Proceedings of the International Conference on Intelligent Computing and Communication for Smart World (I2C2SW-2018)
14-15 December 2018

Steganography Based Data Hiding for Security Applications

G. Ramya
Jai Shriram Engineering College
Tiruppur, India
ramyakarthi22@gmail.com

P.P. Janarthanan
Kongu Engineering College
Erode, India
ppjanarthanan@gmail.com

D. Mohanapriya
Jai Shriram Engineering College
Tiruppur, India

***Abstract*—Steganography is an art of sending hidden data or secret messages over a public channel so that a third party cannot detect the presence of the secret message. It is used widely in banking, military applications, E-commerce and so on because in it transmissions of information are more secure. In the current paper, the data are hidden in two stages. First, the data are hidden within an image and the image is further hidden in an audio file. For data hiding in image and image hiding in audio, Least Significant Bit (LSB) algorithm is used. In order to overcome security threats and to equip the data with high security, binary values of the data are hidden in different locations on the last three bits. The audio file selected may be a .WAV or .AIFF files. If the binary value of image is hidden in the last bit, the execution time is more. To reduce it, the binary value of the image is hidden in the last two bits of an audio file, so that the processing speed gets increased while execution time gets reduced. For security applications, the execution time should be less. Thus, the paper meets the security requirement and it can be used for military applications.**

Keywords—Data Hiding, Security application, Steganography

I. INTRODUCTION

Information security plays a major role in any data transfer. Security can be obtained by information hiding that focuses on hiding the existence of secret messages. Steganography is data hiding technique aims in hiding the existence of the communication, to make other parties unaware of the contribution of steganographic exchange. [1]A novel method of steganography is introduced in order to improve the data hiding in all types of multimedia data formats such as image and audio and to make hidden messages imperceptible. Steganography can be classified into the following.

- Text steganography
- Image steganography
- Audio steganography
- Video steganography

Text steganography can be done by altering the text by formatting certain characteristics of original textual elements. [6] Altering can be anything either changing the format of an existing text, or changing words within a text, or generate random character sequences or to use context-free grammar to generate readable texts. In image steganography, the secrete message to be hidden or transmitted is taken and converted into suitable ASCII values. Then the image is converted into pixels and each pixel is represented in 8 bits. The last bits of the pixels are replaced by binary value of corresponding data and the image obtained is known as stegno image, which contains the secret information. Whereas in audio steganography, the audio signal is sampled and converted into binary values. The sampling rate of audio file is 44.1 KHz. The audio file may be a .WAV or .AIFF file. The data are hidden within audio file. The audio signal is the carrier signal which carries both the image and the data. Video Steganography is a method of hiding any kind of files into a carrying Video file. Its usage can be more acceptable than the other multimedia files considering its size and memory requirements. In military applications, the details like EEG and other related information about the soldiers are transmitted from one base to another. So there are possibilities for intrusion of data. So the in order to ensure the security of data, steganography technique is used. The advantages of steganography are as given below.

- Secrecy
- Accurate recovery of embedded information
- Imperceptibility to a human visual system
- Robust to various kinds of distortions
- High information capacity

II. BACKGROUND SURVEY

Budda Lavanya et al (2013) have described a steganography based method of embedding textual information in an audio file. In the existing steganography technique, initially the audio file is sampled and then an appropriate bit of each alternate sample is altered to insert the textual information. In contrast, in the proposed technique, the secret data are first hided into the image which is then embedded into the audio. In test cases, to visualize in what extent the target has been achieved, the text based data have been successfully embedded to the audio file for further analysis.

Ankit Chadha et al (2013) focused on improving the data encryption in all types of multimedia data format to make hidden message undetectable. This method is employed for image based data hiding. [9] For data hiding in audio, Discrete Cosine Transform (DCT) and Discrete Wavelet Transform (DWT) are employed. Analysis reports prove to be time-efficient and effective. Stegno-image is proved to be visually undetectable compared to original cover-image.

Similarly Pooja et al (2010) have concluded that steganography serves as a better way for message security than cryptography which only focuses on the message content, and not the message existence. The original message is hidden within a carrier data and hence the changes occurred in the carrier are not decrypt able. The method of employing digital images to serve as a carrier is detailed. [7] The performance of the steganography tools is

also analyzed. Collaborating secret data with the carrier image gives the hidden image which is difficult to detect without image retrieval.

Harvinder Singh et al (2013) have described a news steganography that hides the secret message based on the search for the identical bits between the secret messages and image pixel values. The proposed method is compared with the LSB benchmarking method. The results of the proposed and LSB hiding methods are discussed and analyzed based on the ratio between the number of the identical and the non-identical bits between the pixel color values and the secret message values. An approach is taken to generate a cross-platform which can effectively hide a message within a digital image .[8] As an image is the combination of several pixels and each pixel has three color numbers which in turn results in a fact that an image consists of millions of numbers, the change in a few color numbers makes the picture look a lot likes the original image.

Salwa et al (2012) has described a method for hidden image information in the form of wav file. This method takes any type of image file format like BMP, GIF or TIFF containing the hidden image information is represented in its binary form. This file is then is hidden in the wav file replacing the image information with wav file digits.

Samir Kumar et al (2012) have described information hiding as a part of information Security. Steganography is a technique of information hiding that focuses on hiding the existence of secret messages. In practice, there are three types of steganographic protocols used. They are pure steganography, secret key steganography and public key steganography.

III. PROPOSED TECHNIQUE

In military applications, security is a major threat. There is a possibility for hacking of the data, so secure transmission of data is required. In order to obtain security, a technique is proposed. The data to be transmitted are converted into binary values and hidden in then pixels of an image using an LSB Algorithm. The image with the hidden data is called stegno image.

To ensure much security, the stegno image is further hidden within an audio signal that needs to be sampled. [5] Then DWT is applied for original audio signal and audio's DWT coefficients and stegno image pixels are both converted into binary values. The LSB of binary audio is replaced by binary pixel values. Thus, both the image and audio steganography method is utilized.

A. Algorithm

Sender side

Step 1: The secret data may be a text / image / audio.

Step 2: The cover / carrier may be image / audio.

Step 3: The secret data and carrier are both converted into binary values.

Step 4: The binary values of the secret data can be replaced in an LSB of carrier.

Step 5: Now, the stegno image / audio is obtained.

Step 6: stop.

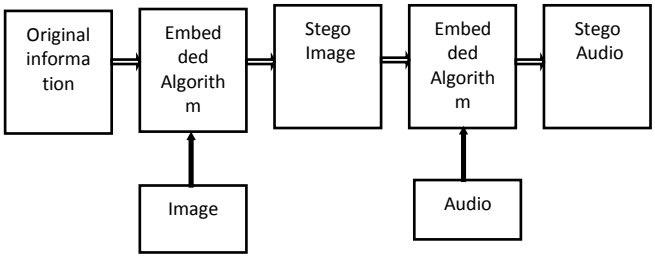

Fig. 1. Block Diagram for Transmitter side

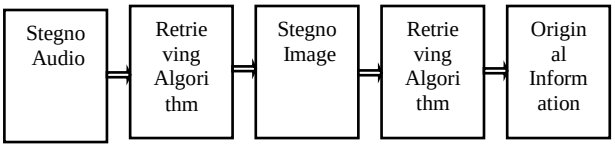

Fig. 2. Block Diagram for Receiver Side

B. Algorithm

Receiver side

Step 1: Receiver should know the length of the secret encoded data

Step 2: The original data can be retrieved from stegno image / audio.

Step 3: The LSB of a stegno image / audio can be taken up to the length of a secret data and then the original data / image can be recovered.

Step 4: Successfully the secret data can be retrieved.

Step 5: Stop.

IV. RESULTS AND DISCUSSION

A. Image Steganography

The Table I,II and III and Fig. 3,4,5,6 and 7 below represent the results of the image and audio steganography after hiding using LSB algorithm. The data to be transmitted are 'run'. The corresponding ASCII values are identified and converted into binary values. The image in which the data to be hidden is taken and the binary values of the pixel of the images is replaced by binary data using LSB Algorithm.Secret data: 'run'

Fig. 3. shows the original gray scale image and its size is 102 x102 and contains 10,404 pixels

ASCII value:[114 117 110]

Binary values: 011100100111010101101110

TABLE I: DATA HIDDEN IN AN LSB OF IMAGE PIXELS

Original image	**Stegno image**
10011100	10011100
10100000	10100001
10011100	10011101
10100000	10100001
10011100	10011100
10011011	10011010
10011100	10011101
10011111	10011110
10011110	10011110
10011011	10011011
10011010	10011011
10011000	10011001
10011101	10011100
10010111	10010111
10011100	10011100
10011101	10011101
10011010	10011010
10010111	10010111
10011001	10011001
10011000	10011000
10011010	10011011
10011011	10011011
10010111	10010111
10010110	10010110

Fig. 4. Data hidden in an LSB of an image pixel (102x102 stegno image)

Fig. 4. shows the stego image that contains the secret message. The secret data and image pixels are converted into binary values. Then they are hidden in an LSB of an image pixel. The differences in the original image and the stegno image is not noticeable by human eyes. So, the hackers cannot predict whether the data is inside an image.

B. Audio Steganography

Then DWT is applied for original audio signal. And audio's DWT coefficients and stegno image pixels both are converted into binary values. The LSB of binary audio is replaced by binary pixel values.

TABLE II. STEGNO IMAGE PIXELS HIDDEN IN AUDIO SAMPLES

Audio samples	**After scaling**	**Binary values**	**Stego audio**
0.5729	57	111001	111001
0.5293	53	110101	110101
0.5129	51	110011	110011
0.568	57	111001	111001
0.5654	57	111001	111001
0.421	42	101010	101011
0.2609	26	11010	11011
0.1505	15	1111	1111
0.0498	5	101	101
0.0464	5	101	101
0.1788	18	10010	10011
0.2886	29	11101	11101
0.3092	31	11111	11111
0.2984	30	11110	11111
0.2611	26	11010	11011
0.2232	22	10110	10111
0.2076	21	10101	10101
0.1569	16	10000	10001
0.0819	8	1000	1001
0.0633	6	110	111
0.1154	12	1100	1101
0.1841	18	10010	10011
0.16052	16	10000	10001
-0.0032	0	0	1
-0.1647	16	10000	10001
-0.1968	20	10100	10101
-0.1723	17	10001	10001
-0.1649	16	10000	10001

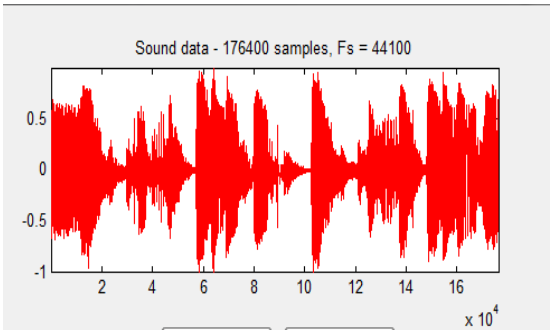

Fig. 5. Original audio-1,76,400 samples

Fig. 5. shows the original audio which contains 1,76,400 samples. The sampling rate of an original audio is 44.1kHz, and the duration of the signal is 4 seconds.

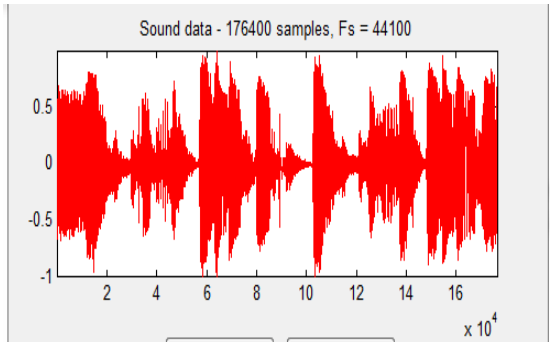

Fig. 6. Image hidden in LSB of an audio (stego audio which contains 102X102 image)

Fig. 6. shows the stegno audio, which contains the 102x102 stegno image. The DWT is applied for original audio signal and then the audio's DWT coefficients and stegno image pixels are also converted into binary values. The LSB of binary audio is replaced by binary pixel values. It takes more time for processing. There is no change between the original and stegno audio file, so the noise cannot be heard by human ear.

Data hidden in different locations in a pixel

Secret data: 'project'
ASCII value: [112 114 111 106 101 99 116]
Binary values:
01110000011100100110111101101010011001010110001101110100

TABLE III. DATA HIDDEN IN DIFFERENT LOCATIONS IN A PIXEL

Original image	**Stegno image**
10011100	10011**10**1
10100000	10100**11**0
10011100	10011**00**
10100000	10100**00**0
10011100	10011**01**0
10011011	10011**11**1
10011100	10011**00**
10011111	10011**10**1
10011110	10011**10**
10011011	10011**10**1
10011010	10011**11**
10011000	10011**11**0
10011101	10011**01**
10010111	10010**10**1
10011100	10011**10**
10011101	10011**10**1
10011010	10011**01**0
10010111	10010**10**
10011001	10011**01**
10011000	10011**01**0
10011010	10011**01**
10011011	10011**10**
10010111	10010**00**0
10010110	10010**11**
10011001	10011**01**1
10011010	10011**11**
10100010	10100**01**0
10011110	10011**00**

Fig. 7. Data hidden in different locatons in a pixel (102x102 stego image)

Fig. 7. shows the stego image that contains the secret message. The secret data and image pixels are converted into binary values and then hidden in different locations in image pixel. Hence the security of data is improved. The difference between the original image and stegno image is not noticeable by human eyes.

V. CONCLUSION

The proposed technique is to provide security to secret information to protect it from hackers. Two levels of steganography are used. First, the secret data are hidden in an image by using LSB algorithm. There is no difference between the original and the stegno image. In order to provide more security, the stegno image is hidden in an audio file. The audio file size should be more than the image size, only then the image can be hidden in that audio. The stegno audio contains the secret data and the stegno image. There is again no difference between the original and the stegno audio, because the LSB value is modified. At the receiver side, the length of the secret information and size of an image should be known, and so only the original information can be recovered. To reduce the forward and reverse processing time, the audio samples are segmented and the stegno image is hidden in the audio. For further reduction in the processing time, the image is hidden in the last 2 bits of audio samples. If the data are hidden in LSB of image pixel, the hackers can easily extract the secret information from the stegno image. The binary values of the secret data are hidden in different locations in the pixels. DWT is applied to audio files and the audio samples are stored in 4 different co-efficient. The approximation coefficient contains more information about the audio, so the image is hidden in the LSB of some other coefficients. Thus the hacker cannot predict which coefficient contains the stegno image.

In future, the proposed technique can be enhanced so that the processing time can be reduced. Further, in the present system, only the audio signals are used. In future, the audio signals from any instrument can be taken directly. Instead of LSB algorithm, the other algorithms like threshold based steganography may be used for audio and image steganography at different stages. The proposed technique can be used in real time applications such as E-commerce, banking, and military and so on for security purposes.

REFERENCES

[1] Ankit Chadha, Dattatray Bade (2013),'An Efficient Method for Image and Audio Steganography using Least Significant Bit (LSB) Substitution' , International Journal of Computer Applications , Volume 77

[2] Ashok V and Janarthanan P P, 'EEG based medical Assistance in the treatment of Mentally Retarded People', International Journal of Printing, Packing and Allied Sciences, Vol. 4, No.2, 2016

[3] Arvind Kumar, Pooja Km (2010),' Steganography-A Data Hiding Technique', International Journal of Computer Applications,Volume9

[4] Budda Lavanya, Srinivasa Rao Elisala (2013),' Data hiding in audio by using image steganography technique', International Journal of Emerging Trends & Technology in Computer Science (IJETTCS), Vol. 2

[5] Gandharba Swain and Saroj Kumar Lenka (2012),' A Technique for Secret Communication Using a New Block Cipher with Dynamic Steganography ', International Journal of Security and Its Applications , Vol. 6

[6] Gunjan Nehru et al (2012),' A Detailed look of Audio Steganography Techniques using LSB and Genetic Algorithm Approach', IJCSI International Journal of Computer Science Issues, Vol. 9

[7] Harvinder Singh, Anuj kumar et al(2013), 'Analysis and Implementation of Algorithm to Hide Secret Message', International Journal of Advanced Research in Computer Science and Software Engineering

[8] Hussein Al-Bahadili (2013),' A Secure Block Permutation Image Steganography Algorithm',International Journal on Cryptography and Information Security (IJCIS), Vol.3

[9] Masoud Nosrati Ronak Karimi (2012),' Audio Steganography: A Survey on Recent Approaches', World Applied Programming, Vol (2)

[10] Sakthisudhan K and Thangaraj P (2012),' Secure Audio Steganography for Hiding Secret information'. IJCA Proceedings on International Conference in Recent trends in Computational Methods

[11] Sakthisudhan K and Dr.Marimuthu C.M (2012),'Dual steganography approach for secure data communication',sciverse sciencedirect

[12] Salwa K. Abd Allteef, Proposed Steganography Method to Hide Image Data in Wav File.

[13] Samir Kumar, Gupta Banik (2012),' LSB Modification and Phase Encoding Technique of Audio Steganography Revisited', International Journal of Advanced Research in Computer and Communication Engineering

[14] Umamaheswari M, Pandiarajan S (2010).' Analysis of Different Steganographic Algorithms for Secured Data Hiding', IJCSNS International Journal of Computer Science and Network Security, Vol.10

[15] Valarmathi.R, (2014),' Information Hiding Using Audio Steganography with Encrypted Data', International Journal of Advanced Research in Computer and Communication Engineering.