Protection of Executables Employing a Novel Dual Stage Digital Data Hiding Scheme

H S Jayaramu[1],Arvind K Gautham[2]

[1]Research Scholar, Mewar University, India.
[2]Department of Management, Research Supervisor, Mewar University, India
Principal, S D College of Eneering, Muzzaffarnagar, India.

Abstract: ***Digital steganography provides efficient means of hiding digital data behind a digital cover like image video or audio as noise or redundant data. One of the important requirement of most steganography technique is that cover data must be significantly larger than the payload to efficiently distribute the redundant information over large data. This ensure better security and becomes challenging in identifying or cracking the Stegano object. Due to aforementioned reason steganography has been predominantly used in text payload.In this work we propose a unique dual stage steganography technique to hide Exe files by first embedding them behind a 2D image file followed by embedding the image in an audio cover. As EXE files are more sensitive to errors and even a single bit error may cause the application to crash, the method needs more accuracy. Also as EXEs are of larger size than normal text, they present significant challenge in ensuring that payload can not be traced in the stego object. To provide application exes better security we use 2D-1D steganography by combining image and audio steganography technique.Results show that for first stage for a PSNR over 50db and produce significantly acceptable result of 45db for 2e-^{3} BPP.***

Keywords: Image Steganography, Audio Steganography, Discrete Wavelet Transform, Spectrum Analysis.

1. INTRODUCTION

1.1 General Introduction

The rapid growth of internet coupled with high bandwidth and low cost computer hardware have propelled an explosive growth of steganography. In modern Image Stenography which exploits the advantages of the present day digital media such as multimedia objects often have a highly redundant representation, generally permits the addition of significantly large amount of payload by means of simple modifications that preserve the perceptual content of the underlying cover image and hence they have been found to be perfect candidates to carry payload. The cover object could be an audio file, video file or an image file and the message to be hidden called the Payload could be a plain text, audio, video or an image. The carrier or the cover object along with the hidden message is known as the stego-object or steganogram. The modern secure image steganography presents a challenging task of transferring the embedded information to the destination without being detected, not just by the limited powers of the Human Visual System (HVS) but also from powerful machine vision of computers. Hence steganographic method should embed information into the cover without causing statistically significant modification to the cover object. A steganographic technique is said to be secure if the relative entropy of the probability distribution of cover images and stego-objects is less than or equal to ε. A steganography technique is perfectly secure if ε is zero.Basically, the purpose of cryptography and steganography is to provide secret communication. However, steganography is not the same as cryptography. Cryptography hides the contents of a secret message from a malicious people, whereas steganography even conceals the existence of the message. Steganography must not be confused with cryptography, where we transform the message so as to make it meaning obscure to a malicious people who intercept it. Therefore, the definition of breaking the system is different. In cryptography, the system is broken when the attacker can read the secret message. Breaking a steganographic system need the attacker to detect that steganography has been used and he is able to read the embedded message. In cryptography, the structure of a message is scrambled to make it meaningless and unintelligible unless the decryption key is available. It makes no attempt to disguise or hide the encoded message. Basically, cryptography offers the ability of transmitting information between persons in a way that prevents a third party from reading it. Cryptography can also provide authentication for verifying the identity of someone or something.In contrast, steganography does not alter the structure of the secret message, but hides it inside a cover-image so it cannot be seen. A message in ciphertext, for instance, might arouse suspicion on the part of the recipient while an “invisible” message created with steganographic methods will not.In other word, steganography prevents an unintended recipient from suspecting that the data exists. In addition, the security of classical steganography system relies on secrecy of the data encoding system. Once the encoding system is known, the steganography system is defeated. It is possible to combine the techniques by encrypting message using cryptography and then hiding the encrypted message using steganography. The resulting stego-image can be transmitted without revealing that secret information is being exchanged. Furthermore, even if an attacker were to defeat the steganographic technique and detect the message from the stego-object, he would still require the cryptographic decoding key to decipher the encrypted message.

1.2 Definitions

1. Cover image: It is an object consisting of the signal stream or data file as a carrier of the embedded object. The most important property of a cover image is the amount of data that can be embedded into it, without changing the noticeable statistical properties of the cover image. Good cover images are (i) grayscale images (ii) uncompressed images containing large number of colors (iii) landscapes and portraits. JPEG format images are very poor choice for cover images because small modifications in cover image can be detected easily.

2. Payload: It is the size of the data i.e., (signal, stream or file) embedded in the cover image.

3. Stego-object: It is a unified object /image obtained from the combination of the cover object and payload.

4. Capacity: It is the amount of data that can be hidden in the cover image without destroying the statistical properties of the cover image. The capacity depends on the type of cover image used. The capacity is given by bits per pixel (bpp) by the Equation 1.1.

$$\text{bpp}= \frac{\textbf{number of bits embedded in cover image}}{\textbf{total number of pixel in cover image}} \qquad (1.1)$$

5. Robustness: The amount of modification that can be withstood by the cover medium without being destroyed completely is defined as robustness. It is the extent of modification that can be tolerated by the stego-object without destroying the hidden image under attacks.

6. Security: It can be considered as safeguarding or protecting information of the payload in the cover image. It is the extent of inability of adversary to detect hidden images accessible only to the authorized user. The quality factor can enhance the security of the image. A steganographic image is perfectly secure when the statistical data of the cover and stego images are identical.

7. Imperceptibility: It is the extent of in distinguishability of the original cover image and stego image. The measure of this can be obtained by the PSNR equation. Though it is not an accurate measure, it can give satisfactory results.

8. Wavelet: Wavelet is a small wave and its analysis is about analyzing a signal with short duration finite energy functions.

9. Wavelet Transform: Wavelet transform provides the time-frequency representation. The wavelet transform of an image is created by repeatedly filtering the image coefficients on a row-by-row and column-by-column basis.

10. Approximation Band: It is the band of an image having the low frequency coefficients in the wavelet domain.

11. Detail Band: It is the band of an image having the high frequency coefficients in the wavelet domain.

12. Mother Wavelet: A mother wavelet, (x) is a prototype that can be scaled and translated. A mother wavelet has to satisfy the condition given below.

$$\int \Psi(x)dx = 0 \qquad (1.2)$$

The wavelet function of a signal, f(x) can be computed using the following analysis and synthesis formulae:

$$c_{i,j} = \int_{-\infty}^{\infty} f(x)\,\Psi_{i,j}(x)dx \qquad (1.3)$$

$$f(x) = \sum_{j,k} c_{j,k}\Psi_{j,k}(x) \qquad (1.4)$$

13. Haar Wavelet: It is a function which consists of a short positive pulse followed by a short negative pulse, which provides orthogonality decomposition of an image signal.

$$\Psi = \begin{cases} 1 & \text{if } 0 \le t \le \frac{1}{2} \\ -1 & \text{if } \frac{1}{2} \le t \le 1 \\ 0 & \text{otherwise} \end{cases} \qquad (1.5)$$

14. Detectability: Identification of the Steganographic image visually or by computer analysis is called detectability. The challenge of steganography is to hide the information which cannot be identified by any means.

15. Histogram: It shows the distribution of intensities of an image. It is the plot of Number of pixels and intensity of the pixel values.

16. Distortion: The distortion of the cover image depends on the size of the pay- load. Larger the payload higher is distortion of the stego image.

17. Mean Square Error (MSE): It is defined as the square of error between cover image and stegoimage. The distortion in the image can be measured using MSE and is calculated using Equation 1.6.

$$MSE = \left\lfloor \frac{1}{N*N} \right\rfloor^{2} \sum_{i=1}^{N}\sum_{j=1}^{N}(X_{ij} - \bar{X}_{ij})^{2} \qquad (1.6)$$

Where:
: The intensity value of the pixel in the cover image.
: The intensity value of the pixel in the stego image.
N: Size of an Image.

18. Peak Signal to Noise Ratio (PSNR): It is the measure of quality of the image by comparing the cover image with the stegoimage, i.e., it measures the statistical difference between the cover and stegoimage, is calculated using Equation 1.7.

$$PSNR = 10log_{10}\frac{255^{2}}{MSE}db \qquad (1.7)$$

19. Pixel: It is an element of the image which is not further divisible from the image analysis point of view. A pair of adjacent pixel values is called Pixel Pair.

2. RELATED WORK

Souvik Bhattacharyya and Gautam Sanyal[1] proposed approach works by converting the gray level image in transform domain using discrete integer wavelet technique through lifting scheme. The aim of this paper is to propose a high-capacity image steganography technique that uses pixel mapping method in integer wavelet domain with acceptable levels of imperceptibility and distortion in the cover image and high level of overall security. Ammar Abdul-Amer Rashed[2] proposed a companied technique for hiding secret messages (text) based on wavelet transform applying in cover image (a gray level image 8bit) and Huffman encoding. The experimental results show that the algorithm has a high capacity and a good invisibility, Moreover PSNR of stego image shows the better results the PSNR above 40 dB, the proposal system was activated according to attacker noise is addition and JPEG compression application are used without detection the secret message.S. K. Muttoo and Sushil Kumar [3] proposed a stiganographic algorithm based on wavelet transforms. The algorithm first uses the Best T-codes to encode the message before embedding into a cover image.. Saddaf Rubab and Dr. M. Younus presented [4] a new devised algorithm to hide text in any colored image of any size using Huffman encryption and 2D Wavelet Transform. The subject algorithm also proved secure as Huffman table is required to decode the information. Manjunatha Reddy and Raja proposed[5] High Capacity and Security Steganography using discrete wavelet transform (HCSSD). The wavelet coefficients of both the cover and payload are fused into single image using embedding strength parameters alpha and beta. The cover and payload are preprocessed to reduce the pixel range to ensure the payload is recovered accurately at the destination. It is observed that the capacity and security is increased with acceptable PSNR in the proposed algorithm compared to the existing algorithms.Lalitha.G et al.[6], proposed a technique for the simultaneous transmission of multiple data securely. They took an advantage of less space required for storing an image than that of a wav file. The proposed technique brings down the required channel capacity to transfer secret data in real time systems besides improving robustness. Elham Ghasemi et al.[7], proposed the application of Wavelet Transform and Genetic Algorithm in a novel steganography scheme. We employ a genetic algorithm based mapping function to embed data in Discrete Wavelet Transform coefficients in 4x4 blocks on the cover image.Kirith saroha and Pradeep kumar singh[8] proposed a new steganographic method for embedding an image in an Audio file. Emphasis will be on the proposed scheme of image hiding in audio and its comparison with simple Least Significant Bit insertion method of data hiding in audio. It is an attempt to find a method that uses an audio file as a cover media to hide an image without making noticeable changes to the file structure and contents of the audio file. The proposed scheme is based on Least Significant Bit insertion method as it has been already proved that modification of LSB creates a minimal change in the audio file format.Akram M. Zeki et al[9]., provided analysis on steganographic techniques and undertake an experiment using five Steganographic software in order to explore their capabilities. Benchmarking tool for identifying different performance aspects of the Steganographic techniques and Steganographic software like visual quality, performance indices, memory requirement and the evaluation of the maximum capacity for each software under this study.

Jayaram P et al[10]., made a survey on audio steganography. They proposed that Least Significant Bit (LSB) coding method is the simplest way to embed secret information in a digital audio file. This proposed method provides greater security and it is an efficient method for hiding the secret information from hackers and sent to the destination in a safe and undetectable manner. This proposed system also ensures that the size of the file is not changed even after encoding and it is also suitable for any type of audio file format.Md. Shafakhatullah Khan et al.[11], proposed a new approach which is sophisticated for concealing the data. They describes how the data is secured form the intruders even though they trace the audio file which contains the confidential data.The basic idea is to provide an optimized method for concealing the private data from intruders and sent to the destination in a safer and secure manner. It is an enhancement of spread spectrum audio data hiding methods.Wei Qin Cheng et al.[12], proposed a robust audio steganography. They implemented a simple Dynamic Linked Library [DLL] by using managed C++ and Microsoft .NET framework. It is implemented by Direct Sequence Spread Spectrum [DSSS] method on data block base.

3. PROBLEM FORMATION

Several works have been presented towards both steganography, cryptography as well as combining the techniques for better data security.

Even though the research of Steganography initially was carried out as a problem of hiding data behind cover images, as the technology has evolved more complex forms of steganography has evolved.

Some of the widely researched and evolved variants of Steganography are:

1) Hiding Image behind Video
2) Hiding Data behind Video
3) Hiding data behind Audio
4) Hiding Audio behind Video

One of the coherent requirements of steganography is that the size of the cover must be higher than that of payload. The higher the size ratio, the better hiding achieved.However with continues evolution of images, image screening for hiding data has also been intensified. Therefore the need of Hybrid steganography is increased. It is a form of steganography where data is first hidden behind one particular type of payload and the resultant stego object is further hidden behind another payload leading to more complex embedding which is difficult to track. This work deals with hybrid steganography where text message is hidden behind Image and the result is hidden behind audio file. The technique emphasize on achieving high PSNR for high BPP such that such a model do not require too many extra bits for stegano process.

Also a text data contains only characters and there is always a high tolerance for the text data. Even if some bits are corrupted, the text can be interpreted well. However in case of application exes, even a single corrupted bit might cause a wrong binding with underneath framework which causes the application to crash upon execution. Exe data is generally binary data. An exe file is generated by compiling a source code with compiler and linker. Compiled C file produces operating system specific exe where as compiled .Net files produce
exes that runs over a .Net virtual machine. These exes can be any application program like calculator, media player, calendar etc.Just like images, every exe data has two

important parts: the header and the data. Preserving header information is extremely important because if header is corrupted then the rest of the data can not be recovered.Therefore while using such data as payload, exe specific algorithm must be generated.

4. Proposed Work

4.1 Architecture and Overview

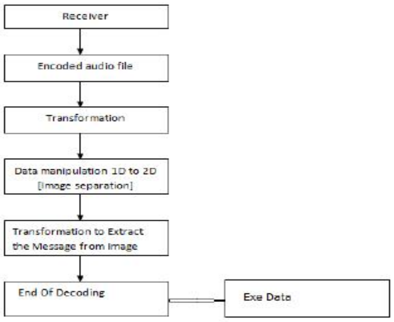

Receiver
Encoded audio file
Transformation
Data manipulation 1D to 2D [image separation]
Transformation to Extract the Message from Image
End Of Decoding
Exe Data

Figure 1: Encoder Block Diagram

Here Secret is the EXE file payload.

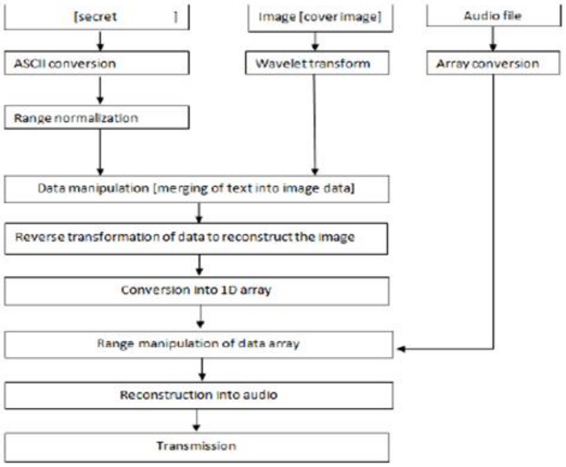

[secret]
Image [cover image]
Audio file
ASCII conversion
Wavelet transform
Array conversion
Range normalization
Data manipulation [merging of text into image data]
Reverse transformation of data to reconstruct the image
Conversion into 1D array
Range manipulation of data array
Reconstruction into audio
Transmission

Figure 2: Decoding Block Diagram

Overall block diagram of the encoding and decoding process is explained through Figure 1 and Figure 2. The techniques are briefly explained as bellow.

Encoding Algorithm

1. Read a Gray scale Image
2. Read a Payload EXE
3. Convert the Data to ASCII
4. Take Wavelet Transform of the Image
5. Find the maximum of the data and normalize the data by dividing it with MAx
6. Hide the normalized data in CV and cD
7. Reconstruct the image from wavelet
8. Reshape the image to single dimensional array.
9. Take the spectrum of the signal. (>3.3 KHz)
10. Store the length
11. Store reshaped Image
12. Reconstruct the Sound.(This is the output of encoder)

Decoding Algorithm

1. Perform FFT and find the signal Out
2. Convert 1d data to 2d and separate the image
3. Perform wavelet on the image part and extract the message part
4. Convert the ASCII data back to binary form
5. Construct the exe

4.2 Methodology

For simplicity of the discussion we will define payload exe as message. The message is in binary format. Initially the message of interest is taken into consideration. This message is to be converted to some machine readable format hence it is converted into ASCII form. Once this is done the image i.e the cover image is taken into consideration. It is converted to an array format so that it can be easily manipulated. Transformation is applied to this image and hence it is now available in the frequency domain.Once the cover image and the secret message are available in the frequency domain, range normalization of this data is carried out and then data manipulation is done so as to merge the secret message into the cover image data. Range normalization is a process in which the data is spread evenly over the entire range of it. After attaining this reverse transformation is applied to the data so as to obtain the stego image. This completes first level of steganography in which the secret message is embedded into the image file.Audio is a one dimensional data which has only amplitude values with respect to time. This data is represented as an array. Now the stego image is converted into array format and merged with the audio array. Audio is reconstructed and thus we have the second level of steganography and the final output is a stego audio. At the decoding end transformation is applied to the stego audio and the 1D data is converted into 2D and the image part of it extracted and the audio is rejected. Once the image is obtained again the transformation is applied and now the reverse transformation is applied so as to separately represent the secret message and image.

4.3 Transformation and Mathematical Model

In the proposed work we embed the data in the transformed domain of the image. Cover image is first converted to multi spectral bands using DWT. Data is than normalized and hidden behind suitable spectra of the cover such that visual distortion in the resultant stego image is minimum.The motivation for using the discrete wavelet transform is to obtain information that is more discriminating by providing a different resolution at different parts of the time–frequency plane. The wavelet transforms allow the partitioning of the time-frequency domain into nonuniform tiles in connection with the time–spectral contents of the signal. The wavelet methods are strongly connected with classical basis of the Haar functions; scaling and dilation of a basic wavelet can generate the basis Haar functions.

Two–dimensional N × N = 2n× 2n forward discrete Haar transform is defined in matrix notation as

$$S = a \bullet H(n) \bullet F \bullet a \bullet H(n)T \quad . (4.1)$$

The inverse transform is defined as
F = b • H(n)T • S • b • H(n) (4.2)
where F is the image in matrix form, the matrix is of dimension N × N pixels, S is the spectrum matrix and a•b = 1/N, hence parameters a or b may be defined as values 1/N,
1/ or 1, n = log2 N.
In Haar Wavelet Transform the low frequency wavelet coefficient are generated by averaging the two pixel values and high frequency coefficients are generated by taking half of the difference of the same two pixels. The four bands obtained are approximate band (LL), Vertical Band (LH), Horizontal band (HL), and diagonal detail band (HH). The approximation band consists of low frequency wavelet coefficients, which contain significant part of the spatial domain image. The other bands also called as detail bands consists of high frequency coefficients, which contain the edge details of the spatial domain image. This DWT decomposition of the signal continues until the desired scale is achieved. Two-dimensional signals, such as images, are transformed using the two-dimensional DWT.The two-dimensional DWT operates in a similar manner, with only slight variations from the one dimensional transform. Given a two-dimensional array of samples, the rows of the array are processed first with only one level of decomposition. This essentially divides the array into two vertical halves, with the first half storing the average coefficients, while the second vertical half stores the detail coefficients. This process is repeated again with the columns, resulting in four sub bands within the array defined by filter output. Since the discrete wavelet transform allows independent processing of the resulting components without significant perceptible interaction between them, hence it is expected to make the process of imperceptible embedding more effective.In those three detail components of a Haar DWT image, we can obtain various features about the original image as follows:

1. Average components are detected by the LL sub-band;
2. Vertical edges are detected by the HLsub-band;
3. Horizontal edges are detected by the LH sub-band;
4. Diagonal edges are detected by the HH sub-band.

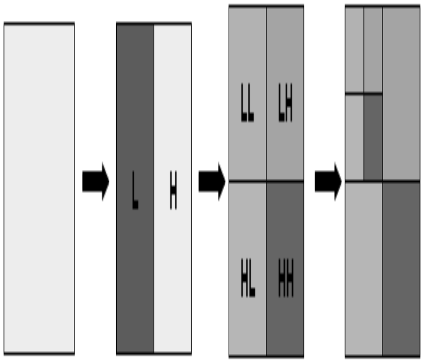


Fig.4.1 Subband coding

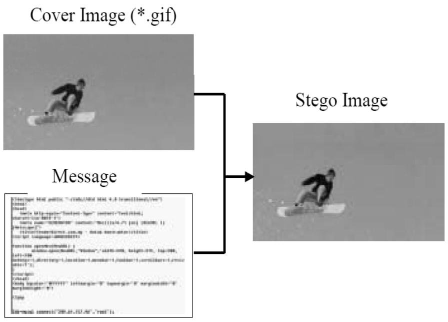


Fig 4.2: Result of Hiding

Audio Steganography

Like the document images, the sound files may be modified in such a way that they contain hidden information, like copyright information; these modifications must be done in such a way that it should be impossible for a pirate to remove it, at least not without destroying the original signal. The methods that embeds data in sound files use the properties of the Human Auditory System (HAS). The HAS perceives the additive random noise and also the perturbations in a sound file can also be detected. But there are some ―holes‖ that we can exploit. While the HAS have a large dynamic range, it has a fairly small differential range. As a result, loud sounds tend to mask out quiet sounds. And there are also some distortions that are so common that the HAS ignores them. The digital sound is obtained from the analog sound by converting it to digital domain. This process implies two sub processes: Sampling and Quantization. Sampling is the process in which the analogue values are only captured at regular time intervals. Quantization converts each input value into one of the discrete values. The most popular file formats for sounds are the Windows Audio-Visual (WAV) and the Audio Interchange File Format (AIFF). There are also compression algorithms such as the International Standards Organization Motion Pictures Expert Group-Audio (ISO MPEG-AUDIO). The most popular format for representing samples of high- quality digital audio is a 16-bit linear quantization e.g., Windows Audio-Visual (WAV) and Audio Interchange File Format (AIFF). Another popular format for lower quality audio is the logarithmically scaled 8-bit m-law. These quantization methods introduce some signal distortion, somewhat more evident in the case of 8-bit m-law. Popular temporal sampling rates for audio include 8 kHz (kilohertz), 9.6 kHz, 10 kHz, 12 kHz, 16 kHz, 22.05 kHz, and 44.1 kHz. Sampling rate impacts data hiding in that it puts an upper bound on the usable portion of the frequency spectrum (if a signal is sampled at ~8 kHz, it is not desirable to introduce modifications that have frequency components above ~4 kHz). For most data-hiding techniques developed, usable data space increases at least linearly with increased sampling rate.

4.2.3 Basic Model of Audio Steganography

The Basic model of Audio steganography consists of Carrier (Audio file), Message and Password. Carrier is also known as a cover-file, which conceals the secret information.Basically, the model for steganography is shown in Fig4.9. Message is the data that the sender wishes to remain it confidential. Message can be plain text, image, audio or any type of file. Password is known as a stego-key, which ensures that only the recipient who 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.

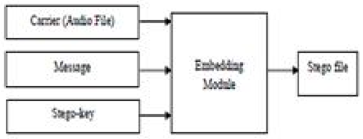


Figure 3: Basic Audio Steganographic Model

The information hiding process consists of following two steps.

i. Identification of redundant bits in a cover-file. Redundant bits are those bits that can be modified without corrupting the quality or destroying the integrity of the cover-file.

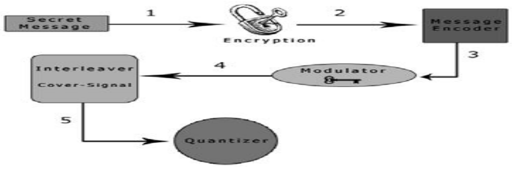
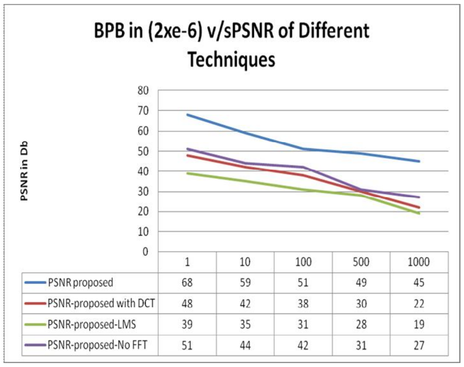


Fig. 4 Spread Spectrum (SS)

1. The secret message is encrypted using a symmetric key, k1.
2. The encrypted message is encoded using a low-rate error-correcting code. This step increases the overall robustness of the system.
3. The encoded message is then modulated with a pseudorandom signal that was generated using a second symmetric key, k2, as a seed.
4. The resulting random signal that contains the message is interleaved with the cover-signal.
5. The final signal is quantized to create a new digital audio file that contains the message.

This process is reversed for message extraction

5. Results



	1	10	100	500	1000
PSNR proposed	68	59	51	49	45
PSNR-proposed with DCT	48	42	38	30	22
PSNR-proposed-LMS	39	35	31	28	19
PSNR-proposed-No FFT	51	44	42	31	27

Result 5.1 Performance Comparison of Various Hybrid Steganography Techniques

As there are not many variants of Hybrid Steganography, We have changed the core model of the work and have compared the performances. The proposed work of DWT based image steganography followed by Spectrum based Audio steganography is compared will following other approaches.

a) DCT based Image steganography, followed by spectrum based audio steganography

b) LMS image steganography followed by Specturn based digital Steganography

c) DWT based image Steganography with LMS based Audio Steganography.

BPP is changed by varying the payload bits. All the experiments are conducted for Uncompressed Monochrome Image of 256x256 size and wav audio file of 2Mb. BPB is measured as Number bits of payload hidden par bit of audio file.Results are shown in Figure 5.1. Results show that the proposed technique is a clear winner in terms of performances against all other forms of steganography compared here.

6. Conclusion

Security plays a vital role in all aspects of life and technology. As the technology grows,its bounds in the positive direction, so do the reverse engineering of it. Data security has been of chief concern these days and plays a major role in terms of its complexity. One such means of providing data security is using steganography. The proposed work is one of the latest advancements accomplished in the field of application security. In this work an application exe binary payload is embedded into an image which is called the cover image. This provides first level of security which is known as primary stage steganography. In the second stage we embed the stego image into an audio file known as the carrier. This provides the final level of security in the two stage steganography that is implemented. For a general view it seems as a simple audio file that is transmitted finally but actually it has got the secret message and image hidden in it.A question now arises as to how this will be secure as one can easily identify the audio quality to be not that good and can try to decode. The answer to this is that maybe the image is extracted from the audio but how can one guess that there is another secret message been embedded in the image as its in gray scale. Thus with two levels of steganography we have achieved one of the very secure application security methods.Further research could be carried out in this direction with analysis of techniques such as Hiding data behind audio and putting that back to image, splitting the data into multiple objects, applying stego with different payloads and finally combining them into a final stego object.

References

[1] K B Shiva Kumar et. al. "Bit length replacement steganography based on DCT coefficients" / International Journal of Engineering Science and Technology
Vol. 2(8), 2010, 3561-3570

[2] K B Shiva Kumar et. al "Hybrid Domain in LSB Steganography" International Journal of Computer Applications (0975 – 8887)
Volume 19– No.7, April 2011

[3] K B Shiva Kumar et. al "Steganography Based on Payload Transformation" IJCSI International Journal of Computer Science Issues, Vol. 8, Issue 2, March 2011
ISSN (Online): 1694-0814. www.IJCSI.org

[4] Saddaf Rubab, Dr. M. Younus. "Improved Image Steganography Technique for Colored Images using Huffman Encoding with Symlet Wavelets" IJCSI International Journal of Computer Science Issues, Vol. 9, Issue 2, No 1, March 2012 ISSN (Online): 1694-0814".

[5] Akram M. Zeki, Adamu A. Ibrahim And Azizah A. Manaf, "Steganographic Software: Analysis and Implementation" International Journal Of Computers And Communications Issue 1, Volume 6, 2012

[6] S. K. Muttoo and Sushil Kumar, "Robust Source Coding Steganographic Technique Using Wavelet Transforms" BVICAM's International Journal of Information Technology.

[7] Kriti Saroha and Pradeep Kumar Singh "A Variant of LSB Steganography for Hiding Images in Audio". International Journal of Computer Applications (0975 – 8887) Volume 11– No.6, December 2

[8] Lalitha.G et al. / International Journal on Computer Science and Engineering (IJCSE), "Secure Transmission of Compound Information Using Image Steganography"

[9] Md. Shafakhatullah Khan et al. "An Optimized Method for Concealing Data using Audio Steganography" International Journal of Computer Applications (0975 – 8887) Volume 33– No.4, November 2011

[10] Pradeep Kumar Singh et. al "Enhancement of LSB based Steganography for Hiding Image in Audio". / (IJCSE) International Journal on Computer Science and Engineering Vol. 02, No. 05, 2010, 1652-1658

[11] Jayaram et al. "Information Hiding Using Audio Steganography –A Survey"The International Journal of Multimedia & Its Applications (IJMA) Vol.3, No.3, August 2011

[12] Elham Ghasemi, Jamshid Shanbehzadeh, Nima Fassihi. " High Capacity Image Steganography using Wavelet Transform and Genetic Algorithm". Proceedings of the international multiconference of engineers and computer scientists 2011 volI

[13]Majunatha Reddy, & K B Raja. "High Capacity And Security Steganography Using Discrete Wavelet Transform".

[14] Moerland, T., "Steganography and Steganalysis", Leiden Institute of Advanced Computing Science, www.liacs.nl/home/ tmoerl/privtech.pdf

[15] Sellars, D., "An Introduction to Steganography", URL: http://www.cs.uct.ac.za/courses/CS400W/NIS/papers99/dsellars/stego.html

[16] Wei Qin Cheng, Fei Han, Man Juon Tung, Kai Xu "Robust Audio Steganography using Direct-Sequence Spread Spectrum Technology".

AUTHOR

H S Jayaramu received the BE degree from Malnad College of Engineering, Hassan. MTech MTech degree from SJCE Mysore, MS degree from Birla Institute of Technology and Science BITS, Pilani, Rajasthan. He has got more than 33 years of teaching experience in various institutions and he has over 13 research publications in National and international conferences and Journals. Currently he is working as Professor
and HOD in the Dept. of Telecommunication Engineering, Sri Siddhartha Institute of Technology, Tumkur. His research interests include Signal processing, image processing, Logic design, and Steganography.

Dr Arvind K Goutam received his M Tech degree in Electronics & Communication Engineering from Rajastan VidhyaPeet & another M Tech degree in Instrumentation Engineering from R E C Kulakshetra and PhD from Meerut University. He has got 18 years of teaching experience and has 40 research publications in National and International conferences. Currently he is working as Principal, S D College of Engineering, Muzzaffarnagar, Uttar Pradesh. His research interests include image processing