A Novel Image Steganogrphy Using Improved LSB Method

Prathibha A
Dept of Computer Science and Engineering
Alvas Institute of Engg and Technology
Manglore,Dakshina Kannada,India
prathibha.a.2307@gmail.com

Manjunath Kamath K
Dept of Information Science and Engineering
Alvas Institute of Engg and Technology
Manglore,Dakshina Kannada,India
manjunathkamathk@gmail.com

***Abstract*— Steganography is a branch of information hiding. It allows the people to communicate secretly. As increasingly more material becomes available electronically, the influence of steganography on our lives will continue to grow.The proposed improved LSB(least Significant bit) based Steganography technique for images provides better information security. This method presents an embedding algorithm for hiding encrypted images in nonadjacent and random pixel locations in edges and smooth areas of images. It first encrypts the secret images, and detects edges in the cover-image using improved edge detection filter. Input bits are then, embedded in the least significant byte of randomly selected edge area pixels and 1-3-4 LSBs of red, green, blue components respectively across randomly selected pixels across smooth area of cover image. This proposed method ensures that the eavesdroppers will not have any suspicion that secret image is hidden in the cover image and standard steganography detection methods can not detect secret image which has been hidden correctly.**

Keywords— Image hiding, Image steganography,LSB Insertion,Edge detection.

I. INTRODUCTION

With the recent advances in computing technology and its intrusion in our day to day life, the need for private and personal communication has increased. Privacy in digital communication is desired when confidential information is being shared between two entities using computer communication. To provide secrecy in communication we use various techniques. One such technique is Steganography.

Steganography is the art of passing information through original files in a manner that the existence of the message is unknown. The innocent files can be referred to as cover text, cover image, or cover audio as appropriate. After embedding the secret message it is referred to as stego-medium.

The essential concept in every data hiding method is the feebleness of human perception such as vision, listening, and hearing. It must be differentiated between steganography and cryptography because both of them are used to hide secret data. The basic dissimilarity between steganography and cryptography is that cryptography focuses on preserving the contents of the message confidential.

Steganography concentrates on preserving the existence of a message confidential at the first place. Hence, if the notion is to conceal the existence of the secret message, then the method of steganography is preferred. Also, it must be differentiated between steganography and watermarking because of the common confusion between them. The essential difference between steganography and watermarking is the absence of an adversary. In watermarking there is an active adversary that would try to forge the watermarks. On the contrary, in steganography there is no such an active adversary. The main difference between cryptography and steganography is that cryptography scrambles the message so that it becomes difficult to understand whereas steganography hides the very existence of a message. Steganography plays the central role in secret message communication.

Image steganography has many applications especially today's modern, hightech world. Privacy and anonymity is a concern for most people on the internet. Image Steganography allows for two parties to communicate secretly and covertly. It allows for some morally-conscious people to safely whistle blow on internal actions; it allows for copyright protection on digital files using the message as a digital watermark. One of the other main uses for Image Steganography is for the transportation of high-level or top-secret documents between international governments. While Image Steganography has many legitimate uses, it can also be quite nefarious. It can be used by hackers to send viruses and trojans to compromise machines, and also by terrorists and other organizations that rely on covert operations to communicate secretly and safely.

II. RELATED WORK

The Review of various Existing methods for Image Steganography has been Discussed in the following section.

The authors Y. K. Jain *et.al.,* [1] 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. This private stego-key has 5 different gray level ranges of image and each range indicates to substitute fixed number of bits to embed in least significant bits of image. 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. It also proposed a method for color image just to modify the blue channel with this scheme for information hiding. This method is targeted to achieve high hidden capacity plus security of hidden message.
To overcome the drawback of using extra bits of signature the authors H.Yang *et.al.,* [2] 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 value of k is high at non-sensitive image region and over sensitive image area k value remain small to balance overall visual quality of image. The LSB's (k) for embedding is computed by the high-order bits of the image. It also utilizes the pixel adjustment method for better stego-image visual quality through LSB substitution method. 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'.

To overcome the limitation of small dataset the authors S.Channalli *et.al.,* [3] 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. Pattern bits are combination of MxN size rows and columns (of a block) and with random key value. In embedding procedure, each pattern bit is matched with message bit, if satisfied it modifies the 2nd LSB bits of cover image otherwise remains the same. 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.

To overcome above drawback the authors C.H. Yang *et.al.,* [4] 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. PVD method generally provides a good imperceptibility by calculating the difference of two consecutive pixels which determine the depth of the embedded bits. Proposed method hides large and adaptive k-LSB substitution at edge area of image and PVD for smooth region of image. 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 the authors K.H.Jung *et.al.,* [5] have proposed a method of Multi-Pixel Differencing (MPD) which used more than two pixel 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 the authors H.Zhang *et.al.,* [6] proposed another pixel value differencing method, it used the three pixels for data embedding near the target pixel. It uses simple k-bit LSB method for secret data embedding where number of k-bit is estimated by near three pixels with high difference value. 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.

The authors *W.J Chen et.al.,* [7] 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. This method is not tested on extensive edges based image like 'Baboob.tif'.

To provide more security the authors Madhu *et.al.,* [8] 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.

To overcome above drawback the author Al-Husainy [9] proposed an image steganographic method of mapping pixels to alphabetic letters. It maps the 32 letters (26 for English alphabetic and other for special characters) 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. According to that table, each letter can be represented in all 4 cases. It utilizes the image 7 MSB (Most Significant Bits) (27 = 128) bits for mapping. Proposed method maps each 4-case from the 7 MSB's of pixel to one of the 32-cases in that table. These 4-cases increase the probability of matching. 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 the authors M.Motameni *et.al.,* [10] 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.

To overcome above drawback authors Babita *et.al.,* [11] uses 4 LSB of each RGB channel to embed data bits, apply median filtering to enhance the quality of the stego image and then encode the difference of cover and stego image as key data. In decoding phase the stego-image is added with key data to extract the hidden data. It increases the complexity to applying filtering and also has to manage stego-key. Proposed scheme has high secret data hiding capacity.

The authors M. Tanvir Parvez *et.al.,* [12] have proposed a pixel indicator technique with variable bits; it chooses one channel among red, green and blue channels and embeds data into variable LSB of chosen channel. Intensity of the pixel decides the variable bits to embed into cover image. The channel selection criteria are sequential and the capacity depends on the cover image channel bits. Proposed method has almost same histogram of cover and stego-image.

Hamid *et.al.,* [13] have proposed a texture based image steganography. The texture analysis technique divides the texture areas into two groups, simple texture area and complex texture area. Simple texture is used to hide the 3-3-2 LSB (3 bits for Red, 3 bits for Green, 2 bits for Blue channels) method. On the other hand over complex texture area 4 LSB embedding technique is applied for information hiding. The above method used the both methods depending on texture classification for better visual quality. Proposed method has high hidden capacity with considering the perceptual transparency measures e.g PSNR etc.

M. Chaumont *et.al.,* [14] have proposed a DCT based data hiding method. It hides the color information in a compress gray-level image. It follows the color quantization, color ordering and the data hiding steps to achieve image steganography. The purpose of method is to give free access to gray-level image to everyone but restricted access of same color images to those who have its stego-key. It has high PSNR plus with noticea$ble artifact of embedding data.

K. S. Babu *et.al.,*[15] proposed hiding secret information in image steganography for authentication which is used to verify the integrity of the secret message from the stego-image. The original hidden message is first transformed from spatial domain to discrete wavelet transform (DWT); the coefficients of DWT are then permuted with the verification code and then embedded in the special domain of the cover image. The verification code is also computed by special coefficient of the DWT. So this method can verify each row of the image of modified or tampered by any attacker.

III. TECHNIQUES USED

For Hiding an image in image by using improved LSB method includes the following Steganographic techniques.

A. Detection of edges in cover image

The most important features of objects in images are edges. The proposed approach uses a Canny Filter which provides better results in detecting edges. Canny filter is used as it provides better demarcation in edge areas and smooth areas which is need of this proposed steganography technique. The Canny method finds edges by looking for local maxima of the gradient of the image. The gradient is calculated using the derivative of the Gaussian filter.

The figure 1, represents original image and the outcome after applying Canny operation on it. In this case the edge has been found, but it becomes “broad” due to the threshold.

Fig. 1. (left) Original Image, (right) Result of Canny

B. Image Based Steganography

Embedding the information into an image requires two files. The first is the innocent-looking image that will hold the hidden information, called the cover image. The second file is the secret image to be hidden. When combined, the cover image and the embedded secret image make a stego-image. A stego-key may also be used to hide then later decode the secret image.

B1. Embedding secret image using Modified LSB

To embed the secret image in the cover image the following methods has been discussed to hide input bits across edge and smooth areas of cover image.

B1.a Embed secret image bits in Least significant byte of each pixel across Edge areas:

To embed the data, the LSB insertion is used. LSB insertion is a common, simple approach in embedding information in a cover file. But in this improved LSB technique we will insert the input bits 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 a image 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 as following.

(00100110 11101001 01000001)

B1.b Embedding secret image bits using 1-3-4 LSB Insertion across Smooth areas

To embed the image in smooth areas 1-3-4 LSBs Insertion technique has been utilized which hides data in 1-bit in 1 least significant bit of Red component, 3-bits in 3 least significant bits of Green component and 4 bits in 4 least significant bits of Blue component of each selected pixel. This ratio 1:3:4 has been taken depending on their respective contribution of each red, green and blue component to the colors of RGB image.

C. Randomly Selecting Edge Pixels

To select the edge pixel randomly, a pseudorandom number generator (PRNG) will be used. Pseudorandom number generator is an algorithm that generates a sequence of numbers, the elements of which are approximately independent of each other. The outputs of pseudorandom number generators are not truly random - they only

approximate some of the properties of random numbers. To use a PRNG, it first requires a seed. Seeding is the technical term for giving it an initial value, from which it can shoot out a sequence. If a PRNG is given the same seed, then it will give the same set of numbers every time and the elements of which are approximately independent of each other.

2. Apply Encryption on input using S-DES algorithm.
3. Embed secret image in least significant byte of all pixels selected in random manner using PRNG across edge areas.
4. Embed secret image using 1-3-4 LSB technique as mentioned above across smooth areas at random locations.

V. RESULTS AND DISCUSSIONS

The following section illustrates the results obtained after the use of above methods.

The image to be hidden in the cover image was first encrypted using the S-DES algorithm. Features (edges, corners, thin straight lines, end of lines etc.) were detected from the cover-images using Canny filter. Random pixel locations were found in the cover-image by the PRNG. Then, secret image bits were embedded at the random-edge area pixel locations and smooth area pixel locations using modified LSB insertion algorithm. Figure 2 presents the results of applying this technique to standard image Lena.

Fig. 2. A. Original image B. Stego image

VI. CONCLUSION

This paper introduse various steganography techniques and they are analysed. Here the research has been carried out for hiding encrypted secret image into the carrier image to provide better security for secret communication. The proposed new technique presents an improved steganography method for embedding secret image bit in least significant byte of nonadjacent and random pixel locations in edges of images and 1-3-4 LSBs of red, green and blue components of randomly selected pixels across smooth areas. The research is aimed towards the evaluation and development of a new and enhanced data hiding technique based on LSB. The primary objective is to propose a solution that is robust, effective and to make it very hard for human eye to predict and detect the existence of any secret data inside the host image.

IV. PROPOSED APPROACH

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

1. Divide the cover image into smooth and edge areas using Canny Filter

REFERENCES

[1] 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**.

[2] 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.**

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

[4] 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, **2008** September 3.

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

[6] H.Zang, G.Geng and C.Xiong, "Image Steganography Using Pixel-Value Differencing", Electronic Commerce and Security, ISECS '09. Second International Symposium on **2009** May.

[7] 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, **2010** April 4.

[8] 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**.

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

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

[11] B.Ahuja, M.Kaur and M. Rachna"High Capacity Filter Based Steganography", International Journal of Recent Trends in Engineering, vol. 1, no. 1, **2009** May.

[12] M. Tanvir Parvez and A. Abdul-Aziz Gutub, "RGB Intensity Based Variable-Bits Image Steganography", IEEE Asia-Pacific Services Computing Conference, pp. 1322-1327, **2008**.

[13] A.M.Hamid and M.L.M. Kiah, "Novel Approach for High Secure and High Rate Data Hidden in the Image Using Image Texture Analysis", International Journal of Engineering and Technology (IJET): 0975-4042, **2009**.

[14] M. Chaumont and W. Puech, "DCT-Based Data Hiding Method To Embed the Color Information in a JPEG Grey Level Image", 14th European Signal Processing Conference (EUSIPCO 2006), Florence, Italy, copyright by EURASIP, **2006** September 4-8.

[15] K.S.Babu, K.B.Raja, K.Kiran Kumar, T.H. Manjula Devi, K.R. Venugopal and L. M. Pataki, "Authentication of secret information in image steganography", IEEE Region 10 Conference, TENCON-2008, pp. 1-6, **2008** November.