Secret Communication Through Image and Audio for Defence

R. A. Jain, Hrushikesh B. Surve, Amit A. Sonar, Swpanil N. Salunke

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 messages. The goal of steganography is different from classical encryption, which seeks to conceal the content of secret messages; steganography is about hiding the very existence of the secret messages. In this paper we mainly discuss combination of steganographic methods.

Keywords- The goal of steganography is different from classical encryption,

I. INTRODUCTION

The word steganography comes from the Greek Stefano's, which means covered or secret and graphy means writing or drawing. Therefore, steganography means, literally, covered writing. Steganography is the art and science of hiding secret information in a cover file such that only sender and receiver can detect the existence of the secret information. A secret information is encoded in a manner such that the very existence of the information is concealed Steganography has been used throughout history to protect important information from being discovered by enemies. Covert communication by embedding a message or data file in a cover medium has been increasingly gaining importance in the all-encompassing field of information technology.

There are numerous methods used to hide information inside of Picture, Audio and Video files Audio steganography takes advantage of the psychoacoustical masking phenomenon of the human auditory system [HAS]. The main goal of this paper was to find a way so that an audio file can be used as a host media to hide text. Using combination of image and audio stegnography .Because Steganography, in general, depends on the imperfection of the human auditory and visual systems.

II. EMBEDDING TEXT IN CONVERT MEDIUM

In cryptography, the structure of a message is scrambled to make it meaningless and unintelligible unless the decryption key is available. But third party can attack actively or passively on system.

And can change the input text. and change the meaning. So along with cryptography stegnography is implemented. An image is an array of numbers that represent light intensities at various pixels. In the below discussion an audio file with ".wav" extension has been selected as host file.

It is assumed that the least significant bits of that file should be modified without degrading the sound quality. and the psychoacoustical masking phenomenon of the human auditory system [HAS] is used.

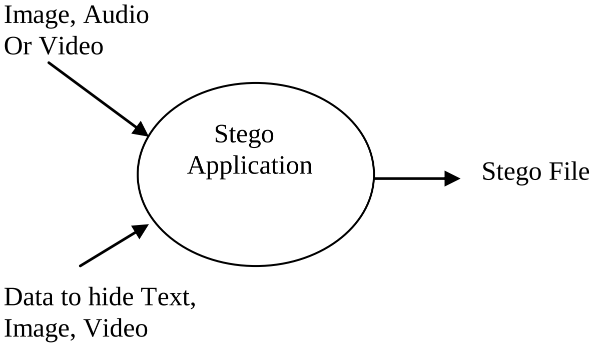

Figure 1.Basic Model of Stegnography

Algorithm followed for embedding process:

1. Here on input plain text .first cryptography algorithm is performed which can convert the input text in some cipher text .Manual algorithm of cryptography is implemented with the help of ASCII value of characters, digits. Manual algorithm is implemented with help of some mathematical equation to make input text to cipher text.

2. LSB (Least Significant Bit) which replaces the least significant bit in some bytes of the cover file to hide a sequence of bytes containing the hidden data. LSB of the input sampled image is changed with the text for that ASCII value of text is used.

e.g. For example, the character '**A**' is represented by the number 65. The equivalent binary representation is '0100 0001'. Multiple bits of each sample of the image have been changed or modified to insert text data in it. The bit modification was done by various ways, like 1, 2, 3, 4 bits can be changed.

And "**u**" has ASCII value 117 and corresponding binary representation is 01110101. to embed the letter "A", the sender has to embed the binary value "01000001".and same case with letter "u" also.

changing of the existing binary values with the intended binary values causes a minimal change in the original file. Image obtained is the **stego image.**

The whole embedding process is as shown in following table. From which we observe that pixel value (1,1) changes to 153 from it's original value 152. And similar kind of minimal change is observed in all pixels.

Manuscript received on April, 2013.

Prof.R.A.Jain: Department of E&TC Engineering, Sinhgad Academy of Engineering, Pune, India

Hrushikesh Babasaheb Surve: Department of E&TC Engineering, Sinhgad Academy of Engineering, Pune, India.

Amit Anil Sonar : Department of E&TC ngineering,Sinhgad Academy of Engineering,Pune, India.

Swapnil Nandram Salunke: Department of E&TC Engineering, Sinhgad Academy of Engineering, Pune, India.

Table I Samples Of Image File With Binary Values Before And After Embedding.

Pixel no	Pixel value	Binary values of correspondi-ng sample	Binary value to be embedded	After embedding
(1,1)	152	10011000	01	153
(1,2)	155	10011011	00	152
(1,3)	145	10010001	00	144
(1,4)	175	10101111	01	173
(2,1)	100	01100100	01	101
(2,2)	110	01101110	01	109
(2,3)	98	01100010	11	99
(2,4)	116	01110100	01	117

The whole retrieval process can be depicted with the following table more thoroughly:. Bits that are stored in the queue.

Table Ii Exraction Of Data From Audio File

Pixel no	Pixel value	Binary values of corresponding sample	Bits that are stored in queue
(1,1)	153	10011000	00
(1,2)	152	10011011	1100
(1,3)	144	10010001	011100
(1,4)	173	10101111	11011100
(2,1)	101	01100100	00
(2,2)	109	01101110	1000
(2,3)	99	01100010	101000
(2,4)	117	01110100	00101000

To hide that image into the host audio. DWT-discrete wavelet transform) along with svd (single value decoded and is used to make stego audio.

The DWT Transform With the DWT, the audio signal can be transformed into frequency domain ranging from low frequency to high frequency.

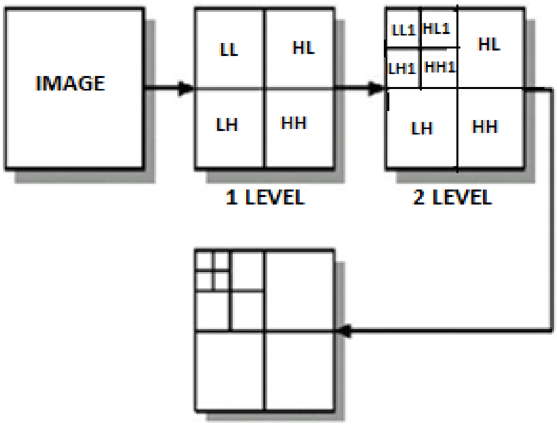

Figure 2.2-D DWT on Image.

Besides, the high frequency spectrum is less sensitive to human ear. That is the reason why the high frequency component is usually discarded in the compression process. Therefore, information to be hidden can be embedded into the low frequency component to against the compression attack..

Singular Value Decomposition (SVD):

Used for hiding an image inside audio file. Decomposed singular value has strong stability. Basic ideas behind SVD: taking a high dimensional, highly variable set of data points and reducing it to a lower dimensional space that exposes the substructure of the original data more clearly and orders it from most variation to the least. What makes SVD practical for many applications is that you can simply ignore variation below a particular threshold to massively reduce your data but be assured that the main relationships of interest have been preserved.

SVD is based on a theorem from linear algebra which says that a rectangular matrix A can be broken down into the product of three matrices - an orthogonal matrix U, a diagonal matrix S, and the transpose of an orthogonal matrix V . The theorem is usually presented
something like this:

$$A_{mn} = U_{mn} S_{mn} V^{T}_{nn}$$

Where UTU = I,$V_T V = I$the columns of U are orthonormal eigenvectors of AA^T, the columns of V are orthonormal eigenvectors of $A^T A$, and S is a diagonal matrix containing the square roots of eigen values from U or V in descending order. Here After hiding image in audio results and obtained in embedded audio which are shown below

III. EXPERIMENTAL RESULTS

Whatever is the plain text or password is first converted to cipher text e.g. crypto123 is plain text.
After using manual algorithm. O/p becomes ahfklkr54
and then performing LSB technique to hide in the an image.

Figure3. Input Image

Any image can be selected to hide plain text and hiding text in the image using LSB i.e. modifying some of the least significant bits of input image according to plain text. After hiding text in image image looks like below.

Figure4. Embedded Image

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

Using this image to hide inside another cover medium i.e. audio (.wav format) because WAV files are lossless, uncompressed, broadcast CD quality music files. WAV files are also the right choice for loops to be processed with Flash for web animations.

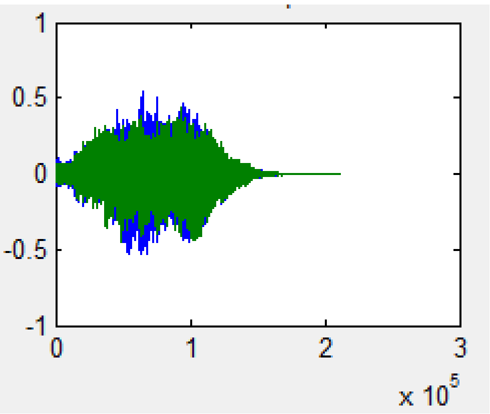

Figure5.Input Audio

First DWT is performed on i/p Audio. With the discrete wavelet transform (DWT), the audio signal can be transformed into frequency domain ranging from low frequency to high frequency. Therefore, information to be hidden can be embedded into the low frequency component to against the compression attack.

On that audio SVD is performed .And we get embedded audio as shown below in Which Image is hidden. such audio is called as stego audio .We get embedded audio which is very close to original Audio.

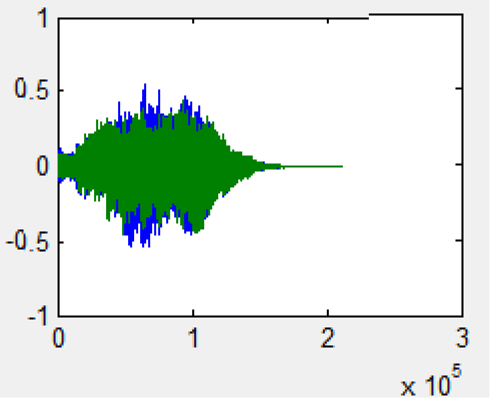

Figure6. Embedded Audio

It can be understand from the result obtained on PSNR and MSE.

The MSE represents the cumulative squared error between the compressed and the original, whereas PSNR represents a measure of the peak error. The lower the value of MSE, the lower the error.

$$\mathrm{MSE} = \sum_{M,N}[\mathrm{I}_1\,(\mathrm{m},\mathrm{n})-\mathrm{I}_2(m,n)]^2 \qquad (1)$$

MSE value observed is 1.68158*10^-6.

$$\mathrm{PSNR}=10log_{10}(\frac{R^2}{MSE}) \qquad (2)$$

In the previous equation, *R* is the maximum fluctuation in the input image data type. For example, if the input image has a double-precision floating-point data type, then *R* is 1. If it has an 8-bit unsigned integer data type, *R* is 255 etc.

PSNR value observed is 57.7428.

IV. APPLICATIONS

1. Enables secret communication.
2. Data hiding in audio or video is of interest for the protection of copyrighted digital media.
3. Tremendous use in Military Applications.
4. In forensic applications for inserting hidden data into audio files for the authentication of spoken words and other sounds.

V. DISCUSSION AND CONCLUSION

Many conventional method are done with one of the cover medium i.e., image, audio or video. A method of embedding text-based data into a host image and audio file using the method of LSB and SVD has been presented in this paper. In proposed technique Image and Audio are used as two cover medium. So that more security can be obtained and

An audio file with size 829 KB has been used. This proposed system will not change the size of the file even after encoding embedded audio file is also of 829KB. And also suitable for any file format. The maximum text file size that can be embedded in this audio file without degrading the file structure can be traced through a survey.

Also the performance parameter are observed which are coming satisfactory.and same algorithm is tested with different images and Audios. The main goal of this research work was embedding of text into audio as a case of steganography. The two primary criteria for successful steganography are that the stego signal resulting from embedding is perceptually indistinguishable from the host audio signal, and the embedded message is recovered correctly at the receiver.

The proposed technique shows promise as a robust method for audio steganography under noisy and cropped conditions.

REFERENCES

1. Pramatha Nath Basu& Tanmay Bhowmik 2010 . International Conference on Recent Trends in Information, Telecommunication and Computing: On Embedding of Text in Audio – A case of Steganography.
2. R SRIDEVI, DR. A DAMODARAM, “EFFICIENT METHOD OF AUDIO STEGANOGRAPHY BY MODIFIED LSB ALGORITHM AND STRONG ENCRYPTION KEY WITH ENHANCED SECURITY”,Journal of Theoretical and Applied Information Technology.
3. Jayaram P, Ranganatha H R, Anupama H,”INFORMATION HIDING USING AUDIOSTEGANOGRAPHY-A SURVEY.” The InternationalJournal of Multimedia & Its Applications (IJMA) Vol.3, No.3,August2011.
4. Johnson, Neil F. and Stefan Katzenbeisser. “A Survey of Steganographic Techniques”, In Information Hiding: Techniques for Steganography and Digital Watermarking. Boston, Artech House. 43-78. 2000.
5. Mohammad Pooyan, Ahmed Delforouzi, “LSB-based Audio Steganography Method Based on Lifting Wavelet Transform”,International Symposium on Signal Processing and Information Technology, IEEE, 2007.