International Journal of Innovative Technologies

WWW.IJITECH.ORG

ISSN 2321-8665
Volume.08, Issue.02,
November, 2020,
Pages:138-142

Complex Wavelet Transform based Audio Steganography in Image

J. SOMASEKHAR[1], M. CHENNAIAH[2], T. CHAKRAPANI[3], K. SUDHAKAR[4]

[1]PG Scholar, Dept of ECE, SJCET, Yemmiganur, Kurnool, Andhra Pradesh, India.
[2]Assistant Professor, Dept of ECE, SJCET, Yemmiganur, Kurnool, Andhra Pradesh, India.
[3]Associate Professor, Dept of ECE, SJCET, Yemmiganur, Kurnool, Andhra Pradesh, India.
[4]Professor & HOD, Dept of ECE, SJCET, Yemmiganur, Kurnool, Andhra Pradesh, India.

Abstract: In this paper, we have modeled a new Steganographic method to steganize an audio signal in image. Towards this prospect, we have focused on the wavelet transform for the transformation of both image and audio. To achieve more resilience to the attacks and to increase the security, this work considers Dual Tree Complex Wavelet Transform (DTCWT) as a transform for the image and Discrete Wavelet Transform (DWT) for audio. To reduce the additional complexity with the secret key generation, a new method of embedding is proposed in this work without any need of secret key. The audio signal itself generates the secret key. The performance evaluation is carried out for the both recovered audio signal and recovered image. Several performance metrics are evaluated under performance evaluation.

Keywords: Image Steganography, DWT, Secret key, PSNR, SSIM, CQM, SPCC.

I. INTRODUCTION

Image steganography [2], [3] is the most common form of steganography and most widely used in various fields for hiding text in image, audio in image, video in image. It is the most popular medium on internet due to its high frequency of usage. There are different forms for coding in image commonly used method are least significant bit insertion , in which hiding any type of data in only least significant two or three bits of a byte. Other way of hiding is using masking and filtering techniques. Some algorithms and transformation are also used for hiding image within image or other mediums. Though there are so many approaches proposed in earlier to hide the secret information in images, still there exists the problem in the tradeoff between security and capacity. The main problem is the provision of an enhanced security along with a limited capacity. Then only the secret information even with large size can be Seganized more efficiently. There are mainly two types of steganography techniques: temporal domain and transform domain. In temporal domain, the actual sample values are manipulated to hide the secret information. In transform domain, the cover object is converted to different domain such as frequency domain, to get the transformed coefficients. These coefficients are manipulated to hide the secret information. Then the inverse transformation is applied on the coefficients to get stego signals.

The temporal domain techniques are more prone to attacks than transform domain techniques because there actual sample values are modified. The transforms that can be used are Fast Fourier Transform (FFT),Discrete Cosine Transform (DCT) or Discrete Wavelet Transform (DWT) [10]. The drawback of FFT is that Fourier Transform gives frequency information, but it does not provide information about its timings. This is because the basis functions (sine and cosine) used by this transform are infinitely long. They pick up the different frequencies of *f(t)* regardless of where they are located. DCT produces artifact problems. In this project, a new method is proposed to hide the audio secret information [4,9] in the image without the need of any secret key. To achieve more resilience to the attacks and to increase the security, this work considers DTCWT as a transform for image and DWT for audio. To reduce the additional complexity with the secret key generation, a new method of embedding is proposed in this work without any need of secret key. The audio signal itself generates the secret key. To increase the capacity, only limited number of bits of secret information is considered for embedding. To illustrate the robustness, the audio samples with various lengths are processed for embedding and extraction. Rest of the paper is organized as follows; section II describes the related work. The complete details of proposed approach are described in section III. Section illustrates the simulation results and finally the conclusions are given in section V.

II. RELATED WORK

In earlier there are so many approaches proposed to achieve an enhanced performance in the image steganography. To test the robustness of Discrete Wavelet Transform based steganography algorithm, Vijay Kumar et.al [10] evaluated the performance of stego-images by subjecting the stego images to different types of attacks and proved that secret image can be retrieved. These attacks include Gaussian noise, Sharpening, median filtering, Gaussian blur, Histogram Equalization and Gamma Correction.

Ali Kansoet.al[11] tested their steganography algorithm against the existing steganalytic attacks like histogram test, RS attack, Chi-square test, PSNR test, Structural Similarity Index Metric (SSIM) test etc. RS attack is used to detect stegos with LSB replacement and to estimate the size of the hidden message [12]. The difference expansion, histogram shifting and interpolation strategies are applied to increase the hiding capacity in image steganography [13]. Ki-Hyun Jung et.al [14] used image interpolation and edge detection to increase payload capacity and image quality.

M.I.Khalil [16] has discussed the possibility of hiding short audio messages inside the digital image. His proposed approach encrypts the audio message before hiding it into the image. He has used cryptography, steganography, audio message, least significant bit (LSB) method whereas the purpose of steganography is to communicate completely in an undetectable manner.

R.A.Jain et al [17] presents a paper that uses different technique of hiding secret information using three formats text, image, and audio makes the system stronger and secure. Cryptography along with steganography is applied, whereas cryptography scrambles the message and makes it Meaningless and unintelligible. On the other hand steganography hides the existence of message itself.

Samarth.K.N and et al [18], give a new idea of replacing the Least Significant bits by selecting the pixels using key that provides better security. Authors gave a predictable method that three bits of data can be hidden in a single byte as it can cause no change in the image as per the human visual system (HVS). This technique will increase the capacity to hide large audio file. RGB color space (most common) and LSB technique is used.

AnkitChadha et al [19], has employed Karhunen-Loève Transform (KLT) for performing steganography and for better image quality pixel matrix of specific size is used. KLT helps in compression, so initially data is compacted using KLT as to accomplish a higher hiding limit, and then afterward packed into LSBs of carrier image, which is in the RGB spatial domain. After that original matrix is divided into sub-matrix and each pixel is further divided into R, G and B pixels, thus the matrix has increased into the size, three times the original image.

P.Prabhu et al [20] presents a method of hiding secret file in the form of audio message within another audio file (.wav). Crypto-Stego technique was used to improve better protection of message. In this paper secret message is first encrypted using private key cryptography and then it is embedded into host audio file.

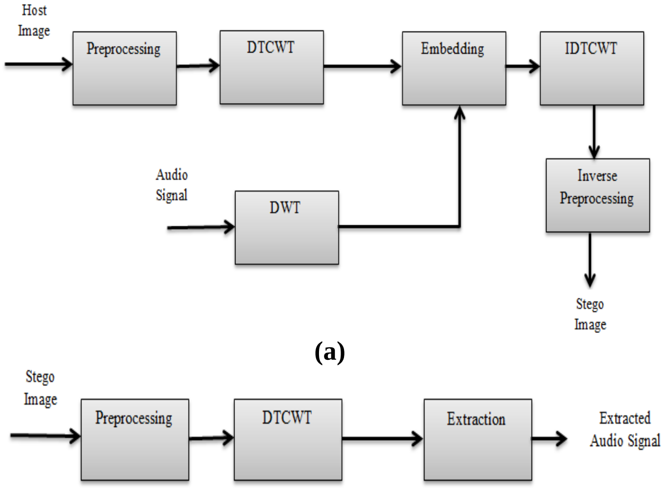
PritamKumari et al [21], has discussed various techniques of image steganography for data security which can be text file, image, audio video. Steganography itself is a technique that covers the invisible communications that can be in any format. The purpose of this paper is to give a complete understanding of image steganography regarding its history, techniques, advantages or disadvantages. Modern methods of image steganography are LSB, palette based LSB, transform domain, patchwork etc.

Buddha Lavanya et al [22], has propose a method of hiding textual data inside an audio file. Firstly the textual data is embedded into the image after that image is embedded into the audio file. The main purpose of this paper is to hide data without damaging the file arrangement and contents of audio file. Modern steganography is generally easy to deal with electronic data and it must have characteristics like secrecy, high capacity, imperceptibility, resistance and accurate extraction.

AshimaWadhwa [23], author has discussed various audio Steganographic techniques, their comparison and evaluation. Cryptography, Digital Watermarking and Steganography are major concerns of digital data security. Cryptography has two type's Symmetric key cryptography (same key is used by sender and receiver) and Asymmetric key cryptography (different key is used by sender and receiver).

III. PROPOSED APPORACH

This section illustrates the complete details about the proposed system architecture and methodology. The algorithm and the working procedure is also illustrated in this section. The system architecture is shown in the figure.1.



(a)

(b)

Figure.1. Block diagram of proposed system (a) Embedding (b) Extraction.

The system architecture of proposed system is represented in figure.1. The complete accomplishment of proposed approach is carried out in two phase, embedding phase (Figure.1(a)) and extraction phase Figure(1(b)). In embedding phase the secret information is embedded din the host image and in the extraction phase the secret information is extracted from the stego image. Here an audio signal is embedded in the image to hide the audio information. The image is considered as a host and the audio is considered as secret. Initially a host image of size 512*512 is preprocessed and converted into YCbCr space from RGB space. Then the Cb component of host image is decomposed through lifting wavelet transform and decomposed into four bands, two low frequencies and two high frequencies. The secret information is also subjected to wavelet decomposition and only approximations are processed for embedding. Only two bits of approximation coefficients are embedded in the high frequency coefficients of host image. Then the Cb component is reconstructed through inverse lifting wavelet transform. The same process is applied over the Cr component. Finally the stego YCbCr image is retransformed into RGB. At the extraction phase, the procedure exactly inverse to the embedding is applied over the stego image to extract the secret information. Further the extracted audio signal is compared with original audio signal to check the performance of proposed approach. Peak Signal to Noise Ratio (PSNR), Structural Similarity Index Measure (SSIM), and Color Image Quality Measure (CQM) are numerical parameters considered for performance evaluation of stego image. Signal to Noise Ratio (SNR), and Squared Pearson Correlation Coefficient (SPCC) are the numerical metrics considered for performance checking of the audio signal.

The complete Process is outlined in the following algorithms;

Algorithm 1: Embedding

Input: cover image C and secret audio S.wav, **output:** stego image G

Step 1: Read cover image C and secret audio S.
C=imread('C.jpg')
S=audioread('S.wav')

Step 2: Represent C in YCbCr and obtain DTCWT of Cb component to get four sub bands CLL, CHL, CLH and CHH.

LS = DTCWT('haar', 'Int2Int')

[CLL,CHL,CLH,CHH] = DTCWT(double(Cb),LS)

Step 3: Obtain DWT of secret audio to get approximation and detail coefficients

[CA, CD] = DWT(double(S),LS)

Step 4: Hide the approximation coefficients of secret audio in the second and third LSB planes of CHH and CLH sub bands after encryption.

{C1, C2} = encode (CA, CLH, CHH)

In this method two bits of the secret message are hidden in one byte of the cover image. Two bits from the secret are XORed with 5th and 4th bits of the cover byte to get encrypted secret bits. Suppose S1 and S0 are two secret bits, then S1' = S1 XOR b5 XOR b4 and S0' = S0 XOR b5 XOR b4, where b5 and b4 are 5th and 4th bits of the cover byte respectively. 3rd and 2nd bits of the cover byte are replaced by these encrypted secret bits. This type of dynamic encryption avoids the need for encryption key. Embedding can be done in the Cr component also in the similar fashion. Here C1 and C2 are the modified CLH and CHH.

Step 5: Obtain inverse DTCWT to get stego Cb. Then convert to RGB format.

G = DTCWT(CLL, CHL, C1, C2, LS)
G=ycbcr2rgb(YGCr)
stegoimage =imwrite(G, 'stego.jpg')

Step 6: End Embedding.

Algorithm2: Extraction

Input: stego image G, output: secret audio S.wav

Step 1: Read stego image G and represent in YCbCr format.
G'=imread('G.jpg')
YCb'Cr=rgb2ycbcr (G')

Step 2: Obtain DTCWT of Cb' to get four sub bands: GLL, GHL, GLH, and GHH.

LS = DTCWT ('haar', 'Int2Int')

[GLL, GHL, GLH, GHH] = DTCWT (double(Cob'),LS)

Step 3: Extract the encrypted secret audio bits from the second and third bit planes of GLH and GHH. Then decrypt.
Cabin = decode (GHH, GLH)

In this method, two encrypted bits of the secret message are obtained from one byte of the stego image coefficient. Then decryption is done as follows: the two encrypted bits are XORed with 5th and 4th bits of the stego byte to get secret bits i.e., S1 = S1' XOR b5 XOR b4 and S0 = S0' XOR b5 XOR b4.

Step 4: Convert to decimal to get approximation coefficients of secret audio.

CA=bin2dec(CAbin)

Step 5: Obtain inverse IWT for approximation coefficients obtained in step 4 and considering zeroes for detailed coefficients. The result is secret audio

S=IDWT(CA,0,LS)

Step 6: End Extracting.

IV. SIMULATION RESULTS

A. Experimental Setup

This section presents a discussion of experimental results obtained from testing the proposed steganography system where it was implemented using Matlab 2012a running on a Windows 8 platform. The proposed system is tested using RGB cover and secret images with different sizes. Both the secret image and the cover image are in the '.JPEG' format. After running the proposed approach to get the best cover image, the embedding phase is then run to get the stego image and then the extraction phase is run to extract the secret image from stego image. Objective tests (PSNR and MSE) are used to evaluate the overall system performance. Figure.2, shows the secret images and the corresponding best cover images used to test the proposed system.

(a) (b)

Figure.2 oriignal Host images (a) Peppers (b) Lena (c) Barbara.

Along with the host images the audios signals considered for performance eualuation are shown in figure.3.

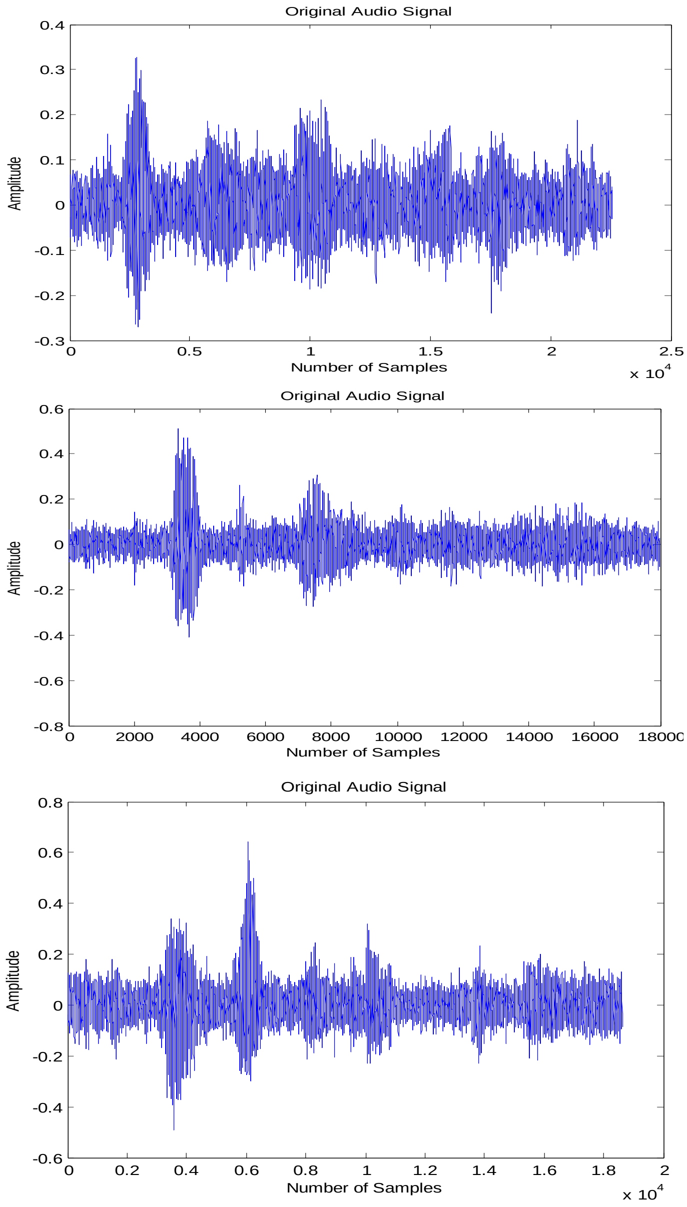
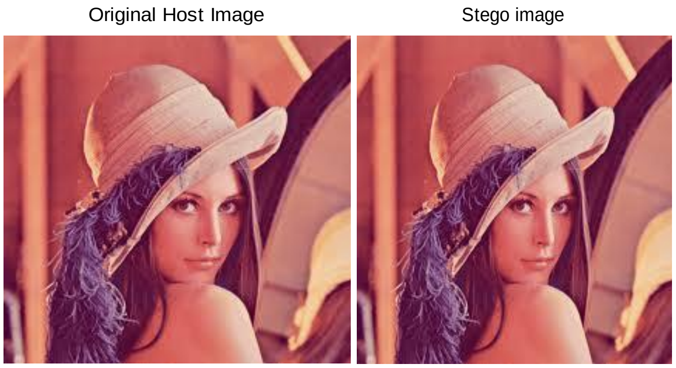


Figure.3. Test Audio Samples 1 to 3.

B. Experimental Results



(a) **(b)**

Figure.4. (a) original image (b) Stego Image.

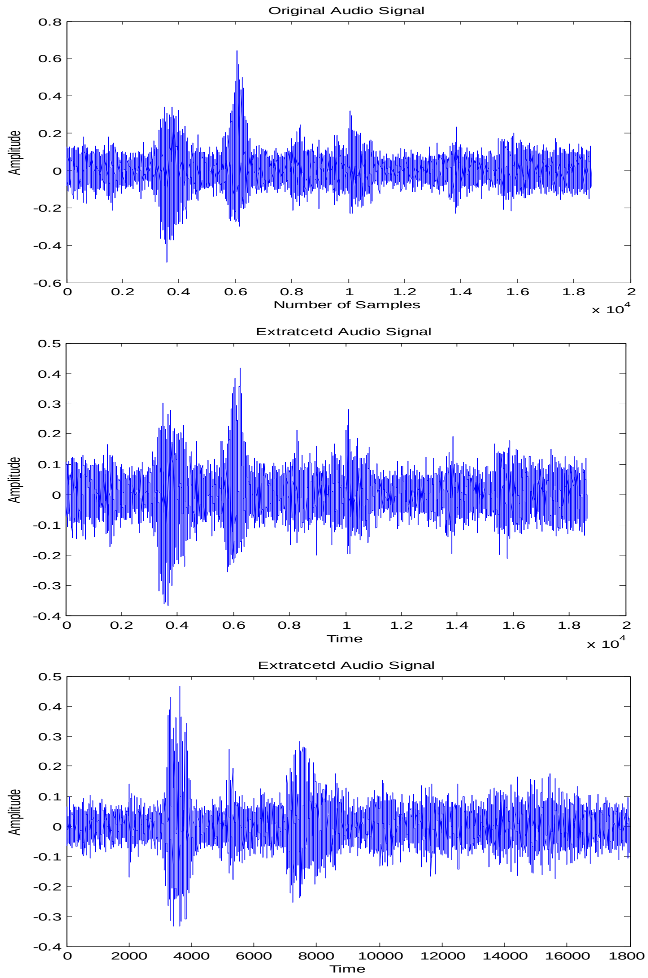


Figure.5. Extracted audio signals 1to 3 from stego image.

Further the extratcted signal is processed for performance evaluation through the mertics specified above. PSNR. SSIM and CQM are used to meausre the performance of stego image, SNR andSPCC are used for the performance evaluation of audio soignal. The obtained metrics for the cases of 1, 2 and 3 are shown in Table.1.

Table1. Performance metrics for the case of lena as a host image

Sample	PSNR	SSIM	CQM	SNR	SPCC
Sample 1	44.1028	0.9628	46.5017	39.3966	0.9576
Sample 2	43.7558	0.9462	46.4412	39.6094	0.8398
Sample 3	44.0567	0.9245	46.4287	40.0068	0.8375

V. CONCLUSION

In this project, an image steganography technique is proposed to hide audio signal in image in the transform domain using wavelet transform. The audio signal in any format (MP3 or WAV or any other type) is encrypted and carried by the image without revealing the existence to anybody. When the secret information is hidden in the carrier the result is the stego signal. Then the obtained stego image is subjected to attacks and then processed through the proposed approach is processed. The performance evaluation is carried out for the both recovered audio signal and recovered image. PSNR, SSIM, UIQI, SNR and SPCC are the metrics evaluated under performance evaluation. The proposed approach gives good values for all the metrics and hence this is an efficient way to send audio files without revealing its existence. The performance against some of the attacks is also good. The technique needs to be tested against other attacks like histogram equalization, cropping, occlusion, translation etc. the experimental results show that the secret audio can be extracted without much distortion in most of the cases.The obtained simulation results also revealed the efficiency of proposed approach both in the provision of security and imperceptibility. The proposed approach also applied for the attack cases and proved the efficiency.

VI. REFERENCES

[1]en.wikipedia.org/wiki/Information security.

[2]en.wikipedia.org/wiki/Steganography.

[3]http://www.slideshare.net/beautifulneha/steganography-10710623.

[4]Diqun Yan, Rangding Wang, Xianmin Yu, Jie Zhu. Steganography for MP3 audio by exploiting the rule of window switching, Computers & Security 31, 2012. Elsevier publications. pp 704-716.

[5]Zhou Wang, Alan Conrad Bovik, Hamid Rahim Sheikh, Eero P. Simoncelli. Image Quality Assessment: From Error Visibility to Structure Similarity. IEEE Transactions on image processing, Vol. 13, No. 4, 2004. pp. 600-612.

[6]C.Sasivarnan, A. Jagan, JaspreetKaur, DivyaJyoti, Dr.D.S. Rao. Image Quality Assessment Techniques in Spatial Domain. IJCST Vol. 2, Issue 3, 2011. pp 177-184.

[7]M. I. Khalil. Image steganography: Hiding short messages within digital images. JCS&T, Vol.11, No. 2. pp 68-73.

[8] YıldırayYalman, ĐsmailErtürk. A new color image quality measure based on YUV transformation and PSNR for human vision system, 2011. Pp. 1-18.

[9] Jose Juan Garcia-Hernandez, Ramon Parra-Michel, Claudia Feregrino-Uribe, Rene Cumplido. High payload data-hiding in audio signals based on a modified OFDM approach. Expert Systems with Applications 40, 2013. Elsevier publications. Pp 3055–3064.

[10] Vijay Kumar and Dinesh Kumar. Performance Evaluation of DWT based Steganography. IEEE 2nd International Advance Computing Conference, 2010. pp 223-228.

[11] Ali Kanso, Hala S. Own. Steganographic algorithm based on a chaotic map. Communication Nonlinear Science Numerical Simulation, 17, 2012. Pp.3287–3302.

[12]S. Geetha, V. Kabilan, S.P. Chockalingam, N. Kamaraj. Varying radix numeral system based adaptive image steganography. Information Processing Letters 111, 2011. pp 792–797.

[13]Tzu-Chuen Lu, Chin-Chen Chang & Ying- Hsuan Huang. High capacity reversible hiding scheme based on interpolation, difference expansion, and histogram shifting, Springer 2013.

[14]Ki-Hyun Jung, Kee-Young Yoo. Data hiding using edge detector for scalable images, Springer 2012.

[15]AnkitChadha, NehaSatam, RakshakSood, Dattatray Bade," An Efficient Method for Image and Audio Steganography using Least Significant Bit (LSB) Substitution", International Journal of Computer Applications Volume 77– No.13, September 2013, ISSN:0975 – 8887.

[16]M.I.Khalil," Image Steganography: Hiding Short Audio Messages within Digital Images", JCS&T, Vol .11 No 2, October 2011.

[17]R.A.Jain, HrushikeshB.Surve, AmitA.Sonar, Swpanil N.Salunke, "Secret Communication through Image and Audio for Defense", International Journal of Science and Modern Engineering (IJISME), Volume-1, Issue-5, April 2013, ISSN: 2319-6386.

[18]Samarth.K.N, Poornapragna.M.S, Sambhav Kumar.P.Jain, Nagarathna, "A Novel Technique Of Hiding An Audio Message In An Image", International Conference on Electronics and Communication Engineering, 28th April-2013, Bengaluru, ISBN: 978-93-83060-04-7.

[19]AnkitChadha, NehaSatam, RakshakSood, Dattatray Bade , "Image Steganography using Karhunen-Loève Transform and Least Bit Substitution", International Journal of Computer Applications ,Volume 79 – No9, October 2013, pp. 0975–8887.

[20] K.Sakthisudan, P.Prabhu and P.thangaraj, "Secure Audio Steganography for hiding Secret Information", International Conference on recent trends in Computational methods, Communication and Controls (ICON3C 2012).

[21] PritamKumari, Chetna Kumar, Preeyanshi and jayaBhushan, " Data Security Using Image steganography And Weighing Its Techniques", International Journal Of Scientific & Technology Research, Volume 2 ,Issue 11,November 2013. ISSN 2277-8616.

[22] BuddaLavanya, Yangala, SrinivasaRao, "Data Hiding In Audio By Using Image Steganography Technique," International Journal Of Emerging Trends & Technology In Computer Science, Volume. 2, Issue 6, Nov-Dec 2013. ISSN: 2278-6856.

[23] AshimaWadhwa, "A Survey on Audio Steganography Techniques for Digital Data Security", International Journal of Advance Research in Computer Science and Software Engineering, Volume 4, Issue 4, April 2014. ISSN: 2277-128X.