# Data Hiding of Stream Cipher in Audio File using Random Permutation Technique

Asmaa A. Jaber
Department of Computer Science,
College of Science,
University of Basra, Iraq

Hameed A. Younis
Department of Computer Science,
College of Science,
University of Basra, Iraq

## ABSTRACT

The universal development of computer and communication technologies and the spread of network on a global scale, has led to the appearance of numerous techniques for the transmission of confidential information such as cryptography. Because of the hacking and breakthrough of these technologies, the need for more sophisticated and difficult techniques and methods to transfer confidential information in a secure manner. Steganography is where secret information is hidden in a way that does not allow the third party to know hidden information. It is added with stream cipher to increase the security of information transmission and uses media such as, image, audio, text or video as a transmission medium for that information.

The aim of this paper is to use a method to hide confidential information (image or audio) into audio file as a cover in such a way as to certify that hacking does not reach that information by making the size of the cover equal to the size of the original file. The audio file resulting from the masking process is similar to the original file and the human ear can not sense the change between them. By splitting the original audio cover into frames and applying the random function to the clutter of the hiding locations after separating the layers of the color image in the case of the confidential information image or fragmentation of the audio to be hidden into frames and then applying this function to select hiding locations.

In the case of retrieval, the process is reversed where the embedded audio file is fragmented stego-audio and apply the random function to select hiding locations. In the audio segmentation process, we use a key that represents the size of the image to be hidden, as well as frames, and serves as a cryptographic key for the original voice to increase security. The success rate of image recovery was obtianed. The sound retrieval process was also good.

## General Terms

Data Hiding, Random Permutation.

## Keywords

Steganography, Stego-Audio, PSNR, SNR, Stream Cipher.

## 1. INTRODUCTION

Over the past years, the information security has become the focus of researchers' efforts to ensure the safe transfer of information through networks, especially the Internet, without any breach of this information. The result of the continuous increase in the use of the networks and the computers at present has a significant impact on the need to provide security measures to deliver the information to the person authorized in a manner that does not give rise to suspicion and attention and prevent the intruder or thief from tampering with them and change the content, so all security technologies, both in the field of cryptography and concealment information hiding, have one-way which aims at protecting the content of the data and information and preventing it from changing and communicating to none but the properly authorized person [1].

Steganography is a method of protection that makes incoming and outgoing data invisible by hiding certain messages within a particular cover. The objective of the concealment process is not to raise any doubt about the existence of hidden data, whereas the goal of the concealment analyzer is to suspect all messages sent, and to check them to make sure of the existence of the hidden data. The process in which a party attempts to detect, read, change or delete hidden information is called a *steganoanalysis*. Steganography can be defined as the art of masking a message which is different from cryptography that relies on hiding the meaning of the message and not enabling the unauthorized person to understand the content. It is different in concealing that the unintended person will not be able to know that there is a message in any form [2].

The wider area of this art is the integration of messages with sound files, images and videos in a way that prevents detection, and there are three main factors that can affect the concealment of messages in the digital files: the first factor is the amount to hide, the second one is the extent of contrast and the similarities in the data to hide the message within so as not to discover the difference easily between the compact data and original data, and the third is the immunity of the original data against detection and attacks. However, the main problem with data hiding is that it requires a relatively large audio file if the message is large, and the discovery of the message will lead to the knowledge of its contents directly, which requires encryption keys to hide the content, which needs more size in the cover file to show how to hide the sound [2].

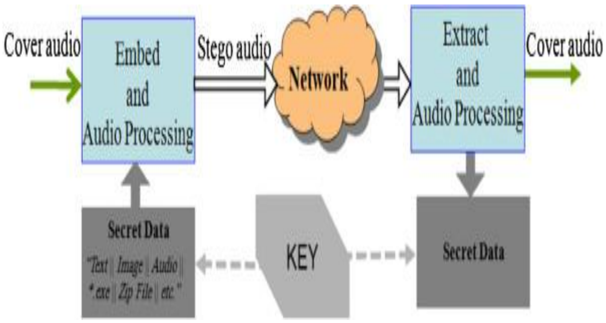

Cover audio
Embed and Audio Processing
Stego audio
Network
Extract and Audio Processing
Cover audio
Secret Data
"Text | Image | Audio | *.exe | Zip File | etc."
KEY
Secret Data

**Fig 1: Hide in audio.**

Because of the urgent need for this modern system both in terms of security and personality, many researches have been conducted despite the fact that it is so. In 2005, Abdul-Lateef, A**.,** [3] introduced a system that hid text in an audio file based on the phase coding method. The system hides the confidential message data of a text file in any sound file (wave _ mono) so that the output system is an audio file that is similar to the audio file used as a masking medium. In 2013, Parmar, S. B., *et.al*, [ 4] have presented a method to hide text in the center of audio using the technique (LSB), after converting the text to the code (ASCII), and then converting it to Binary Values and entering the process of inclusion after leaving the header of the file cover sound using the technique (LSB). In 2015, Bah, J., Ramakishore, R., [5] proposed a way to hide the secret message (text) in an audio file using parity to encode the text and hide it in the top layer of LSB and achieved high robustnees. [6] Abdul-Kareem, H., *et.al,* A.suggested a way to hide multimedia data (text, sound, and binary image) into color image data, the proposed method is to store data bits in the third layer (LSB3) rather than the first layer (LSB1). Data was scrambled by using a key before the masking process to increase security.

## 2. BASIC PRINCIPLES

### 2.1 Encryption of Minimum Or Least Signififcant Bit LSB Coding

It is a simple and common way to embedded data by replacing the least significant bit in the cover file to hide a string of bytes, i.e., equivalent to binaries of a secret message, and the advantages are the simplest way to embed information in an audio file it allows a large amount of data. Less significant bits (LSB) are one of the hidden writing methods used in the audio and video field. It is a common and easy way to hide large amounts of confidential data in the cover or the chosen host medium. It processes information directly, can re-embed data several times, and provides good system security. It is an ephemeral method because it depends on the substitution and compensation processes that get the unused bits (LSB). It is also vulnerable to interference from sound modulation, providing noticeable noise in the audio file [7, 8].

The process of concealment is to replace the bits of the least significant bits (LSB) of the selected cover or medium and to compensate them for bits of the secret message using different techniques.

### 2.2 Wav File Format Structure

This search was treated with wav type audio files. The latter is a special kind of file called *Resource Interchange File Format (Riff Files)*, a general file known by *Microsoft* that is currently used in Windows systems and there are two types of RIFF files [3]:

Type I: Which is known as *WAV File* and deals with audio files.

Type II: Which is known as *AVI File* and deals with video files.

### 2.3 Stream Cipher

The cryptographic coding system divides explicit text M into binary orders (m1, m2,m3,.....) or sequential codes, and encrypts each mi using ki from the sequential key (k1, k2, k3, .....), that [9]:

$$E_K(M)=E_{K1}(m_1)E_{K2}(m_2)E_{K3}(m_3)... \qquad ...(1)$$

These systems are periodic when the sequence is a periodic key with a cycle of length (d) which repeats itself after (d) code.

The cryptographic coding system consists of two main parts [9]:

1. Sequence generation key algorithm.

2. Mixer (XOR).

The algorithm generates a sequential key based on a key that feeds it and then blends the sequence generated with the explicit text of the carburetor to generate the enccrypted text.

If the binary system is used to represent explicit text and encoded text, the carburetor is the combination of XOR.

Encryption process is done as follows [9]:

$$C_i = P_i \oplus K_i \qquad ...(2)$$

$$P_i = C_i \oplus K_i \qquad ...( 3)$$

$P_i$: plaintext, $K_i$: encrption key, $C_i$: ciphertext.

### 2.4 Ramdom Function

We used the random function to generate correct random numbers within a specified range. One of the disadvantages of this function is to repeat the numbers within the specified periods. We have updated them according to a special approach to obtain a certain number of correct random numbers generated from them and not repeated.

## 3. THE PROPOSED DATA HIDE METHOD

The hidden write system is composed of two separate main phases, the sender's first phase, hide secret message, the second phase of the receiver, extraction the secret message, according to the following algorithms:

### ➢ The Algorithm for Hiding the Image into Audio File is:

1. Read the audio of the wav-type as cover.
2. Split audio into frames to generate as binary matrix and number of frames (No. frames) as the key to the extract phase.
3. Read the color image.
4. Separated into three layers (RGB).
5. Encrypt the color image using stream cipher encryption.
6. Configure each layer to a frame the size of the dimensions of the image to be hidden: (x * y).
7. Generating the random function.
8. Perform the embedded process by the positions generated by the correct random number function.
9. The Output will be Stego-Audio.

### ➢ The Algorithm for Image Extraction from Audio File is:

1. Read the audio object file (Stego-Audio).
2. Perform the process of fragmentation of the sound (Stego-Audio) frames and according to the key of the partation.
3.Apply a function to locate the random function.
4. Combining the frames of the hidden image.
5. Decrypt the image using stream cipher.
6. Output of secret image.

### ➢ The Algorithm for Audio Hide into Audio File is:

1. Read the audio file cover of wav type.
2. Split the sound into frames and create a binary matrix and the number of frames as the key to the extract phase.
3. Read the audio file to be hidden (secret).
4. Encryp of the sound to be hidden using the stream cipher.

5. Split the sound file (secret) into frames and create a binary matrix and the number of frames.
6. Generate the random function.
7. Select the hiding locations according to the random number function and include the audio frames in the audio cover file.
8. The output will be Stego-Audio.

## ➢ The Algorithm for Extract Audio from Audio File:

1. Read the audio file (Stego-Audio).
2. Perform the process of fragmentation into frames and according to the partation key.
3. Implement the random function to determine where the audio file is hidden.
4. Combin the frames of the sound that is hidden in those locations.
5. Convert secret audio to a one-dimensional matrix.
6. Decrypt secret audio using stream cipher.
7. The Output will be audio secret.

As in the following Fig 2. 2

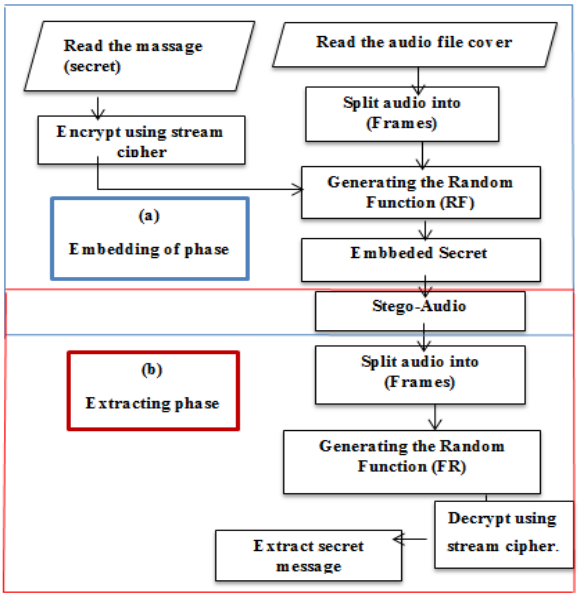

Read the massage (secret)
Read the audio file cover
Split audio into (Frames)
Encrypt using stream cipher
Generating the Random Function (RF)
(a)
Embedding of phase
Embbeded Secret
Stego-Audio
Split audio into (Frames)
(b)
Extracting phase
Generating the Random Function (FR)
Decrypt using stream cipher.
Extract secret message

**Fig 2: (a) Embedding of phase ,(b) Extracting phase.**

## 4. EXPERIMENTAL RESULTS

The following equations have been used as measures for retrieving images. Measuring the aspect ratio and the noise ratio between the original audio file and the sound file (stego-audio).

**1. Mean Square Error (MSE):** These parameters are defined by the following equation:

$$MSE = \frac{1}{M \times N} \sum_{x-0}^{M-1} \sum_{y=0}^{N-1} \left[ B(x,y) - A(x,y) \right]^2 \quad ..(4)$$

when:

A(x, y): The original image matrix.

B(x, y): Retrieved image matrix.

M, N: Number of rows and columns in sequence.

**2. Mean Absolute Error (MAE):** These variables are defined by the formula:

$$MAE = \frac{1}{M \times N} \sum_{x-0}^{M-1} \sum_{y=0}^{N-1} \left| \left[ B(x,y) - A(x,y) \right] \right|$$

...(5)

when:

A(x, y): The original image matrix.

B(x, y): Retrieved image matrix.

M, N: Number of rows and columns in sequence.

**3. The Peak Signal To Noise Ratio (PSNR):** These variables are defined by the equation:

when:

Dr: Range the largest number of dynamic image data.

**4. Signal To Noise Ratio (SNR):** Which are defined as follows [3, 10]:

$$MSE = \sum_{i=1}^{n} \left| Origialsample(n) - Newsample(n) \right|^2 \quad ...(7)$$

n: Audio file size.

Originalsample (n): The size of the original sample.

Newsample (n): Stego sample size.

$$SNR = 10 \log 10 \frac{Soundsize^2}{MSE} \quad ...(8)$$

when: Soundsize: : Audio file size.

**5. Root Mean Sequare Error (RMSE) [10]:**

$$RMSE = \sqrt{\frac{1}{n} \sum (X(i) - Y(i))^2} \quad ...(9)$$

Calculate the sequre error between two arrays.

## 4.1 Experimental Results of the frist phase hide image

### Experiment 1

A color image has been hidden in size (128*128) which (49152 bytes) in the audio file of type (wav, mono) in size (95302665 bytes) and the ratio noise was PSNR (99.0 dB) and the message retrieval ratio (image) is high resolution SNR for sound (98.1195 dB) , RMSE (2.405*$10^{-7}$).

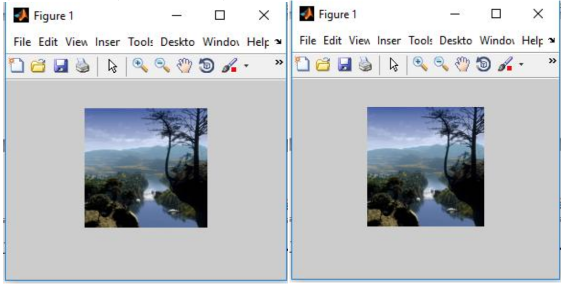
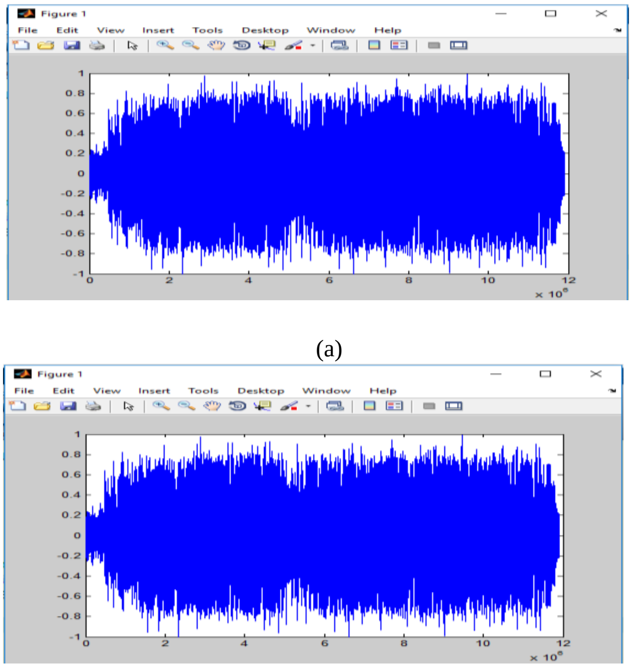


Figure 1
File Edit View Insert Tools Desktop Window Help
Figure 1
File Edit View Insert Tools Desktop Window Help

(a) (b)

Fig 3: a) Image befor; b) Image after hiding.



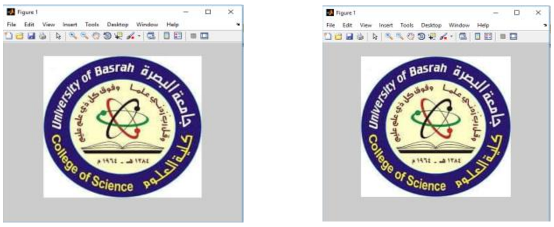
(a)

(b)

Fig 4: a) audio file (cover); b): audio file (stego-udio).

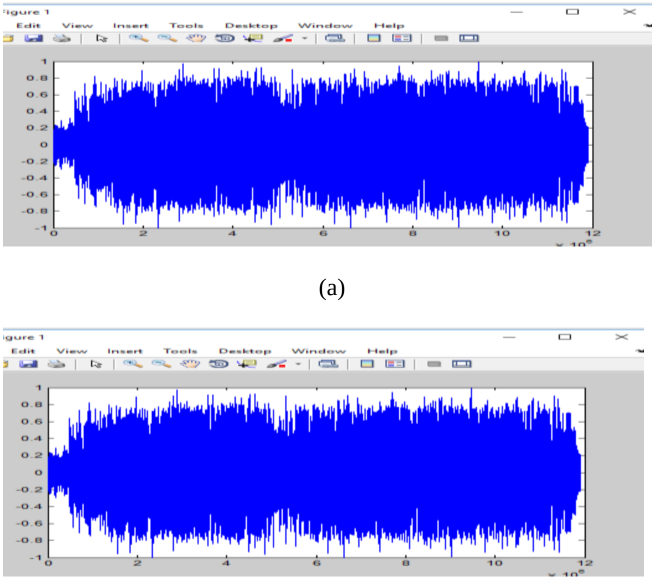
## Experiment 2

A color image has been hidden in size (256*256) which (196608 bytes) in the audio file of type (wav, mono) in size (95302665 bytes) and the ratio noise was PSNR(99.0 dB) and The message retrieval ratio (image) is high resolution SNR for sound (92.5943 dB), RMSE (1.2057*$10^{-7}$).



(a) (b)

Fig 5: a) Image before hiding; b) Image after hiding.



(a)

(b)

Fig 6: a) audio file (cover); b): audio file (stego-udio).

Table (1): embedded ratio and The noise values are in an audio-type (mono).

| **No. Exprement** | **Image size secret)((Byte)** | **PSNR (dB)** | **SNR (dB)** | **RMSE** |
|---|---|---|---|---|
| **1** | 64*64 | 99.0 | 98.2865 | 4.8103*$10^{-7}$ |
| **2** | 128*128 | 99.0 | 94.1278 | 2.3926*$10^{-7}$ |
| **3** | 160*160 | 09.0 | 92.2218 | 1.9135*$10^{-7}$ |
| **4** | 192*192 | 99.0 | 89.1956 | 1.5871*$10^{-7}$ |
| **5** | 256*256 | 99.0 | 82.6203 | 1.9018*$10^{-7}$ |

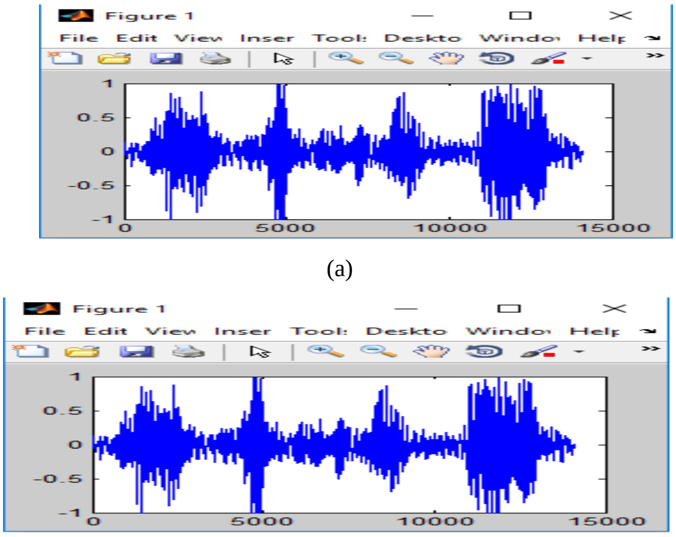
Table (2): embedded ratio and the noise values in an audio-type (stereo).

| **No. Exbriment** | **Size image secret) (Byte)(** | **PSNR (dB)** | **SNR (dB)** | **RMSE** |
|---|---|---|---|---|
| **1** | 49152<br>(128*128) | 99.0 | 98.6201 | 6.2931*$10^{-7}$ |
| **2** | 76800<br>(160*160) | 99.0 | 95.1812 | 5.3020*$10^{-7}$ |
| **3** | 110592<br>(192*192) | 99.0 | 91.9115 | 3.0408*$10^{-7}$ |
| **4** | 196608<br>(256*256) | 99.0 | 88.9794 | 2.2424*$10^{-7}$ |
| **5** | 307200<br>(320*320) | 99.0 | 85.5704 | 1.5830*$10^{-8}$ |

## 4.2 Experimental Results of the Second Phase Hide Audio

### Experiment 3

Wav-mono (7867 byte) is hidden in the wav-mono audio file (95302665 bytes) and SNR is between cover-audio and stego-audio (83.5471 dB) and The SNR ratio between secret-audio and exctrated audio is (98.67881 dB).



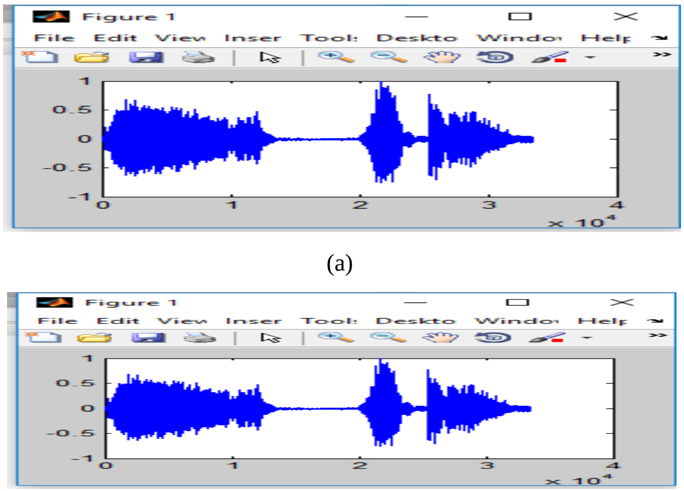
(a)

(b)

Fig 7: a) Secret audio file before hiding; b): Audio file after extraction.

## Experiment 4

Wav-mono (34506 bytes) is hidden in the wav-mono audio file (95302665 bytes) and SNR is between cover-audio and stego-audio (85.5129 dB) and The SNR ratio between secret-audio and extracted audio is (90.5434 dB).



(a)

(b)

Fig 8: a) Secret audio file before hiding; b): Audio file after extraction.

This method was proposed to ensure the security of the transmission of confidential information through the network and not to penetrate it or to know the existence of this information only by the sender and recipient because the rate of confusion in the audio file carrier is little or not. Also, the size of the original file itself not to draw attention by the hacker and the difficulty of extracting this information is because of more than one key.

The success of this method according to the results in the above experiments was:

1. The image is resized for minimizing the noise and the probability of the sound is a small, this lead to facilitate in hidding information process.

2. The combination between data hidden techniques and cryptography operations gave more confidentiality for the hidden message

3. The experiments have been done on sound file of type (wav-mono), as well as, the file of type (wav-stereo) and scaled the confidentiality image, the PSNR values between the secret image and retrieved was (99.0 dB), this mean it was identical to the original.

4. The SNR values (the ratio of the noise sound signal between the original and modified signal) were proportional with the size of a secret image. Since, when the SNR value was minimized, the noise ratio in the embedded sound file was minimized also.

5. If the sound file (loudly music or spoken) it is difficult for the human ear sensing noise or confusion that given agood results from the additional confidential information.

6. In the experiments of hiding a secret sound file, the retrieve ratios of the secret sound was ranged between (80-90)% and it was audible.

# 5. DISCUSSION AND CONCLUSIONS

The methods of hide secret information in audio media in steganography play an important role in securing information and transmission it by the sound which is one of the most popular medium today. There are many local and international researches in this field. In this paper, we were a design system for hiding file (audio or image) in an audio file based on the embedded method by splitting an audio into frames and added the confidentiality message to produce (stego-audio).

The basic idea of the program is based on using the data of the audio frame which is chosen and exploit it in hiding data frame of a confidentially message. This method is based on three keys, the first key for splitting the original audio file into frames and the another one for concealment, as well as, the stream cipher key. Whereas, the system consists from two basic phase: the first phase is embedding process that produces audio file called *audio -stego* and it were in the same size of the original audio.

The second phase is extraction process that extracts the data of the secret message and it is an opposite process of embedded.

The practical experiments was proved the efficiency of the proposed method in the concealment operation that emerged through achieved the goals that are the backbone of the security system as following :

## ➢ Data Security

It is the most important of the security goal and in the first level. The high security is stand out in this work through the complexity that provided by the system in its operation and accuracy in understanding and comprehension the steps of concealment based on:

First, use keys for concealing and retrieves and it in hiding position known only between the sender and receiver, also chose random embedding positions that is based on the function of random numbers which was the main function in the generation of the random values and those non-repetition positions. Also, the encryption added security and the confidentially to the information. Since, even if the concealment was discovered, it is difficult to know the content of the information.

The combination between steganography technique and cryptography operation gave more confidentially to the hidden message. Also, the concealment method by using secret key gave more confidentially to the transmitted data. The stream cipher was chosen because of its fast implementation and the ease of avoiding errors in case of their occurrence and its uses in scientific applications.

### ➢ Capacity of Embedded

It represents the embedded capacity of confidential message (audio or image) in the audio file which is chosen as conceal a medium. The practical experiments were proved the efficiency of the embedded capacity through depending on the size of the audio file. Since, the capacity of the embedded data is proportional to the capacity size of the concealment sound medium (cover), also the size of the secret message (image, audio) .

### ➢ Perceptual Transparency

This property determines the similarity between the original and extracted message during signal processing and attacks that the noise ratios are not noticeable, whereas it is difficult to know the presence of the embedded a secret message. Use of frequent frequency audio files was preferred and avoiding the audio files that content flat audio period because it was more a vulnerable to the impact after the concealment . The audio is considered as the best medium for transmitting data although it is difficult to deal with it. So, the techniques of coverage exploit the characteristics of the human perception system and exploit the weaknesses of this system.

## 6. REFERENCES

[1] Alturki, F. , & Mersereau, R. 2001 A Novel Approach for Increasing Security and Data Embedding Capacity in Images for Data Hiding Applications. In Information Technology: Coding and Computing, Proceedings. International Conference, PP. 228-233, IEEE.

[2] Djebbar, F., Ayad, B., Meraim, K. A., & Hamam, H. 2012 Comparative Study Of Digital Audio Steganography Techniques. EURASIP Journal on Audio, Speech, and Music Processing.

[3] Abdul-Lateef, A., 2005 Text Embedded in Audio Steg System Design. A Thesis Master, Dept. of Computer Science, College of Science, University of Basrah.

[4] Parmar, S. B., Pokharna, P. P., & Patil, A. B.2013. A Conceptual Study of Various Data Hiding Techniques – A Review. International Journal of Advanced Research in Computer Science and Software Engineering, Vol. 3, Issue 2.

[5] Bah, J., & Ramakishore, R., 2015. Audio Steganography Using Parity Method at Higher LSB Layer as a Variant of LSB Technique. International Journal of Innovative Research in Computer and Communication Engineering.

[6] Abdul-Kareem, H., &Y., Ahmed, I. A. 2016 Multimedia Data Hiding: Three-in-One. The Forth Scientific Conference of the College of Science University of Kerbala.

[7] Kekre, H. B., Athawale, A., Rao, S., & Athawale, U. 2010. Information Hiding in Audio Signals. International Journal of Computer Applications, Vol. 7, No. 9, PP. 0975 – 8887.

[8] Gupta, N., & Sharma, N. 2013. Hiding Image in Audio using DWT and LSB . International Journal of Computer Applications, Vol. 81, No. 2.

[9] Adul Kaream, H., 2000 Attacking Stream Cipher Systems Using Genetic Algorithm, A Thesis Of Master, Deptment. Computer Science, College Science, University Of Basrah.

[10] Chai1, T. , & Draxler, R. R. 2014. Root Mean Square Error (RMSE) or Mean Absolute Error (MAE)? – Arguments Against Avoiding RMSE in the Literature. Geosci. Model Dev., Vol. 7, PP. 1247–1250.