iJRASET
International Journal For Research in Applied Science and Engineering Technology

# INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

**Volume:** 9 **Issue:** VI **Month of publication:** June 2021

**DOI:** https://doi.org/10.22214/ijraset.2021.35105

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
*ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.429*
*Volume 9 Issue VI Jun 2021- Available at www.ijraset.com*

# Wavelet Transform based Steganography

Nikhil Jain[1], Prateek Kumar[2], Pratham Shiwal[3], Shubham Jain[4], Deepak Aneja[5]
[1,2,3,4] *Student,* [5]Assistant Professor, *Dept. of Computer Science & Engineering, Krishna Engineering College, U.P., India*

***Abstract:*** ***Steganography is a technique which is used to hide audio signal behind an image in the transform domain using wavelet transform. The audio signal can be of any type, any format like MP3 or WAV or any other type is encrypted and hide behind an image without disclosing even the existence of audio signal to anyone. It gives the best way to send an audio signal by hiding the secret data.***
***Keywords:*** ***Steganography, transform, wavelet transform.***

## I. INTRODUCTION

Steganography is a word which is derived from two greek words Steganos(covered) and Graptos (Writing) which means 'covered writing' means hide data and information into plain sight. Now-a-days, everyone is sharing data and information with each other. The development in data sharing with their increased use, the data security issue became an essential step. For data security, different methods available such as Steganography, cryptography etc. Steganography is a way of hiding data and information through this, so that a person is not able to know whether hidden information is there or not. The hidden data are not visible directly whereas cryptography is the way of protecting the data, the message in cryptography is in an encrypted form, and there is encryption key which is shared between authorized persons. in cryptography there is nothing like hiding up of data it's just a way of protecting the data.

### *A. Steganographic Techniques*

There are two types of steganography techniques available temporal domain and transform domain. The secret information is hidden by manipulating actual sample values in temporal domain. The cover object is converted to different domain such as frequency domain to get transformed coefficients in transform domain. These coefficients are manipulated to hide secret information. The transforms that can be used: Fast Fourier Transform (FFT), Discrete Cosine Transform (DCT), and Discrete Wavelet Transform (DWT). The disadvantage of FFT is that it does not provide information about its timings, it only gives frequency information. DCT have artifact problems. In our project, DWT is used because frequency content of a function f(t) is given as a function of time by wavelet transform.

### *B. Steganographic Medium*

There are many Steganography techniques available relying on the kind of item to be protected in a way to achieve security.

1) *Image Steganography:* To hide the information use of pixel intensities is done, if the cover object taken is image then it is known as image steganography.
2) *Video Steganography:* In this technique for hiding information in images in the video the discrete cosine transform (DCT) adjusts the value which is not conspicuous through human eye. Mp4, AVI, etc video formats are used by video steganography.
3) *Audio Steganography:* In this technique audio is chosen for information hiding, that's why it is called Audio Steganography. WAVE, MPEG, etc. digital audio formats are used in audio steganography.
4) *Network Steganography:* In this technique the cover object chosen is as network protocol, such as UDP, ICMP etc and these protocols are used as carrier.
5) *Text Steganography:* In this technique, for information hiding, capital letters, white spaces, number of tabs and many others are used.

### *C. Steganographic Standard*

1) *Secured:* When there is invisible difference between cover image and steganographic image, a steganographic system is said to be secured.
2) *Cost effective:* Two parameters used for cost effectiveness are data hiding and data retrieval of any steganography approach.
3) *Analytical Attacks:* These are the attacks in which the embedded secret messages are extracted. The algorithm which is used must show robustness to analytical attacks.
4) *Quality:* An appropriate amount of data and a valid approach should be done in order to not degrade the quality of data as Increment in data amount decreases the quality,
5) *Indistinct:* When the cover image and the steganographic image are not distinguished by human eye, then it can be indistinguishable and perfect.

©IJRASET: All Rights are Reserved

6) *Loading Capacity:* It can be defined as the amount of hidden information that the cover image can implant in it. The rate of implantation is given in complete amount like the secret message length.

*D. Steganographic Terminologies*

1) *Cover Image:* Real image acting as a carrier for the hidden file.
2) *Steganographic Image:* embedded information inside the cover image is steganographic image.
3) *Message:* The information which is actually hidden into images, it can be a image or a plain text.
4) *Steganographic key:* For getting the message from steganographic image, steganographic key is used.
5) *Implanting Algorithm:* For hiding the information inside the image, an algorithm is used known as implanting algorithm.
6) *Detaching Algorithm:* For getting the information from steganographic image, an algorithm is used known as detaching algorithm.

*E. Discrete Wavelet Transform (DWT)*

In Discrete wavelet transform, mother wavelet is selected, mother wavelet can be defined as a function that is not zero in some small interval and it is used to know the properties of the function f (t) in that interval. Then the mother wavelet is translated to another interval of time and used in the same way. So, by using wavelet, sharp discontinuities can become approximated and they also provide time-frequency representation of the signal. There are many types of wavelets which can be used for this purpose. The simplest wavelet is the Haar Wavelet among all the wavelets. In real-life situations, the Information that analyzed is discrete. Rather than a continuous function, we get information in form of number. That's why discrete one is used in practice. When the input data consists of sequences of integers as in images, the wavelet transforms which map integers to integers can be used. Integer Wavelet Transform (IWT) is one of another approach.

## II. LITERATURE SURVEY

Frequency domain hiding gives better result than time domain when we talk about image quality. As human eye is minor changes in luminance but not that sensitive in terms of chrominance. One of its representations is YCbCr,
Where, Y:- is the luminance
Cb and Cr:- are the chrominance components.
The modification in chrominance part that is Cb and Cr can be done very easily without affecting the overall image quality visually. Author M.I Khalil suggested a way for how to conceal small audio in the cover image data without affecting the quality of image very much. From the available embedding method, he used least significant bits (LSB) for embedding private data and gave the short description of audio steganography. In this a small audio message is embedded in the least significant bits of all bytes of a pixel. The maximum size of secret audio is given by 3*W*H, where W is width, H is the height of cover image. As LSBs are used for embedding, during compression, cropping, filtering, the possibility of losing data is high.

*MSE and PSNR*

MSE stands for mean-square error and PSNR stands for peak signal-to-noise ratio, they are used to compare image compression quality. It is not right to judge the quality of an image on the basis of MSE and PSNR.

*SSIM and UIQI*

SSIM and UIQI used to measure the similarity between two images and Universal Image Quality. Yalman gave a full-reference Color Image Quality Measure (CQM), based on reversible YUV color transformation and PSNR measure. Orthogonal Frequency Division Multiplexing (OFDM) approach is used for increasing hiding capacity but it requires original cover at the receiver. In extension to blind steganography, the payload and quality are low. Luminance and chrominance are measured by eye's perception. By using the CQM together, the traditional PSNR approach provides distinguishing results.

## III. METHODOLOGY

*A. Embedding (At Sender's side)*

1) First step to read the cover image 'C' and secret audio 'S'.
   C=imread('C.jpg'), S = audioread('S.wav')
2) Represent C in YCbCr and then obtain IWT of Cb components to get 4 sub bands (CLL, CLH, CHL and CHH).
   LS=liftwave('haar','Int2Int')
   [CLL,CHL,CLH,CHH]=lwt2(double(Cb),LS)
3) To get the approximation and detail coefficients, obtain IWT of secret audio.
   [CA, CD]=lwt(double(S),LS)

©IJRASET: All Rights are Reserved

*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 one byte of the cover image hides two bits of the secret message. To get encrypted secret bits, two bits from the secret message are XORed with 4th and 5th bits of the cover byte.
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.

*B. Extraction (At Receiver's side)*

*1)* Firstly read the stego image G and represent in YCbCr format.
G'=imread(G.jpg)
YCb'Cr=rgb2ycbcr(G')

*2)* To get the 4 sub bands, obtain IWT of Cb:
GLL, GHL, GLH, GHH.
LS=liftwave('haar','Int2Int')
[GLL,GHL,GLH,GHH]=lwt2(double('Cb'),LS)

*3)* The second and third bit planes of GLH and GHH are used to extract the encrypted secret audio bits. Decrypt it.
CAbin=IWTdecode(GHH,GHL)
In this method, From one byte (8 bits) of the stego image/signal coefficient, two encrypted bits of the secret information are obtained. Then decryption is done as follows:
the two encrypted bits are XORed with 4tand 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)* To get approximation coefficient of secret audio, convert to decimal.
CA=bin2dec(CAbin).

*5)* In step 4, obtain inverse IWT for approximation coefficient and consider zeroes for detailed coefficients. The result is this secret audio. S=ilwt(CA,0,LS)

*6)* End Extracting.

## IV. EXPERIMENT RESULTS

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

©IJRASET: All Rights are Reserved

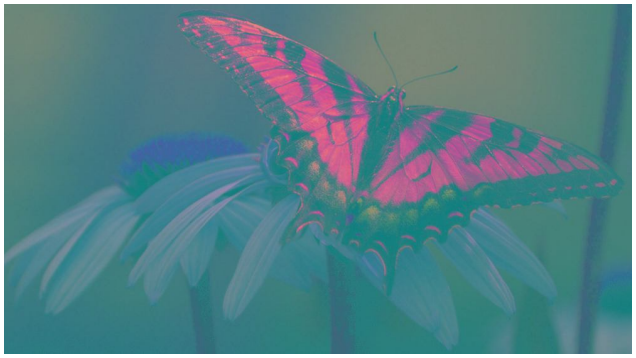


Fig-2: YCbCr image

Fig-3: Y component

Fig-4: Cb component

Fig-5: Cr component

©IJRASET: All Rights are Reserved

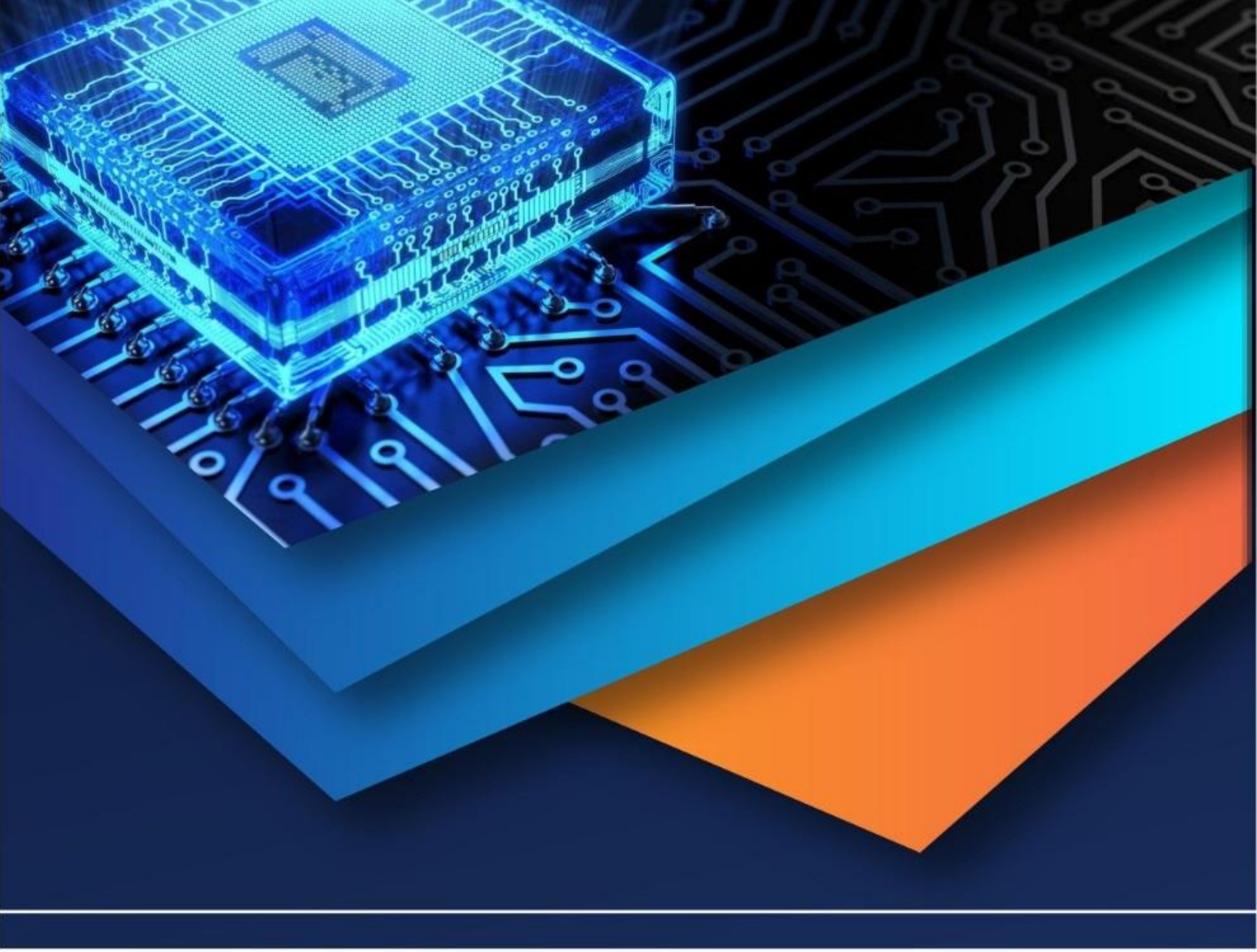
## V. CONCLUSIONS

In this paper, a technique is used to send the audio signal behind an image by hiding the audio signal. It gives the best way to send an audio signal by hiding the existence. The technique needs to be tested against attacks such as histogram equalization, cropping, occlusion, translation etc. The experimental results shows that we can extract the secret audio without much distortion in most of the cases.

## REFERENCES

[1] 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.
[2] International Journal of Engineering and Advanced Technology (IJEAT) ISSN: 2249 – 8958, Volume-9 Issue-4, April, 2020.
[3] Information Hiding in Images Using Steganography Techniques Issue-3, March,2013.
[4] International Journal of Innovative Research in Electrical, Electronics, Instrumentation and Control Engineering nCORETech LBS College of Engineering, Kasaragod Vol. 3, Special Issue 1, February 2016.
[5] M. I. Khalil. Image steganography: Hiding short messages within digital images. JCS&T, steganography using hybrid domain technique," Computing Communication & Networking Vol.11, No. 2. pp 68-73.
[6] Reddy, H.S.M.; Sathisha, N.; Kumari, A.; Raja, K.B., "Secure Technologies (ICCCNT), 2012 Third International Conference on , vol., no., pp.1,11, 26-28 July 2012.
[7] 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.
[8] 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.
[9] 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.
[10] Yıldıray YALMAN, Đsmail ERTÜRK. A new color image quality measure based on YUV transformation and PSNR for human vision system, 2011. pp 1-18.
[11] Vijay Kumar and Dinesh Kumar. Performance Evaluation of DWT based Steganography. IEEE 2nd International Advance Computing Conference, 2010. pp 223-228.
[12] Ali Kanso, Hala S. Own. Steganographic algorithm based on a chaotic map. Communication Nonlinear Science Numerical Simulation, 17, 2012. pp 3287–3302.
[13] Thenmozhi, S.; Chandrasekaran, M., "Novel approach for image steganography based on integer wavelet transform," Computational Intelligence & Computing Research (ICCIC), 2012 IEEE International Conference on , vol., no., pp.1,5, 18-20 Dec. 2012.

©IJRASET: All Rights are Reserved



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

# INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)