Volume 5, Issue 6, June 2015 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

A Novel Approach to Image Steganography Using Hash-LSB and DWT Technique

Nikita Sharma[*]
M.Tech. Student, CSE Dept.
PDM College of Engineering and Technology,
Haryana, India

Meha Khera
Assistant Professor in CSE Dept.
PDM College of Engineering and Technology,
Haryana, India

Abstract—This paper is a review about two techniques of image steganography. In this paper, two techniques of image steganography are to be combined inorder to achieve secure transmission between sender and receiver. First is Hash-LSB Technique with RSA algorithm and another is Discrete Wavelet Transform (DWT) Technique. Both the techniques are of different domains. The Hash-LSB technique is from spatial domain where cover-image is first decomposed into bits planes and then least significant bit (LSB) of the bits planes are replaced with the secret data bits. The DWT (Discrete Wavelet Transform) is from transform domain where the wavelet coefficients are used to hide the message bits into an image bits. The Hash-based LSB technique with RSA algorithm encrypts the message before hiding it into cover image to perform cryptography and hide that encrypted secret message bits into the image bits to perform steganography. The DWT (Discrete Wavelet Transform) focuses on decreasing the complexity in image hiding while providing lesser detectability, better security and lesser distortion in the image. The DWT Technique used in this paper is "Haar DWT". This is a unique attempt to simplify the embedding procedure and to reduce the effort of concealing the secret image in the cover image and offer better results. Our main motive is to apply both the techniques to hide a message into a cover image in such a way that no one except the intended recipient can know the message. In any case if the attacker is able to decode the image from the secure stego image obtained by applying DWT technique, he can never have any idea that the image has the message encoded in it. Thus we can obtain a highly secure and highly robust image steganography by using these techniques.

Keywords— Image Steganography, Hash-LSB, RSA, DWT etc.

I. INTRODUCTION

Image Steganography is the art and science of invisible communication. The word steganography is derived from the Greek words "stegos" meaning "cover" and "grafia" meaning "writing" defining it as "covered writing". It is an art of hidden writing in which a secret message can be hidden behind an image without even knowing by the unintended recipient that the message exists. This is accomplished through hiding information in other information, thus hiding the existence of the communicated information. Steganography is the practice of hiding private or sensitive information within something that appears to be nothing out to the usual. Many different carrier file formats can be used, but digital images are the most popular because of their frequency on the internet.

For hiding secret information in images, there exists a large variety of steganography techniques some are more complex than others and all of them have respective strong and weak points. Different applications may require absolute invisibility of the secret information, while others require a large secret message to be hidden. What Steganography essentially does is exploit human perception, human senses are not trained to look for files that have information hidden inside of them, although there are programs available that can do what is called Steganalysis (Detecting use of Steganography.) The most common use of Steganography is to hide a file inside another file. When information or a file is hidden inside a carrier file, the data is usually encrypted with a password.

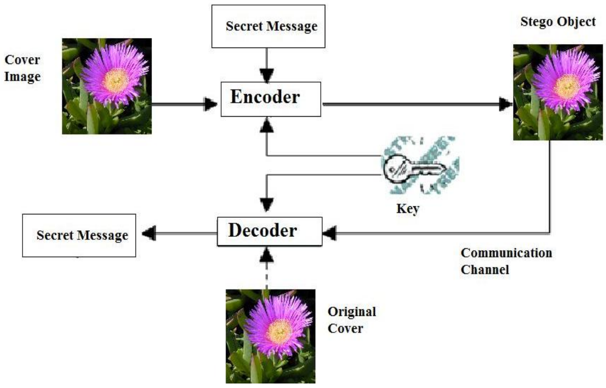


Fig1: Model of image steganography

Steganography is often confused with cryptology because the two are similar in the way that they both are used to protect important information. The difference between two is that steganography involves hiding information so it appears that no information is hidden at all. If a person or persons views the object that the information is hidden inside of he or she will have no idea that there is any hidden information, therefore the person will not attempt to decrypt the information.

In image Steganography, secret communication is achieved by embedding a message into cover image (used as the carrier to embed message into) and generate a stego-image (generated image which is carrying a hidden message). It is a high security technique for long data transmission.

II. TECHNIQUES USED

In this paper two techniques are proposed .Both of these techniques are from different domains. These techniques are:

1. Hash-LSB with RSA Algorithm
2. Discrete wavelet Transform(DWT) Technique

A. Hash-LSB (Least Significant Bit) technique

In hash-LSB technique, the least significant bit position where the secret data is to be hidden is determined by using the hash function .It finds the position of least significant bit of each RGB pixel, and then message bits are embedded in this RGB pixel independently. Firstly the cover image is broken or fragmented into RGB format. Then Hash-LSB will use the values from the hash function to integrate or hide data into the LSB of RGB pixel. In this technique, the secret message is converted into binary form as binary bits; each 8 bits at a time are included in the least significant values of RGB pixel image covering about 3, 3 and 2 bits respectively. Under this method 3 bits are embedded in red pixel LSB, 3 bits are embedded in green pixel and 2 LSB bits are embedded in blue pixel [3].These 8 bits are inserted in this order because the chromatic influence of blue color to the human eye is more than red and green color. Therefore the distribution pattern chooses the 2 bits to be hidden in blue pixel. Thus the quality of the image will be not sacrificed [1].

Hash function

The hash function deals with the LSB position and the pixel position of each pixel masked image, and also with the number of LSB bits. Hash value takes a variable size input and returns a fixed-size digital output string. Hash function is also used to detect duplicate folder in large files. Hash function generally given by:

i= j % k

Where, i is the position of LSB bit within the image pixels, j represents the position of each hidden image pixel and k is number of bits of LSB [3].

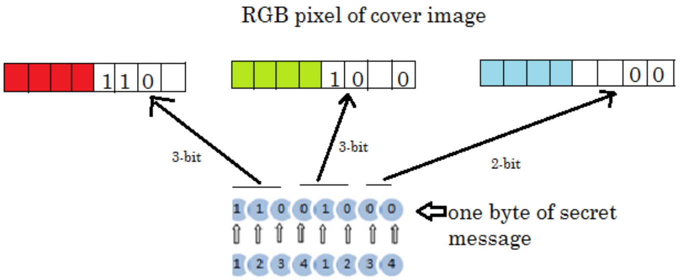


Fig 2: Hash-LSB Process

RSA algorithm

RSA is an algorithm used by modern computers to encrypt and decrypt messages. It is an asymmetric cryptographic algorithm. Asymmetric means that there are two different keys. This is also called public key cryptography, because one of them can be given to everyone. The other key must be kept private.

The RSA algorithm was defined by Rivest, Shamir and Adleman. This algorithm is used to encrypt the secret message into scrambled form. This algorithm works by taking two values of prime's and then the product of these values. This product value is used to make a public and a private key and this is also used in the encryption and decryption methods. The RSA algorithm can be used in combination with Hash-LSB so that the original message is inserted into the cover image frame as cipher text. RSA algorithm increases the security level of image steganography [3]. It provides security by converting secret data into a cipher text, which will be difficult for any intruder to decrypt it without the recipient private key. When RSA is used with Hash-LSB technique, first of all we take cipher text encrypted from the secret message to be embedded in the cover image. Then we convert cipher text into binary form to convert it into bits. Then by using hash function it will select the positions and then 8 bits of message at a time will be embedded in the order of 3, 3, and 2 in red, green and blue channel respectively. The process is continued till entire message of bits will got embedded into the cover image. Thus in this way by using RSA algorithm with Hash-LSB technique both the cryptography as well as steganography can be achieved. So the chances of security would be more [1].

RSA algorithm procedure can be illustrated in brief as follows:

(i) Select two large strong prime numbers, p and q. Let n = p q.
(ii) Compute Euler's totient value for n: f (n) = (p - 1) (q - 1).
(iii) Find a random number e satisfying 1 < e < f (n) and relatively prime to f (n) i.e., gcd (e, f (n)) = 1.
(iv) Calculate a number d such that d = e-1 mod f (n).

(v) Encryption: Given a plain text m satisfying m < n, then the Cipher text c = m^e mod n.
(vi) Decryption: The cipher text is decrypted by m = c^d mod n.

Hash-LSB with RSA Technique (embedding of secret message into cover image)

Step1: Select the 24-bit RGB cover image.
Step2: Take the secret message that is to be embedded into the cover image.
Step3: Encrypt the secret message using RSA Algorithm.
Step4: Convert the encrypted message into binary form.
Step5: Find 4 least significant bits of each RGB pixels from cover image.
Step6: Apply a hash function on LSB of cover image to get the position. Step 5: Embed eight bits of the encrypted message into 4 bits of LSB of RGB pixels of cover image in the order of 3, 3 and 2 respectively using the position obtained from hash function.
Step7: Send stego image to receiver.

B. DWT technique

Discrete wavelet transforms are used to convert the image in spatial domain to frequency domain, where the wavelet coefficients so generated, are modified to conceal the image. In this kind of transformation the wavelet coefficients separates the high and low frequency information on a pixel to pixel basis**.**

The DWT represents an image as a sum of wavelet functions, known as wavelets, with different location and scale. It represents the data into a set of high pass (detail) and low pass (approximate) coefficients. The input data is passed through set of low pass and high pass filters. The output of high pass and low pass filters are sampled. The output from low pass filter is an approximate coefficient and the output from the high pass filter is a detail coefficient. Human eyes are less sensitive to the high frequency signals.

When DWT is applied on an image, it divides the image in frequency components. The low frequency components are approximate coefficients holding almost the original image and high frequency components are detailed coefficients holding additional information about the image. These detailed coefficients can be used to embed secret image. Here we will take an image as cover object and another small image as secret message. In embedding process, first we convert cover image in wavelet domain. After the conversion we manipulate high frequency component to keep secret image data. These secret image data further retrieved in extraction procedure to serve the purpose of steganography.

Haar DWT

In this paper, Haar DWT" is proposed which is simplest of all the wavelet transform approaches. In this transform, time domain is passed through low-pass and high pass filters and the high and low frequency wavelet coefficients are generated by taking the difference and average of the two pixel values respectively. The operation of Haar DWT on the cover image results in the formation of 4 sub-bands, namely the approximate band (LL), horizontal band (HL), vertical band (LH) and the diagonal band (HH). The approximate band contains the most significant information of the spatial domain image and other bands contain the high frequency information such as edge details. Thus, the DWT technique describes the decomposition of the image in four non overlapping sub-bands with multi-resolution. This process can be iterated on one of the sub-band of first level DWT to get the further second level sub bands for better results [2].

A 2-dimensional Haar-DWT consists of two operations: One is the horizontal operation and the other is the vertical one. Detailed procedures of a 2-D Haar-DWT are described as follows:

Step 1 Scan the pixels from left to right in horizontal direction. Then, perform the addition and subtraction operations on neighbouring pixels. Store the sum on the left and the difference on the right.
Step 2 Repeat this operation until all the rows are processed. The pixel sums represent the low frequency part (denoted as symbol L) while the pixel differences represent the high frequency part of the original image (denoted as symbol H).
Step 3 Scan the pixels from top to bottom in vertical direction. Perform the addition and subtraction operations on neighbouring pixels and then store the sum on the top and the difference on the bottom.
Step4: Repeat this operation until all the columns are processed. Finally we will obtain 4 sub-bands denoted as LL, HL, LH, and HH respectively. The LL sub-band is the low frequency portion and hence looks very similar to the original image.

III. PROPOSED WORK

The proposed work is to combine these techniques (hash-LSB with RSA algorithm and DWT technique) to make message transmission between two parties more secure. In this work we are first encrypting the secret message using RSA algorithm. By applying RSA algorithm we obtain cryptography because it encrypts the message and convert it into unreadable form so that if unfortunately the message is revealed the intruder does not get any idea about the actual message. Then by applying Hash-LSB we are embedding the message into the cover image and obtain a stego image. Then we are applying DWT technique to embed this stego image into another cover image to obtain a secure stego image.

A. Steps followed in proposed work:

Step1: Secret message is first converted into encrypted form using RSA Algorithm.
Step 2: Then the encrypted message is converted into binary bits.

Step 3: 8 bits at a time are embedded in LSB of RGB pixel values of cover image in the order of 3, 3, and 2 respectively.
Step 4: 3 bits are embedded in red pixel LSB, 3 bits are embedded in green pixel LSB and 2 bits are embedded in blue pixel LSB.
Step 5: Their position is obtained by the formula:

$$k = p \% n$$ ……….……………..……

k is the LSB bit position within the pixel;

p represents the position of each hidden image pixel and n is the number of bits of LSB.

Step 6: After embedding the data in cover image, a stego image is obtained.
Step7: Input another cover image and then apply the 2-level DWT transform on the image. This will result in the formation of four bands i.e. LL1, HL1, LH1 and HH1.
Step8: For better imperceptibility, the DWT transform is applied once again on the LL band to get the next coarser scale of wavelet coefficients resulting in another level of sub-bands in HH1 band as LL2, HL2, LH2 and HH2.
Step9: Select LL2 sub-band for embedding the stego image for smooth and better extraction of the secret at the receiver's side.
Step10: Replace the 4 LSB of the LL2 band coefficient by 4 MSB of the secret image pixel.
Step11: Iterate the above step for n times (where n*n is the size of the secret image) and hence get the embedded secret.
Step12: Apply inverse DWT twice to retranslate the frequency domain information to the spatial domain and obtain the stego image which appears to be the same as the cover image.
Step13: Send the key information to the receiver

Key information=size of secret + name of the band + no of MSB bits of the secret embedded

IV. PERFORMANCEANALYSIS AND RESULTS

This work is implemented in MATLAB with an objective of better security and lesser detectability. It is capable of hiding an encrypted text message (by RSA Algorithm) within an image using Hash-LSB technique. Then the stego image so formed is successfully hidden behind another cover image using DWT technique. Thus more security, confidentiality and lesser detectability is obtained from this work. To Show this we have compared the PSNR and MSE values of this technique (Hash-LSB with RSA algorithm and DWT technique) with PSNR and MSE of simple LSB with RSA algorithm technique. The performance of the Hash-LSB with DWT Technique has been evaluated on the basis of two measures –Mean Square Error(MSE) and Peak to Signal Noise Ratio(PSNR) and obtained values are much better than simple LSB Technique with RSA Algorithm. PSNR and MSE values between the Cover and Stego image can be obtained as follows:

$$\text{PSNR} = 10 \log (\text{peak})^{2}/\text{MSE}$$

And

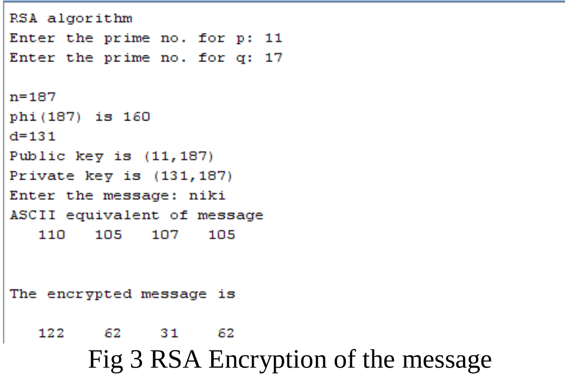
$$\text{MSE} = 1/MN\ ((S-C)\ 2)$$

Where MSE is mean-square-error,

Peak = 255,

M and N are the dimensions of the image,S is the resultant stego-image, and C is the cover image.

For this ,An image of Rabbit(jpeg format) is taken as a cover image to hide a encrypted message and that image of Rabbit with message encrypted within it is hidden behind another cover image of Lion(jpeg format)which results in secure stego image. Following results of the figures shows the above process in more details.



```
RSA algorithm
Enter the prime no. for p: 11
Enter the prime no. for q: 17

n=187
phi(187) is 160
d=131
Public key is (11,187)
Private key is (131,187)
Enter the message: niki
ASCII equivalent of message
   110   105   107   105


The encrypted message is

   122    62    31    62
```

Fig 3 RSA Encryption of the message

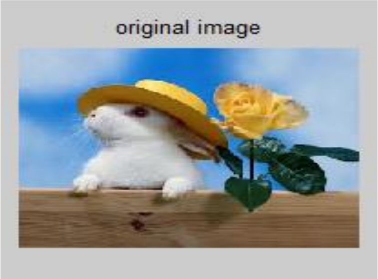
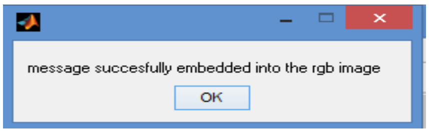


Fig 4 Original image



message succesfully embedded into the rgb image

Fig 5 Message successfully embedded into the image

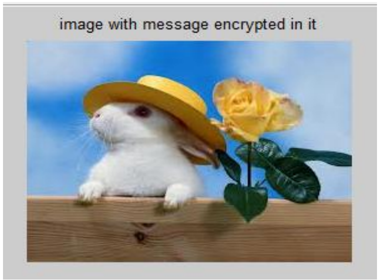


Fig 6 Stego image with hidden message

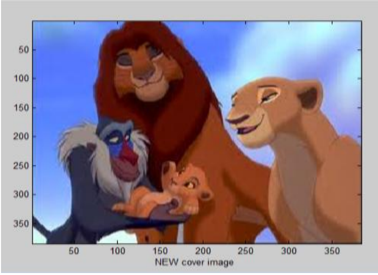


Fig 7 New cover image

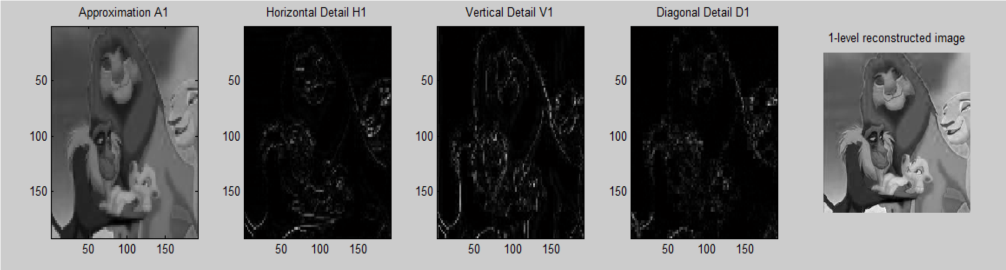


Fig 8 1-level DWT decomposition

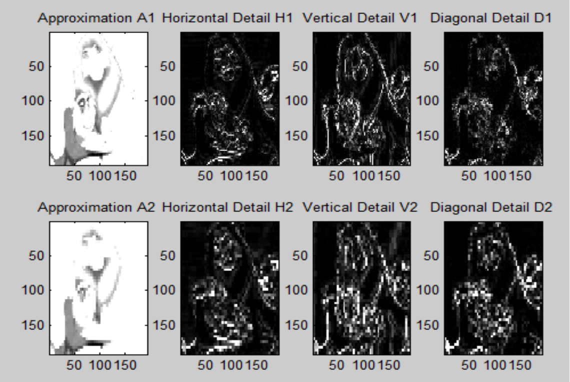


Fig 9 2- Level DWT decomposition

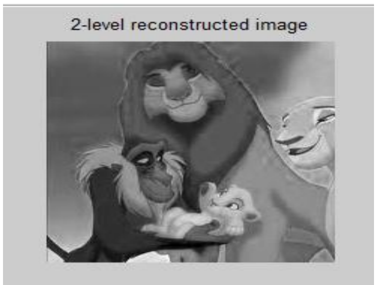


Fig 10 2- Level reconstructed image

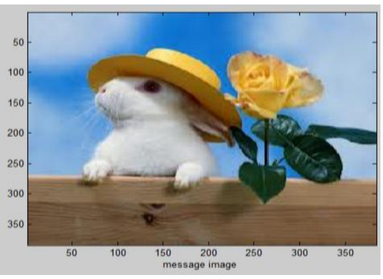


Fig 11 Message image

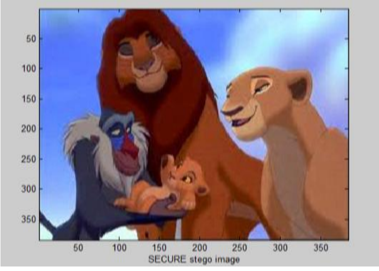


Fig 12 Secure stego image (Final Steganographed image)

After obtaining the final steganographed image using DWT technique we can decode that secure stego image by applying inverse of dwt i.e. idwt technique. Following images shows the decoding process.

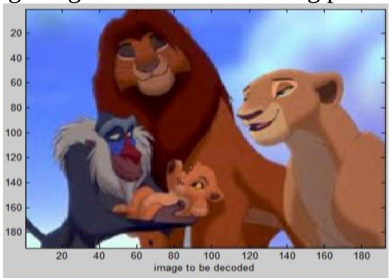


Fig 13 Image to be decoded

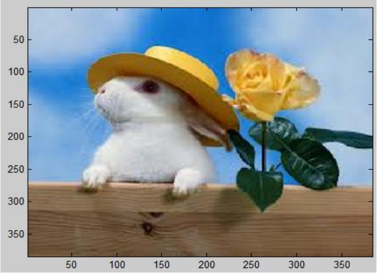
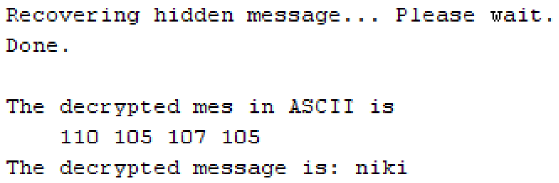


Fig 14 Decoded image



```
Recovering hidden message... Please wait.
Done.

The decrypted mes in ASCII is
    110 105 107 105
The decrypted message is: niki
```

Fig 15 Decrypted message

Table 1: Comparison of our results with LSB technique

Technique used	PSNR value	MSE value
Hash-LSB with RSA algorithm and DWT technique	51.18	0.4955
LSB with RSA algorithm	35.6742	16.25

The above result shows that PSNR value obtained from our work is 51.18 which is much more than PSNR obtained from LSB with RSA algorithm technique and the MSE obtained from our work is much less than the MSE value obtained from LSB with RSA technique. Thus we obtained larger PSNR value and lesser MSE value.

V. CONCLUSION

When Hash –LSB with RSA and DWT techniques are combined, chances of security in terms of lesser detectability, and lesser distortion in an image would be more because here the message is encrypted first before embedding into an image. When the stego image is achieved it will be again embedded into another cover image so that if in case if intruder is successful in obtaining the image within the cover image, he/she cannot get any idea that there is the message embedded in the image. If at worst case the intruder is successful in obtaining the message in the image he/she cannot revealed the message because it is in encrypted form. We are successful in achieving the above mentioned objectives. We are succeeded in hiding an encrypted message into an image using Hash-LSB Technique and that image is successfully hidden behind another image using DWT Technique which results in more secure stego image. This work results better PSNR value(51.18) than the PSNR value(35.67) obtained from LSB technique and lesser MSE value(0.49) than the MSE value(16.25) obtained from LSB technique with RSA Algorithm. When we perform image hiding at other bits like 7th, 6th we still obtain better PSNR and lesser MSE values than the value obtained from simple LSB technique with RSA algorithm. So this work gives better results in terms of security, confidentiality and detectability. This work is successfully implemented in MATLAB.

.

VI. FUTURE SCOPE

We can enhance this work by using different algorithm for encryption like AES, DES etc. which is more suitable for longer message encryption. Further we can use another technique for image hiding like DCT, IWT technique etc. This work can be enhanced for other data files like video, audio, text. Similarly the steganography technique can be developed for 3D images. The further work may contain combination of this method to message digesting algorithms

REFERENCES

[1] Anil kumar, Rohini Sharma, A Secure image Steganography based on RSA algorithm and Hash-LSB technique: A research paper published in International Journal of Advanced Research in Computer Science and Software Engineering Volume 3,Issue 7, pp 363-372, July 2013.

[2] Aayushi Verma, Rajshree Nolkha, Aishwarya Singh and Garima Jaiswal“Implementation of Image Steganography Using 2-Level DWT Technique”: A Research paper published in International Journal of Computer Science and Business informatics Vol.1, No.1, May 2013.

[3] Manpreet kaur and Amandeep kaur,”Improoved Security Mechanism of Text in Video Using Steganographic Technique”:A Research published in International Journal of Advanced Research in Computer Science and Management Studies Volume 2 , Issue 10,October 2014 .

[4] Kousik Dasgupta, J.K. Mandal and Paramartha Dutta,“Hash based least significant bit technique for video steganography (HLSB)":A Research published in International Journal of Security, Privacy and Trust Management Vol.1,No.2,April 2012 .

[5] NitinJain, Sachin Meshram, Shikha Dubey,”Image Steganography Using LSB and Edge Detection Technique”,A Research published in International Journal of Soft computing and Engineering(IJSCE*)* .Vol 2, issue 3, july 2012.

[6] Barnali Gupta Banik, Prof Samir K. Bandyopadhyaya ,”A DWT method for Image Steganography”,A Research published in International Journal of Advance research in Computer Science and Software Engineering2013. Vol 3, issue 6, pp 983-989.

[7] Prof.Dr. P R Deshmukh and Bhagyashri Rahangdale,”Hash Based Least Significant Bit Technique for Video Steganography”, A Research published in International Journal of Engineering Research and Application20. Vol 4, issue 1, Jan. 2014 pp 44-49

[8] Mamta Juneja, Parvinder Singh Sandhu, “Designing of Robust Image Steganography Technique Based on LSB Insertion and Encryption”, A Research published in International Conference on Advances in Recent Technologies in Communication and Computing, Pages No. 302 – 305, 27-28 Oct., 2009.

[9] Ying Wang, Pierre Moulin, “Perfectly Secure Steganography: Capacity, Error Exponents, and Code Constructions,” IEEE Trans. On Information Theory, Vol. 54, No. 6, June 2008.

[10] Swati Tiwari, R. P. Mahajan, “A Secure Image Based Steganographic Model Using RSA Algorithm and LSB Insertion”, A Research published in International Journal of Electronics Communication and Computer Engineering (IJECCE), Vol. 3, Issue No. 1, 2012.

[11] N. F. Johnson, S. Jajodia, "Steganography: seeing the unseen”, IEEE Computer, Vol. 31, Issue No. 2, Pages No. 26 - 34, Feb., 1998