An Enhanced Steganographic Model Based on DWT Combined with Encryption and Error Correction Techniques

Dr.Adwan Yasin[1]
Computer Science Department
Arab American University
Jenin, Palestine

Dr.Muath Sabha[3]
Multi Media Department
Arab American University
Jenin, Palestine

Mr.Nizar Shehab[2]
Computer Science Department
Arab American University
Jenin, Palestine

Mariam Yasin[4]
Computer Science Department
Arab American University
Jenin, Palestine

Abstract—**The problem of protecting information, modification, privacy and origin validation are very important issues and became the concern of many researchers. Handling these problems definitely is a big challenge and this is probably why so much attention directed to the development of information protection schemes. In this paper, we propose a robust model that combines and integrates steganographic techniques with encryption, and error detection and correction techniques in order achieve secrecy, authentication and integrity. The idea of applying these techniques is based on decomposing the image into three separate color planes Red, Green and Blue and then depending on the encryption key we divide the image into N blocks. By applying DWT on each block independently, this model enables hiding the information in the image in an unpredictable manner. The part of the image where information embedded is a key depended and unknown to the intruder and by this we achieve blinded DWT effect. To enhance reliability the proposed model that uses hamming code which helps to recover lost or modified information. The proposed Model implemented and tested successfully.**

Keywords—Steganography; DWT; LSB; hamming code; encryption and decryption

I. INTRODUCTION

Mark kahs in [1] has defined steganography as the art and main science of communicating such that the existence of communications is unknown. The goal of steganography is hiding messages into another carrier, in a way that does not allow outsiders to detect or recognize that there is a hidden message. Encryption is another technique that can be used to protect the information and provide secure communication, but in this case the outsiders know and can see the cipher text but they could not understand and use it [2].

Cryptography and steganography are both used to protect information from disclosure by unwanted parties. While cryptography is about protecting the contents of messages, the main purpose of steganography is to hide the data in a covered media, so that others would not be able to get or to notice it, which is preferable it does not attract the attentions or suspicions of hidden message existence. Many experts prefer using both techniques in order to achieve and provide more security and protection. Stenography has different types according to the way that used to hide the data in covered media. The first one is called audio stenography this type embeds secret messages in audio. This technique is the most challenging technique because it is extremely hard to add or remove data from audio file structure. The second type is the text stenography, and it means hiding the secret messages into other texts. It is a very challenging task. This is because of the small amount of redundant information to replace with a secret message in the text files. The most used type is the Image stenography in which it embeds the secret message into digital images. Image stenography has two major techniques according to its domain, spatial domain and the transform domain. Least Significant Bit (LSB) technique is the simplest and most common one used in the spatial domain. The Discrete Cosine Transformation (DCT) and the Discrete Wavelet Transformation (DWT) are the two most common steganografic domain transformation methods used in the transform domain and they are the most complex and efficient techniques. DCT and DWT hides the data in the areas of the image that are less exposed to Cropping, Compression, and Image processing. Steganography faces and has to overcome three main challenges, the Invisibility "Security of Hidden Communication ", Robustness and the size of embedded data. There is no steganographic technique, capable of resolving all the three challenges at a high level of accuracy. It is not possible to attain high robustness to signal modifications and high insertion capacity at the same time [3].

This paper addresses the main steganographic challenges in order to achieve a compromise between the capacity of the embedded data and the robustness to certain attacks, while keeping the perceptual quality of the stego-medium at an acceptable level. The rest of the paper organized as follows:

1) Section II Literature review.
2) Section III discusses the proposed Model.
3) Section IV discusses the implementation results.
4) Section V conclution.
5) Secttion VI future work.

II. Literature Review

A. LSB Technique

It’s the simplest technique used in image steganography, in LSB technique the data that we want to hide inserted into the least significant bits of the pixel information [4]. This technique is widely used because it has less chance of distortion of the original image, more capacity to hide information and it is less complex. Despite all these advantages LSB techniques have some serious disadvantages like the hidden information can be lost with image manipulation, hidden data can be destroyed by simple attacks and it requires a high transmission rate due to the large size of stego image.

Mamta Juneja et al., in [5] presents two components based on LSB technique for embedding secret information in the LSB's of the blue plan and partial green plan of random locations of pixels at the edges of the cover images, it's integrated with an Advanced Encryption Standard to be more robust.

Shamim Ahmed Laskar et al., in [6] used a method to embed data in the red plan of the image and it select pixel by generating random numbers, changes in image can’t be noticed. Stego key used to generate random number in order to select pixel locations. It focuses on increasing the security of the hidden information and reducing distortion rate.

Y. K. Jain et al., in [7] used a method to divide the image pixel range and generates a stego key, this private key has five different ranges of the gray level in the image and each range present the replaced bits number to be embedded in the least significant bits of the image. It has a drawback that it hides extra bits of signature with hidden message

S. Channalli et al., in [8] used a stego key to hide data, it modifies the LSB of the pixel and the secret data bits. A combination of pattern bits of M x N size and random key value. The first step of embedding is by matching each pattern bit with a secret message bit, if suit it modifies the 2nd LSB bits of cover image "original" otherwise remains the same. This technique has low hidden capacity because each secret bit requires a block of (MxN) pixels.

H. Motameni et al., in [9] introduced data hiding technique that finds dark areas of the stego image to hide the secret information using the LSB technique. This method required high computation to find dark regions and has not tested on high texture images and it is not useful for gray or color images just for binary images.

V. Madhu Viswanatham et al., in [10] introduced an image steganography technique, based on LSB replaces and selection of random pixel in the cover image area. It generates random numbers and selects the area of interest where the secret data supposed to be hidden. The biggest advantage of this technique is the security of hidden data and the drawback is data embedding, does not take care of the Visual Quality when pixels selected.

M. Tanvir Parvez et al., in [11] introduced a pixel indicator method with variable bits; it chooses one plan among red, green and blue planes and embeds data into variable LSB of the chosen plan. The plan selection is sequential and the size depends on the cover image "original" bits.

B. DWT

This technique used to convert the spatial domain into the frequency domain; it separates the high frequency and low frequency information.

DWT divides component into four frequency bands called sub bands known as

LL- Horizontally and vertically low pass
LH - Horizontally low pass and vertically high pass
HL - Horizontally high pass and vertically low pass
HH - Horizontally and vertically high pass

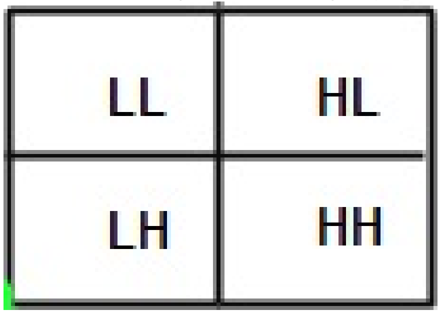


Fig. 1. One phase decomposition using DWT

Human eyes are more sensitive to the low frequency (LL sub band) the other three sub-bands are high frequency they contain unimportant information like the edge and texture details and they are not sensitive to small changes. Accordingly hiding secret data in these sub-bands does not reduce the image quality, at variance of LL sub-band, which is very sensitive to small changes and not used for information hiding.

K. S. Babu et al., in[12] for authentication purposes the proposed a method hides the data into a cover image, which then used to prove the integrity of the embedded secret data. The secret message transformed from the spatial domain to the discrete wavelet transform and then the coefficients of DWT transposed with the verification code before embedding in the spatial domain of the cover image. This method is computationally complex.

Dr.H.Rohil et al., in [13] applied DWT on colored images and its use Arnold transformation to improve the security. The cover image splits into " Red, Green and Blue plan" then DWT is applied to all plans, after that secret image is changed using Arnold transform and every color plan of the changed secrete images is separated. Then secret images plans embedded into HL, HH, and LH sub bands.

Aayushi Verma et al., in [14] proposed an algorithm for embedding and extraction of secret image embedded behind cover gray scale image. 2-level DWT is applied to the original image and then targeted band is selected to be modified. Then the size of secret image is calculated, after that the five most significant bits of secret image embedded into high frequency bands.

Barnali Gupta Banik et al., in [15], used a method that applies Haar-DWT for decomposing the cover image, it generates random number and the detailed horizontal & vertical coefficients are modified by adding these random numbers when data bit is 0. Then apply Inverse DWT.

L. Tong and Q. Zheng-ding, in [16] proposed a DWT based color image method. In this approach, the secret information embedded in a publicly accessed color image by a quantization-based strategy. However, the latter case method processes grayscale images as cover object to create a subliminal channel and it utilizes transform coefficients of 2-Dimensional Discrete transform for embedding process.

T. Narasimmalou[17] Proposed an optimal discrete wavelet transform (DWT) based steganography. This method shows enhancement in the generated peak signal noise ratio (PSNR).

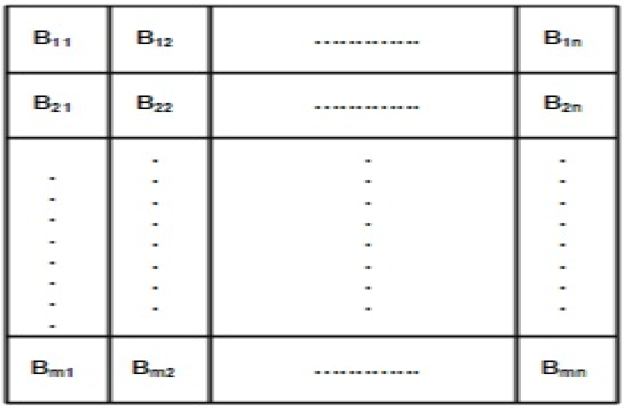
Nag et al., in [18] proposed a steganographic technique based on DWT and applied Huffman coding on Secret message before embedding it in high frequency components of the 2-D cover image, the low frequency component is kept untouched, which retains the visual quality of the image. The algorithm has high capacity and satisfactory security.

All the above mentioned approaches are very susceptible to steganographic analysis and attacks as the information are embedded in a predefined and expected locations. The goal of the proposed technique is to achieve high resistance against steganographic analysis and sustains well known attacks.

III. Proposed Model

A. Secret Data Hiding

In order to enhance security, and reliability, we integrate encryption and error detection and correction techniques along with blinded DWT. The blinded DWT achieved by dividing the image into NxN Blocks as shown in figure 2 where N, key dependent or determined by the User and unknown to the outsiders.



B_{11}	B_{12}	....	B_{1n}
B_{21}	B_{22}	....	B_{2n}
. . . .	. . . .	. . . .	. . . .
B_{m1}	B_{m2}	....	B_{mn}

Fig. 2. Image Division

The Proposed technique applies DWT on each candidate block that will be used to hide information randomly or in a sequential manner and this is the second level of DWT blinding. The proposed model (see figure 7). Consists of the following main steps:

1) *Encrypt the secret data.*

2) *Compute the hamming code of the encrypted data.*

3) *Divide the image into N blocks.*

4) *Determine the candidate Blocks*

5) *Decompose the candidate Block into three color planes (R, G and B).*

6) *Apply DWT on each candidate block independently.*

7) *Secret Message and the hamming code embedded into LSB of the HH and LH bands of each candidate block.*

8) *Apply inverse transformations.*

9) *Combine the three color planes that generate the final stego image.*

B. Description of the proposed Model

The proposed model enables the user to select any symmetric encryption algorithm, but we recommend to use Advance Encryption Standard (AES) as it is a very secure algorithm and supports larger key sizes and it is faster in both hardware and software.

The cipher text is very susceptible to alteration so we used hamming code error detection and correction technique. We suggest the usage of five check bits for every group of three bytes, which is a compromise between the redundancy and reliability. The image resized or cropped to be squared one as this is necessary for the next processing step. The Block number and the candidate blocks which are should be kept secret can be determined by the user or can be generated from encryption key which is better as it is very difficult for the user to maintain bulky secret information. In the proposed model we suggest to use the following modified linear congruential generator as it is very fast pseudo-random sequence generator and convenient for our model as high-quality randomness is not critical and the duplicated numbers should be excluded in case of sequence duplication:

$$\boldsymbol{B_0 = K_0} \text{ Mod } \boldsymbol{N} \quad \textbf{(1)}$$

$$\boldsymbol{B_m=(K_m+1)*B_{m-1}+g)} \text{ mod } \boldsymbol{N} \quad \textbf{(2)}$$

Where : N - Blocks Number ; $m=1,2,\ldots N-1;$

$B_m = m^{th}$ Block ; $K_m = m^{th}$ Key Code;

g should be selected carefully to be relatively prime to N

The candidate block decomposed into three colors plans (R, G, B) If the covered image is a color one. (See figure 3).

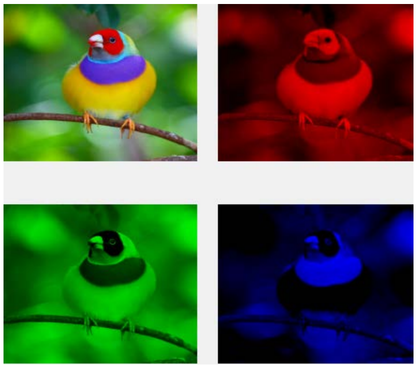


Fig. 3. Cover Image (R,G, B) color plans

In order to enhance accuracy and to be able to use DWT, which needs to deal with fractions and negative numbers which is not applicable for Pixels values, we use the following scale transformation:

$$New\ Value = (D_{max} - D_{min}).(V - S_{min}) / (S_{max} - S_{min}) + D_{min} \quad (3)$$

Where:

$[D_{min},\ D_{max}]$ = *new range*
$[S_{min}\ ,S_{max}]$ = *old range*
V = *Pixel color value*

We apply a simplified form of DWT on the scaled data by using the following Transformation algorithm:

```
For each Row and Column in the Candidate Block(Bc)
{
Row length=Column Length
h=Row length/2;
For(i=0; i<h; i++)
  For(j=0; j<h; j++)
   {
k=j*2;
$B_c[j,i]=(B_c[k,i] + B_c[k+1,i])/2;$
$B_c[j+h,i]=(B_c[k,i] – B_c[k+1,i])/2$
    }
}
```

The output of the described transformation at different levels shown in figure 4 and 5.

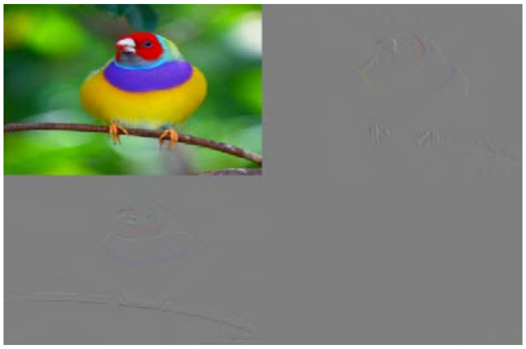


Fig. 4. Cover Image after 1 level of DWT

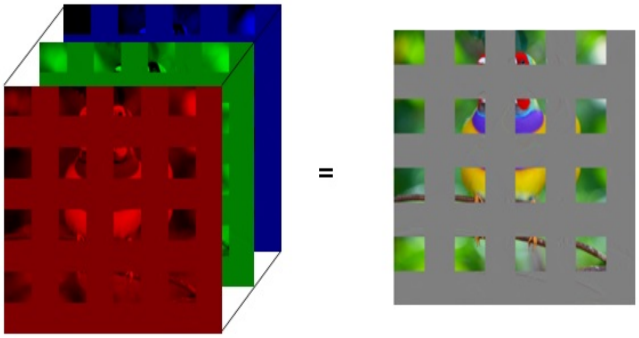


Fig. 5. Cover Image after 4 levels of DWT

At this moment candidates Blocks and the data are ready to start embedding process in which each bit of the data byte inserted in predefined least significant bits of HH color planes (see figure 6) and the hamming code in the LH color plans

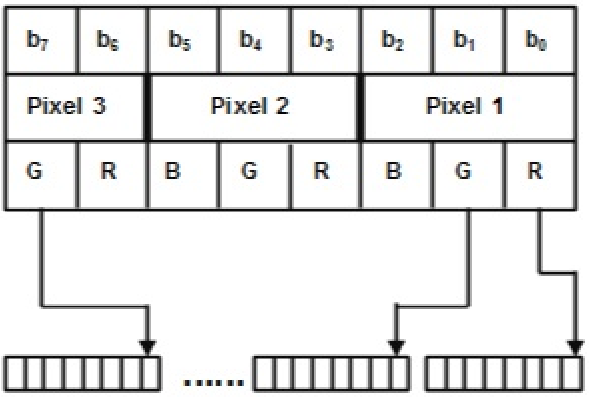


Fig. 6. Data Embedding Diagram

After embedding the data we apply the Inverse DWT and generate the final stego image by combining the three color plans (R, G, B).

C. Secret Data Extraction

The steps of data extraction can be summarized as the following:

1) Divide the image into N blocks.
2) Determine the candidate Blocks
3) Decompose the candidate Block into three color planes (R, G and B).
4) Apply DWT on each candidate block independently.
5) Extract the Secret Data and the hamming code embedded into LSB of the HH and LH bands of each candidate block.
6) Compute the hamming code of the encrypted data
7) If the computed hamming=embedded hamming code there are no errors

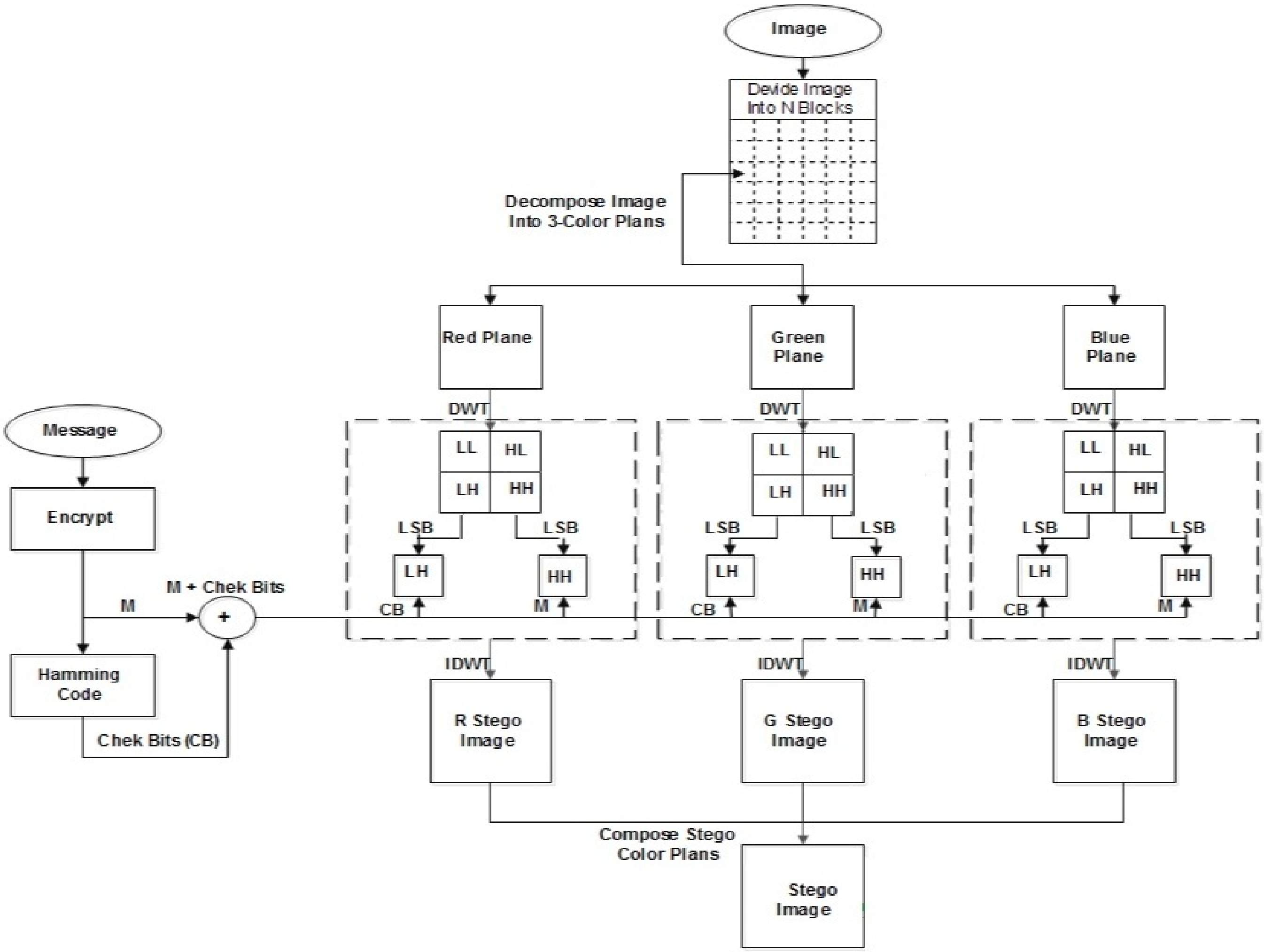


Fig. 7. Proposed Model Structure

Otherwise correct the error.

1) *Decrypt the cipher*

2) *Apply inverse transformations*

3) *Combine the three color planes that generate the final stego image.*

IV. Implementation of the Proposed Model

The proposed model implemented by using C# and tested successfully under various images types: size, color, gray scaled and various levels of DWT transformation, the result shows that it is has a good stego image quality, high level of reliability and security. In Figure 8,9 and 10 illustrated the cover image before and after embedding the data (Stego-Image).

Fig. 8. Cover Image

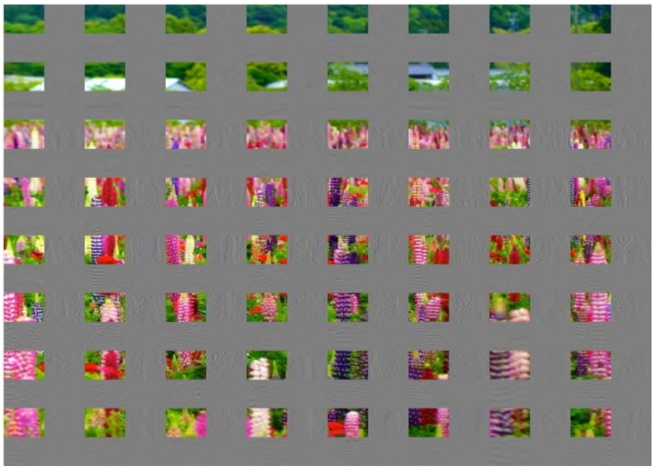


Fig. 9. 8 Level Blinded DWT

Fig. 10. Stego Image

The proposed technique evaluated and compared by LSB and DWT based-techniques. The evaluation done based on the following parameters:

- Capacity - measures the amount of embedded data with minimum distortion effect on the cover image.
- Invisibility - describes how much the quality of cover image remains intact, which makes the human vision unable to distinguish between the stego-image and the cover one.
- Resistance- measures the hidden data tolerance to image updates and stego-attaches.
- Security- describes how it is difficult for outsider to detect and disclose the hidden data.
- Performance- describe how fast the process of data embedding and extraction.

The evaluation results shown in table 1.

The results show that the proposed technique has better resistance and security characteristics than LSB and DWT, whilst it has the worst capacity characteristic. All techniques have the same degree of invisibility.

TABLE I. COMPARISON RESULTS

Techniques Parameters	LSB Based	DWT Based	Proposed Technique
Security	Low	Medium	Very High
Capacity	High	Medium	Low
Resistance	Low	Medium	High
Performance	Very High	Medium	Medium
Invisibility	High	High	High

V. CONCLUSION

In this Paper, we introduced a new steganographic technique that increases the secrecy and reliability of the hidden data without losing the image quality or losing any data in the image, the secrecy achieved by using encryption algorithm in addition to hiding the part of image where the information embedded. The division of image into key dependent number of blocks, hiding the data into unknown blocks and applying multi levels of DWT increase the confusion of the outsider. The reliability achieved by using error detection and correction technique that enables the recovery of altered data. This technique demonstrates that it is very effective and can resist many steganographic attacks, as it has a high degree of blinding characteristics.

Compared to other steganographic systems, the size of embedded data reduced as result of the embedding redundant hamming code. The user can reduce the redundancy by selecting larger blocks without affecting the security and still maintains a high degree of data integrity.

VI. FUTURE WORK

The proposed technique will be enhanced to increase the size of embedded date and decrease the redundancy in addition to adapting it to be effectively used in image watermarking .

REFERENCES

[1] Johnson,NeilF.,“Steganography”,2000URL:http://www.jjtc.com/stegdoc/sec201.html.

[2] Stallings, W. (1995). Network and internetwork security: principles and practice(Vol. 1). Englewood Cliffs: Prentice Hall.

[3] Hong-Juan Zhang, Hong-Jun Tang,"A Novel Image Steganography Algorithm Against Statistical Analysis",Proceedings of the Sixth International Conference on Machine Learning and Cybernetics, Hong Kong, 19-22 August 2007.

[4] Kaur, R., & Singh, B. (2012). Survey And Analysis of Various Steganographic Techniques. International Journal of Engineering Science and Advanced Technology, 2, 561-566

[5] Juneja, M., & Sandhu, P. S. (2013). A new approach for information security using an improved steganography technique. Journal of Information Processing Systems, 9(3), 405-424.

[6] Laskar, S. A., & Hemachandran, K. (2013). Steganography based on Random Pixel Selection for Efficient Data Hiding. International Journal of Computer Engineering and Technology, 4(2), 31-44.

[7] Jain, Y. K., & Ahirwal, R. R. (2010). A novel image steganography method with adaptive number of least significant bits modification based on private stego keys. International Journal of Computer Science and Security, 4(1), 40-49.

[8] Channalli, S., & Jadhav, A. (2009). Steganography an art of hiding data. arXiv preprint arXiv:0912.2319.

[9] Viswanatham, V. M., & Manikonda, J. (2010). A novel technique for embedding data in spatial domain. International Journal on Computer Science and Engineering, IJCSE, 2(2010).

[10] Motameni, H., Norouzi, M., Jahandar, M., & Hatami, A. (2007, October). Labeling method in Steganography. In Proceedings of world academy of science, engineering and technology (Vol. 24, pp. 349-354).

[11] Parvez, M. T., & Gutub, A. A. (2008, December). RGB intensity based variable-bits image steganography. In Asia-Pacific Services Computing Conference, 2008. APSCC'08. IEEE (pp. 1322-1327). IEEE.

[12] Babu, S. K., Raja, K. B., Kiran, K. K., Manjula Devi, T. H., Venugopal, K. R., & Patnaik, L. M. (2008, November). Authentication of secret information in image steganography. In TENCON 2008-2008 IEEE Region 10 Conference (pp. 1-6). IEEE.

[13] Dr. Harish Rohil, Parul1, Manju2, “Optimized Image Steganography using Discrete Wavelet Transform (DWT)”, International Journal of Recent Development of Engineering and Technology, ISSN 2347 - 6435 (Online) Volume 2, Issue 2, February 2014.

[14] Aayushi Verma, Rajshree Nolkha, Aishwarya Singh and Garima Jaiswal, “ Implementation of Image Steganography Using 2-Level DWT Technique”, International Journal of Computer Science and Business Informatics

[15] Banik, B. (2013). Prof. Samir K. Bandyopadhyay, A DWT Method for Image Steganography. International Journal of Advanced Research in Computer Science and Software Engineering, 3(6), pp. 983-989.

[16] T. Liu and Z. Qiu, “A DWT-Based Color Image Steganography Scheme,” in Proc. IEEE, 6th International Conference on Signal Processing , 2002, vol. 2, pp. 1568-1571.

[17] Narasimmalou, T., & Joseph, R. A. (2012, March). Discrete Wavelet Transform based steganography for transmitting images. In Advances in Engineering, Science and Management (ICAESM), 2012 International Conference on (pp. 370-375). IEEE.

[18] A. Nag, S. Biswas, D. Sarkar and P. P. Sarkar, A novel technique for image steganography based on DWT and Huffman coding, IJCSS, vol. 4, no. 6, pp. 561-570