RESEARCH ARTICLE OPEN ACCESS

Digital Image Steganographic Approach (DISA) to Enhance Quality and Imperceptibility

Shampy Sharma [1], Dr. Ashish Oberoi [2], Pavninderpal Kaur [3]
Department of Computer Science and Engineering [1] & [2]
MMEC Mullana, Ambala, Haryana
Department of Computer Science and Engineering
LLRIET Moga, Punjab
India

ABSTRACT

Steganography is the secret communication technique, in which only the sender and the intended recipient know about the existence of message. The proposed work introduces an improved digital image steganographic approach focused on reducing the image degradation rate. For this purpose, initially an RGB image was divided into layers followed by segmenting any of the layers into four equal sized blocks. Message was then embedded in highest entropy block among the four blocks to reduce the imperceptibility of message. The concept of forward and reverse identical pair matching between the intensity values of pixel and the bits of secret message was applied to improve the quality of the steganographic image. To ratify the proposed algorithm, two performance measures namely, peak signal to noise ration and correlation coefficient are used.

Keywords:- Steganography, entropy, embedding, extraction.

I. INTRODUCTION

Steganography is a word of Greek origin, which consists of two words, namely, *Steganos* and *Graphie*. The word Steganoes means something covered or protected and graphie means drawing or writing. So, on the whole the referred term stands for 'concealed writing' [1][2]. In the field of information hiding, the Greek meaning of the term is molded as per its use in that domain. It is defined as the phenomenon of covering the secret message behind any multimedia object to serve the purpose of secret communication. Formally, it is the art of secret communication aimed at concealing the message, so that no one except the sender and intended recipient know about the existence of message [3].

Steganography is not a new-fangled idea. Its history is dates back to centuries, though it kept changing its forms. This technique was drilled in by Greeks. They used to shave the head of their slave and then tattoo the message there on its bald head. After the hair had grown back, the slaves were sent to the intended recipient who again shaves the head of slave to read that message [4]. This method had an obvious disadvantage of delayed transmission and limited size of message. Later, people used to write messages on the wood and then cover it with wax. These items known as wax tablets were then sent to the recipient, who used to peel off the wax in order to read that secret message [5]. During World War I and II, Germans introduced another form of steganography in terms of null ciphers. For example, actual message was formed by using the first alphabet of every word of the sent message [6]. During American Revolution, invisible inks came into existence. Secret messages were used to be written on paper using these inks, which can be read by exposing these papers to fires or another such rays [5].

Steganography is carried out at the two ends, i.e., at the sender and receiver side. The steganographic process carried out at the sender end is termed as embedding process and it is called as extraction process at the receiver side. During embedding process, the secret message to be sent is inserted inside the digital cover image to form steganographic image. Steganographic image is nothing, but the cover image with message present in it. On the other hand, while extraction process the embedded secret message is plucked out of the steganographic image [7]. The use of secret key is optional. It is mandatory while extraction, if it is used during embedding [8]. The block diagram of embedding and extraction process is shown in Figure 1.

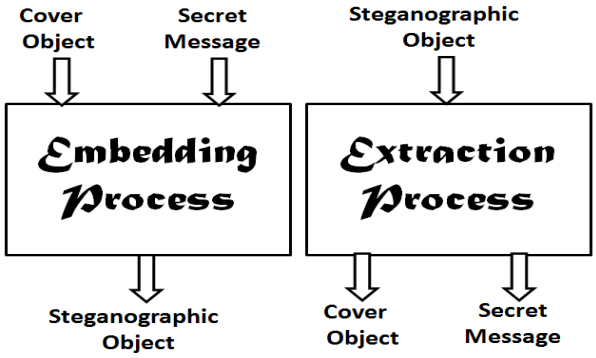


Fig. 1: Block diagram of steganography

In this paper, an improved steganographic algorithm is proposed to improve the steganographic quality of an image by embedding the message in highest entropy block using the concept of identical matching. Entropy is a measure of randomness used to denote the texture of any image. It is the number of gray levels that individual pixels of an image can adopt. If P is the histogram count, then entropy can be calculated as in (1).

$$E = -\sum P \log_2 P \qquad (1)$$

Entropy is low in the images which are perfectly histogram equalized. If all the pixels of an image have same value, its entropy is zero [9].

In section II, literature review is discussed followed by the proposed work discussed in Section III. Section IV shows the results of proposed work on test images. Conclusions and future work are summarized in Section V followed by references.

II. LITERATURE REVIEW

To clarify what steganography is and what it can do, a large number of approaches were outlined that were used to hide encrypted copy right marks or serial numbers in digital audio or video. Number of attacks was also presented on information hiding techniques [10]. Most embedding methods had a common drawback that original image is inevitably distorted by some small amount of noise due to data embedding itself. Although the distortion was quite small, but it was not acceptable for medical imagery or military images inspected under unusual viewing conditions. So, a lose less steganographic approach was proposed for high capacity data embedding [11]. An optimal block mapping least significant bit method was proposed based on genetic algorithm A rule was discussed to select the best block size for embedding message. The main idea was to minimize the degradation of the stego image by finding a best mapping function between host and secret image blocks at global scope [12].

Later two hybrid least significant bit substitution methods were proposed for improving the quality of steganographic image. The first method coupled the optimal least significant bit substitution and optimal pixel adjustment process to improve the quality of steganographic image. The second method was the variation of the first one which replaces the optimal LSB substation with the worst LSB substitution [13]. A reversible data hiding method based on image interpolation and the detection of smooth and complex regions in cover images was also proposed. Pixels were interpolated according to the constructed binary image, and the interpolation errors were then used to embed data through histogram shifting. The pixel values in the cover image were modified one grayscale unit at most to ensure the production of high quality stego-image [14]. Another reversible data hiding scheme was also introduced that provides the ability to hide the data into a host image and then recover the host image without losing any information when the secret data is extracted [1].

A robust technique of hiding data in image based on least significant bit insertion and RSA encryption technique was proposed to encrypt the secret data. Then the encrypted data was converted into a bit stream and divided into number of segments. However, the cover mage was also divided into same number of segments. Each segment of data was compared with each segment of image to find the best match segment, in order to create a random sequence of events that were then inserted in cover image [15]. A novel steganographic approach to embed secret message into image using block complexity in wavelet domain was also introduced to improve robustness. Experimental results illustrated that steganographic image is indistinguishable from the original image by human eye and algorithm offered good quality in terms of peak signal to noise ratio and structural similarity index matrix [16].

A standalone steganographic technique that hides the secret message based on searching about the identical bits between the secret message bits and image pixel values was proposed. To embed message, it searched about identical match between message bits and pixel values at four locations. If match was found then its address is stored else LSBs of pixel are changed [17]. A steganographic algorithm based on least significant bit substitution to hide text file inside the digital image was presented. All the three layers of an RGB image were used alternatively to embed data in the least two significant bits of selected pixel. In order to increase the storage capacity, a compression

algorithm was also used. Furthermore, two cover images were used [2]. A hybrid approach to steganography based on the two above mentioned techniques was later introduced. It was a standalone steganographic technique that was focused on reducing the changes in the least significant bits of cover image by finding identical matches between image pixel values and message bits. In order to improve the security of message, the concept of jump table is used, i.e., message is scattered on the blocked image rather than embedding it on continuous pixels which makes extraction a semi-blind process [3].

III. PROPOSED WORK

The proposed DISA is based on the concept of entropy as discussed in Section I. Entropy measure is used to improve the imperceptibility of message in steganographic image. In high entropy areas, where the intensity of pixels change frequently, human eyes are not able to detect the changes. This is because human eyes are unable to track out gradual changes to shade. So in proposed work, message is embedded in high entropy blocks. This work is studied under two sections, i.e., embedding process and extraction process as discussed under.

A. Embedding Process

Embedding process is the phenomenon carried out at the sender's side. During this process, number of steps is taken to insert the secret message in the cover image. This number of steps together is commonly referred to as embedding algorithm. The flowchart of proposed embedding process is shown in Fig. 2.

Initially, the image is resized to 512×512 and then divided into four equally sized 256×256 blocks. Afterwards entropy of each block is calculated using (1). Then the block with highest entropy is chosen for embedding the secret message into it. If the length of message exceeds the capacity of one block, then block with second highest entropy is chosen for further embedding and so on.

Using the proposed embedding algorithm, 2 bits can be embedded in one pixel. It means one character of 8 bits can be embedded in 4 pixels. Since the considered block size has 256 rows and 256 columns, i.e. 65,536 pixels, this means that 8192 characters can be embedded in one block. In the whole image 65536×4=32768 characters can be embedded. After choosing the required block/s actual embedding takes place based on the concept of identical matching.

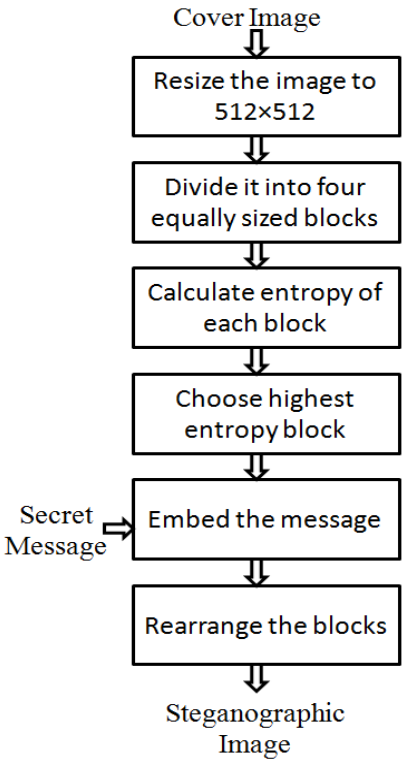


Fig. 2. Flowchart of Embedding Process.

To understand the concept of identical matching between message bits and intensity values of pixels, consider the following binary secret message: 10 10 11 10. Let the intensity values of first three pixels of an 8 bit image to be: 00 10 00 01, 00 00 00 01, 0 10 00 00 respectively.

To embed first two bits of message, i.e., 10 in first pixel, it searched about the identical pair at seven different locations in forward direction as shown in Fig. 3(a). After finding the match, it stores the location of those bits. Then, it moved on to next two bits of message, i.e. 10 again and the second pixel. It can be seen that no identical match exists in forward direction. Then it starts searching in reverse direction and found the match in the direction of arrow as shown in Fig. 3(b). In the last case, in order to embed 11 no match exists in both the directions. So it will perform the bitwise NOT operation on the message bits and again start finding the match in forward as well as reverse direction. If the match is found it will store the bit position, else in the end, if match is not found then the two least significant bits of pixel are replaced with message bits. This process is carried out until the whole message is embedded in the image.

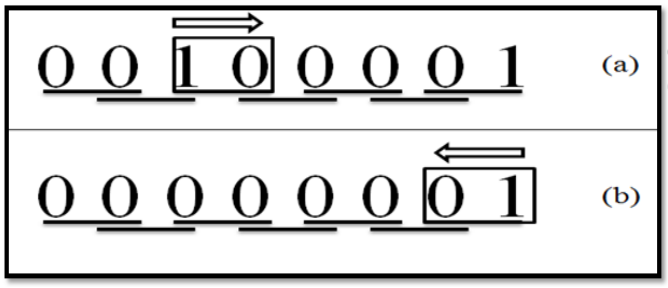


Fig.3. Example Showing the Embedding of Message

B. Extraction Process

The extraction process is simply the reverse of embedding process. This is carried out at the receiver's end. Steganographic image is passed to the system to pluck out the secret message from the image. The flowchart of extraction process is shown in Fig. 4.

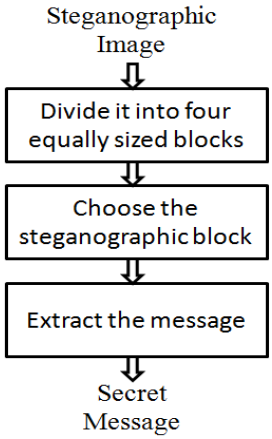


Fig. 4. Flowchart of Extraction Process

IV. RESULTS AND DISCUSSIONS

The proposed algorithm tested against four test images, namely, autumn.tif, onion.png, lena.jpg and baboon.png shown in Fig.4.

The proposed work is validated using two performance metrics namely peak signal to noise ratio (PSNR) and correlation coefficient (CC). To measure PSNR, first of all, mean square error (MSE) is calculated [18][19]. MSE is defined as the mean of square of differences in the intensity values of pixels of two images. It is calculated using (2) where M and N represents the total number of rows and columns of an image and i , j represents the coordinates of an image:

$$MSE = \frac{1}{MN}\sum_{i=0}^{M-1}\sum_{i=0}^{N-1}\left[\{x(i,j)-y(i,j)\}^2\right] \quad (2)$$

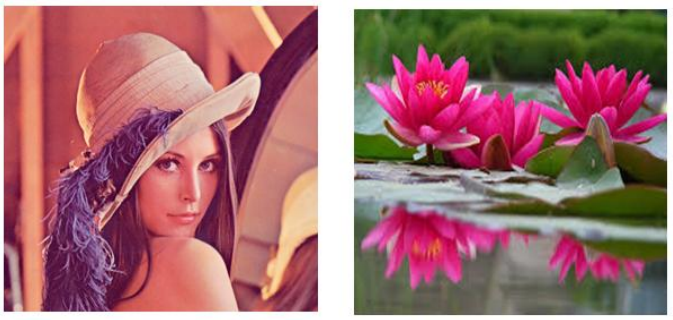
PSNR is used to track out the difference between the cover and steganographic image. It is measured in decibels (dB) and can be calculated as in (3) [3]:

$$PSNR = 10\log 10\left(\frac{255\times 255}{MSE}\right) \quad (3)$$

CC is used the similarity between the two images of same size [3]. It can be calculated by using (4) where C represents the original image and S represents the steganographic image.

$$CC = \frac{\sum(C(i,j)-M1)(S(i,j)-M2)}{\sqrt{\sum(C(i,j)-M1)^2}\sqrt{\sum(S(i,j)-M2)^2}} \quad (4)$$

(a) (b)



(c) (d)

Fig. 5. Test Images (a) Autumn.tif (b) Onion.png,

(c) Lena.jpg (d) Flowers.jpg

As clear from (2), the value of MSE should be low because it represents the error, i.e., changes made to the original image. Since, MSE is inversely proportional to PSNR, higher values of PSNR are required. The ideal value of MSE is 0, hence, for PSNR it is infinity. On the other hand, the value of CC lies between 0 and 1, where 1 is the best value. The values of these performance metrics between the cover image and steganographic image are listed in Table 1 for test images.

TABLE 1. COMPARISON OF COVER AND STEGANOGRAPHIC IMAGE USING DISA

Image name	Performance Metrics	
	PSNR (dB)	*CC*
onion.png	92.3647	1.00
autumn.tif	84.0053	1.00
lena.jpg	84.4392	1.00
flowers.jpg	84.055	1.00

As clear from the table, the value of PSNR is generally around 84 dB for three images but for onion.png, it fluctuates to 92 dB approximately. This may be the result of more identical pair matches found between the image pixel values and message bits. The ideal value of CC in all cases denotes almost negligible changes in the image after embedding message. Hence, it can be said that images are indistinguishable to the human eye. In other words, message is imperceptible in the image, thus, achieving the first and foremost objective of steganography, i.e., confidentiality.

V. CONCLUSIONS AND FUTURE SCOPE

The proposed DISA is an improved digital image steganography. It is aimed at reducing the image degradation by using the concept of forward and reverse identical pair matching between the intensity pixel values and secret message bits. Section IV shows that the experimental result is very promising in terms of PSNR and CC for all the test images. This is because very few changes are made to the original cover image for inserting the secret message into it. Changes are made only in case no match exists between the pair of message bits and intensity values of pixels, taken two bits at a time. This improves the quality of image by decreasing the image degradation rate. Furthermore, the message is embedded in high entropy block, thus improving the imperceptibility of message in the steganographic image. For future work, the robustness of message in the image can be considered in any frequency domain.

ACKNOWLEDGMENT

I would like to take this opportunity as a special note of thanks to Dr. Ashish Oberoi, Assoc. Professor, Department of Computer Science and Engineering, for his valuable and expert supervision, attention grabbing views and obliging nature which led to the successful completion of this work. I also place on record, my sense of gratitude to Pavninderpal Kaur, for her unceasing encouragement and support. I would not have been able to complete this work without her motivation.

REFERENCES

[1] S. Ananthi and A. Anjanadevi, (2012), "Reversible image hiding using predictive coding technique based on steganographic scheme", vo. 2, pp. 27-33.

[2] V. Sharma and S. Kumar, "A new approach to hide text in images using steganography," International Journal of Advanced Research in Computer Science and Software Engineering, vol. 3, April 2013.

[3] P. Kaur, H. Singh, A. Gupta and A. Girdhar, (2014), "*An improved steganographic approach to diminish data modification for enhancing image quality*," Internationaal conference on medical imaging, m-health and emerging communication systems (Medcom), pp. 329-333.

[4] H. Wang and S. Wang, "Cyber: Warfare: Steganography vs Steganalysis", Communications of the ACM, 2004.

[5] R. Doshi, P. Jain and L. Gupta, (2012), "*Steganography and its applications in security*," International Journal of Modern Engineering Research, vol.2.

[6] T. Morkel, "Image Steganography Applications for Secure Communication," Universiteit van pretoria, May 2012.

[7] W. Peter, "Disappearing cryptography: Information hiding: Steganography and watermarking," San Francisco, 1992.

[8] S. Channalli and A. Jadhav, "Steganography: An Art of Hiding Data," International Journal on Computer Science and Engineering, vol. 1, 2009.

[9] V. F. Rajkumar, GRS. Manekandan, V. Santhi, "Entropy based robust watermarking scheme using hadamard transformation technique," International Journal of Computer Science Applications, vol. 12, January 2011.

[10] R. J. Anderson and F. A. P. Petitcolas, (1998), "*On the limits of steganography*," IEEE Journal of Selected Areas in Communications, pp. 474-481.

[11] M. Goljan, J. Fredrich and R. Du, (2001), "*Distortion-free data embedding for images*,"

Proceedings of the 4th International Workshop on Information Hiding, pp. 27-41.

[12] R. Ji, H. . Yao, S. Liu, L.Wang, "Genetic algorithm based optimal block mapping method for LSB substitution," IEEE International Conference on Intelligent Information Hiding and Multimedia Signal Processing, pp. 215-218, 2006.

[13] C. C. Chang and H. W. Tseng, "Data hiding in images by hybrid LSB substitution," Third International Conference on multimedia and Ubiquitous Engineering, pp. 360-363, 2009.

[14] W. Hong, T. Chen and M. Wu, "An improved human visual system based reversible data hiding method using adaptive histogram modification," Optics Communications, vol. 291, pp. 87-97, 2011.

[15] E. T. Khalaf and N. Sulaimann, "A robust data hiding technique based on LSB matching", World Academy of Science, Engineering and Technology, vol. 5, pp. 75-79, 2011.

[16] G. Dhanarasi and A.M. Prasad, "Image steganography using block complexity analysis," International Journal of engineering science and technology, vol. 4, pp. 3439-3445.

[17] A. M. Al-Shatnawi, "A new method in image steganography with improved image quality," Applied Mathematical Sciences, vol. 6, 2012.

[18] A. Oberoi, E. Walia, "An efficient algorithm eradicating semantic gap with help of image quality assessment", in International Journal of Engineering Sciences and Technology, Vol. 2(9), pp. 5050-5057, October 2010.

[19] C. Sahrma , A. Oberoi, "An Efficient Watermarking Approach for Digital Images", in International Journal of Engineering Research and Applications, Version II, pp. 45-48, March 2014.