IARJSET
ISSN (Online) 2393-8021
ISSN (Print) 2394-1588
International Advanced Research Journal in Science, Engineering and Technology
ISO 3297:2007 Certified
Vol. 3, Issue 12, December 2016

# Performance Evaluation of DWT and LSB Based Audio Steganography

**Punita Parnami[1], Kamal Niwariya[2], Manish Jain[2]**
M. Tech Scholar, Department of ECE, RKDFIST[1]
Assistant Prof., Department of ECE, RKDFIST[2]
Associate Prof., Department of ECE, RKDFIST[3]

**Abstract:** Information security, Steganography is a vast field of computer science that develops numerous intelligent systems for secret communication. Image steganography is the most popular dimension due to its frequency on the internet in this field. The goal of this research work is to provide high level of security, maximum embedding capacity, efficiency and reliability for secret communication using image processing and steganographic techniques. Same work has been done before through cryptographic techniques but with time steganography emerges as a more secure and power full technique, where as cryptography lacks in many ways. Now in modern era, steganography has come up with all the deficiencies of cryptography. In this research work, preprocessing, enhancement is applied on image. After that audio file is taken as secret information and on that sound file Discrete Cosine Transform (DCT) will be applied for compressing audio message .for Enhancing the security Advance encryption standard (AES) is used for the encryption of audio file and this encryption technique is more securing then other encryption techniques. Finally using Least Significant Bit (LSB) secret msg will be embedded in that image. The purpose of this work is to provide an intelligent system for secure communication within different security agencies as well as for institutes and to reduce the statistical attacks.

**Keywords:** Audio steganography, DWT, PSNR, LSB, Data Hiding, Digital data security.

## I. INTRODUCTION

This Steganography is the idea of hiding the existence of secret info by concealing it into another medium like image or audio. It originates from the Greek word steganos (covered) and graptos (writing). Steganography is completely different from cryptography, which is the science of hiding the meaning of information. Steganography and watermarking techniques embed info in a digital media in a transparent manner. Steganography may be a technique for covert info, but digital watermarking may not hide the existence of the message from 3rd persons. Information security [1] in today's world is a sense of declaration against threats, means that important information must be secured and there risks of attacks as well as controls must be balanced. Information security actually starts with the emergence of first main frame computer. But with the introduction of information security many viruses and code breakers were also developed that breaks the security channel and damage the important information.[6]

Steganography is a combination of two words "stegano" means covered and "graphy" means writing. Steganography [2] is an art of hiding the existence of the message so it dose attract the attention toward the secret message, hence third party or illegal person cannot be able to detect the message. Steganography is used in ancient times, like messages are written on the bodies using invisible inks, whereas other ways of sending messages is writing messages on envelops in areas which are covered with stamp. Modern methods of steganography are known as digital steganography.[6]

Modern steganography entered into this world in 1985 with the emergence of classical steganography problems. Approximately 725 multimedia steganography applications have identified by steganography analysis and research center (SARC). Steganography techniques include hiding within text file, text in image or audio or video, images within images, images within audios or videos, hiding messages in voice-over-IP, WLAN steganography is also used for sending information over local area network.[2] The main difference between cryptography and steganography, cryptography hides the message but the message cannot be decoded until unless public or private key is not known. On the other hand steganography hides the existence of the message, secret message is not difficult to decode in case of steganography but most of the people are not able to detect the presence of the message.[7]

Audio steganography is another dimension that is in audio format and can be in any other format that hide and transmit the information by manipulating audio file in an understandable manner. [3]Audio file is encode by three methods which are echo hiding, least significant bit, phase coding. Audio steganography is a secure medium as compare to others because sound frequency changes at every single bit. [4].

## II. STEGANOGRAPHY

Our focus is on image steganography and audio steganography because our matter of concern is related to

IARJSET
ISSN (Online) 2393-8021
ISSN (Print) 2394-1588
International Advanced Research Journal in Science, Engineering and Technology
ISO 3297:2007 Certified
Vol. 3, Issue 12, December 2016

these two dimensions as our topic is to hide audio file inside an image using Least Significant Bit technique and discrete cosine transform. Digital image processing techniques like preprocessing, enhancement, works for the manipulation of an image before embedding the audio file inside the image. [9] After image processing audio file is processed , Compressed using discrete transform and secured using (Advance Encryption Standard) AES algorithm. Advance Encryption standard is the strongest algorithm of cryptography until now, introduced by Vincent Rijmen, Joan Daemen in 1998 by US government. It works for the security of sensitive material of any type using 128, 192, 256 bits of key sizes. For compression of audio file discrete transform is used like DCT, DWT. These transform discard the values of audio file at high frequency without damaging much of file. Least significant bit insertion technique is used for the embedding of audio file inside an image.[5]

Over the last few years, Steganographers has achieved a lot of success upon hiding secret information or confidential data from intruders. With the emergence of modern steganography techniques, new and more power attacks were also developed. Many techniques like, JPEG, Outguess, F5 pixel value differencing etc has been deployed for secret communication but still in some cases the attackers broke these algorithms easily and retrieve the secret information. F5 algorithm is considered best for embedding high capacity data and better security at the same time. [5] This can reduce the risk of stealing the secret information during transformation but it is time consuming method. The incentive of this research is to provide a strong system to the Steganographers for secure communication, so that the powerful attackers cannot be able to break the algorithm. Main goal of steganography is to communicate securely in an entirely imperceptible way and to avoid drawing suspicion to the transmission of a hidden data. It's not only prevents others from knowing the hidden data, simply it also prevents others from thinking that the data even exists. Although a steganography technique causes somebody to suspect there's secret info in a carrier medium, then the method has failed. The ways that embeds data in sound files use the properties of the Human auditory system (HAS).[2].

## III. PROPOSED METHODOLOGY

The propose approach that uses numerous techniques like thresholding, DCT, LSB, it works with efficiency and supply maximum space at a similar time will increase security level, wherever because the quality of Steganographic image is additionally improved.

The new idea has been proposed for the security of secret information and parties as well. The main goal of this method is to develop an efficient security system for the protection of confidential data during the transformation process. The basic idea of this system is to analyze the image, secure the secret file as well as the cover files with strong algorithm. The system consist of two main phases encryption and decryption various stages of encryption are; image acquisition, preprocessing, enhancement, read and convert audio file, applying compression using DCT transform, Embedding audio in image using LSB technique, Stego image is retrieved. In preprocessing stage, if image contain any type of noise, smoothing will be applied to remove noise.[3] Afterwards, in enhancement phase, the visual appearance of the image will be improved using histogram equalization. Proceeding towards audio file, read and compression is performed using DCT (discrete cosine transforms). Now encrypt the audio file using AES (advance encryption algorithm), it is the strongest algorithm for encryption until now. [6] After encryption audio file is embedded in image using LSB (least significant bit) technique and Stego image is retrieved. Now decryption phase, embedded image is retrieved. Secret data is recovered. Decrypt the audio file; convert the audio file from hexadecimal to decimal integer. Retrieve the original audio file.[3].

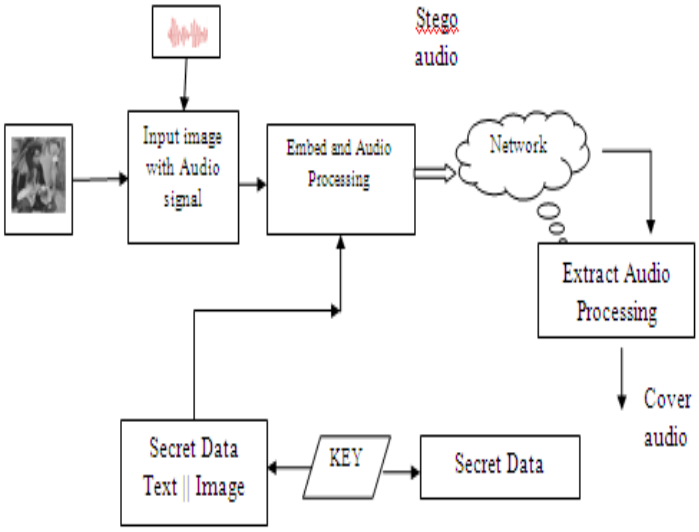



Fig. 1 Blocks diagram for audio steganography.

IARJSET
ISSN (Online) 2393-8021
ISSN (Print) 2394-1588
International Advanced Research Journal in Science, Engineering and Technology
ISO 3297:2007 Certified
Vol. 3, Issue 12, December 2016

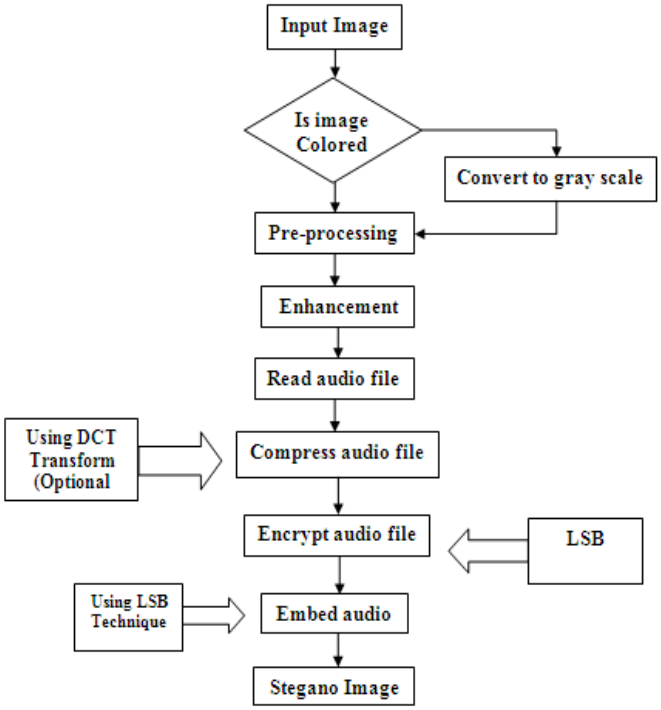



Fig.2 Flow chart of propose solution

The propose solution is analyzed on the basis of PSNR (peak signal to noise ratio) and MSE (mean square error) frequency. Whereas PSNR is used to measure the image quality of original and Stego image. Generally, high value of PSNR indicates that Stego image is of higher quality. [5] MSE is a risk function that represents average square error between the original image and Stego image.

A. MSE

The Mean Square Error (MSE) and the Peak Signal to Noise Ratio (PSNR) are the two error metrics used to compare image compression quality. The MSE represents the cumulative squared error between the compressed and the original image, whereas PSNR represents a measure of the peak error.

The lower the value of MSE, the lower the error:

$$MSE = \frac{\sum_{M,N}\left[I_1(M,N) - I_2(M,N)\right]^2}{M * N}$$

B. PSNR

To compute the PSNR, the block first calculates the mean-squared error using the following equation: In the previous equation, M and N are the number of rows and columns in the input images, respectively. Then the block computes the PSNR using the following equation:

$$PSNR = 10\log_{10}\frac{R^2}{MSE}$$

In the previous equation, R is the maximum fluctuation in the input image data type.

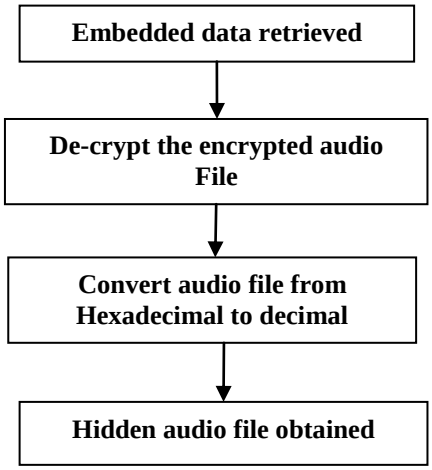



Fig.3 Decryption process

## IV. RESULT & DISCUSSION

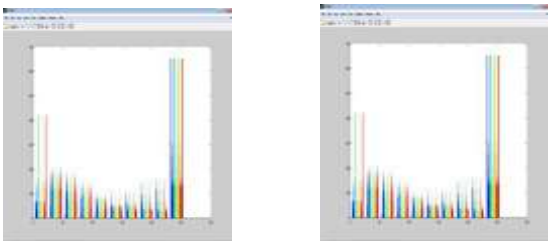
The The simple LSB technique is applied on the images below. Single bit of each byte is manipulated using LSB and the change is too minor that it can't be seen by naked eye. After implementation Original-images, Embedded-images along with their histograms are shown respectively.


(a)Before Embedding


(b) After Embedding


DOI 10.17148/IARJSET.2016.31232

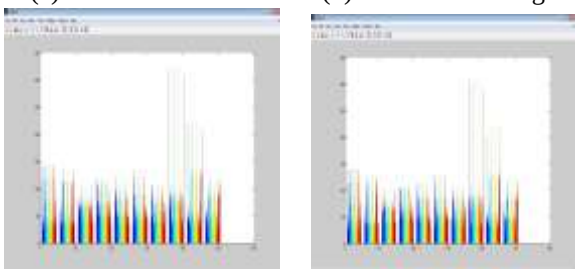
IARJSET
ISSN (Online) 2393-8021
ISSN (Print) 2394-1588
International Advanced Research Journal in Science, Engineering and Technology
ISO 3297:2007 Certified
Vol. 3, Issue 12, December 2016



Histogram Original Image Histogram Embedded Image
Fig. 4: 'Landscape.jpeg'

This figure 4 shows the Landscape .jpeg image. In this fig.(a) the original image and fig.(b) is the after embedding process we get the output image. Fig. (c) shows the histogram of original image and fig.(d) is the histogram of embedded imge.

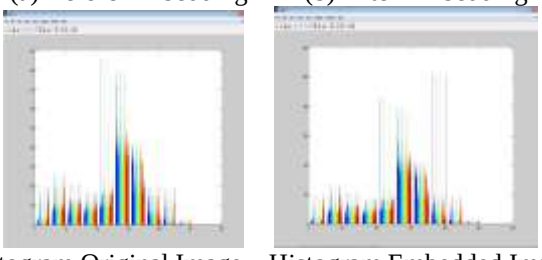
(a) Before Embedd (b) After Embedding



Histogram Original Image Histogram Embedded Image
Fig. 5: 'jaar.bmp'

This figure5 shows the Jaar .bmp image. In this fig.(a) the original image and fig.(b) is the after embedding process we get the output image. Fig. (c) shows the histogram of original image and fig.(d) is histogram of embedded imge.

(a) Before Embedding (b) After Embedding



Histogram Original Image Histogram Embedded Image
Fig. 6: 'Ship.png'

This figure 6 shows the Ship .png image. In this fig.(a) the original image and fig.(b) is the after embedding process we get the output image. Fig. (c) shows the histogram of original image and fig.(d) is the histogram of embedded imge.

## V. CONCLUSION

The proposed method effectively produces Stego image in which secret data is embedded and encrypted as well using AES algorithm. The Efficiency of the technique is measured by using different evaluating parameters. Among all PSNR and MSE are the two most reliable parameters to analyze the quality of the Stego image. From Experimentation, it has been observed that the value of PSNR is high and MSE is low. Higher value of PSNR of embedded image shows that there are no modifiable changes in it. The amount of hidden data is quite reasonable. It has been approved that Least Significant Bit technique perform better and is best to be used with grayscale Platte or one with ordinary change in shades. Better substitution method for hiding data in grayscales then in RGB image.

## REFERENCES

[1] Neha Gupta, Ms. Nidhi Sharma, "Dwt and Lsb Based Audio Steganography" 2014 International Conference on Reliability, Optimization and Information Technology - ICROIT 2014, India, Feb 6-8 2014
[2] Mansour Sheikhan, Kazem Asadollahi and Reza Shahnazi "Improvement of Embedding Capacity and Quality of DWT-Based Audio Steganography Systems" World Applied Sciences Journal 13 (3): 507-516, 2011 ISSN 1818-4952
[3] Ankit Chadha, Neha Satam, Rakshak Sood, Dattatray Bade "An Efficient Method for Image and Audio Steganography using Least Significant Bit (LSB) Substitution" International Journal of Computer Applications (0975 –8887) Volume 77–No.13, September 2013
[4] Fatiha Djebbar, Beghdad Ayady, Habib Hamamzand Karim Abed-Meraimx "A view on latest audio steganography techniques" 2011 International Conference on Innovations in Information Technology
[5] Haider Ismael Shahadi, Razali Jidin "High Capacity and Inaudibility Audio Steganography Scheme" 978-1-4577-2155-7/11/$26.00 2011 IEEE
[6] M. M Amin, M. Salleh, S. Ibrahim, M.R.K atmin, and M.Z.I.Shamsuddin "Information Hiding using Stegangraphy" 4th National Conference on Telecommunication Technology Proceedings, Shah Alam, Malaysia, 2003.
[7] N F. Johnson. Steganography tools. Available from: http://www.jjtc.com/Security/stegtools.htm 2005.
[8] R.Anderson, F.Petitcolas: On the limits of the steganography, IEEE Journal Selected Areas in Communications, VOL .16, NO.4, MAY 1998.
[9] M. Wu, B.Liu. "Multimedia Data Hiding", Springer- Verlag New York, 2003
[10] N.F. Johnson Z.Duricands. jajodia "Information Hiding Steganography and Water marking –Attacks and Countermeasures", Kluwer Academic Publishers, 2001