An Efficient Steganography Model Using Video Compression and Image Steganography

Baheja KudhairShukur Saba Mohammed Hussain Ali Kadhim AL-Bermani
College of Information Technology, University of Babylon
baheja2003@yahoo.com saba_muh@ymail.com ali@itnet.uobabylon.edu.iq

Abstract

A process of hiding the secret information in the cover media (i.e. image, audio, video, etc.) is called as Steganography, these cover media suffer from different problems that effect on their efficiency and performance such as the capacity of cover media. This paper overcome this problem and provide a method for embed secret image into videos which provide high security with computing speed, and without producing visible changes, which reduce the size of the cover video image clip before hiding secret color image (BMP format) in it, this method applied discrete wavelet transform (DWT) on the frames resulted from the video image, which produced LL, HH, LH, HL bands. Block based algorithm used to hide the secret information or image in the random selected LL frame, where a video can be viewed as a sequence of still images (frames) and the secret image are inserted in these frames. This method depends on searching for the similarity among the hiding data blocks and others in the cover image.

Then construct the compressed video clip containing secret data. in the other side the receiver used inverse discrete wavelet transform (IDWT) after cutting the compressed video into frames to done the decompression process on it ,then extract the secret image from the stego frame .Finally construct the uncompressed video.

Mean Square Error(MSE), Peak signal to noise ratio (PSNR) and average difference(AD)are used to measure the quality of the compressed cover frame image and stego image, also compression ratio(C.R) are calculated between the original video clip image and stego-compressed video clip image, which show a very good result ,this system implemented using Visual basic.6 programming language.

Key words: C.R, AD, PSNR, DWT, IDWT, Steganography.

الخلاصة

علم الإخفاء هو العلم الذي يقوم بإخفاء المعلومات السرية في وسائط الغطاء مثل الصور, الصوت والفيديو والتي تعاني من مشاكل متعددة في كفاءتها وانجازها مثل سعة وسائط الخزن.ولتلافي مثل هذه المشاكل قدم هذا البحث طريقة لإخفاء الصور في مقاطع من الفيديو والتي وفرت أمنية عالية وسرعة في الحساب وبدون حصول تغييرات ملحوظة ,حيث يتم تقليل حجم صورة الفيديو الغطاء قبل إخفاء الصورة المراد إيصالها بداخله وذلك باستخدام طريقة التحول المويجي على الفريمات الناتجة من تقطيع صورة الفيديو والتي تكون أربع حزم **HL, LL, LH, HH.**

تستخدم طريقة تشابه البلوكات لإخفاء الصور في فريمات حزمة الـ **LL** المختارة عشوائيا ,والتي تعتمد على إيجاد التشابه بين كتل البيانات المخفية والأخرى في الصورة الغطاء.

وبعدها يتم إرجاع الفيديو وعرضه وهو يحمل بداخلة معلومات الصورة المخفية وعند الاستلام تجري عملية فتح الضغط باستخدام معكوس التحويل المويجي لاسترجاع الحجم الأصلي لصور فريمات الغطاء ومن ثم استخلاص الصورة المخفية من صورة الفريم الغطاء .

ولقياس كفاءة هذه الطريقة المستخدمة للإخفاء تم استخدام ومعدل الاختلاف و **MSE** و **PSNR** بين فريمات صورة الغطاء المضغوطة وبين صورة الغطاء .وكذلك تم احتساب **C.R** بين الصورة المضغوطة والصورة المسترجعة .

الكلمات المفتاحية: نسبة الضغط، معدل الفرق، نسبة الاشارة للضوضاء، تحويل الاشارة الموجي، معكوس تحويل الاشارة المويجي، اخفاء المعلومات.

1-Introduction

The origin of this word is Greek, which consist of two parts the first one is "concealed writing" from the Greek words steganos which means "covered or protected", and the second part is graph that means "to write" (Sravanthi and Sunitha Devi, 2012).

Steganography is the science that maintain communication and makes the information in it to be secret. This secret information can be hidden in multimedia such

as image, audio, or video (Hemalatha, *et al.*, 2013). The hiding system must satisfy three different facts i.e. capacity, security, and robustness. The meaning of the capacity is that the cover media that the data are to be hidden should contain the data (Shamim and Kattamanchi, 2012). Security means the encryption algorithm must be secure enough against the attacker, finally, robustness means the manipulation on the cover image can be made without being noticeable by anyone.

One kind of steganographic systems is an image steganographic scheme, where the same hiding method is used to hide the secret information in a digital image(Nitin and Sachin, 2012).To recover the hidden information from the image the receiver is used as an embedding technique. The information embedded image is called a stego image and the original image is called a cover image in steganography, (Amin *et al* 2003).

Three requirements have been used to satisfy the strong steganography technique (i) the amount of load embedded into the cover image is called the ability measurement . (ii) Ambiguities are the cover image which should be like the stego image. (iii) The steganographic algorithm should not be revealed to hackers (Prabakaran and Bhavani, 2013).

The steganographic techniques are classified according to the choosing of the hiding medium as the criteria, (i) Text based Steganography uses printed normal text to hide secret information. (ii) Audio based Steganography uses a cover audio file to hide the message. (iii) Image based Steganography uses the images to hide the secret message. Hide secret information in intensity of image pixel directly is called the spatial domain approaches. When the images are transformed into frequency coefficients and secret information are hidden in transformed coefficients the method is called the transform domain technique. With digital data being the carriers and networks being the high-speed delivery channels the steganography techniques are mostly used for computers (Mamta and Sandhu, 2009).

The form of video and digital image need huge quantity of storage space and capacity. To display the digital data related to video and image in a reasonable amount of time across the internet, where these data seem to be too large to be transmitted through the internet a number of techniques are used, called compression (Harjeetpal and Sakhi , 2012).

Both of lossy and losses compression techniques save storage space but have diverse consequences. The first type of compression which saves more space and attains a high level of compression and supplies much higher compression ratios than lossless method .The quality of the reconstructed images of this method made it adequate for most applications, but the originality of the image may be affected and the bits may be altered largely (Joab and Karen, 2002).This type includes a number of techniques like: Transformation coding, vector quantization, fractal coding, block truncation Coding and sub band coding. (Khalil, 2010).The second type is lossless compression where the original image data stay as it is before the compression process ,which is preferred for medical imaging, technical drawings .Since they do not add noise to the video/image, therefore this type of compression techniques is called noiseless. Sometimes it is identified as entropy coding because it utilizes statistics/decay techniques to remove/reduce redundancy. This method include number of techniques such as:Run length encoding, Huffman encoding, LZW coding and Area coding.(Navrisham 2013).
In this paper the discrete wavelets transform (WT) used in the image steganographic model which partitions the image into two parts which are the high-frequency and low-frequency information on a pixel by pixel. The use of this transform shows the capacity and robustness of the Information Hiding system.

2-The structure of the suggested system:

The structure of this system includes two parts; compression and steganography. The compression part includes the application of the DWT on the frames resulted from video clips. The steganography part includes hiding the secret message using hiding algorithm in random selected frame. Figure (1) and figure (2) show the block outline of the main stages for compression and hiding and the decompression and extracting processes.

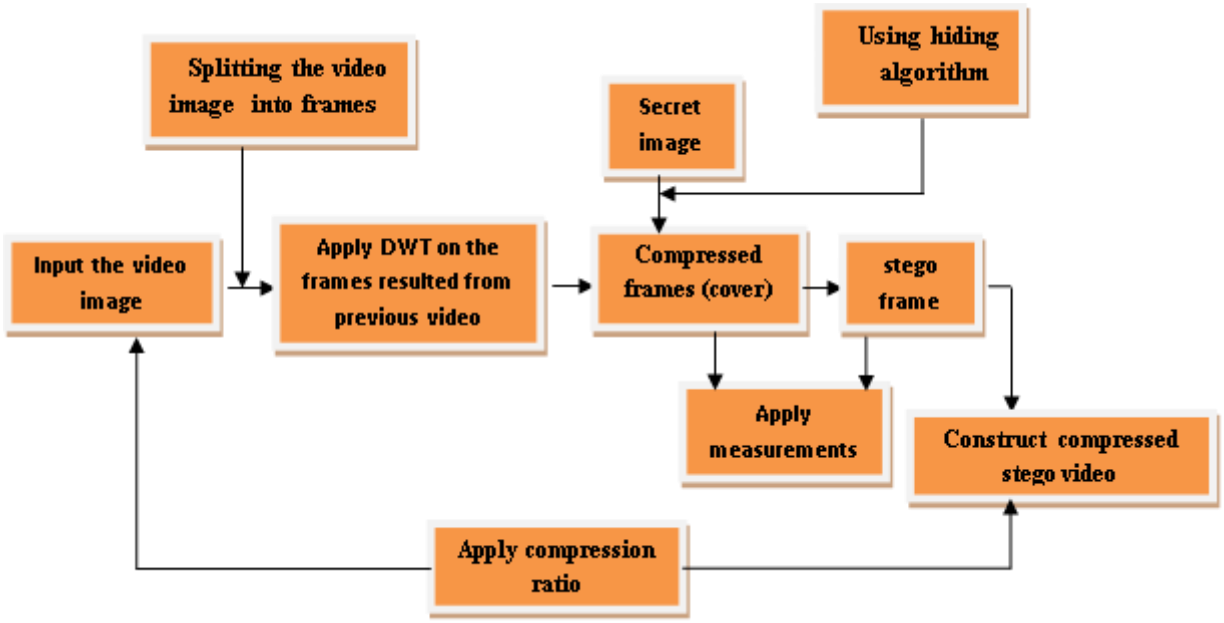

Figure (1):The compression hiding process stage

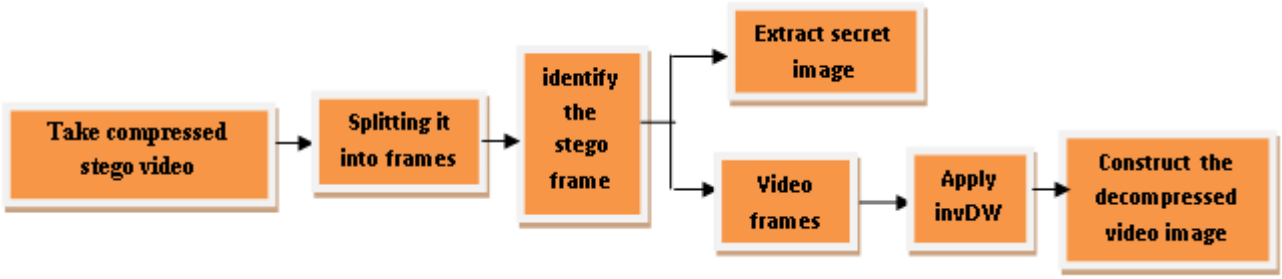

Figure (2):The decompression and extracting process stage

3- The DWT of an Image

In two dimension discrete wavelet transform for the image divided into four bands, which are approximation and details. The first one of these is, which hold the most energy of image while the three others hold the little energy information (Padmaja, and Nirupama, 2012). This process for image compression is carried out by two analysis filter pair which are a lowpass and a highpass filters(Souvik Bhattacharyya, Gautam Sanyal, 2012).To get low frequency components of the row Convolve the lowpass filters with rows of image. To obtain the Lowpass-Lowpass (LL) subimage Convolve the lowpass filters with the columns resulted above. Also to obtain the (LH) Subimage the lowpass filtered

rows convolved with the highpass filter on the column. To extract the high frequency the row of the original image convolve with the highpass filters. To acquire the (HL) Sub image convolves the result of the highpass filter with the lowpass filtered on the columns. Finally convolves the result of the highpass filter on the column with the highpass filter to find the Highpass_Highpass (HH) sub image. By choosing only the odd or even locations of the sub-bands the down sampler are implementing (Mohammed, 2012).In the process of the inverse wavelet transform performed the enlarging operation on the wavelet transform data to its original size. Then horizontally and vertically insert zeros between each two values, and the (lowpass and highpass) inverse filters to each of the four sub images convolve corresponding, at last to obtain the original image sum the results.

4-The Hiding Algorithm:

In data hiding most researches used LSB method, which suffer from many problems that affect on the efficiency of the resulted embedding method. This method is used for hiding BMP image (stego image) file in video file (cover image) using similar blocks between the cover image and secret image.

At the first step the image is divided into blocks . Different sizes for block are used to obtained high security for different experiments. To obtain high capacity the cover image frames are also divided into overlapping blocks.

In second step, the absolute difference calculated between each embedded stego block and all blocks of the video image to find the similarity using the following equation:

$$AD(S_i) = \left| \sum_{j=1}^{n} S_i - V_j \right|,$$ S_i and V_j represent the block of secret image and compressed cover video frame respectively.

Whereas the numbers of blocks in cover image are represented by n. The near less absolute difference selected and store it, to use in the restoring process to represent a key sequence.

4.1Hiding algorithm:

1- Choose the secret image.

2- Select randomly the cover video frame which is resulted from DWT.

3- For each secret image and selected compressed video frame separate them into size **(**N*N) of blocks.

4- For each block of the secret image select embed block from secret image blocks.

5- For each block of the compressed cover video frame select cover blocks and achieve the absolute difference equation to obtain the less absolute difference.

6--Save the block number in a file.

In the extraction process each block of stego image is extracted from video image frame using the positions that are stored in the separated key sequence.

4.2Extracting Algorithm:

1.For each block of the stego image.

2.Get the position of the key sequence.

3.The Extract embed block extract from video frame block at that position obtain from key sequence.

5- Performance measurements:

For assessment of the quality and robustness of steganograpic system, also to make it difficult to detect by interceptors a number of quality measurements is used

such as the **MSE**, which is defined as a common measure of estimation error between compressed video frame image and image to be embedded , can be defined as follows:

$$MSE = \sum_{x=0}^{N-1} \sum_{y=0}^{M-1} [S(x,y) - V(x,y)]$$

Second formula is **PSNR**, which calculates the ratio between the peak signal to noise between compressed video image frame and stego image as shown in this formula:

$$PSNR = 10 \log_{10} \frac{(L-1)^2}{\frac{1}{(N \times M)} \times \sum_{x=0}^{N-1} \sum_{y=0}^{M-1} [S(x,y) - V(x,y)]^2}$$

Where L is the number of the level in the image.

The third equation which computes the AD between the video image frame and the image to be embedded denoted by an Average Different (AD), the equation is as shown:

$$AD = \sum_{x=0}^{N-1} \sum_{y=0}^{M-1} [S_{xy} - V_{xy}] / MN$$

6- Experiments results

To prove the efficiency of the suggested system a number of experiments are studied as shown in the tables and histograms below:

Table (1) shows the video images used with their resulted DWT images and the size of the original and compression file and the time of these clips:

Table (1): The video images used with their resulted DWT images and the size of the original and compression file and the time for these clips

Video images	DWT frames images	Original size In byte	Compressed size in byte	Compression ratio	Time in second
		4,288,512	1,062,912	75.21	4
		4,772,352	1,122,816	76.47	4
		5,763,072	1,442,816	74.964	1
		1,082,880	272,896	74.79	1
		3,157,504	792,576	74.89	3
		26,501,120	9,128,448	65.554	7
		6,974,976	1,747,456	74.94	8

While table (2) show the measurements used to evaluate this study such as PSNR, MSE and AD:

Table (2): The resulted measurements used to evaluate this study such as PSNR, MSE and AD.

Cover image	secret image	Stego image	PSNR	MSE	AD
			91.930	.464	-.976
			75.853	.563	-1.071
			70.150	.608	-1.2687
			83.782	.509	.153
			64.7991	.6585	.6301
			85.1471	.5011	-.4861
			127.184	.3255	.42188-

Figure (3) shown the original image which considered as cover image frame and the image embedded in it and the histogram of them.

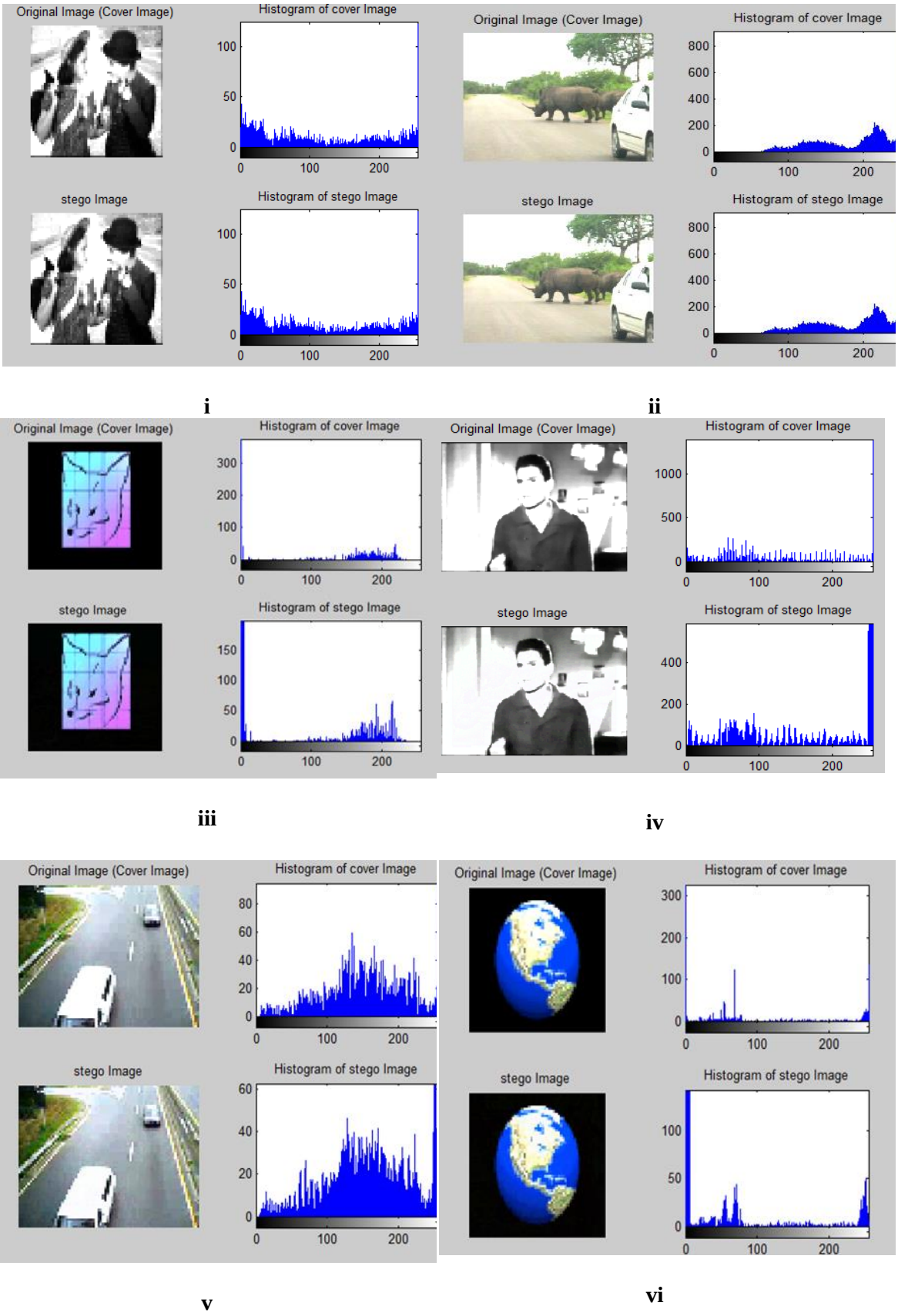

Figure (3) The Histogram of cover frame image and stego images.

7- Conclusion

1- The method of the compression is used to reduce the size of the video image and make it easy to transmit in less time, which achieves a good compression ratio without any effect on the quality of the resulted video.
2- This system provides high security, which combine the compression and stegaanography together, where it begins at video image compression then hiding secret image in it.
3- Our results refer to higher image quality, which comes from performance measurements such as PSNR, MSE, and AD. i.e. there is only little difference between the cover image frame and the stego image.
4- The histogram of the compressed video frame and stego image show there is no or little difference between them depending on the resulted measurements.
5- The suggested method is is much stronger than stegano analysis, since he needs to find the key sequence and the number of the frame that the secret image puts in it.
6- The method of hiding in the LL band of the video frame and the hiding algorithm provide a higher hiding capacity with lower distortion.

References

Amin, M.M.; M. Salleh, S. Ibrahim, M.R.Katmin, M.Z.I. Shamsuddin, 2003 "Information Hiding using Steganography" Proceedings of 4th National Conference on Telecommunication Technology, Shah Alam, Malaysia.

Harjeetpal singh, Sakhi Sharma, October 2012 "Hybrid Image Compression Using DWT, DCT & Huffman Encoding Techniques", International Journal of Emerging Technology and Advanced Engineering, ISSN 2250-2459, Volume 2, Issue 10 .

Hemalatha , U Dinesh Acharya, Renuka, Priya R. Kamath, February 2013,"A Secure and High Capacity Image Steganography Technique", Signal & Image Processing : An International Journal (SIPIJ) Vol.4, No.1.

Joab Winkler, Karen Lees, May 2002 "Image Compression Using Wavelets".

Khalil, M.I.; 1 February, 2010 "Image Compression Using New Entropy Coder", International Journal of Computer Theory and Engineering, Vol. 2, No.

Mamta, J. and P.S. Sandhu, 2009 "Designing of robust image steganography technique based on LSB insertion and encryption", Proceedings of the IEEE International Conference on Advances in Recent Technologies in Communication and Computing, Oct. 27-28, IEEE Xplore Press, Kottayam, Kerala, pp: 302-305. DOI: 10.1109/ARTCom.2009.228

Mohammed Mustafa Siddeq, 2012, "Using Two Levels DWT with Limited Sequential Search Algorithm for Image Compression ", Journal of Signal and Information Processing, 3, 51-62

Navrisham Kaur,January 2013, "A Review of Image Compression Using Pixel Correlation & Image Decomposition with Results", International Journal of Application or Innovation in Engineering & Management (IJAIEM), Volume 2, Issue 1, ISSN 2319 - 4847.

Nitin Jain, Sachin Meshram, Shikha Dubey, July 2012" Image Steganography Using LSB and Edge – Detection Technique ",International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307, Volume-2, Issue-3.

Padmaja, G.M.; P.Nirupama May 2012, "Analysis of Various Image Compression Techniques", ARPN Journal of Science and Technology, VOL. 2, NO. 4, ISSN 2225-7217.

Prabakaran Ganesan and R. Bhavani, 2013 "A High Secure and Robust Image Steganography Using Dual Wavelet and Blending Model", Journal of Computer Science, (3): 277-284, ISSN 1549-3636.

Shamim Ahmed Laskar, and Kattamanchi Hemachandran, December 2012 "High Capacity data hiding using LSB Steganography and Encryption", International Journal of Database Management Systems (IJDMS) Vol.4, No.6.

Souvik Bhattacharyya, Gautam Sanyal, 2012, " A Robust Image Steganography using DWT Difference Modulation (DWTDM) ", I.J. Computer Network and Information Security, 7, 27-40.

Sravanthi, G.S.; Mrs.B.Sunitha Devi, S.M.Riyazoddin& M.Janga Reddy, 2012, "A Spatial Domain Image Steganography Technique Based on Plane Bit Substitution Method", Global Journal of Computer Science and Technology Graphics & Vision, Volume 12 Issue 15 Version 1.0.