IJCSE International Journal of Computer Sciences and Engineering Open Access
Research Paper Volume-2, Issue-7 E-ISSN: 2347-2693

# Color Image Steganography Using Discrete Wavelet Transformation and Optimized Message Distribution Method

Juned Ahmed Mazumder[1*], Kattamanchi Hemachandran[2]

[1*]*Department of Computer Science, Assam University, Silchar, Assam, India, junedmazumder29@yahoo.in*
[2] *Department of Computer Science, Assam University, Silchar, Assam, India, khchandran@rediffmail.com*

**www.ijcseonline.org**

Received: 24 /06/ 2014 Revised: 30/07/ 2014 Accepted: 20 /07/ 2014 Published: 30 /07/ 2014

***Abstract:*** Steganography is the science of concealing secret information into any digital media such as images, audio, video etc so that no eavesdropper can empathies this secret communication. In this paper we have propounded a high security steganographic technique using discrete wavelet transformation and optimized message dispersing method. Here we have used Haar wavelet transformation which decomposes the cover image into high frequency and low frequency information and high frequency information contains information about the edges, corners etc. of the image where we have dispersed our secret information. Secret Message is inserted into all the color components of high frequency sub-bands that are Red, Green and Blue color components starting from the last column of each of the color components from top to bottom depending upon the length of the message. To measure the imperceptibility of the proposed steganography method we have used MSE and PSNR. For this experiment we have taken four image formats: PNG, BMP, JPEG and TIFF and we have inserted the secret message of sizes starting from 2 KB to 20 KB and evaluated their corresponding MSR and PSNR using standard method. Besides the analysis of MSE and PSNR we have also evaluated the message insertion and the message extraction time. Our experimental result shows that the MSE and Capacity are improved with acceptable PSNR compared to other methods.

***Keywords:*** Steganography, DWT, MSE, PSNR, PNG, BMP, JPEG, TIFF

## 1. INTRODUCTION

Steganography is one of the most effective secured data communication. It provides a protection for secret messages by embedding them into digital media and making them inconspicuous and invisible to eavesdroppers [1]. In contrast to the traditional cryptography whose purpose is to hide the content of secret messages being exchanged between the two communicating parties, the purpose of steganography is to hide not only the content but also its very existence. Therefore, it can offer a better security in many ways. Two other technologies that are closely related to steganography are watermarking and fingerprinting [2] which involves the embedding of information in some media. These technologies are mainly concerned with the protection of intellectual property, thus the algorithms have different requirements than steganography [3]. The kind of information hidden in objects when using watermarking is usually a signature to signify origin or ownership for the purpose of copyright protection [4]. With fingerprinting on the other hand, different, unique marks are embedded in distinct copies of the carrier object that are supplied to different customers [3].

The major goal of steganography is to enhance communication security by inserting secret message into the digital image, modifying the nonessential pixels of the image [5]. The image after the embedding of the secret message, so-called stego-image, is then sent to the receiver through a public channel. The most basic type of steganography is the Least significant Bit (LSB) replacement technique. The LSB planes replace the least significant bits of the cover image with secret data. For k-bit LSB substitution, the exhaustive search method would take a long period of time to find an optimal substitution matrix [6]. On the other hand depending on image characteristics LSB insertion method is divided into fixed size and variable size. In fixed length technique same number of bits in each pixel of cover image and another one variable number of bits in each pixel are used for message [7]. It is the most common and also it is a high capacity steganographic method but it is not so much robust against certain attacks like low pass filtering and image compression. The JPEG format uses discrete cosine transform (DCT) to transform successive 8 × 8 pixel blocks of the image into 64 DCT coefficients. Here, LSBs of the quantized DCT coefficients are used as redundant bits [8,]. This technique is much robust against certain attacks like filtering and image compression. The most important requirement is that a steganographic algorithm has to be imperceptible. There are some set of criteria to further define the imperceptibility of an algorithm. These requirements are as follows [3]:

**Invisibility** – The invisibility of a steganographic algorithm is the basic requirement, since the strength of steganography lies in its ability to be unnoticed by the human eye. The moment that one can see that an image has been tampered with, the algorithm is compromised

**Payload capacity** – Unlike watermarking, which needs to embed only a small amount of copyright information, steganography aims

 

at hidden communication and therefore requires sufficient embedding capacity.

**Robustness against statistical attacks** – Statistical steganalysis is the practice of detecting hidden information through applying statistical tests on image data. Many steganographic algorithms leave a 'signature' when embedding information that can be easily detected through statistical analysis. To be able to pass by a warden without being detected, a steganographic algorithm must not leave such a mark in the image as be statistically significant.

**Robustness against image manipulation** – In the communication of a stego image by trusted systems, the image may undergo changes by an active warden in an attempt to remove hidden information. Image manipulation, such as cropping or rotating, can be performed on the image before it reaches its destination. Depending on the manner in which the message is embedded, these manipulations may destroy the hidden message. It is preferable for steganographic algorithms to be robust against either malicious or unintentional changes to the image.

**Independent of file format** – With many different image file formats used on the Internet, it might seem suspicious that only one type of file format is continuously communicated between two parties. The most powerful steganographic algorithms thus possess the ability to embed information in any type of file. This also solves the problem of not always being able to find a suitable image at the right moment, in the right format to use as a cover image.

**Unsuspicious files** – This requirement includes all characteristics of a steganographic algorithm that may result in images that are not used normally and may cause suspicion. Abnormal file size, for example, is one property of an image that can result in further investigation of the image by a warden.

## 2. RELATED WORKS

In the last couple of years, enormous research efforts have been invested in the development of digital image steganographic techniques. Hajizadeh et al. [9] proposed a block-based and high capacity steganographic method which is the extended form of Zhang and Wang's EMD method and it uses eight modification directions to hide multiple secret bits into a cover pixel pair at a time. In this method blocks are selected in a random order scheme of the image, to eliminate the bias between the image and the confidential data. Simulation results shows that the method can obtain various hiding capacities of 1 to 5 bpp and corresponding good visual qualities of either 53.68 to 30.05 dB or 52.97 to 29.40 dB in the case of 4 × 4 or 8 × 8 blocks, respectively.

Singh et al. [10] proposed a two layer data hiding method for RGB color image. This method is an enhancement of Wu and Tsai's method (PVD) and J. K. Mandal's method (Color Image Steganography Based on Pixel Value Differencing in Spatial Domain). The method used two layer data hiding and LZW compression technique to enlarge the data hiding capability. In second layer of data hiding, left pixel of the pixel pair is considered as right pixel and vice-versa to improve the stego image quality. Stego image in this technique is totally indistinguishable from the original image by the human eye and it is secure against the RS detection attack. Beside this it also avoids falling of boundary problem of the pixels.

Saraireh [11] employs cryptographic algorithm together with steganography for provides high level of security, scalability and speed. In this method filter bank cipher is used to encrypt the secret text message then a discrete wavelet transforms (DWT) based steganography is employed to hide the encrypted message in the cover image by modifying the wavelet coefficients. The performance of the proposed system is evaluated using peak signal to noise ratio (PSNR) and histogram analysis. The simulation results show that, the proposed system provides high level of security. The results showed that, the PSNR of the proposed system are high, which ensure the invisibility of the hidden message through the cover image.

Bandyopadhyay et al. [12] uses genetic algorithm (GA) with steganography technique in order to get better the quality of stego image and robustness of the steganography we have built up a competent optimal robust steganography technique. The watermarks are implanted into the HL and LH frequency coefficients in bi-orthogonal wavelet transform (BWT). In order to achieve a balance between robustness and fidelity, the coefficients at widespread sub-bands HL and LH are selected for watermark embedding based on artificial intelligent technique. The embedding process is carried out in two cases based on the embedded bit value of the Hidden Image that can be either 0 or 1. For embedding of each bit, we use HL and LH sub band one after another continuously until the total hidden image get embedded. At first we embed the height and width information i.e. two integer values into first 16 pixels then we embed pixel information of Hidden Image.

Mamta and Sandhu [13] proposed an Enhanced form of LSB based Steganography which embeds data in only 2-3-3 LSBs of red, green, blue components respectively of each pixel. This helps to achieve better capacity and immunity to suspicion. In addition, it provides means for secure data transmission using Data Encryption Standard algorithm.

Balasubramanian et al. [14] proposed a high payload image steganography with reduced distortion using octonary pixel pairing scheme based on the principle that edge areas can tolerate a larger number of changes than smooth areas and hence hold more number of bits. So the edge areas are identified first in the region selection phase. Subsequently, the number of bits that can be embedded inside each pixel pair is determined by referring to the range table. If the regions are sufficiently large enough for hiding the given secret message, then secret data is embedded into the selected regions. Otherwise the smooth regions are utilized for hiding after using all the edge regions and Data hiding is performed as per the Octonary PVD scheme. Finally to improve the perceptual quality and the statistical undetectability of the stego image, the pixel re-adjustment phase is implemented. Then finally some post processing is done to obtain the stego image.

Yang [15] used radius weight mean (RWM) and the feature-embedding technique to present a novel watermarking scheme for color images. Stego-images generated by the proposed scheme are robust against most common image-processing operations, such as compression, color quantization, bit truncation, noise addition, cropping, blurring, mosaicking, zigzagging, inversion, (edge) sharpening, and so on. The feature-embedding technique consists of two procedures: the X-sampling technique and the directional-sampling technique. Specifically, two data bits can be embedded into a host block by using the X-sampling technique followed by the directional-sampling technique if neither technique violates the RWM decision policy during bit embedding..

Chakraborty et al. [16] implemented a lossless image steganography approach to minimized distortion of cover image due to strganographycal process. In this method the cover image is not be changes at all after implementation of staganography approach. To maintain less distortion of cover image they used DNA sequencing, Sudoku solution matrix and (t, n)-threshold sharing system. DNA sequencing is used to represent secret image by minimum no. of bits and Sudoku solution matrix represents the cover image. Here 16×16 Sudoku solution matrix is used and matrix is divided into 4×4 blocks. Secret image is embedded into cover image by

 

camouflaging process. Camouflaging is done by (t, n)-threshold sharing system.

Shejul et al. [17] proposed a steganography method based on DWT using biometrics, the biometric feature used to implement steganography is skin tone region of images. The secret data is embedded within skin region of image that provides an excellent secure location for data hiding. For this skin tone detection is performed using HSV (Hue, Saturation and Value) color space. Additionally secret data embedding is performed using frequency domain approach - DWT (Discrete Wavelet Transform), Secret data is hidden in one of the high frequency sub-band of DWT by tracing skin pixels in that sub-band. Different steps of data hiding are applied by cropping an image interactively. Cropping results into an enhanced security than hiding data without cropping i.e. in whole image, so cropped region works as a key at decoding side. Also they [18] proposed a steganographic method based on biometrics and the biometric feature used to implement Steganography is skin tone region of images. Secret data is hidden in one of the high frequency sub-band of DWT by tracing skin pixels in that sub-band. For data hiding two cases are considered, first is with cropping and other is without cropping. In both the cases different steps of data hiding are applied either by cropping an image interactively or without cropping i.e. on whole image. Both cases are compared and analyzed from different aspects. This is concluded that both cases offer enough security. Main feature of with cropping case is that this results into an enhanced security because cropped region works as a key at decoding side. Whereas without cropping case uses embedding algorithm that preserves histogram of DWT coefficient after data embedding also by preventing histogram based attacks and leading to a more security.

Chen and Lin [19] embed the secret messages in frequency domain using discrete wavelet transformation. The algorithm is divided into two modes and 5 cases. Unlike the space domain approaches, secret messages are embedded in the high frequency coefficients resulted from Discrete Wavelet Transform. Coefficients in the low frequency sub-band are preserved unaltered to improve the image quality. Some basic mathematical operations are performed on the secret messages before embedding. These operations and a well-designed mapping Table keep the messages away from stealing, destroying from unintended users on the internet and hence provide satisfactory security.

Tolba et al. [20] presents a cover-screw algorithm based on the wavelet based fusion. In this method the wavelet decomposition of both the cover image and the secret message are merged into a single fused result using an embedding strength factor. The algorithm also applies a preprocessing step on the cover image to shrink the range of the pixels components in order to guarantee that the embedded message will be recovered with acceptable accuracy. Experimental results showed the high invisibility of the model as well as the large hiding capacity it provides.

Safy et al. [21] proposed a novel technique for hiding data in digital images by combining the use of adaptive hiding capacity function that hides secret data in the integer wavelet coefficients of the cover image with the optimum pixel adjustment (OPA) algorithm. The coefficients used are selected according to a pseudorandom function generator to increase the security of the hidden data. The OPA algorithm is applied after embedding secret message to minimize the embedding error. This system showed high hiding rates with reasonable imperceptibility compared to other steganographic systems.

Raja et al. [22] proposed a novel steganographic scheme called robust image adaptive steganography using integer wavelet transform (RIASIWT), which is capable of hiding large volumes of data without causing any perceptual degradation of the cover image. The scheme embeds the payload in every non-overlapping 4times4 blocks of the low frequency band of cover image, two pixels at a time, one on either sides of the principal diagonal. Tests for the similarity between the condition number of the cover image and the stego image are done for further embedding also perform cover image adjustment before embedding the payload in order to ensure lossless recovery. Embedding done in the low frequency bands ensures robustness against attacks such as compression and filtering.

Bhattacharya et al. [23] convert the cover image into frequency domain using DWT which decomposed the cover image into four sub bands. Two secret images are embedded within the HL and HH sub bands respectively. During embedding secret images are dispersed within each band using a pseudo random sequence and a Session key. Secret images are extracted using the session key and the size of the images. In this approach the stego image generated is of acceptable level of imperceptibility and distortion compared to the cover image and the overall security is high.

Torres-Maya et al. [24] used Integer Wavelet Transform (IWT) to obtain wavelet coefficients in which the data hiding (embedding) is realized in bit planes. To increase data hiding capacity while keeping the imperceptibility of the hidden data, the replaceable IWT coefficient areas are defined by a complexity measure used in the Bit-Plane Complexity Segmentation Steganography (BPCS). The system shows a high data hiding capacity (more than 2 bpp in many case), while keeping a high fidelity of stego image (more than 35 dB of PSNR). Also Error Control Coding is introduced to the system to make the system robust enough to some distortion caused by non-ideal communication channel, which can reduce the Bit Error Rate (BER) of extracted hidden data when the stego image receive some channel distortion.

Chen and Yuan [25] conceal a secret image into the cover image of the same size without noticeable degradation. In this approach, discrete wavelet transform (DWT) and set partitioning in hierarchical trees (SPIHT) codec are used to obtain a low bit rate and high reconstructed quality image compression. In the embedding process, an adaptive phase modulation (APM) mechanism and discrete Fourier transform (DFT) were adopted for secret data embedding. Simultaneously, nearest phase modulations (NPM) was used to improve the imperceptibility and decrease degradation of cover image. Both the chaotic mechanism (CM) and frequency hopping (FH) structure were hired to enhance the security of the scheme.

Cheng and Huang [26] presented an additive approach to transform-domain information hiding and the performance analysis for images and video. The watermark embedding method is designed to satisfy the perceptual constraints and improve the delectability as well as the information embedding rate. The statistical behaviors of sub-band coefficients are modeled by the generalized Gaussian distribution. The structure of the optimum detection is built and the performance of the exact asymptotic detection is evaluated using large deviation theory.

## 3. PROPOSED METHOD

In the proposed method we have used discrete wavelet transformation for converting image from its spatial domain to frequency domain. A **wavelet** is a wave-like oscillation with amplitude that starts out at zero, increases, and then decreases back to zero. Unlike the Fourier transform, which only construct a frequency representation of a signal, the wavelet transform is able to construct a time-frequency representation of a signal simultaneously. The main purpose of converting an image into frequency domain during steganography is that when we insert our

 

secret information into frequency domain it is very difficult to detect steganography. In discrete wavelet transformation for images we separate the high frequency and low frequency information. Low frequency information contains information about the smoother places of the image and it is very sensitive information where slight modification affects the reconstructed (Stego image) image. On the other hand high frequency information contains the information about the edges, corners, etc of the image hence modification in this information results less noise in the reconstructed image. The discrete wavelet transform (DWT) is a linear transformation that operates on a data vector whose length is an integer power of two, transforming it into a numerically different vector of the same length. It is a tool that separates data into different frequency components, and then studies each component with resolution matched to its scale [27]. DWT [28] is computed with a cascade of filters followed by a factor 2 sub sampling

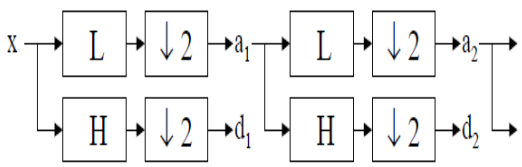


Fig. 1: DWT Tree

*H* and *L* denotes high and low-pass filters respectively, ↓2 denotes sub sampling. Outputs of this filters are given by equations (1) and (2)

$$a_{j+1}[p] = \sum_{n=-\infty}^{+\infty} l[n-2p]a_j[n] \quad \text{..... (1)}$$

$$d_{j+1}[p] = \sum_{n=-\infty}^{+\infty} h[n-2p]a_j[n] \quad \text{..... (2)}$$

Elements $a_j$ are used for next step (scale) of the transform and elements $d_j$, called wavelet coefficients, determine output of the transform. *l[n]* and *h[n]* are coefficients of low and high-pas filters respectively One can assume that on scale *j+1* there is only half from number of *a* and *d* elements on scale *j*. This causes that DWT can be done until only two $a_j$ elements remain in the analyzed signal These elements are called scaling function coefficients. DWT algorithm for two-dimensional pictures is similar. The DWT is performed firstly for all image rows and then for all columns (Fig.2).

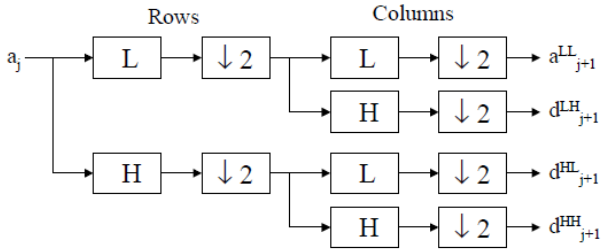


**Fig. 2.** Wavelet decomposition for two-dimensional pictures.

The main feature of DWT is multiscale representation of function. By using the wavelets, given function can be analyzed at various levels of resolution. The DWT is also invertible and can be orthogonal [27]. In this proposed method we have used Haar wavelet transformation. It was proposed by the mathematician Alfrd Haar in 1909. At each level the Haar transform decomposes a discrete signal into two components with half of its length: an approximation and a detail component. The first level of approximation $a^1=(a_1,a_2,..a_{N/2})$ is defined as

$$a_m = \frac{X_{2m-1} + X_{2m}}{2} \quad \text{..... (3)}$$

for m= 1,2,3,.....N/2 , where X is the input signal. The multiplication of 1/2 ensures that the Haar transform preserves the energy of the signal.

The first level detail $d^1 = (d_1,d_2,..d_{N/2})$ is

$$a_m = \frac{X_{2m-1} - X_{2m}}{2} \quad \text{..... (4)}$$

Let us take an example: X=(4,6,8,10,13,9,3,3) , the first level approximation and detail components are

$a^1$ = (5,9,11,3)
$d^1$ = (-1,-1,2,0)
$a^2$ = (7,7)
$d^2$ =(-2,4)

Using this methodology we have developed a steganographic algorithm based on Discrete Wavelet Transformation and Optimized Message Distribution Method.

### 3.1. Message embedding algorithm

Step1: Apply 2D-Haar DWT to the cover image, where we get the four sub-bands which separate the high and low frequency information.

- When we apply Haar wavelet to an image it is called 2D Haar wavelet. Let us consider an example for better understanding the 2-D Haar DWT of an image.

| | | | |
|---|---|---|---|
| 7 | 6 | 3 | 2 |
| 1 | 0 | 6 | 7 |
| 4 | 5 | 9 | 3 |
| 2 | 1 | 3 | 7 |

| | | | |
|---|---|---|---|
| (7+6)/2 | (3+2)/2 | (7-6)/2 | (3-2)/2 |
| (1+0)/2 | (6+7)/2 | (1-0)/2 | (6-7)/2 |
| (4+5)/2 | (9+3)/2 | (4-5)/2 | (9-3)/2 |
| (2+1)/2 | (3+7)/2 | (2-1)/2 | (3-7)/2 |

→

| | | | |
|---|---|---|---|
| 6.5 | 2.5 | 0.5 | 0.5 |
| 0.5 | 6.5 | 0.5 | -0.5 |
| 4.5 | 6 | -0.5 | 3 |
| 1.5 | 5 | 0.5 | -2 |

Horizontal Operation

| | | | |
|---|---|---|---|
| 6.5 | 2.5 | 0.5 | 0.5 |
| 0.5 | 6.5 | 0.5 | -0.5 |
| 4.5 | 6 | -0.5 | 3 |
| 1.5 | 5 | 0.5 | -2 |

→

| | | | |
|---|---|---|---|
| 3.5 | 4.5 | 0.5 | 0 |
| 3 | 5.5 | 0 | 0.5 |
| 3 | -2 | 0 | 0.5 |
| 1.5 | 0.5 | -0.5 | 2.5 |

Vertical Operation

 

$$A = \begin{bmatrix} 3.5 & 4.5 \\ 3 & 5.5 \end{bmatrix} \begin{bmatrix} 0.5 & 0 \\ 0 & 0.5 \end{bmatrix} = V$$

$$H = \begin{bmatrix} 3 & -2 \\ 1.5 & 0.5 \end{bmatrix} \begin{bmatrix} 0 & 0.5 \\ -0.5 & 2.5 \end{bmatrix} = D$$

- **A**: approximation area that includes information of the average of the image.
- **H**: horizontal area that includes information about the vertical edges/details in the image.
- **V**: vertical area that includes information about the horizontal edges/details in the image.
- **D**: diagonal area that includes information about the diagonal details, e.g., edges, corners, in the image.

After applying DWT to an image lina.jpg we get the following sub-bannds

Original Image DWT representation

Fig. 3: DWT representation of image —lena.png

Message normalization and distribution is as follows

Step2: Calculating the length of the message (n) and save it to the sub-bands H.
Step3: Convert the each character of the message into its ASCII format.
Step4: Then we optimize these values using 1-D, DWT
Step5: Then we insert these values to the coefficients of V and D sub-band. We do not insert message in H sub-bands because in this sub-band we hide others information like length of the message, secret key etc.
Step6: Message is inserted into all the color components of V and D sub-bands that are Red, Green and Blue color components. Message is inserted starting from the last column of each of the color components from top to bottom depending upon the length of the message.
Step7: If the message length is larger than the No. of rows of each of the color components of each of the sub-bands then rest of the normalized message will go to the second last column of the each component, in this way all the normalized message is to be distributed.
Step8: Insert the secret key in the H sub-band.
Step9: At the last step we have to take the Inverse Discrete Wavelet Transformation (IDWT) so that we can get the stego-image.

### 3.2. Message extraction algorithm

Step1: Apply 2D-Haar DWT to the stego image, where we get the four sub-bands which separate the high and low frequency information.
Step2: Get the first coefficient from the sub-band H for calculating the length of the message (n) and second coefficient for getting the secret key.
Step3: Then we get all the coefficients from V and D sub-band up to the length of the message which we have already calculated from the sub-band H.
Step4: Now apply inverse 1-D DWT to these coefficients to get the normalized ASCII format of the message character.
Step5: After that convert these normalized ASCII coefficients to character format.

## 4. EXPERIMENTAL ANALYSIS

To measure the imperceptibility of steganography several metrics are used. The metrics indicates how similar (or different) the stego-image compared with Cover Image. The following metrics are used in the literature including the work of [29]:
Mean Squared Error (MSE) is computed by performing byte by byte comparisons of the Cover Image and stego-image. The computation can be expressed as follows:

$$MSE(f,g) = \frac{1}{MN}\sum_{i=1}^{M}\sum_{j=1}^{N}(f_{ij} - g_{ij})^2 \quad \text{..... (5)}$$

Where M, N are the number of rows and columns in the original matrix, fij is the pixel value from cover Image, and gij is the pixel value from the stego-image. Higher value of MSE indicates dissimilarity between compared images.
Peak signal-to-noise ratio measures in decibels the quality of the stego-image compared with the Cover Image. The higher PSNR the better the quality. PSNR is computed using the following equation:

$$\mathrm{PSNR}(f,g) = 10\log_{10}\frac{255^2}{MSE(f,g)} \quad \text{..... (6)}$$

Besides the analysis of MSE and PSNR we have also calculated the message insertion and the message extraction time.
For this experiment we have taken four image formats: PNG, BMP, JPEG and TIFF and for each image format we insert ten secret messages of sizes starting from 2 KB to 20 KB and evaluate their corresponding MSR and PSNR. The following table describes the MSE and PSNR for different image formats and for different message size.

 

Table 1: Comparison between steganography using DWT and the Proposed Method (DWT + Optimized Message Distribution Method)

| Image Format | Image Size | Message Size (KB) | MSE | | PSNR | | Message Insertion Time (In sec) | | Message Extraction Time (In sec) | |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | DWT | Proposed method | DWT | Proposed Method | DWT | Proposed method | DWT | Proposed method |
| PNG | 131 | 2 | 0.09193 | 0.00230557 | 58.4958 | 74.503 | 0.04645 | 0.0775965 | 1.20287 | 0.989289 |
| PNG | 131 | 4 | 0.35538 | 0.00461081 | 53.6238 | 71.493 | 0.05936 | 0.135157 | 2.81804 | 1.7405 |
| PNG | 131 | 6 | 0.56482 | 0.00922309 | 50.6117 | 68.482 | 0.06112 | 0.469276 | 4.86875 | 3.31263 |
| PNG | 131 | 8 | 0.77647 | 0.00922309 | 49.2295 | 68.4822 | 0.66749 | 0.0482753 | 7.57466 | 3.5982 |
| PNG | 131 | 10 | 1.20272 | 0.0115293 | 47.3292 | 67.5128 | 0.76751 | 0.0454515 | 10.3154 | 4.11327 |
| PNG | 131 | 12 | 1.55031 | 0.0138356 | 46.2266 | 66.7208 | 0.84931 | 0.703861 | 13.788 | 4.80433 |
| PNG | 131 | 14 | 1.63718 | 0.0161428 | 45.9898 | 66.051 | 0.96525 | 0.0429986 | 17.7564 | 5.62473 |
| PNG | 131 | 16 | 1.9454 | 0.0186679 | 45.2407 | 65.4199 | 0.99449 | 1.23972 | 22.6268 | 6.35803 |
| PNG | 131 | 18 | 2.1363 | 0.0206785 | 44.8342 | 64.9756 | 1.05662 | 0.0474645 | 26.9396 | 7.21059 |
| PNG | 131 | 20 | 2.31199 | 0.023283 | 44.4909 | 64.4604 | 1.65987 | 0.0544336 | 33.2301 | 8.01349 |
| | | | | | | | | | | |
| BMP | 192 | 2 | 0.09193 | 0.00230557 | 58.4958 | 74.503 | 0.05178 | 0.0129431 | 0.877405 | 0.972742 |
| BMP | 192 | 4 | 0.35538 | 0.00461081 | 52.6238 | 71.493 | 0.05394 | 0.02603 | 1.55533 | 2.54800 |
| BMP | 192 | 6 | 0.56482 | 0.00691691 | 50.6117 | 69.7317 | 0.05733 | 0.0321908 | 2.07578 | 2.59616 |
| BMP | 192 | 8 | 0.77647 | 0.00922268 | 49.2295 | 68.4822 | 0.06690 | 0.0391846 | 2.75667 | 3.20428 |
| BMP | 192 | 10 | 1.20272 | 0.0115293 | 47.3292 | 67.5128 | 0.07480 | 0.0415222 | 3.52606 | 3.92203 |
| BMP | 192 | 12 | 1.55031 | 0.0138356 | 46.2266 | 66.7208 | 0.08117 | 0.0415829 | 4.17792 | 4.69734 |
| BMP | 192 | 14 | 1.63718 | 0.0161428 | 45.9898 | 66.051 | 0.08783 | 0.0419869 | 4.85999 | 5.40322 |
| BMP | 192 | 16 | 1.9454 | 0.0186679 | 45.2407 | 65.4199 | 0.09466 | 0.0450616 | 5.57951 | 6.23749 |
| BMP | 192 | 18 | 2.1363 | 0.0206785 | 44.8342 | 64.9756 | 0.15770 | 0.0482416 | 6.15232 | 6.83959 |
| BMP | 192 | 20 | 2.31199 | 0.023283 | 44.4909 | 64.4604 | 0.19477 | 0.0496969 | 6.88796 | 7.71274 |

 

Table 2: Comparison between steganography using DWT and the Proposed Method (DWT + Optimized Message Distribution Method)

| Image Format | Image Size (KB) | Message Size | MSE | | PSNR | | Message Insertion Time | | Message Extraction Time | |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | DWT | Proposed method | DWT | Proposed Method | DWT | Proposed method | DWT | Proposed method |
| JPEG | 101 | 2 | 0.233181 | 0.00230557 | 54.453 | 74.503 | 0.0703104 | 0.036897 | 1.2429 | 0.967086 |
| JPEG | 101 | 4 | 0.403995 | 0.00461081 | 52.067 | 71.493 | 0.0771458 | 0.047835 | 2.72391 | 1.70156 |
| JPEG | 101 | 6 | 0.691771 | 0.00691691 | 49.731 | 69.7317 | 0.079376 | 0.055922 | 4.7325 | 2.43255 |
| JPEG | 101 | 8 | 0.933584 | 0.00922268 | 48.429 | 68.4822 | 0.080747 | 0.067597 | 7.23236 | 3.17237 |
| JPEG | 101 | 10 | 1.12332 | 0.0115293 | 47.625 | 67.5128 | 0.0851928 | 0.074345 | 10.2997 | 4.01008 |
| JPEG | 101 | 12 | 1.39004 | 0.0138356 | 46.700 | 66.7208 | 0.0969749 | 0.083475 | 13.6823 | 4.71153 |
| JPEG | 101 | 14 | 1.63514 | 0.0161428 | 45.995 | 66.051 | 0.1573086 | 0.095912 | 17.8253 | 5.49103 |
| JPEG | 101 | 16 | 1.89649 | 0.0186679 | 45.351 | 65.4199 | 0.168771 | 0.141337 | 22.695 | 6.23867 |
| JPEG | 101 | 18 | 2.13874 | 0.0206785 | 44.829 | 64.9756 | 0.23987 | 0.245508 | 27.984 | 6.92889 |
| JPEG | 101 | 20 | 2.50382 | 0.023283 | 44.144 | 64.4604 | 0.29078 | 0.342702 | 31.4975 | 7.6895 |
| | | | | | | | | | | |
| TIFF | 207 | 2 | 0.164745 | 0.00230557 | 55.962 | 74.503 | 0.0503232 | 0.0402137 | 1.16967 | 0.940811 |
| TIFF | 207 | 4 | 0.485681 | 0.00461081 | 51.267 | 71.493 | 0.0555466 | 0.0442489 | 2.73012 | 1.69717 |
| TIFF | 207 | 6 | 0.745267 | 0.00691691 | 49.407 | 69.7317 | 0.0597502 | 0.0450942 | 4.76685 | 2.45016 |
| TIFF | 207 | 8 | 1.40609 | 0.00922268 | 46.650 | 68.4822 | 0.0669025 | 0.0476847 | 7.20858 | 3.16609 |
| TIFF | 207 | 10 | 1.80700 | 0.0115293 | 45.561 | 67.5128 | 0.074804 | 0.0495552 | 10.2564 | 3.93268 |
| TIFF | 207 | 12 | 2.14137 | 0.0138356 | 44.823 | 66.7208 | 0.0811713 | 0.0563617 | 13.7166 | 4.6986 |
| TIFF | 207 | 14 | 2.32473 | 0.0161428 | 44.467 | 66.051 | 0.0878323 | 0.0665469 | 17.6781 | 5.46061 |
| TIFF | 207 | 16 | 2.66345 | 0.0186679 | 43.876 | 65.4199 | 0.0946611 | 0.0734195 | 22.6537 | 6.23946 |
| TIFF | 207 | 18 | 2.83955 | 0.0206785 | 43.598 | 64.9756 | 0.1577032 | 0.0846147 | 27.0635 | 6.91924 |
| TIFF | 207 | 20 | 3.27993 | 0.023283 | 42.972 | 64.4604 | 0.194743 | 0.0991187 | 31.0987 | 7.78676 |

 

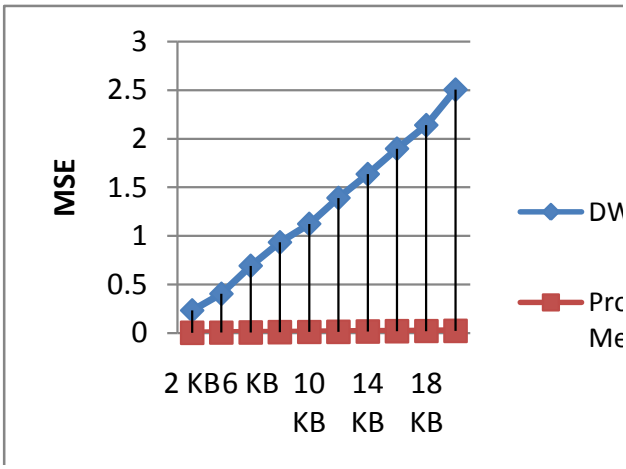


Fig. 4: MSE comparison of DWT and Proposed Method for PNG image format w.r.t. payload

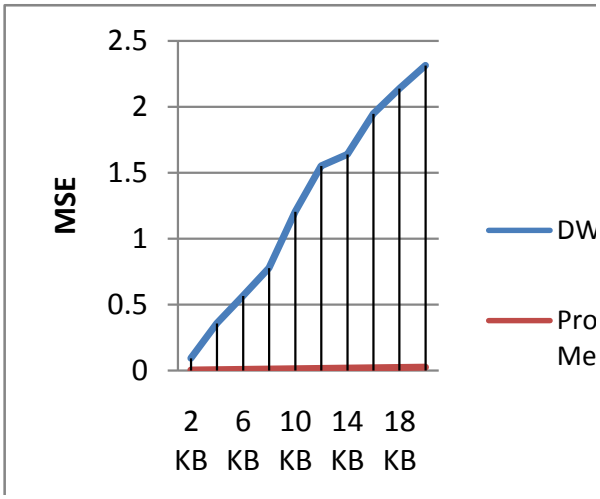


Fig. 5: MSE comparison of DWT and Proposed Method for BMP image format w.r.t. payload

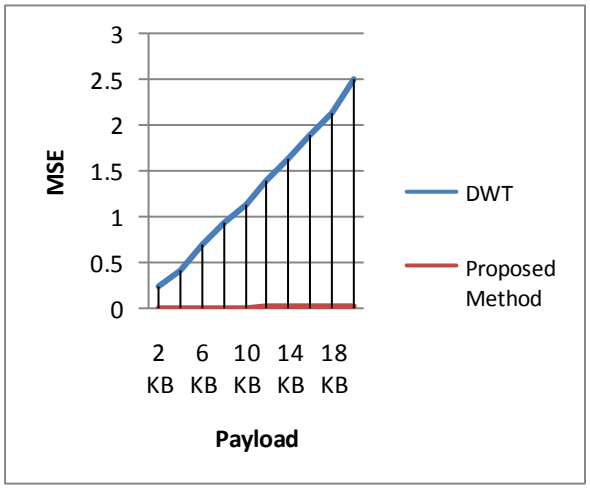


Fig. 6: MSE comparison of DWT and Proposed Method for JPEG image format w.r.t. payload

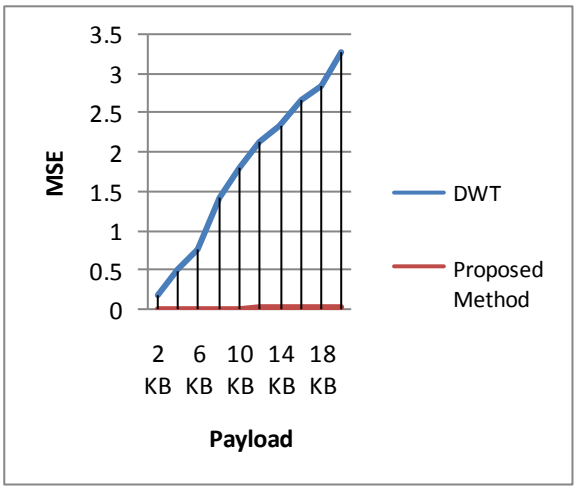


Fig. 7: MSE comparison of DWT and Proposed Method for JPEG image format w.r.t. payload

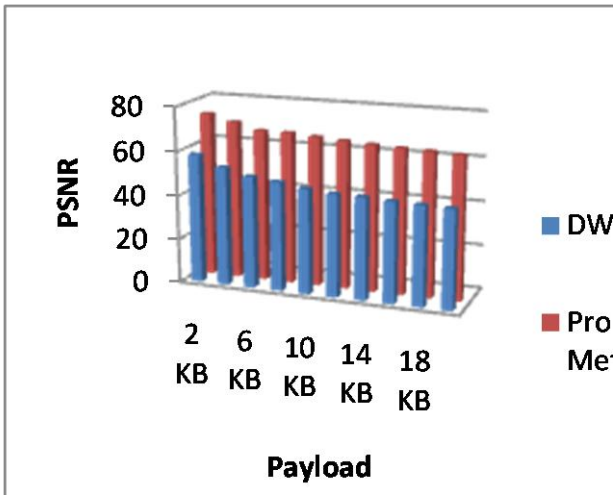


Fig. 8: PSNR comparison of DWT and Proposed Method for PNG image format w.r.t. payload

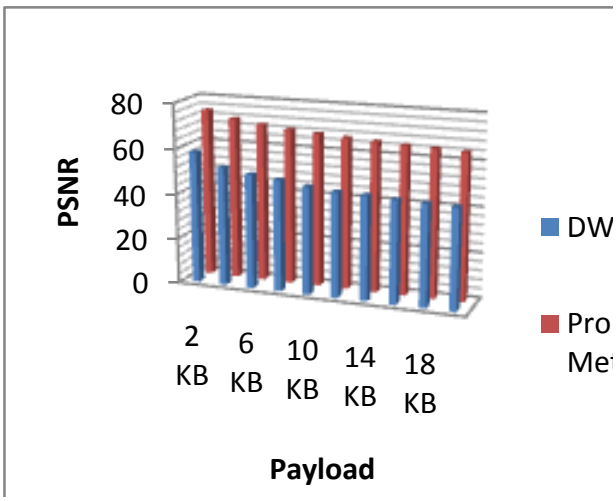


Fig. 9: PSNR comparison of DWT and Proposed Method for BMP image format w.r.t. payload

 

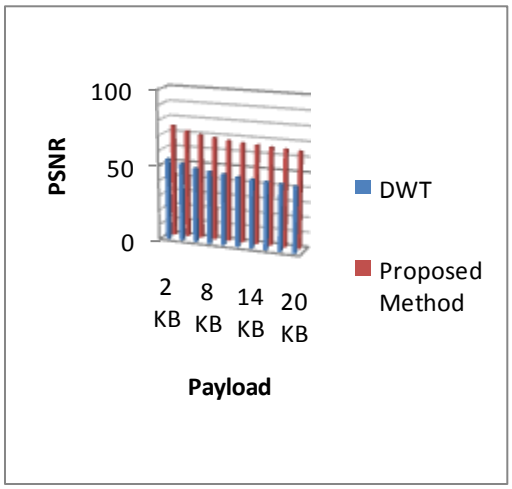


Fig. 10: PSNR comparison of DWT and Proposed Method for JPEG image format w.r.t. payload

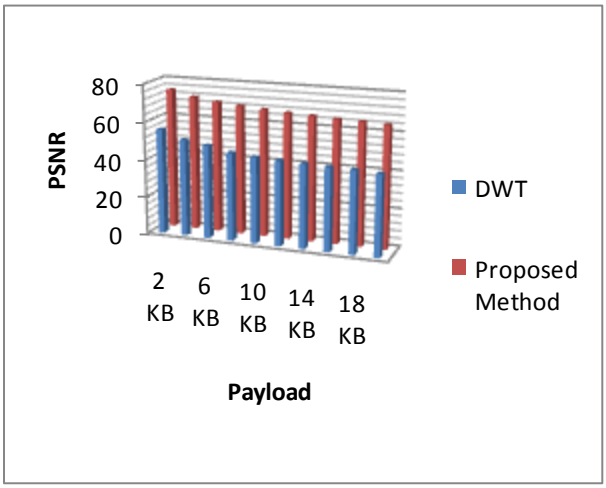


Fig. 11: PSNR comparison of DWT and Proposed Method for TIFF image format w.r.t. payload

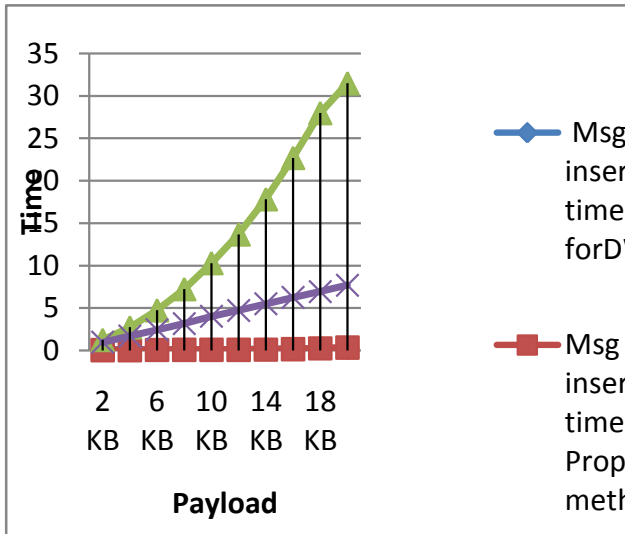


Fig. 12: Message insertion time and Message Extraction time for DWT and Proposed Method for PNG image format w.r.t. payload

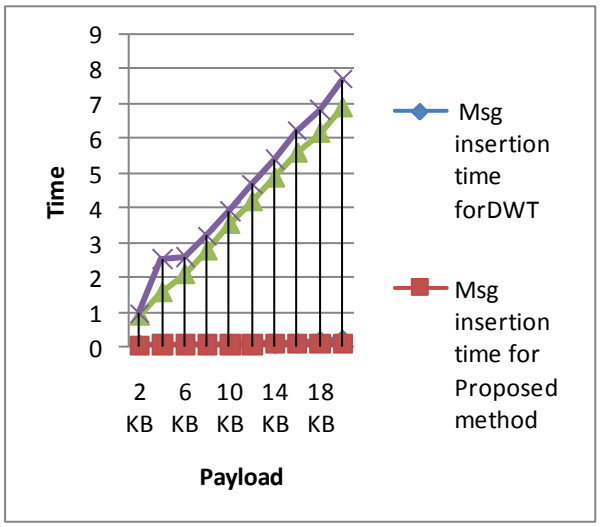


Fig. 13: Message insertion time and Message Extraction time for DWT and Proposed Method for BMP image format w.r.t. payload

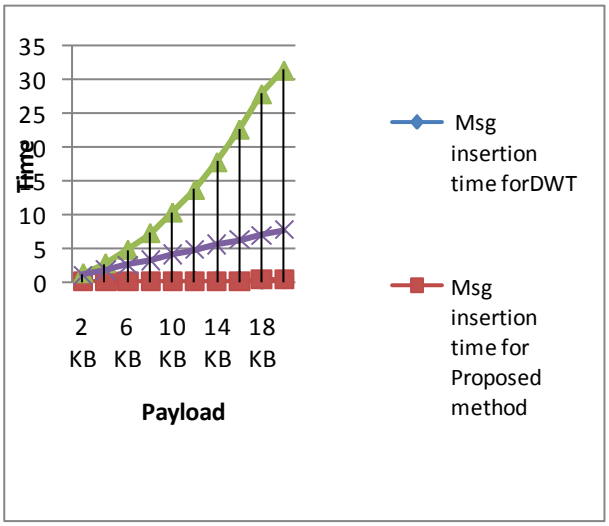


Fig. 14: Message insertion time and Message Extraction time for DWT and Proposed Method for JPEG image format w.r.t. payload

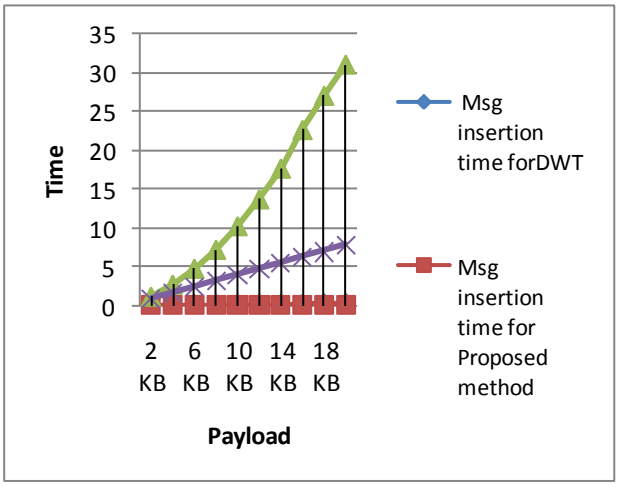


Fig. 15: Message insertion time and Message Extraction time for DWT and Proposed Method for TIFF image format w.r.t. payload

## 5. CONCLUSION

In the present study an attempt has been made to study the high capacity and security steganography of color images in the domain of discrete wavelet transformation. The secret message is normalized and distributed as a optimized way into the wavelet coefficient of the cover image. The security of the method is increased as the only high frequency coefficient of the cover image is used by the secret information. The capacity of the proposed algorithm is increased as coefficient of all three color component that is red, green and blue of each of the high frequency sub-band of the cover image are considered. The MSE and Capacity are improved with acceptable PSNR compared to the existing method.

## REFERENCES


[1] Tian, Lei; Zhou, Ke; Jiang, Hong; Liu, Jin; Huang, Yongfeng; and Feng, Dan, "An M-Sequence Based Steganography Model for Voice over IP" (2008). *CSE Technical reports.* Paper 68.

[2] Cheddad, Abbas, Joan Condell, Kevin Curran, and Paul Mc Kevitt. "Digital image steganography: Survey and analysis of current methods." *Signal Processing* 90, no. 3 (2010): 727-752.

[3] T Morkel, JHP Eloff and MS Olivier, "An Overview of Image Steganography," *in Proceedings of the Fifth Annual Information Security South Africa Conference (ISSA2005)*, Sandton, South Africa, June/July 2005 (Published electronically)

[4] Marvel, L.M., Boncelet Jr., C.G. & Retter, C., "Spread Spectrum Steganography", *IEEE Transactions on image processing, 8:08*, 1999

[5] Anderson, R.J. & Petitcolas, F.A.P., "On the limits of steganography", *IEEE Journal of selected Areas in Communications*, May 1998

[6] Marghny Mohamed, Fadwa Al-Afari and Mohamed Bamatraf, "Data Hiding by LSB Substitution Using Genetic Optimal Key-Permutation", International Arab Journal of e-Technology, Vol. 2, No. 1, pp. 11-17, January 2011

[7] Elham Ghasemi, Jamshid Shanbehzadeh, and Nima Fassihi, "High Capacity Image Steganography Based on Genetic Algorithm and Wavelet Transform", Intelligent Control and Innovative Computing, Vol. 10, pp. 395-402, 2012

[8] Fard, Amin Milani, M-R. Akbarzadeh-T, and Farshad Varasteh-A. "A new genetic algorithm approach for secure JPEG steganography." In *Engineering of Intelligent Systems, 2006 IEEE International Conference on*, pp. 1-6. IEEE, 2006.

[9] Hajizadeh, Hamzeh, Ahmad Ayatollahi, and Sattar Mirzakuchaki. "A new high capacity and EMD-based image steganography scheme in spatial domain." In *Electrical Engineering (ICEE), 2013 21st Iranian Conference on*, pp. 1-6. IEEE, 2013.

[10] Singh, Ravindra Kumar, Harsh Kumar Verma, and Charan Kamaljit Singh. "Bi-directional pixel-value differencing approach for RGB color image." In*Contemporary Computing (IC3), 2013 Sixth International Conference on*, pp. 47-52. IEEE, 2013.

[11] Saraireh, Saleh. "A SECURE DATA COMMUNICATION SYSTEM USING CRYPTOGRAPHY AND STEGANOGRAPHY." *International Journal of Computer Networks & Communications* 5, no. 3 (2013).

[12] Bandyopadhyay, Samir K., and Sabyasachi Pramanik. "Application of Steganography in Symmetric Key Cryptography with Genetic Algorithm."*INTERNATIONAL JOURNAL OF COMPUTERS & TECHNOLOGY* 10, no. 7 (2013): 1791-1799.

[13] Juneja, Mamta, and Parvinder S. Sandhu. "Data Hiding with Enhanced LSB Steganography and Cryptography for RGB Color Images."International Conference on Latest Computational Technologies (ICLCT'2013) June 17-18, 2013 London (UK)

[14] Balasubramanian, C., S. Selvakumar, and S. Geetha. "High payload image steganography with reduced distortion using octonary pixel pairing scheme."*Multimedia Tools and Applications* (2013): 1-23.

[15] Yang, Ching-Yu. "Robust Watermarking Scheme Based on Radius Weight Mean and Feature-Embedding Technique." *ETRI Journal* 35, no. 3 (2013).

[16] Chakraborty, Suman, Sudipta Roy, and Samir K. Bandyopadhyay. "Image Steganography Using DNA Sequence and Sudoku Solution Matrix."*International Journal* 2, no. 2 (2012).

[17] Shejul, Anjali A., and Umesh L. Kulkarni. "A DWT based approach for steganography using biometrics." In *Data Storage and Data Engineering (DSDE), 2010 International Conference on*, pp. 39-43. IEEE, 2010.

[18] Shejul, Anjali A., and Umesh L. Kulkarni. "A secure skin tone based steganography using wavelet transform." *International Journal of computer theory and Engineering* 3, no. 1 (2011): 16-22.

[19] Chen, Po-Yueh, and Hung-Ju Lin. "A DWT based approach for image steganography." *International Journal of Applied Science and Engineering* 4, no. 3 (2006): 275-290.

[20] Tolba, Mohamed Fahmy, MA-S. Ghonemy, IA-H. Taha, and Amal Said Khalifa. "High capacity image steganography using wavelet-based fusion." In *Computers and Communications, 2004. Proceedings. ISCC 2004. Ninth International Symposium on*, vol. 1, pp. 430-435. IEEE, 2004.

[21] El Safy, R. O., H. H. Zayed, and A. El Dessouki. "An adaptive steganographic technique based on integer wavelet transform." In *Networking and Media Convergence, 2009. ICNM 2009. International Conference on*, pp. 111-117. IEEE, 2009.

[22] Raja, K. B., S. Sindhu, T. D. Mahalakshmi, S. Akshatha, B. K. Nithin, M. Sarvajith, K. R. Venugopal, and Lalit M. Patnaik. "Robust image adaptive steganography using integer wavelets." In *Communication Systems Software and Middleware and Workshops, 2008. COMSWARE 2008. 3rd International Conference on*, pp. 614-621. IEEE, 2008.

[23] Bhattacharya, Tanmay, Nilanjan Dey, and S. R. Chaudhuri. "A novel session based dual steganographic technique using DWT and spread spectrum." *arXiv preprint arXiv:1209.0054* (2012).

[24] Torres-Maya, Silvia, Mariko Nakano-Miyatake, and Hector Perez-Meana. "An image steganography systems based on bpcs and iwt." In *Electronics, Communications and Computers, 2006. CONIELECOMP 2006. 16th International Conference on*, pp. 51-51. IEEE, 2006.

[25] Chen, Wen-Yuan. "Color image steganography scheme using set partitioning in hierarchical trees coding, digital Fourier transform and adaptive phase modulation." *Applied Mathematics and Computation* 185, no. 1 (2007): 432-448.

[26] Cheng, Qiang, and Thomas S. Huang. "An additive approach to transform-domain information hiding and optimum detection structure." *Multimedia, IEEE Transactions on* 3, no. 3 (2001): 273-284.


 

[27] Kociołek, Marcin, Andrzej Materka, Michał Strzelecki, and Piotr Szczypiński. "Discrete wavelet transform-derived features for digital image texture analysis." In *International Conference on Signals and Electronic Systems, Łódź-Poland*, pp. 99-104. 2001.

[28] S. Mallat: *A wavelet Tour of Signal Processing*, Academic Press, San Diego 1998

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

[30] Mazumder, Juned Ahmed, and Kattamanchi Hemachandran. "A High Capacity and Secured Color Image Steganographic Technique Using Discrete Wavelet Transformation." *IJCSIT) International Journal of Computer Science and Information Technologies* 4, no. 4 (2013): 583-589.

[31] Mazumder, Juned Ahmed, and K. Hemachandran. "Study of Image steganography using LSB, DFT and DWT." *INTERNATIONAL JOURNAL OF COMPUTERS & TECHNOLOGY* 11, no. 5 (2013): 2618-2627.

[32] Mazumder, Juned Ahmed, and K. Hemachandran. "Review Of Different Techniques Used In Recent Steganography Researches." *International Journal of Engineering* 1, no. 8 (2012).

[33] Devi, Ningthoujam Sunita, and K. Hemachandran. "Automatic Face Recognition System using Pattern Recognition Techniques: A Survey."

## AUTHORS

Juned Ahmed Mazumder received his Master of Science in Computer Science (5 years integrated course) degree with first class in 2011 from Department of Computer Science, Assam University, Silchar, where he is currently doing his Ph.D. His research interest includes Image Processing, Steganography, Neural Network and Data Security.

Prof. K. Hemachandran is associated with the Department of Computer Science, Assam University, Silchar, since 1998. Currently he is serving as the Head of the Department in the Department of Computer Science, Assam University, Silchar. He obtained his M.Sc. Degree from Sri Venkateswara University, Tirupati and M.Tech and Ph.D Degrees from Indian School of Mines, Dhanbad. His areas of research interest are Image Processing, Software Engineering and Distributed Computing.

 