Design a Hybrid Cryptosystem Based Chaos and Sharing for Digital Audio

Mahmood Z. Abdullah[1], Zinah J. Khaleefah[2]
[1,2]*Computer Engineering Department, Mustansiriyah University, Baghdad, Iraq,*
e_mail: drmzaali@uomustansiriyah.edu.iq, zinah.jamal@uomustansiriyah.edu.iq

Abstract— *With the growth rate of wireless communication with internet and multimedia. The wireless network has expanded their applications in our life. Cryptography and steganography play important role within data security. This paper chiefly produces a novel hybrid cryptography and steganography for digital audio base chaos system and secret sharing scheme algorithm. These algorithms have multilevel of processing with the digital audio to increase the level of security. In this algorithm, digital audio was encrypted with a novel encryption method based Lorenz chaos map. Then, divide the encrypted audio to N encrypted audio based on secret sharing scheme. Finally, hiding N encrypted audio in N cover images with chaos system process. The result shows that the algorithm for audio encryption have a high degree of confidence, large key space reached more than 2672 possible of a key, key sensitivity, and high quality of recovered digital audio. Chaos system and secret sharing process with multi-cover images offers additional space, security for the secret audio message, and quality for cover images. The power signal to noise ratio of cover images reached to 57db with embedding 334 KB of secret audio with four cover images.*

Index Terms— *Lorenz chaotic map; Audio cryptography; Steganography; Secret sharing scheme; Encryptio; Dycryption.*

I. INTRODUCTION

The security for the digital audio was achieved by many techniques such as steganography, cryptography, and others. Cryptography was applied with many mathematical transformations on secret information in order to protect the secret information during the transform. But the steganography is the process of hiding the secret information within other information [1].

Encryption of digital audio is more complex and difficult than text encryption. The audio has the negative amplitude which may be lost after some transformations [2]. Audio encryption is a process of adding noise to the original sound. Audio encryption is a process of adding noise (key) to the original sound and results in several important properties such as confidentiality, authentication, integrity, non-repudiation, access control [3].

Chaos is one of the behaviors that associated with the nonlinear system. The chaos system contains some important properties, such as: sensitive to initial conditions and system parameters, no periodicity, pseudorandom property, and topological transitivity, etc. There are several chaotic systems such as Lorenz system, RÖssler system, Chua system, Logistic map, Hénon map, Arnold Cat map (ACM) [4].

Received 4 may 2017; Accepted 2 November 2017
 ISSN 1811-9212

In this paper, two type of chaos is used (Lorenz Chaotic and Logistic map). With Lorenz chaotic has three deferential equations known as Lorenz equations form, as shown in (1), (2) and (3).

$$dx/dt = \sigma (y-x) \quad (1)$$

$$dy/dt = \gamma x - xz - y \quad (2)$$

$$dz/dt = xy - \beta z \quad (3)$$

Where t, x, y, z, σ, γ, β ∈R and σ, γ, β are positive constants. If σ = 10 and β = 8/3, whe γ > 24.74, the dynamical orbit will be confused [5].

The logistic map is the simplest type of the chaotic equation, defined below:

$$x_{n+1} = \mu x_n (1 - x_n) \quad (4)$$

Where xn is the initial value, μ is controlled parameter[6], the chaotic region with 3.5699456 <μ<= 4 [7].

Secret sharing is a technique of great importance in data encryption. Shamir and Blakley are the first to invent the secret sharing in 1979 respectively [8]. A (t,n) Shamir secret sharing threshold is a technique for sharing a secret data to n groups, each one holds a portion of the secret data. with any combination of t groups (where t ≤ n), the original data can be recovered without errors. The secret sharing was obtained by equation (5), And the original data was returned by equation (6) [9]:

$$s(xn) = m + s1xn + \ldots\ldots + st\text{-}1xnt\text{-}1 \ (mod\ p) \quad (5)$$

$$m \equiv \sum_{n=1}^{t} yn \prod_{\substack{j=1 \\ j \neq n}}^{t} \frac{-xj}{xn - xj} \ (mod\ p) \quad (6)$$

Where p is the prime number, x_1,...., x_n are the different integer numbers, s_1,.....,s_{t-1} are the original data. s(x_1),..., s(x_n) are the secret share data, m recovered of the original data.

II. RELATED WORKS

In[10] presented a new voice encryption method based on substitution and permutation of the voice samples by using a secret key with transform domain. Two approaches are used, The first approach was used henon chaos and the second approach was used Arnold cat map. In [11] presented a new voice encryption method is based on substitution and permutation of the audio sample. The proposed algorithm has used the wavelet and the Arnold cat map for audio encryption. In [12] presented a new voice encryption and decryption method based on chaotic dynamic behavior by nonlinear discrete-time dynamical. In [13] presented a novel higher dimensional of the chaotic system for encryption the audio. The algorithm has high security and sensitive to the initial condition. In [14] presented a novel algorithm based on a shuffling procedure to the audio encryption process. A large number of possible secret keys provided a brute-force attack on this algorithm. In [15] presented four chaotic map algorithms for audio encryption, These algorithms are used the audio encryption for both times and transform domains.

III. PROPOSED METHOD

In the transmitter side, the proposed algorithm has four main phases. The phases of the proposed algorithm are as follows, which is shown in Fig. 1.

Phase1: secret key generation based on Lorenz equations and logistic map.

Phase2: encrypts the digital audio with a novel encryption process based a secret key.

Phase3: distribute the encrypted audio from phase2 to four groups based on secret sharing scheme.

Phase4: embeds the groups from phase3 with cover images based on random sequence generated from Logistic map equation.

Received 4 may 2017; Accepted 2 November 2017

ISSN 1811-9212

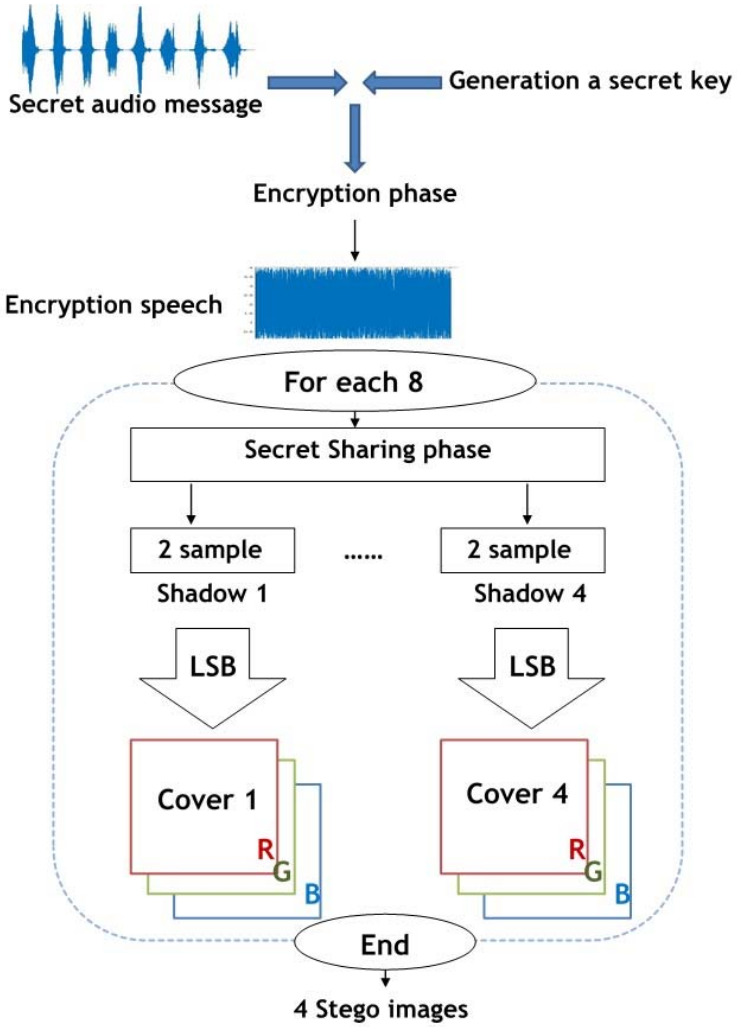

FIG. 1. PROPOSED ALGORITHM IN THE TRANSMITTER SIDE.

A. Secret key Generation

The Secret Key Generation for the audio encryption is done in the following steps which are shown in Fig. 2.

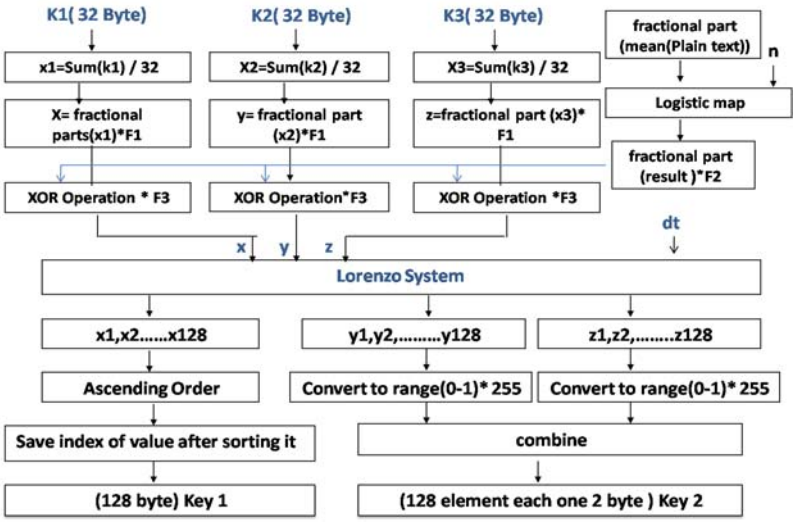

FIG. 2. SECRET KEY GENERATION WITH LORENZ MAP.

Received 4 may 2017; Accepted 2 November 2017

ISSN 1811-9212

Input: initial secret key, sensitive parameters, factor parameters.
Output: Secret key1, Secret key2.
Steps:

1- Take the summation for each initial secret key, each one has 32 of ASCII character and multiplied the fractional part of the result for each one by factor parameter F1. The value of factor F1 equal 106, these result 1.
2- Compute the mean of plain text, and applied the fractional part of the result to the logistic map equation and multiplied the fractional part of the result by factor parameter F2. The value of factor F2 equal 108, these result 2.
3- Applied XORing operation between each the value of result 1 with the value of result 2 and multiplied the fractional part of the result by factor parameter F3. The value of factor F3 equal 10-6, three value is generated as initial to Lorenz system.
4- Lorenz system was generated three arrays (X, Y, and Z).
5- Applied ascending order to the value of array X and save the index of the value after sorting to generated secret key as permutation secret key 1.
6- Convert the range value of the arrays X and Y to the range (o to 1) and then combined them to generated secret key 2.

B. Encryption Phase

Encryption process was applied for digital audio with the following steps:

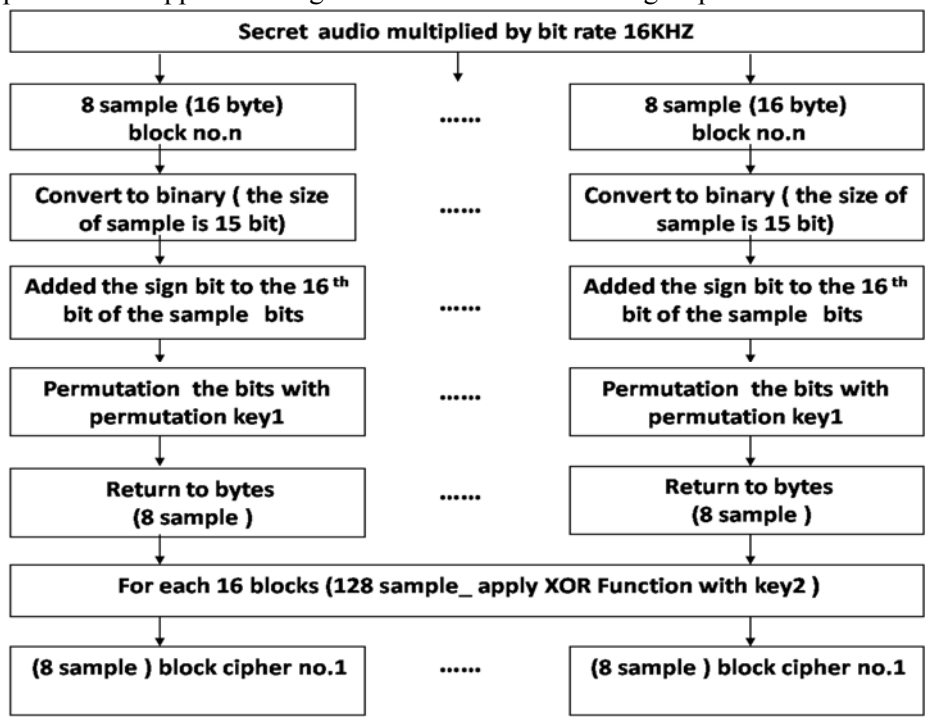

FIG. 3. ENCRYPTION THE PLAIN AUDIO PROCESS.

Input: plain audio , secret key1 , secret key2.
Output: cipher audio.
Steps:

1- Multiplied the plain audio with scale factor (16 kHz) to convert the range of sample value from (0 - 1) to (0 - 16384).
2- Divided the plain audio to the blocks of 8 sample (16 bytes), if the number of sample in the last block less than 8 sample, 0 value was applied to these block.

Received 4 may 2017; Accepted 2 November 2017

ISSN 1811-9212

3- Convert the sample value to the binary form, each sample has (15 bit).
4- Added the sign bit (0 for a positive sign, 1 to the negative sign) of each sample to the 16th bit of the sample bits.
5- Scrambling the bits of each block of audio with the secret key1.
6- Convert the sample value to decimal.
7- XORing operation was applied to the samples of each 16 blocks with the secret key2.
8- encrypted audio was produced.

C. Secret Sharing Phase

In this paper, a threshold (4,4) secret sharing scheme is used to produce four groups for each block. with the below, steps for described the sharing scheme process.

Input: cipher text.

Output: n shadow.

Steps:

1- For each block of 8 sample (16 byte), reshape the block to new dimension 2*4 sample (the size of each sample 2 byte).
2- For each block, apply the Shamir's threshold (4,4) scheme equation to each row of block [9]:

$$S(X_i)=S_0X_i+S_1X_i+S_2X_i^2+S_3X_i^3 \pmod{65537} \quad (7)$$

where i=1 to 4. the sample value of the cipher audio is between 0 and 65535, then 65537 is the closest prime number to 65535.
3- For each block, 4 shadow are produced.

D. Embedding Phase

The embedding phase was summarized in the following steps:

Input: 4 shadow for each block, 4 RGB cover images, secret key for embedding phase.

Output: 4 RGB stego images.

Steps:

1- Three secret key was generated with logistic map equation (key-stego1, key-stego2, key-stego3), as shown in Fig. 4.

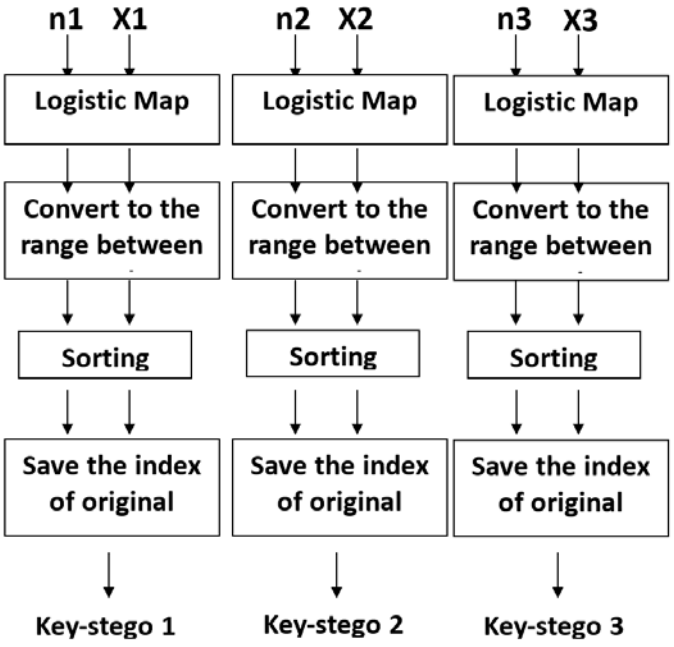

FIG. 4. SECRET KEY GENERATION BASED ON LOGISTIC MAPS.

Received 4 may 2017; Accepted 2 November 2017

ISSN 1811-9212

2- For each cover image, the image was divided into the blocks with size (16*16 bytes) and each block was selected with key-stego1 and key-stego2 for row and column sequence respectively of the cover image.
3- Each shadow was inserted to the pre-selected block in the step2 with LSB process and key-stego3 sequence. With a secret sharing phase, the value of the sample may be equal 65536 in shadow, this value was taken seventeen bit. For every sixteen pixels of the cover image, seventeen bit was embedded with LSB for pixels as shown in Fig. 5.
4- Stego images produced.

$b_{1,1}$.... $s_1 s_2$	$b_{2,1}$... $b_{2,7} s_3$	$b_{3,1}$... $b_{3,7}$ s_4	$b_{4,1}$.... $b_{4,7}$ s_5
$b_{5,1}$... $b_{5,7}$ s_6	$b_{6,1}$.. $b_{6,7}$ s_7	$b_{7,1}$... $b_{7,7}$ s_8	$b_{8,1}$..... $b_{8,7} s_9$
$b_{9,1}$... $b_{9,7}$ s_{10}	$b_{10,1}$.. $b_{10,7}$ s_{11}	$b_{11,1}$.. $b_{11,7} s_{12}$	$b_{12,1}$.....$b_{12,7} s_{13}$
$B_{13,1}$... $b_{13,7} s_{14}$	$B_{14,1}$.. $b_{14,7}$ s_{15}	$B_{15,1}$..$b_{15,7}$ s_{16}	$B_{16,1}$....$b_{16,7} s_{17}$

FIG. 5. EMBEDDING METHOD, 17-SECRET BITS WAS EMBEDDED WITH 16 PIXELS OF COVER IMAGE.

In the receiver side, all the phases in transmitter side applied with reverse direction, The phases were summarized in the following, as shown in Fig. 6:

Phase1: secret key generation based on Lorenz equations and logistic map.
Phase2: extracted the shadows from the cover images based on random sequence generated by Logistic map equations.
Phase3: inverse secret sharing was applied for each 8 sample (2 sample for each shadow) to produce cipher audio.
Phase4: Decryption the cipher audio with secret key based Lorenz equation to produce plain audio.

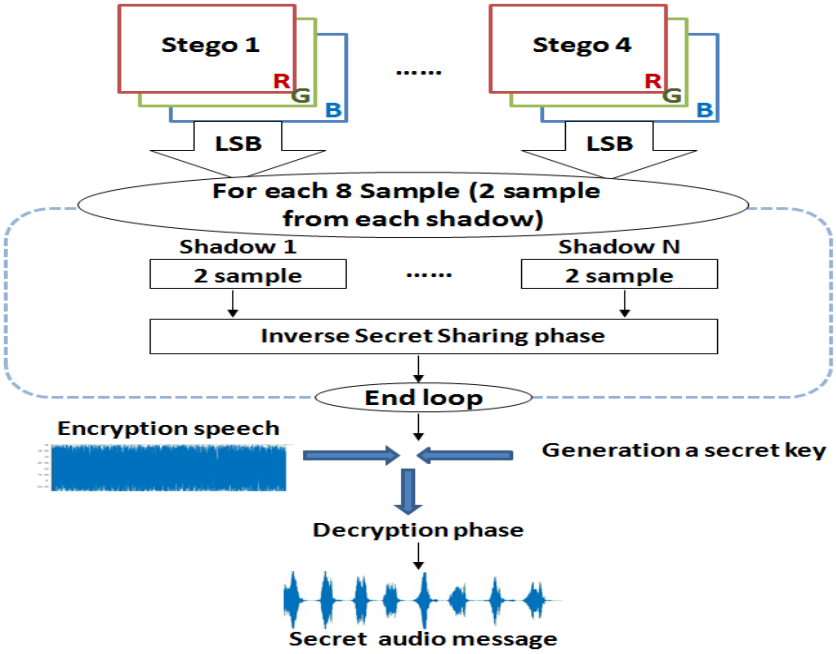

FIG. 6. PROPOSED ALGORITHM FOR RECEIVER SIDE.

IV. EXPERIMENTAL RESULTS

In this section, experimental results divided into two parts: In the first part, the performance of encryption audio algorithm was evaluated. And in the second part, the performance of embedding algorithm was evaluated. Hardware specification used in the simulation results, represented by a laptop,

Received 4 may 2017; Accepted 2 November 2017

ISSN 1811-9212

Lenovo, Processor intail (R) coreTM i7, CPU 2.4 GHZ, RAM 8GB, Operating system windows 8 , Software Matlab (R 2015a). Six test audio wave were used with the proposed algorithm with size 25.6 KB, 48.9 KB, 51.3 KB, 78.1 KB, 234 KB, 312 KB receptivity, with a sample rate 8KHZ and 16 bit/sample.

A. Encryption

Chirp test1 wave audio (size: 25.6 KB, duration time: 1.6027 sec, sample rate: 8KHZ, quantization: 16 bit/sample) was used with the flowing secret key. The plain audio was shown in Fig. 7, the cipher audio was shown in Fig. 8, and the decryption audio with the correct secret key was shown in Fig. 9.

k1='Z&QBZH8ATBbCdaFEHijkkl-Z23456N#9'

k2='B2BB5M7#AC%+cdEfgQijNklm1N%4567#'

k3='BZHO56BZ8AAbCdeRgHiKk*l%1234567#'

alpha=28 sigma=10 beta=8/3 dt=0.009 n=3.98

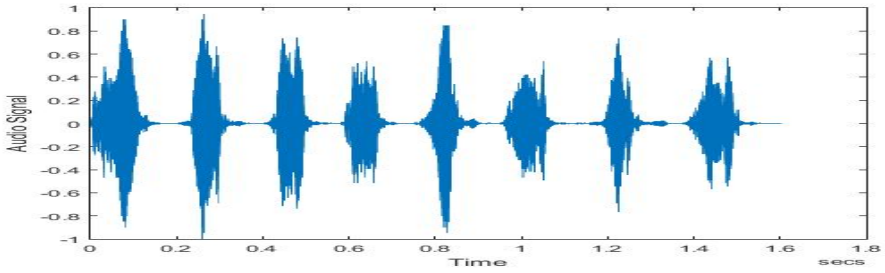

FIG. 7. PLAIN AUDIO.

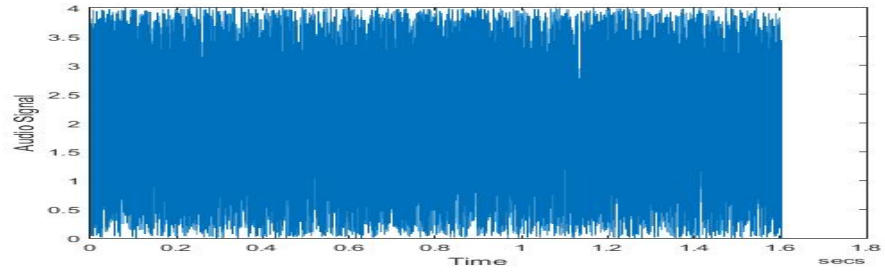

FIG. 8. CIPHER AUDIO.

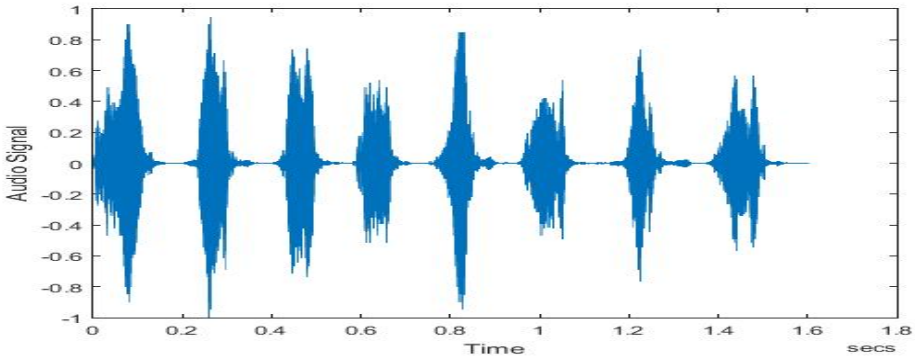

FIG. 9. DECRYPTION THE CIPHER AUDIO.

B. Secret key Space

The key space is the total number of the different keys that are used in the proposed algorithm. The proposed algorithm has three secret key of 32 ASCII form for each one, In addition to some of the initial

Received 4 may 2017; Accepted 2 November 2017

ISSN 1811-9212

parameter for Lorenz, logistic system equations. The key in the proposed algorithm has a large space reach more than 2^{672} possible different secret key.

C. Secret key Sensitivity

With a good encryption system must be very sensitive with a secret key [4]. In the Fig. 10, 11, 12,and 13 was shown the different results of the decryption the cipher audio when used one digit alter with the secret key.

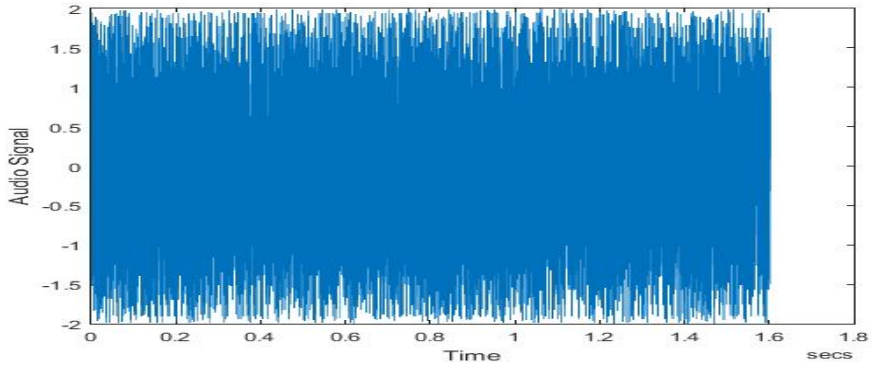

FIG. 10. DECRYPTION THE CIPHER AUDIO WHEN A SECRET KEY CHANGE WITH K1='Y&QBZH8ATBBCDAFEHIJKKL-Z23456N#9'.

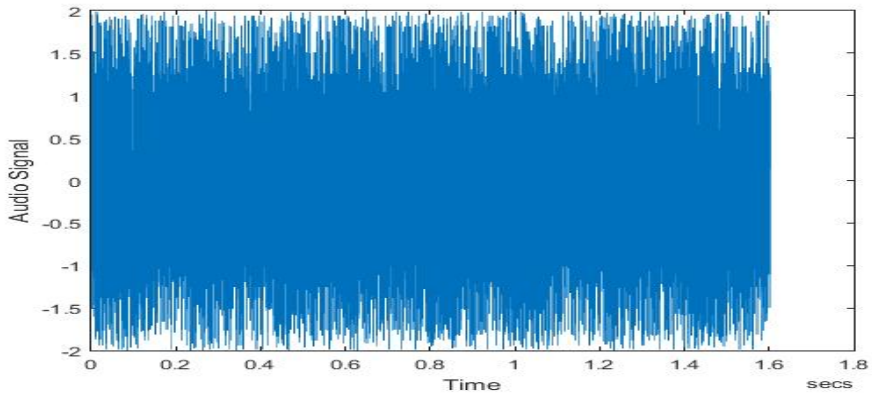

FIG. 11. DECRYPTION THE CIPHER AUDIO WHEN A SECRET KEY CHANGE WITH K2='B2BB5M7#AC%+CDEFGQ IJMKLM1N%4567#'.

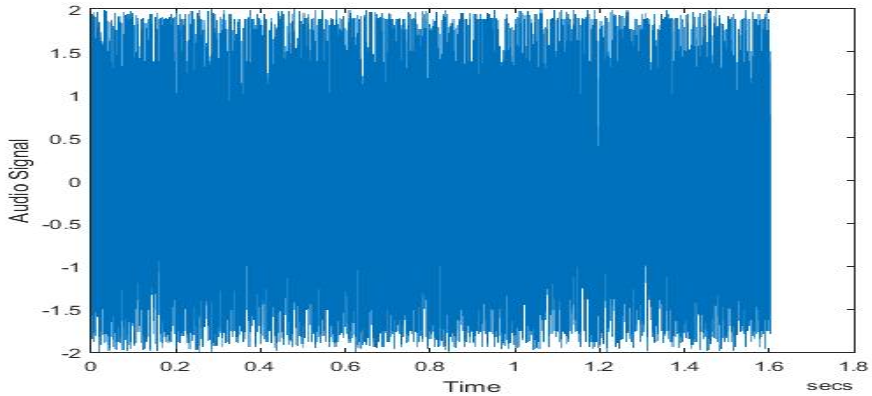

FIG. 12. DECRYPTION THE CIPHER AUDIO WHEN A SECRET KEY CHANGE WITH K3='BZHO56BZ8AABCDERGHIJK #L%1234567#'.

Received 4 may 2017; Accepted 2 November 2017

ISSN 1811-9212

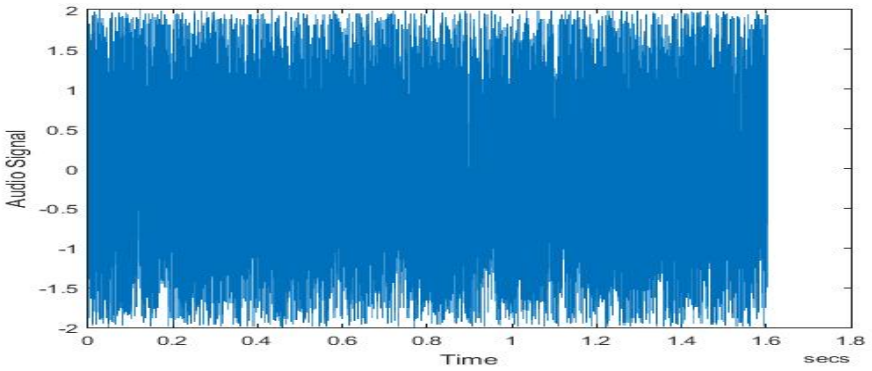

FIG. 13. DECRYPTION THE CIPHER AUDIO WHEN A SECRET KEY CHANGE WITH DT=0.0091.

D. Frequency Analysis

The frequency analysis was depended on the histogram properties, The histogram of an ideal encryption audio must have a uniform distribution with their frequency [10]. The histogram of plain audio shown in Fig. 14, Histogram of the encryption audio shown in Fig. 15, And the histogram of the decryption audio shown in Fig. 16.

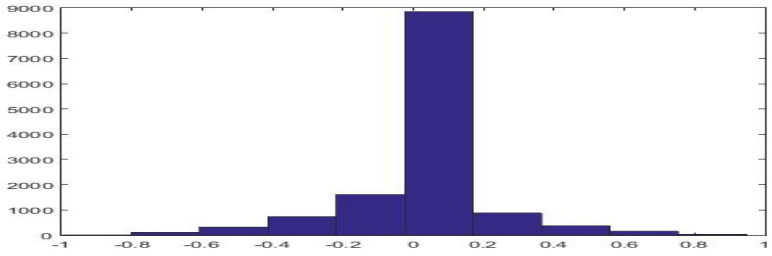

FIG. 14. HISTOGRAM OF THE PLAIN AUDIO.

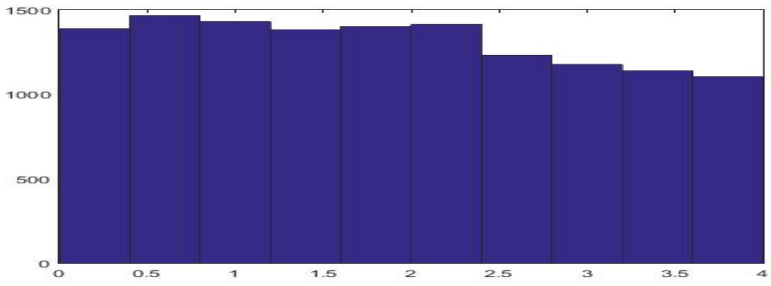

FIG. 15. HISTOGRAM OF THE ENCRYPTION AUDIO.

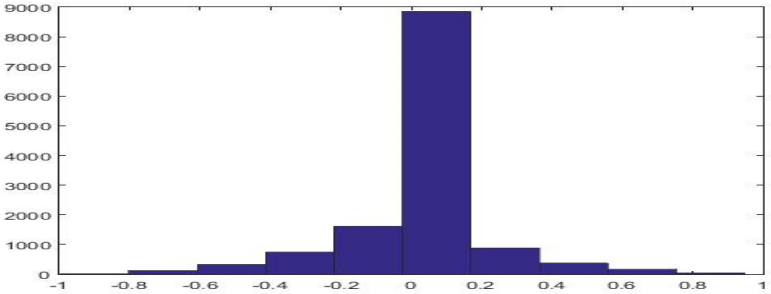

FIG. 16. HISTOGRAM OF THE DECRYPTION AUDIO.

Received 4 may 2017; Accepted 2 November 2017

ISSN 1811-9212

E. Correlation Coefficient Analysis

Correlation value was determined the relationship between plain audio and encryption audio, It is an important metric to the quality encryption algorithm for evaluating. The encryption quality is good when the correlation coefficient value is low with encryption audio and high with decryption audio [15]. The results of the correlation value of the plain audio with the encryption audio and the plain audio with decryption audio were shown in the table1.

TABLE 1. CORRELATION.

Secret Audio	Plain -encryption	Plain -decryption
Test1.wav	0.007690	0.999999 =1
Test2.wav	-0.003446	0.999999 =1
Test3.wav	0.014967	0.999999 =1
Test4.wav	-0.006587	0.999999 =1
Test5.wav	-0.006680	0.999999 =1
Test6.wav	0.003556	0.999999 =1

F. Information Entropy Analysis

Information entropy represents the probability of the sample in the audio message m. The entropy can be calculated as below [14]:

$$H(m)=\sum_{i=0}^{2^N-1} p(m_i)\ \log_2\left(\frac{1}{p(m_i)}\right) \quad (8)$$

where $p(m_i)$ represents the probability of audio message m, N is the number of the bits of the audio sample, 2^N means all possible samples. Table 2, show the entropy of the plain audio and encryption audio. With the purposed algorithm. The samples of encryption audio appeared the same probability. The maximum value of the entropy shall be 16 with proposed algorithm.

TABLE 2. ENTROPY RESULTS.

Secret Audio	Original	Encryption	Decryption
Test1.wav	6.803766	12.850383	6.803767
Test2.wav	11.613564	13.700705	11.073960
Test3.wav	6.803767	13.436860	6.803767
Test4.wav	12.497809	14.289598	11.866024
Test5.wav	11.765619	14.519646	11.041317
Test6.wav	12.625253	14.799182	11.940218

G. Power Signal to Noise Ratio

To evaluate the security performance of the algorithm, SNR is an important metric to the quality encryption algorithm for evaluated [16].

$$PSNR = 10 * \log_{10}\frac{MAX^2}{MSE} \quad (9)$$

$$MSE=\frac{\sum_{I-0}^{M-1}\sum_{J=0}^{N-1}|I_1\ (i,j)-I_2\ (i,j)|\text{^}2}{M} \quad (10)$$

Received 4 may 2017; Accepted 2 November 2017

ISSN 1811-9212

where I_1 and I_2 plain audio, encryption audio respectively and M is the size of the audio samples. table 3, show the PSNR of the plain audio with encryption audio and the plain audio with decryption audio.

TABLE 3. PSNR.

Secret Audio	Plain -encryption	Plain -decryption
Test1.wav	-7.057408	Inf
Test2.wav	-6.888944	Inf
Test3.wav	-7.037881	Inf
Test4.wav	-6.862787	Inf
Test5.wav	-6.862079	Inf
Test6.wav	-6.972653	Inf

H. Processing Time

The processing time for the chirp test1 wave audio of (13129 sample) was taken 0.705981 sec for the encryption process.

I. Power Signal to Noise Ratio for cover images

To check the performance of cover images after embedding process, PSNR is the important measure for the cover image quality, PSNR was calculated with the flowing equation [17]:

$$\text{PSNR} = 10 * \log_{10} \frac{\text{MAX}^2}{\text{MSE}} \tag{11}$$

$$\text{MSE} = \frac{\sum_{I-0}^{M-1} \sum_{J=0}^{N-1} | I_1 (i,j) - I_2 (i,j)|\text{^}2}{M*N} \tag{12}$$

where I_1 and I_2 cover, stego image respectively and N*M the size of the image. Four images (Sailboat, baboon, Lean, Peppers) with size 512*512 from the USC-SIPI image database were used in the proposed algorithm. Table 4, show the PSNR results for embedding different text wave audio.

TABLE 4. PSNR OF COVER IMAGE.

Secret Audio	Sailboat	Baboon	Lean	Peppers
Test1	**65.742138**	**64.305140**	**64.321189**	**64.313845**
Test2	**62.299154**	**61.741570**	**61.612376**	**61.502130**
Test3	**61.853853**	**61.380235**	**61.353361**	**61.272128**
Test4	**60.072426**	**59.677713**	**59.449917**	**59.543320**
Test5	**57.780981**	**57.679413**	**57.461970**	**57.344786**
Test6	**57.775685**	**57.678915**	**57.499627**	**57.328871**

V. CONCLUSION

Some important conclusions can be found with the proposed algorithm:

- The proposed algorithm was encrypted the plain audio with multilevel which makes increases the security of the plain audio and the cryptanalysis is a difficult task.
- The proposed algorithm is sensitive to the secret key and initial parameters of the chaos system. The key sensitivity was provided the algorithm with high security.

Received 4 may 2017; Accepted 2 November 2017

ISSN 1811-9212

- The key space of the proposed algorithm is a large was reached more than 2672 possible of the key, makes the brute force attack impracticable.
- The recovered audio with the proposed algorithm is high quality.
- Chaos system and secret sharing process with multi-cover images offers additional capacity, security for the secret audio message, and quality for cover images.
- The power signal to noise ratio of cover images reached to 57db with embedding 334 KB (160000 samples) of secret audio with four cover images.

REFERENCES

[1] Srividya L, and P.N. Sudha, "Literature Survey On Recent Audio Encryption Techniques," IJECET, Volume 7, Issue 6, 2016, pp. 91–95.

[2] V. B. Pawar, P. A. Tijare, and S. N. Sawalkar, "A Review Paper on Audio Encryption," International Journal of Research in Advent Technology, Vol.2, No.12, December 2014, E-ISSN: 2321-9637.

[3] Mansi, and R. Chawla, "An Audio Multiple Shuffle Encryption Algorithm," ijecs, ISSN: 2319-7242, Volume 4, Issue 9, Sep 2015, Page No. 14098-14104.

[4] A. S. Hameed, "Hiding of Speech based on Chaotic Steganography and Cryptography Techniques," International Journal of Engineering Research, ISSN:2319-6890, Volume No.4, Issue No.4, pp : 165-172, 01 April 2015.

[5] Rezza Moieni, Subariah Ibrahim, and Leyla Roohi, "A High Capacity Image Steganography Method Using Lorenz Chaotic Map ", ACIT 2013.

[6] Mrs Nilam C. Patil, and Mr.Vijaykumar V. Patil, " Advance Data Hiding in Spatial Domain Image Using Chaotic Map ", IJSETR, Vol.5, Issue.1, January, 2016.

[7] Dr.S.Bhargavi, Shobha .M.J, Swetha.T.N, and Pushpa.M.J,Li Liu, "An Image Steganography Based On Logistic Chaotic Map In Spatial Domain ",IJRISE,vol.1,issue.2

[8] L. Liu, A. Wang, C. Chang, and Zhihong Li, "A Secret Image Sharing with Deep-steganography and Two-stage Authentication Based on Matrix Encoding," International Journal of Network Security, Vol.19, No.3, PP.327-334, 2017.

[9] E. B. Abdelsatir, S. Salahaldeen, H. Omar, and A. Hashim, "A Novel (K,N) Secret Sharing Scheme From Quadratic Residues For Grayscale Images," IJNSA, Vol.6, No.4, 2014.

[10] F. Abd Elzaher, M. Shalaby, and S. H. El Ramly, " Securing Modern Voice Communication Systems using Multilevel Chaotic Approach," International Journal of Computer Applications (0975 – 8887), Volume 135 – No.9, February 2016.

[11] S. N. Al Saad, and E. Hato, "A Speech Encryption based on Chaotic Maps," International Journal of Computer Applications (0975 – 8887), Volume 93, No 4, May 2014.

[12] M. Pandey, "Encrypting Digitized Voice Signals using the Chaotic Behavior of a Nonlinear Discrete Time Dynamical System," Proceedings of the World Congress on Engineering, 2016, Vol I, London, U.K.

[13] Ganesh babu. s, and Ilango. p, "A Speech Encryption based on Chaotic Maps," IEEE, 2013.

[14] A. A. Tamimi, and A. M. Abdalla, "An Audio Shuffle-Encryption Algorithem," WCECS 2014, 22-24 October, 2014, San Francisco, USA.

[15] M. Farouk, O. Faragallah, O. Elshakankiry, and A. Elmhalaway, "Comparison of Audio Speech Cryptosystem Using 2-D Chaotic Map Algorithms," Mathematics and Computer Science, 2016, 1(4): 66-81.

[16] A. Abdulgader, M. Ismail, and N. Zainal, "Robust Audio Encryption Method for MPEG-2 AAC Audio Based on Module Arithmetic and Chaotic Maps," International Review on Computers and Software (I.RE.CO.S.), Vol. 10, N. 1, ISSN 1828-6003, January 2015.

[17] A. S. Shinde, and A. B. Patankar, "Image Steganography: Hiding Audio Signal in Image Using Discrete Wavelet Transform," International Conference On Emanations in Modern Technology and Engineering (ICEMTE-2017), ISSN: 2321-8169, Volume: 5, Issue: 3, 331 - 334.

Received 4 may 2017; Accepted 2 November 2017

ISSN 1811-9212