A Review on "Image Steganography with LSB & DWT Techniques"

Neha[1*], Mohit[2]

[1]Dept. of Computer Science, Guru Jambheshwar University Hisar, India
Dept. of Computer Science and Engineering
[2]Dept. of Science and Technology, Guru Jambheshwar University Hisar, India
Dept. of Computer Science and Engineering

[*]*Corresponding Author: nehagill9454@gmail.com*

Abstract– In all the fields of steganography such as image, text, audio, video there are many techniques used to transfer the secret messages without known to other person. Using the Steganography technique to hide the data or message in an image,LSB and DWT are two easy techniques which are usefull and implemented easily to improve robustness and performance of algorithms. LSB method used to transfer the large data and replace some information in pixel with information from the data in image. Overall use of LSB doesn't affect the representation of image. In this technique, LSB method will be used to transfer the large data and replace some information in pixel with information from the data in an image.DWT method is used to embed converted data into cover medium to conceal its presence. For the security, we will use the technique DWT which is used with the low frequency (used for narrow bandwidths) and high frequencies (for wider bandwidths) and for the flexibility.

Keywords – Steganography, Least-significant-bit (LSB), Discrete Wavelet Transform(DWT)

I. INTRODUCTION

The Steganography was launched in 1499 by Johannes Trithemiu[1]. It's a combination of two words Stegano + Graptie. Stegano means "Covered" and Graptie means "Writing" which means "cover writing". The technique of hiding secret data in any object which doesn't come in notice by hackers. The concept of Steganography is the secret message send is not noticed by human eye. The sender fix message into text, image, video, audio file by which hackers will not found the message. This technique is not discovered recently, it's very advanced in years[3]. The Steganographic methods used by secret agents contain invisible ink and microdots. Agents used wooden tablets and covered with wax to design secret messages. People used tattoos on shaved head, then their hair grow again and save the message further when they reach to receiver to reveal the message they use to shave their head again. The goal of steganography, save and keep out secret messages. In the method of steganography[14] we need a medium or image in which we can hide the information called as the carrier. The secret message is hidden in the carrier to make the steganography image or medium. Steganography key helps in encoding or extraction of information in the image. In short:

Steganography image/ medium =steganography key + hidden message + carrier

Fields of Steganography technique
There are many fields in which steganography techniques are used for hiding data [1][8]. Some fields are as following:
Text Steganography: This successfully reach by changing in characters or text format[8].
Image Steganography: Used as the message carriers. Images called cover objects used for steganography.[1]

Audio Steganography: In this, secret message changed into digitized audio signal. The techniques used in this are phase coding, echo hiding, phase coding.[1]
Video Steganography: In this, the secret data is hidden in video file format. This use many video compression techniques as intra-inter frame predication, transformed coefficient, motion vectors etc.[1]
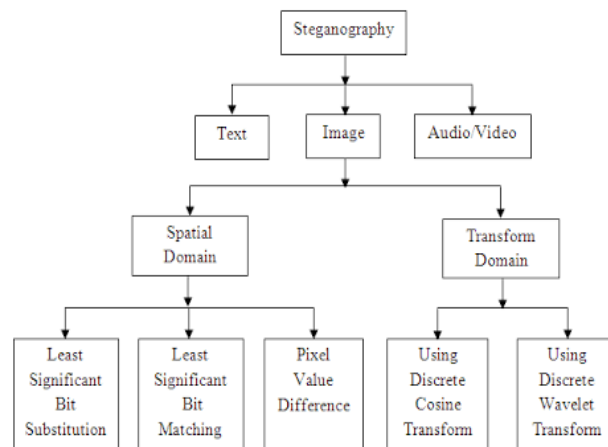

Fig 1. Categorization of Steganography [11]

II. TECHNIQUES USED IN IMAGE STEGANOGRAPHY

There are many techniques which are used to send information by images. On the bases of survey image steganography can estimated using techniques such as:

LEAST SIGNIFICANT BIT (LSB)

In LSB [8],[11], least bits of cover up image information are worn for hiding communication. In LSB steganography techniques data bit is changed or replaced with least significant bit of image. LSB substitute steganography use last bit of informationstandards to hide communication.

In this technique[2], the image is converted into grayscale image. For hiding the text, the image act as reference image. By using the reference image of grayscale the data use to be hidden. Character of data is represented with 8-bits. When reference image and data files are transmitted together we get steganography effects. The image used as the reference so the image is not all distorted. Vast data kept out using usual image. Because of unthreatened, identifying text not possible to catch image or data file differently. Technique works best when file is larger then message file and in grayscale.

DISCRETE WAVELET TRANSFORMATION(DWT)

DWT worn to convert a indicationcommencing spatial to frequency area and vice versa[11]. Wavelets are positions of waves that decomposed quickly. There are many applications that performed in many fields such as speech recognition, smoothing, fingerprint verification, signal dispensation, data compress, representation de-noising. Wavelet transform applied to steganography technique for increasing capacity and robustness. It's easy to perform and decrease computer time and tools requirements.

The DWT[5], used the proposed steganography technique. It is the simplest transform in wavelet mathematics, because it uses square pulses to approximate the original function. It is used to exchangeenveloprepresentationaddicted to four sub-bands which estimate, vertical, horizontal and diagonal coefficients, which symbolize low-low, high-low, low-high and high-high frequencies, correspondingly. Estimateconstantsresolve not be wornedhideundisclosed data, as individual eyes are extremelyperceptive to undersizedchange in low-low frequency[10]. Though,respite of coefficients hold high frequencies, thereforeundisclosedinformation will be correct and coveredinside these groups by exploitation of both least significant bit and virtualindiscriminatemagnitude of methods. Inverse of DWT performed when hiding process is completed to make stego image.
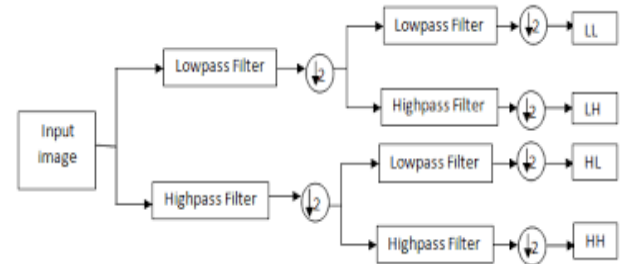

Fig 2. One level DWT

III. LITERATURE REVIEW

In this section, we proposed the reviews and work done by many researchers which done work on the bases of steganography using many techniques.

Er. MunishKatoch et al. [1], proposed Steganography and work of Image Steganography with many insertion techniques. It's deals with Steganography Software and Applications. This research implement two techniques (a) Steganography (b) Cryptography for kept out imparting information and deals with security and privacy.

K.Dhinesh et al. [2], proposed improved LSB method basedsteganography is used for hiding secret information or message. The process has improvedunremarkable and consignmentcapability than accessible steganography methods. The strength of communicationentrenched inprotectionpurpose is enhanced, that's displaytechnique is very operative. The image not reform in hugequantity and value at implantingcommunicationaddicted to image and communication is threatened with the private key. When the stegano picture is exaggerated by noise in communication network and stenographicaloccurrences and similarly not conceivable to terminate the concealdispatchentrenched in cover object therefore this process is very operative and assumedimprovedoutcomes.

In May 2015, L.Baby Victoria[3], many research papers used spatial area and transform field for representationthrashingplaced in group. The steganographic techniques principles guides to improve its applications in new areas.

In February 2016, Sukhjinder Singh et al. [4], In this paper, a steganographic method for data hiding with the help of quantized tange table and local area pixel. This improves two features of digital steganography methods which are (a) steganographic capability and (b) stego image significance. The research recommended in demand to rise the steganographic ability and stego image superiority.

In April 2016, S. Thenmozhi et al. [5], this paper proposed a novel image steganography method to make greater size of secret information. Proposed method had accomplished amount of image data hiding without any attracting state of

being distroted on cover image with image quality pick up to Infinity. This approach had reached the noiselessness besides protecting the quality of image to human eyes. The PSNR, MSE had been used to measure the image quality. This method is showing better performance against the first order steganalysis histogram measurement.

In March 2016, Mamta Jain et al. [6], proposed to recoverprobability of detecting outflow and identifyresponsiblegathering "realistic but fake" data recordsinject. We use envelop image headed for fix undisclosedcommunication using steganography techniques. The steganography is valuable when one require to transmit a confidentialtext with the help of Internet. With embedding the unseen data interested in the envelopsignificance unnoticed, we have sent more than a harmless message. Steganography at phase of improvement which allowuser to concealrecords of outsized area and as wellconservemanifestation of information by any enveloprepresentationworn. The original image and final embedded image noticed by human being.

In 2016, S. Krishnan et al. [7], attaching information in audio seems secure because of less steganalysis techniques for hacking to audio. Main reasons are complication sensitivity and difficulty. There are not much algorithms and techniques present for image. It has been limited to some restrictions.

In February 2016, Ms. Kajal Prakash kamble et al. [8], it proposed that Steganography used for secret communication with others. We used LSB and RGB techniques on images to get safe stego-image. Results shows for lossless compression it's better to use RGB as secret key. The image doesn't differ much and unnoticeable when fix message in image and image is prevented by using personal key. So, unauthorized person cannot damage the data in image. It is also more difficult to identify by hackers when compared with LSB method. Hence it is more advantageous over the LSB method for use of steganography.

In February 2016, Komal Kapoor [9], deliberated for resolution of safety and verification in internet electivescheme, capable steganographic performance has been accessible inbroadsheet. The suggestedtechnique is recycled for smacking the impression image of a constituent in his makeover image.

Ashley S.Kelsey et al. [10], in this, method negligible for quality effect in image, making it rigid for secret listener to find existence of hidden message in image. The converting process of information security layer make difficult for eavesdroppers to find information. Methods make better overall security, capacity of hiding data, imperceptibility, quality or condition of image, create secure and organized steganographic methods.

In January – March 2016, Deepak Garg et al. [11], discussed the network security become usefull as large data exchanged on Internet. Steganography has ability and follow rules for hiding messages in a way that only the sender and receiver have the idea of pressence of the message.

In June 2016, Mohit [21], discussed about the security of data transformation over network transmission. Using LSB substitution embeds the hidden data in master image without detectable by anyone. The data hidden capacity depends on pixels of master image.

S.No	Title	Author	Proposed Work	Advantages	Disadvantages
1.	Image Steganography: A Review	Er. MunishKatoch and ReenuJaswal	To combine steganography and cryptography technique	High level security and privacy	Limited embedding capacity,Higher time complexity
2.	An Improved LSB Based Steganography Technique for Grayscale and Color Images	K.Dhinesh, K.Meenachi, A.Selvabharathi, S.Senthamilselvan	Use of LSB for grayscale and color image	Payload capacity and robustness	Higher time complexity
3.	A Study on Spatil Domain and Transform Domain Steganography Techniques used in Image Hiding	L.Baby Victoria	Use of spatial domain and transform domain	protection and time less transmission	Limited embedding capacity, no robust
4.	A Robust Image Steganography Technique using Quantized Range Table and Local Area Pixel Value Differencing	Sukhjinder Singh, KulbhushanSingla, Dr. Rahul Malhohtra	using Quantized VarietyStand and NativePart Pixel Significance	Better image quantity and capacity	No robust and lower PSNR value
5.	Multilayered, High Capacity,	S. Thenmozhi,	Using DWT and	Robustness,	Higher time

	Distortionless Image Steganogaphy using ANN	M.Chandrasekaran,	back propagation Neural Network	security and high capacity payload	complexity
6.	A Review on Data Leakage Prevention using Image Steganography	Mamta Jain and Saroj Kumar Lenka	Using cryptography with LSB	Prevention	Limited embedding capacity,Higher time complexity
7.	A Discrete Wavelet Transform Approach for Enhanced Security in Image Steganography	Ashley S.Kelsey, CajetanM.Akujuobi	Using cryptography with DWT	Hiding capacity, imperceptibility, robustness & security	Higher time complexity
8.	An Enhanced Least Significant Bit Steganography Technique	Mr. Mohit	To use LSB Technique on BMP images	Robustness, Image quality and capacity	Lower PSNR value
9.	An Implementation of LSB Steganography Using DWT Technique	G. Raj Kumar, M. MaruthiPrasada Reddy, T. Lalith Kumar	To combine LSB and DWT in FPGA	Analyse & manipulate LSB	Limited embedding capacity,Higher time complexity
10.	Color Image Steganography Using Discrete Wavelet Transformation and Optimized Message Distribution Method	Juned Ahmed Mazumder, KattamanchiHema chandran	Using DWT and Optimized message distribution method	High capacity and imperceptibility	No robustness and lower PSNR value
11.	A Review on Steganography-Least Significant Bit Algorithm and Discrete Wavelet Transform Algorithm	Vanitha T, Anjalin D Souza, Rashmi B, Sweeta Dsouza	Using DWT and LSB technique	High security and better quality image	Higher time complexity and no robust
12.	DWT and LSB algorithm based Image Hiding in a Video	M Abhilash Reddy, P. Sanjeeva Reddy, GS Naveen Kumar	Using LSB & DWT in video	High data security	Higher time complexity
13.	FPGA Implementation of Image Steganography Using LSB & DWT	KalpanaShete, MangalPatil, J.S. Morbale	Using LSB & DWT in implementation FPGA	Higher PSNR value	No quality and no robust
14.	Least Significant Bit and Discrete Wavelet Transform Algorithm Realization for Image Steganography Employing FPGA	Kalpana Sanjay Shete, MangalPatil and J.S. Chitoda	LSB & DWT together employing FPGA	Robustness and security	Higher time complexity and low capacity
15.	A Review of Comparison Techniques of Image Steganography	StutiGoel, ArunRana&Manpreet Kaur	To combine DWT & DCT & LSB	Robustness and higher PSNR value	Limited embedding capacity,Higher time complexity
16.	Dual Steganography Technique Using Status LSB and DWT Algorithms	Manisha and DeepkiranMunjal	Using DWT, cryptography, dual steganography	High security, capacity, high PSNR value, robustness	Higher time complexity

Table 1- shows different literature survey image steganography techniques introduced by different researcher

IV. CONCLUSION

In this paper various image steganography techniques were studied. From the literature reviews and survey, we discovered or say found that LSB and DWT techniques are widely used in image steganography. Both the techniques have their own advantages to be used in the data transformation secretly. Using LSB technique, the image is converted into grayscale image. For hiding the text, the image act as reference image. By using the reference image of grayscale the data use to be hidden. When reference image and data files are transmitted together we

get steganography effects and get the similar sized image as pixels values were rearranged by sliding over each other quickly. Using DWT technique, the image composition is changed due to the decomposed given data to obtain uncorrelated data. This influence the whole image and reorganized image is insignificant in size. DWT technique is used for increasing capacity and robustness. It's easy to perform and decrease computer time and tools requirements.

REFERENCES

[1]Er. MunishKatoch and ReenuJaswal, " Image Steganography: A Review," International Journal of Advanced Research in Computer and Communication Engineering, Vol. 5, Issue 4, April 2016.

[2]K.Dhinesh, K.Meenachi, A.Selvabharathi, S.Senthamilselvan, "An ImprovedLSB Based Steganography Technique for Grayscale and Color Images," International Journal of Advanced Research in Electronic and Communication Engineering, Vol. 5, Issue 4, April 2016.

[3]L.Baby Victoria, "A Study on Spatil Domain and Transform Domain Steganography Techniques used in Image Hiding," International Journal of Innovative Technology and Creative Engineering, Vol.5 No.5 May 2015.

[4]Sukhjinder Singh, KulbhushanSingla, Dr. Rahul Malhohtra, "A Robust Image Steganography Technique using Quantized Range Table and Local Area Pixel Value Differencing," International Journal of Advanced Research in Electronic and Communication Engineering, Vol. 5, Issue 2, February 2016.

[5]S.Thenmozhi, M.Chandrasekaran, "Multilayered, High Capacity, Distortionless Image Steganogaphy using ANN," South Asian Journal and Technology, Vol.2,No.21 pp.63- 73, 2016.

[6]Mamta Jain and Saroj Kumar Lenka, "A Review on Data Leakage Prevention using Image Steganography," Mamta Jain et al./ International Journal of Computer Science Engineering, Vol.5, No.002, Mar 2016.

[7]S.Krishnan, M.S. Abdullah, "Enhanced Security Audio Steganography by Using Higher Least Significant Bit," Journal of Advanced Research in Computing and Applications ISSN(ONLINE), Vol.2,No.1.pp.39-54, 2016.

[8]Ms.Kajal Prakash kamble, Ms SwapnaliVasantKhabale, Mr. AnkushShahu Morale, "An Infallible Method to Transfer Confidential Data using Delta Steganography,"International Research Journal of Engineering and Technology, Vol.03, Issue:02, Feb-2016.

[9]Komal Kapoor, "Digital Image Steganography based Security Model using Wavelet for Internet Voting Environment," International Journal of Advanced Research in Electronics and Communication Engineering, Volume 5, Issue 2, February 2016.

[10] Ashley S.Kelsey, CajetanM.Akujuobi, " A Discrete Wavelet Transform Approach for Enhanced Security in Image Steganography," International Journal of Cyber-Security and Digital Forensics(IJCSDF) 5(1):10-20,The Society of Digital Information and Wireless Communications, 2016 (ISSN:2305-0012).

[11]DeepakGarg, Gourav Sharma, "Applications of Steganography in Information Hiding," International Journal of Advanced Research in Education Technology, Vol.3, Issue 1, Jan-Mar. 2016.

[12]MsVedantiM.Khandare, Dr. SiddharthA.Ladhake,Mr.U.S.Ghate, "An Approach of ECG Steganography to Secure the Patient's Confidential Information," International Research Journal of Engineering and Technology, Volume: 03, Issue: 03| Mar-2016.

[13]Sumanth C, Dr. M B Meenavathi, "Audio-Video Steganography using Face Recognition Technique for Authentication," International Journal of Advanced Research in Electronics and Communication Engineering, Volume 5, Issue 5, May 2016.

[14] Md. Mizanur Rahman, Pronab Kumar Mondal, Indrani Mandal, Habiba Sultana, "Secure RGB Image Steganography Based on Triple-A Algorithm and Pixel Intensisty," International Journal of Scientific & Engineering Research, Volume 7, Issue 3, March- 2016.

[15]Seema S. Girare, Malvika U. Saraf, "Literature Review on Different Watermarking & Steganography Technique," International Research Journal of Engineering and Technology, Volume: 03, Issue: 04| Apr-2016.

[16] Don Caeiro and Sanjana S, "Detection of Steganography Using Metadata in JPEG Files," The International Journal of FORENSIC COMPUTER SCIENCE(www.IJoFCS.org),2015.

[17]SaurabhPaliwal, " A Surve& Applications of Various Image Steganography Techniques," International Journal of Scientific & Engineering Research, Volume 7, Issue 1, January-2016.

[18]RiyadhBassilAbduljabbar, " Steganography System using Slantlet Transform," Journal of Information, Communication, and Intelligence Systems(JICIS), Volume 2, Issue 1, February2016.

[19]Hamad A. Al- Korbi, Ali Al- Ataby, Majid A.Al-Taee and Waleed Al-Nuaimy, " Highly Efficient Image Steganography Using Haar DWT for Hiding Miscellaneous Data," Jordanian Journal of Computers and Information Technology (JJCIT), Vol.2,No. 1,April 2016.

[20] Mamta Jain and Saroj Kumar Lenka, " A Review of Digital Image Steganography Using LSB and LSB Array," International Journal of Applied Engineering Research ISSN 0973-4562 Volume 11, Number 3(2016).

[21] Mr. Mohit "An Enhanced Least Significant Bit Steganography Technique," International Journal of Advanced Research in Computer Engineering & Technology(IJARCET) Volume 5, Issue 6, June 2016.

[22]G. Raj Kumar, M. MaruthiPrasada Reddy, T. LalithKumar,"An Implementation of LSB Steganography Using DWT Technique," International Journal of Engineering Research and General Science Volume 2, Issue 6, October-November,2014.

[23]Juned Ahmed Mazumder, KattamanchiHemachandran, "Color Image Steganography Using Discrete Wavelet Transformation and Optimized Message Distribution Method," International Journal of Computer Sciences and Engineering, Volume-2, Issue-7, July 2014.

[24]Vanitha T, Anjalin D Souza, Rashmi B, SweetaDSouza, " A Review on Steganography- Least Significant Bit Algorithm and Discrete Wavelet Transform Algorithm," International Journal of Innovative Research in Computer and Communication Engineering Vol.2, Special Issue 5, October 2014.

[25]M Abhilash Reddy, P. Sanjeeva Reddy, GS Naveen Kumar, "DWT AND LSB ALGORITHM BASED IMAGE HIDING IN A VIDEO," International Journal of Engineering Science & Advanced Technology Volume-3, Issue-4, Aug-Sep 2013.

[26]KalpanaShete, MangalPatil, J.S. Morbale "FPGA Implementation of Image Steganography Using LSB & DWT," International Journal of Computer Science and Network, Volume 4, Issue 6, December 2015.

[27] Kalpana Sanjay Shete, MangalPatil and J.S. Chitoda, "Least Significant Bit and Discrete Wavelet Transform Algorithm Realization for Image Steganography Employing FPGA," I. J. Image, Graphics and Signal Processing Vol.6, June 2016.

[28]StutiGoel, ArunRana&Manpreet Kaur, " A Review of Comparison Techniques of Image Steganography," Global

Journal of Computer Science & Technology Graphics & VisionVolume-13, Issue-4 Version 1.0, 2013.

[29]Manisha and DeepkiranMunjal, "Dual Steganography Technique Using Status LSB and DWT Algorithms," International Journal of Innovative Research in Computer and Communication Engineering, Volume 4, Issue 6, June 2016.

Authors Profile

Neha pursed Master in Computer Application from GJUS&T University Hisar in 2016.She is currently pursuing M-Tech in the Computer Science & Engineering Department from GJUS&T University, Hisar (Haryana), India. My research interested areas are Image processing, and Data security in image steganography.

Mr. Mohit (Co-Author) pursed Master of Technology from Guru Jambheshwer University Hisar, India in 2014. He is currently pursuing Ph.D. and currently working as Assistant Professor in Department of Computer Sciences Engineering, Hisar India. His main research work focuses on Image Processing and Data Security. He is regular researcher in the field of security in steganography and Image Processing.