Journal of Theoretical and Applied Information Technology
31st August 2018. Vol.96. No 16
© 2005 – ongoing JATIT & LLS

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

AN EFFICIENT AUDIO ENCRYPTION BASED ON CHAOTIC LOGISTIC MAP WITH 3D MATRIX

[1]YUSSRA MAJID HAMEED, [2]NADA HUSSIEN M. Ali
[1]College of Science, University of Baghdad, Computer Science, Baghdad, Iraq
[2]College of Science, University of Baghdad, Computer Science, Baghdad, Iraq

E-mail: [1]yussra.majid@gmail.com, [2]nada_husn@yahoo.com

ABSTRACT

The widespread popularity of the Internet and the fast developments in computer technologies influence the expansion of electronic data exchange and digital communications. Consequently, digital audio communication is used in daily life activities such as banking, commerce, e-learning, military, education and politics. As a result, a huge amount of critical audio data is exchanged everyday over shared and open networks. In consequence of the rapid growth of data communications and digital audio, the issue of providing a high level of audio security becomes a foremost importance. Chaotic maps have been used recently in cryptography for large scale data encryption such as text, image, video and audio data, due to their strong properties such as sensitivity to changes in system control parameters and initial conditions, pseudo-randomness and aperiodicity. This paper has been presented a chaos-based audio confusion and diffusion system. A symmetric block audio encryption approach have been introduced, which is based on substitution and shuffling using chaotic logistic map with 3D-matrix. The confusion process is done by searches for positions of the audio symbols in 3D-matrix which is generated by chaotic logistic map system. Then, these symbols are replaced accordingly. Then the shuffle mechanism is done to the positions of the matrix depending upon the system key. Moreover, the resulting confused audio are prepared to diffusion mechanism which is achieved by the exclusive-or operation between random value and chaotic logistic map array. So, all of the cipher audio will get affected even if only one-bit of audio sample have been changed. The control parameters and initial conditions are extracted from the encrypted key, so the system is key sensitive. Further, Parity added to ensure integrity. Information theory of Shannon entropy test, NIST tests and security analysis show that the suggested scheme is secure and can be used in audio encryption.

Keywords: *Logistic Map, Chaotic Systems, Confusion, Diffusion, Block Cipher, 3D-Matrix, Shuffle, Encryption.*

1. INTRODUCTION

One of the most considerable needs of our world is a safe communication. Many studies on encrypt data types like text, images, audios and videos have been achieved in order to meet such need. The general goal of audio encryption is to inhibit the possession of data by undesired people. Nowadays, conversations in any place can easily be supervised with help of some certain technological devices. So, it has become a necessity to take many security reservations to protect such information. Although many encryption systems appear, it is generally accepted that they can still be decrypt the encrypted data with some techniques and in a certain amount of time. Therefore, complexity and other factors of algorithms used during encryption have become important in encryption process [13]. Also, traditional encryption algorithms are efficient in the texts only, they cannot be used as a security algorithms for a sensitive audio data because of the high redundancy and huge capacity of the audio data, thus, audio data needs strong cryptosystem algorithms before transmission. Therefore, producing efficient techniques of audio encryption that produce high security level are new challenges [6], [9-11].

Recently, number of encryption algorithms using chaotic systems has start increasing. Chaotic systems have become more public in encryption because they can successfully maintain security by achieving diffusion and confusion mechanisms through providing complexity and sensitivity to initial conditions [13].

Chaos systems are used in cryptography due to their sensitivity on control parameters and initial conditions, pseudorandom property, no periodicity, etc. Almost all of its properties fulfill the demands of cryptography (e.g. diffusion, confusion, etc.), Therefore, chaotic systems can provide a secure and fast means for data transmission over a rapid communication channel (e.g. the broadband internet communication) [11].

In 1998, a new symmetric block encryption In 1998, a new symmetric block encryption scheme was proposed by J. Fridrich [1] with 2-D chaotic map on a square or on a torus, this approach consist of three steps: the first step introduce parameters to generate the chaotic map system, the second step discretize the chaotic as a points of finite lattice that represent pixels and the last step extend the discretized chaotic map to 3D matrix with a simple diffusion mechanism. In 2004, a new system was proposed by G. Chen et al. [2], the position of image pixels is shuffled using 3D chaotic cat map, and then the relation between the cipher-image and original plain-image was confused by another chaotic map. In 2009, Patidar et al. [3] proposed a new system of lossless symmetric encryption based on the substitution and diffusion mechanisms which are employed chaotic standard and chaotic logistic maps. The number of iterations and the parameter of the chaotic map with the initial condition together compose the secret key of the algorithm. In 2010, Pareek et al. [5] produced a block cipher based on chaotic logistic and henon map, with a secret key. In this system, confusion and diffusion are accomplished with assistance of secret key (which depend on permutation boxes) and chain block ciphering. In 2011, Kanso et al. [4] suggested encryption system based on 3-dimentional chaotic map that can overcomes attacks. The system based on three phases to produce a strong and efficient encryption system comprising confusion and diffusion characteristics. In 2015, Elshamy et al. [6] presented cryptosystem based on a combination between chaotic map and optical encryption. The paper uses two security phases: chaotic system based on either cat or baker map and optical encryption with double random phase encoding (DRPE), respectively. In 2017, kumur et al. [7] proposed a new encryption algorithm based on confusion, diffusion and shuffling mechanisms. The algorithm uses 3D matrix, which it is generated using chaotic dynamical system with dependence on the key.

The paper structured is organized as follows: section 2 presents a general discussion of chaotic systems and logistic map while section 3 produces the proposed encryption algorithms with details of the 3D-matrix, shuffling engine and others whereas section 4 discusses the security analysis and results with a comparison with other works. Finally, section 5 summarizes the essential conclusions of the paper.

2. CHAOTIC SYSTEM

Chaotic system is any nonlinear deterministic and dynamic system that produce pseudo-random behavior. The chaotic systems output depends on initial conditions, and control parameters. i.e., different parameter or/and various initial conditions values produce various outputs. Chaotic systems are used in applications of cryptography and pseudorandom number generators due to their sensitivity to control parameter and initial conditions and their random-like behavior. As a result of these special properties, chaotic systems are able to achieve the cryptographic characteristics like disorder, confusion and diffusion [6].

Chaotic systems structure are highly complex, therefore, predict and analyze are difficult. Chaotic map with its different types have been used by researchers, and one of the most well-known among these maps is the logistic map [18-21]. The still existing systems of security which used chaotic maps can be divided into two different types: diffusion and permutation. In the permutation, samples of audio file locations in the plain audio are manipulated through chaotic system sequences or certain array transformations. The permutation algorithm shows a good encryption effect without altering samples values, therefore, the histograms of the encrypted and plain audio are similar of each other. As a result, the security of thus algorithms can be broken by statistical analysis. In the diffusion stage, the samples values of the plain audio are altered by chaotic system sequences. Diffusion may produce higher security than permutation, but encryption influence is poor, therefore, several researchers have gathered permutation and diffusion to increase encryption influence and secrecy. A one dimension chaotic map is used in audio encryption algorithms. But a single chaotic map may result in a low security and small key space [22], [24]. As a result, more than one dimensional chaotic systems are currently used by recent researches [23], [25], [27], [29]. The cipher audio of the encryption algorithm with a 3D map offer better balance and influence than that with a 2D map. The 3D also gives an avalanche effect. Moreover, 3D systems provide good security against cryptanalytic attacks [24-25], [28]. Therefore, in the current study, 3D logistic chaotic map are applied for the proposed algorithm.

2.1 Logistic Map

Logistic Map is a quite commonly used in chaotic system. Figure 1 displays bifurcation diagram that shows at which intervals logistic map enters chaos. Parameter (r) was examined between 0 and 4 values. Bifurcation diagram in Figure 1 shows that the control parameter (r) value must be chosen between 3.5699 and 4 so that the system can enter chaos (also see Figure 2). Otherwise, the system will not enter chaos and thus chaotic encryption will not be possible [8].

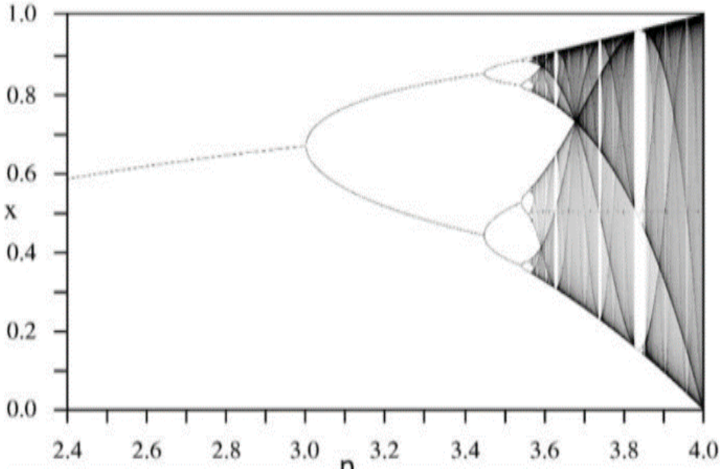


Figure 1 : Logistic Map System Become More Chaotic in Nature When the Control Parameter (r) Become Closer to 4.

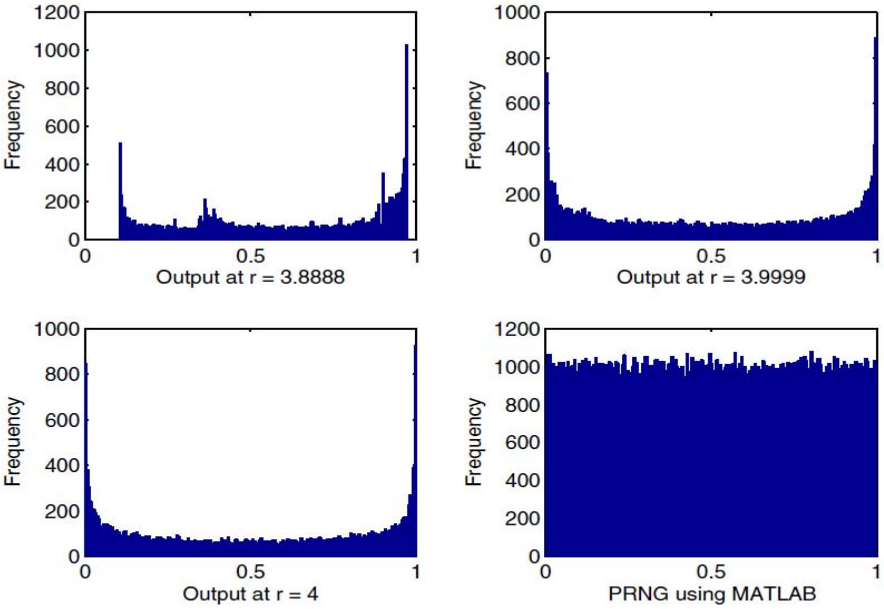


Figure 2 : Plot showing the histogram of values generated by the Logistic map with respect to different values of control parameter r. It is noticeable here that while the value of control parameter r is equal to or greater than 3.9999, the distribution is more uniform as compared to lower values of r. One can also notice the histogram of PRNG using MATLAB which is uniform as that of the logistic maps.

The logistic map is defined as following equation: [7], [12-13]:

$$x(n+1) = r * (x(n) * (1 - x(n))) \qquad (1)$$

3. PROPOSED SYSTEM

In this paper, encryption algorithm for audio file has been proposed by achieving confusion and diffusion based on a 3D-matrix chaotic map. The sequence of such systems depends on the sensitivity to the control parameters and initial conditions, i.e. the close starting points spread quickly and become un-related soon. Chaos match the Shannon requirements of diffusion and confusion. According to Shannon, confusion means that every bit on the cipher-text should depend on many parts of the key, concealing the relation between the two and make it as complex as possible and diffusion means that if only one bit (digit) of the plain file have been changed, statistically, half of the cipher should change, and vice versa, therefore, making the analysis so difficult. In the proposed method, substitution using 3D-matrix has achieved to produce the confusion, and then the diffusion process produced by applying exclusive-OR (XOR) to the confused plain audio with an initial value and then making a chaining cipher, i.e. if one bit of the plain audio or of the initial value changed, then all the cipher audio will be change.

3.1 Key and parameters generations

The proposed algorithm is key sensitive, i.e. if one bit of the key changed, all the cipher-audio will be changed because the key is used in all stages of the algorithm (e.g. 3D-matrix generation and shuffling engine). This adds robustness to the algorithm and make brute force difficult. The key of the proposed algorithm consist of 16-byte, sub-keys calculated from the key, each consist of 1 byte and their values range between 1 and 128. The sub-keys are used to calculate parameters and initial conditions of the algorithm. The sub-keys generated from the original key as follows:

$$k_i = ASCCI\ code\ (byte_i\ of\ key) \qquad (2)$$

Where i ranges from 0 to 15.

Now, parameters of the algorithm are generated, they are consist of logistic map conditions, scaling factors, selection condition of matrix size and iteration parameter required to generate matrix.

Logistic map initial conditions computed as follows:

$$x1(0) = ((k_0 \times k_4) + (k_5 + k_{15}))\ mod\ 1 \qquad (3)$$

$$x2(0) = ((k_2 \times k_8) + (k_9 + k_{14}))\ mod\ 1 \qquad (4)$$

$$x3(0) = ((k_6 \times k_{10}) + (k_5 + k_{11}))\ mod\ 1 \qquad (5)$$

Note that the length of arrays x1, x2 and x3 is equal to the wave data length.

Iteration of chaotic map first matrix generation are as follows:

$$ir = ((k_1 \times k_{11}) \times 2) + 200 \qquad (6)$$

Scaling factors are computed as following equations:

$$s1 = (k_{12} / k_8) \times (k_{15} \times k_{13}) + 113 \qquad (7)$$

$$s2 = (k_9 / k_6) \times (k_{10} \times k_{14}) + 117 \qquad (8)$$

$$s1 = (k_{13} / k_3) \times (k_1 \times k_{15}) + 131 \qquad (9)$$

Logistic map initial parameters used in matrix selection generated as follow:

$$im = (k_7 \times k_2 / (k_8 \times k_{10}))\ mod 1 \qquad (10)$$

$$m = \lceil ((4 \times im \times (1 - im)) \times s1) \rceil \mathrm{mod} 9 + 1 \qquad (11)$$

3.2 3D-Matrix

3.2.1 3D-Matrix properties

A 3D-matrix produced to replace the information by achieving shuffling mechanism of the element of matrix. The matrix shaped as a cubic as shown in Figure 3. Because of the audio file data ranges between (0-255) and to hold all of these data elements, the matrix would contain 256 position. The dimensions of the matrix would be one of the following: (8 x 8 x 4) or (8 x 4 x 8) or (4 x 8 x 8) sided 3D-matrix with 256 cells forms a perfect cubic. Audio file elements can now be positioned in as many as 256! ways.

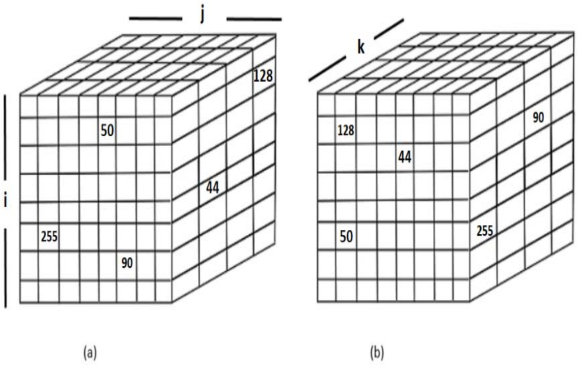


Figure 3 : A (8 x 8 x 4) sided matrix with indexes (i,j,k), the matrix shows the positions of different element before and after shuffling of element. (a) The position of 128 is (2,8,4). (b) The position of 128 after shuffling is (2,2,1).

3.2.2 3D matrix generation

The 3D-matrix can be names the core of the proposed encryption algorithm model which it is used to perform substitution and permutation. The matrix generated by using chaotic characteristics. The chaotic robustness due to its properties of strong random behavior and sensitivity on control parameters and initial conditions both derived from the key.

The matrix uses a logistic map which provide a series of random real numbers with interval 0 to 1. The equation of logistic map is defined in equation 1. The (ir) parameter produce the minimum number of iteration and it is calculated from the key.

After generating the series of logistic map, the output is now scaled up by the scaling factor s1, and then convert the scaled series into integer values as follows:

$$y(n) = \lceil (x(n) * s1) \rceil \bmod 255 \qquad (12)$$

where x(n) is the output of the logistic map and y(n) is the final integer output series.

The 3D-matrix M generated by removing repeated values from array Y, and then convert Y to 3D-matrix. Note that the length of array M is 256. The function generates numbers between 0 and 255 randomly. As the audio file data lies between 0 and 255.

3.3 Shuffling Engine

The shuffling engine rearrange matrix data and produce a new combination of the elements of matrix, the shuffling engine ruled by two arrays which are generated by separate dynamical chaotic system. The two arrays used to shuffle the element of the 3D-matrrix and they are generated by using logistic map equation with two initial conditions x2 and x3 which are derived from the key. The two arrays which produce the dynamical system are contain 270 elements (for each array), the final value of previous iteration turns into initial values of the current iteration. A number is generated at each iteration, then the number scaled up by a scaling factor s2 for the first array and s3 for the second array and later converted the arrays into integers. The scaling factors are also generated from the key to make the system more key sensitive.

The arrays of dynamical chaotic system are generate by the following equations:
First array generation:

$$p_i = 4 \times x2_i(1 - x2_i) \qquad (13)$$

$$array1_i = \lceil (p_i \times s2) | \bmod 255 + 1 \qquad (14)$$

Second array generation:

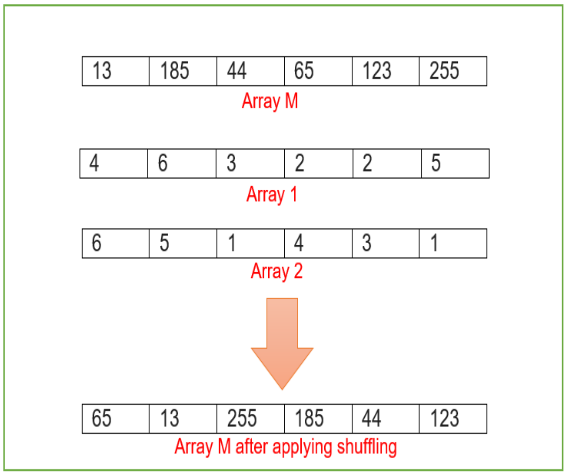
$$q_i = 4 \times x3_i(1 - x3_i) \qquad (15)$$

$$array2_i = \lceil (q_i \times s3) | \bmod 255 + 1 \qquad (16)$$

Shuffling Engine Steps:

Step 1: convert 3D-matrix to 1 dimension array.
Step 2: select element from array1 (array1[i]), treat it as an index of array M, and select the element of array M at that position.
Step 3: substitute the element of matrix M at that location with the index indicated by (array 2[i]).
Step 4: repeat steps (3 & 4) 256 times, the result is shuffled M matrix.
Step 5: finally, the array M rearranged again as 3D-matrix with one of the possible dimensions.

Figure 4 illustrate the shuffling steps as below.



13	185	44	65	123	255

Array M

4	6	3	2	2	5

Array 1

6	5	1	4	3	1

Array 2

65	13	255	185	44	123

Array M after applying shuffling

Figure 4: Shuffling of Matrix Containing Only 6 Elements, the Figure Shows the Matrix Before and After the Shuffle.

3.4 The Proposed Encryption System:

The proposed encryption algorithm of audio file data is consist of 2 parts: *confusion and diffusion*. The confusion is implemented by shuffling of the 3D-matrix, so producing different symbols for different position and different position for different symbols. The diffusion mechanism is achieved by applying Exclusive-OR (XOR) operation to the data with initial random value (IRV). The diffusion spreads any change in only one bit of the data to the all of cipher-audio, so the sensitivity increased.

3.4.1 Confusion stage

The confusion mechanism steps are achieved as follows:

Step 1: generate two arrays of logistic maps with initial parameters x1 and x3 and scaling factors s2 and s3. Use these two arrays to shuffle the plain-audio data by shuffling mechanism.

Step 2: arrange the shuffled plain-audio data as blocks of 10 elements each and add padding if necessary.

If (Size of plain-audio data) mod 10 ≠ 0
padding zeros to plain-audio data

If (Size of plain-audio data) mod 10 = 0
no padding

Step 3: initial array of 3D-matrix is generated using different parameter of logistic map.

Step 4: the dimension of the matrix M are calculated depending on the parameter (m) and matrix M is arranged accordingly.

m = 1 or 4 or 7 ⇒ dimension = 4 × 8 × 8

m = 2 or 5 or 8 ⇒ dimension = 8 × 4 × 8

m = 3 or 6 or 9 ⇒ dimension = 8 × 8 × 4

Step 5: loop for all blocks of the shuffled plain-audio data, each symbol of current block is searched in 3D-matrix. Replace the value of each element by corresponding positions (coordinates) which are noted as number of 3 digits (expressly from 111 to (884 or 848 or 488) according to matrix dimensions).

Step 6: matrix M is now shuffled according to parameters derived earlier. For each block of data, steps (5, 6 and 7) are repeated until all the blocks are processed.

Step 7: calculate even or odd parity bit of each symbol in the block, concatenate each parity bit of all the block symbols to produce binary string of 10 bits, convert the string to equivalent decimal number and close it at the end of the block (i.e. the block size will be 11 instead of 10).

Step 8: now the blocks of data are returned as array of one dimension.

Step 9: the values of the array now are range between 111 and 884, 848 or 488 (according to 3D-matrix dimensions), and the parity element values range between 0 and 1023 (because it consist of 10 bits), to convert these values to 0-255 (audio data range), take every 10 least significant bit (LSB) of each element by remove left zeros padding, and then put each 8 bit on a byte array consequently, i. e. first 8 bits of the first element of confused array will be the first element of byte array, bits (9-10) of the first element and bits (1-6) of the second element of confused array will generate the second element of the byte array, and so on all the rest of the values.

3.4.2 Diffusion stage

After finishing confusion steps, diffusion mechanism is achieved by applying XOR operation as follows:

$$New\_Array[0] = Array[0] \oplus IRV \oplus LMA[0] \quad (17)$$

$$New\_Array[i] = Array[i] \oplus Array[i-1] \oplus (LMA[i] \otimes LMA[i-1]) \quad (18)$$

Where IRV is Initial Random Value, Array[i] is the current audio samples and LMA is Logistic Map Array composed by the logistic map equation with initial value $x1$ and scaled by a scaling factor $s3$.

3.5. Decryption of the Proposed System

Detailed procedure to recover the original audio data is explained in this section, the decryption procedure is exactly the reverse of encryption procedure. The same initial parameters and initial conditions are derived from the secrete key. The reverse of the diffusion mechanism is done with same logistic map parameters and then the audio data are rearranged as blocks of 11 symbols, now calculating the parity bits to verifying if the received data are exactly as the sent data and not tempered during transmission. If parity bit error appears, then the block which contain the error is discarded and may be request for retransmission. Matrix M has to be generate by following same procedure as used in encryption with same parameters. Then, the data is recovered from the respective positions of the matrix. Finally, shuffling of matrix with same order as used in the encryption process produces the original audio data.

4. SECURITY ANALYSIS

An efficient encryption system ought to be strong enough against all existing attacks (e.g. brute force and statistical attacks) [4]. This section discusses the high security degree of the proposed cryptosystem by exhibiting its functionality on the authority of a number of security analyzes such as key space analysis, plaintext sensitivity, information theory entropy and NIST tests.

4.1 Key Space Analysis

A good audio encryption algorithm should be sensitive to the cipher keys, and the key space should be large enough to make brute-force attacks infeasible. For the proposed encryption system, the key space analysis have been carefully studied and can be summarized as follows:

4.1.1 Key sensitivity analysis

A major feature for a good crypto-system is an extreme key sensitivity which ensure the security of the crypto-system across the brute-force attack in a measure. Key sensitivity of any crypto-system can be detected in two various ways: Firstly, the cipher audio generated by any crypto-system should be very sensitive to the key, for example, if two a bit different secret keys have been used to encrypt same original plain-audio then the two generated cipher-audio produced ought to be completely disconnected to each other. Secondly, the cipher audio cannot be decrypted correctly even if there is just a bit variation among encryption and decryption secret keys. In the proposed encryption algorithm, cipher audio depended on each bit of the key, this dependency achieved by the derivation of the initial conditions and control parameters from that key, the key sensitivity showed in Figures 5 and 6. Figure 5 shows different cipher audio of same plain audio encrypted with two keys differ from each other in only one bit and Figure 6 also shows that if we change only one bit of the key, then the resulting decrypted audio is extremely different from the original plain-audio.

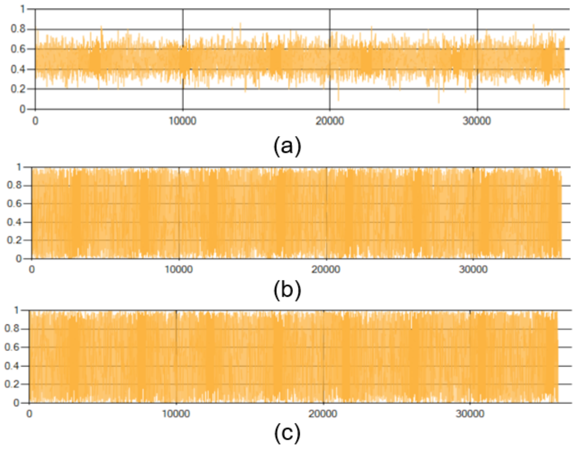


Figure 5: Different Encryption Process Of Same File Audio With Two Keys Differ From Each Other In Only One Bit, (a) Shows Original Wave Audio File Before Encryption and (b,c) Shows The Same Wave File Encrypted With The Two Keys.

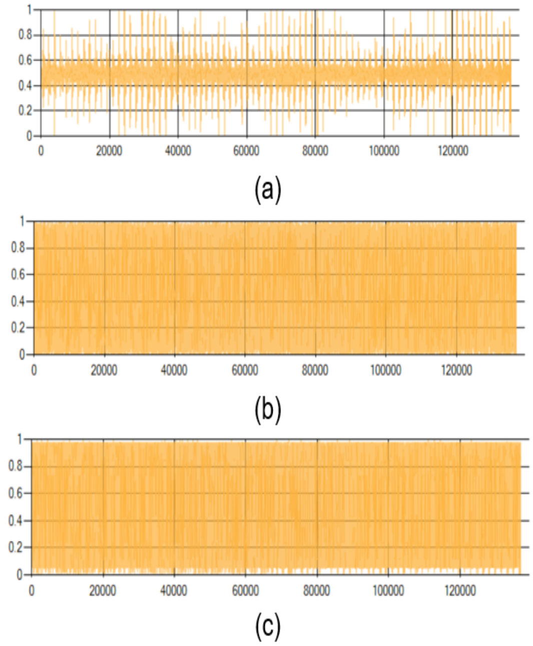


Figure 6: Plot of Waveform Decrypted With a Key Differ In Only One Bit from the Original Key
(a) Original Waveform Plot
(b) Plot of Waveform Decrypted With a Key Differ In Only One Bit from the Original Key
(c) Plot of Waveform Decrypted With a Key Differ In Only One Bit From the Original Key on Another Position From (b).

4.1.2 Exhaustive key search

The brute-force attack has the capability of attacking against existing types of encryption, with variant levels of success. In this kind of attack, the attackers have compromised the secret key and cipher audio as well, and they try to check each distinct secret key automatically with a help of a computer which is quick to search for the exact key faster. The brute-force attack basically starts with one digit secret key, and then goes to two-digit secret key going on until the end of secret key. In order to withstand against this kind of attacks, the secret key space should be totally large [31]. The secret key space of the proposed system is 2^{128}. Thus, the proposed encryption system has a large enough key space to withstand against all kinds of brute-force attacks.

4.2 Plaintext Sensitivity

With a view to deal with different attacks such differential analysis (chosen plaintext attack), when a little change of plain-audio happens, cipher-audio should extremely changes, so that the attacker cannot obtain any meaningful connection between the plain-audio and cipher-audio. Therefore; the proposed method dealt with this kind of attack and tried to make it infeasible by making the chaining series of plaintext at the diffusion stage. As a result, all the resulting cipher will be changed even if only one bit of the original audio data had been changed. Also, the effectiveness of the IRV value which change with every run time, thus the resulting cipher audio will be different every execution time even if the same plain audio and secrete key have been used, i.e. the chosen plaintext attack will be infeasible. Figure 7 shows different execution process for same audio file. The figure indicates that for each encryption process, the resulting cipher-audio will be different.

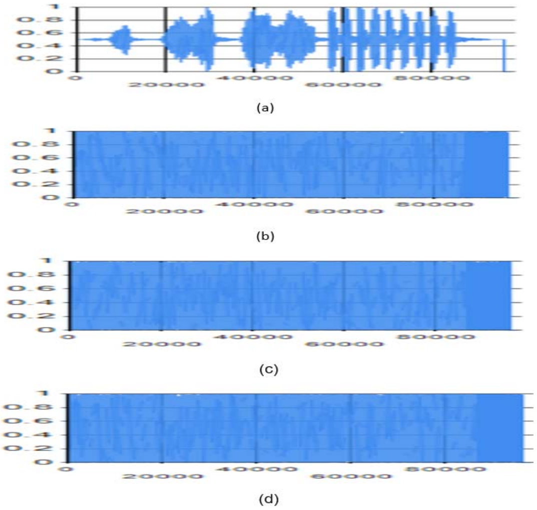


Figure 7: Different Encryption Process for Same FIle Audio With Same Encryption Key, (a) Shows Original Wave Audio File Before Encryption and (b,c,d) Show The Same Wave File Encrypted With Same Key Different Times.

4.3 Entropy of Encrypted Audio

The entropy is regarded as one of the most essential property of randomness and it is a significant measure in information theory, information entropy refers to the amount of chaos of a system. The cipher data should be confused sufficient to protect against the statistical analysis attack. Here, information entropy can be used to compute, the more confusing the cipher data is the more the entropy is 8 [71]. The first order information entropy can be calculated by the following equation [7]:

$$h(s) = -\sum_{i=0}^{2^n-1} p(s_i)\log_2 p(s_i) \qquad (19)$$

Moreover, the second order Information Entropy can by calculated as follows [31]:

$$2^{nd}\ h(s) = -\sum_{i=0}^{n-1}\sum_{j=0}^{n-1} P(s_i, s_j)\log(P(s_i, s_j)) \quad (20)$$

where $p(s_i)$ denotes the probability of the symbol (s_i) being released from s. Table 1 shows first and second entropy order of the proposed crypto-system.

Table 1 Entropy for Proposed Encryption Algorithm

File name	Audio data size (byte)	Sample rate (Sample/ Second)	First order entropy value before proposed encryption	Second order entropy value before proposed encryption	First order entropy value after proposed encryption	Second order entropy value after proposed encryption
Noise	14439	22050	6.1100	12.2032	7.9861	15.9634
Water 2	35222	8000	6.1691	12.3365	7.9943	15.9855
Water	48513	22050	6.1638	12.3247	7.9961	15.9898
Helicopter	68598	11025	5.3864	10.7152	7.9967	15.9916
Region	96979	11025	5.4982	10.9656	7.9983	15.9953

4.4 Randomness Tests

Randomness characters are essential requirements for an efficient cryptosystem, The NIST Test Suite is an arithmetical package containing many tests that were established to assess the randomness of (randomly long) binary series formed by either hardware or software based cryptographic pseudorandom number generators or random. These evaluations emphasize a range of various kinds of non-randomness that could exist in a series [30], the proposed method had been tested by the NIST three important tests (frequency test, block test and runs within a block test). The average value of these tests for 30 audio samples is shown in Table 2 as bellow:

Table 2: NIST Tests Results of the Proposed System

Test name	P-value
Frequency	0.6515
Block	0.4985
Runs	0.6147

Note that the Pass-value (P-value) of the three NIST statistical tests above must have value >= 0.01, Otherwise the conclusion is that the series is not random. From Table 2, it is obvious that the proposed algorithm has highly random behavior.

4.5 Chaos Effect (Encryption Effect Analysis)

It is important to know that for each element of data there is a combination of 256! ways of 3D-matrix positions, this huge combination with sensitivity to initial conditions and parameters of the chaotic systems makes the brute force attacks infeasible.

4.6 Comparison with Other Works

The proposed system improved the performance of the algorithm reported in [7]; the proposed scheme had been extended the 3D matrix length. In [7], the 3D matrix length is composed of 96 elements, whereas the same matrix in the proposed system has 256 elements. Besides, the 3D matrix dimensions of [7] either 4 × 4 × 6 or 4 × 6 × 4 or 6 × 4 × 4, while the dimensions of the proposed 3D matrix could be 4 × 8 × 8, 8 × 4 × 8 or 8 × 8 × 4. Thus, the proposed cryptosystem improved the security of the system by the expansion of the 3D matrix. Therefore, the system made almost all the existing attacks more difficult. In addition, the diffusion stage algorithm of the proposed system is different compared to the diffusion stage algorithm in [7].

Furthermore, this section shows a comparison with others encryption algorithms [14-18] with first order entropy, which are shown in Table 3, note that the best result is illustrated by a bold font.

Table 3: First Order Entropy Comparison between Proposed Algorithm and Many Other Works

References	First order entropy
Ref. 14	7.9874
Ref. 15	7.9974
Ref. 16	7.9971
Ref. 17	7.9971
Ref. 18	7.9024
Proposed	**7.9983**

5. CONCLUSION AND FUTURE WORK

Audio security is involved with ensuring secrecy, accessibility, reliability, and confidentially of audio data. The essential goal of audio security is to keep audio systems away from unauthorized access, alteration, annihilation and disruption. This paper has been suggested a new encryption system based chaotic logistic map system. The proposed algorithm composed of two stages: confusion and diffusion stages. At confusion stage, logistic map is used in order to shuffle the audio samples. Also, 3D logistic map matrix is utilized by the shuffling engine in order to confuse the samples for each block of data. The dimensions of the 3D matrix are variable and they are depending on an initial condition. At diffusion stage, an XOR operation is made between random values with current and previous values of audio sample as well as the logistic map array. All the parameters and initial conditions of the proposed scheme are derived from the secrete key, thus making the system key sensitive. The security analysis reported in section 4 shows the high randomness and robustness of the proposed system. Also the results show that the system can overcomes many existing attacks. One of the essential future recommendations is to speed up the system through applying parallel programming with an intention to reduce the execution time.

REFERENCES:

[1] J. Fridrich, “Symmetric ciphers based on two-dimensional chaotic maps”, *International Journal of Bifurcation and Chaos,* Vol. 8,No. 06, 1998, pp. 1259–1284.

[2] Chen, Guanrong, Yaobin Mao, and Charles K. Chui., "A symmetric image encryption scheme based on 3D chaotic cat maps." *Chaos, Solitons & Fractals, Vol.* 21, No. 3, 2004, pp. 749-761

[3] Patidar, Vinod, N. K. Pareek, and K. K. Sud., "A new substitution–diffusion based image cipher using chaotic standard and logistic maps." Communications in Nonlinear Science and Numerical Simulation, Vol. 14, No. 7, 2009, pp. 3056-3075.

[4] Kanso, A., and M. Ghebleh., "A novel image encryption algorithm based on a 3D chaotic map." *Communications in Nonlinear Science and Numerical Simulation* , Vol. 17, No. 7, 2012, pp. 2943-2959.

[5] Pareek, Narendra K., Vinod Patidar, and Krishan K. Sud., "Block cipher using 1D and 2D chaotic maps." *International Journal of Information and Communication Technology*, Vol. 2, No. 3, 2010, pp. 244-259.

[6] Elshamy, E. M., El-Rabaie, E. S. M., Faragallah, O. S., Elshakankiry, O. A., El-Samie, F. E. A., El-Sayed, H. S., & El-Zoghdy, S. F., "Efficient audio cryptosystem based on chaotic maps and double random phase encoding." *International Journal of Speech Technology*, Vol. 18, No. 4. 2015, pp. 619-631.

[7] Kumar, M., Kumar, S., Budhiraja, R., Das, M. K., & Singh, S., "A cryptographic model based on logistic map and a 3-D matrix." *Journal of Information Security and Applications,* Vol. 32, 2017, pp.47-58.

[8] Akgül, Akif, and Sezgin Kaçar., "An Audio Data Encryption with Single and Double Dimension Discrete-Time Chaotic Systems." *Turkish Online Journal of Science & Technology*, Vol. 5, No. 3, 2015, pp. 14-23.

[9] Al Saad, Saad Najim, and Eman Hato., "A speech encryption based on chaotic maps." *International Journal of Computer Applications*, Vol. 93, No. 4, 2014, pp. 19-28.

[10] Zhao, H., He, S., Chen, Z., & Zhang, X., "Dual key speech encryption algorithm based underdetermined BSS." *The Scientific World Journal*, Vol. 2014, 2014, pp. 1-7.[11] *Maysaa, A. A. J., & Qays,* I., “*Speech encryption using chaotic map and blow fish algorithms”*. Journal of Basrah Researches, *Vol. 39, No. 2, 2014, pp. 68–76.*

[12] Haojiang Gao, Yisheng Zhang, Shuyun Liang, and Dequn Li, “A new chaotic algorithm for image encryption ", *Chaos Solitons and Fractals*, Vol. 29, No. 2, 2006, pp. 393-399.

[13] Akgül A, Kaçar S, Pehlivan İ., “An Audio Dta Encryption with Single and Double Dimension Discrete-Time Chaotic Systems”. *The Online Journal of Science and Technology*, Vol. 5, No.3, 2015, pp. 14-23.

[14] Liu, Hongjun and Wang, Xingyuan and others, Image encryption using DNA complementary rule and chaotic maps, *Applied Soft Computing,* vol. 12, No. 5, 2012, pp. 1457—1466.

[15] Wang, Xingyuan and Liu, Lintao and Zhang, Yingqian, A novel chaotic block image encryption algorithm based on dynamic random growth technique, *Optics and Lasers in Engineering,* Vol. 66, 2015, pp. 10-18.

[16] Wang, Xing-Yuan and Zhang, Ying-Qian and Bao, Xue-Mei, A novel chaotic image encryption scheme using DNA sequence operations, *Optics and Lasers in Engineering,* Vol. 73, 2015, pp. 53—61.

[17] Wei, Xiaopeng and Guo, Ling and Zhang, Qiang and Zhang, Jianxin and Lian, Shiguo, A novel color image encryption algorithm based on DNA sequence operation and hyper-chaotic system, *journal of Systems and Software*, Vol. 85, No. 2, 2012, pp. 290—299.

[18] Niyat, A. Y.; Hei, R. M. H.; Jahan, M. V., "A RGB image encryption algorithm based on DNA sequence operation and hyper-chaotic system" .

[19] Chai, X.; Gan, Z.; Yuan, K.; Chen, Y.; Liu, X., "A novel image encryption scheme based on DNA sequence operations and chaotic systems". *Neural Computing and Applications* 2017, pp. 1-19.

[20] Enayatifar, R.; Abdullah, A. H.; Isnin, I. F.; Altameem, A.; Lee, M., "Image encryption using a synchronous permutation-diffusion technique". *Optics and Lasers in Engineering* Vol. 90, 2017, pp.146-154.

[21] Mokhtar, M. A.; Gobran, S. N.; El-Badawy, E.-S. A. "In Colored Image Encryption Algorithm Using DNA Code and Chaos Theory", *Computer and Communication Engineering (ICCCE), International Conference on, IEEE*, 2014, pp 12-15.

[22] Zhang, Q.; Guo, L.; Wei, X., "Image encryption using DNA addition combining with chaotic maps". *Mathematical and Computer Modelling, Vol. 52, No. 11,* 2010, pp. 2028- 2035.

[23] Singh, K.; Kaur, K., "Image encryption using chaotic maps and DNA addition operation and noise effects on it". *International Journal of Computer Applications*, Vol. 32, No. 6, 2011.

[24] Zhang, Q.; Xue, X.; Wei, X., "A novel image encryption algorithm based on DNA subsequence operation". *The Scientific World Journal*, Vol.2012, 2012.

[25] Khade, P. N.; Narnaware, M., "3D chaotic functions for image encryption". *IJCSI International Journal of Computer Science Issues*, Vol.9, No. 3, 2012, pp. 323-328.

[27] Alabaichi, A. M., "Color Image Encryption using 3D Chaotic Map with AES key Dependent S-Box". *International Journal of Computer Science and Network Security (IJCSNS)*, Vol. 16, No.10, 2016, pp. 105.

[28] Lv, Z.; Zhang, L.; Guo, J. "In A Symmetric Image Encryption Scheme Based on Composite Chaotic Dispersed Dynamics System", *IEEE Proceedings of the Second International Symposium on Computer Science and Computational Technology (ISCSCT'09),* 2009; pp 191-194.

[29] Tong, X.-J.; Zhang, M.; Wang, Z.; Liu, Y., "A image encryption scheme based on dynamical perturbation and linear feedback shift register". *Nonlinear Dynamics*, Vol.78, No. 3, 2014, 2277-2291.

[30] Rukhin A., Soto J., J. Nechvatal, Smid M., Barker E., S. Leigh, Levenson M.,Vangel M., Banks D., A. Heckert, Dray J., and Vo S.,"NIST Special Publication 800-22rev1a: A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications", 2010. Available at *https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-22r1a.pdf*

[30] El-Latif , Ahmed A., Niu, Xiamu, "A hybrid chaotic system and cyclic elliptic curve for image encryption", *AEU-International Journal of Electronics and Communications*, vol. 67, no. 2, 2013, pp. 136–143.

[31] Enayatifar, Rasul, Abdullah, Abdul Hanan, Isnin, Fauzi I., "Chaos-based image encryption using a hybrid genetic algorithm and a DNA sequence", *Optics and Lasers in Engineering*, vol. 56, 2014, pp. 83-93.