Int. j. inf. tecnol. (August 2021) 13(4):1463–1471
https://doi.org/10.1007/s41870-021-00714-x

ORIGINAL RESEARCH

A novel audio encryption method using Henon–Tent chaotic pseudo random number sequence

Subhajit Adhikari[1] · **Sunil Karforma**[2]

Received: 20 November 2020 / Accepted: 18 May 2021 / Published online: 15 June 2021

Abstract Encryption algorithms based on chaos theory are frequently used due to the sensitivity of initial conditions, control parameters, and pseudo-randomness. They are very useful for data encryption for images, audio, or videos. In this paper, a novel audio encryption method is proposed to provide information security. Firstly, the one-dimensional uncompressed 16-bit audio file of even length is taken. Then chaotic Henon map and tent map is XORed to create the pseudo-random number sequence as the secret key. Next, the secret key is XORed with the original audio file to produce a cipher audio file. The encrypted audio file can be used for the e-learning process to create an audio password that can be used as login credentials instead of an invitation link. Security analysis shows that our encryption method is better than other existing methods in many aspects with less time.

Keywords Audio encryption · Chaotic tent map · Henon map · E-learning · Security · Spectrogram · Correlation · Entropy · SNR · NSCR

✉ Subhajit Adhikari
subhajit15dec@gmail.com

Sunil Karforma
sunilkarforma@yahoo.com

[1] Department of Computer Application, Dinabandhu Andrews Institute of Technology and Management, Kolkata, WB, India

[2] Department of Computer Science, The University of Burdwan, Burdwan, WB, India

1 Introduction

In today's world, protecting multimedia data against unauthorized access is very much needed [1]. E-learning comprises multimedia data like text, audio, and video. Security threats in e-learning may be unauthorized access to information, stealing personal information, and tracking online activity. So, there is a need to provide information security for multimedia data. Encryption is one of the methods of cryptography, frequently used to provide information security. Symmetric-key approaches like AES, DES, IDES, and 3DES are widely used in cryptography. But AES is not applicable for multimedia data security due to strong correlation, redundancy, and public data with the degraded performance of encryption. In this paper, a novel audio encryption method is proposed with a new Henon–Tent chaotic pseudo-random number generation algorithm. The symmetric key cryptographic approach is used, where the random number sequence acts as a secret key. The secret key is generated both at the sender and receiver's end. In the encryption phase, the xor operation is performed between the original audio file data and the random number sequence to create the cipher audio file. The cipher audio file is decrypted with the same random number sequence in the decryption phase. The encrypted audio file can be used in many e-learning processes instead of invitation links as an audio password. The statistical analysis is also performed. The encryption and decryption time of the audio file is very less compared to others. There are some advantages of our proposed audio encryption method. The encrypted audio file has a uniform spectrogram and histogram with a large keyspace to resist brute force attacks and statistical attacks. The values of the correlation coefficient indicate no dependency between original and cipher audio data values. The entropy is also high. The negative values of SNR and low values of PSNR represent powerful encryption and the presence of a high level of noise respectively. The high value of NSCR proves our method is resistant against differential attacks. The audio password will provide better security than invitation links to join any online activity for the e-learning process.

2 Preliminaries

Chaos theory represents complex nature and unpredictability with small initial values and control parameters [2, 3]. Chaotic tent map [4, 5] is piecewise linear and continuous map with a unique maximum and the equation is given below.

$$x_{i+1} = \begin{cases} \mu * x_i & \text{if } x_i < 0.5 \\ \mu * (1 - x_i) & \text{otherwise} \end{cases} \mu \in (0,2) \text{ and } x \in (0,1) \tag{1}$$

We take the value of $\mu \in [1, 2]$ and the initial value of x_0=0.4. The henon map is one of the utmost studied examples of the dynamical systems [6, 7] and can be written as

$$x_{n+1} = 1 - a \times x_n^2 + y_n \, , \, y_{n+1} = b \times x_n \tag{2}$$

The values of a and b are set to 1.4 and 0.3. The initial point x_0, y_0 is set to (0.1, 0.3). The 2D Henon map and 1D Tent map are used in our encryption method to generate the pseudo-random number sequence.

3 Literature review

A chaotic system with both the confusion and diffusion technique is proposed to encrypt the dual-channel audio data with a one-time key. The method has a large keyspace to prevent brute force attacks [8]. The cosine number transformation has already been applied to non-compressed 16-bit audio data block by block and to create a secret key [9]. A novel combining henon and economic maps is used to create the sequence. The confusion and diffusion technique are repeatedly applied to plain audio data to compute cipher audio data [10]. DNA coding and chaotic system has also been used for confusion and diffusion of audio data. The hash value of audio is used to compute the initial value of the chaotic system [11]. In a new encryption approach, the audio signal is converted into data using a lifting wavelet scheme. Then it is encrypted using a chaotic dataset and hyperbolic function [12].

The concept of block cipher and chaotic maps are used for .wav file encryption block by block. A chaotic tent map is used in the permutation step. Then the obtained block XORed with a key block. The resultant block is substituted with the multiplication inverse-based method of substitution [13]. A new method of audio transmission is discussed with self-adaptive scrambling, chaotic maps, DNA coding, and cipher feedback mechanism. Five different chaotic maps with eight control parameters are combined and used to create a pseudo-random number [14]. An encryption algorithm for audio data is proposed where the chaotic circle map and modified rotation equations are used to generate the pseudo-random number [15]. An audio encryption method is proposed with the help of the permutation of audio samples using a discrete modified Henon map followed by substitution operation. The keystream is obtained from the modified Lorenz-Hyperchaotic system. Different quality metrics are implemented to evaluate the quality of the encryption algorithm [16].

A novel method of encryption of the speech signal is discussed using multiple chaotic maps and cryptographic protocols. In the scrambling process, the input signal is divided into four segments using a cubic map. To secure all the parameters of chaotic maps, the blowfish algorithm is used with the private key. Hashing algorithm for authentication of shared data and the blowfish key of the system is implemented between sender and receiver's ends. The message digest is used for secure communication providing authentication and verification of the parameters of chaotic maps. Several statistical tests are carried out to prove the method's efficiency [17]. A new multiuser speech encryption method has been done using a chaos-based cryptosystem. The Chua chaotic systems are implemented to the transmitters and receiver to produce the chaotic encryption and decryption keys. The chaotic matrix operation for randomization and XOR operation are combined to encrypt the speech signal. The security analysis shows the sensitivity to the secret keys, large keyspace to resist the brute-force attack. The lifetime of the battery of the transmitter has been increased by the strong diffusion and confusion mechanisms [18]. A new scheme of audio encryption has been studied with a substitution-permutation algorithm using DNA encoding. The key generation of uses a key chaining mode, that produces a new key block for every plain block using the chaotic logistic map. Several security attacks are performed to evaluate the system. The chosen ciphertext, the chosen plaintext attacks, and a cycle attack are successfully demonstrated [19].

4 Henon–Tent pseudo random number generation algorithm

The new Henon–Tent pseudo random number generation algorithm is given below.

```
Step 1.  Read the audio signal and save it to audiodata
Step 2.  Compute the size of the audio signal and save it to an variable s
Step 3.  If s%2 == 0 then
Step 4.  Read the parameters a = 1.3, b = 0.3, X_new = 0.1, Y_new = 0.3 and Initialize two lists X_list = [], Y_list = []
Step 5.  Loop i = 0 to s/2
Step 6.  X_new,Y_new = HenonMap (X_new,Y_new)
Step 7.  X_list.append (X_new) and Y_list.append(Y_new)
Step 8.  End Loop
Step 9.  Save list C_list = X_list+Y_list
Step 10. Compute C_list = C_list × $10^5$ and convert into to integer sequence and Save C_list to HenonSeq.
Step 12. Else
Step 13. Go to step 1
Step 14. End If
Step     15. Read parameters r = 1.0,rmax = 2.0, rstep = 0.001, x = 0.4,k, Initialize float array TentSeq and integer
          array nTentSeq
Step 17. While k<s
Step 18. Loop
Step 19. x = TentMap(x,r)
Step 20. If r< =rmax then
Step 21. r = r+rstep
Step 22. Else
Step 23. r = 1.0
Step 24. TentSeq[k] = x
Step 25. End If
Step 26. End Loop
Step 27. TentSeq = TentSeq × max(audiodata)
Step 28. Convert TentSeq to integer sequence nTentSeq
Step 29. Compute MixSeq = HenonSeq XOR nTentSeq
Step 30. Stop.
```

The block diagram of this process is also given in Fig. 1.

5 Audio encryption and decryption algorithm

The encryption Algorithm has the following steps.

Step 1. Read the original audio file and save it to audiodata
Step 2. Read the pseudo random number sequence MixSeq
Step 3. Compute audiodata XOR MixSeq and Save it to CipherAudio
Step 4. Write CipherAudio to EncAudio.wav

The decryption Algorithm has the following steps.

Step 1. Read the EncAudio.wav file and save it to EncryptedAudiodata
Step 2. Read the pseudo random number sequence MixSeq
Step 3. Compute EncryptedAudiodata XOR MixSeq and Save it to DecipherAudioPassword
Step 4. Write DecipherAudio to original audio file

In the Fig. 2, the block diagram of encryption process and decryption process is given, where pseudo random numbers generated from mixed chaotic maps as secret key is used.

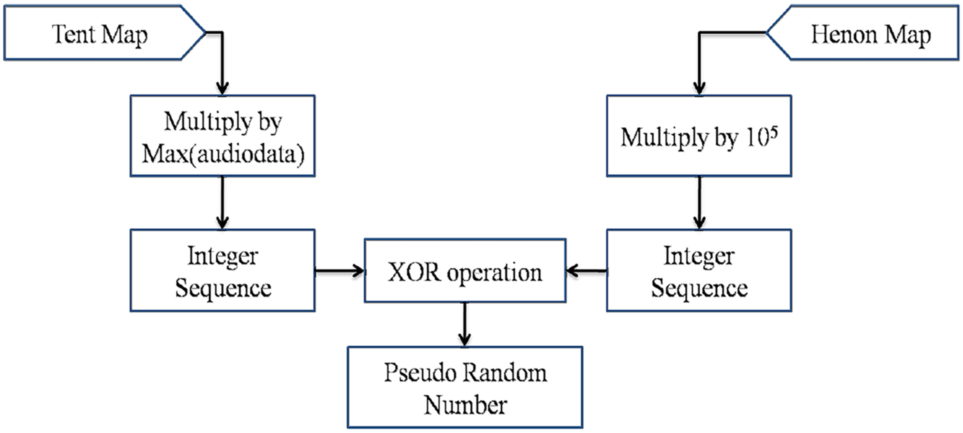

Fig. 1 Block diagram of pseudo random number generation using Henon–Tent map

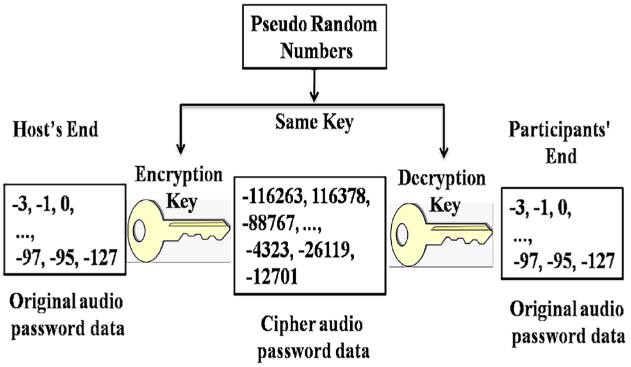

Fig. 2 Block diagram of encryption and decryption process

6 Simulation result and security analysis

Simulation is done in the software SageMath 8.0 and Matlab R2016b with 1.70 Ghz Intel processor having 4Gb RAM. The content of the 16-bit uncompressed audio files (.wav) are given in Table 1 [20, 21].

The recorded audio password_1.wav contains "154bca401". The security analysis of these audio password files are given in the next section.

6.1 Key space analysis

The keyspace is defined by initial values from Equations and represents all the possibilities. The keyspace is obtained from the equation (1) and (2) the number of changing variables is four. So, according to the IEEE floating-point standard, the precision of 64 bits double variables is about 10^{-15}. In our proposed algorithm, we have four double variables as μ,x_i,x_n,y_n and so the final keyspace is about $10^{60} \approx 2^{249.14461}$. This large keyspace represents our encryption method is secure against all types of brute force attacks.

6.2 Spectrogram analysis

A spectrogram is a visual representation of an audio file frequency spectrum varying with time and is used to analyze audio signals [14, 15]. If the spectrogram of the encrypted audio is uniform, the audio signals are successfully encrypted [6]. In our proposed method, the encrypted audio file has a uniform spectrogram. This means the original audio signals are successfully encrypted. The result is shown in Fig. 3.

6.3 Histogram analysis

The histogram analysis is used to compute the distribution of values and to measure the quality of encrypted speech signals [15, 16]. It is preferable to have an encrypted speech file consists of equally probable sample values to resist against statistical attacks It has been obtained from Fig. 4, that the histogram of the encrypted speech file is almost uniform, so our algorithm is secure against different statistical attacks.

6.4 Correlation

The correlation coefficient between two audio files represents the dependency between their sample values. If the values are in between $|0.3 - 0|$, it is considered as a weak correlation. Lower value of correlation represents good encryption method with desirable resistance properties [6].

$$\rho(A, B) = \frac{cov(A, B)}{\sigma_A \sigma_B} \qquad (3)$$

where $cov(A, B)$, σ_A and σ_B are the covariance and standard deviation between two audio files A and B respectively.

From the Table 2, It is found that the correlation coefficient values are close to zero or negative. So, there is no dependence between the original and encrypted files and

Table 1 Content of standard audio files

File	Content of the audio file
A_eng_f7.wav	"I see jewel cracked the strong defense.Grape juice and water mix well. Roads are paved with sticky tar. Fake stone shine but costs little"
A_eng_m7.wav	"Rice is often served in round bowls. The young kid jumped the rusty gate. I guess the results from the first scores. Assault pickled tastes fine with ham"
B_eng_f1.wav	"I was away for 9 weeks the dining room is lit by gas there were no vegetables left"
B_eng_m4.wav	"He was not in the mood for music. I can well understand your feelings. I have rented a small house"
gettysburg.wav	"4 score and 7 years ago our fathers brought forth on this continent a new nation conceived in liberty and dedicated to the proposition that all men are created equal now we are engaged in a great civil war testing whether that nation or any nation so conceived and so dedicated can long endure"

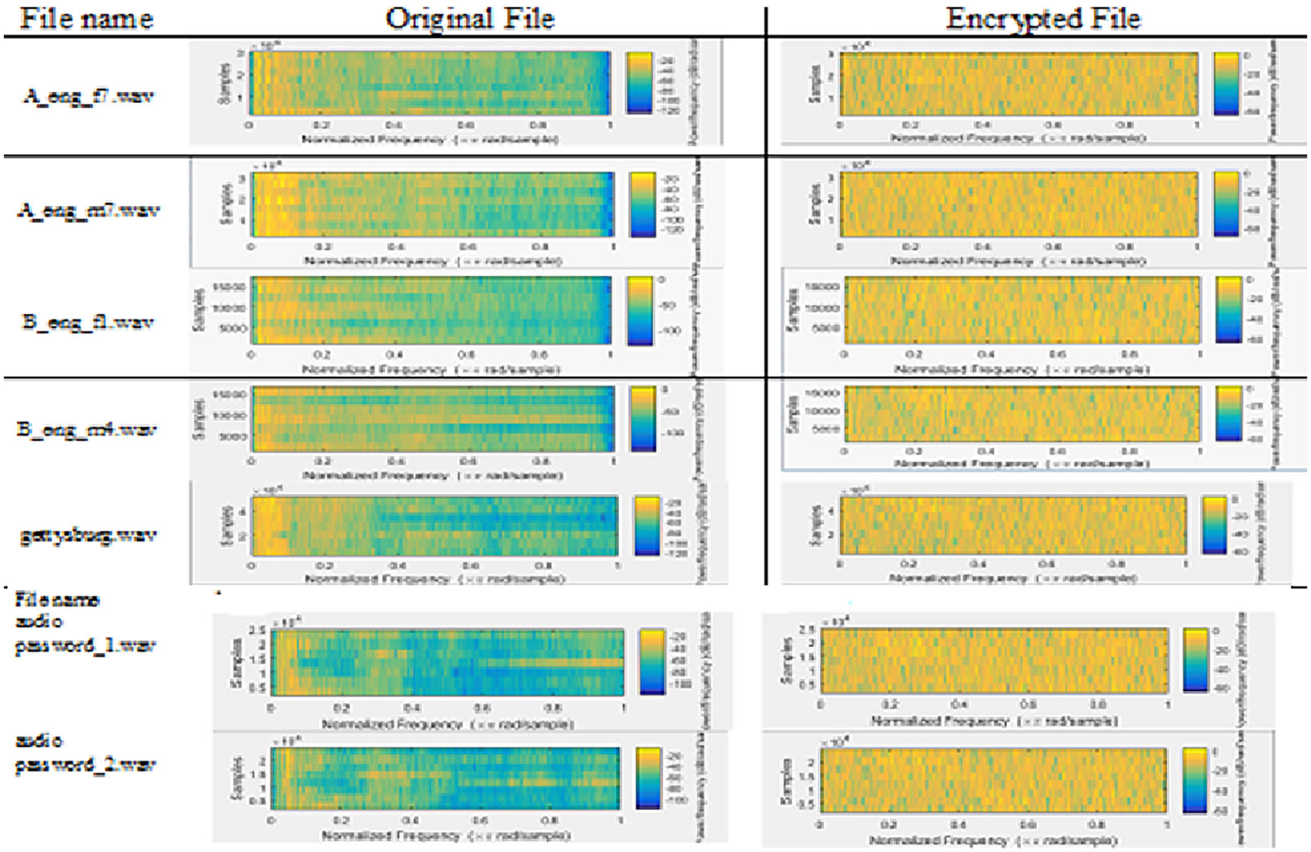

Fig. 3 Spectrogram of original and encrypted audio files

Fig. 4 Histogram of original and encrypted audio files

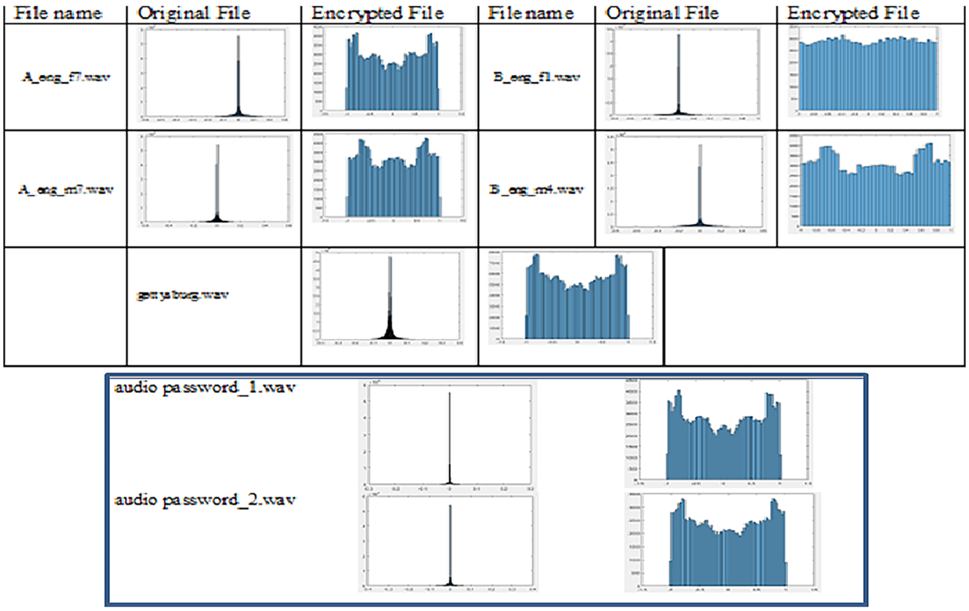

Table 2 Correlation analysis of standard audio files

File	File size (kb)	File length (sec)	Correlation coefficient
A_eng_f7.wav	395	0.12	0.0202
A_eng_m7.wav	426	0.13	0.0223
B_eng_f1.wav	255	0.07	0.0130
B_eng_m4.wav	247	0.07	0.0128
gettysburg.wav	757	0.17	0.0225
audio password_1.wav	368	0.11	0.0174
audio password_2.wav	321	0.10	0.0245

Table 3 SNR of standard audio files

File	File size (kb)	File length (sec)	SNR (dB)
A_eng_f7.wav	395	0.12	– 22.0270
A_eng_m7.wav	426	0.13	– 20.6805
B_eng_f1.wav	255	0.07	– 14.9909
B_eng_m4.wav	247	0.07	– 16.3453
gettysburg.wav	757	0.17	– 24.5799
audio password_1.wav	368	0.11	– 29.9476
audio password_2.wav	321	0.10	– 26.5632

our encryption scheme is a good encryption scheme with the desirable resistant property.

6.5 Signal to noise ratio

Signal to noise ratio (SNR) determines the quality of the signals. It is also used to validate the encryption algorithm’s performance [16]. The algorithm is more powerful if it has a more negative value of SNR [14]. For this test, we need both plain and encrypted audio files to calculate the SNR as follows: where x_i and y_i are corresponding sample values from audio files, and n is the number of samples.

$$SNR = 10\log_{10}\frac{\sum_{i=1}^{n} \times {x_i}^2}{\sum_{i=1}^{n}[x_i - y_i]}(dB) \tag{4}$$

Table 4 entropy of standard audio files

File	Original	Encrypted
A_eng_f7.wav	2.2661	5.0058
A_eng_m7.wav	2.3874	5.0087
B_eng_f1.wav	2.8572	5.0155
B_eng_m4.wav	2.6307	4.9815
gettysburg.wav	2.2801	4.9650
audio password_1.wav	1.1496	4.9795
audio password_2.wav	1.3697	4.9832

From the Table 3, it is clear that our proposed method gives negative values of SNR, so our method is very powerful encryption method.

6.6 Information entropy

The information entropy analysis finds the degree of uncertainty. The higher entropy value is desired to prevent statistical attacks [6, 13]. The equation of entropy is used to calculate the entropy value of the encrypted audio files [22], where peakval is the maximum value of the audio data and p_i is the probability of the occurrence of value i.

$$entropy = -\sum_{i=1}^{peakval}(p(i)\log_2(p(i))) \tag{5}$$

From the Table 4, it is clear that the encrypted file has more entropy value, so the file is protected from any statistical attack.

6.7 Peak Signal to Noise Ratio

Peak Signal to Noise Ratio (PSNR) is used to calculate the power of clean signals concerning the power of noise. The decreased values of PSNR are desired indicating the high level of noise in the encrypted audio files to resist any attacks [14]. PSNR is calculated as follows:

$$PSNR = 10\log_{10}(\frac{peakval^2}{MSE}), MSE = \frac{1}{n}\sum_{i=1}^{n}(a[i]] - b[i]])^2 \tag{6}$$

Table 5 PSNR of standard audio files

File	File size (kb)	File Length (sec)	PSNR (db)
A_eng_f7.wav	395	0.12	4.2145
A_eng_m7.wav	426	0.13	4.5392
B_eng_f1.wav	255	0.07	4.6771
B_eng_m4.wav	247	0.07	4.4761
gettysburg.wav	757	0.17	4.2766
audio password_1.wav	368	0.11	4.2247
audio password_2.wav	321	0.10	4.2896

Table 6 NSCR of standard audio files

File	File size (kb)	File length(sec)	NSCR(%)
A_eng_f7.wav	395	0.12	99.9995062021
A_eng_m7.wav	426	0.13	99.9981685149
B_eng_f1.wav	255	0.07	99.9991353221
B_eng_m4.wav	247	0.07	99.9976303318
gettysburg.wav	757	0.17	99.9994839695
audio password_1.wav	368	0.11	99.999470339
audio password_2.wav	321	0.10	99.9987864078

Table 7 Encryption time of standard audio

File	File size (kb)	File length (sec)	Encryption time (sec)
A_eng_f7.wav	395	0.12	0.003
A_eng_m7.wav	426	0.13	0.005
B_eng_f1.wav	255	0.07	0.003
B_eng_m4.wav	247	0.07	0.003
gettysburg.wav	757	0.17	0.007
audio password_1.wav	368	0.11	0.004
audio password_2.wav	321	0.10	0.003

Table 8 Encryption time of other audio files with ours

File	File size (kb)	File length (sec)	Encryption time (sec)
ours	368	0.11	0.004
Ref. [11]	127	4.6	4.572
Ref. [13]	332	–	42.45
Ref. [14]	156	57.11	21.1307
Ref. [15]	41.1	0.47	0.130
Ref. [23]	–	–	7.265394

Where peakval is the maximum possible value of audio stream and MSE is the mean square error between the plain and encrypted file and a and b represent the plain and encrypted audio file. From Table 5, it can be concluded that our encryption provides a lower psnr value for encrypted audio files, so a high level of noise is present. The algorithm is strong enough to resist any attacks.

6.8 Number of sample change rate

Number of sample change rate is used for the robustness of encryption algorithms. The test is done to compare sample values of the original and encrypted audio files in percents and the ideal value is 100%. In Eq. (7), N is the total number of samples, x_i and y_i are the corresponding sample values of the plain and encrypted files. The value of D_i is 1 when $x_i \neq y_i$ and 0 otherwise. From Table 6, we can say that the results demonstrate NSCR values are close to the ideal values. So, the proposed method has a high-security level.

$$NSCR = \frac{\sum_{i=1}^{N} D_i}{N} \times 100\% \tag{7}$$

Table 9 Security analysis of proposed audio encryption algorithm with others

Method	Keyspace	CC	SNR	PSNR	NSCR
Ours Method	2^{249}	0.0174	– 29.9476	4.2247	99.999
Ref. [6]	3.4764×10^{115}	0.0017	–	–	99.94041
Ref. [8]	3.4×10^{80}	0.0043	–	4.5299	–
Ref. [9]	2^{150}	0.0021	–	–	99.9992
Ref. [12]	$4.295 \times l_2 \times 10^{91}$	0.1578	–	–	–
Ref. [15]	2^{149}	– 0.004	– 16.0483	1.4524	100
Ref. [22]	–	0.0263	–	4.373	–
Ref. [23]	2^{144}	0.0092	–	–	–
Ref. [24]	2^{238}	– 0.0070	– 12.51	–	–

6.9 Speed and performance analysis

In Table 7, the encryption time in seconds of different audio files is depicted. The comparative study of the encryption time of other audio files with ours is given in Table 8. From Table 9, the comparative analysis proves our audio encryption method performs better than others concerning different security parameters.

7 Conclusion and future scope

In this paper, a novel audio encryption and decryption method has been discussed using the chaotic pseudo-random number as a secret key. From the experimental result, it can be concluded that the method is robust against all types of security attacks. In the future, the audio password can be used for login credentials in the e-learning process to provide information security. The different file formats like .mp3 for an audio password may be taken for further experiments. Elliptic curve cryptography may be implemented to exchange the secret key. The concept of the session of the audio password may be incorporated.

References

1. Sasikaladevi N, Geetha K, Srinivas KV (2018) A multi-tier security system (SAIL) for protecting audio signals from malicious exploits. Int J Speech Technol 21(2):319–332
2. Al-Shameri WFH, Mahiub MA (2013) Some dynamical properties of the family of tent maps. Int J Math Anal 7(29):1433–1449
3. Abdelfatah RI (2019) Secure image transmission using chaotic-enhanced elliptic curve cryptography. IEEE Access 8:3875–3890
4. Li C, Luo G, Qin K, Li C (2017) An image encryption scheme based on chaotic tent map. Nonlinear Dyn 87(1):127–133
5. Parvaz R, Zarebnia M (2018) A combination chaotic system and application in color image encryption. Opt Laser Technol 101:30–41
6. Shah D, Shah T, Jamal SS (2019) Digital audio signals encryption by Mobius transformation and Hénon map. Multimed Syst 26:1–11
7. Akgul A, Kacar S, Pehlivan I, Aricioglu B (2018) Chaos-based encryption of multimedia data and design of security analysis interface as an educational tool. Comp Appl Eng Educ 26(5):1336–1349
8. Liu H, Kadir A, Li Y (2016) Audio encryption scheme by confusion and diffusion based on multi-scroll chaotic system and one-time keys. Optik 127(19):7431–7438
9. Lima JB, da Silva Neto EF (2016) Audio encryption based on the cosine number transform. Multimed Tools Appl 75(14):8403–8418
10. Parvees MM, Samath JA, Bose BP (2018) Audio encryption-a chaos-based data byte scrambling technique. Int J Appl Syst Stud 8(1):51–75
11. Wang X, Su Y (2019) An audio encryption algorithm based on DNA coding and chaotic system. IEEE Access 8:9260–9270
12. Roy A, Misra AP (2017) Audio signal encryption using chaotic Hénon map and lifting wavelet transforms. Eur Phys J Plus 132(12):524
13. Albahrani EA (2017) A new audio encryption algorithm based on chaotic block cipher. In: 2017 Annual Conference on New Trends in Information & Communications Technology Applications (NTICT), pp 22–27 IEEE. https://doi.org/10.1109/NTICT.2017.7976129
14. Abdelfatah RI (2020) Audio encryption scheme using self-adaptive bit scrambling and two multi chaotic-based dynamic DNA computations. IEEE Access 8:69894–69907
15. Kordov K (2019) A novel audio encryption algorithm with permutation-substitution architecture. Electronics 8(5):530
16. Farsana, F.J., Devi, V.R. & Gopakumar, K., 2020. An audio encryption scheme based on Fast Walsh Hadamard Transform and mixed chaotic keystreams. App Comp Info. https://doi.org/10.1016/j.aci.2019.10.001
17. Kaur G, Singh K, Gill HS (2021) Chaos-based joint speech encryption scheme using SHA-1. Multimed Tools Appl 80(7):10927–10947
18. Hashemi S, Pourmina MA, Mobayen S, Alagheband MR (2021) Multiuser wireless speech encryption using synchronized chaotic systems. Int J Speech Technol. https://doi.org/10.1007/s10772-021-09821-3
19. El Hanouti I, El Fadili H (2021) Security analysis of an audio data encryption scheme based on key chaining and DNA encoding. Multimed Tools Appl 80(8):12077–12099
20. http://www.itu.int/net/itu-t/sigdb/genaudio/AudioForm-g.aspx?val=1000050. Accessed 4 June 2020

21. https://www2.cs.uic.edu/~i101/SoundFiles/. Accessed 24 Feb 2020
22. Tamimi AA, Abdalla AM (2014) An audio shuffle-encryption algorithm. In: The world congress on engineering and computer science WCECS 2014, 22–24 October, 2014, San Francisco, USA
23. Ghasemzadeh A, Esmaeili E (2017) A novel method in audio message encryption based on a mixture of chaos function. Int J Speech Technol 20(4):829–837
24. Hato E, Shihab D (2015) Lorenz and Rossler chaotic system for speech signal encryption. Int J Comp Appl 128(11):09758887