Audio Steganography Using LSB Edge Detection Algorithm

Navneet Kaur[1] and Sunny Behal[2]
[1,2]*Department of Computer Sc. & Engineering,*
Shaheed Bhagat Singh State Technical Campus, Ferozepur, India
E-mail: [1]navneet18kaur@gmail.com, [2]sunnybehal@rediffmail.com

***Abstract*—Digital Steganography is used to protect digital content or data such as text, images, audio and videos that have been tampered maliciously. In this paper we maintain the quality of audio and image and to ensure the ownership, we propose a new LSB (least significant bit) using edge detection in digital steganography. We apply a 2-level steganography on images and audio which make the data which may be text or image in more secure form. By using lsb techniques may effects less the image pixel quality and audio sound quality, in this wecan randomly selected edges and embed the text or image by considering image quality, audio quality and audio imperceptibility.**

Keywords: Digital Steganography, Audio Steganography, LSB (Least Significant Bit), Performance Evaluation Metrics, Lsb Algorithm

I. INTRODUCTION

Digital Steganography is the technique of securing digitized data by hiding it into another piece of data which may be any text, image, audio, and video. The main task of the field of steganography is the storing, hiding, and embedding of secret data in all types of digital data. [1]The main goal of steganography is to communicate securely in a completely undetectable manner [2] such that no one can suspect that it exist some secret information. Unlike cryptography, which secures data by transforming it into another unreadable format, steganography makes data invisible by hiding (or embedding) them in another piece of data [3] [4].

In this type of steganography we can embed secret messages into digital sound in audio steganography. It is more complex process as compare to embedding messages in other media. This steganography method can embed messages in WAV, AU And even MP3 sound files [5]. The audio steganography consists of Carrier or Audio file, Message and Password. Carrier is also known as a cover-file, which conceals the secret information. In steganography model the secret message that the sender sends wants to remain it secret.[6] Message can be of any type may be text, image, audio or any type of file,.in secret stego key which only the receiver knows the corresponding decoding key will be able to extract the message from a cover-file. The cover-file with the secret information is known as a stego-file [7].

Applications of Audio Steganography

1. Confidential communication and secret data storing.
2. Protection of data alteration
3. Access control system for digital content distribution
4. Media Database systems.
5. To improve the quality.

The rest of the paper is organized as section 2 defines the Related Works. Section **3** describes the Performance Evaluation Metrics. Section 4 describes Proposed Architecture. Section 5 describes Proposed Algorithm. Section 6 defines Experimental Results.

II. RELATED WORK

The techniques involved in audio steganography are:

1) Echo Hiding

Echo hiding used to embeds secret data in a audio file by pass an echo into the discrete signal. This technique has advantages of providing a high data transmission rate and robustness when we make comparison of echo hiding to other methods [8] [9].

2) Phase Coding

Phase coding exploits HAS insensitivity to relative phase of different spectral components. In this method we can replace selected phase components from the original sound signal spectrum with hidden information.due to in audibility of information, phase components medication should be kept small [10].

3) Parity Coding

This technique is one of the robust audio steganographic techniques. Instead of breaking a signal into individual samples, it breaks a signal into separate samples sections and embeds each bit of the secret message information from a parity bit. If the of a selected parity bit region does not match the secret message bit to be encoded, the process inverts the LSB of one of the section in the region. Then the sender has many choices for encoding the secret bit [11].

4) Spread Spectrum

In this technique spread out the encoded information across the available frequencies. This is analogous to a system using an implementation of the LSB coding that randomly spreads the message bits over the entire sound file [12][13].

5) Tone insertion

Tone insertion used on the inaudibility of lower power tones in the presence of significantly higher ones. This method used resist to attacks such as low-pass filtering and bit truncation [14][15].

6) LSB (Least Significant Bit)

LSB in images: It is a simple approach to embedding information in image, in other mainly image manipulation can destroy the hidden information in the image. Due to this by applying LSB to each byte of 24 bit image, 3 bits can be encoded to each pixel or each pixel can be encoded by 3 bytes. Applying LSB technique each byte of 8 bit image only one bit can be encoded into each pixels as each pixel is represented by one byte.

In Audio LSB coding, two least significant bits of a data is replaced with two message bits. If we increase the amount of information encoded will also increase the noise in the sound file. Like, a sound file that was recorded in a bustling subway station would mask low-bit encoding noise[16]In secret message extraction from an LSB encoded audio file, the recipient needs access to the sequence of sample indices used in the embedding process. The length of the secret message to be encoded is smaller than the total number of section in audio file. We also know about how to choose the subset of samples which contain the secret message or information and communicate that decision to the recipient[17]. One trivial it is to start at the beginning of the audio file and perform LSB coding unto message completely embedded, leaving the remaining sections unchanged. But it creates a problem like in the first part of the audio file will have different statistical properties than the second part of the audio file which was not modified. Solution to this problem is to pad the secret message with random bits so that the length of the message is equal to the total number of samples. LSB (Least Significant Bit), this method is one of the important and easiest methods used for data hiding [18]. Traditionally, it is based on embedding each bit from the message in the least significant bit of the cover audio in a deterministic way.

Advantages: more embedding capacity for information and easy to implement or to combine with other hiding methods.

Disadvantage: less robustness to noise addition which reduces its security performance since it becomes vulnerable even to simple attacks [19].

III. Performance Evaluation Metrics

The performance of the watermarked images must be evaluated by using some quality measures such as MSE, SNR, PSNR and BER.

1) The MSE (Mean Square Error): [20] Defined it as Average Squared Difference Between a Reference Image and a Distorted Image. It is Calculated as:

$$MSE = \frac{1}{XY}\sum_{i=1}^{X}\sum_{j=1}^{Y}(c(i,j) - e(i,j))^2$$

X represents the height and Y represents the width of the image c (i,j) and e (i,j) are the respective pixel value of the original image and embedded image. [20]

2) The PSNR (Peak Signal to Noise Ratio): It is a Quality Metric Used to Determine the Degradation in the Embedded Image with Respect to the Host Image or also Defined as Ratio between Maximum Power of a Signal and Power of Distorted Signal [20]. It is Most Easily Defined via the Mean Squared Error (MSE) as:

$$\text{PSNR} = 10log_{10}\frac{L*L}{MSE}$$

L denotes the peak signal value of the cover image which is equal to 255 for 8 bit images.

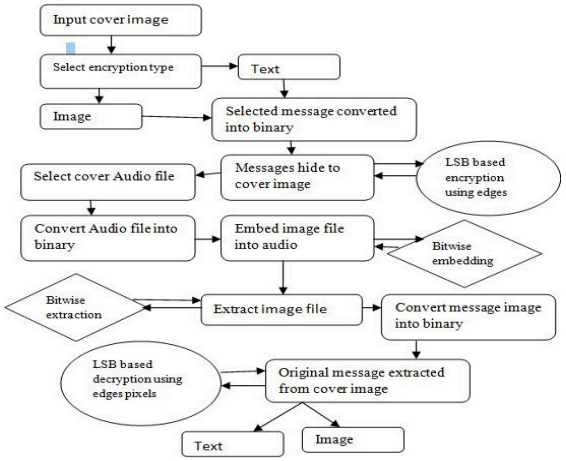


Fig. 1 Proposed Architecture

IV. Proposed Architecture

We used this method to make the security level of steganography more secure against attacks. Purposed method is consisting of 2-Level Security Process. In this first we select any input cover image then select encryption type which may be text or image and then message converted into binary. After conversion message hide to cover image by LSB based encryption using edges. Then select a cover audio file, then convert

audio file into binary, then embed image file into audio file by bitwise embedding.

Extraction Process: After embedding we can extract image file from audio file by Bitwise Extraction and then convert into binary. After converting original message extracted from cover image which may be text/image by LSB based decryption using edge pixels.

V. Proposed Algorithm

In Audio Steganography, we use a least significant bit using edge detection.

A. *Embedding Algorithm*

1. Select an Input cover image.
2. Select Encryption type which may be an image or text.
3. Selected message(text/image) converted into binary.
4. Using least significant bit (LSB) based Encryption using Edges to message hide in cover image.
5. Select an Audio cover file.
6. Convert selected Audio cover file into Binary.
7. Using bitwise embedding to embed Image file into Audio file.

B. *Extracting Algorithm*

1. Extract image file using bitwise extraction.
2. Convert message image into binary.
3. Original message which may be text or image is extracted from cover image by least significant bit (LSB) based decryption using Edges.

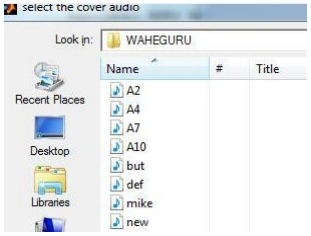
VI. Experimental Results

In Audio steganography, we have made a 2-level steganography. In steganography mainly we can embedding a text in an image or embedding a text in an audio, But in this paper we can modified the methods by combination of two methods to make it 2-level,Firstly we can embed the text message in an image and then embed the encrypted text message in an audio wav file. In embedding first select a cover image of size

Select a cover image and enter the text message which we want to encrypt

Enter a message which we want to encrypt
1111111111111
Encrypted image with hidden message

Select an Audio file and using bitwise embedding to embed encrypted image in audio



Extracting process:
Extract image from audio

Extract Original message from image:
1111111111111

TABLE I (Experimental Results)

Image	LSB3	Jae Gilyu	First Component Alteration Technique	Improved LSB	LSB Using Edge Detection
PSNR	37.92	38.98	46.11	46.65	68.60

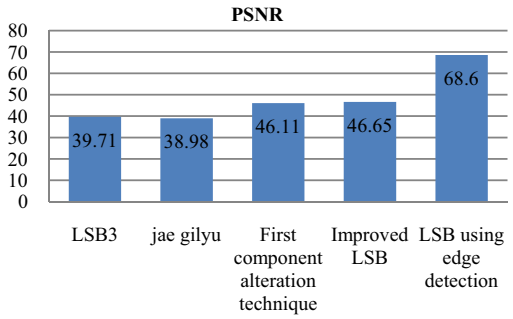


Fig. 1 Comparative Study of Various Methods with Proposed Techniques

VII. CONCLUSION

This paper provides that proposed algorithm is more secure due to 2-level steganography which gives the robustness and good quality of images or audio. In future work focus on size image with respect to time, because as we increase the size of message, increases the size of cover image as well as size of audio wav file increase which consumes more time.

ACKNOWLEDGMENT

This is to express my sincere gratitude to Mr. Sunny Behal, Assistant Professor, Department of Computer Science & Engineering, SBS State Technical Campus, Ferozepur (Punjab), India, for sparking in me the enthusiasm and initiative to discover and learn. I am truly thankful to him for guiding me through the entire paper and being my mentor and guide in this learning curve.

REFERENCES

[1] Artz, Donovan. Digital steganography: hiding data within data internet computing, IEEE 5.3 (2001): 75–80.

[2] Amin, Muhalim Mohamed, *et al.,*. Information hiding using steaganography. Telecommunication Technology 2003. NCTT Proceedings, 4th National conference on IEEE, 2003.

[3] Amin, Shashikala Channalli and Ajay Jadhav, " Steganography An Art of Hiding Data", International Journal on Computer Science and Engineering, IJCSE Vol. 1, No. 3, 2009.

[4] Shashkila channalli, Ajay jadhav, "Steganography an art of hiding data" International journal on Computer science and engineering Vol. 1(3), 2009, 137–141.

[5] Prof. Samir Kumar, Bandyopadhyay Barnali, Gupta Banik," LSB Modification and Phase encoding Technique of Audio Steganography Revisited". Vol. 1. (4) IJARCCE 2012.

[6] Dalal N. Hmood, Khamael A. Khudhiar and Mohammad S. Altaei (2012). A New Steganographic Method for Embedded Image In Audio File. International Journal of Computer Science and Security (IJCSS) 6(2): pp. 135–141.

[7] Chandrakar, Pooja, Minu Choudhary, and Chandrakant Badgaiyan. "Enhancement in Security of LSB based Audio Steganography using Multiple Files." International Journal of Computer Applications 73 (2013).

[8] HS, Anupama. "Information Hiding Using Audio Steganography A Survey." International Journal of Multimedia & Its Applications 3.3 (2011).

[9] Mat Kiah, M.L., *et al.,*. "A review of audio based steganography and digital watermarking." International Journal of Physical Sciences 6.16 (2011): 3837–3850.

[10] Samir K Bandyopadhyay, Debnath Bhattacharyya, Debashis Ganguly, Swarnendu Mukherjee and Poulami Das, "A Tutorial Review on Steganography".

[11] Jenkins, Neil, and Jean Everson Martina "Steganography in audio." University of Cambridge CST Part II Dissertation (2009).

[12] Malviya, Swati, Manish Saxena, and Dr Anubhuti Khare. "Audio Steganography by Different Methods". International Journal of Emerging Technology and Advanced Engineering.

[13] L.M. Marvel, C.G. Boncelet Jr., C.T. Retter, Spread spectrum image steganography, IEEE Trans. Image Process. 8 (8) (1999) 1075–1083

[14] Pramatha Nath Basu, Tanmay Bhowmik,'On Embedding of Text in Audio–A case of Steganography' International Conference on Recent Trends in Information, Telecommunication and Computing.

[15] Nosrati, Masoud, Ronak Karimi, and Mehdi Hariri. "Audio Steganography: A Survey on Recent Approaches." World Applied Programming 2.3 (2012): 202–205.

[16] Kumar, H.; Anuradha "Enhanced LSB technique for audio steganography". Computing Communication & Networking Technologies (ICCCNT), 2012 Third International Conference o*n,* On page(s): 1–4.

[17] xiaolong Li, Bin yang, Daofong Cheng and Tieyong Zeng "A generalization of LSB matching", IEEE signal processing Letters, Vol. 16, No. 2, Feb-2009.

[18] Singh, Pradeep Kumar, Hitesh Singh, and Kriti Saroha. "A survey on Steganography in Audio." National Conference on Computing for Nation Development, India com. 2009.

[19] Nitin jain,Sachin mesh ram and Shikhar dubey, "Image steganography using LSB and EDGE detection techniques", International journal of soft computing and engineering, ISSN: 2231–2307, Vol. 2, Issue: 3.