A Survey on Various Approaches of Image Steganography

Priyanka B. Kutade
Dept. of E and TC Engg.,
G.H. Raisoni College of Engg. and Management,
University of Pune, Pune,
India

Parul S. Arora Bhalotra
Assistant Professor, Dept. of E and TC Engg,
G.H. Raisoni College of Engg. and Management,
University of Pune, Pune,
India

ABSTRACT

Steganography is an art of concealing the fact with the purpose of communication, by hiding one information in other information. In steganography, many different carrier file formats are used now days, but the digital images are most popular for hiding information because of their frequency on Internet. There is a large variety of techniques of steganography are available for hiding secret information into images. Each of them has its strong & weak points. Choice of which steganography technique is used it depends on the different requirements of the application. For example, some applications may have need of a bigger secret message to be concealed and some need absolute invisibility of the secret message. This paper gives an overview of different techniques used for image steganography. Among these following techniques DCT & DWT techniques are widely used because of their efficiency.

General Terms

DWT, DCT, LSB

Keywords

Image Steganography, DWT, LSB, DCT

1. INTRODUCTION

The word steganography [2] is original from the Greek language words '*stegos grafia'* the meaning is 'covered or concealed writing'. In image steganography the information is secreted entirely in images.

Steganography is the ability and skill of hidden way of communication. This is fulfilled during hiding secret information in any other information, as a result concealing the presence of the communicated information data.

The Image steganography technique is broadly used procedure to protected information used for hidden communication. Such as featured tagging, military agencies copyright protection, and for various more applications correlated to secure communications.

This paper intends to recommend a state of the art general idea of the different algorithms utilized designed for image steganography which will helps to demonstrate the security prospective of steganography for business and personal use.

In next section types of image steganography will be explained

2. VARIOUS TYPES OF IMAGE STEGANOGRAPHY

2.1 (LSB) Least Significant Bit Insertion Image

Least significant bit insertion (LSB) is a simple common method to hide data into a cover image. As discussed in [2] that, in an image the 8th bit of a particular byte or all of the bytes is replaced with a bit of secret image or message. In a color image there are Red, Green and Blue color components. Each component represents a byte. So, 3 LSBs can be used to store in a pixel.

Ever since there are 256 probable intensities of every primary color, make happen small variations in the intensity of the colors as a result of altering the LSB of a pixel. These changes cannot be identified by the human being eye. Hence the message is effectively concealed. Through a suitable image, one can still conceal the secret message in the least bit also in adjacent bit of LSB besides still not see the difference.

This method succeeding bytes that are from first to last bytes of the image information are taken to alter the information data. This steganography approach is very easy for attacker. So for adding the security, sender and intended receiver has to share a secret key. That secret key shares the information which states only some definite pixels to be altered.

According to [18], they have developed the tool for hide the image in cover image and again retrieving the original image. In this, they were designed two methods for hiding the image into cover image. In first method i.e. in Simple mode method the firstly the pixel is selected in cover image. Then the image is hided in LSB bits of that randomly selected pixel of cover image. For retrieving the original image, the location of chosen pixel, dimensions of original image and no. of bits used to store image these parameters were used. And all these information were stored in secret key which is in decrypted form.

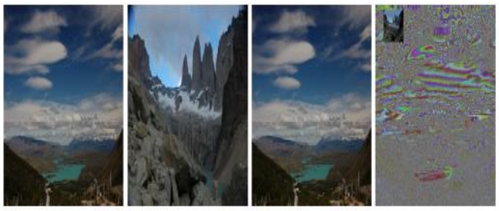


Fig.1.1 a) Cover image b) Secret image c) Stego image d) Lower bits of Stegified Image

In second method i.e. in Shuffle mode method take cover image of size A X B is taken and the image to be hide of size a X b size taken. Then select A no. of rows out of A and select b no. of columns out of B columns in cover image are selected. Then hide image in that selected rows and columns of cover image. For retrieving original image we want that no. of rows and columns in cover image.

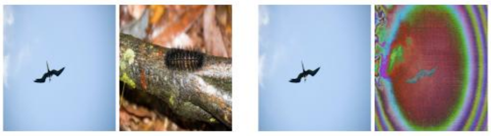


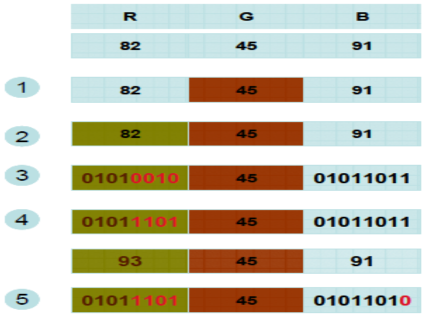
Fig. 1.2 a) Cover image b) Secret image c) Stego image d) Lower bits of Stegified Image

In [16] they have given idea about a concealed algorithm for hiding encoded messages in smooth areas and edges of images within the random and nonadjacent pixel locations. In that first task is to encrypt the message to be embedded then by using edge detection filter detect edges of the cover image. Then the encrypted message is embedded in LSB of the random edge area as well as at the LSBs of RGB of randomly selected pixel of the cover image. It guarantees that the attackers or hackers will not have any doubt with the intention of message bits are concealed in the image. Or any Standard steganographic detection methods cannot guess the length of the hidden message properly.

2.2 RGB Intensity based Image Steganography

In this type [6] presents algorithm which gives the idea of storing flexible number of secret information bits in every color channel (R, G or B) of pixel depending upon the definite color values of that pixel that is lower color component stores upper number of bits. This algorithm proposes very high capacity for cover image distinguished to other remaining algorithms. The approach in this algorithm is that, for 'insubstantial' colors, expressively additional bits can be altered every byte channel of an RGB color image. The basic concept of this algorithm is that, as compared to higher value, the lower color-value of a channel has a smaller amount of influence change on the overall color of the pixel. As a result, additional bits can be altered in a low value channel than high value channel.

Figure given below will help us to understand of loading secret information bits in a color channel described in [6]. Step one is randomly color channel G is selected as indicator. In next step for storing the secret information bits the color channel R is selected. Then depending on the present color channel value as well as scheme of partition, Number of secret information bits to store is determined. After that loads the secret information bits. And last then changes the other channel (B) LSB, which is used while extracting the secret information data.



	R	G	B
	82	45	91
1	82	45	91
2	82	45	91
3	01010010	45	01011011
4	01011101	45	01011011
	93	45	91
5	01011101	45	01011010

Fig. 2.1 Example

In [14] technique, the cover image is divided into 8 no. of blocks. Then secret message information is also divided into 8 no. of blocks. Next, one block of the message to be hidden is embedded into the one block of color image by a sub user defined key. For each block indicator is selected out of 3 color components i.e. R, G or B. and other two used for storing 4 bits of LSB data or secret message each. And important point is that after embedding 4 bits LSB of secret message the value of each color component should be less than or equal to 7. The same procedure is repeated for all 8 blocks. For the purpose of more security the RSA algorithm is used at sender and receiver for encryption and decryption respectively. So, [14] proposes very unique method of storing bits into RGB based steganography.

[10] proposes which is a key feature based algorithm. In which it uses color components to decide which channel will be used for hiding the information and at what extent. Randomly it selects indicator by the criteria which channel has capacity of 4 bit storage among R, G, B. Algorithm classify the channels on the basis of capacity of zero or two or four bit insertion,

After that the indicator is selected. At the LSBs of the other two channels are used to hide the message bits. The presence of LSB of the indicator gives an idea about the data is hidden into the other two channels. So, the major aspects of the [10] developed method are its good quality of stego image, the exact extraction of the hidden image and robustness.

2.3 Spread Spectrum Image Steganography

Spread spectrum communication defines the procedure of distribution the bandwidth of a narrowband frequency over a wideband of frequencies. We can achieve this by spreading the narrowband waveform over a wideband waveform, for example white noise. Once spreading done, the energy or strength of the narrowband (or weak) signal in every frequency band is small and as a result hard to detect or perceive. This method uses Gaussian noise to store the message and combines it with original image. So, at low noise, image changes are not detectable to human and if high noise then it appears as flecks or speckles.

The [17] system presents a spread spectrum steganography algorithm in which first step, construct encrypted message by the use of ECC. In step 2, create the encrypted message the equal size as the image. In step 3, interleave the encrypted secret message. In step 4, a pseudorandom noise sequence is produced. In step 5, AES algorithm is used to encrypt the message, for generating the noise modulates the sequence. In last step, noise is added to the original image.

For extracting the hidden message a filter is used which removes noise from stegoimage. And we will get the approximated original image. For extraction process the whole procedure given above is reversed.

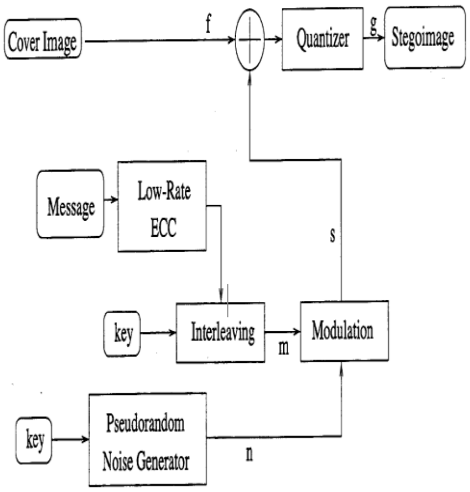


Fig. 3.1 Embedding process

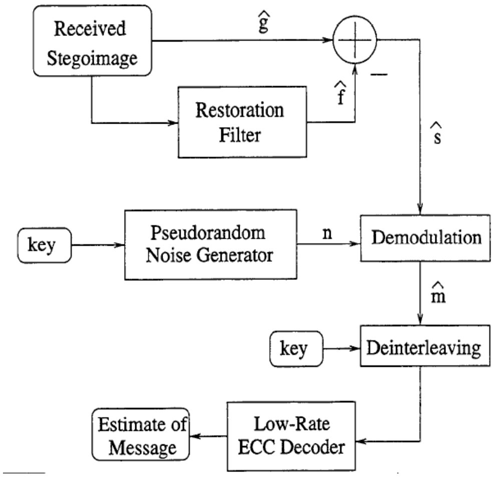


Fig.3.2 Extraction process

2.4 DCT based Image Steganography

This method [13] gives higher capacity as compared with earlier methods. If we consider stego image superiority, image quality is greater than the other methods.

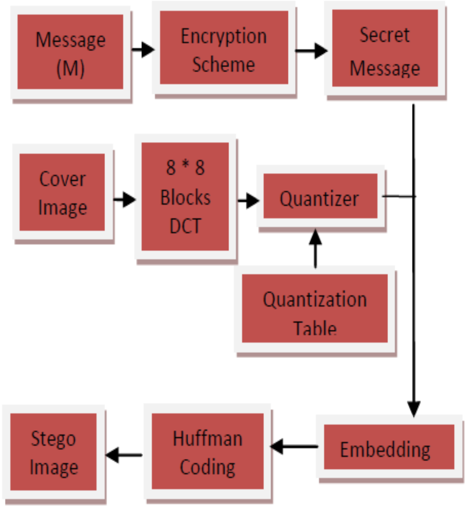


Fig. 4.1 The block diagram of the embedding procedure

Input is a cover-image, a secret key and message and Output is: A stego-image.

The embedding procedure starts with taking a cover-image of size N*N pixels and then divide that cover image into the non-overlapping blocks. Then DCT is applied to each non-overlapping block so the DCT coefficient matrix is obtained. Then modified quantization table p is taken to quantize the coefficient matrix. Then the message is encrypted by applying an encryption procedure with the secret key. Then the secret bits are loaded into selected DCT coefficient. Then Huffman coding is applied. So, we finally get JPEG stego image.

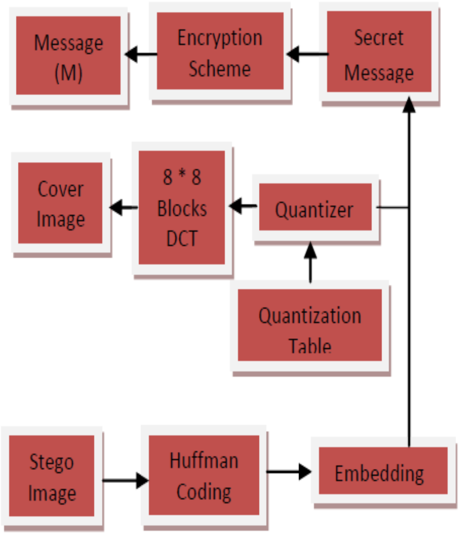


Fig 4.2 The block diagram of the extracting procedure

Input**:** M×N Stego-image.

Output: The Retrieved Secret image.

The extracting procedure starts with first dividing the stego image to non overlapping blocks of 8×8 size. Then Discrete Cosine Transform is applied on each block of stego image. As of 1st 8 × 8 DCT block size of the encrypted bit stream is retrieved by collecting LSBs of all of DCT coefficients in the 1st 8 × 8 block. Then The LSBs of all of the DCT coefficients within 8×8 block are collected (excluding the first) and added to a 1-D array. Awaiting the dimension of the 1-D array becomes equivalent to size which is extracted in step 2nd step and step 3 is repeated. Huffman table is constructed by doing the extraction of LSBs of all of DCT coefficients inside 8×8 blocks (excluding the first block) and block which is mentioned in step 3. The 1-D array obtained in step 3 is decrypted using Huffman table which is obtained in step 5.

In this method, the capacity of message which is being embedded is increased, but the image degrades as it changes all DCT coefficients of every block.

According to [21], first step is DCT is applied to cover image. Then DCT coefficients detect the randomized location of pixel. Then in next step, then secret message is hided into the selected LSB of pixel. This method gives better results than blind steganalysis methods.

In [15] paper a combined approach of cryptography and steganography used. In which LSB and DCT based steganography is used to hide the data. This method is for steganography for spatial and frequency domains with Asymmetric key cryptography. The idea is to make use of a considerable bit of the DCT coefficients of a cover image to conceal encoded secret message bits. Then, embedded bits of the information coefficients are spread in the stego image with applying the inverse of the DCT method.

2.5 DWT Image Steganography

The DWT (Discrete Wavelet Transform) divides the image in frequency components. High frequency components are nothing but detailed coefficients which hold the additional information about image. Low frequency components are nothing but approximate coefficients that hold almost the original image. These detailed coefficients can be used for embedding secret image. Here we take an image as cover object and other small image as the secret message. In the process of embedding, first we do is that conversion of cover image in the wavelet domain. Then the manipulation of high frequency component is done for keeping the secret image data. This secret image data is further retrieved in the extraction procedure to serve the steganography. Embedding Procedure In this step, is carried out. The pseudo-random number is additional component used rather than usual steganographic objects. Pseudo-random sequences demonstrate the statistical randomness while being generated by completely deterministic causal process generator. This generator is nothing but a program that on input a seed, generating numbers random sequence.

According to[19], the input is a m × n carrier image and secret image or message. Output is m × n stego-image. The process starts with reading the cover image and then calculating its size. Then secret image is read and then secret image is prepared as a message vector. Then cover image is decomposed using the Haar wavelet. A pseudo random number is then generated and the detailed i.e. horizontal & vertical coefficients are modified by adding pseudo random number when message bit is 0. Finally the inverse DWT is applied and the stego image is thus prepared to display.

Extraction Procedure: Additionally correlation theory is being used. The correlation between two equal size matrices is found by: the Input taken m × n size of cover image and m × n size of stego-image. Output is a secret image or message. The correlation is referred as the degree to which the two or more quantities are linearly associated. Extraction process starts with reading cover image and stego image. Then both are decomposed using Haar WT. Then a message vector is generated of all ones then the correlation between the original along with modified coefficients is found and if the mean correlation value is less than the correlation value, message vector bit is turned to zero. Then the message vector is prepared for displaying secret image.

In this paper [12], The DWT is applied on color images and to improve the security, Arnold transformation is used. First the cover and secrete images are read and cover image is split into its components. Then the DWT is applied on all the three components. Then secrete images are changed using Arnold transform and every color component of the changed secrete images is separated. Then secrete images components are embedded into HL, HH, and LH sub band. The inverse DWT is applied and the stego image is thus obtained. The reverse of embedding is recovery process. Reading of cover and stego image, then splitting cover image and stego image into components, then applying the inverse of Arnold transform furthermore obtain the secrete images.

This paper [20] has proposed algorithm for embedding and extraction of secret image embedded behind cover gray scale image. Embedding process starts with inputting the cover image. Then the 2-level DWT is applied on the cover image and the band is selected to be modified as ‘m’ i.e. LL2. Then the secret image is read. Then the size of the secret is found say ‘n’. Then, for each n*n coefficient of m band, ‘p LSB bits’ are replaced by the ‘p MSB bits’ of secret image. Inverse DWT is applied twice and stego image is obtained. Thus key information is formed as K = n + m + p. Extracting procedure starts with reading the stego image. Then a2-level DWT transform is applied on the stego image. The loading the key information K and assigning corresponding values in m, n and p are done. Then extract the ‘p LSB’ of the band coefficient to ‘p MSB’ of new matrix vector starting from top left corner of m band. Repetition of this step for n times in both dimensions is done and names this new matrix vector as secret image. The secret image is displayed.

DWT and DCT are also used in Shot Boundary Detection using Radon Projection Method to remove the illumination effect and in CBIR technique [23], [24], [25].

3. CONCLUSION

Even though only few of the main image steganography techniques were discussed in this paper, researcher can observe that there exists a large choice of approaches or methods to hiding secret information in images. All these techniques try to satisfy three most important factors of steganographic design i.e. capacity, undetectability, and robustness. Spatial domain LSB techniques have a high payload capacity, but they frequently fail to prevent the statistical attacks. So they are detected easily. Especially when the hidden message is small, the promising techniques like DWT, DCT and adaptive steganography are not prone to attacks. They change the coefficients in transform domain, resulting in the minimum image distortion. Experiments on DCT coefficients introduced promising results and diverted researchers’ attention towards JPEG images. Message embedding in the DWT domain reveals the constructive results and it outperforms the DCT embedding. For all these benefits, DCT and DWT are superior choices.

4. ACKNOWLEDGEMENT

I would like to say thanks to my guide “Prof. Parul S. Arora Bhalotra” who gave her knowledge and time in order to complete this paper. This paper would never complete without her and the support of faculty members.

5. REFERENCES

[1] Dr. Sudeep Thepade, Smita S. Chavan, “ Appraise Of Multifarious Image Steganography Techniques”, (IJERA) International Journal of Engineering Research and Applications Vol. 3, Issue 2, March -April 2013, ISSN: 2248-9622

[2] T Morkel, MS Olivier and JHP Eloff, "An Overview of Image Steganography," (ISSA2005), in Proceedings of the Fifth Annual Information Security South Africa Conference Sandton, South Africa, (Published electronically) June/July 2005

[3] M, Raju, B, Priya, Suchitra, “Image Steganography Based On DCT Algorithm for Data Hiding”, (IJARCET) International Journal of Advanced Research in Computer Engineering & Technology Volume 2, Issue 11, November 2013 3003

[4] Rosziati Ibrahim and Teoh Suk Kuan, “Steganography Algorithm to Hide Secret Message inside an Image”, Computer Technology and Application 2 (2011) 102-108, Published: February 25, 2011.

[5] Rupinder Kaur, Mandeep Kaur, Rahul Malhotra, " A New Efficient Approach towards Steganography", (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 2 (2) , 2011, 673-676

[6] Adnan Abdul-Aziz and Gutub Mohammad Tanvir Parvez, "RGB Intensity Based Variable-Bits Image Steganography", IEEE Asia-Pacific Services Computing Conference 2008

[7] LinjieGuo, Student Member, IEEE, Jiangqun Ni, Member, IEEE, and Yun Qing Shi, Fellow, IEEE, "Uniform Embedding for Efficient JPEG Steganography", IEEE Transactions On Information Forensics And Security, Vol. 9, No. 5, May 2014

[8] A.A.Al-Saffar , "Proposed Steganography Method Based on DCT Coefficients", IBN AL- HAITHAM J. FOR PURE & APPL. SCI. VOL.24 (3) 2011

[9] Jiri Fridrich, "A New Steganographic Method for Palette-Based Images", Center for Intelligent Systems, SUNY Binghamton, Binghamton, NY 13902-6000

[10] Surbhi Gupta, Parvinder S. Sandhu, "Exploiting the RGB Intensity Values to Implement a Novel Dynamic Steganography Scheme", International Journal of Research in Engineering and Technology (IJRET) Vol. 2, No. 4, 2013 ISSN 2277 – 4378

[11] Hung-Ju Lin, Po-Yueh Chen, "A DWT Based Approach for Image Steganography", International Journal of Applied Science and Engineering 2006.

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

[13] Er. Rohini Sharma, Er. Mahender Singh, Er. Dinesh Garg, " A New Purposed Issue for Secure Image Steganography Technique Based On 2-D Block DCT and DCT", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 2, Issue 7, July 2012 ISSN: 2277 128X

[14] Sarojkumar Lenka, Gandharba Swain, "A Novel Approach To RGB Channel Based Image Steganography Technique", International Arab Journal of e-Technology, Vol.2 , No.4, June 2012.

[15] Deepak Singla1, Rupali Syal2, "Data Security Using LSB & DCT Steganography In Images", International Journal Of Computational Engineering Research/ ISSN: 2250–3005

[16] Mamta Juneja and Parvinder S. Sandhu, "An Improved LSB Based Steganography Technique for RGB Color Images", International Journal of Computer and Communication Engineering, Vol. 2, No. 4, July 2013

[17] B.Padmasri, M.Amutha surabi, "Spread Spectrum Image Steganography with Advanced Encryption Key Implementation", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 3, March 2013 ISSN: 2277 128X

[18] Ankit Gupta, Rahul Garg, "Detecting LSB Steganography in Images"

[19] Barnali Gupta Banik, Prof. Samir K. Bandyopadhyay, "A DWT Method for Image Steganography", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 6, June 2013, ISSN: 2277 128X

[20] 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

[21] Ajit Danti, Preethi Acharya, "Randomized Embedding Scheme Based on DCT Coefficients for Image Steganography", IJCA Special Issue on "Recent Trends in Image Processing and Pattern Recognition" RTIPPR, 2010.

[22] S. S. Nassar, N.M.Ayad, M.H. Kelash, O. S., M. A. M. El-Bendary, "Image Contents Verification Algorithm using Transform Domain Techniques" International Journal of Computer Applications (0975 – 8887) Volume 97– No.9, July 2014

[23] Nilam N Ghuge, Parul S Arora Bhalotra, B. D. Shinde, "CBIR using Textural Feature", International Journal of Computer Applications, Volume 56– No.11, October 2012

[24] Nilam N Ghuge, Parul S Arora Bhalotra, B. D. Shinde,"Shot Boundary Detection for a Video under the Influence of Illumination: A Adaptive Thresholding Approach, International Journal of Computer Applications, Volume 56– No.11, October 2012

[25] Parul S. Arora Bhalotra, Bhushan D. Patil, "Shot Boundary Detection using Radon Projection Method" ACEEE Int. J. on Signal and Image Processing , Vol. 4, No. 3, Sept 2013