



## Transposition Technique Based Efficient Data Hiding Using Audio Frames

**Seema Payal**  
Student, ECE, PPIMT,  
Hisar, India

**Abstract:** This paper is for study the cryptographic and Steganographic methods needs for security purposes. The combination of these techniques provides the better security because of the hidden property of Steganography and encryption property of cryptograph as there is need of transmission security of data over network. The paper has been proposed the transposition technique and then the information hiding steps will hide the information. The data matrix will form and transposition will change the location of data matrix in the route of zigzag and it will be start from one position in the matrix. By following these steps, the information will be converted to encrypted form. The cryptographic transposition method's output further will be hidden in audio frames by the Steganographic technique known as LSB (Least Significant Bit). The media Steganography takes the cryptographic out as input for embed in the audio frames. This paper has been described an efficient way to secure the information and helpful for secure data transmission.

**Keywords:** Transposition, Steganography, Cryptography, Audio, LSB.

### I. INTRODUCTION

Encryption transforms data into an unusable form, reducing the risk in the case of unauthorized access. There are many research studies in the database security field. Some of them have efficient implementations. Also, many encryption algorithms have been proposed, some of which have appealing features but still need further development, one such algorithm is the Transposition. Once employed only for the most sensitive government secrets, encryption is today a common practice with strategic importance for businesses of all types. Financial institutions, retailers, healthcare providers, and others must protect customer information and are often bound by data breach disclosure laws. All types of businesses must keep private their diverse information about employees, customers, business operations, and intellectual property. Given that failure to protect confidential information may be not only embarrassing but also illegal, it's easy to see why encryption is becoming a core component in a broad data protection and IT security strategy. Transposition transformation changes the location of the data matrix elements by using diagonal transposition that reads the data matrix in the route of zigzag diagonal starting from the upper left corner after getting the data.

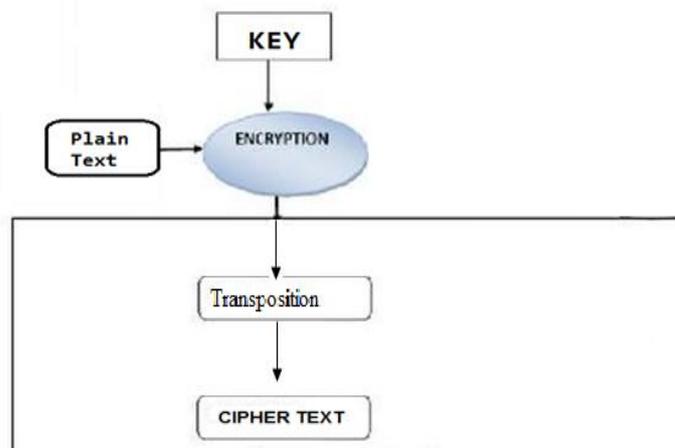


Fig 1 Graphical Representation of Transposition Encryption

Least significant bit (LSB) coding is the simplest way to embed information in a digital audio file. The LSB Technique is widely used for protecting the information. In this, the sampled output of the Audio file will be generated which will be substituted by the least significant bit of each sampling point with a binary message. Least Significant bit (LSB) technique allows for a large amount of data to be encoded.

The message 'HEY' is demonstrated by the below diagram:

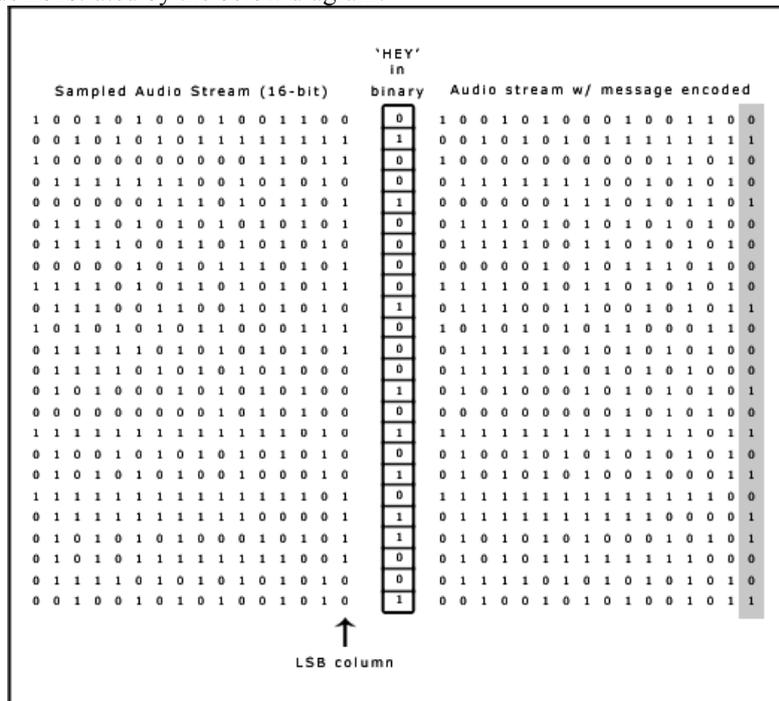


Figure 2 Low-Bit Encoding Technique

It performs bit level manipulation to encode the message. The following steps are

- a. Receives the audio file in the form of bytes and converted in to bit pattern.
- b. Each character in the message is converted in bit pattern.
- c. Replaces the LSB bit from audio with LSB bit from character in the message.

## II. LITERATURE REVIEW

The researchers has been studied the multiple approaches for secure the information and even the encryption, the hiding is still the main aspect. The authors has been researched the different techniques and mentioned in this our survey.

The author has been proposed the audio Steganography and the techniques for hiding the information in the particular carrier. They explained that increased use of electronic communication has given birth to new ways of transmitting information securely. Audio steganography is the science of hiding some secret text or audio information in a host message. The host message before steganography and stego message after steganography have the same characteristics. Least Significant Bit (LSB) modification technique is the most simple and efficient technique used for audio steganography. The conventional LSB modification technique is vulnerable to steganalysis. The author proposes two ways to improve the conventional LSB modification technique. The first way is to randomize bit number of host message used for embedding secret message while the second way is to randomize sample number containing next secret message bit. The improvised proposed technique works against steganalysis and decreases the probability of secret message being extracted by an intruder. Advanced Encryption Standard (AES) with 256 bits key length is used to secure secret message in case the steganography technique breaks. Proposed technique has been tested successfully on a. wav file at a sampling frequency of 8000 samples/second with each sample containing 8 bits [1]. The another author explained the hiding techniques with different strategy. Steganography is an information hiding technique where secret message is embedded into unsuspecting cover signal. Measurement of good steganography algorithm includes security, capacity, robustness and imperceptibility. These measures are contradicted, therefore improving one, affects the others. In this paper, they propose a new high capacity audio steganography algorithm based on the wavelet packet transform with adaptive hiding in least significant bits. The adaptive hiding is determined depend on the cover samples strength and bits block matching between message and cover signals. The results show that message can be embedded up to 42 % of the total size of the cover audio signal with at least of 50 dB signal to noise ratio [2].

The author [3] explained that the Security has its importance and application in wide area. It is a measure of human negligence, in desire to seize the latest technological inventions. This measure may have adverse effect on human perception to the deployment of application, which needs serious concern in terms of security. Audio steganography is a technique used to transmit hidden information by modifying an audio signal in an imperceptible manner. The main challenge in audio steganography is to obtain robust high capacity steganographic systems. The author provides implementation of two level encryption of user data by combining two areas of network security, cryptography and steganography. The combination of LSB technique with XORing method is described in this paper, which gives additional level of security. Varieties of techniques for embedding information in digital audio have been established. They attend the general principles of hiding secret information using audio technology, and an overview of functions and techniques [3].

The idea of author is to invent a new strategy in Steganography to get the minimum effect in audio which is used to hide data into it. Progress always involves risk and Fredrick Wilcox observed that technological progress of computer science and the Internet altered the way we lived, and will continue to cast our life. In this paper they have presented a Steganography method of embedding text data in an audio file. The basic approach behind this paper is to provide a good, well-organized method for hiding the data and sent to the destination in safer manner. In the proposed technique first the audio file is sampled and then appropriate bit is modified. In selected sample one bit is modified at least significant bit .The remaining bits may be used but it may be cause noise. They have attempted to provide an overview, theoretical framework about audio Steganography techniques and a novel approach to hide data in an audio using least significant bit (LSB) [4].

In this paper, author has proposed a new Steganography algorithm that is used to hide text file inside an image. In order to increase/ maximize the storage capacity they have used a compression algorithm that compresses the data to be embedded. The compression algorithm they have used works in a range of 1bit to 8 bits per pixel ratio. By applying this algorithm they have developed an application that would help users to efficiently hide the data. This paper proposed a new Steganography algorithm for hiding text files in images. Here they have also used an underlying compression algorithm with maximum compression ratio of 8 bits/ pixel. They have developed a system in java based on the proposed algorithm. Here they have tested few images with different sizes of text files to be hidden and concluded that the resulting stego images do not have any noticeable changes. Also they found that for .bmp images this algorithm works very efficiently. Hence this new Steganography approach is robust and very efficient for hiding text files in images [5].

### III. OBJECTIVES

In the research scenario, the information needs to be secured over the internet such as for the online payment transfer, secure documents transmission. This information's should not be altered in any circumstances. So, the main objective of this research is explained as:

1. To study the existing security and Hiding techniques.
2. To implement transposition based encryption of information.
3. To hide the encrypted information in sound frames.
4. To analyze the security of the proposed work to check the vulnerability in proposed work.
5. To generate the real working of the algorithm using development language.

### IV. PROPOSED METHODOLOGY

There are some steps need to be follow until the research will be completed. These steps will helpful to design the security algorithm. These are elaborated as:

1. Study the Steganography and Transposition Working.
2. Analyze the Point of Security Implementation and study the flow of working.
3. Generate the new flow development for enhance the security over network transmission.
4. Implement the proposed technique in any of the programming language.
5. Generate appropriate results and graphs.
6. Source of Research will be internet, Web Sites and Journals.

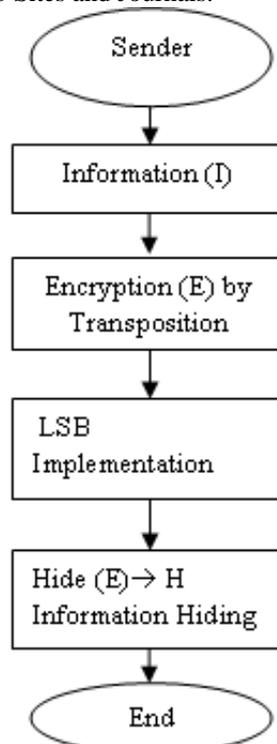


Fig 2 Flow Chart

## V. APPLICATION

1. Confidential transmission and store protected data:  
The confidentiality of the hidden and embedded data is the critical in transmission.
  - a. It provides the method to hide the confidential information.
  - b. Difficult to analyze the hidden information or embedded data and pattern.
  - c. Strengthen the secrecy of the cipher information.
2. Data Integrity Provision for assure and maintain accuracy.
3. Resource Protection using access control system for content sharing:  
The information sharing over the network is common now days. The example can be of music industry which release the latest music albums and distribute over the network. In this scenario, the content is shared equally to the user and they can easily access it by accessing the particular page. The sharing cannot be to the specific user or to page requested user. So the information is hidden and publicizes it to the user which can be further transmitting to the customer either by E-mail service or by social web services.
4. Databases for Media Files  
In this media Databases system, the problem is the separation of data from the media files such as image, sound, etc. There is need to associate the Media data such as picture, movie, etc with media database system. A photo picture, for instance, may have the following.
  1. Time and Data of Picture Snapshot.
  2. Electronic Devices information such as camera information.
  3. The picture's information.

## VI. CONCLUSION AND FUTURE WORK

In the paper, we have been explained the concept of security algorithm, the transposition technique and LSB Data Hiding technique. The encrypted information will be hide in audio frames using the least significant bit and the proposed work's implementation is under research and will be explained in next paper.

## REFERENCES

- [1] Gopalan, K., Qidong Shi, "Audio Steganography Using Bit Modification - A Tradeoff on Perceptibility and Data Robustness for Large Payload Audio Embedding", Computer Communications and Networks (ICCCN), 2010 Proceedings of 19th International Conference 2010 , Page(s): 1 – 6.
- [2] Sujay Narayana and Gaurav Prasad (2010)," Two New Approaches For Secured Image Steganography Using Cryptographic Techniques And Type Conversions".
- [3] Hamid.A.Jalab, A.A.Zaidan, B.B.Zaidan (2010), "New Design for Information Hiding with in Steganography Using Distortion Techniques".
- [4] Zaidoon Kh. AL-Ani, A.A.Zaidan, B.B.Zaidan and Hamdan.O.Alanazi (2010)," Overview: Main Fundamentals for Steganography".
- [5] Usha, S. (2011), "A secure triple level encryption method using cryptography and steganography", Computer Science and Network Technology (ICCSNT), 2011 International Conference, Page(s):1017 - 1020
- [6] Djebbar, F. ; Ayad, B. ; Hamam, H. ; Abed-Meraim, K, "A view on latest audio steganography techniques", Innovations in Information Technology (IIT), 2011 International Conference on 2011 , Page(s): 409 - 414
- [7] Nugraha, R.M., "Implementation of Direct Sequence Spread Spectrum steganography on audio data", Electrical Engineering and Informatics (ICEEI), 2011 International Conference 2011 , Page(s): 1 – 6
- [8] Asad, M. ; Gilani, J., "Khalid, A, "An enhanced least significant bit modification technique for audio steganography", Computer Networks and Information Technology (ICCNIT), 2011 International Conference, 2011 , Page(s): 143 – 147.