Suresh GyanVihar University, Jaipur
International Journal of Converging Technologies and Management (IJCTM)
Volume 4, Issue 1, 2018
ISSN: 2455 - 7528

# Improved Approaches for Steganography Using Noise Attacks

Abhinav Agarwal, Nirupama Tiwari
Dept. of (CSE/IT)), S.R.C.E.M College, Gwalior (India)
Abhinavkiot2410@gmail.com, girishniru@gmail.com

***Abstract*— Steganography alludes to the strategy of obnubilating secret messages into media, for example, content, sound, picture and video with no doubt, while steganalysis is the art and science of apperception of the propinquity of steganography. It can be utilized for the advantage of the humanity to accommodate us and in additament by psychological oppressors and offenders for malevolent purposes. Both steganography and steganalysis have gotten a plethora of mentally conceived from law execution and media. Afore, sundry steganographic methods with properties of intangibility, imperceptibility, power and constrain have been proposed. More au courant and more intricate steganographic strategies for implanting mystery message will require all the more excruciating steganalysis techniques for location. Calculate PSNR and BPP**

***Keywords*— *image steganogrphy; DCT block compression;LSB***

**. I. Introduction**

In today's world the data communication is the fundamental desideratum of every growing area. Each and every person wants a robust, secure and high capacity steganography technique for maintaining secrecy and safety of their communicating data. The organizations such as internet banking, e-commerce, diplomacy and medicine, private communications are essential. In this manner it has expanded the desideratum of putting away an abundance of information and their security.

"Steganography" is a Greek word which denotes "hiding inditing ". Steganography word is the coalescence of two sections: Steganos which betokens "secret" and Graphic which denotes "composing". Steganography is defined as the process of obnubilating sensitive information on any multimedia cover like image, audio, video and protocol etc in a such way that unauthorized person can't be apperceived the subsisting of sensitive information in to the cover media. The information that to be covered up is called Stego and the cover media in which information to be covered up is called has. The primary distinctive between in cryptography and steganography is, cryptography ascertain the substance of the message while steganography conceals the way that a secrate message is being sent and additionally to shroud the substance of the message. [1]

In this incipient form of double steganography utilizes steganography inside steganography. In this secret data is embedded in cover image utilizing the status LSB (Least Consequential Bits) embedding algorithm and engender a stego-image .Next stego-image is considered as a secret data and embedded in other cover image utilizing the DCT (Discrete Cosine Transforms) embedding algorithm which is engendered a final stego –image. A dual steganography amalgamated with two algorithms will be a potent and efficient implement for data security.

The security and the unwavering quality of information transmission likewise enhanced with engenderment of steganography as now no other individual could transmute the sent information. The primary application fields of steganography are [2]:

- Copyright Protection
- Feature Tagging
- Secret Communication
- Use by terrorists
- Digital Watermarking

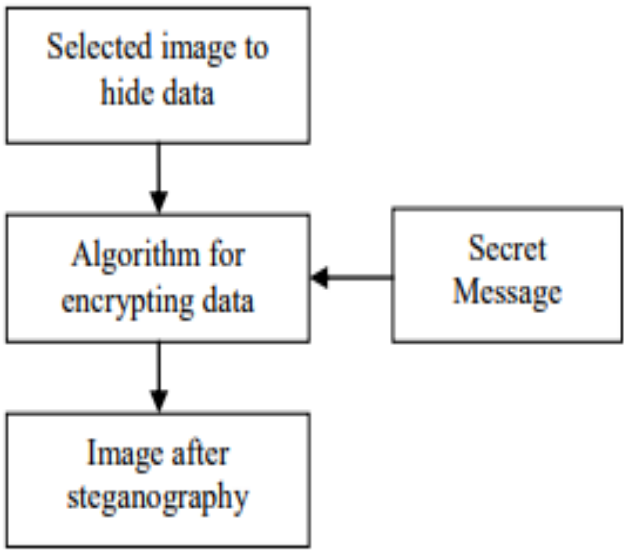



Figure 1 Diagram of Steganography

## II. USING TECHINQUES

### *a. LSB*

. The Least Paramount Bit (LSB) is one of the essential techniques in spatial domain photograph steganography. LSB is the bottom sizably voluminous bit inside the byte value of a photograph pixel. The LSB predicated picture steganography embeds the designation of the game in least good sized bits of pixels values of the quilt photograph. It exploits the truth that the caliber of precision in lots of picture formats is a long way more preponderant than that perceivable through average human imaginative and prescient. Consequently, an altered image with moderate versions in hues might be indistinguishable from the unique via a human being, simply by optically canvassing it. In LSB approach only four byte of pixels are adequate to hold one message byte. Rest of bits in the pixel remains the equal [3]

### b. Discrete Cosine Transform compression

. After color coordinate transformation, the subsequent stage is to isolate the three color segments of the picture into lots of 8×8 blocks. For a 8-bit picture, in the first square every component falls in the range [0,255]. Information elongate that is revolved around zero is engendered in the wake of subtracting the mid-point of the range (the esteem 128) from every component in the first piece, with the goal that the adjusted range is peregrinate from [0,255] to [-128,127]. Pictures are isolated into components of sundry frequencies by the DCT. The quantization step disposes of less essential frequencies and the decompression step utilizes the imperative frequencies to instaurate the picture [4]

## I. RELATED WORK

Ramadhan J. Mstafa (2016) —Over the past few decades, the art ofzz privily embedding and communicating digital data has gained gargantuan attention because of the technological development in both digital contents and communication. The imperceptibility, obnubilating capacity, and toughness in juxtaposition of assailments are 3 main essentialities that some video steganography way should get into thought. In this, a tough and bulwarked video steganographic algo within the Discrete Wavelet Transform (DWT) and Discrete Cosine Transform (DCT) domains is to be predicated on Multiple Object Tracking kenned as MOT algo and Error Rectifying Codes that is kenned as (ECC) is being proposed. Primarily, kineticism-predicated MOT algorithm be implemented reposing on host videos to differentiate the regions of attention in moving objects. After that, the process of data obnubilating is being performed by concealing top secret message into DWT and DCT coefficients of each and every kineticism regions in video depending on center masks. Our experimental outcome exemplify that suggested algo not only ameliorates capacity of embedding and imperceptibility albeit it
supplementally enhances its safety and robustness by encoding the secret message and withstanding against sundry attacks.[5]

Alavi Kunhu et.al (2016) In this paper, we suggest an incipient blind color video watermarking way for copyright auspice of multimedia color videos by the utilization of index mapping conception. The inventiveness in obtainable approach consists in crafty a hybrid DWT and DCT predicated digital video watermarking of color watermark image by designates of record mapping technique. distortion caused all the way through watermarking be assess by way of peak signal to sound ratio (PSNR) along with correspondence structure index measure (SSIM) what's more, heartiness inside restriction to divergent sorts of assaults have been surveyed utilizing StirMark. The proposed video watermarking algo provide amended imperceptibility within harmony by way of human visual system and offers advanced toughness in opposition to signal processing attacks.[6]

. Ch.Sathi Raju et.al (2016) Compression is solemn trouble in applications of capsule endoscopy. In this paper hybrid DCT compression method and DWT compression method is being employed to capitalise advantages of together techniques. The technique includes in engendering color information of the white band and restricted band pictures in a halfway arrangement and after that engendering the decompressed picture. The quality of decompressed image is being evaluated in conditions of mean square error (MSE), signal to noise ratio kenned as (SNR) and PSNR.[7]

N.V.Lalitha (2016) steganography is method of embedding information into signal in a technique that is intricate to abstract.here , a dynamic capacity of audio watermarking system is utilized to establish data and take away them via singular value decomposition withal kenned as (SVD). With avail of SVDbased algor and by income of hoisting wavelet transform apperceived as (LWT), discrete cosine transform (DCT)and DWT . DCT-SVD, DWT-SVD, DWT-DCT-SVD, LWT-DCTSVD methods are developed. It be observed so as to by growing the quantization levels signal-to-noise ratio (SNR) value decreases exponentially which leads to deformation in the pristine signal. It is moreover observed with the aim of robustness is withal more preponderant than afore by applying dissimilar malevolent attacks like resampling, echo additament, cropping, additive white gaussian noise (AWGN), and signal subtraction to enclosed signal with the aim of doesn’t perturb novel signal and mine image. [8]

Uma Rajput. (2015) in this paper The aim of Digital Watermarking is on the way to provide safety in conditions of information obnubilating and copyright sentinel. The researchers be perpetually working to engender robust digital picture watermarking method. In paper proposed a novel way for RGB digital watermarking predicated on 2-Discrete Cosine Transform well-kenned as (DCT) all the way through discrete wavelet transform (DWT) algo. For utilization of this two images- first one is cover image and 2nd is top secret imageFor providing ameliorated security, we worked RGB elements. Experimental results Shows that PSNR, NE value, and PSNR reach up to 56%.[9]

Ammad Ul Isla (2016) in this paper the expeditious advancement of information correspondence in current period requests secure trade of data. Steganography is apperceived way intended for obnubilating information as of unauthorised access. Steganographic systems conceal mystery information in sundry document arrangements, for example, image, text, audio, and video. Invisibility, capacity of payload, and PSNR security and toughness are key challenges to steganography. In this , a pristine image stegnography way predicated on majority consequential bits (MSB) of pixels is proposed. Bit No. 5 is utilized to store the secret bits predicated on the difference of bit No. 5 and 6 of cover image. If the difference of bit No. 5 and 6 is unique in cognation to mystery information bit then the estimation of bit No. 5 is transmuted. The outcomes express that the proposed system guarantees eminent transmutations in flag to commotion proportion. Customarily, hackers fixate on the LSB bits for top secret data mining but proposed method utilizes MSB bits that engender it more forfended from illicit access. [10].

## IV Proposed methodology

a) Steganography Algorithm & Process

Proposed Algorithm

- Step1: First browse a cover image to be obnubilate secret image.
- Step2: Browse secret image and divide image into DCT blocks.
- Step3: Obnubilate secret blocked image into cover image utilizing LSB.
- Step4: Apply Noise Attack on embedded image.
- Step5: Abstract noise from embedded noise image.
- Step6: Extract secret image from noise free embedded image.
- Step7: Calculated PSNR and BPP.

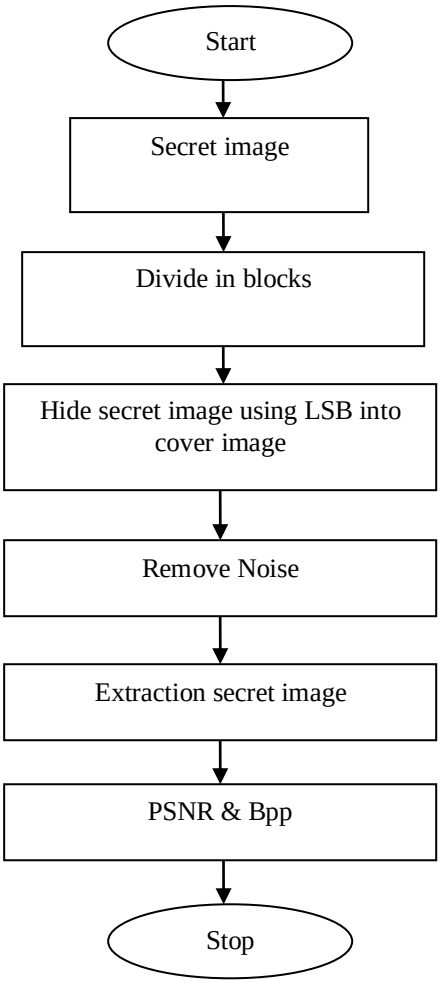



Fig 2: Block dig of Propose Process

## V.RESULT ANALYSIS

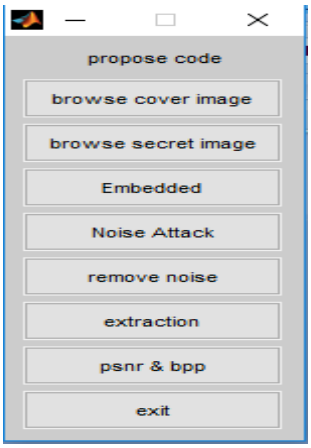



Fig. 3 First run the code than we obtain this menu bar.

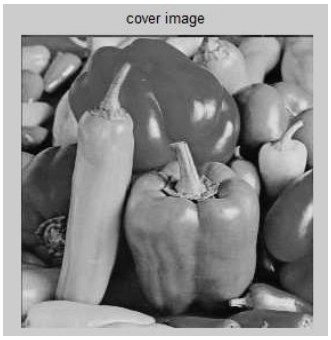



Fig. 4 First browse the cover image to be hide secret image.

Enter the value of M for block size:-4


Fig. 5 browse secret image and divide secret image into 4x4 blocks.


Fig. 6 hide blocked image into cover image.

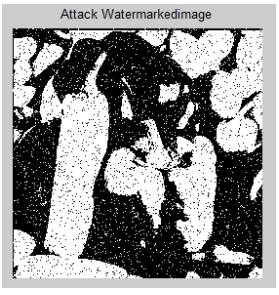



Fig. 7.Apply noise attack on embedded image.


Fig. 8 Remove noise from the embedded noisy image.

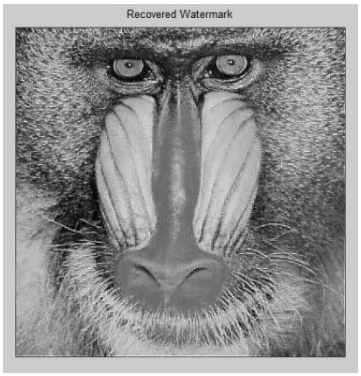
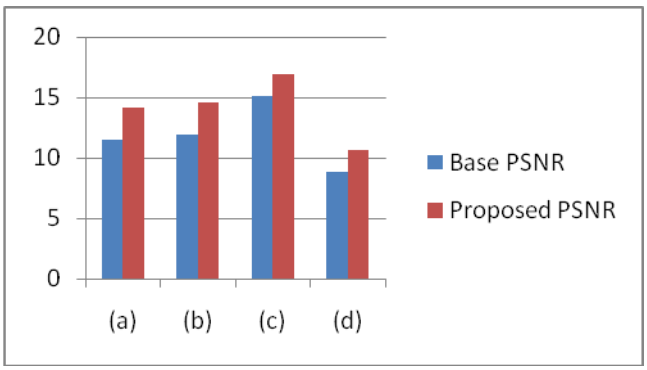



Fig.9. extract the secret image from embedded noise free image.

## II. RESULT ANALYSIS

Table1.Comparison between base and Proposed PSNR

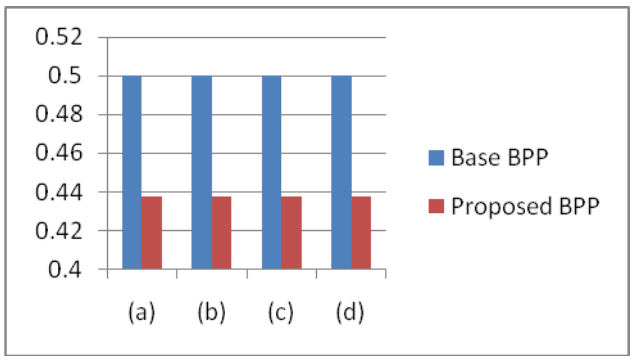
| Cover Image | Base PSNR | Proposed PSNR |
|---|---|---|
| (a) | 11.4510 | 14.1402 |
| (b) | 11.8901 | 14.5433 |
| (c) | 15.1320 | 16.9444 |
| (d) | 8.8700 | 10.5922 |




Graph.1 Comparison between base and Proposed PSNR

Table2. Comparison between base and Proposed BPP

| Cover Image | Base BPP | Proposed BPP |
|---|---|---|
| (a) | 0.500 | 0.4375 |
| (b) | 0.5000 | 0.4375 |
| (c) | 0.5000 | 0.4375 |
| (d) | 0.5000 | 0.4375 |




Graph.2 Comparison between base and Proposed BPP

## Conclusion

Steganography is the process of embedding an imperceptible signal (data) into the given signal (data). The invisible sign is called as watermark and given sign is referred to cover work. This cover up paintings might be image, audio or video file. This embedded data can later be extracted from the multimedia for bulwark functions. This paper exhibits a substructure dialog on authentic calculations of steganography and steganalysis for computerized pictures. Some imperative calculations of steganography in spatial area are verbalized about in points of interest with exceptional accentuation so specialists and steganalysts will ken about how to grow such systems.

In this modern eras of technology with the incrementation in desideratum of secure and robust communication for military ,astuteness agencies, internet banking etc, the information technology area looks towards the future research in the field of double steganography. Some future explores may include: 1. Developing up a framework by joining the advantages of both sound and picture steganography. 2. concentrating on different techniques like sound, video, and so on to shroud the mystery information. 3. Developing an environment which should be platform independent. 4. Utilization of best calculations to accomplish high efficacy, power and inserting limit with regards to secure. 5. Consolidating the conceptions of half breed cryptography and sound steganography to give more preponderant security.

## *References*

[1] Manisha, Deepkiran Munjal, “A Review Paper of Dual Steganography Technique Using Status LSB and DWT Algorithms”. Manisha et al. / International Journal of Computer Science & Engineering Technology (IJCSET) ISSN : 2229-3345 Vol. 7 No. 05 May 2016

[2] Ashadeep Kaur* , 2Rakesh Kumar, 3Kamaljeet Kainth, “Review Paper on Image Steganography”. International Journal of Advanced Research in Computer Science and Software Engineering. ISSN: 2277 128X Volume 6, Issue 6, June 2016

[3] Deepika Dongre, Rina Mishra, “A Review on Edge Based Image Steganography
International Journal on Recent and Innovation Trends in Computing a nd Communication ISSN: 2321.8169Volume: 2 Issue: 9 2862 - 28

[4] A.M.Raid1 , W.M.Khedr2 , M. A. El-dosuky1 and Wesam Ahmed1, “Jpeg Image Compression Using Discrete Cosine Transform - A Survey International Journal of Computer Science & Engineering Survey (IJCSES) Vol.5, No.2, April 2014.

[5] Ramadhan J. Mstafa1 ,Khaled M. Elleithy1 and Eman Abdelfattah2, “A Robust and Secure Video Steganography Method in DWT-DCT Domains Based on Multiple Object Tracking and ECC” , 2169-3536 (c) 2016 IEEE

[6] Alavi Kunhu, Nisi K, Sadeena Sabnam, Majida A, Saeed AL-Mansoori, “Index Mapping based Hybrid DWT-DCT Watermarking Technique for Copyright Protection of Videos Files” , 978-1-5090-4556-3/16/$31.00 ©2016 IEEE.

[7] Ch.Sathi Raju, D.V.Rama Koti Reddy, “On Compression Characteristics of White Band and Narrow Band Images Using Hybrid DCT and DWT” , 978-1- 4788-7225 -8/15/$31.00©2015 IEEE.

[8] N.V.Lalitha, P.Vara Prasad, S.UmaMaheshwar Rao, S.UmaMaheshwar Rao , “Performance Analysis of DCT and DWT Audio Watermarking based on SVD” ,978-1-5090-1277-0/16/$31.00 ©2016 IEEE

[9] Uma Rajput, Nirupma Tiwari, “A novel technique for RGB Invisible Watermarking Based on 2-DWT-DCT Algorithm” , 978-1-4799-8553-1/15/$31.00 © 2015 IEEE.

[10] Ammad Ul Islam1 , Faiza Khalid2 , Mohsin Shah2 , Zakir Khan2 , Toqeer Mahmood3 , Adnan Khan2 , Usman Ali2 , Muhammad Naeem4, “An Improved Image Steganography Technique based on MSB using Bit Differencing” , 978-1-5090-2000-3/16/$31.00 ©2016 IEEE