International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 06 Issue: 05 | May 2019 www.irjet.net p-ISSN: 2395-0072

Wavelet Transform Based Steganography

Riya Gupta[1], Riya Tyagi[2], Prachi Sahansarval[3] , Nitika Tyagi[4]

[1,2,3,4] *Student, Dept. of Computer Science & Engineering, Inderprastha Engineering College, U.P., India*

Abstract - *Information security is one of the most important factors to be considered when secret information has to be communicated between two parties. There are two techniques used for this purpose: Cryptography and steganography. Cryptography scrambles the information, but it reveals the existence of the secret information. Whereas Steganography hides the actual existence of the information so that anyone other than sender and the recipient cannot recognize the transmission. In steganography the secret information is made invisible by hiding it in some other carrier wave. In this paper an image steganography techniques 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. In this work, the results show good quality stego signal and the stego signal is analyzed for different attacks. It is found that the technique is robust and it can withstand the attacks. Peak Signal to Noise Ratio(PSNR) , Structural Similarity Index Metric (SSIM) are used to measure quality of stego image. Signal to Noise Ratio (SNR), Squared Pearson Correlation Coefficient (SPCC) are used to measure quality of extracted secret audio signal. The results show good values for these metrics.*

Keywords: **Information security, Discrete Wavelet Transform, Steganography, SSIM, SNR, PSNR, Secret communication.**

1. INTRODUCTION

Over many years information security is the biggest challenge for researchers. Since cryptography cannot make anything invisible, it is replaced by steganography for unseen communication. Steganography hides secret information in other objects known as cover objects. Cover object along with the hidden information is called stego object. This cover can be image, audio or video. And the secret can be image, audio or text message. In this paper the cover is an image and secret information is an audio file.

1.1 Steganography techniques

There are two kinds of steganography techniques: temporal domain and transform domain. In temporal domain, the secret information is hidden by manipulating actual sample values. While 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. Transform domain techniques are better as unlike temporal domain they use modified actual sample values. The transforms that can be used are: Fast Fourier Transform (FFT), Discrete Cosine Transform (DCT), and Discrete Wavelet Transform (DWT). In this paper DWT is used because frequency content of a function f (t) is given as a function of time by wavelet transform. The demerit of FFT is that it gives frequency information, but it does not provide information about its timings. This is because the basis functions (sine and cosine) used by it are infinitely long. They pick up the different frequencies off (t) regardless of where they are located. DCT products artifact problems.

1.2 Discrete Wavelet Transform (DWT)

In wavelet transformation, a mother wavelet is selected, mother wavelet is a function that is nonzero in some small interval, and it used to explore the properties of the function f (t) in that interval. The mother wavelet is then translated to another interval of the time and used in the same way. So, with wavelet sharp discontinuities can be approximated and also they provide a time-frequency representation of the signal. There are many wavelets which can be used for this purpose. Haar wavelet is the simplest one among all the wavelets. Information that are analyzed in real-life situations is discrete. These information come in the form of number, rather than a continuous function. This is why discrete is used in practice. When the input data consists of sequences of the integers as in the images, wavelet transforms that map integers to integers can be used. Integer Wavelet Transform(IWT) is one such approach. Image is the most popular cover object used in steganography.

1.3 Image

Image is one of the most popular cover object used for steganography. Cover images may be gray scale images or color images. Colour images have large space for information hiding and therefore color images are more Popular than gray scale image steganography. There are various format to represent the color image such as YIQ, YCbCr (Luminance, Chrominance) etc. When the wavelet transformation is applied to a color image, the transformation coefficients are obtained for all the three channels in the corresponding representation. When wavelet transform is applied to an image, it is decomposed into four sub-bands LL, LH, HL, HH. LL is the low frequency sub-band and contains the approximation coefficients. The significant features of the image are contained in this sub-band. Other three sub-bands are high frequency sub-bands and contain less significant features. Image can be reconstructed by considering only LL sub-band.

1.4 Audio

Audio signals are analog signals. To use digital signal processing methods on an analog signal, it is sampled periodically in time. It produces sequence of samples. WAV file is the simplest among all the audio file formats. WAV format store samples "in the raw" form where no pre-processing is required. The MP3 standard involves a coding technique that includes several methods namely, sub-band decomposition, filter bank analysis. The encoder operates on successive tracks of the audio signal. Each track contains 1152 samples and one track is divided into two pieces with 576 samples each. When audio samples are transformed, approximation and detailed coefficients are produced. Approximation coefficients contain the most significant features. In this case also it is possible to reconstruct the audio signal by considering only approximation coefficients.

1.5 Characteristics of steganography

Following characteristics are possessed by an effective steganography scheme:

- Secrecy: The hidden data in the host medium should not be extracted by any person without the knowledge of the proper secret key used in the extracting procedure.
- Imperceptibility: The medium should be indiscernible after being embedded with the hidden data from the original medium. One should not become suspicious of the existence of the secret information in cover object.
- High capacity: The maximum length of the convert message that can be embedded should be as long as possible.
- Resistance: The secret data should survive in case of host medium manipulation, for example by Some lossy compression schemes.

From the medium should be accurate and reliable.

2. LITERATURE REVIEW

It has been proved that hiding in frequency domain rather than time domain will give better results in terms of image quality.

In the 2011 Author M.I Khalil[1] 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 used LSB (least significant bits) for embedding secret data and gave the brief of audio steganography. In this a short audio message is embedded in the least significant bits of all bytes of a pixel. Hence, the maximum size of secret audio is 3*W*H, where W is the width and H is the height of the cover image. Since LSBs are used for embedding, possibility of losing data is more during compression, cropping, filtering etc.

In the 2012 Reddy, H.S.M Sathisha , N.Kumari

,A.Raja,K.B [2] worked on the steganography. They worked on Secure Steganography using hybrid domain technique(SSHDT). The cover image of different formats and sizes are considered and resized to dimensions of power of two. The Daubechies Lifting wavelet transforms (LWT) is applied on cover image to generate 4 sub-bands XA, XH, XV and XD. Out of all the 4 bands XD band is considered and divided into two equal blocks say upper and lower for payload embedding. The payload of different formats are taken and resized to dimensions of power of two. The payload is fragmented into 4 equal blocks. Further scrambling of the stego object is done to improve security to the payload using Decision Factor based manipulation (DFBM). Stego objects XA, XH, XV and XD are subjected to Dubechies Inverse LWT(ILWT) in order to obtain stego image in spatial domain. According to observations PSNR and embedding capacity of the proposed algorithm is better compared to the existing algorithm.

In the 2015 Della Baby[3] proposed a "Novel DWT based Image Securing method using Steganography". In their work new steganography technique is proposed in which multiple RGB images are embedded into single RGB image using DWT steganographic technique. The

Cover image is split into 3 colors i.e. red, green and blue color space. These three color spaces are utilized to hide secret information. Values of Peak Signal to Noise Ratio (PSNR) and Structural Similarity Index Matrix(SSIM) index values. Authors have found that their experimental results are better than the existing approaches and have increased embedding capacity because of data compression. So overall security of their approaches high with less perceptible changes in stego image. SSIM and Universal Image Quality Index(UIQI) are widely used method for measurement of image quality based on Human Visual System(HVS)[4,5].

YALMAN[6] proposed a full-reference Color Image Quality Measure(CQM), based on reversible YUV color transformation and PSNR meeasure. It is based on HVS. It is measured by the human eye's perception to luminance and chrominance. Using the CQM together with the traditional PSNR approach provides distinguishing results. To increase the hiding capacity Orthogonal Frequency Division Multiplexing (OFDM) approach is used but it requires original cover at the receiver. The payload and quality are low in extension to blind steganography.

To test the robustness of DWT based steganography algorithm**, Vijay Kumar[7]** evaluated the performance of stego-images by subjecting the stego images of 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 Kanso[8] tested their steganography algorithm against the existing steganalytic attacks like histogram test, RS attack, Chi square test, PSNR test, SSIM test etc. RS attack is used to detect stegos with LSB replacement and to estimate the size of hidden message.

In the 2012 Hemlatha S,U.Dinesh Acharya,Renuka A[9] proposed the wavelet based steganography technique to hide audio signals in image. In this the cover image is converted to YCbCr mode(YCbCr is a family of color spaces where 'Y' is the luma component and Cb, Cr are the blue-difference and red-difference chroma components. The approximate coefficients of the secret audio signal are hidden in the second and third planes of high frequency coefficients of the Cb and Cr.

3. METHODOLOGY

Embedding(At Sender's side)

1. Read the cover image C and secret audio S.
C=imread('C.jpg')

S=audioread('S.wav')

2. Represent C in YCbCr and obtain IWT of Cb components to get the four sub bands CLL, CLH, CHL and CHH.

LS=liftwave('haar','Int2Int')
[CLL,CHL,CLH,CHH]=lwt2(double(Cb),LS)

3. Obtain IWT of secret audio to get the approximation and detail coefficients.

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

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

{C1,C2}=IWTencode(CA,CHL,CHH)

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

5. Obtain inverse IWT to get stego Cb. Then convert to RGB

format. G=ilwt2(CLL,CHL,C1,C2,LS) G=ycbcr2rgb(YGCr) stegoimage=imwrite(G,'stego.jpg')

6. End Embedding.

Extraction(At Receiver's side)

1. Read stego image/signal G and represent it in YCbCr format.

G'=imread(G.jpg) YCb'Cr=rgb2ycbcr(G')

2. Obtain IWT of Cb to get four sub bands: GLL, GHL, GLH, GHH.

LS=liftwave('haar','Int2Int')
[GLL,GHL,GLH,GHH]=lwt2(double(Cb'),LS)

3. The encrypted secret audio bits are extracted from the second and third bit planes of GLH and GHH. Then decrypt it.

CAbin=IWTdecode(GHH,GHL)

In this method, two encrypted bits of the secret information are obtained from one byte(8 bits) of the stego image/signal coefficient. Then decryption is done as follows: the two encrypted bits are XORed with 4th

and 5th bits of the stego byte to get secret bits i.e., S1=S1' XOR b4 XOR b5 and S0=S0' XOR b4 XOR b5.

4. Convert to decimal to get approximation coefficient of secret audio.

CA=bin2dec(CAbin)

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

S=ilwt(CA,0,LS)

6. End Extracting.

4. EXPERIMENT/RESULTS

Fig-1: Cover image(image is in RGB format)

Fig-2: YCbCr image

Fig-3: Y component

Fig-4: Cb component

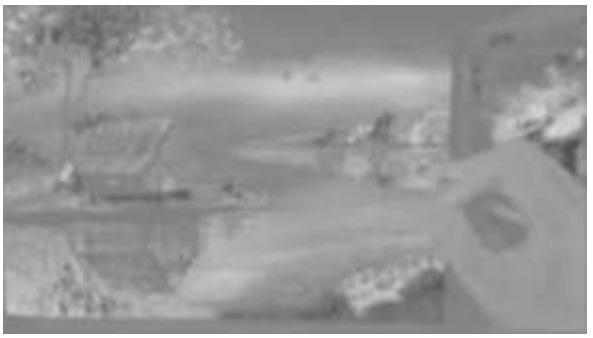

Fig-5: Cr component

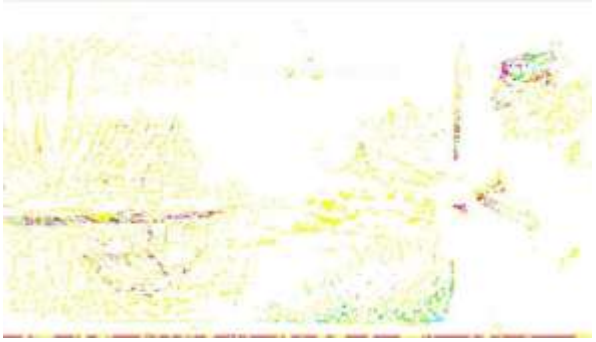

Fig-6: Modified Cb component

Fig-7: Stego image

5. QUALITY ANALYSIS

5.1 Peak Signal to Noise Ratio (PSNR)

The PSNR measures the peak signal-to-noise ratio, in decibels, between two images. This ratio is often used as a quality measurement between original and a compressed image. The higher the PSNR, the better would be the quality of the compressed, or restructured image.

5.2 Structural Similarity Index Metric(SSIM)

The Structural Similarity Index is a perceptual metric that computes image quality degradation caused by processing such as data compression or by losses in data transmission. It is a full reference metric that needs two images from the same image capture- a reference image and a processed image. It actually computes the perceptual difference between two similar images. It is based on visible structures in the image.

5.3 Signal to Noise Ratio (SNR)

SNR is a measure that compares the level of a required signal to the level of background noise. It is defined as the ratio of signal power to the noise power, it is often expressed in decibels. A higher ratio indicates more signal than noise.

5.4 Squared Pearson Correlation Coefficient (SPCC)

SPCC computes the similarity level between two signals. The SPCC is directly proportional to the similarity level. Its range is between 0 and 1.

6. CONCLUSION

In this paper a secure, robust and high capacity image steganography technique is proposed. It 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 experimental results show the secret audio can be extracted without much distortion in most of the cases.

6.1 Limitations:

The proposed technique needs to be tested against other attacks like histogram equalization, cropping, occlusion, translation etc. It involves complicated computations.

6.2 Applications:

- **Intelligent Services**
- **Defence Services**
- **Banking Services**

7. REFERENCES

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

[2]Reddy, N.Kumari, H.S.M Sathisha A.Raja, K.B, "Secure steganography employing hybrid domain technique", Computing Communication & Networking Technologies(ICCCNT), 2012 Third International Conference on vol 1, no.11, pp 26-28

[3]D.Baby,J. Thomas, G. Augustine, E. George, N.R. Michael, "A Novel DWT based Image Securing method using Steganography", International Conference on Information and Communication Technologies (ICICT), Procedia Computer Science, April 2015, pp. 612-618.

[4]Diqun Yan, Rangding Wang, Xianmin Yu, Jie Zhu. Steganography for MP3 audio by utilizing 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 : Error Visibility is changed to Structure Similarity. IEEE Transactions are done on image processing, Vol.13, No.4, 2004, pp. 600-612.

[6]Yildiray YALMAN, Dsmail ERTURK. YUV transformation and PSNR for human vision system on which new color image quality measure is based, 2011 pp.1-18

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

[8]Ali kanso, Hala S.Own. Steganographic algorithm based on chaotic map. Numerical Simulation of Communication Nonlinear Science , 17, 2012, pp 3287-3302

[9]Hemalatha S, U. Dinesh Acharya, Renuka A, "Wavelet transform based steganography technique to hide audio signals in image", Procedia computer science 47, 2015, pp272-281.