ISSN:0975-9646

Navjot Kaur et al, / (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 5 (6) , 2014, 8135-8137

A review on Digital Image Steganography

Er. Navjot Kaur [#1], Er. Ashima Bansal [*2]

[#1]*HOD, GVIET,BANUR*

[*2]*GVIET, BANUR*

***Abstract*— Steganography is an important area of research in recent years involving a number of applications. It is the science of embedding information into the cover image viz., text, video, and image (payload) without causing statistically significant modification to the cover image. This paper deals with hiding text in an image file using using various Steganography techniques. Discrete Cosine Transform (DCT) based Steganography and Discrete Wavelet Transform (DWT) steganography algo. We are comparing results of these techniques to find out the better technique for stegnography.**

***Keywords*— DCT, DWT, Steganography**

I. INTRODUCTION

The rapid growth of internet usage over high bandwidth and low cost computer hardware has propelled the explosive growth of steganography [1].In the present year, secure and hidden communication is the foremost requirement of the people. Therefore steganography is gaining attraction by people due to the security issues over internet. Steganography means covert writing. Steganography has evolved into a digital strategy of hiding a file in some form of multimedia, such as an image, an audio file or even a video file. The objective of steganography is hiding the payload (embedded information) into the cover image such that the existence of payload in the cover image is imperceptible to the human beings. There are different techniques to implement Steganography namely least significant bit (LSB), discrete cosine transform (DCT) & discrete wavelet transform(DWT) technique. There are two types of domains in which There are two types of domains in which steganography is implemented i.e. spatial domain & frequency domain. In spatial domain, processing is applied directly on the pixel values of the image whereas in frequency domain, pixel values are transformed and then processing is applied on the transformed coefficients.

II. KINDS OF STEGNOGRAPHY

Almost all digital file formats can be used for steganography, but the formats that are more suitable are those with a high degree of redundancy. Redundancy can be defined as the bits of an object that provide accuracy far greater than necessary for the object's use and display. The redundant bits of an object are those bits that can be altered without the alteration being detected easily. Image and audio files especially comply with this requirement, while research has also uncovered other file formats that can be used for information hiding. Figure shows the four main categories of file formats that can be used for steganography.

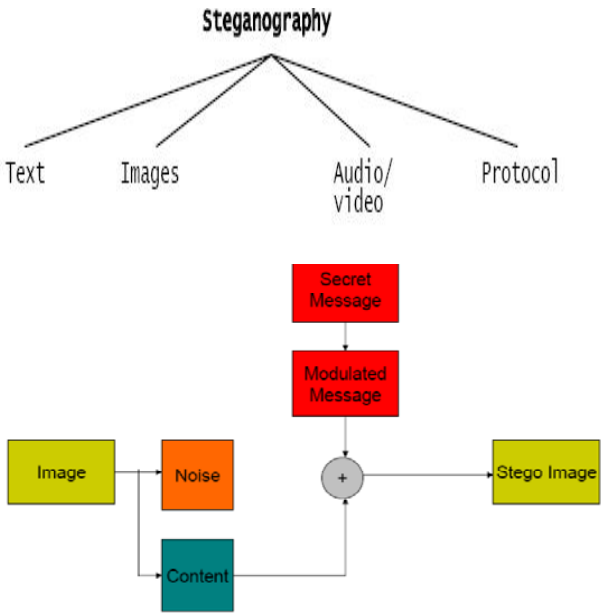

Fig1. Digital Image Stegnography

III. APPLICATION OF STEGNOGRAPHY

Steganography can be used for wide range of applications such as, in defence organisations for safe circulation of secret data, in military and intelligence agencies, in smart identity cards where personal details are embedded in the photograph itself for copyright control of materials. In medical imaging, patient's details are embedded within image providing protection of information and reducing transmission time and cost1, in online voting system so as to make the online lection secure and robust against a variety of fraudulent behaviours2, for data hiding in countries where cryptography is prohibited, in improving mobile banking security3, in tamper proofing so as to prevent or detect unauthorised modifications and other numerous applications.

IV. FEATURES OF STEGNOGRAPHY

Steganographic techniques have various features which characterises their strengths and weaknesses. Features include:

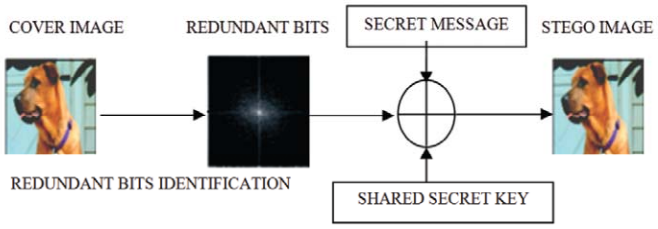

Fig. Generic steganography process

Embedding capacity*:* It refers to the amount of data that can
be inserted into the cover-media without deteriorating its integrity.

Perceptual transparency: It is necessary that to avoid suspicion the embedding should occur without significant degradation or loss of perceptual quality of the cover media.

Robustness: It refers to the ability of embedded data to remain intact if the stego-image undergoes various transformations such as scaling, rotation, cropping or compression.

Tamper resistance: It refers to the difficulty to alter or forge a message once it is embedded in a cover-media, such as replacing a copyright mark with the one claiming legal ownership.

Computational complexity*:* Computational complexity of steganography technique employed for encoding and decoding is another consideration and should be given importance.

V. IMAGE STEGNOGRAPHY METHODS

In this section, some of recent studies and techniques of image steganography will be covered. Methods are briefly described in each part.

High capacity image steganography based on genetic algorithm and wavelet transform: Elham Ghasemi *et al.* employ a GA based mapping function to embed data in discrete wavelet transform coefficients in 4*4 blocks on the cover image. The optimal pixel adjustment process (OPAP) is applied after embedding the message. The main idea of applying OPAP is to minimize the error between the cover and the stego-image.

Data embedding technique for gray scale image using genetic algorithm (DEGGA): J. K. Mandal *et al.* present another GA-based algorithm termed DEGGA. Focus in this method is on large amount of hidden data and the results are compared with another method by Ran- Zan *et al*. In Mandal method, large volume of message/ image is embedded in spatial domain using 3 x 3 masks from the source image. Four bits of the secret message / image is embedded per byte of the source image onto the rightmost 4 bit of each pixel. Mutation is applied on the embedded image. Also, a method of bit handling is applied to keep the fidelity high.

Secure steganography method based on genetic algorithm: Shen Wang *et al.* present a new steganography method based on genetic algorithm. There is no approach for embedding data in host image in proposed method. But, securing the stego-image is done after data embedding. After embedding the secret message in LSB (least significant bit) of the cover image, the pixel values of the stego-image are modified by the genetic algorithm to keep their statistic characters.

Improving the performance of LSB substitution against RS by minimizing detection probability: One of the most notable steganalysis algorithms is the RS attack which detects the stego-message by the statistic analysis of pixel values. Another steganographic algorithm is presented by Vijay Kumar Sharma *et al*. based on genetic algorithm. In this method, after embedding the secret message in LSB (least significant bit) of the cover image, the pixel values of the stego image are modified by the genetic algorithm to keep their statistic characters.

Improved adaptive LSB steganography based on chaos and genetic algorithm: Lifang Yu *et al.* present a steganography method in JPEG images with high performance. Proposed method is consisting of 2 parts. First, improved adaptive LSB steganography is presented, which can achieve high capacity while preserving the first-order statistics. Second, in order to minimize visual degradation of the stego image, shuffling bits order of the message based on chaos is done, whose parameters are selected by the genetic algorithm.

VI. RELATED STUDY

J.R. Krenn explained steganography and its implementation techniques [1]. Deshpande Neeta, et. al. proposed the Least Significant Bit embedding technique suggests that data can be hidden in the least significant bits of the cover image and the human eye would be unable to notice the hidden image in the cover file. This paper explains the LSB embedding technique and presents the evaluation results for 2, 4, 6 Least significant bits for a .png file and a .bmp file [2]. K.B. Raja, et. al. proposed a challenging task of transferring the embedded information to the destination without being detected. In this paper, the image based steganography that combines Least Significant Bit (LSB), Discrete Cosine Transform (DCT), and
compression techniques on raw images to enhance the security of the payload [3]. Vijay Kumar Sharma, et. al. has worked upon a new steganography algorithm for 8bit (gray scale) or 24bit (color image) based on Logical operation to ensure the security against the steganalysis attack[4]. Po-Yueh Chen, et. al. proposed a new steganography technique which embeds the secret messages in frequency domain. According to different users' demands on the embedding capacity and image quality, the proposed algorithm is divided into two modes and 5 cases [5]. Chen Ming, et. al. focused on the steganography tools algorithms. Based on the analyses of the algorithms, various tools are divided into five categories: (1). Spatial domain based steganography tools; (2). Transform domain based steganography tools; (3). Document based steganography tools; (4) File structure based Steganography tools; (5) other categories, e.g. video compress encoding and spread spectrum technique based [6]. Aneesh Jain, et. al. proposed a scheme which hides data in bitmap images, in a way that there is almost no perceptible difference between the original image and this new image and which is also resistant to JPEG compression[7]. Beenish Mehboob,et. al. discusses the art and science of Steganography in general and proposes a novel technique to hide data in a colorful image using least significant bit[8]. Hassan Mathkour, et. al. seta a criteria to analyze and evaluate the strengths and weaknesses of the presented techniques and a more robust steganography technique has been developed that takes advantages of the strengths and avoids the limitations[9]. Nageswara Rao Thota, et. al. attempted to implement basic JPEG compression using only basic MATLAB

functions[10]. Mamta Juneja, et. al. discusses the design of a Robust image steganography technique based on LSB (Least Significant Bit) insertion and RSA encryption technique[11]. K.B. Shiva Kumar, et. al. discusses the important issue of modern communication is establishing secret communication while using public channel and is achieved by steganography. In this paper, Coherent Steganography Technique using Segmentation and Discrete Cosine Transform (CSSDCT) is proposed. The cover image is divided into 8*8 blocks and DCT is applied on each block. The number of payload MSB bits is embedded into DCT coefficients of the cover image coherently based on the values of DCT coefficients. It is observed that the proposed algorithm has better PSNR, Security and capacity compared to the existing techniques [12]. Dr. Ekta Walia, et. al presents analysis of Least Significant Bit (LSB) based Steganography and Discrete Cosine Transform (DCT) based Steganography [13]. K Suresh Babu, et. al.proposed an image Steganography that can verify the reliability of the information being transmitted to the receiver. The method can verify whether the
attacker has tried to edit, delete or forge the secret information in the stego-image [14]. Atalla I. Hashad, et. al. describe the LSB insertion technique, the Discrete Cosine Transform (DCT) insertion technique is described and finally we will propose a new technique that uses the idea of inserting a bit in the spatial domain combined with the DCT insertion technique[15]. ArvindKumar, et. al. discusses how digital images can be used as a carrier to hide Messages and also analyses the performance of some of the steganography tools[16]. Vijay Kumar, et. al. intends to observe the effect of embedding the secret message in different bands such as CH, CV and CD on the performance of stego image in terms of Peak Signal to Noise Ratio (PSNR). Experimentation has been done using six different attacks. Experimental results reveal that the error block replacement with diagonal detail coefficients (CD) gives better PSNR than doing so with other coefficients [17]. Ali Al-Ataby, et. al. proposed a modified high-capacity image steganography technique that depends on wavelet transform with acceptable levels of imperceptibility and distortion in the cover image and high level of overall security[18]. T. Narasimmalou, et. al. Proposed an optimal discrete wavelet transform (DWT) based steganography. Experiments show that the peak signal noise ratio (PSNR) generated by the proposed method is better[19]. NedaRaftari, et. al. proposed a novel image steganography technique that combines the Integer Wavelet Transform (IWT) and Discrete Cosine Transform (DCT) is proposed which embeds secret image in frequency domain of cover image with high matching quality[20].

VII. CONCLUSION

Steganography in image files uses 2 general techniques: LSB (Least Significant Bits) and DWT (Discrete Wave Transform). Proposed methods of steganography use one of these techniques. Robustness is the main consideration in steganography. Furthermore, capacity is considered as an important factor, too. Stego methods concentrate on these factors and commonly there make a sensible proportion between them.

REFERENCES

1. J.R. Krenn, “Steganography and Steganalysis”, January 2004. Deshpande Neeta, Kamalapur Snehal, Daisy Jacobs, “Implementation of LSB Steganography and its Evaluation for Various Bits”.
2. K.B. Raja, C.R. Chowdary, Venugopal K. R, L.M. Patnaik, “A Secure Image Steganography using LSB, DCT and Compression Techniques on Raw Images”, IEEE-0-7803-9588-3/05/$20.00.
3. Vijay Kumar Sharma, Vishalshrivastava, “A Steganography Algorithm for Hiding Images by improved LSB substitution by minize detection.” Journal of Theoretical and Applied Information Technology, Vol. 36 No.1, ISSN: 1992-8645, 15th February 2012.
4. Po-Yueh Chen and Hung-Ju Lin, “A DWT Based Approach for Image Steganography”, International Journal of Applied Science and Engineering 4, 3: 275-290.
5. Chen Ming, Zhang Ru, NiuXinxin, Yang Yixian, “Analysis of Current Steganography Tools: Classifications & Features”,International Conference on Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP'06), IEEE- 0- 7695-2745-0/06 $20.00
6. Aneesh Jain, Indranil Sen. Gupta, “A JPEG Compression Resistant Steganography Scheme for Raster Graphics Images”, IEEE-1-4244-1272- 2/07/$25.00.
7. Beenish Mehboob and Rashid Aziz Faruqui, “A Steganography Implementation”, IEEE -4244-2427- 6/08/$20.00 ©2008.
8. Hassan Mathkour, Batool Al-Sadoon, Ameur Touir, “A New Image Steganography Technique”, IEEE- 978-1-4244-2108-4/08/$25.00 © 2008.
9. Nageswara Rao Thota, Srinivasa Kumar Devireddy, “Image Compression Using Discrete Cosine Transform”, Georgian Electronic Scientific Journal: Computer Science and Telecommunications, No.3 (17), 2008.
10. MamtaJuneja, Parvinder Singh Sandhu, “Designing of Robust Image Steganography Technique Based on LSB Insertion and Encryption”, International Conference on Advances in Recent Technologies in Communication and Computing, 2009.
11. Dr. EktaWalia, Payal Jain, Navdeep, “An Analysis of LSB & DCT based Steganography”, Global Journal of Computer science & technology, Vol. 10 Issue 1 (Ver 1.0), April 2010.
12. K.B. Shiva Kumar, K.B. Raja, R.K. Chhotaray,Sabyasachi Pattnaik, “Coherent Steganography using Segmentation and DCT”, IEEE-978-1-4244- 5967-4/10/$26.00 ©2010.
13. K Suresh Babu, K B Raja, Kiran Kumar K, Manjula Devi T H, Venugopal K R, L M Patnaik, “Authentication of Secret Information in Image Steganography” .
14. Arvind Kumar, Km. Pooja, “Steganography- A Data Hiding Technique”, International Journal of Computer Applications (0975 – 8887), Volume 9, No.7, November 2010.
15 .Atalla I. Hashad, Ahmed S. Madani, “A Robust Steganography Technique Using Discrete Cosine Transform Insertion”.
16. Vijay Kumar, Dinesh Kumar, “Performance Evaluation of DWT Based Image Steganography”, IEEE- 978-1-4244-4791-6/10/$25.00_c 2010.
17. Ali Al-Ataby and Fawzi Al-Naima, “A Modified High Capacity Image Steganography Technique Based on Wavelet Transform” The International Arab Journal of Information Technology, Vol. 7, No. 4, October 2010.
18. T. Narasimmalou, Allen Joseph .R, “Optimized Discrete Wavelet Transform based Steganography”, IEEE International Conference on Advanced Communication Control and Computing Technologies (ICACCCT), 2012.
19. NedaRaftari and Amir Masoud Eftekhari Moghadam, “Digital Image Steganography Based on Assignment Algorithm and Combination of DCTIWT”, Fourth International Conference on Computational Intelligence, Communication Systems and Networks, 2012.
20. Ankita Sancheti, “Pixel Value Differencing Image Steganography Using Secret Key” International Journal of Innovative Technology and Exploring Engineering (IJITEE), ISSN: 2278-3075, Volume-2, Issue-1 and December 2012.