Transmission of an Encryption Audio Message Using Chaotic Map in a Noisy Channel

Zainab N. Abdulhameed
Al-Anbar University, Engineering College/Electrical Department, Iraq
Email: zaynabnajeeb82@gmail.com

Abstract—For the last decades, the secure transmission of the media including (audio, image and video) is a big issue. In this paper a method of transmitting an encrypted audio message in a noisy channel was implemented, this was done by applying a random two-dimensions map which generated by using two dimensions of chaotic map (Modified Arnold Cat Map MACM) as a key, and the noisy channel used in this work is Addaptive White Gaussian Channel (AWGN). The tests of encryption are performed and the results are observed by Matlab. Also this algorithm was implemented and tested for different sizes of audio files.

Index Terms—Audio, encryption, cat map, noisy cannel

I. Introduction

Now a day's a communication between people was done by using computers and mobile, so that the security was important to secure their personal information in these speech processing. A speech communications become more and more widely used, so improving and increasing a level of security is important and necessary [1]-[4].

In ref. [1] In this work the message is initially encrypted with DES and the keys of DES are encrypted with RSA then the hybrid of both DES-RSA is embedded inside the speech with help of genetic algorithm. Results of the technique provide a stronger security. The encryption time is also faster than the previous techniques as well as brute force attack to this technique is almost not possible.

In ref. [2], a multimedia data (audio sound, grey scale and color images) of different sizes encryption algorithm based 1-D logistic maps is presented. Experimental results show that the proposed approach is really effective and performs with higher security, and very useful for critical data transmission over unsecured open networks.

In ref. [3], the chaotic H ́enon map and the lifting wavelet transforms together with Sine and Cosine hyperbolic functions. The lifting scheme used to own many advantages compared to the ordinary scheme of wavelet transforms. First the audio signal is transformed into a data signal by the lifting wavelet scheme, and then the transformed data is encrypted by the chaotic H ́enon map and Sine and Cosine hyperbolic functions. The key space is considered to be large enough to resist any kind of attack.

Ref. [4] used transposition technique that corresponds to a WAV file extension. The original sounds can be encrypted with various combinations using a password, and the results of randomization sounds can be restored to the original sounds using the correct password. And it is recommended that users need to employ complicated password, such as long-character or mix-character passwords. In other words, the transposition technique is able to ensure the security of audio data files.

II. Cryptography

Defines cryptography as "the art and science of keeping messages secure". Cryptography is the science of protecting privacy and authenticity of information under unfriendly conditions. One of the most used cryptography methods was the encryption. The purpose of encryption is to take unencrypted data, called the plaintext, and produce an encrypted version of it, called the cipher text. The generated encrypted data is called "cipher text". The structure of an encryption session is shown in Fig. 1 [2].

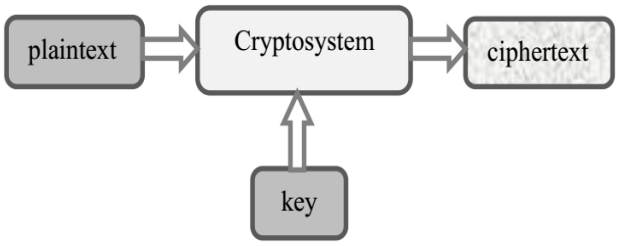


Fig. 1. An encryption session

Mainly, encryption techniques are classified into two categories: Symmetric and asymmetric.

The detailed definitions of these two categories [10]:

A. Symmetric

When both encryption and decryption of the message are used the same secret key. So the sender and receiver must know the secret key in order to handle any secure and fast communication by using this kind of encryption.

Also, this category subdivided into block ciphers and stream ciphers and by this type encryption was done faster.

Manuscript received July 1, 2018; revised January 12, 2019.
doi:10.12720/jcm.14.2.142-147

B. Asymmetric

Asymmetric encryption, defines as the key of encryption is different for that which used for the decryption. The encryption key is public while the decryption key is private. This type of encryption has many advantages like it was practical because there is no necessary to Since there is no need to agree on the sharing of secret key by the sender and receiver. In another side, this type hastwo disadvantages; First it was based on mathematical computations, and it was much slower than the symmetric type.

III. Chaotic System

A chaotic system is a nonlinear deterministic dynamical system which generates a pseudorandom sequences [6]. Due to the important properties of chaos signals, they are considered good for multimedia encryption and increases the robustness of cryptosystem against statistical attacks. These properties includes [5]:

- Pseudo-random
- Non-periodicity
- High sensitive to system parameters
- High sensitive to initial conditions
- Ergodicity
- Mixing

The behavior of a dynamical system is predictable if the initial conditions are known, otherwise the system exhibits randomness [3]. Chaos sequences are generated by the use of difference equations.

A chaotic sequences have a properties which are similar to confusion and diffusion cryptography properties; so they have been used to build good cryptosystems. So, these properties make chaotic cryptosystems strong against statistical attacks [6]. And also using chaos in encryption system will security, complexity, speed, computing power, etc. [2]. One of well-known 2-D chaos sequence is Modified Arnold Cat Map. The Arnold Cat chaotic map is described as follows [5]:

$$\begin{pmatrix} x' \\ y' \end{pmatrix} = \begin{bmatrix} 1 & B + C^2 \\ A & 1 + AB + A\,C^2 \end{bmatrix} \begin{pmatrix} x \\ y \end{pmatrix} \pmod N \qquad (1)$$

where A,B and C are positive integer value assumed to be as a control parameters and (A, B, C) ∈ R, N is the size of the data after converting it to two dimensions, (x, y) is the original data location, and (x', y') are the values of the shuffled data after applying Modified Arnold cat Map (MACM).

MACM can manipulate with the original date by changing it's position, after that and after many iterations depending on the size of the data which used the data will return to it's original position [5].

IV. Addaptive White Gaussian Channel (AWGN) and Signal to Noise Ratio (SNR)

The information theory has a basics such as channel capacity and SNR and they can be defined as:

The maximum limit of information for any channel is a channel capacity, and if any noise occurred or increased tis limit will decreased, Channel capacity is measured in bits per second (bits/s), as in Fig. (2).

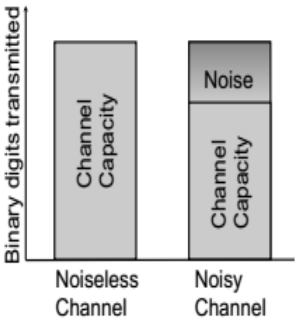


Fig. 2. The channel capacity of noiseless and noisy channels

As a signal pass through a channel, noise will be added as in eq.(2), so the output y is a noisy input signal as in Fig. 3:

$$y = x + \eta \qquad (2)$$

If Gaussian distribution used in the noise then the channel defined as a Gaussian channel [8].

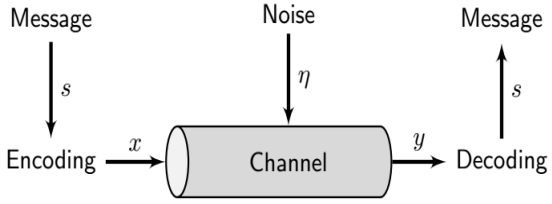


Fig. 3. The communication channel. A message as input to a channel, which adds noise. Recovering the message by the receiver in channel output

SNR measuring the quality of the receiving signal, and it is the ratio of the strength of received signal over the noise strength (noise of the channel and other unwanted signals) SNR measured in decibels and can be evaluated by Eq. (3).

$$SNR=10\log10(SignalPower/NoisePower)dB \qquad (3)$$

if SNR is high this indicate that the source is isolate from the noise and the transmission can be done in high quality[8], [9].

V. Proposed System

The proposed system was designed in MATLAB. The audio message first converted into two-Dimension to diffuse and confuse it by 2-D Modified Arnold cat Map (MACM). For secure system, the key space should be large enough to make sure that the brute force attack is impracticable. Increasing the key length exponentially increases the time that it takes an attacker to perform a brute force attack, when the attacker trying all possible key combinations to break the system.

In this algorithm, the key space of the parameters A,B,C of MACM was large as mentioned above, and

they are ∈ R with positive integer value, the size of the audio message after converting it to two dimensions M,N can be used as keys, so by this procedure the key became large enough to get secure transmission.

Before generating the MACM the initial condition of chaotic map was taken from another random series like PN sequence or another and this became another secure stage on this system.

After that the diffusion will begin which mean the position of the original data was randomized by MACM as shown in Fig. 4 to explain the action of MACM to the position, then the confusion will begin which mean the value of each bit was x-ored with random value generated from MACM so the original value of the data will confuse and became another value in another position as shown in Fig. 5.

1	2	3
4	5	6
7	8	9

a

9	6	3
5	2	7
8	4	1

b

Fig. 4. Changing the position by MACM (a-original position b- shuffled position)

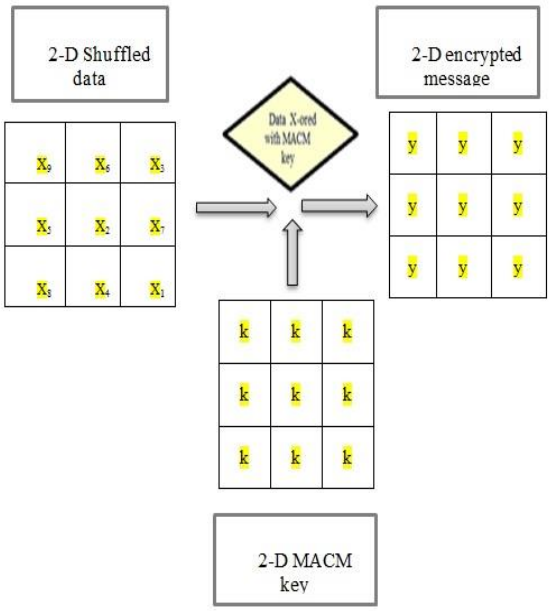


Fig. 5. Confusion process to the shuffled data

All these steps represent the encryption process, while in real world when the message have been sent there is a noise added by a channel, so to discuss this effects of the noisy channel, Additive White Gausian Noise Channel (AWGN) will be used and see it's effect to the received message after the decryption process and then compared the results of the encrypted message and recovered message with the original message while it sent and received on this channel.

Another important issue is determine the correct initial condition to work with the chaotic map , so in the decryption process even it used the correct procedure but with small different in the initial conditions the output will be totally different from the original message .

The decryption process just opposite to the encryption process and all was illustrated in Fig. 6 and in steps below:

A. *Encryption Process*

Step 1: Input the Audio message.

Step 2: Convert to 2-D and use it's Dimensions M*N as a key to determine the block dimension of the MACM in the next steps.

Step 3: Shuffling the order of arrangement by Applying 2-D Modified Arnold cat map.

Step 4: Generate the random seed to the next key.

Step 5: Confusion each bit by X-OR with 2-D Modified Arnold cat map (beginning with random seed in step 4).

Step 6: Transmit into AWGN channel.

Step 7: Cheek the results using NC and SSSNR.

B. *Decryption Process*

Step 1: Receive the encrypted Audio message.

Step 2: Convert to 2-D with size M*N.

Step 3: Generating 2-D MACM to rediffusion

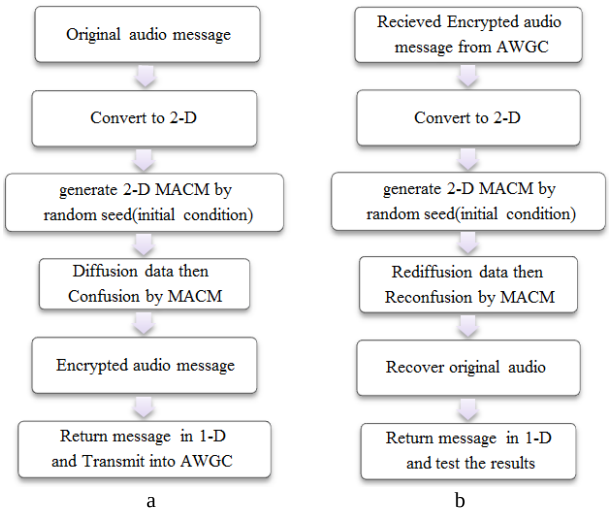
With the correct initial conditions

Step 4: Generate the random seed.

Step 5: Reconfusion each bit by X-OR with 2-D MACM (beginning with random seed in step 4).

Step 6: Recover the audio message and convert to 1-D

Step 7: Test the results by SSSNR and Cor.



a b

Fig. 6. Proposed System (a-Encryption Process b-Decryption Process)

VI. Measuremen Methods

To test the strength of an encryption algorithm before using it in real communication. Otherwise it waste of time and useful resources. several types of tests will be used in testing and measuring the strength of the proposed system[5]. These are:

C. Segmental Spectral Signal to Noise Ratio (SSSNR)

The segmental spectral signal to noise ratio in frequency domain of speech is defined by eq. (4):

$$SSSNR = 10\log_{10}\frac{\sum_{K=1}^{N}|xi(k)|^2}{\sum_{K=1}^{N}[|xi(k)|-|y\mathbf{i}\ (k)|]^2}dB \quad (4)$$

where $x_i(k)$, $y_i(k)$ is the Discreet Fourier Transform of the frames (0,…ith) of the original, encrypted speech samples respectively, as in Fig. 7.

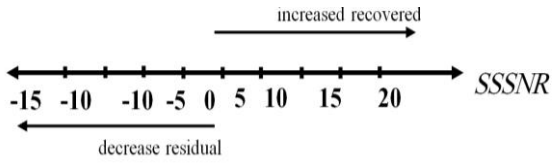


Fig. 7. SSSNR measure

D. Normalized Correlation

Normalized correlation NC measuring the similarity between encrypted message and original message according to eq.(5):

$$NC = \frac{\sum_{k=1}^{QN} M(K)M\prime(K)}{\sqrt{\sum_{k=1}^{QN} M(K)^2}\sqrt{\sum_{k=1}^{QN} M\prime(K)^2}} \quad (5)$$

where M and M´ are original and encrypted message respectively, QN represents number of samples in each one of them [7].

VII. Results

This system was implemented and simulated by Matlab and the important information about it as below: Samples of wav. Extension audio messages with different sizes such as: (24 -37) Kilo Bytes will be used to test this system as shown in Table I.

The values of M and N is 1024,16 respectively which represent the 2-d of the original message as explained above.

And another values are A,B, and C should be known, here in this system A=2313, B=33311 and C=43312

Table I: Results of Proposed System for Different Sizes with SNR=45

Filesize (wav) KB	Encrypted audio		Recovered audio	
	SSSNR	Cor.	SSSNR	Cor.
24.5	-96.184	0.0113	21.1973	0.9962
28	-93.2504	0.0018	23.5034	0.9978
32	-93.43	0.0050	22.9922	0.9975
37	-92.3693	0.0070	22.0454	0.9969

Fig. 8 shows the original audio message (28 Kilo Bytes KB) then the encrypted message and after that when recovered the audio message, and from the figure below it's clear that the recovered message has some different value because of the noisy channel.

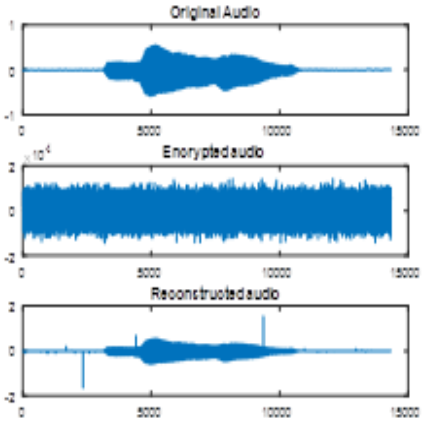


Fig. 8. Encrypted and recovered audio message

To show the effects of transmitted on a noisy channel such as AWGN channel, Table II viewed this effects with different values of SNR (signal to noise ratio).

Fig. 9 shows that when the SNR increased the results of the recovered message will improve (SSSNR increased) due to the decreasing of the noise effects.

Table II: Results of Recovered Audio Message (28KB) with Different SNR Awgn

SNR(AWGN)	SSSNR	Cor.
15	16.9863	0.9890
25	18.332	0.9928
45	24.4615	0.9982
65	32.3307	0.9997

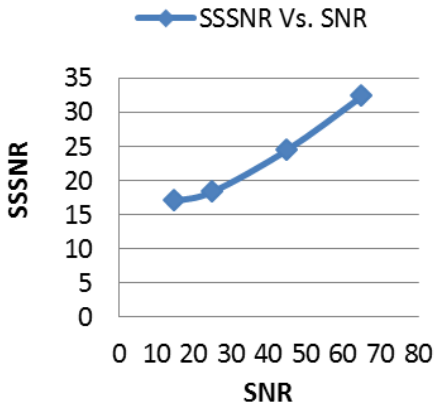


Fig. 9. (SSSNR Vs. SNR)

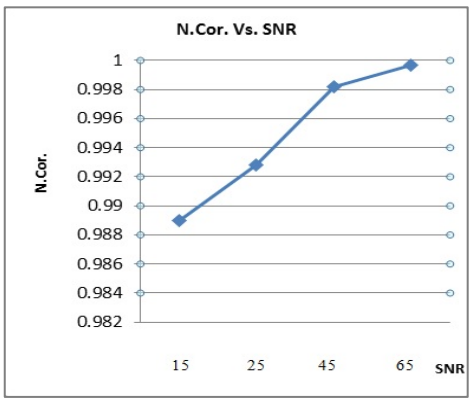
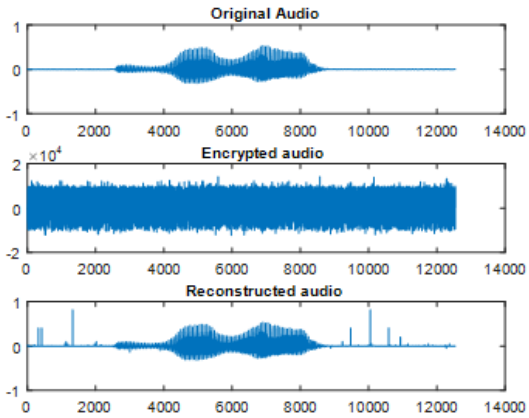
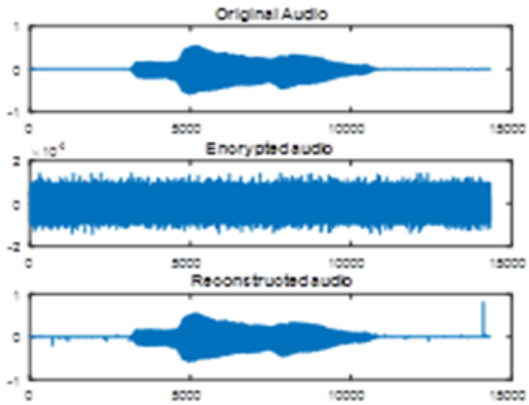


Fig. 10. (SSSNR Vs. SNR)

Also Fig. 10 shows that when the SNR increased the results of the recovered message will improve (Cor. Increased and became near 1) due to the decreasing of the noise effects so SNR increased.



(a)



(b)

Fig. 11. (a-SNR=15 b-SNR=45)

And finally Fig. 11 shows that the effects of the noise on the recovered audio message when SNR = 15 and 45 respectively and also it's clear the second one is better because of the decreasing of the noises power so SNR ratio became greater.

VIII. Conclusion

SSSNR and NC was used as a performance measure of the encryption and decryption process by using the MACM with random initial condition to randomize the audio file and from the measurement results of this system, which shows the robustness of this system because of the used of chaotic map with many keys and this can be used to add security to the audio files and increase the encryption efficiency. The original sounds can be encrypted with various combinations of initial conditions, and the results of recovered message can be restored to it's origin using the correct initial condition of MACM. Also increasing key space by using many parameters for the chaotic sequence and for reshaping the audio file (as a secret key) makes a brute-force attack on the algorithm difficult. System implementation is easy and it requires a short time, the proposed algorithm is implemented and tested for wave extension and it can be extended for another ones and for a big size of the audio files.

IX. Future Works

For the future work, this algorithim can be implemented with high dimentions chotic maps such as Lorenz, etc. and can used the filters to decrease the noise effects and improve the quality of the recovered messages.

References

[1] E. J. Sharma and J. Rani, "An efficient hybrid approach for secure speech cryptography," *International Journal of Computer Science and Mobile Computing*, vol. 6, no. 1, pp. 23–29, January 2017.

[2] B. Boulebtateche, M. M. Lafifi, and S. Bensaoula. A multi media chaos-based encryption algorithm. [Online]. Available:https://www.researchgate.net/publication/228437181

[3] A. Roy and A. P. Misra, "Audio signal encryption using chaotic h ́enon map and lifting wavelet transforms," arXiv.org , cs , arXiv: 1708.08021, Aug. 23, 2017.

[4] A. Jawahir and Haviluddin, "An audio encryption using transposition method,: *International Journal of Advances in Intelligent Informatics*, vol. 1, no. 2, pp. 98-106, July 2015.

[5] H. N. Abdullah-MIEEE and H. A. Abdullah, "Image encryption using hybrid chaotic map," in *Proc. International Conference on Current Research in Computer Science and Information Technology*, Slemani – Iraq, April 2017.

[6] A. V. Prabu, S. Srinivasarao, T. Apparao, M. Jaganmohan, and K. Babu Rao, "Audio encryption in handsets," *International Journal of Computer Applications*, vol. 40, no. 6, February 2012.

[7] A. A. Tamimi and A. M. Abdalla, "An audio shuffle-encryption algorithm," in *Proc. World Congress on Engineering and Computer Science*, San Francisco-USA ,October 2014.

[8] J. V Stone, "Information theory: A tutorial introduction," arXiv.org , cs , arXiv: 1802.05968v2, Feb. 2018.

[9] D. K. Chy and M. Khaliluzzaman, "Evaluation of SNR for AWGN, rayleigh and rician fading channels under DPSK modulation scheme with constant BER," *International Journal of Wireless Communications and Mobile Computing*, vol. 3, no. 1, pp. 7-12, 2015.

[10] Mansi and R. Chawla, "A review on audio cryptography," *International Journal of Modern Communication Technologies & Research*, vol. 3, no. 7, July 2015.

Zainab N. Abdulhameed was born in Baghdad, Iraq, in 1982. He received the B.S. in electrical engineering degree from the Mustansiriyah University, college of engineering, Baghdad, Iraq in 2004 and the M.S. degree from the Mustansiriyah University, college of engineering, Baghdad, Iraq in 2014, in electronics and communication engineering. Her research interests include communication security, signal processing, and information theory