International Journal of Latest Engineering and Management Research (IJLEMR)
ISSN: 2455-4847
www.ijlemr.com ‖ Volume 02 - Issue 02 ‖ February 2017 ‖ PP. 30-35

IMAGE STEGANOGRAPHY

Prof. Moses Praveen
Adithya College
Dept of Computer Science

Abstract: This paper presents a steganography technique for images imparting better information security by an embedding algorithm for hiding secret images in nonadjacent and random pixel locations in edges and smooth areas of images. This work is an attempt to develop Blind Hide, Modified LSB and Channel indexing technique for image hiding. Data Encryption Standard (DES) is used to provide two tier security. It ensures that the eavesdroppers will not have any suspicion that secret image is hidden in the cover image that is to provide high imperceptibility and standard steganography detection methods can not estimate the size of the secret image correctly. A model for Blind Hide, Modified LSB and Channel indexing technique has been developed for various images. To find the suitability of these two approaches several experiments has been conducted and detailed analysis has been made on the obtained results. The results obtained for Channel indexing technique achieved improved imperceptibility than the various existing techniques along with better resistance to various steganalysis attacks and is quite promising for the high PSNR values than Modified LSB and Blind Hide method.

Keywords: Data hiding, Image steganography, LSB Insertion, Edge detection.

I. Introduction

As a society, humans have continually sought new and efficient ways to communicate. The earliest methods included cave drawings, smoke signals, and drums. Advancements of civilization introduced written language, telegraph, radio/television, and most recently electronic mail. As more and more communication is conducted electronically, new needs, issues, and opportunities are born. At times when we communicate, we prefer that only the intended recipient have the ability to decipher the contents of the communication. We want to keep the message secret. A common solution to this problem is the use of encryption. While encryption masks the meaning of a communication, instances exist where we would prefer that the entire communication process not be evident to any observer that is, even the fact that communication is taking place is a secret. In this case, we want to keep the communication hidden.

Steganography can be used to hide or cover the existence of communication. A major drawback to encryption is that the existence of data is not hidden. Data that has been encrypted, although unreadable, still exists as data. If given enough time, someone could eventually decrypt the data. A solution to this problem is steganography. Steganography word is originated from Greek words Steganos (Covered), and Graptos (Writing) which literally means "cover writing" [1]. Generally steganography is known as "invisible" communication. Steganography means to conceal messages existence in another medium (audio, video, image, communication). Today's steganography systems use multimedia objects like image, audio, video etc as cover media because people often transmit digital images over email or share them through other internet communication application. It is different from protecting the actual content of information. In simple words it would be like that, hiding information into other information.

Steganography means is not to alter the structure of the secret information, but hides it inside a cover-object (carrier object). After hiding process cover object and stego-object are similar. So, steganography (hiding information) and cryptography (protecting information) are totally different from one another. Due to invisibility or hidden factor it is difficult to recover information without known procedure in steganography. Detecting procedure of steganography known as Steganalysis.

For an image steganalysitical system, there are two factors, capacity and invisibility should be carefully considered. The capacity, how much bits can be embedded in a cover image, is easy to be understood. The invisibility against perceptual analysis means the embedding cannot introduce perceptual distortion to arise the analyzer's suspicion, and that against steganalysis means the message embedding cannot introduce the detectable alteration on statistics of a cover image. Usually, the first invisibility is defined as imperceptibility, and the second is defined as security. In most cases, how to deal with the trade-off between capacity and security is core issue to design a steganalysitical algorithm. In all embedding schemes, LSB steganography is most popular.

II. Related Work

This section focuses on various schemes that are reported in recent works on image steganography in spatial domain.

There are many versions of spatial steganography, all directly change some bits in the image pixel values in hiding data. Least Significant Bit (LSB) based steganography is one of the simplest techniques that hide a secret message in the LSBs of pixel values without introducing many perceptible distortions. Changes in the value of the LSB are imperceptible for human eyes.

Y. K. Jain *et.al.,* [2] have proposed an adaptive least significant bit spatial domain embedding method. This method divides the image pixels ranges (0-255) and generates a stego-key. The strength of proposed method is its integrity of secret hidden information in stego-image and high hidden capacity. The limitation is to hide extra bits of signature with hidden message for its integrity purpose. This method is targeted to achieve high hidden capacity plus security of hidden message.

To overcome the drawback of using extra bits of signature, **H.Yang *et.al.,* [3]** proposed an adaptive LSB substitution based data hiding method for image. To achieve better visual quality of stego-image it takes care of noise sensitive area for embedding. Proposed method differentiates and takes advantage of normal texture and edges area for embedding. This method analyzes the edges, brightness and texture masking of the cover image to calculate the number of k-bit LSB for secret data embedding. The overall result shows a good high hidden capacity, but dataset for experimental results are limited; there is not a single image which has many edges with noise region like 'Baboon.tif'.

S.Channalli *et.al.,* [4] have proposed LSB based image hiding method. Common pattern bits (stego-key) are used to hide data. The LSB's of the pixel are modified depending on the (stego-key) pattern bits and the secret message bits. This technique targets to achieve security of hidden message in stego-image using a common pattern key. This proposed method has low hidden capacity because single secret bit requires a block of (MxN) pixels.

C.H. Yang *et.al.,* [5] proposed a Pixel Value Difference (PVD) and simple least significant bits scheme are used to achieve adaptive least significant bits data embedding. In Pixel Value Differencing (PVD) where the size of the hidden data bits can be estimated by difference between the two consecutive pixels in cover image using simple relationship between two pixels. So in this way the technique provide both larger capacity and high visual quality according to experimental results. But this method is complex due to adaptive k generation for substitution of LSB.

To provide less complexity, **K.H.Jung *et.al.,* [6]** have proposed a method of Multi-Pixel Differencing (MPD) which used more than two pixels to estimate smoothness of each pixel for data embedding and it calculate sum of difference value of four pixels block. For small difference value it uses the LSB otherwise for high difference value it uses MPD method for data embedding. Strength is its simplicity of algorithm but experimental dataset is too limited.

To provide better simplicity, **H.Zhang *et.al.,* [7]** proposed another pixel value differencing method, it used the three pixels for data embedding near the target pixel. To retain better visual quality and high capacity it simply uses optimal pixel adjustment method on target pixels. Advantage of method is histogram of stego-image and cover-image is almost same, but dataset for experiments are too small.

W.J Chen *et.al.,* [8] have introduced a high capacity of hidden data utilizing the LSB and hybrid edge detection scheme. For edge computation two types of canny and fuzzy edges detection method applied and simple LSB substitution is used to embed the hidden data. This scheme is successful to embed data with higher Peak Signal to Noise Ratio (PSNR) with normal LSB based embedding. The proposed scheme is tested on limited images dataset.

To provide more security, **Madhu *et.al.,* [9]** proposed an image steganography method, based on LSB substitution and selection of random pixel of required image area. This method is target to improve the security where password is added by LSB of pixels. It generates the random numbers and selects the region of interest where secret message has to be hidden. The strength of method is its security of hidden message in stego-image, but has not considers any type of perceptual transparency.

Al-Husainy [10] proposed an image steganographic method of mapping pixels to alphabetic letters. It maps the 32 letters with the pixel values. Five (5) bits are required to represent these 32 letters and authors have generated a table where 4 cases design to represent these 32 letters. This algorithm keeps the matching pattern of cover-image which is then used for extracting data from the stego-image. Proposed method does not required any edge or smoothness computations but secret data should be in the form of text or letter for embedding.

To hide data other than text, **M.Motameni *et.al.,* [11]** have introduced a data hiding technique where it finds out the dark area of the image to hide the data using LSB. It converts it to binary image and labels each object using 8 pixel connectivity schemes for hiding data bits. This method required high computation to find

dark region its connectivity and has not tested on high texture type of image. Its hiding capacity totally depends on texture of image.

III. Techniques Used

- **Modified LSB approach**

The proposed new technique is for hiding secret image in cover images with high capacity and imperceptibility. This new modified approach works in following steps [12]:

1. Divide the image into smooth and edge areas using Canny Filter.
2. Embed data in least significant byte of all pixels selected in random manner using PRNG and Enhanced LSB method across edge areas and smooth areas at random locations.
3. Apply encryption for stego image using DES algorithm to provide more security for the secret image.

- **Canny Edge Detection technique**

The most important features of objects in images are edges. Canny edge detector is the optimal and most widely used algorithm for edge detection. Compared to other edge detection methods like Laplace filter, Sobel filter, Prewitt filter, etc, canny edge detector provides robust edge detection, localization and linking. It is a multi-stage algorithm and the stages involved are illustrated in Figure 3.1. Thus, instead of providing the whole algorithm as a single API, kernels are provided for each stage. This way, the user can have more flexibility and better buffer management. Canny filter is used as it provides better demarcation in edge areas and smooth areas which is need of this proposed steganography technique.

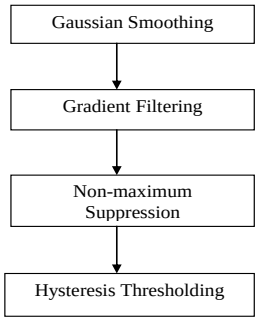

Figure 3.1: Flow Diagram of Canny edge detecting filter

- **Embedding data using Modified LSB Insertion method**

To embed the data in each pixel across edge areas, the Enhanced LSB insertion is used. LSB insertion is a common, simple approach in embedding information in a cover file. But in this Enhanced LSB technique, the data will be inserted only in last significant byte i.e. blue component of a pixel as that having lowest contribution to the color image according to Human Visual System analysis. To hide an image in a cover image, the B component of each pixel of RGB color image is modified.

To hide a message in a 24-bit image, the B component of each pixel of RGB color image is modified. For example, the letter A can be hidden in a pixel with original data as:

(00100111 11101001 11001000) .

The binary value for A is 01000001. Inserting the binary value for A in the given pixel would result in following bits replacement.

(00100110 11101001 <u>01000001</u>)

- **Channel Indexing Technique**

Figure 3.2 shows the Channel indexing technique [13] taking the secret image, the carrier image, and the password based generated key, as inputs and produces The channel indexing technique of Figure 3.2 which needs to have a pseudorandom number generator. The assumption for PRNG is to give two new random numbers in every iteration.The seeds of these PRNGs namely Seed1 (S1) and Seed2 (S2 are formed as a function of the Key (K). S1 is restricted to generate numbers in [0, 6] while S2 is restricted to the interval [1, 3]. S1 random number is used to determine the component of the RGB image which is going to be used in hiding the secret image. Table 3.1 shows how (S1) random number selects the RGB components. Seed2 (S2) random number determines the number of the component(s) least significant bits that is used to hide the secret data. On the same way Table 3 shows how (S2) random number determines the number of component bits. X-position and Y-position for the pixels with hidden data is distributed inside the image according to the size of the secret data.

IV. Embedding stage

Embedding is the process of hiding the secret image pixels generating the stego image. Hiding information may require a Stegokey which is additional secret information, such aspassword, required for embedding the information .Forexample, when a secret message is hidden within a cover image, the resulting product is stego image.

The main algorithm for the Embedded stage can be listed asfollow.

1. Input the secret image that to be hide in the coverimage .
2. Select the cover image from list of images
3. detect the edges in the cover image
4. Use Modified LSB method to hide secret image across randomly selected edge and smooth area of cover image
5. Use Channel indexing technique to hide secret image across edge area by considering the two seed values
6. Apply DES encryption on stego image

The Block diagram of the encoder is shown in the figure 5.1,the encoder consist of two stages ,the first stage is the embedding process, Thesecond stage of the encoder is the DES algorithm which encrypt each byte of the stego image.

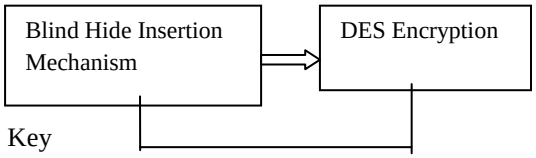

Fig. 4.1Embedding stage of proposed system

V. Extracting stage

Extracting is the process of getting the embedded secret image out of the stego image again. New terminology with respect toattaches and breaking steganography schemes is similar tocryptographic terminology. however there are somesignificant differences. Just as a cryptanalyst appliesCryptanalysis in an attempt to decoder or crock encryptedmessage, the stegonalyst is one who applies steganalysis in anattempt to detect the existence of hidden information.

After the encryption of stego image is created and transmittedthrough a communication channel, if we assume ideal channelthe encrypted stego image is received properly by the decoder circuit,again the decoder has two inputs (the extraction key and thestego image) and single output which is the secret image. Thesequence of operation here is reversed, the decryption of stegoimage is first done then the secret image is gained by applying the extraction mechanism that is reverse procedure of modified LSBand channel indexing technique, the blockdiagram of this operation is illustrated in the figure 6.1.

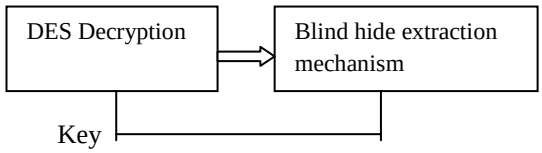

Fig. 5.1 Extracting stage of proposed system

VI. Results and Discussions

The performance of the proposed Blind Hide Technique, Modified LSB method and the Channel Indexing Technique has been analyzed by calculating the PSNR, MSE, hiding capacity and displaying the histograms which has been discussed in the following section.

PSNR: Imperceptibility takes advantage of human psycho visual redundancy, which is very difficult to quantify. Peak Signal to Noise Ratio can also be used as metrics to measure the degree of imperceptibility.

The PSNR values have been calculated by using the formula:

$$PSNR = 10 \log_{10} (255^2/MSE) \text{ dB} \quad \text{(i)}$$

The Mean Square Error can be calculated by using the following formula:

MSE =(1/M*N) $\sum_{x-0}^{M-1}\sum_{y-0}^{N-1}\left(P(x,y)-P'(x,y)\right)$ (ii)

Where M and N are the number of rows and columns of the cover image, P(x, y) is the pixel value from the cover image, p'(x, y) is the pixel value from the stego image. Signal to noise ratio quantifies the imperceptibility, by regarding the secret information as signal and as the noise. The comparison of PSNR and MSE values for various images is shown in following tables.

VII. Conclusion & Future Enhancement

The proposed image steganography technique for images imparting better information security presents an embedding algorithm for hiding secret images in nonadjacent and random pixel locations in edges and smooth areas of images. This project work is an attempt to develop Blind Hide, Modified LSB and Channel indexing technique for image hiding.

To hide secret image in the cover image the blind hide technique uses all pixels in the cover image, the principle that edge areas being high in contrast, color, density and frequency can tolerate more changes in their pixel values, so a model for Modified LSB and Channel indexing technique has been developed for various images. The modified LSB method embedds the secret image pixels across the edge and smooth area of cover image by using the enhanced method and PRNG method. It will increases the capacity and imperceptibilty of the stego image.

To achieve the better PSNR results than modified approach Channel indexing technique has been developed which uses two seed values to hide secret image pixels across edge area of the cover image which increases PSNR value and achieves less distortion in the extracted secret image. By analyzing the results of two approaches the conclusion of proposed work is that Channel Indexing technique is better in PSNR result, imperceptibility, and achieves less distortion in secret image as compared to Modified LSB method.

The future enhancement of the proposed work is that these two approaches can be advanced to use in video steganography to hide an image in video or to use in different types of steganography approach.

REFERENCES

[1] Pfitzmann, B., "Information hiding terminology - results of an informal plenary meeting and additional proposals". *In Proceedings of the First International Workshop on Information Hiding*. Springer-Verlag, London, UK, pp. 347–350. 1996.

[2] Y. K. Jain and R. R. Ahirwal, "A Novel Image Steganography Method With Adaptive Number of Least Significant Bits Modification Based on Private Stego-Keys", *international Journal of Computer Science and Security (IJCSS)*, vol. 4, 2010.

[3] H. Yang, X. Sun and G. Sun, "A High-Capacity Image Data Hiding Scheme Using Adaptive LSB Substitution", Journal: Radioengineering, vol. 18, no. 4, pp 509-516, 2009.

[4] S. Channalli and A. Jadhav, "Steganography an Art of Hiding Data", *International Journal on Computer Science and Engineering, IJCSE*, vol. 1, no. 3, 2009.

[5] C.H. Yang, C.Y. Weng, S.J. Wang, Member, IEEE and H.M. Sun, "Adaptive Data Hiding in Edge Areas of Images with Spatial LSB Domain Systems", IEEE Transactions on Information Forensics and Security, vol. 3, pp. 488-497, September 3,2008.

[6] K.H. Jung, K.J. Ha and K.Y. Yoo, "Image data hiding method based on multi-pixel differencing and LSB substitution methods", *In proceedings of International Conference on Convergence and Hybrid Information Technology (ICHIT '08), Daejeon (Korea),* 2008.

[7] H.Zang, G.Geng. and C.Xiong,"Image Steganography Using Pixel-Value Differencing", *In proceedings of Second International Symposium on Electronic Commerce and Security, ISECS*, May 2009

[8] W. J. Chen, C. C. Chang and T. H. N. Le, "High Payload Steganography Mechanism Using Hybrid Edge Detector", Expert Systems with Applications (ESWA 2010), vol. 37, pp. 3292-3301, April 4, 2010.

[9] V. Madhu Viswanatham and J. Manikonda, "A Novel Technique for Embedding Data in Spatial Domain", *International Journal on Computer Science and Engineering, IJCSE*, vol. 2, 2010.

[10] M. A. Al-Husainy, "Image Steganography by Mapping Pixels to Letters", *Journal of Computer Science*, vol. 5, no. 1, pp. 33-38, 2009.

[11] H. Motameni, M. Norouzi, M. Jahandar and A. Hatami, "Labeling Method in Steganography", World Academy of Science, Engineering and Technology, France, 2007.

[12] Mamta Juneja, and Dr. Parvinder S. Sandhu., " An Improved LSB based Steganography Technique for RGB Color Images", *In proceedings of 2nd International Conference on Latest Computational Technologies (ICLCT'2013),* June 17-18, 2013.

[13] Namita Tiwari, Madhu Shandilya., "Secure RGB Image Steganography from Pixel Indicator to Triple Algorithm-An Incremental Growth", *International Journal of Security and Its Applications,* Vol. 4, No. 4, October, 2010.