Engineering Universe for Scientific Research and Management
(International Journal)
Impact Factor: 3.7
ISSN(ONLINE) : 2319-3069
Vol. 6 Issue 11
November 2014

DWT Domain Based Secure High Capacity Image Steganography Method

Arun Sharma
M.Tech.,C.S.E., S.a.t.i., Vidisha, 464001, India
Arunsharma9dec@gmail.com

***Abstract*— Steganography is a one of the technique for information hiding. With the help of steganography people can communicate secretly. It involves communicating secret data in an appropriate multimedia carrier such as Text, Image, audio, and video files. The main motive of steganography is to ensure that the transmitted message is completely hidden inside the cover signal, and thereby ensuring that the message is accessible only by the intended receiver and not by any intruders or unauthorized parties. The main purpose of this research is to propose a novel and secure high-capacity image steganography technique with the help of wavelet transform with acceptable levels of imperceptibility and high level of overall security. our method works as follows: first gray scale image and secrete information is encrypted for security purpose and then message is hidden inside the encrypted grey scale image in dwt domain while maintaining high capacity of secret information and finally decrypts the image for maintaining same visual quality. Advantage of this method is full reconstruction of secret data without having original image present on the recipient side. According to the Analysis, the proposed approach provides fine image quality and enough embedding capacity.**

***Index Terms*— Image steganography , payload, stego image, cover image, secret sharing.**

1. INTRODUCTION

The rising possibilities of modem communications need the special means of security especially on computer networking . The network security is becoming more important as the number of data being exchanged on the Internet increases. So, the confidentiality and data integrity are required to protect data against unauthorized access and this resulted in an explosive growth of the field of information hiding. Information hiding techniques are receiving much attention today due to fear of encryption services getting illegal, and copyright owners who want to track confidential and intellectual property , copyright protection against unauthorized access and use in digital materials (music, film, book and software) through the use of digital watermarks. Advance security is not maintained by the password protection but it is gained by hiding the existence of the data which can only be done by Steganography [1].

Steganography is an art and science of hiding information in some cover media. The term originated from Greek words means "covered writing". The objective of steganography is to hide the fact of communication. In the steganography the sender embeds a secret message into digital media (e.g. image) where only receiver can extract this message. It simply takes one piece of information and hides it within another. This hidden information can be plain text, cipher text, or even images. It is not intended to replace cryptography but supplement it. With the help of Steganography the chance of hidden message being detected can be reduced [2].

The performance of a steganographic system can be measured using imperceptibility, capacity, and robustness. The most important property is the statistical undetectability (imperceptibility) of the data, which measures how difficult it is to determine the existence of a hidden message. Other associated measures are the steganographic capacity, which determines the maximum information that can safely embedded in a work without having statistically detectable objects and robustness, which refers to how well the steganographic system resists the extraction of hidden data [3].

In the last decade, several steganographic methods have been developed, which can be classified into two types. Spatial domain methods and transform domain methods. Steganography techniques that modify the cover image and the secret image in the spatial domain are known as spatial domain methods. Various spatial domain based steganography namely LSB [4-6], PVD[7-8] , and GLM [9] has been proposed in literatures. In Spatial Domain based methods insertion is simpler and good for steganography, but it has major drawbacks: the ease of extraction. We don't want that an eavesdropper be able to read everything we are sending.

The need for enhanced security, has led to the development of other algorithms. LSB technique has weak resistance to attacks. So to overcome this shortcoming, researchers found a better way for hiding information in transform domain of the image . Transform Domain methods hides messages in significant areas of cover image which makes them robust against various image processing operations like

compression, cropping, enhancement etc. Many transform domain methods exist. The widely used transformation functions include Discrete Cosine Transformation (DCT)[10-13] , Fast Fourier Transform (DFT) [14], and Wavelet Transformation [15-19]. The basic idea to hiding information with DCT, FFT or Wavelet is to transform the cover image into frequency domain,, modify the coefficients, and then convert back to spatial domain. When the selection of coefficients is good and the size of the changes manageable, then the result is pretty close to the original.

In this paper we propose a novel method, that allows hiding a secret information in grey scale image while maintaining good visual quality and high capacity of secret information. Advantage of this method is full reconstruction of secret data without having original image present on the recipient side.

The organization of the paper is as follows. In the next section, basic image steganography model is described. . In Section 3 we give overview of DWT technique in the context of image steganography ,Section 4 defines the proposed methodology. We describe objective visual quality measurements to simulate human perception which are PSNR[dB] and PSNR [dB] modified by Contrast Sensitivity Function to better reflection of Human Visual System (HVS) model In Section 5.sectioin 6 gives the results of proposed method in manner of PSNR value using cover image with different detail levels. Some open problems of image steganography related to transform domain and some interesting direction that may be worth future research are discussed in Section 6. Finally, we conclude our paper in Section 7 with discussion and contribution of our proposed method to the image steganography.

2. Image Steganography model

The main goal of steganography is to communicate securely in a completely undetectable manner and to avoid drawing suspicion to the transmission of a hidden data. Steganography not only is used to prevents others from knowing the hidden information, but it also is used to prevents others from thinking that the information even exists [7].

Image steganography technique consists of Carrier file (Image), Secret message and Password. Carrier is also known as a cover-file, in which the secret information is to be embedded. Message is the data that the sender wishes to remain it confidential and wants to send inside the cover files. Message can be plain text , audio , image, or any type of file. Password is known as a stego-key, which is used to ensures that only the recipient who knows the corresponding decoding key will be able to extract the message from a cover-file. In general, The cover-file with the secret information is known as a stego-file.

To hide the data inside the cover image takes following two steps [7].

i. Identification of redundant bits in a cover-image. We can say that redundant bits are those bit that can be modified without corrupting the quality or destroying the integrity of the cover-image.

ii. To embed the secret information in the cover image, the redundant bits in the cover image is replaced by the bits of the secret information.

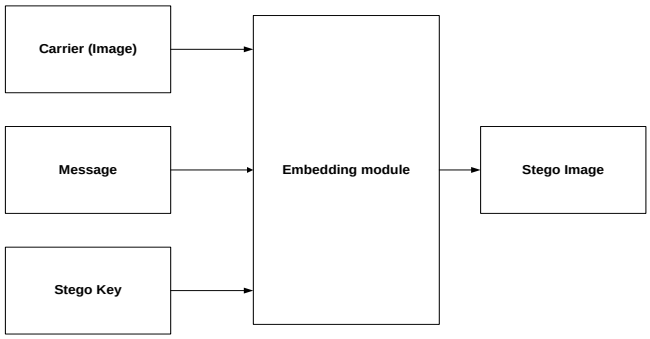


Fig1. Basic Image steganography model

3. Wavelet Transform in Steganography

Wavelets have been effectively utilized as a powerful tool in image processing [19,20]. Many practical tests propose to use the Wavelet transform domain for steganography because of a number of advantages that can be gained by using this approach. The use of such transform will mainly address the capacity and robustness of the Information- Hiding system features. The work described in this paper implements steganography in the Wavelet domain. The hierarchical nature of the Wavelet representation allows multi-resolutional detection of the hidden message, which is a generally Gaussian distributed random vector added to all the high pass bands in the Wavelet domain. It is shown that when subjected to distortion from compression, the corresponding hidden message can still be correctly identified at each resolution in the Discrete Wavelet Transform (DWT) domain [20,21].

In Wavelet transform, the original signal (1-D, 2-D, 3-D) is transformed using predefined wavelets. The wavelets are orthogonal wavlets, orthonormal wevlets, or biorthogonal wevlets, scalar or multiwavelets [21]. The DWT used in this paper is implemented using the functions available with MATLAB to simplify the analysis and minimize development time [21].

Engineering Universe for Scientific Research and Management
(International Journal)
Impact Factor: 3.7
Vol. 6 Issue 11
November 2014

For images, an algorithm similar to the one dimensional case is possible for two-dimensional Wavelets and scaling functions obtained from one dimensional ones by tensor product [22]. This kind of two-dimensional DWT leads to a decomposition of approximation coefficients at level j in four components: the approximation at level j+1, and the details in three orientations (horizontal, vertical, and diagonal), as depicted in Fig. 2.

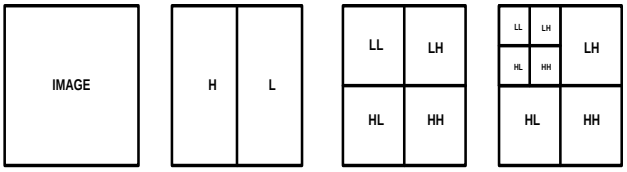


Fig 2. Two dimensional wavelet transformation of an image.

Fig. 3 describes the basic decomposition step for images using the 2D Wavelet transform. Increasing the levels will add complexity and computational overhead, but the robustness of the steganography method will be enhanced[20].

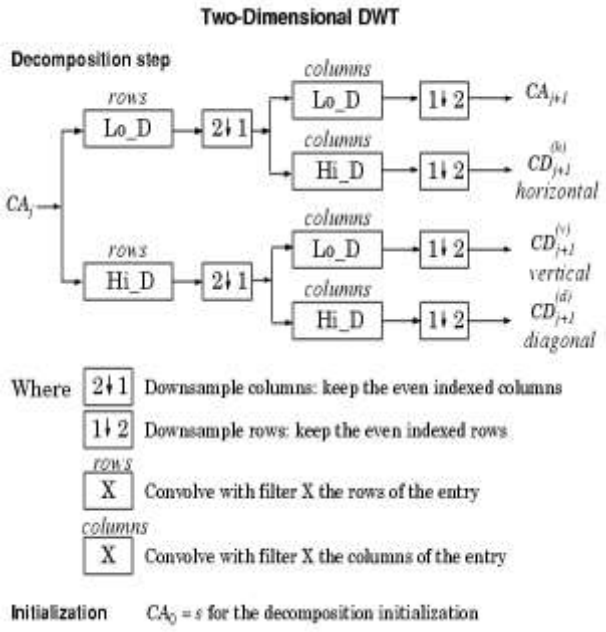


Fig 3.. Two dimensional wavelet decomposition.

4. Proposed Methodology

Proposed image steganography technique is divided into two modules:

A. Data Embedding Module
B. Data Extracting module

4.1 Data Embedding Module

1) Selection of the cover image in which data is to be hide and secret message which is to be embedded into cover image is performed in this step. The secret message can be any text file or image or any audio wave file. To embed the entire message ,Cover message must be sufficient large enough .Let X is the original 8-bit gray-level cover-image of M×N pixels.It is denoted as:

$$X = \{x_{ij} \mid 1 \le i \le M, 1 \le j \le N, x_{ij} \in \{0,1,...,255\}\}$$

2) To encrypt the image by using XOR operation, we first divide cover image X into block of 2 pixels × 2 pixels. And Then perform XOR operation on each and every pixel of block Bi,j of X ,Which returns encrypted block . To perform block level XOR operation ,we used 32 bit key which is divided into four eight bit sub key K1 , K2, K3 and K4 . XOR operation on each block with key is given below.

$$E_{1.1} = X_{1.1} \oplus K_1$$
$$E_{1.2} = X_{1.2} \oplus K_2$$
$$E_{2.1} = X_{2.1} \oplus K_3$$
$$E_{2.2} = X_{2.2} \oplus K_4$$

Where Xi,j is the pixel value at ith and jth location in block .and Ei,j is the encrypted pixel value at ith and jth location in new block.
When we perform XOR operation on each block with same 32-bit key we get the encrypted image E.

3) This step deals with encryption of the secret message. To do so, we convert the secret data or message into its binary form. Let P is the n-bit secret message represented as:

$$P = \{p_i \mid 1 \le i \le n, p_i \in \{0,1\}\}$$

Random number generator function is used to generate a random sequence K of length n and then apply X-OR operator on P with K to generate the cipher message K of length n bits.

$$S = P \oplus K$$

Where $K = \{k_i \mid 1 \le i \le n, k_i \in \{0,1\}\}$ and

Engineering Universe for Scientific Research and Management
(International Journal)
Impact Factor: 3.7
Vol. 6 Issue 11
November 2014

$$S = \{s_i \mid 1 \le i \le n, s_i \in \{0,1\} \text{ and } s_i = p_i \oplus k_i\}.$$

4) To obtain the frequency domain matrix F, We apply DWT on Encrypted image E . Frequency domain matrix is composed of 4 sub-bands denoted as F_{LL}, F_{HL}, F_{LH} and F_{HH} (size of all 4 sub-bands have the same M/2 × N/2). To hide the data , coefficient must be selected. So, The coefficients suitable for embedding are elected from detail areas F_{HL}, F_{LH} and F_{HH} which is F_{HH} and denoted as

$$F = \{f_{ij} \mid 1 \le i \le M/2, 1 \le j \le N/2\}$$

That is resized to same dimension as S.

5) Secret message embedding stage is based on one of the selected detailed coefficient of each image. The process of embedding message is defined as following pseudo code:
C=floor(Fij/T);
if S_{ij} == 0 ^ C mod 2 ==1 then C=C+1 and F'ij=C*T;
if S_{ij} == 0 ^ C mod 2 ==0 then F'ij=C*T;
if S_{ij} == 1 ^ C mod 2 ==0 then C=C+1 and F'ij=C*T;
if S_{ij} == 1 ^ C mod 2 ==1 then F'ij=C*T;
Where F'ij are modified coefficients of DWT detail area. and value of T should be multiple of 0.25.because applying DWT in 2D you eventually have to divide pixel values by 4 somewhere. So, when you obtain your image you will have pixel values with .00, .25, .50 and .75.

6) Based on modified detailed coefficient and unmodified approximate coefficient , IDWT is used that reconstruct the segments of stego- image. Stego image E' is obtained after Hiding all secret data and performing inverse DWT (IDWT) on F'ij.

7) Next Step is to performs the block level X-OR operation on encrypted stego image E'. Again we divided E' into block of 2 pixels × 2 pixels . And then XOR operation is performed to each and every pixel of block Bi,j of E'. X-OR operation on E' is applied by Same 32 bit key.:

$$X'_{1.1} = E'_{1.1} \oplus K_1$$

$$X'_{1.2} = E'_{1.2} \oplus K_2$$

$$X'_{2.1} = E'_{2.1} \oplus K_3$$

$$X'_{2.2} = E'_{2.2} \oplus K_4$$

Where X'i,j is the pixel value at ith and jth location in block inside pixel of Decrypted stego image X' and it is ready to be sent to receiver site.

4.2 Data Extracting Module

The extraction process is divided into multiple steps and defined as follows.

1) In the message recovery algorithm, we select the stego image Y from which data is to be extracted. Let the 8-bit gray-level stego-image of M × N pixels is represented as:

$$Y = \{y_{ij} \mid 1 \le i \le M, 1 \le j \le N, y_{ij} \in \{0,1,...,255\}\}$$

2) In this step is we perform the same X-OR operation on stego image Y with same key . We divided stego image Y into 2 pixels × 2 pixels blocks. Then XOR operation is performed to each and every pixel of block Bi,j of Y That yields the decrypted block .block level XOR operation is applied by same 32 bit key and work as follows.

$$E_{1.1} = Y_{1.1} \oplus K_1$$

$$E_{1.2} = Y_{1.2} \oplus K_2$$

$$E_{2.1} = Y_{2.1} \oplus K_3$$

$$E_{2.2} = Y_{2.2} \oplus K_4$$

3) Next apply DWT on E to obtain the frequency domain matrix F'. The 4 sub-bands obtained by applying DWT are denoted as F'_{LL}, F'_{LH}, F'_{HL},F'_{HH}.

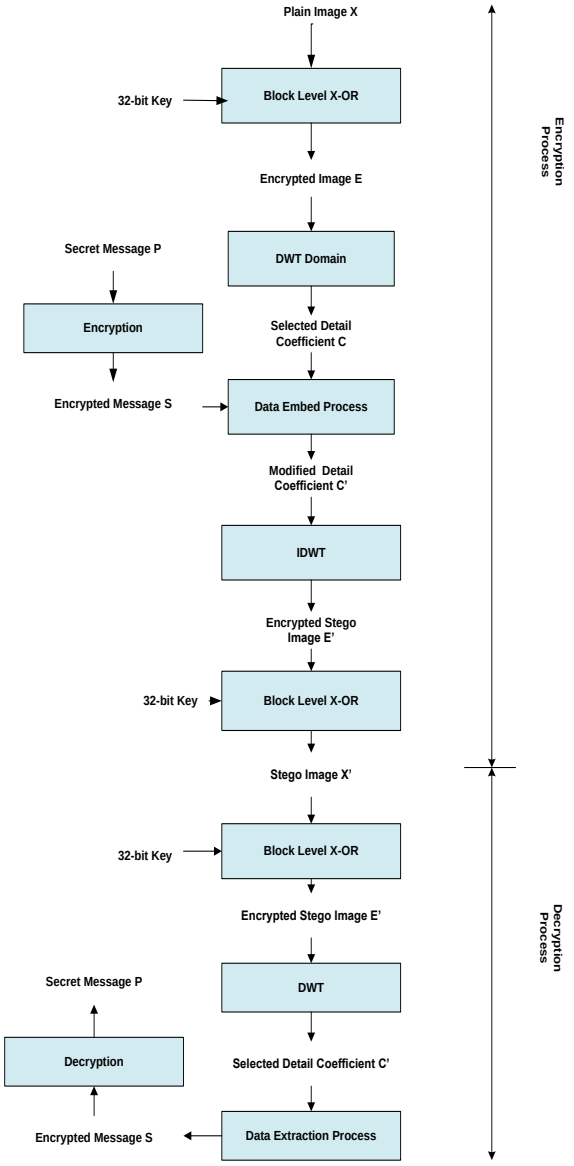
4) Secret message recovery stage is very simple and based on modulo operation of stego image coefficients F'ij in following way:

$$\hat{S}'_{ij} = \begin{cases} 0 \text{ if } C \bmod 2 == 0 \\ 1 \text{ if } C \bmod 2 == 1 \end{cases}$$

Where C=Floor (F'ij/T).

5) To decrypted the secrete message we use the same key that was used at the time of encryption. To generate the same key, we use the same random number generator. and then apply X-OR operation to get the original message of length n bits. And finally convert message of its binary form to text format .and delivered to the receiver.

Engineering Universe for Scientific Research and Management
(International Journal)
Impact Factor: 3.7
Vol. 6 Issue 11
November 2014



6)

Fig 4 Block diagram of the proposed system

5. Quality Measurement

The quality of the stego image and the extracted secret image is determined by calculation of certain quality measurement metrics [19,23]. These metrics gives the comparison ratio between the original image and the modified image. The quality may be assessed on the basis of these values. The metrics used in this paper are as follows:

5.1 Peak signal to noise ratio (PSNR)

The PSNR depicts the measure of reconstruction of the compressed image. This metric is used for discriminating between the cover and stego image. The easy computation is the advantage of this measure. It is formulated as:

$$PSNR = 10 \log_{10} \frac{255^2}{MSE}$$

A low value of PSNR shows that the constructed image is of poor quality.

5.2 Mean square error (MSE)

MSE is one of the most frequently used quality measurement technique followed by PSNR. The MSE [19,23] can be defined as the measure of average of the squares of the difference between the intensities of the stego image and the cover image. It is popularly used because of the mathematical tractability it offers. It is represented as:

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

Where f (i, j) is the original image and f‟ (i, j) is the stego image. A large value for MSE means that the image is of poor quality.

5.3 Peak signal to noise ratio (PSNR) Weighted by CSF

PSNR-CSF calculates the peak signal to noise ratio weighted by CSF function. The aim of this objective measure is to approximate to ideal subjective measures. The Human Visual System model (HVS) is part of PSNR calculation, where its frequency sensitivity is represented by 2D FIR filter. The coefficients for HVS are derived from CSF function. The weighting of correspondent spatial frequencies is attained by application of the 2D FIR filter to the error image. d

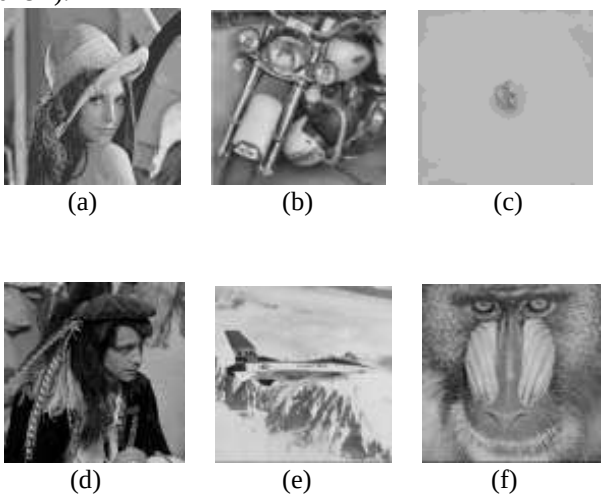
$$PSNR_{CSF} = 10 \log_{10} \frac{255^2}{\frac{1}{N_1.N_2} \sum_{i=1}^{N_1} \sum_{j=1}^{N_2} ((I - I^W) * g_{CSF})^2} [dB]$$

6. Experiment Result

Proposed technique, are implemented on Windows PC having Intel 2.4 GHz processor and 2GB RAM, and run using

Engineering Universe for Scientific Research and Management
(International Journal)
Impact Factor: 3.7
Vol. 6 Issue 11
November 2014

Matlab 9a. We have considered six different image files in this experiment to embed digital data. They are "Lena.bmp,"moterbikel.bmp","apple.bmp","Man.bmp",Plane .bmp"and "Baboon.bmp". All the images are 8 bit gray scale images and the dimension of all the image is 256×256 pixels shown in Fig 5. The embedded data is a text file of size (2048B).



(a) (b) (c)

(d) (e) (f)

Fig 5. Cover Images a) lena b) MoterBike c) Apple d) Man e)Plane f)Baboon

The capacity of the proposed method is represented by 1/4 of cover image size for 1-level decomposition of the cover image and it remains the same. The payload is 0.25 bit/pixel in case of using the maximum capacity and it also varies depending on numbers of detail coefficient are used during the embedding phase. The proposed algorithm employs 1-Level L decomposition of the image hence the total capacity (in bits) is represented by 1/4 of image size number of DWT detail coefficient altered. In our proposed system we set threshold value T to 0.5.

Table 1 shows comparison of PSNR values (quality) of obtained encrypted stego images by proposed method and base paper method [18]. The quality of our method's stego image is good and acceptable compared to the stego images' quality of steganography methods [18].

Table 1: The PSNR(dB) of Our proposed Steganography Method and other method considered

Cover Image		H_{HH} Selected Coefficient	
		Method[18]	Proposed Method
Lena	PSNR [dB]	63.174	63.1792
256×256	$PSNR_{CSF}$[dB]	311.286	310.9584
	Extraction %	49.908%	99.20%
Moterbike 256×256	PSNR [dB]	63.114	63.1313
	$PSNR_{CSF}$[dB]	311.662	310.9613
	Extraction %	49.56	99.5%
Apple 256×256	PSNR [dB]	63.096	62.6751
	$PSNR_{CSF}$[dB]	98.957	309.6617
	Extraction %	48.999	98.40%
Man 256×256	PSNR [dB]	-------	63.202
	$PSNR_{CSF}$[dB]	-------	312.7282
	Extraction %	-------	99.25%
Plane 256×256	PSNR [dB]	-------	63.1486
	$PSNR_{CSF}$[dB]	-------	309.9545
	Extraction %	-------	99.35%
Baboon 256×256	PSNR [dB]	-------	63.1977
	$PSNR_{CSF}$[dB]	-------	311.3252
	Extraction %	-------	98.45%

In our method, we embedded the secret bits by modifying high coefficients; therefore the stego images of our method have good quality. However, we can embed the same message by slightly modified the middle and low frequency coefficients, the visual quality of image may be depredated but the robustness will be increased.

7. Conclusion

The research aim of this paper is to increase the steganographic capacity and improve the quality of stego images. In this paper, we proposed a novel and secure image steganography method utilizing the features obtained from DWT coefficients. Because the secret messages are embedded in the high frequency sub-bands which human eyes are less sensitive to visualize, So Quality of embedded images is increased. Experimental shows that, the proposed approach provides fine image quality and enough embedding capacity. Furthermore, respectable security is maintained as well since no message can be extracted without the "Key matrix" and the decoding rules.

The proposed scheme was tested for different hiding capacity and the results showed that it has excellent output quality. From the tests we find the proposed algorithm support high capacity rate reach up to ¾ bits per pixel and that is form above 75% from the size of the input image cover file at PSNR above 63 dB for the output signal.

REFERENCES

[1]. Zaidoon Kh., AL-Ani, A.A.Zaidan, B.B.Zaidan and Hamdan.O.Alanazi," Overview: Main Fundamentals for

Steganography ", journal of computing, volume 2, issue 3, March 2010.
[2]. Rajkumar Yadav," Study of Information Hiding Techniques and their Counterattacks", International Journal of Computer Science & Communication Networks, p.p. 142-164 Vol 1(2), Oct-Nov 2011.
[3]. Shikha Sharda,, Sumit Budhiraja," Image Steganography: A Review", International Journal of Emerging Technology and Advanced Engineering, Volume 3, Issue 1, January 2013.
[4]. C.K. Chan. and L. M.Cheng. Hiding data in images by simple lsb substitution. Pattern Recognition, 37:469–474, 2004.
[5]. Y. K. Lee. and L. H.Chen. High capacity image steganographic model.IEE Proc.-Vision, Image and Signal Processing, 147:288–294, 2000.
[6]. C.F. Lin. R.Z. Wang. and J.C. Lin. Image hiding by optimal lsb substitution and genetic algorithm.Pattern Recognition, 34:671–683, 2001.
[7]. D.C. Wu. and W.H. Tsai. A steganographic method for images by pixel value differencing. Pattern Recognition Letters, 24:1613–1626, 2003
[8]. P Huang. K.C. Chang., C.P Chang. and T.M Tu. A novel image steganography method using tri-way pixel value differencing. Journal of Multimedia, 3, 2008.
[9]. Potdar V.and Chang E. Gray level modification steganography for secret communication. In IEEE International Conference on Industria Informatics., pages 355–368, Berlin, Germany, 2004.
[10]. Derek Upham. Jsteg http://zooid.org/~paul/crypto/jsteg/.
[11]. [Andrew Westfeld. F5-a steganographic algorithm: high capacity despite better steganalysis. In Proceedings of the 4th Information Hiding Workshop, volume 2137 of LNCS, pages 289{302. Springer, 2001.
[12]. [K. Solanki, A. Sarkar, and B. S. Manjunath. Yass: Yet another steganographic scheme that resists blind steganalysis. In Proceedings of the 9th Information Hiding Workshop, volume 4567 of LNCS, pages 16{31. Springer, 2007.
[13]. Ajit Danti and Preethi Acharya. Randomized embedding scheme based on dct coefficients for image steganography. IJCA Special Issue on Recent Trends in Image Processing and Pattern Recognition, 2010.
[14]. Debnath Bhattacharyya , Tai - hoon Kim ; — Image Data Hiding Technique Using Discrete Fourier Transformation ‖ , Ubiquitous Computing and Multimedia Applications Communications in Computer and Information Science,2011.
[15]. Po-Yueh Chen and Hung-Ju Lin. A dwt based approach for image steganography. International Journal of Applied Science and Engineering, 4:275–290, 2006.
[16]. V. Kumar and D. Kumar. Performance evaluation of dwt based image steganography. In Proceedings of Advance Computing Conference (IACC), 2010 IEEE 2nd International, pages 223–228, 2010.
[17]. H S Manjunatha Reddy and K B Raja. High capacity and security steganography using discrete wavelet transform. International Journal of Computer Science and Security (IJCSS), 3:462–472.
[18]. Vladimír BÁNOCI, Gabriel BUGÁR, Dušan LEVICKÝ, A Novel Method of Image Steganography in DWT Domain", 21st International Conference on Radioelektronika , Page(s):1 - 4 , April 2011.
[19]. Vikas pratap singh and Prof. Shrikant Lade "A Novel and Secure technique for image Steganography using DWT", International Journal of Computer Technology and Electronics Engineering (IJCTEE) Volume 3, Issue 5, October 2013.
[20]. Jamil, T., "Steganography: The art of hiding information is plain sight", IEEE Potentials, 18:01, 1999.
[21]. Rajkumar Yadav," Study of Information Hiding Techniques and their Counterattacks", International Journal of Computer Science & Communication Networks, p.p. 142-164 Vol 1(2), Oct-Nov 2011.
[22]. http://www.techopedia.com/definition/14738/data-hiding.
[23]. Sumathi Poobal, G. Ravindran,"The Performance of Fractal Image Compression on Different Imaging Modalities Using Objective Quality Measures," International Journal of Engineering Science and Technology (IJEST), Vol. 2, Issue 1, Jan-Feb 2011, pp 239-246.