# PICTURE STEGANOGRAPHY HAING DISCRETE COSINE TRANSFORM (DCT) AND LEAST SIGNIFICANT BIT (LSB)

[1] Mohit Kumar [2] Priyanka
[1] M.Tech( Student), [2]Assistant Professor (CRSU, Jind)
[1]Department of Computer Science & Application, CRSU, Jind
[1]CRSU, Jind, Haryana (India)

**ABSTRACT**

Steganography is an imperative zone of research lately including various applications. It is the exploration of implanting data into the cover picture viz., content, video, and picture (payload) without making measurably critical adjustment the cover picture. The cutting edge secure picture steganography introduces a testing errand of exchanging the inserted data to the goal without being distinguished. In this paper we exhibit a picture based steganography that consolidates Least Significant Bit (LSB) and Discrete Cosine Transform (DCT) to upgrade the security of the payload. At first, the LSB calculation is utilized to install the payload bits into the cover picture to infer the stego-picture. The stego-picture is changed from spatial area to the recurrence space utilizing DCT. It is watched that safe pictures with low MSE and BER are exchanged without utilizing any watchword, in examination with prior works.

## I. INTRODUCTION

Throughout time, transmission of data securely over network has gained utmost importance. It is mandatory to transmit data in such a way that its existence cannot be depicted by anyone. Image Steganography is one such method that facilitates the process of secret communication. The word steganography is of Greek origin and means "covered writing" as it combines the words steganos meaning "covered", and graphein meaning "writing". It mainly aims to camouflage data in a cover medium known as carrier. This carrier can then be transmitted to the receiver who can decrypt the information as per the key provided by the sender. A cover medium may include an image, audio, text or video. The medium that contains the embedded message is known as stego-medium as shown below:

**Cover medium + message + secret key = stego-medium**

The most common files for hiding messages are images. Thus image in which data is embedded is referred to as stego-image. The information to be hidden may also be known as payload.

A famous example of steganography is "prisoner's problems" where, two prisoners A and B wish to escape from the jail and their cellars are far apart. The only mode of communication is sending messages via the prison officer. Before they are arrested, they agree upon a stego system that describes the way the secret message is embedded into the covert text. If the prison officer detects conspiracy, the security will be further tightened. The prison officer can deliberately modify the stego text to foil the prisoners' escape.

In modem image stenography which exploits the advantages of the present day digital media, the earlier examples appear simple but the concepts are similar. This is largely due to the fact that, multimedia objects which generally permits the addition of significantly large amount of payload by means of simple modifications that preserve the perceptual content of the underlying cover image. Hence multimedia objects have been found to be perfect candidates for use as cover messages. A steganographic technique is said to be £-secure if the relative entropy of the probability distribution of cover images and stego-objects is less than or equal to £. A steganography technique is perfectly secure if £ is zero. Some of the well-known steganography methods are the following: LSB, masking and filtering and transform technique. In the LSB approach, the basic idea is to replace the Least Significant Bits (LSB) of the cover image with the Most Significant Bits (MSB) of the image to be hidden without destroying the statistical property of the cover image significantly. The LSB-based technique is the most challenging one as it is difficult to differentiate between the cover-object and stego-object if few LSB bits of the cover- object are replaced. In masking and filtering techniques two signals are embedded into each other in such a manner that only one of the signals is perceptible to the

human eye. This is mainly used in watermarking techniques. In the transform-based method, the spatial domain is transformed to frequency domain using DCT, Fast Fourier Transforms (FFT), and Wavelets etc.

Hiding information into a medium requires following elements:

1. The cover medium(C) that will hold the secret message.

2. The secret message (M), may be plain text, digital image file or any type of data.

3. The steganography techniques

4. A stego-key (K) may be used to hide and unhide the message.

In modern approach, depending on the cover medium, steganography can be divided into five types: Text Steganography, Image Steganography, Audio Steganography, Video Steganography and Protocol Steganography.

- **Text steganography:** Hiding information in text file is the most common method of steganography. The method was to hide a secret message into a text message. After coming of Internet and different type of digital file formats it has decreased in importance. Text stenography using digital files is not used very often because the text files have a very small amount of excess data.

- **Image steganography:** Images are used as the popular cover medium for steganography. A message is embedded in a digital image using an embedding algorithm, using the secret key. The resulting stego-image is send to the receiver. On the other side, it is processed by the extraction algorithm using the same key. During the transmission of stego- image unauthenticated persons can only notice the transmission of an image but cant see the existence of the hidden message.

- **Audio steganography:** Audio steganography is concerned with embedding information in an innocuous cover speech in a secure and robust manner. Communication and transmission security and robustness are essential for transmitting vital information to intended sources while denying access to unauthorized persons. An audible, sound can be inaudible in the presence of another louder audible sound .This property allows to select the channel in which to hide information. Existing audio steganography software can embed messages in WAV and MP3 sound files. The list of methods that are commonly used for audio steganography are listed and discussed below.

  - **LSB coding**
  - **Parity coding**
  - **Phase coding**
  - **Spread spectrum**
  - **Echo hiding**

- **Video steganography:** Video Steganography is a technique to hide any kind of files in any extension into a carrrying Video file.

- **Protocol steganography:** The term protocol steganography is to embedding information within network protocols such as TCP/IP. We hide information in the header of a TCP/IP packet in some fields that can be either optional or are never used.

**Objective**

The project is carried out with the following objectives:

- To hide the message or a secret data into an image which acts as a cover medium using LSB technique?

- The primary motivation of my current work is to increase PSNR of the stego-image (peak signal to noise ratio).

## II. RELATED WORK

**[1] Deepak Kumar Jain, Devansh Gaur [Algo-Ref],** Image Compression means reducing the volume of data needed in order to represent an Image. Image compression techniques are divided into two main techniques: trans- forms (DCT, JPEG, FFT, and Wavelet) and non transforms (PCM, DPCM).In this paper we present the DCT transform to compress the Image with high quality. In achieving those results, the wavelet scheme tries to identify the wavelet filter that would result in the smallest number of non- zero coefficients (thus giving a high compression ratio), uses an HVS based Processing Module to adaptively quantize wavelet coefficients, and efficiently codes the processed Wavelet Transform

**[2] Monika Gunjal, Jasmine Jha,** Steganography is one of the methods of secret communication that hides the existence of message so that a viewer cannot detect the transmission of message and hence cannot try to decrypt it. It is the process of embedding secret data in the cover image without significant changes to the cover image. A cryptography algorithm is used to convert the secret messages to an unreadable form before embedding. These algorithms keep the messages from stealing, destroying from unintended users on the internet and hence provide security. Cryptography was introduced for making data secure. But alone cryptography cannot provide a better security approach because the scrambled message is still available to the eavesdropper. There arises a need of data hiding. So the propose technique use a combination of steganography and cryptography for improving the security. The proposed technique use Discrete Cosine Transform (DCT) and Blowfish algorithm. The proposed method calculates LSB of each DC coefficient and replace with each bit of secret message. The proposed embedding method using DCT with LSB obtained better PSNR values. Blowfish algorithm is used for encryption and decryption of text message using a secret-key block cipher. This technique makes sure that the message has been encrypted before hiding it into a cover image. Blowfish is an improvement over DES, 3DES, etc designed to increase security and to improve performance.

**[3] Deepika Bansal, Rita Chhikara,** in this paper, a steganographic technique for hiding secret data in image file formats is proposed. This technique uses the Quantized DCT coefficients for hiding the secret information. The proposed steganographic method can provide a high information hiding capacity and successfully increase the security. Steganography is the art and science of hiding secret messages in the other file formats, so that the existence of the secret message is not revealed. In this paper, a steganography algorithm using DCT domain is proposed, Shield Algorithm. The two different tools are used to perform the analysis of images using the classification accuracy and PSNR, in comparison to the proposed algorithm. On the basis of above analysis, we can conclude that the Shield algorithm is giving better PSNR results from F5 and PQ, and better classification accuracy is obtained than F5 steganography tool.

**[4] K. Munivara Prasad, V.Jyothsna, S.H.K. Raju, S.Indraneel,** We propose a new approach to steganography for hiding secret images in the digital media. Steganography differs from digital watermarking because both the information and the very existence of the information are hidden. We refer it as Blind Consistency based Steganography, which provides high imperceptibility and security for information from subterfuge attack. The Existing Steganographic approaches are unable to handle the Subterfuge attack i.e, they cannot deal with the opponents not only detects a message ,but also render it useless, or even worse, modify it to opponent favor. The advantage of BCBS is the decoding can be operated without access to the cover image and it also detects if the message has been tampered without using any extra error correction. To improve the imperceptibility of the BCBS, DCT is used in combination to transfer stego-image from spatial domain to the frequency domain. The hiding capacity of the information is improved by introducing Fractal Compression and the security is enhanced using by encrypting stego-image using DES. Finally the Embedding and Extraction process are detailed in the paper, along with the analysis on capacity, security and imperceptibility. The experimental results are provided as well.

**[5] Debiprasad Bandyopadhyay, Kousik Dasgupta, J. K. Mandal, Paramartha Dutta,** This paper presents a novel approach of building a secure data hiding technique in digital images. The image steganography technique takes the advantage of limited power of human visual system (HVS). It uses image as cover media for embedding secret message. The most important requirement for a steganographic algorithm is to be imperceptible while maximizing the size of the payload. In this paper a method is proposed to encrypt the secret bits of the message based on chaos theory before embedding into the cover image. A 3-3-2 LSB insertion method has been used for image steganography.

Experimental results show a substantial improvement in the Peak Signal to Noise Ratio (PSNR) and Image Fidelity (IF) value of the proposed technique over the base technique of 3-3-2 LSB insertion.

**[6] Champakamala .B.S, Padmini.K, Radhika D. K.,** Steganography is one of the most powerful techniques to conceal the existence of hidden secret data inside a cover object. Images are the most popular cover objects for Steganography and in this work image steganography is adopted. Embedding secret information inside images requires intensive computations, and therefore, designing Steganography in hardware speeds up Steganography. This is implemented using ARM7TDMI processor and GSM 900.

There are several techniques to conceal information inside cover-image. The spatial domain techniques manipulate the cover-image pixel bit values to embed the secret information. The secret bits are written directly to the cover image pixel bytes. Consequently, the spatial domain techniques are simple and easy to implement.

The Least Significant Bit (LSB) is one of the main techniques in spatial domain image steganography. In this work, a new technique of LSB steganography has been proposed which is an improvised version of one bit LSB technique.

**[7] Adel Almohammad, Gheorghita Ghinea, Robert M. Hierons,** The two most important aspects of any image-based steganographic system are the imperceptibility and the capacity of the stego image. This paper evaluates the performance and efficiency of using optimized quantization tables instead of default JPEG tables within JPEG steganography. We found that using optimized tables significantly improves the quality of stego-images. Moreover, we used this optimization strategy to generate a 16x16 quantization table to be used instead of that suggested. The quality of stego-images was greatly improved when these optimized tables were used. This led us to suggest a new hybrid steganographic method in order to increase the embedding capacity. This new method is based on Jpeg-Jsteg methods. In this method, for each 16x16 quantized DCT block, the least two-significant bits (2-LSBs) of each middle frequency coefficient are modified to embed two secret bits. Additionally, the Jpeg-Jsteg embedding technique is used for the low frequency DCT coefficients without modifying the DC coefficient. Our experimental results show that the proposed approach can provide a higher information-hiding capacity than the other methods tested. Furthermore, the quality of the produced stego-images is better than that of other methods which use the default tables.

**[8] P.M.Siva Raja and E.Baburaj,** As an important component of multimedia information security, information hiding has received wide attention in recent years. In fact, intellectual properties are becoming harder to protect and so are original contents, that's why we need techniques to be developed such as Image Steganography. Steganography is a technique for information hiding. It aims to embed secret data in to digital cover media, such as Images, Audio and Video without being suspicious. Evolutionary algorithms are stochastic search methods that mimic the natural bio logical evolution and the social behaviour of species. Such algorithms have been developed to arrive at near optimum solutions to large-scale optimization problems. For which traditional mathematical techniques may fail. In this paper, a novel stenographic method, based on Particle Swarm Optimization algorithm (PSO) is proposed, PSO is an evolutionary computational model based on Swarm intelligence. Kennedy and Elbe hart developed PSO through simulating social behaviour. In PSO, each individual is called a "particle" and the position of each particle is a candidate solution to a problem. LSB Matching Revisited (LSBMR) image steganography using Particle Swarm Optimization algorithm (PSO) is proposed, in Particle Swarm Optimization algorithm (PSO) is used to select the embedding regions according to the size of the secret message and to optimize the threshold value of the selected image regions. In order to improve the quality of stego images, an optimal substitution matrix for transforming the secret messages is first derived by means of the PSO algorithm. The experimental results show that our proposed method has larger message capacity and better image quality then the existing method.

**[9] Guo-Shiang Lin, Yi-Ting Chang, and Wen-Nung Lie,** picture quality and statistical undetectability are two key issues related to steganography techniques. In this paper, we propose a closed-loop computing framework that iteratively searches proper modifications of pixels/coefficients to enhance a base steganographic scheme with optimized picture quality and higher anti-steganalysis capability. To achieve this goal, an anti-steganalysis tester and an embedding controller—based on the simulated annealing (SA) algorithm with a proper cost function—are incorporated into the processing loop to conduct the convergence of searches. The cost function integrates several performance indices, namely, the mean square error, the human visual system (HVS) deviation, and the differences in statistical features, and guides a proper direction of searches during SA optimization. Our proposed framework is suitable for the kind of steganographic schemes that spreads each message information into multiple pixels/coefficients. We have selected two base steganographic schemes for implementation to show the applicability of the proposed framework. Experiment results show that the base schemes can be enhanced with better performances

in image PSNR (by more than 5.0 dB), file-size variation, and anti-steganalysis pass-rate (by about 10% 86%, at middle to high embedding capacities).

**[10] Rita Rana Chhikara Latika Singh,** Feature Selection is a preprocessing technique with great significance in data mining applications that aims at reducing computational complexity and increase predictive capability of a learning system. This paper presents a new hybrid feature selection algorithm based on Discrete Firefly optimization technique with dynamic alpha and gamma parameters and t-test filter technique to improve detectability of hidden message for Blind Image Steganalysis. The experiments are conducted on important dataset of feature vectors extracted from frequency domain, Discrete Cosine Transformation and Discrete Wavelet Transformation domain of cover and stego images. The results from popular JPEG steganography algorithms nsF5, Outguess, PQ and JP Hide and Seek show that proposed method is able to identify sensitive features and reduce the feature set by 67% in DCT domain and 37% in DWT domain. The experiment analysis shows that these algorithms are most sensitive to Markov features from DCT domain and variance statistical moment from DWT domain.

**[11] Amandeep Kaur, Rupinder Kaur, Navdeep Kumar**, With the evolution of Internet Technology the need for the security of information during its transmission has also increased rapidly. Steganography plays a prominent role in the field of data hiding and providing a means for secret communication. Steganography basically refers to the process of secretly hiding messages into a cover medium in a way that only the receiver can suspect its existence. In this paper a new technique for image steganography has been discussed that utilizes the LSB substitution in the contour region of the image. The Pixel Value difference of the region has also been taken in to account in order to increase the embedding capacity of data. A new fitness function has been designed for the Artificial Bee Colony Optimization Algorithm that helps to calculate the best positions where data can be embedded. The results obtained using the proposed method provides an increase of approximately 33% in the hiding capacity as compared with the previous technique. It also results into an effective PSNR range varying from 60 to 75 thus increasing the visual quality of image.

## III. IMPORTANT ALGORITHMS

### Discrete Cosine Transform (DCT)

A discrete cosine Transform(DCT) communicates a limited arrangement of information focuses as far as an aggregate of cosine capacities wavering at various frequencies. DCTs are critical to various applications in science and designing, from lossy pressure of sound (e.g. MP3) and pictures (e.g. JPEG) (where little high-recurrence segments can be disposed of), to otherworldly techniques for the numerical arrangement of incomplete differential conditions. The utilization of cosine instead of sine capacities is basic for pressure, since it turns out (as depicted beneath) that less cosine capacities are expected to rough a run of the mill flag, while for differential conditions the cosines express a specific decision of limit conditions.

Specifically, a DCT is a Fourier-related change like the discrete Fourier change (DFT), yet utilizing just genuine numbers. The DCTs are for the most part identified with Fourier arrangement coefficients of an occasionally and symmetrically broadened grouping though DFTs are identified with Fourier arrangement coefficients of an intermittently expanded succession. DCTs are identical to DFTs of generally double the length, working on genuine information with even symmetry (since the Fourier change of a genuine and even capacity is genuine and even), though in a few variations the info or potentially yield information are moved considerably an example. There are eight standard DCT variations, of which four are normal

The DCT transforms a signal from a photograph depiction right into a frequency representation, by grouping together the pixels into 8 × 8 pixel blocks and remodelling the pixel blocks into 64 DCT. DCT is used in Steganography as- Image is busted into 8×8 blocks of pixels. Working from left to right, top to bottom, the DCT is put on every single block. Almost Every block is pressurized throughout quantization table to degree the DCT coefficients and information is actually integrated in DCT coefficients.

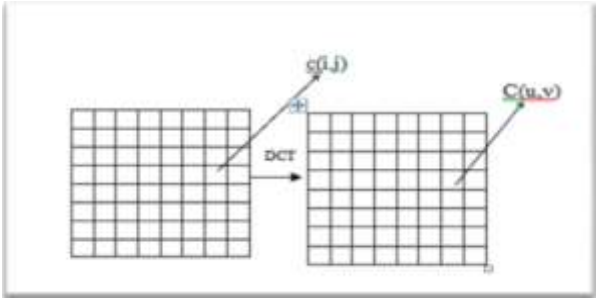


**Fig 1 Discrete Cosine Transform of an Image**

Although Steganography aims at transferring images without worrying about visual wreckage or perhaps modifications for naked observer, it cannot distribute alongside transforming spatial and transform level specifics in order to embed the data.

DCT coefficients are used for JPEG compression. It separates the image into parts of differing importance. It transforms a signal or image from the spatial domain to the frequency domain. It can separate the image into high, middle and low frequency components.

Image is broken into 8×8 blocks of pixels. Working from left to right, top to bottom, DCT is applied to each block. Each block is compressed through quantization table to scale the DCT coefficients and message is embedded in DCT coefficients.

**Least-Significant Bit (LSB) Technique**

LSB mechanism is a common and simple approach to embed secret message in a cover image. The least significant bit (in other words, the 8th bit) of some or all of the bytes inside an image is changed to a bit of the secret message. Digital images are mainly of two types (i) 24 bit images and (ii) 8 bit images. In 24 bit images we can embed three bits of information in each pixel, one in each LSB position of the three eight bit values. Increasing or decreasing the value by changing the LSB does not change the appearance of the image; much so the resultant stego-image looks almost same as the cover image. In 8 bit images, one bit of information can be hidden. The resulting stego image appears to be identical as cover image to the human eye.

LSB insertion is very vulnerable to a lot of transformations, even the most harmless and usual ones.

Lossy compression, e.g. JPEG, is very likely to destroy it completely. The problem is that the "holes" in the Human Visual System that LSB insertion tries to exploit - little sensitivity to added noise - are the same that lossy compression algorithms rely on to be able to reduce the data rate of images.

Geometrical transformations, moving the pixels around and especially displacing them from the original grid, are likely to destroy the embedded message, and the only one that could allow recovery is a simple translation.

Any other kind of picture transformation, like blurring or other effects, usually will destroy the hidden data.

All in all, LSB insertion is a very little robust technique for data hiding.

**IV- CONCLUSION**

In this paper we have utilized the blend of LSB calculations and DCT change on crude pictures to acquire secure stego-picture. The LSB strategy has been utilized to oblige most extreme payload. The whole payload is inserted into the cover picture to acquire the stego-protest. The stego-protest in the spatial area is changed into recurrence space by applying DCT. A precisely invert methodology is taken after to recover the payload at the beneficiary. The incorporated approach of joining LSB and DCT empower secure exchange of payload with low BER and MSE contrasted with before procedures.

## V- REFERENCES

[Algo-Ref] Deepak Kumar Jain, Devansh Gaur, Kavya Gaur, Neha Jain, **"Image Compression using Discrete Cosine Transform and Adaptive Huffman Coding",** International Journal of Emerging Trends & Technology in Computer Science (IJETTCS), Volume 3, Issue 1, January – February 2014, ISSN 2278-6856

[01] Monika Gunjal, Jasmine Jha, **"Image Steganography Using Discrete Cosine Transform (DCT) and Blowfish Algorithm",** International Journal of Computer Trends and Technology (IJCTT) – volume 11 number 4 – May 2014, ISSN: 2231-2803,

[02] Deepika Bansal Rita Chhikara, **"An Improved DCT based Steganography Technique",** International Journal of Computer Applications (0975 – 8887), Volume 102– No.14, September 2014,

[03] K. Munivara Prasad, V.Jyothsna, S.H.K. Raju, S.Indraneel, **"High Secure Image Steganography in BCBS Using DCT and Fractal Compression",** IJCSNS International Journal of Computer Science and Network Security, VOL.10 No.4, April 2010,

[04] Debiprasad Bandyopadhyay, Kousik Dasgupta, J. K. Mandal, Paramartha Dutta, **"A Novel Secure Image Steganography Method Based On Chaos Theory In Spatial Domain",** International Journal of Security, Privacy and Trust Management (IJSPTM) Vol 3, No 1, February 2014,

[05] Champakamala .B.S, Padmini.K, Radhika D. K., **"Least Significant Bit algorithm for image steganography",** International Journal of Advanced Computer Technology (IJACT), VOLUME 3, NUMBER 4, ISSN:2319-7900,

[06] Adel Almohammad, Gheorghita Ghinea, Robert M. Hierons, **"JPEG steganography: a performance evaluation of quantization tables",** 2009 International Conference on Advanced Information Networking and Applications, 1550-445X/09 $25.00 © 2009 IEEE, DOI 10.1109/AINA.2009.67,

[07] P.M.Siva Raja and E.Baburaj, **"An Efficient Data Embedding Scheme for Digital Images Based On Particle Swarm Optimization with LSBMR"**, Third International Conference on Computational Intelligence and Information Technology (CIIT 2013),2013, January 2013, DOI: 10.1049/cp.2013.2568, ISBN: 978-1-84919-859-2

[08] Guo-Shiang Lin, Yi-Ting Chang, and Wen-Nung Lie, **"A Framework of Enhancing Image Steganography with Picture Quality Optimization and Anti-Steganalysis Based on Simulated Annealing Algorithm",** IEEE TRANSACTIONS ON MULTIMEDIA, VOL. 12, NO. 5, AUGUST 2010, Digital Object Identifier 10.1109/TMM.2010.2051243,

[09] Rita Rana Chhikara Latika Singh, **"An Improved Discrete Firefly and t-Test based Algorithm for Blind Image Steganalysis",** 2015 6th International Conference on Intelligent Systems, Modelling and Simulation, 2166-0670/15 $31.00 © 2015 IEEE, DOI 10.1109/ISMS.2015.50

[10] Amandeep Kaur, Rupinder Kaur, Navdeep Kumar,**"Image Steganography using Discrete Wavelet Transformation and Artificial Bee Colony Optimization",** 2015 1st International Conference on Next Generation Computing Technologies (NGCT-2015), 5th September 2015