IJIREEICE

ISSN (Online) 2321 – 2004
ISSN (Print) 2321 – 5526

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH IN ELECTRICAL, ELECTRONICS, INSTRUMENTATION AND CONTROL ENGINEERING
Vol. 4, Issue 4, April 2016

A Review on Audio Steganography

Tejaswini Y. Mullemwar[1], Prof. Sanjay I. Nipanikar[2]

PG Student, E & TC Department, PVPIT, Bavdhan, India[1]

Asst. Professor, E & TC Department, PVPIT, Bavdhan, India[2]

Abstract: Steganography is the art of data hiding context of secret message, without the knowledge of third party. Audio steganography is to send secret audio file more securely. Various techniques has introduced for performing steganography along with the various transform to increase the security of transmission. To enhance the security of the data transmission of secret data this methods found to be the best techniques. This paper specifies the techniques to find the gaps in existing techniques.

Keywords: Steganography, DWT, OPAP.

1. INTRODUCTION

The main purpose of Steganography, which means 'writing in hiding' is to hide data in a cover media so that others will not be able to notice it. From the rise of the internet, the use of it for communication or data transfer has increased day by day, as the use of internet for communication has increased; the security of the data transfer also becomes a main factor, for this purpose steganography can be used, its basic diagram shown in fig 1.1 and different techniques taken into consideration. In this study, we are going to have a survey on some published algorithms and methods in this steganography field on the secret data. Different existing techniques to perform embedding are available along with those techniques different transforms can be use, those transforms survey done here.

2. LITERATURE REVIEW

As frequency domain provides more security to the data transfer than the spatial domain technique. Authors Po-Yueh Chen and Hung-Ju Lin propose a new steganography technique in 2006 which embeds the secret messages in frequency domain with high PSNR. To embed secret data in frequency domain, the detail procedure of 2D DWT is given by the author. This technique, keep the messages away from stealing, destroying from unintended users on the internet and hence provide satisfactory security.

Mekelweg author in 2009 gives a thesis, in these details of different transform algorithms such as DWT and DCT are given with reason for consideing the DWT algorithms, as several multimedia standards such as the JPEG2000 and MPEG-4 are based on the DWT. These new standards brought new requirements such as progressive, low bit rate transmission, and region-of-interest coding. In addition he proposes that, the DCT based compression standards are block-based causing blocking artifacts in the output image.

Amanjot Kaur, Jaspreet Kaur, in june 2012 discussed the comparison between DCT and DWT based on parameters such as PSNR, MSE, BER, TIME and they found that DWT provides higher compression ratios and DCT takes more time than DWT.

Steganography is checked on two aspects imperceptibility and embedding capacity (payload), authors Shaikh Salman, Prof. S. R. Kinge in 2013 discussed different techniques such as LSB, OPAP, APPM and DE. They proposes that if we want to embed large amount of data and if stego image quality is not so important then use OPAP method, but when image quality is of greater importance than embedding capacity, then DE & APPM are the best choice.

Additional improvement in the quality of image while embedding is given by authors N.Vinothkumar, T.Vigneswaran in March 2013, they proposes that image quality of the stego image is improved by this as the Optimal Pixel Adjustment Process is applied after embedding the message. The frequency domain is employed to increase the robustness of the steganography method. A variant of LSB method can be found in that proposes an Optimal Pixel Adjustment Process in which image quality of the stego-image can be improved with low computational complexity.

Different steganography techniques and performance measures are given by these authors Rajashree Shitole, S.R.Todmal, in May 2014. They introduces that LSB method has average embedding capability and in EMD payload cannot be increased and it is limited to 5-ary notational system. For extraction, more than one pixel needs to be modified, which affects overall performance and OPAP have high payload with less degradation of image quality is introduced. The different techniques of stegnography given along with their algorithm steps in brief by these authors.

Author M. I. Khalil in 2011 proposed a technique for how to hide a short audio message in the cover image data; with the less degradation of image quality. Among available embedding techniques he uses LSB for embedding secret data and gave the brief of audio steganography.

3. EMBEDDING & EXTRACTION PROCEDURE OF SECRET DATA

3.1. Embedding Procedure:

Step 1: To begin, we have two data files one cover and second secret data file, so the first step is to read the files. Then check for the size mismatch of secret and cover data file. All cover data file size should be greater than the

IJIREEICE
ISSN (Online) 2321 – 2004
ISSN (Print) 2321 – 5526
INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH IN ELECTRICAL, ELECTRONICS, INSTRUMENTATION AND CONTROL ENGINEERING
Vol. 4, Issue 4, April 2016

secret data files. If it is not so then cover and secret files sizes mismatched; message will be display.
Step 2: Find reference pixel to which the data is to be embedded.
Step3: Using any steganography technique embeds the secret data file in the cover data file in the reference pixel and we get the stego data file.

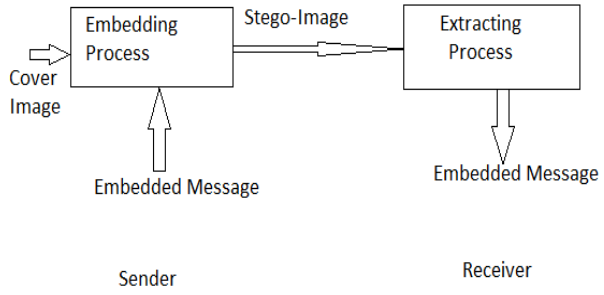

Fig 1.1: Basic Diagram of Steganography

3.2. Extraction Procedure:

Step 1: Take the stego image i.e., the cover data file in which the secret data file is embedded.
Step 2: Now using any of the extracting techniques and extract secret information data file from the stego data file.
Step 3: After doing extraction, we get the secret information data file extracted from the cover data file with the better quality.

4. AUDIO STEGANOGRAPHY

Audio steganography is the technique in which hiding information inside audio signals or hiding secret audio file in cover file. There are number of types of audio files, most commonly used WAV file (.wav) and MPEG layer 3 file (mp3). It has found that the audio wav files are probably the simplest for storing audio samples. As digital image uses 8-bit or 24-bits colour. If using 8-bit then 256 colour shades will be there, but for 24-bit colour scheme, it uses 24-bits per pixel and thus more sets of colours. In this case, each pixel is represented by 3 bytes; each pixel represents the intensity of three primary colours red, green, and blue. On the other hand, hiding capacity depends on the size of cover image.

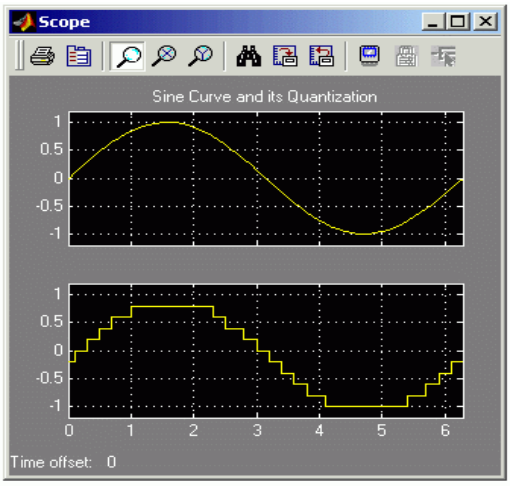

Fig 4.1: Sine wave and its quantization

Message size must be smaller than cover image. First, on the continuous audio wave signals quantization is done shown in fig.4.1, to get discrete samples i.e., each field is converted into bit arrays and embedded bit by bit in the cover file. These bits can embed in any order, it is not mandatory to insert in sequential order. For ex, if cover file is image file and secret data is audio file then the relation between audio file bytes(A) and image pixels(P) for embedding audio is given as:

$$8 \times A = 3 \times W \times H$$

Where, W is width of image; H is height of image; 8 x A gives size of the audio file. The flowchart for embedding data is shown in fig 4.2. Audio file extracting is reverse of audio embedding, its flowchart given in fig 4.3. The secret data extracted from secret location of cover image file. The contents of bit arrays are converted to bytes and appended to the audio file. The length of data information is given in the header file.

5. DIFFERENT STEGANOGRAPHY TECHNIQUES

5.1. Least Significant Bit:

LSB hiding is a simple and fast method for embedding information in the cover data file. It consists of embedding each bit from the secret message in the least significant bit of the cover data file in a specific way. When using a 24-bit image, a bit of each of the red, green and blue colour components can be used, since they are each represented by a byte.

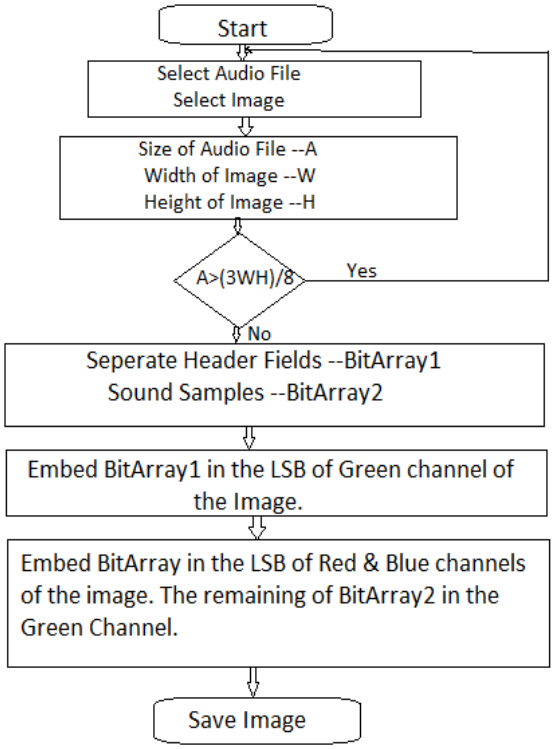

Fig 4.2: The flowchart for Audio Embedding

In other words, one can store 3 bits in each pixel. The length of the secret message to be encoded should be smaller than the total numbers of samples in a sound file. For example: a grid for 3 pixels of a 24-bit image can be as follows:

IJIREEICE
ISSN (Online) 2321 – 2004
ISSN (Print) 2321 – 5526
INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH IN ELECTRICAL, ELECTRONICS, INSTRUMENTATION AND CONTROL ENGINEERING
Vol. 4, Issue 4, April 2016

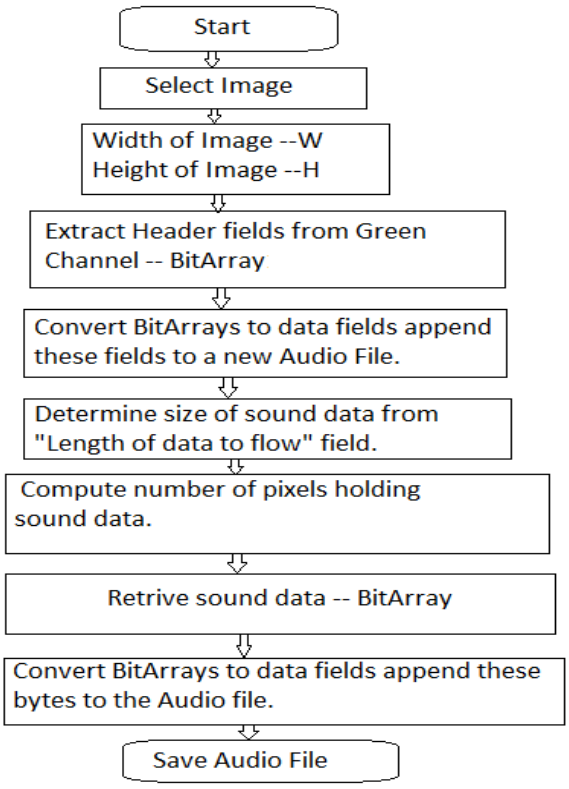

Fig4.3: The flowchart of Audio Extraction

When the number 200, which binary representation is 11001000, is embedded into the least significant bits of this part of the image, the resulting grid is as follows:
(00101101 00011101 11011100)
(10100110 11000101 00001100)
(11010010 10101100 01100010)
Although the number was embedded into the first 8 bytes of the grid, only the 3 underlined bits needed to be changed according to the embedded message

5.2. The Exploiting Modification Direction (EMD) Embedding Scheme:

The EMD method improved the image quality of stego image by fully exploiting the modification direction. The basic concept of this method is n cover pixels carry (2n+1)-ary notational secret digit and only 1 pixel value is changed i.e. increased or decreased by 1. In n cover pixels, for one pixel 2n states are possible pixel value 1 is added or subtracted. But if no pixels are modified (2n+1) different cases are obtained. Secret message (binary form) is segmented to L bits where L is given as:

$$L = [K * \log_2 (2n+1)]$$

For ex., Secret message bits are (1101 0110 1001) segment as (23 11 14) in 5-ary rotational system where L=4 and K=2.
Let Px_1, Px_2, ...Px_n denote value of pixel in a group extraction function (f) is given as follows:

$F(Px_1, Px_2 ... Px_n) = [\sum_{i=1}^{n} Pxi * i]$

If n=2,

$F(Px_1, Px_2) = [\sum_{i=1}^{n} (Pxi * i) \bmod (2n+1)]$

$= [\sum_{i=1}^{n} (Pxi * i) \bmod 5]$

By using this function we can insert secret data in the required locations.

5.3. Optimal Pixel Adjustment Process (OPAP):

The Optimal Pixel Adjustment (OPA) is applied for embedding the message. The main idea of applying OPA is to minimize the error between the cover and the stego image.

OPA Process:
Consider Px_i, Px_i', Px_i'' represent pixel values at it h pixel in the host image H, stego image S.
Let, $\delta_i = Px_i' - Px_i$.
Where, δ_i = embedding error.
Cover or host image of M*N pixels is represented as H = x (i, j)E {0, 1...255}
Secret message m in K secret bit is
m = {mi | 0 ≤ i< n, mi Є {0, 1}}
To convert Px_i' to Px_i'' i.e. original pixel to stego pixel three cases are defined.

Case 1: $(2^k-1 < \delta_i < 2^k)$

$Px_i'' = Px_i' - 2^k$; $Px_i' \geq 2^k$

$= Px_i'$; otherwise

Case 2: $(-2^k-1 \leq \delta_i \leq 2^k-1)$

$Px_i'' = Px_i'$; for all

Case 3: $(-2^k < \delta_i < -2^k-1)$

$Px_i'' = Px_i' + 2^k$; $Px_i' < 256 - 2^k$

$= Px_i'$; otherwise

5.4. Diamond Encoding (DE):

The basic concept of DE is based on Pixel Pair Matching. It is an extension of EMD method. DE is used to conceal the secret digit in N-ary notational system into pixel pair. Where, N = 2k2 + 2k + 1 when k ≥ 1, where k is embedding parameter. Diamond Characteristic value is calculated so that one secret N-ary digit is concealed.
Consider, size of cover image is m*m and secret message digit is D_N, N stands for N-ary notational system. But embedding parameter k should satisfy the following condition:

$$[(m*m)/2] \geq |S_N|$$

Where, $|S_N|$ represents no. of secret message digits in N-ary notational system.
In the diamond encoding method, when neighbourhood values are found, they form a diamond shape. Payload is given by ½ log2 (2k2 + 2k + 1) bits per pixels.

Table 1: PSNR values for different methods

IMAGES	LSB	OPAP	EMD	DE
Lena	37.97	40.77	44.63	45.00
Baboon	37.90	40.85	41.87	44.98
Pepper	37.94	40.60	42.62	42.72

6. DIFFERENT TRANSFORMS

The transform of a signal is just another form of representing the signals. Two processing-domain categories have been introduced for digital steganography algorithms, namely **spatial domain** and **frequency domain**. A Steganography technique based on the spatial domain spread secret data to be embedded in the pixel value. However, the techniques in the spatial domain still have relatively low-bit capacity and are not resistant enough to lossy image compression and other image processing. On the other hand, frequency domain-based

IJIREEICE

ISSN (Online) 2321 – 2004
ISSN (Print) 2321 – 5526

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH IN ELECTRICAL, ELECTRONICS, INSTRUMENTATION AND CONTROL ENGINEERING
Vol. 4, Issue 4, April 2016

techniques can embed more bits for steganography and are more robust to attack. In addition, transform-domain watermarking techniques are typically much more robust to image manipulation compared to the spatial domain techniques. This is because the transform domain does not use the original image for embedding the secret data file. Hence, in transform domain includes important transforms such as DCT and DWT.

6.1 Discrete Cosine Transform:

Discrete cosine transform is widely used in image and video compression applications such as JPEG or JPG and MPEG. These multimedia standards partition an input image file into 8 × 8 blocks after that the DCT for each block is computed. The steganography techniques embed secret data into the middle frequency bands of a transformed image. The middle frequency bands are chosen such that they avoid the most visual parts of the image (the low frequencies) without overexposing themselves to removal through compression and noise attacks (high frequencies).

A 2D DCT is efficiently computed by 1D transforms on each row followed by 1D transforms on each column. There are different algorithms to compute the 2D DCT. For example, one such algorithm is by using matrix multiplication and it is explained as follows. The M × M transform matrix T is given by Equation: $Tij = \frac{1}{\sqrt{M}}$ if i=0, $0 \le j \le (M-1)$

$$= \sqrt{\frac{2}{M}} * \cos \frac{\prod (2j+1)i}{2M}$$

if $1 \le i \le (M-1), 0 \le j \le (M-1)$

For an M ×M matrix A, T ∗A is an M x M matrix whose columns contain the 1D DCT of the columns of A. The 2D DCT of A can be computed as B = T ∗ A ∗ T ′.

6.2 DWT (Discrete Wavelet Transform):

6.2.1 Wavelets Definition:

Wavelets are mathematical functions that cut up data into different frequency components.

6.2.2 Wavelet Transform:

The most important feature of wavelet transform is it allows multi-resolution decomposition. An image that is decomposed by wavelet transform can be reconstructed with desired resolution. The procedure for this is a low pass filter and a HPF is chosen, such that they exactly halve the frequency range between themselves. This filter pair is called the Analysis Filter pair. First of all, the low pass filter is applied for each row of data, and then we obtain low frequency components of the row. As the LPF is a half band filter, the output data consists of frequencies only in the first half of the original frequency range. By Shannon's Sampling Theorem, they can be sub sampled by two, so that the output data contains only half the original number of samples, similarly the high pass filter is applied for the same row of data, and now the high pass components are separated, and placed by the side of the low pass components. This procedure is done for all rows. Next, the filtering is done on each column. As a result we get four bands of data, each labelled as LL (low-low), HL (high-low), LH (low-high) and HH (high-high).The LL band can be decomposed once again in the same manner, thereby producing even more sub bands. This can be done up to any level, thereby resulting in a pyramidal decomposition as shown below the LL band at the highest level can be said as most important, and the other bands are of lesser importance, the degree of importance decreases from the top of the pyramid to bottom.

The comparative table for both transforms given below for different parameters:

Table 2: Comparative table for DCT & DWT

PARAMETERS	DCT	DWT
Compression Ratio	20.1763	20.3955
PSNR	0.0263	38.6309
MSE	10.3820	8.9123
BER	37.9680	0.0259
Time	7.4121	3.5139

7. CONCLUSION

Many techniques have been proposed so far for document audio steganography as given above. All these techniques have their advantages and disadvantages. LSB is very easy and efficient method, but with less hiding capacity. In EMD payload cannot be increased and it is limited to 5-ary notational system. For extraction, more than one pixel needs to be modified, which affects overall performance. OPAP & DE techniques have the high payload with very less image degradation.. Security of System increases but execution time for OPAP is more. There are various frequency domain transforms available but wavelet transform allows multi-resolution decomposition and no need to decompose image into 8x8 blocks every time.

REFERENCES

1. Po-Yueh Chen, Hung-Ju Lin, A DWT Based Approach for Image Steganography, International Journal of Applied Science and Engineering 2006. 4, 3: 275-290.
2. M.I.Khalil, Image Steganography: Hiding short audio message within digital images,JCS&T,2011 Vol.11 NO.2
3. N.Vinothkumar, T.Vigneswaran, Steganographic Method Image Security Based on Optimal Pixel Adjustment Process and Integer Wavelet Transform, International Journal of Advanced Research in Electronics and Communication Engineering (IJARECE) Volume 2, Issue 3, March 2013
4. Dr. Harish Rohil, Parul, Manju, Optimized Image Steganography using Discrete Wavelet Transform (DWT), International Journal of Recent Development in Engineering and Technology, (ISSN 2347 - 6435 (Online) Volume 2, Issue 2, February 2014)
5. Abdulaleem Z. Al-Othmani, Azizah Abdul Manaf and Akram M. Zeki, A Survey on Steganography Techniques in Real Time Audio Signals and Evaluation,(IJCSI) Vol. 9, Issue 1, No 1, January 2012 .
6. Mitra, Thesis on Digital Image Watermarking Robustness: A Comparative Study, Computer Engineering Mekelweg 4, 2628, 2009, CD Delft the Netherlands http://ce.et.tudelft.nl/
7. Shaikh Salman, Prof. S. R. Kinge, Data Hiding Method Using Adaptive Pixel Pair Matching, (IJSR), 2013.
8. Rajashree Shitole, S.R.Todmal, Steganographic Methods In Spatial Domain - Optimal Pixel Pair Matching And Diamond Encoding, International Journal of Advances in Engineering & Technology, May, 2014. ISSN: 22311963.