International Journal of Current Trends in Engineering & Technology
ISSN: 2395-3152
Volume: 03, Issue: 05 (SEPTEMBER -OCTOBER, 2017)

# Digital Image Steganography using Particle Swarm Optimization with DCT and BPPCM

**Swati Patel [1], Prof. Jitendra Agrawal[2]**
Department of Computer Science & Engineering
RGPV, Bhopal, M.P., India
swati.sagwaliya@gmail.com, jitendra@rgtu.net

**Abstract:-** *In the field of Steganography is the hiding information using the different technique used to exchange the secret message or secret data with low distortion of the cover medium or cover image. Number of different cover medium pattern like data image and image text or information as image is used to data hide the key information. Particle Swarm optimization has been search within the image data and determining in image coefficients through transforms and concept of image Steganography is explained and an analysis of recent image Steganography methods and its applications is presented Security, embedding capacity, and imperceptibility based design very old Steganography algorithms. Proposed technique to embed secret information in the cover image based on bit change method. Propose technique a good stability that enables us to hide secret information without degrading the perceptual quality. Propose technique good robustness against various attacks and image processing. Image stenography technique is a rising procedure because information or image data are transfer secure and found different application in the fields of image stenography. The frequency domain techniques are extremely most popular for image stenography applications in transform. PSO primarily based approach the image data is embedded into cover image manner within the transform bit Particle position modification .PSO primarily based transform coefficients change but not best in terms of the watermarked image data secure quality and data secure embedding capability but our proposed technique good embedding capacity and privacy.*

***Keywords:-*** *Discrete cosine transform, least significant bit, discrete wavelet transform, Steganography, Particle Swarm Optimization. Image Steganography, Image Processing.*

## I.INTRODUCTION

Information security is a challenging task due to widespread use and growth of internet and multimedia usage. Transmission and reception of secret information are carried out frequently over public communication channels. Due to the weakness of human visual system and cheaper options available for image storage, communication & processing, image Steganography has become the popular way of secret communication. The word Steganography has been derived from two Greek words, segos' means cover and graa means writing, denting it as covered writing. The concept of Steganography is usually modeled by the prisoner's problem and is one of the branches of information hiding Information hiding system generally involves both watermarking and Steganography. A main goal of the watermarking system is the high level of robustness, in order to make the removing of watermark impossible by a third party without degrading the data object's quality. Steganography, on the other hand, is used to pursue high capacity and security [1]. Now a day, lots of applications are Internet-based and in some cases it's desired that the communication be created secret. There are 2 techniques are available to achieve this goal. One is cryptography, wherever the sender uses AN encoding key to cipher the message, this encrypted message is transmitted through the insecure public channel, and decryption algorithmic program is employed to decode the message. The reconstruction of the initial message is feasible given that the receiver has the decryption key. The second methodology is Steganography, wherever the key message is inserted in another medium. Steganography is that the art of activity data through original files in such a way that the existence of the message is unknown. Digital image Steganography is also a Greek word Steg, that also another meaning Covered Text. The initial files will be stated as cover text, cover image, or cover audio. Once inserting the key message it's stated as stego-medium. A stego-key is employed for activity method to limit detection and/or recovery of the embedded knowledge. Whereas cryptography is protects data or information the content of messages, Steganography protects data or information hides the message so intermediate persons cannot see the message. Steganography differs from cryptography. The aim of cryptography is to secure communications by ever-changing the information into a kind that can't be perceived. In this method a Steganography technique, another side, data or information hides the existence of the message itself that makes it difficult for a third person to search out wherever the message is. Generally sending encrypted data could draw attention, whereas invisible data won't. Consequently, cryptography isn't the nice resolution for secure communication; it's only a part of the answer. Each technique will be used along to higher protect data. In this case, even if Steganography fails, the message cannot be recovered because a cryptography technique is

employed additionally. The cracking of steganographic messages is termed steganalysis. The aim of steganalysis is to identify the data and determining that whether or not or not they need hidden messages encoded into them and if possible, extract the hidden data [2].

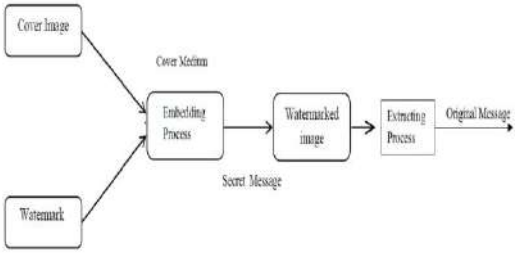


Figure 1 General Hiding Information System.

Steganography is a good candidate in secure communications in cases where the use of cryptography is not allowed or raises suspicion. One of these applications is military and intelligence agents where a high priority is saving an agent's life. Even if the cryptography is used, the detection of secret messages by cryptanalysis techniques may rapidly lead to an attack on the agent. In addition, Steganography can be used in the protection of data alteration, in companies for the safe circulation of secret data, and in accessing the control systems for digital content distribution and so on. A number of specifications are to be possessed by watermarking or Steganography algorithms in order to be efficient.

**Imperceptibility**: A watermark should not be visible to the users. It should not affect the carrier signal so that it remains imperceptible to the viewers.

**Robustness:** A watermark should be tolerant to any lossy compression technique or any signal processing operations (signal enhancement, noise, filtering, geometric image operations) so that it could be detected easily and as such at receiver's end

**PSNR:** Peak signal to noise ratio of the digital signal carrying the watermark should be high which implies that the signal is not much affected by the noise and data is received as intended at the receiver [3].

**Types of Steganographic Techniques**

This paper introduced various stenography techniques for hiding data in images. The images are represented with numerical values of each pixel where the value represents the color and intensity of the pixel. Images are mainly of two types: 8-bit images, 24-bit images 8-bit images: In 8-bit images maximum numbers of colors that can be present are only 256 colors.24-bit images: Each pixel in these images have 24 bit value in which each 8 bit value refers to three colors red, blue and green. There are several Steganographic techniques for image file format which are as follows:

**1. Spatial Domain Technique:** There are several versions of spatial Steganography, all directly modification some bits within the image element values in hiding information. Least important bit (LSB)-based image Steganography is one amongst the only techniques that hides a secret message inside the LSBs of part values whereas not introducing many perceptible distortions. To our human eye, changes inside the value of the LSB are inaudible. Embedding of message bits could also be done either consecutive or indiscriminately. Least vital Bit (LSB) replacement, LSB matching, Matrix embedding and element worth, differencing are a number of the spatial domain techniques. Benefits of spatial domain LSB technique are: there's less probability for degradation of the initial image. Hiding capability is a lot of i.e. a lot of info may be hold on in a picture. Disadvantages of LSB technique are: Less robust, the hidden data is also lost with image manipulation. Hidden data is also merely destroyed by straightforward attacks.

**2. Transform Domain Technique:** this is often a lot of advanced means of hiding info in a picture. Varied algorithms and transformations are used on the image to cover info in it. Transform domain embedding may be termed as a website of embedding techniques that varieties of algorithms are advised. The method of embedding information within the frequency domain of a proof is far stronger than embedding principles that operate within the time domain. Most of the robust steganographic systems these days operate at intervals the transform domain transform domain techniques have a plus over LSB techniques as they hide information in region of the image Steganography that are not as much of exposed to density, cropping, and image Steganography method. Some transform domain techniques don't appear addicted to the image format and that they could run lossless and lossy format conversions. Transform domain techniques are generally classified into [4].

1. Discrete Fourier transformation technique (DFT).
2. Discrete cosine transformation technique (DCT).
3. Discrete Wavelet transformation technique (DWT)

**3. Distortion Techniques**. Distortion techniques want information of the first cover image throughout the cryptography method wherever the decoder functions to see for variations between the first cover image and also the distorted cover image so as to restore the key message. The encoder adds a sequence of changes to the cover image. So, data is represented as being keep by signal distortion [5].Using this method, a stego object is made by applying a sequence of modifications to the cover image. This sequence of modifications is use to match the key message needed to transmit .The message is encoded at pseudo-randomly chosen pixels. If the stego-image is completely different from the cover image at the given message component, the message bit may be a "1." otherwise, the message bit may be a "0." The encoder will modify the "1" price pixels in such a way that the statistical properties of the image don't seem to

be affected. However, the requirement for causing the cover image limits the advantages of this method. In any steganographic technique, the cover image ought to ne'er be used over once. If associate attacker tampers with the stego-image by cropping, scaling or rotating, the receiver will simply discover it. In some cases, if the message is encoded with error correcting data, the modification will even be reversed and also the original message will be recovered [6].

**a. Least important Bit (LSB):** LSB is that the lowest bit during a series of numbers in binary. E.g. within the binary number: 10110101, the least important bit is way right one. The LSB primarily based Steganography is one of the steganographic strategies that is employed to infix the key information in to the least important bits of the component values in a cover image. e.g. 210 will be hidden within the initial eight bytes of 3 pixels during a 24 bit image.

## II.LITERATURE SURVEY

**Payal Jainb et al.** [7] provides analysis of Least Significant Bit (LSB) based Steganography and Discrete Cosine Transform (DCT) based Steganography. LSB based Steganography insets the text message in lsb of digital data. Converting a picture from a format like BMP or GIF that reconstructs the initial message precisely to a JPEG that doesn't so back might destroy the knowledge hidden within the LSBs. DCT based Steganography embed the text message in lsb bits of the discrete cosine (DC) coefficient of digital picture. When information is hidden inside video, the program hiding the information usually performs the DCT. DCT slightly changes each of the images in the video. An implementation of both these methods and their performance analysis has been done for LSB based and DCT based stego images using PSNR ratio shows that PSNR ratio of DCT based Steganography scheme is high as compared to LSB based Steganography scheme for all types of images. DCT based Steganography scheme works perfectly with minimal distortion of the image quality as compared to LSB based. DCT primarily based image Steganography theme is usually recommended owing to the minimum distortion of image quality.

**W. Lin et. al.** [8] proposed an intelligent watermarking by invoking particle swarm optimization (PSO) technique in wavelet domain. The cover image is transformed into frequency bands and the coefficients are randomly selected from different sub bands to make up a block to increase the security so that an unauthorized party is unable to remove the watermark or to detect the existence of the watermark. This concept is called significant difference of the wavelet coefficients quantization. The SDWCQ method decomposes the original image into wavelet domain by 3-level. A block is constructed by taking every seven consecutive coefficients from LH3 sub band. *Nw*blocks are selected randomly and every block is embedded one watermark bit $wi \in \{1, -1\}$ . The normalized correlation coefficient (*NC*) is computed to find the existence of watermark, using the original watermark *wi* and extracted watermark *wi'*.

**B. Durga Devi et al.** [9] in their proposed system they have chosen a random pixel in a cover image and in that they took last two bits for encrypting the data. So, the data length of the secret message can be extended. In the proposed technique they have embedded a character with the help of only 2 pixels instead of using the 3 pixels. So we can insert more characters in a single image by using this technique. In old technique the main disadvantages of using LSB technique requires a fairly large cover image to create a usable amount of hiding space. Even nowadays uncompressed images of 800 x 600 pixels are not often used on the Internet, so using these might raise suspicion. But in their proposed system it can overcome the problem by inserting a character in last two bits of the byte. This shows the efficiency over the other existing systems

**I. Science et. al**. [10] proposed a digital watermarking algorithm with gray image based on 2 dimensions discrete wavelet and cosine transform. They transformed the cover image into discrete wavelet domain by decomposing it three times and then split the image into sub-blocks and transformed every block into discrete cosine domain. Watermark was also transformed into discrete cosine domain and was embedded in to the cover image by altering its transform coefficients..

**Yu, Y.H et al.** [11], proposed a steganographic method for hiding a colour or a gray scale secret image in a true colour host image. There are three image-hiding types in the scheme: hiding a colour secret image in a true colour image, hiding a palette-based 256-color secret image in a true colour image, and hiding a gray scale image in a true colour image, which depends on the secret image that is to be hidden in a true colour host image. In all three types of hiding, secret data are encrypted by data encryption standard (DES) method before they are embedded into the host image. The hiding capacity and good image quality are the results in that proposed method.

**Wang et. al.**[12]proposed a blind watermarking method with particle swam optimization (PSO) on discrete wavelet transform (DWT). The watermark is embedded in a digital image by quantization of adjacent wavelet coefficients on wavelet trees and can be extracted blindly. PSO is employed to achieve the robustness and imperceptibility. A host image $Iw \times Ih$ is transformed into frequency domain by *L*-level DWT, where *Iw* and *Ih* denote the width and the height of the host image, respectively. Wavelet trees are constructed with root.

Before embedding the watermark, wavelet trees and watermark bits are shuffled in a pseudorandom manner.

**Li Leung et al.** [13].introduced a new image hiding scheme by exploring the block similarity between the cover-image and the secret-image. Both of the duvet image and also the secret image area unit 8- bit grey scale pictures. Supported the block distinction, the most effective match cover image block of the key image is chosen. Then, the error-matrix, the normalized-error-matrix, the difference-degree and also the quantized-error-matrix between the cover-image block and secret-image block are computed. After that, the normalized-error-matrix and quantized error- matrix is used to modify the cover-image block. This scheme provides a high quality and the secret-image is completely extracted.

**Xiaoxia Li et al. [14]** .proposed the use of Particle Swarm Optimization algorithm to find an optimal substitution matrix which would encrypt the entire secret message. The method also used modified quantization table to increase the capacity of the stego object.

**J. C. Lin et al. al. [15],** proposed a simple and fast method for high-hiding capacity based on the modulus operation. A good image vision quality is achieved by exploitation this methodology while not the requirement for post-processing. Although, this methodology is nearly as straightforward because the LSB methodology in each embedding and extracting, it's a high-hiding capability during which it will hide a 256 × 256 or 256 × 512 image during a 512 × 512 host image.

**III. SIMULATION TOOL AND RESULT ANALYSIS (a) Setup Tool:** It is a MATLAB (matrix laboratory). The Performance analysis of MATLAB version 14 (R2008a) i.e. used for this thesis Implementation of data mining provides processor optimized libraries for fast execution and computation and performed on input cancer dataset. It is a uses of just in time compilation tools in mat lab and give execution fast speeds in programming languages. It can also further advantage of multi core and computers use multi processor. Matrix laboratory provides many multi threaded linear algebra and numerical function. These functions physically perform on several computational threads in a single matrix laboratory, to perform quicker on multicore computers.

**(b) Result Analysis:** PSNR Values Analysis: Exiting method PSO less PSNR but our proposed method BPPCM good PSNR. In this experimentation used airplane image, city image etc (Cover image in jpg and size NxN) and uit_logo image and email icon image (secret data image in jpg and size MxM).

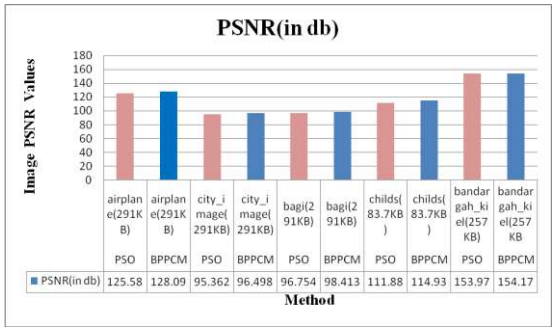


Figure 2 PSNR Comparison Graph between PSO and BPPCM

**2. Analysis of Normal Correlation:** Exiting method PSO and our proposed method BPPCM average normal correlation between images. In this experimentation used airplane image, city image etc. (cover image in jpg and size NxN) and uit_logo image and email_icon image (secret data image in jpg and size MxM).

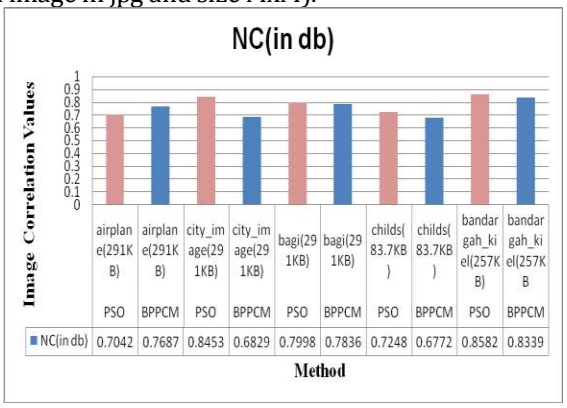


Figure 3 NC Comparison Graph between PSO and BPPCM

## IV. CONCLUSION

Digital image Steganography using bit particle position changing method (BPPCM).our proposed technique would be in minimize total computation time and improved Peak single to noise ratio. The BPPCM gives enhanced image data show in result and it is also evaluate to the PSO. It is not as much of level to attack evaluate to PSO. Algorithm optimizes the watermark embedding function so as to make the watermarked image good robust. Certain variations can be introduced into the algorithm to make it more efficient by improving its local and global search ability thereby increasing the robustness and imperceptibility of the watermark. Wavelet domain has been used which has a number of advantages over spatial domain like high hiding capacity, more robustness and high compatibility. PSO has been used as an optimizing function. The particle swarm Optimization is analysis on DCT but our proposed method get enhanced of PSNR and compared to existing method. So the BPPCM algorithms get better the performance and minimize total computation time compared to PSO. The performance

measure to evaluate the entire proposed technique is PSNR and NC. The proposed method obtained better PSNR values as compare optimization technique PSO. Digital image Steganography method provides a reliable image and it is providing good protected digital image or secrete data or information. It is providing secures in data hiding in digital image. It is good robustness, ownership and decreasing the computation time with improved PSNR. The future work would be in minimize total computation time and using video and audio .In future work on real time video and location map find best possible robustness.

## REFERENCES

[1]. G. J. Simmons. The prisoner's problem and the subliminal channel. Advances in Cryptology: Proceedings of CRYPTO'83, pages 51-67, 1983.
[2]. Ramanpreet Kaur, Prof. Baljit Singh "Survey and Analysis of Various Steganographic Techniques" International Journal of Engineering Science & Advanced Technology Volume-2, Issue-3, 561 – 566, May-June 2012.
[3]. L. Robert, C. Science, and G. A. College, "A Study on Digital Watermarking Techniques," vol. 1, no. 2, pp. 223–225, 2009.
[4]. N. F. Johnson, S. Katzenbeisser. "A Survey of steganographic techniques. " in Information Hiding Techniques for Steganography and Digital Watermarking, S. Katzenbeisser and F. Petitcolas, Ed. London: Artech House, pp. 43-78, 2000.
[5]. H. S. Majunatha Reddy and K.B. Raja. "High capacity and security Steganography using discrete wavelet transform." International Journal of Computer Science and Security. pp. 462-472, 2009.
[6]. S. C. Katzenbeisser. "Principles of Steganography." in Information Hiding Techniques for Steganography and Digital Watermarking, S. Katzenbeisser and F. Petitcolas, Ed. London: Artech House, pp. 43-78, 2000,
[7]. Dr. Ekta Waliaa, Payal Jainb "An Analysis of LSB & DCT based Steganography ", Global Journal of Computer Science and Technology, 4 Vol. 10 Issue 1 (Ver. 1.0), p4-8,
[8]. Y. Wang, W. Lin, and L. Yang, "An intelligent pso watermarking," no. July, pp. 11–14, 2010.
[9]. M. Sivaram ,B. DurgaDevi J. Anne Steffi " Steganography Of Two Lsb Bits" International Journal of Communications and Engineering Volume 01– No.1, Issue: 01 March, p82-87, 2012.
[10]. I. Science and W. No, "A Digital Image Watermarking Algorithm Based on Discrete Wavelet Transform and Discrete Cosine Transform Yang Qianli," pp. 1102–1105,2005.
[11]. Yu, Y.-H., C.-C. Chang and I.-C. Lin ,"A new steganographic method for color and grayscale image hiding." Computer Vision and Image Understanding 107(3): 183-194, 2007.
[12]. Y. Wang, W. Lin, and L. Yang, "A Blind Pso Watermarking Using Wavelet Trees Quantization," pp. 10–13, 2011.
[13]. Li, S.-L., K.-C. Leung, L. Cheng and C.-K. Chan "A novel image-hiding scheme based on block difference." Pattern Recognition 39(6): 1168-1176, 2006.
[14]. Li, X. and Wang, J. 2007. A steganographic method based upon JPEG and particle swarm optimization algorithm. Elsevier. pp. 3099-3109, 2007.
[15]. Thien, C.-C. and J.-C. Lin (2003). "A simple and high-hiding capacity method for hiding digit-by-digit data in images based on modulus function." Pattern Recognition 36(12): 2875-2881.