A Secured Image Steganographic Technique for RGB Images Using Discrete Wavelet Transform

RAJSHREE NOLKHA, AAYUSHI VERMA, GAURAV AGRAWAL, VIRENDRA P. VISHWAKARMA
Department of Computer Science and Engineering
Inderprastha Engineering College, Ghaziabad
Gautam Buddh Technical University, Uttar Pradesh
INDIA
rajshreenolkha92@gmail.com, aayushi291091@gmail.com, virendravishwa@rediffmail.com

Abstract: - Due to the commendable increase in rate of growth of internet usage as a medium to transfer data and high risk of data theft on internet, the concern is raised in favour of the confidentiality of the information, which is vital. Now to ensure security and to safeguard the private information, many techniques have been used. Image steganography is one of the technique which deals with hiding the secret information as an image behind an image. In this paper, we propose a new and much secured approach for image steganography on RGB images, which works in wavelet domain and the existence of the hidden RGB secret image is highly imperceptible. The high level of security is assured as the receiver is not able to extract the good quality secret image without the knowledge of the key information, provided by the sender to the intended receiver only. The quality of the images is measured by using certain quality metrics such as peak signal to noise ratio (PSNR). Furthermore, the RGB image with hidden content, called as stego image is exposed to certain kind of visual distortions and the secret is extracted out of that modified image, and the quality of image found is satisfactory. Moreover, the experimental results shows better result in comparison with other existing image steganography approach for RGB images.

Key-Words: - Cover Image, Discrete Wavelet Transform, Peak Signal to Noise Ratio, Secret Image, Steganography, Stego Image.

1. Introduction

Security of information has been a major concern since the historic times. Ancient people used to transfer the secret things hidden in a carrier box or they used the humans as the carrier of the secret information. Historical data [1] says that ancient people used to make people bald, and then scribed the information on their head. In many years from then on, certain key concepts have been evolved from earlier used methods. They are Cryptography, Watermarking and Steganography [2]. As a well-known fact, cryptography is a popularly known method to modify the secret information, which can be brought back in the original form, only with the help of the cipher key. Many different algorithms have been developed and used under this category. If explained in a general way, then watermarking is defined as a method to bifurcate the stamp of the owner to ensure that no copies can be made of the data without the permission of the owner [3]. Then we have steganography-"Hiding secret information behind cover information" [4]. Steganography serves the similar purpose of cryptography by not letting the unintended person get hold on secret data, but has a major difference in base concept. Steganography is concerned with concealing the information thereby making it unseen whereas cryptography is concerned with encrypting the information thereby making it unreadable [5]. The concept of watermarking has also found a major difference in terms of intent, i.e. the purpose of steganography is hiding the information whereas watermarking is merely extending the cover source with extra information.

Steganography has been introduced to us by our ancestors and they used this technique frequently for serving their purpose. Basically, the word steganography is derived from two Greek words 'Stegnos' meaning 'covered' and 'Graphtos' meaning 'writing' [6]. It is the process of hiding a secret message or information behind a cover image, audio or video file in such a way that no one can even predict that some information is hidden behind

the carrier. Thus, the information can be transmitted from the sender to the receiver without the risk of detectability. Steganography is having an incremental growth in the current scenario and has been a vast area of research. There are many types of steganography such as text, image, audio, video etc [7]. In this paper we have focused on the image steganography, as we hide a secret image behind a cover image. Talking about image steganography, there are various image steganography techniques available such as least significant bit substitution (LSB) technique, discrete cosine transformation (DCT), discrete wavelet transformation (DWT). In this paper, we have proposed a new approach to image steganography for RGB images using DWT as it is one of the most robust and secured method among the different image steganographic techniques. The secret and cover images used in this paper are colored images in RGB form. The RGB images can be formed from the concatenation of the three planes i.e. red plane, green plane and blue plane respectively with the pixel intensity values ranging from 0-255, and similarly the RGB image can be distributed in its three planes.

The figure given below, shows the flow of two basic processes of image steganography in which first one is embedding where the sender embeds the RGB secret image behind the RGB cover image forming the RGB stego image is sent to the receiver along with the encrypted key information and the second one is extraction where the receiver extracts the secret image from the received RGB stego image with the help of the key information obtained after decryption.

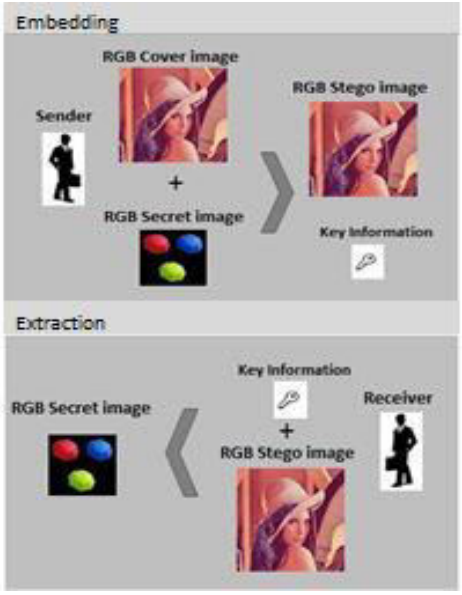

Fig. 1. Basic Principle of Image Steganography

2. Discrete Wavelet Transform

The Discrete Wavelet Transformation (DWT) involves a process of decomposition based on the wavelet functions which results in four overlapping sub bands with multi resolution. It transforms the image from spatial domain to frequency domain where the generated wavelet coefficients are modified in order to conceal the image. The wavelet transform clearly separates the high and low frequency information on a pixel by pixel basis [8]. In 1-level DWT, with the help of high pass filter and low pass filter inputs are convolved. In 2-level DWT, initially 1-level DWT is applied to all rows and then to all columns. This decomposition results into four band coefficients namely the approximate band (LL), horizontal band (HL), vertical band (LH) and the diagonal band (HH). In this paper, we have used 'Haar DWT' which is the simplest of all the wavelet transform. In this transform, the low and high frequency wavelet coefficients are generated by taking the average and half of the differences of two pixel values respectively.

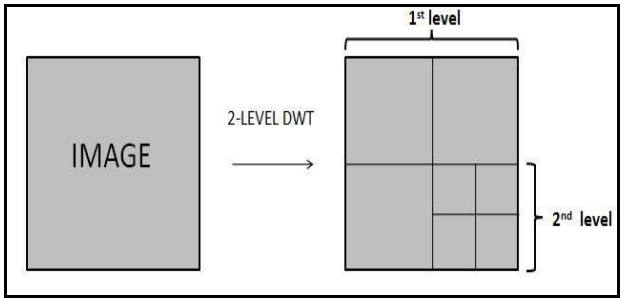

Fig. 2 Sub bands formed after applying 1-level DWT and 2-level DWT

The above figure shows the 4 sub-bands that are formed in the 1st level diagonal band, after applying 2-level Haar DWT on a 2-dimensional image.

3 The Proposed Model

In this paper, the proposed model is a unique and simple method for embedding the secret image behind the cover image and then extracting the secret image from the cover image. The model can be broadly classified into two sub modules where one module deals with the embedding of the secret image and the other module deals with the extraction of the secret image. The modules are explained as follows:

3.1 Embedding model

In this sub module, two inputs are loaded i.e. the RGB cover image and the RGB secret image and a RGB stego image is obtained as output, which appears exactly the same as the cover image and then the stego image is ready for use which can be sent to the intended recipient along with the key information through the public network and the risk is very less as the existence of the communication being held is hidden.

3.1.1 Step 1

The input RGB cover image is loaded as the first input and then it is processed to get the three different planes i.e. R, G and B. The size of the cover image used in our procedure is 512*512. The RGB cover image is broken down to the three planes as stated with the help of the MATLAB commands and what we get as output is three different grayscale images with intensity ranges from 0 to 255. The step can be better understood with the help of the diagram as shown below in Fig. 3.

Fig. 3 R, G and B plane of the RGB cover image

3.1.2 Step 2

The RGB secret image is loaded. The max size allowed for the secret is one-fourth of the size of the cover image, means if the size of the cover image is 512 *512 then the maximum allowed size of the secret image is its one-fourth i.e. 128*128. Here the size of the secret image **('m')** is taken to be the max allowed. To get the process completed, the RGB secret is also broken down to the three planes i.e. R plane, G plane and the B plane respectively. The working can be explained through the diagram shown below in Fig. 4.

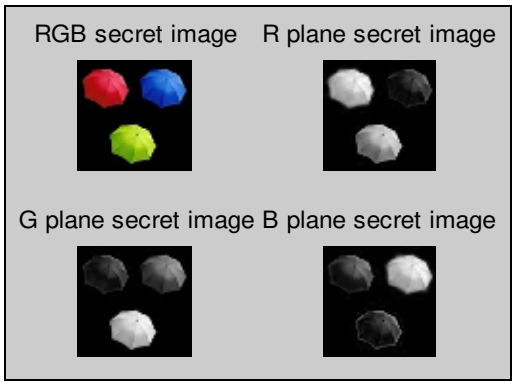

Fig. 4 R, G and B plane of the RGB secret image

3.1.3 Step 3

Now we have the R, G and B plane of the cover and the secret image. Now, 2-level DWT is applied on any two planes of the cover image. In this paper we have randomly chosen the R and the G plane and 2-level DWT is applied on the R and the G plane of the cover image. The diagram shows the details in Fig. 5 and Fig.6.

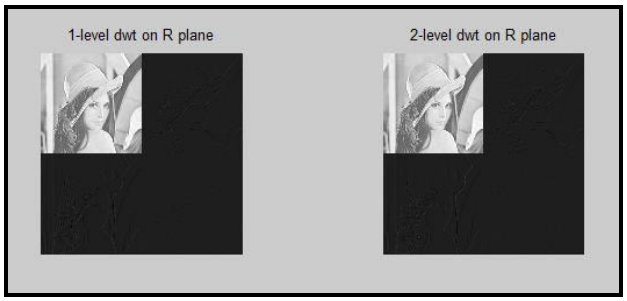

Fig. 5 Application of the 2-level DWT on the R plane of the RGB cover image

Fig. 6 Application of the 2-level DWT on the G plane of the RGB cover image

3.1.4 Step 4

The concealing of secret information in the different planes of the cover image actually starts at this step. The embedding can be broken down under three parts as shown:

3.1.4.1 Embedding of R plane of Secret Image

The R plane of the secret is to be embedded in the 2nd level approximate band (LL2) of the R plane of the cover image and this information is stored in variable n_1 (n_1=LL2 band of R cover plane). The concealing of secret R plane can be summarised as follows:

- ***Right bitshift the bits of the secret R plane pixel values such that we get the 5 MSB at the 5 LSB position. The no. of bits shifted is stored as a parameter value for key generation in a variable as 'x'=5.***

- ***Replace the 5 MSB of the secret with that of the 5 LSB of the applroximate band coefficient.***

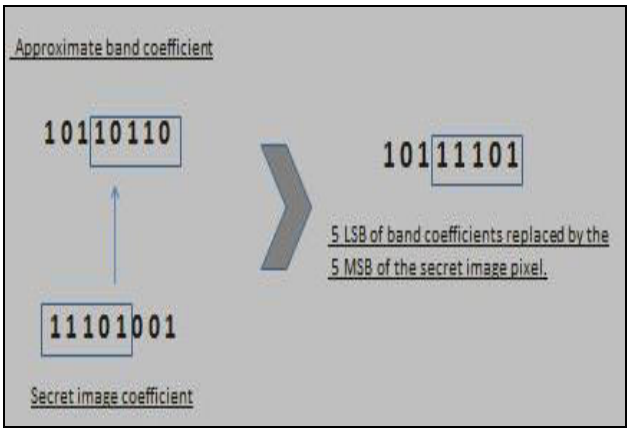

Fig. 7 Process of embedding 5 MSB of secret image plane into 5 LSB of Cover image plane [9]

This is how we actually embed the secret information in the cover image and get the secret concealed in the cover plane. W implement tis step to embed the R plane of the secret image in the 2nd level approximate band of the R plane of the cover image. The output of this substep can be shown as:

Fig. 8 R plane of secret image embedded

3.1.4.2 Embedding of G plane of Secret Image

The embedding of the G plane of the secret image is similar to that of the embedding of R plane of the secret image. The G plane of the secret image is embedded in the 2nd level approximate band(LL2) of the G plane of the cover image with the the procedure as explained above and n_2 is obtained as n_2=LL2 band of G cover plane). The G cover plane is shown in fig 9 after embedding.

Fig. 9 G plane of secret image embedded

3.1.4.3 Embedding of B plane of Secret Image

The embedding of the B plane of the secret is quite different to that of the above two steps, as we embed the B plane of the secret image in the horizontal band of the R palne of the cover image. The embedding procedure with the bits is the same only the location of the embedding is different in this case. So, n_3=HL2 band of R cover plane as shown in Fig. 10.

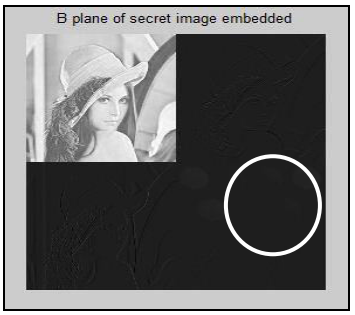

Fig. 10 B plane of secret image embedded

3.1.5 Step 5

In this step the stego image is obtained by applying the inverse DWT operations first on the R plane and the G plane respectively and then finally concatenating all the three planes of the cover image together to obtain the RGB stego image [10]. The stego image so formed after this step appears to be the same as the user input for cover image.

Fig. 11 The input cover image and the stego image

3.1.6 Step 6

The key information finally needs to be generated, which is sent along with the stego image to the intended receiver for proper extraction of the RGB secret image, hence adding security in data transmission.

Key = 'Size of secret image' + 'location of R secret plane' + 'location of G secret plane' + 'location of B secret plane' +'No. of MSB bits of secret embedded'

Key = 'm' + 'n_1' + 'n_2' + 'n_3' + 'x'

In our project we consider the key information as:
Key = 128 LL2-R LL2-G HL2-R 5

Now, the sender can ensure the security, by further encrypting the key information before sending, by a method approved by the sender and reciever in advance, such that if key information is stolen, then also the secret image is preserved. One of the method is mentioned in the following sub section.

3.1.7 Proposed scheme for encryption of key information

The sequence of alphabets and numbers can be modified according to the look up table.

Look up table for numbers

0	1	2	3	4	5	6	7	8	9
A	B	C	D	E	F	G	H	I	J

Look up table for uppercase alphabets

A	B	C	D	E	F	G	H	I	J
n	o	p	q	r	s	t	u	v	w

K	L	M	N	O	P	Q	R	S	T
x	y	z	a	b	c	d	e	f	g

U	V	W	X	Y	Z
h	i	j	k	l	m

Using the information given in look up table, the key information can be encrypted as:

Key = 128 LL2-R LL2-G HL2-R 5

Key after encryption:

Encrypted Key = BCI yyC-e yyC-t uyC-e F

The embedding procedure ends up here and the stego image is now used as a carrier to transport the secret image to the intended recipient via. any network or route or channel along with the encrypted key info.

3.2 Extracting model

This is the second module which deals with the extraction of the secret image at the receiver's side. The receiver gets the key information and resassign all the corresponding values in the variables 'm', 'n_1','n_2', 'n_3' and 'x'. The extraction algorithm is also carried out in a number of steps. These steps are detailed as:

3.2.1 Step 1

The receiver now will process the received image for secret image extraction. To do this, the first basic step is to divide the RGB image into its three planes for the further processing. This first step deals with the extraction on R, G and B plane of the received image.The Fig.12. depicts this step.

Fig. 12 Three planes of the received image

3.2.2 Step 2

The reciever has the encrypted key sent by the sender, now to extract the required key information, decryption is done according to the given look up table.

Decrypted Key = 128 LL2-R LL2-G HL2-R 5

3.2.3 Step 3

As the receiver now has the three planes and the required information about the location of the secret in the plane as 'n_1', 'n_2' and 'n_3'. Therefore the receiver may directly reach at that band and extarct the secret by applying the specified modifications. For this he first needs to apply 2-level DWT on the the received image's two planes as specified by the sender.

3.2.4 Step 4

Then the particular modifications are done on the approximate and horizontal band of these planes to get the extracted secret out of it. The modifications which are to be done are quite simple in terms of bitoperations. It simply states that, for each band coefficient load the 5LSB of the coeffient to the 5 MSB place to a new image pixel and repeat this step for each coefficient of the specified band. The Fig. 13 given below describes the process.

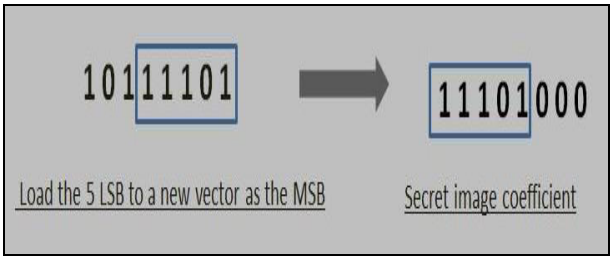

Fig. 13 Process of extraction of bits from band coefficients to form secret image plane

When this operation is performed then we get the three planes of the secret image which was embedded.

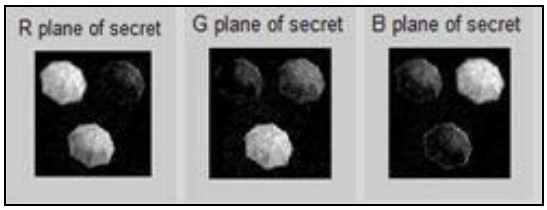

Fig. 14 R, G and B plane of the extracted secret image

3.2.4 Step 5

After we obtain the R, G and B plane of the extracted secret they are concatenated to give the output [12]. The expected output of the extraction algorithm is the secret image. The colored secret image should be obtained.

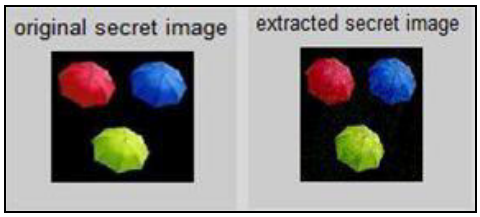

Fig. 15 The embedded secret image and the extracted secret image

Thus, at the end of the extraction algorithm we get the extracted secret image at the receiver side. The receiver can now deploy the secret as he require and the goal of the proposed technique is achieved.

4. The Basic Algorithm

The whole process as explained in the proposed model can be enumerated in the form of an algorithm showing the flow of operations.

4.1 Algorithm for Embedding

The steps involved in the embedding algorithm performed at the sender's side, are given as:

1. Load the RGB cover image.

2. Obtain the three different planes of the cover image as three different gray scale images, R (R plane), G (G plane) and B (B plane).

3. Apply the 2-level Haar DWT on the R and G plane of the cover image.

4. Load the RGB secret image (size of secret image (**m**) <= $1/4^{th}$ of size of cover image).

5. Obtain the three different planes of the secret image in r (R plane), g (G plane) and b (B plane).

6. Concealing the secret plane in cover plane is done as:
   - Select one of the appropriate bands among 2-level DWT bands of the cover plane as '$\mathbf{n_i}$.'
   - For each of the m*m coefficient of the LL2 band, the **'x** MSB' are inserted in place of the '**x** LSB' (i.e. 5 bits) of the band coefficient.
   - Apply 2-level inverse DWT (IDWT) operation.

   The stego plane is obtained.

7. The above step is repeated, for hiding each of the three planes of the secret image in the band coefficients of, one of the cover image plane.($\mathbf{n_1}$, $\mathbf{n_2}$, $\mathbf{n_3}$ stores the name of the selected band to be modified for embedding R plane, G plane and B plane of secret image respectively).

8. Concatenate all the three stego planes to form a RGB stego image.

9. The key is generated as: **Key= $\mathbf{m+n_1+n_2+n_3+x}$.**

10. Then the encryption is performed on the key, by the look up table as described above, which is been agreed by the receiver and sender in advance and the encrypted key is sent along the stego image.

4.2 Algorithm for Extracting

The steps involved in extraction of the secret image at the receiver's side are given as:

1. Load the RGB secret image.

2. Obtain the three planes of the stego image as R', G' and B'.

3. Load the key and decrypt the key according to the look up table and assign the values of the corresponding variables in m, n_1, n_2, n_3 and x.

4. Extracting the secret image's information is done as:
   - Apply 2-level DWT on R', G' and B'.
   - For each m*m coefficient of the 'n_i' band, obtain the 'x LSB' and load it into 'x MSB' of a new image matrix.

5. Repeat step 4, to obtain three planes of the secret image in r', g' and b'.

6. Concatenate r', g' and b' to generate the RGB secret image.

5. Visual Attacks on Stego Image

The security of the hidden content is a vital issue, and it should be maintained even if any intruder maliciously attacks on the stego image to destroy the secret image. Though, the presence of secret image behind a cover image is concealed, but ensuring the security of the secret image against attacks should be analysed, in order to encompass all possibilities. So, our algorithm also aims to extract the secret image with minimum modification, even if the stego image is attacked visually. So, the stego image was exposed to some of the visual attacks such as toning the stego image in sepia mode, daylight mode and night mode. These attacks are known as visual stego attacks, because these attacks modify the pixel intensity values of the stego image plane, and the result of applying attack on the stego image can be seen by naked eyes.

5.1 Sepia Mode Toning

In this attack, the stego image is toned in popularly known sepia mode by changing the corresponding intensity values of the R, G and B plane of the stego image. The following figure shows the result of this attack on the stego image as developed as the output of embedding procedure.

Fig. 16 Comparison of the stego image and the sepia mode toned stego image

When, the extraction algorithm was applied on the attacked stego image, then the extracted secret image appeared as:

Fig. 17 Comparison of secret images extracted with and without sepia mode toned stego.

5.2 Daylight Mode Toning

In this attack, the stego image is modified to appear as a daylight mode toned image. The stego image is made to appear as if it is clicked under day light mode and the stego image is visually modified accordingly. Fig. 18 describes the difference occurred in the stego image after application of this attack.

Fig. 18 Comparison of the stego image and the daylight mode toned stego image

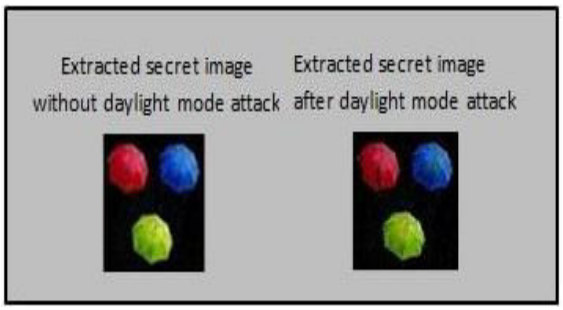

Fig. 19 Comparison of secret images extracted with and without daylight mode toned stego.

The above figure shows the comparison of the secret image extracted from the normal stego and the day light mode toned stego image. The secret image is hardly modified and has undergone minute changes. Thus the clarity in the extracted secret even after the attack, displays the robustness of our proposed algorithm.

5.3 Night Mode Toning

In this visual attack, the stego image intensity values of the planes are modified which changes its appearance and it gets toned in the night mode. The figure shown below shows the result of this attack.

Fig. 20 Comparison of stego image and the night mode toned image

On applying the same extraction algorithm on this attacked stego image, the extracted secret appeared:

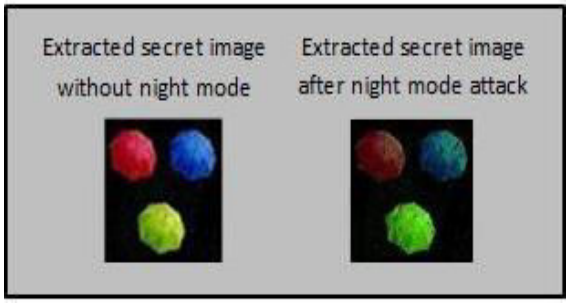

Fig. 21 Comparison of secret images extracted with and without night mode toned stego.

The above figure shows the comparison of the secret image extracted from the normal stego and the night mode toned stego image.

5.4 Brightening R plane of stego image

Brightening the R plane is actually not a visual attack, but it simply enhances the R component of the stego image and the stego image appears to be modified visually as the stego image now appears to be more reddish than the original stego image. The figure given below shows the effect of this visual modification categorised as visual attack in our paper.

Fig. 22 Comparison of stego image and the R brightened image

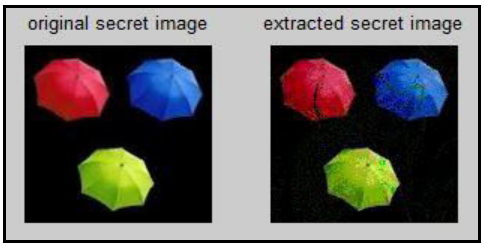

Fig. 23 Comparison of secret images extracted from stego and R brightened image.

5.5 Brightening G plane of stego image

In this section, we brighten the G component of the stego image and the stego image appears to be more greenish visually as the green component is being enhanced. The figure shown below, shows the result of this modification when the brightening is applied to the G plane.

Fig. 24 Comparison of stego image and the G plane brightened image.

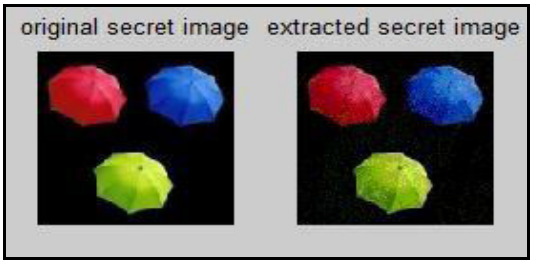

Fig. 25 Comparison of secret images extracted from stego and G brightened image.

5.6 Brightening B plane of stego image

This section lines up about the brightening of the B plane of the stego image and shows how the brightening affects the stego image and make the stego image appear bluish visually, with the help of the figure given below.

Fig. 26 Comparison of stego image and the B plane brightened image.

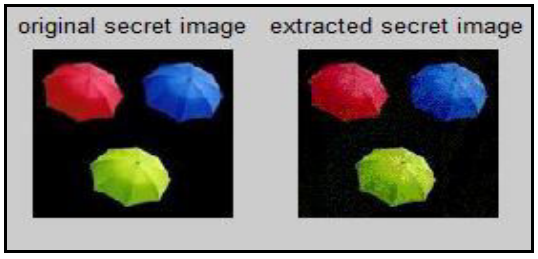

Fig. 27 Comparison of secret images extracted from stego and B plane brightened image.

In this section, we can see that the proposed algorithm is robust enough to sustain such type of visual attacks as the receiver is still able to acquire the secret image safely, with minimum modifications.

6. Experimental Summary

Security, capacity and the imperceptibility are the three main critics which decides how good a technique is, in accomplishing the aim of image steganography. Our proposed method offers a good capacity of secret to be embedded. Also, the security

has been further enhanced by encrypting the key information before sending it to the receiver. A next criterion is the imperceptibility. The stego image formed by the proposed method appears to be the same as the original cover image, but the similarity needs to be measured. So, in order to consolidate the three pillars of steganography in the favour of our proposed scheme, Peak Signal to Noise Ratio (PSNR) was used as the quality measurement metric. It is a measure that maps the similarity in images in terms of decibels (dB). Larger value of PSNR depicts that the images are more similar and the modified image is of high quality with greater similarity with the original one. PSNR is formulated as [14]:

$$PSNR = 10 \times \log_{10}\left(\frac{255^2}{MSE}\right) \quad \ldots (1)$$

Here, MSE stands for Mean Square Error and '255' is the maximum number for the 8-bit colored image depicting 256 levels in any of the three planes, i.e. R, G and B plane. The formula for MSE is given below.

$$MSE = \frac{1}{MN}\sum_{i=1}^{M}\sum_{j=1}^{N}(f(i,j) - f'(i,j))^2 \quad \ldots (2)$$

In this formula, M and N shows the height and width of the image, which clearly shows that MSE is inversely proportional to the size of the images compared. And f (i, j) and f' (i, j) depicts the pixel value of the original image and the processed image.

It is clear by the above argument that the PSNR is directly proportional to the size of the images compared, because PSNR is inversely proportional to MSE. If the images compared are of the smaller size, then PSNR value will be smaller and vice-versa.

$$PSNR \propto \frac{1}{MSE} \propto \text{Size of image}$$

Fig. 28 Relationship between PSNR, MSE and Image Size

In addition to the average PSNR value, RMS value of the three PSNR values (PSNR-R, PSNR-G, and PSNR-B) is also calculated and tabulated along.

$$\text{Average PSNR} = \frac{\text{PSNR-R} + \text{PSNR-G} + \text{PSNR-B}}{3} \quad \ldots (3)$$

$$\text{RMS} = [\,(\text{PSNR-R})^2 + (\text{PSNR-G})^2 + (\text{PSNR-B})^2\,]^{0.5} \quad \ldots (4)$$

In the following section, the experimental results are shown which were obtained, when the proposed algorithm was simulated using MATLAB 7.6.0.

Five cover images are used of size 512*512 and two secret images are used of size 128*128. All images are in bitmap format (.bmp). The following figures, Fig. 22 and Fig. 23 show the set of RGB cover and secret images respectively.

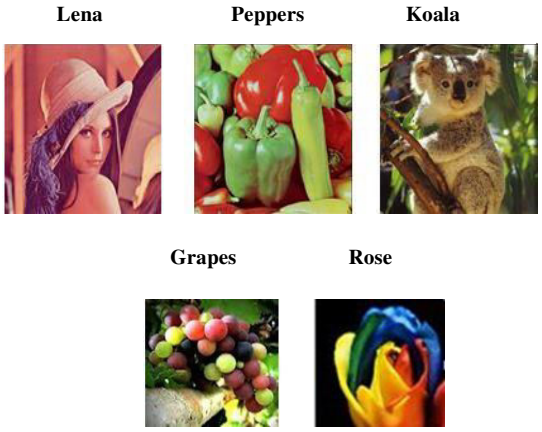

Fig. 29 Cover Images (.bmp)

Fig. 30 Secret Images (.bmp)

6.1 Comparison between Cover Image and Stego Image

Table 1 shows the PSNR values which are calculated between the original cover image and the formed stego image for the five cover images and two secret images used in the experiment. The obtained PSNR values are high depicting better quality of the stego image. Also, the stego images formed when "secret1" was embedded in all the five cover images is shown below:

Fig. 31 Stego images with "secret1.bmp" embedded

Table 1 PSNR Values for comparison between cover image and stego image (in dB)

Cover Image (512 X 512)	Secret Image (128 X 128)			
	Secret1.bmp		Secret2.bmp	
	Avg. PSNR	RMS	Avg. PSNR	RMS
lena	41.58	58.87	45.41	64.26
pepper	41.65	58.97	45.59	64.52
grapes	45.74	59.06	45.75	64.75
koala	41.55	58.84	45.35	64.19
rose	41.67	59.00	45.64	64.59

6.2 Comparison between original secret image and extracted secret image

Table 2 shows the PSNR value which are calculated between the original secret image which is embedded behind the cover image in the embedding module and the extracted secret image which is extracted from the received stego image in the extracting module.

Table 2 PSNR Values for comparison between original secret image and extracted secret image

Cover Image (512 X 512)	Secret Image (128 X 128)			
	Secret1.bmp		Secret2.bmp	
	Avg. PSNR	RMS	Avg. PSNR	RMS
lena	45.41	12.76	41.58	19.85
pepper	45.59	12.75	41.65	19.84
grapes	45.75	12.74	45.74	19.82
koala	45.35	12.77	41.55	19.86
rose	45.64	12.61	41.67	19.75

6.3 Comparison between original secret image and extracted secret image after applying visual attacks

This section shows the PSNR and RMS values comparing the original secret and the extracted secret from the visually attacked stego image. The stego images considered here are the two stego image formed with cover image as 'Lena' and both the secret images respectively. When the PSNR was calculated between the original secret and the extracted secret from attacked stego images, it was found that the quality of secret is not being degraded much, and is good enough to be accepted, as the PSNR values are close to the values of PSNR calculated in Table2.

Table 3 PSNR Values for comparison between original secret image and extracted secret image from attacked stego image with cover image as Lena

Type of attack	Secret1		Secret2	
	Avg. PSNR	RMS	Avg. PSNR	RMS
SEPIA MODE	7.14	12.55	11.33	19.65
DAYLIGHT MODE	7.23	12.72	11.41	19.81
NIGHT MODE	7.38	12.39	11.20	19.45
R plane BRIGHT	7.05	12.41	11.19	19.43
G PLANE BRIGHT	7.24	12.73	11.42	19.84
B plane BRIGHT	7.26	12.76	11.43	19.83

Hence, we can say that our proposed scheme is robust enough to sustain such kind of visual attacks.

7. Conclusion

The proposed model for image steganography on RGB images using DWT transform is a very secure, robust and simple approach which offers good imperceptibility and high embedding capacity, allowing the maximum size of secret image to be $1/4^{th}$ of the size of cover image. The existence of the communication is hidden as the stego image which is sent over network to the receiver appears to be the same as cover image, offering the PSNR values of about 40 dB, which is a fair enough value [15] depicting good quality of the image. Also, with the help of encryption of the key information, the security level is increased and the receiver is able to extract the best quality RGB secret image with PSNR of about 20dB (it is lesser in number, as image size is small), after decrypting the key information. Even if any intruder modifies the stego image by applying visual attacks, then also the algorithm is capable of delivering the secret to the recipient with least modifications.

References:

[1] L. Marvel, C. G. Boncelet, Jr, and C. T. Retter, "Spread spectrum image steganography*", IEEE Transactions on Image Processing*, Vol. 8, No. 8, pp. 1075–1083, Aug. 1999.

[2] Ying Wang, Pierre Moulin, "Perfectly Secure Steganography: Capacity, Error Exponents, and Code Constructions," *IEEE Transactions on Information Theory*, Vol. 54, No. 6, June 2008.

[3] Po-Yueh Chen and Hung-Ju Lin, "A DWT Based Approach for Image Steganography", *International Journal of Applied Science and Engineering* 2006. Vol 4, No. 3, pp 275-290.

[4] Tanmay Bhattacharya, Nilanjan Dey, S. R. Bhadra Chaudhuri, "A session based multiple hiding techniques using DWT and DCT" ,*International Journal of Computer Applications* (0975-8887), Vol. 38,No. 5, January 2012.

[5] Arvind Kumar, Km. Pooja, "Steganography-A data hiding technique", *International Journal of Computer Applications* (0975 – 8887) Volume 38– No.5, January 2012

[6] Zaidoon Kh. AL-Ani, A.A.Zaidan, B.B.Zaidan And Hamdan O.Alanazi,"Overview: Main Fundamentals for Steganography ", *Jounal For Computing*, Volume 2, Issue 3, March 2010

[7] Shashikala Channalli, Ajay Jadhav, "Steganography-An art of hiding data", *International Journal of Computer Application* (0975 – 8887), Volume 9– No.7, November 2010

[8] Yedla Dinesh and Addanki Purna Ramesh, "Efficient Capacity Image Steganography by Using Wavelets ", *International Journal of Engineering Research and Applications (IJERA)*, Vol. 2, Issue 1, Jan-Feb 2012, pp 251-259.

[9] Aayushi Verma, Rajshree Nolkha, Aishwarya Singh, Garima Jaiswal, "Implementation of Image Steganography Using 2-Level DWT Technique", *International Journal of Computer Science and Business Informatics*, ISSN: 1694-2108, Vol. 1, No. 1, May 2013.

[10]S.sarreshtedari, S.Ghaemmaghami, "HighCapacity Image Steganography in Wavelet Domain" *IEEE Transactions, 2010*

[11] Parvez, M.T., Gutub, A.A.: RGB Based Variable-Bits Image Steganography. *In: Proceedings of IEEE Asia Pacific Services Computing Conference*, pp. 1322–1327 (2008).

[12] Tiwari, N., Shandilya, M.: Secure RGB Image Steganography from Pixel Indicator to Triple Algorithm- An Incremental Growth. *International Journal of Security and Its Applications* 4(4), 53–62 (2010)

[13] Adnan Gutub, Mahmoud Ankeer, Muhammad Abu- Ghalioun, Abdulrahman Shaheen, and Aleem Alvi, ―Pixel Indicator high capacity Technique for RGB image Based Steganography‖, *WoSPA 2008 – 5th IEEE International Workshop on Signal Processing and its Applications*, University of Sharjah, Sharjah, U.A.E. 18 – 20 March 2008

[14]A.A. Abdul Latef, "Color Image Steganography Based on Discrete Wavelet and Discrete Cosine Transform" ,Ibn Al-Haitham Journal of Pure and Application Science ,Vol. 24, No. 3, May 2011.

[15] Yuan-Hui Yu, Chin Chen Chang, Iuon-Chang Lin, "A new steganographic method for color and gray scale hiding" ,*Elsevier Computer Vision and Image Understanding,* November 2006.