therefore the total asymptotic time complexity of the permutation step is $\mathcal{O}(M \times N)$, where $M \times N$ denote the dimension of the audio matrix. Similarly, in the substitution step S-box with constant number of elements has been used. Thus, the substitution of each element of the audio data takes constant time $\mathcal{O}(1)$. Consequently, the total time complexity of the substitution step is $\mathcal{O}(M \times N)$. Since,

Table 5 Differential analysis

No Audio		NPCR	UACI	Size
1	Animal sound.wav	99.98368	33.1233	530/Kilobyte
2	Alarm sound.wav	99.99611	33.456	24,000 / Kilobyte
3	Applause sound. Wav	99.99861	33.2203	783/ Kilobyte
4	Bells sound. Wav	99.98761	33.1202	32,000/ Kilobyte
5	Birds sound.wav	99.99484	33.1344	307/ Kilobyte
6	Female sound.wav	99.99576	33.9205	32/ Kilobyte
7	44,100 Hz tone.wav	99.99654	31.6479	434/Kilobytes
8	Male sound.wav	99.99728	33.74039	345/Kilobytes
9	Machine sound.wav	99.99652	33.0987	26,000 /Kilobyte
10	Music sound.wav	99.98916	33.67.8	11,000/Kilobyte
11	New intro sound.wav	99.98921	33.6345	900 /Kilobyte
13	Ref. [26]	99.9972	-	98.6/k
14	Ref. [17]	99.9996	-	138/k
15	Ref. [23]	99.9992	-	138/k
16	Ref. [7]	99.9989	33.3421	
17	Ref. [9]	99.6521	33.2122	

the complexity of each step of the encryption algorithm is the same, therefore the complexity of the overall encryption procedure is linear that is $\mathcal{O}(M \times N)$. To figure out the execution time of the encryption scheme, we implemented the scheme in Matlab 2019b running on personal computer Window 10, 64-bit operating system. The computer is equipped with processer Inter(R) Core (TM) -i7-5600U CPU @ 2.60 GHz and 16 GB Ram. The execution time of the encryption of different audio having different character is listed in Table 6.

5.7 Peak signal to noise ratio

Peak signal to noise ratio is a phenomenon that mainly related to the quality of the data after decryption using cypto-algorithems. The PSNR score between original audio A and encrypted audio A', in decibel(db), is then calculated by computing the ratio between the maximum possible pixel value and corrupted noise value. In addition, the higher score of PSNR is enough indication of efficiency of an encryption algorithm. The PSNR is defined via mathematical expression as

Table 6 Execution time

No audio		Time/ Sec	Size
1	Animal sound.wav	1.2300	530/Kilobyte
2	Alarm sound.wav	4.653	24,000 / Kilobyte
3	Applause sound. Wav	1.456	783/ Kilobyte
4	Bells sound. Wav	6.341	32,000/ Kilobyte
5	Birds sound.wav	0.612	307/ Kilobyte
6	Female sound.wav	0.015	32/ Kilobyte
7	44,100 Hz tone.wav	0.987	434/Kilobytes
8	Male sound.wav	0.832	345/Kilobytes
9	Machine sound.wav	5.123	26,000 /Kilobyte
10	Music sound.wav	2.091	11,000/Kilobyte
11	New intro sound.wav	1.896	900 /Kilobyte

Table 7 PSNR and MSE analysis

No audio		PSNR	MSE	Size
1	Animal sound.wav	10.5780	3.2456×10^{04}	530/Kilobyte
2	Alarm sound.wav	10.5301	3.2645×10^{04}	24,000 / Kilobyte
3	Applause sound. Wav	10.6864	3.2645×10^{04}	783/ Kilobyte
4	Bells sound. Wav	10.9876	3.5231×10^{04}	32,000/ Kilobyte
5	Birds sound.wav	10.7701	3.2631×10^{04}	307/ Kilobyte
6	Female sound.wav	10.7921	3.2646×10^{04}	32/ Kilobyte
7	44,100 Hz tone.wav	8.4426	3.2640×10^{04}	434/Kilobytes
8	Male sound.wav	10.7677	3.2645×10^{04}	345/Kilobytes
9	Machine sound.wav	10.5099	3.2649×10^{04}	26,000 /Kilobyte
10	Music sound.wav	10.1054	3.2646×10^{04}	11,000/Kilobyte
11	New intro sound.wav	9.7890	3.2646×10^{04}	900 /Kilobyte

$$PSNR = 20 \cdot \log_{10}\left(\frac{255}{(MSE)^{1/2}}\right)$$

where

$$MSE = \frac{1}{M \times N} \sum_{i=0}^{M} \sum_{j=1}^{N} \left[I(i,j) - I'(i,j)\right]^2$$

where $A(i,j)$ and $A'(i,j)$ are the pixel values of the original and the encrypted audio respectively. The PSNR and MSE result of proposed encryption scheme is listed in Table 7. The results demonstrate that the proposed scheme has low PSNR values and high MSE.

5.8 NIST statistical test

In this section, we analyzed the sequence of the random number, which is generated by the proposed random number generator scheme to evaluate the random number generator for cryptographic applications. To test the randomness of the generated sequence, we convert the sequence into binary, because NIST test is applicable for binary data. The NIST statistical test consists of sixteen tests method tabulated in Table 8. It can be observed from the table that the generated sequence passed the entire randomness test, which evidence that the proposed scheme generates good quality random sequences that are appropriate for audio encryption application.

6 Conclusion

This paper introduced a three-dimensional chaotic map and its applications to audio encryption applications. In the first part of the paper, we presented a three-dimensional chaotic map. The map is evaluated through phase plots and bifurcation diagrams. We further use the suggested chaotic maps and design a novel audio encryption scheme. The chaotic sequences are used to shuffle the data of the plain audio to achieve the diffusion property. In the confusion module, initially, the permuted fifteen-bit integers block is dived into two subblocks, consist of eight-bit integers and seven-bit integers. Besides,

Table 8 NIST randomness test for cryptographic applications

No	Type of test		*P* value	Conclusion
1	Frequency Test (Monobit)		0.9253077508893466	Random
2	Frequency Test within a Block		0.347578425321557	Random
3	Run Test		0.45321310856174435	Random
4	Longest Run of Ones in a Block		0.43428142438827533	Random
5	Binary Matrix Rank Test		0.7454887332471692	Random
6	Discrete Fourier Transform (Spectral) Test		0.12497609962873209	Random
7	Non-Overlapping Template Matching Test		0.622298646456104	Random
8	Overlapping Template Matching Test		0.1716767122905817	Random
9	Maurer's Universal Statistical test		−1.0	Random
10	Linear Complexity Test		0.4812517437344084	Random
11	Serial test:		0.10591374411110245	Random
			0.013298006380999879	Random
12	Approximate Entropy Test		0.05546464072097093	Random
13	Cummulative Sums (Forward) Test		0.9649804508015285	Random
14	Cummulative Sums (Reverse) Test		0.9921805530466228	Random
15	Random Excursions Test:			
	State	Chi Squared	P Value	Conclusion
	−4	4.231459930911139	0.5165952795839326	Random
	−3	1.7332705882352937	0.8846818589822677	Random
	−2	4.758896151053014	0.4460076827348852	Random
	−1	5.110294117647058	0.4025686933278576	Random
	1	3.360294117647059	0.6446240816842567	Random
	2	4.065904139433551	0.5399669541380107	Random
	3	5.608141176470588	0.34623345685245316	Random
	4	3.5139157703897883	0.6212830486499479	Random
16	Random excursions variant test:			
	State	Count	P- Value	Conclusion
	−9.0	197	0.4354513954635062	Random
	−8.0	187	0.3467223774673953	Random
	−7.0	193	0.34751940774812573	Random
	−6.0	195	0.3195447712837526	Random
	−5.0	227	0.5201464362953949	Random
	−4.0	251	0.7336253801663413	Random
	−3.0	248	0.645387747869369	Random
	−2.0	259	0.5772743837452569	Random
	−1.0	291	0.41529084384812753	Random
	+1.0	334	0.12485048506719687	Random
	+2.0	353	0.12039826619568533	Random
	+3.0	337	0.29218929257880555	Random
	+4.0	326	0.4402662823371424	Random
	+5.0	303	0.6886093783541819	Random
	+6.0	285	0.8771471277417655	Random
	+7.0	278	0.9470425588556117	Random
	+8.0	270	0.9834073848505813	Random

the Möbius transformation deployed that generate good quality 8 × 8 and 7 × 7 S-boxes. The S-boxes are then used to substitute the block of eight-bit integers and seven-bit integers, which produce optimum confusion in ciphered blocks. The simulation demonstrates that the proposed encryption successfully encrypts the audio and converts it into an unrecognizable uniform sound. Moreover, the scheme is scrutinized against various attacks, the performance result determines that the proposed encryption scheme exhibits better resistance to statistical and differential attacks.

References

1. Arshad U et al (2019) An efficient image privacy scheme based on nonlinear chaotic system and linear canonical transformation. Physica A: Statistical Mechanics and its Applications:123458
2. Arshad U et al (2019) An efficient image privacy scheme based on nonlinear chaotic system and linear canonical transformation. Physica A: Statistical Mechanics and its Applications:123458
3. Bhargava B, Shi C, Wang S-Y (2004) MPEG video encryption algorithms. Multimed Tools Appl 24(1):57–79
4. Conrad E (1997) Advanced encryption standard. White Paper
5. Farah MAB, Kachouri A, Samet M (2011) Improvement of cryptosystem based on iterating chaotic map. Commun Nonlinear Sci Numer Simul 16(6):2543–2553
6. Farah MAB et al (2020) A new design of cryptosystem based on S-box and chaotic permutation. Multimed Tools Appl:1–22
7. Farsana FJ, Devi VR, Gopakumar K (2019) An audio encryption scheme based on fast Walsh Hadamard transform and mixed chaotic keystreams. Applied Computing and Informatics
8. Grangetto M, Magli E, Olmo G (2006) Multimedia selective encryption by means of randomized arithmetic coding. IEEE Trans Multimed 8(5):905–917
9. Habib Z, (2017) Secure speech communication algorithm via DCT and TD-ERCS chaotic map. 4th international conference on electrical and electronic engineering (ICEEE). IEEE, 2017.
10. Haider MI, et al. (2020) Block cipher's nonlinear component design by elliptic curves: an image encryption application. Multimed Tools Appl: 1–26.
11. Hussain, Sadam, et al. (2020) A power associative loop structure for the construction of non-linear components of block cipher. IEEE Access
12. Jahangir S, Shah T (2020) Designing S-boxes triplet over a finite chain ring and its application in RGB image encryption. Multimed Tools Appl 79:26885–26911
13. Kalpana M, Ratnavelu K, PagavathiBalasubramaniam (2019) An audio encryption based on synchronization of robust BAM FCNNs with time delays. Multimed Tools Appl 78(5):5969–5988
14. Khan M, Masood F (2019) A novel chaotic image encryption technique based on multiple discrete dynamical maps. Multimed Tools Appl 78(18):26203–26222
15. Khan M, Hussain I, Jamal SS, Amin M (2019) A privacy scheme for digital images based on quantum particles. Int J Theor Phys 58(12):4293–4310
16. Kordov K (2019) A novel audio encryption algorithm with permutation-substitution architecture. Electronics 8(5):530
17. Lima JB, da Silva Neto EF (2016) Audio encryption based on the cosine number transform. Multimed Tools Appl 75(14):8403–8418
18. Lima JB, da Silva EF, Neto (2016) Audio encryption based on the cosine number transform. Multimed Tools Appl 75(14):8403–8418
19. Madain A, Abu Dalhoum AL, Hiary H, Ortega A, Alfonseca M (2014) Audio scrambling technique based on cellular automata. Multimed Tools Appl 71(3):1803–1822
20. Min L, et al. (2013) A novel 3 dimensional chaotic system and design of pseudorandom number generator. Ninth International Conference on Computational Intelligence and Security. IEEE, 2013.
21. Mosa E et al (2011) Chaotic encryption of speech signals. Int J Speech Technol 14(4):285
22. Naseer Y, Shah D, Shah T (2019) A novel approach to improve multimedia security utilizing 3D mixed chaotic map. Microprocess Microsyst 65:1–6
23. Naskar PK, Paul S, Nandy D, Chaudhuri A (2019) DNA encoding and channel shuffling for secured encryption of audio data. Multimed Tools Appl 78(17):25019–25042
24. Rivest RL (1994) The RC5 encryption algorithm. International Workshop on Fast Software Encryption. Springer, Berlin, Heidelberg
25. Sathiyamurthi P, Ramakrishnan S (2017) Speech encryption using chaotic shift keying for secured speech communication. EURASIP Journal on Audio, Speech, and Music Processing 2017(1):1–11
26. Sathiyamurthi P, Ramakrishnan S (2017) Speech encryption using chaotic shift keying for secured speech communication. EURASIP Journal on Audio, Speech, and Music Processing 1(2017):20
27. Servetti A, De Martin JC (2002) Perception-based partial encryption of compressed speech. IEEE Trans Speech Audio Process 10(8):637–643
28. Servetti A, Testa C, De Martin JC (2003) Frequency-selective partial encryption of compressed audio. IEEE International Conference on Acoustics, Speech, and Signal Processing, 2003. Proceedings.(ICASSP'03).. Vol. 5. IEEE

29. Shah T, Shah D (2019) Construction of highly nonlinear S-boxes for degree 8 primitive irreducible polynomials over $\mathbb{Z}$ 2. Multimed Tools Appl 78(2):1219–1234
30. Shah D, Shah T (2020) Binary Galois field extensions dependent multimedia data security scheme. Microprocess Microsyst 103181
31. Shah T, Haq TU, Farooq G (2020) Improved SERPENT algorithm: design to RGB image encryption implementation. IEEE Access 8:52609–52621
32. Standard, Data Encryption (1977) Federal information processing standards publication 46. National Bureau of Standards, US Department of Commerce 23
33. Thorwirth NJ, et al. (2000) Security methods for MP3 music delivery. Conference Record of the Thirty-Fourth Asilomar Conference on Signals, Systems and Computers (Cat. No. 00CH37154). Vol. 2. IEEE
34. Ul Haq T, Shah T (2020) 12× 12 S-box design and its application to RGB image encryption. Optik:164922
35. Ullah A, Jamal SS, Shah T (2018) A novel scheme for image encryption using substitution box and chaotic system. Nonlinear Dynamics 91(1):359–370
36. Ullah A, Javeed A, Shah T (2019) A scheme based on algebraic and chaotic structures for the construction of substitution box. Multimed Tools Appl 78(22):32467–32484
37. Waseem HM, Khan M, Shah T (2018) Image privacy scheme using quantum spinning and rotation. Journal of Electronic Imaging 27(6):063022
38. Waseem HM, Alghafis A, Khan M (2020) An efficient public key cryptosystem based on dihedral group and quantum spin states. IEEE Access 8:71821–71832
39. Yan W-Q, Wei-Gang F, Kankanhalli MS (2008) Progressive audio scrambling in compressed domain. IEEE Transactions on Multimedia 10(6):960–968
40. Zhou J, Au OC (2010) Security and efficiency analysis of progressive audio scrambling in compressed domain. IEEE International Conference on Acoustics, Speech and Signal Processing. IEEE, 2010.
41. Zimmermann R, Curiger A, Bonnenberg H, Kaeslin H, Felber N, Fichtner W (1994) A 177 Mb/s VLSI implementation of the international data encryption algorithm. IEEE J Solid State Circuits 29(3):303–307