Volume 4, Issue 3, March 2014 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

A New Edge Based Image Steganography Technique for RGB Images

Deepali Singla*, Mamta Juneja
UIET,Panjab University
India

Abstract— Steganography is a branch of information security. Steganography aims at hiding the existence of the actual communication. This aim is achieved by hiding the actual information into other information in such a way that intruder cannot detect it. A variety of carrier file formats can be used to carry out steganography e.g. images, text, videos, audio, radio waves etc. But mainly images are used for this purpose because of their high frequency on internet. Number of image steganography techniques has been introduced having some drawbacks and advantages. These techniques are evaluated on the basis of three parameters imperceptibility, robustness and capacity. In this paper we will propose a new steganography technique for RGB images based on least significant bit (LSB) technique and hybrid edge detector. Main idea behind this technique is that edges can bear more variation than smooth areas without being detected.

Keywords— edge based image steganography, LSB substitution, canny edge detector, Hough transform, and fuzzy edge detector.

I. INTRODUCTION

The use of internet is increasing day by day and transfer of important information through it is also increasing. As important information is transferred; security of such information is also necessary. Encrypting, such information is one of the ways to provide security. In encryption information is changed in such a way that intruder cannot read this information. But during encryption; message is changed therefore it becomes distorted and intruder may easily suspect about the presence of confidential information. Steganography is another way of securing the secret information. Steganography is a branch of information security that hides the important and confidential information in to an innocent media in such a way that no one except recipient can extract the information [1]. Different steganographic techniques have been introduced since ancient times. Ancient techniques made use of invisible ink; microdots character arrangement etc. [2]. Due to digitization in modern times, digital media has become the source of steganography e.g. images, text, audio and video files. Many other digital mediums are used for steganography like floppy disk, hard drive, radio waves and network packet etc. [3]. Main goal of steganography is to make the hidden information undetectable. Main components of image steganography are as shown in the figure1.

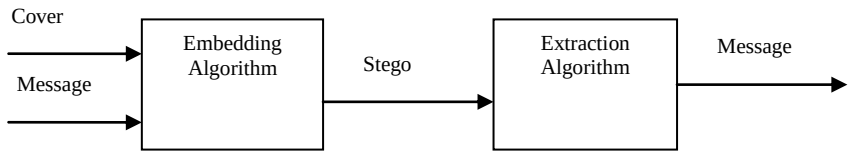

Fig.1. Basic components of Steganography[4]

In the above figure firstly both cover image and message bits are given as input to the embedding algorithm. An Embedding algorithm is a steganography technique that will embed the message bits into the cover image such that intruder is unable to detect it. This algorithm will generate stego-image as an output. Stego image is the cover image containing message bits inside it. This image is communicated over the media between sender and receiver. At the receiver end an extraction algorithm will work on the stego image and extracts the hidden message bits from the stego image.

There are three basic parameters for evaluation of different steganography techniques.

1. Imperceptibility: It is the ability of steganography method to avoid detection of hidden message through human visual system (HVS) and statistical analysis. It can be measured through peak signal to noise ratio (PSNR) [5].
2. Capacity: It is number of bits of message that are hidden into a stego image.
3. Robustness: It is ability of the steganography technique to retain the hidden message after many image related operations. These operations are compression, cropping, rotation and filtering etc.

Many steganography techniques have been introduced so far to achieve higher imperceptibility, capacity and robustness. The organization of this paper is as follows. Section 2 provides the analysis of edge based image steganography techniques. Section 3 discusses the new proposed technique. Section 4 highlights the conclusion and the future work that can be done on the proposed method.

II. LITERATURE SURVEY

Number of image steganography techniques has been introduced so far. At the beginning a simplest method i.e. least significant bit (LSB) substitution has been introduced to hide information. This technique replaces the least significant bits of each pixel are replaced with the binary data (i.e. information) [6].However this is not a secure technique as the stego image contains flecks at the place where the message bits are hidden and hidden message bits can easily be recovered through repetition of the same process. Many attacks like sample pair analysis [7], difference image histogram [8], blind detection algorithm [9] has been performed on this method.

In order to overcome the problem of LSB substitution a new tool named ―Hide and Seek for Windows 95 ‖has been introduced. This tool distributes the information to be hidden randomly across the image pixels[10]. But drawback is that the information hidden using both these methods can be easily detected by the intruder. An attack can be performed on these two methods using Laplace formula [11].

In 2006, a new algorithm named as first filter algorithm has been introduced to overcome the problems of above mentioned techniques. The main idea in this algorithm is that variation in features of image is less noticeable. First filter algorithm uses edge detection filters like Laplace formula. Also author has purposed another algorithm named battlesteg through the combination of first filter algorithm and hide seek method. Battle steg stands for battleship steganography. Main drawback of this method is that further processing cannot be done on the stego image e.g. segmentation [12].

In 2006 only, an adaptive filtering based image steganography technique has been introduced. The challenging issue in existing adaptive steganography methods is that they don't specify any method to control the number of bits hidden in carrier medium [13]-[16]. In this technique data bits are hidden into the high intensity components and low intensity components are not used for hiding data. During embedding, magnitude of the pixel is also considered. Higher the value of magnitude, higher the number of bits embedded in that pixel. Magnitude in high frequency component is always considered to be greater than 128 so embedding rate of 1bpp is achieved in this technique. Instead of using high pass filter multi band filter can also be used. The main advantage of this technique is that it limits the quantity of hidden information by adjusting cut off frequency. It is less prone to stego attacks. High embedding rate and high confidentiality is achieved through this method. Disadvantage is that if there is small variation in the cut off frequency and order of filter at receiver and sender end the message decoded will not be same as that of original message [17].

In 2007, Random edge LSB (RELSB) technique has been introduced. This approach randomly hides the message bits into the regions that have least similarity with their neighborhood. These regions generally contain edges, thin lines, end of lines etc. Robert cross gradient operator is used to extract such regions. Then random locations in these regions are selected using random number generator algorithm i.e. PRNG. The simplified data encryption standard (S-DES)is used to encrypt the message bits. Encryption is done to provide another layer of security. Data is hidden is such a way that same edges and line pixels are detected before and after data embedding. This approach has been better than LSB substitution [6], random LSB Embedding [10], edge LSB embedding [12]as gradient energy technique can detect number of hidden bits in all these three technique but not in RELSB [18].

In 2008 another edge based LSB steganography technique has been introduced. This is based on pixel value differencing (PVD) and LSB replacement [19] with some modification in these and provides more capacity and imperceptibility. The difference of a given pixel with its neighbor pixel is used to decide the embedding rate for that pixel. The difference of two pixels is used to categorize blocks into levels i.e. lower level, middle level and higher level. According to the level in which the block falls embedding is done. After embedding if level of a block is changed then value of pixel is modified in such a way that level remains same. This provides high fidelity stego image. Main drawback of this method is that range table used at sender end is also needed to send to receiver for extraction [20].

In order to overcome the main drawback of edge adaptive steganography [20], a new method has been introduced in 2009 named as variable rate steganography using neighbor pixel relationship. This technique also overcomes the drawback of PVD technique [21] which also uses range table. The pixel's relationship with its neighborhood is used to decide whether it is an edge pixel or smooth area pixel. On the basis of neighborhood relationship three methods ―four neighbors method‖, ―diagonal neighbor method‖, ―eight neighbor method‖ were given. All these methods have better peak signal to noise ratio (PSNR). But main drawback is that only half numbers of the pixels are used for embedding rather than using almost all pixels [22].

In 2010, to increase the embedding capacity with higher PSNR rate a new technique has been introduced using hybrid edge detection. Hybrid edge detector is combination of canny edge detector [23] and fuzzy edge detector[24]. Combination of both these detectors provides more number of edge pixels than that of their individual results. In this method after getting edge pixels using hybrid detector image is divided into non overlapping block of size say n. LSBs of first pixel in each block is used to describe the status of other pixels in the block i.e. edge pixels or a non-edge pixels. Edge pixels are embedded with the more number of bits than the non-edge pixels. This method resist statistical analysis based attack as data is not hidden in all the pixels. Beyond providing high embedding capacity higher PSNR is also ensured by this method [24]. In 2011, a new edge embedding technique has been introduced that target on higher PSNR rather than higher embedding rate. This method provides better PSNR than [20][22][24]. Edges of the image are obtained using sobel/canny edge detector. Only horizontal edges of a particular edge length are used further. These edge pixels are used for embedding purpose but to calculate the difference of these edge pixels with upper edge boundary. If this difference i s greater than some predefined difference then these upper boundary pixels are used for embedding data bits accordingly. In this way the stego image with least perceptual transparency is obtained. The strong point of this method is high PSNR value but having a drawback of least embedding capacity. Another drawback is that it uses horizontal direction edge pixel boundary only [25].

In 2012, a new parameterized canny edge detection based embedding approach has been introduced. Parameterized canny edge detector uses three parameters i.e. higher threshold value, Gaussian filter and lower threshold value. This property makes the stego image more robust as different values of these parameters yields different outputs. In this approach three LSBs of all three channels of edge pixels are replaced with the secret data bits. The advantages of this approach are imperceptibility and irrecoverability [26].

In 2013, a new LSB based edge embedding technique using hybrid edge detection filter has been introduced to improve the capacity and PSNR. Rather than applying Canny with fuzzy edge detector as in [24] combination of the Canny and enhanced Hough edge detector is used to get edge pixels. Message to be embedded is encrypted with AES [27] to provide another level of security. The encrypted message bits are hidden in the smooth area pixels and edge area pixels. This method ensures the higher PSNR value and high embedding capacity. Also this method provides security against various attacks e.g. visual analysis, histogram analysis, chi-square and RS analysis [28].

III. PROPOSED METHOD

A larger number of techniques proposed so far have not achieved all the three goals of steganography simultaneously. Some lacks in achieving high capacity some in robustness and some in achieving imperceptibility. So a technique must be derived which can achieve all these three goals appropriately. On the basis of analysis on previously done work, a new technique is proposed in this paper which will address previously mentioned problems.

As mentioned previously edge areas can be used for embed more pixels where as smooth areas are more sensitive to the changes. So in this proposal we are going the use hybrid edge detector to have better results. Then embedding is done according the edge pixel and smooth area pixel. Steps to be followed in the proposed technique are given as follow:

Step1: Apply hybrid edge detector (Canny+ Hough +fuzzy) on the cover image I and get edge image.

Step 2: Apply AES (advanced encryption standard) cryptography algorithm on the message to be hidden.

Step 3: Embedding Encrypted message into cover image.

For edge pixels use 1-4-8 LSB technique.

For non-edge pixels use 3 LSBs of blue channel to embed message bits.

Step 4: Resulting stego image I' is send to receiver.

Step 5: At the receiver end inverse procedure is applied to get the message bits.

Flowchart of proposed work is shown in figure 2 and figure 3.

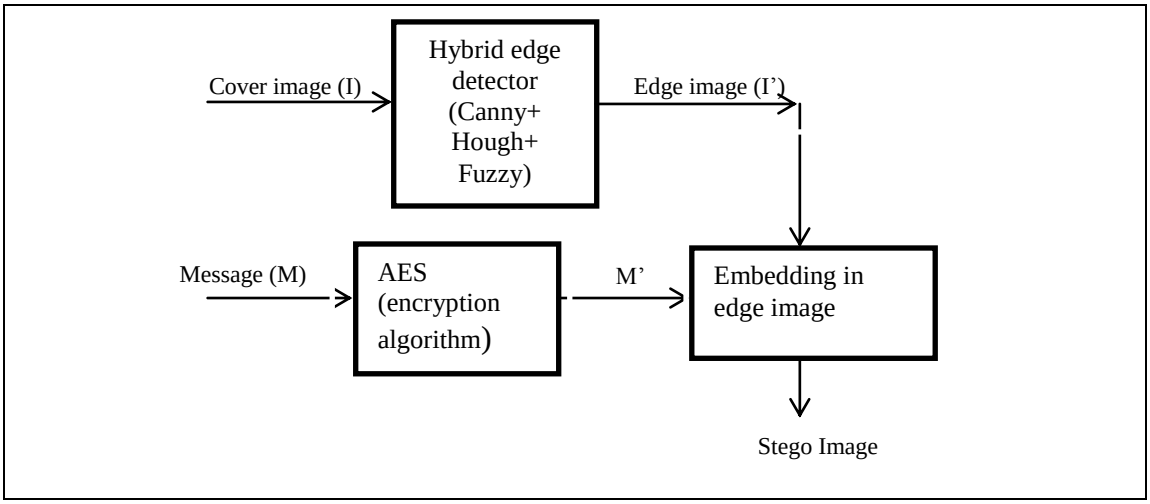

Fig. 2 Proposed Work

Description of the embedding in edge image is given in figure 3.

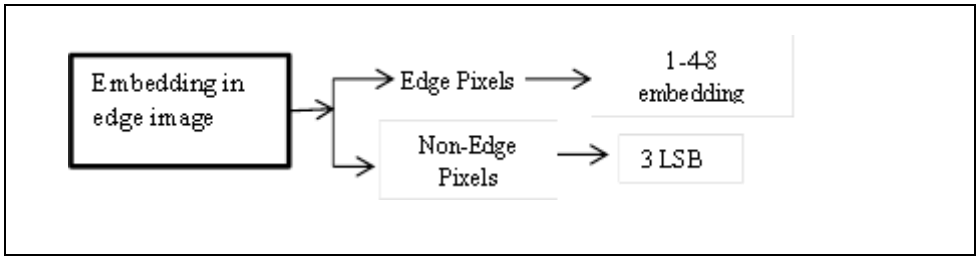

Fig. 3 Embedding in Image

In the above figure edge pixels use 1-4-8 embedding where as non-edge pixels are using 3 LSB embedding. In 1-4-8 embedding 1 LSB of red channel, 4 LSBs of green channel and 8 LSBs of blue channel are used to hide the message bits. In 3 LSB embedding only 3 LSBs of blue channel are used to hide the message bits.

IV. CONCLUSIONS

Steganography is an important field of information security and digital image processing. Various steganography techniques introduced to provide high Imperceptibility, robustness and capacity. Initially LSB substitution technique was explored. But this technique was more prone to statistical attacks. According to HVS, human eye can recognize changes in continuous areas more easily than in non-continuous areas. On the basis of this image steganography techniques started using the features of image to hide data bits. In this paper, a new technique for RGB images is proposed which is based on previously mentioned algorithms. This technique uses optimal edge detectors to find the edge areas and smooth areas. More bits of edge pixels are used for embedding the message bits than bits of smooth area pixels.

In future implementation of the proposed method will be done on some simulator. Comparison of the proposed method with existing methods will be done.

REFERENCES

[1] Artz, D., ―Digital Steganography: Hiding Data within Data, IEEE Internet Computing Journal,vol. 5(3), pp. 75-80,2001.

[2] Anderson R. J., ―Stretching the Limits of Steganography,Springer Lecture Notes in Computer Science, vol.1174,pp. 39–48, 1996 .

[3] Westfeld A, J. Camenisch et al., "Steganography for Radio Amateurs— A DSSS Based Approach for Slow Scan Television", Springer-Verlag Berlin Heidelberg, pp. 201-215, 2007.

[4] M. Hossain, S.A. Haque, F. Sharmin, "Variable Rate Steganography in Gray Scale Digital Images Using Neighborhood Pixel Information," Proceedings of 2009 12th International Conference on Computer and Information Technology, pp. 21-23, 2009.

[5] A. Shaddad, J. Condell, K. Curran, and P. Mckevtt., "Biometric inspired digital image steganography," Proceedings of 2008 15th Annual IEEE International Conference and Workshop on the Engineering of Computer Based Systems, pp. 159-168, 2008.

[6] Thien, C. C., Lin, J. C., "A Simple and High-Hiding Capacity Method for Hiding Digit-By-Digit Data in Images Based On Modulus Function," Pattern Recognition, vol. 36, pp. 2875-2881, 2003.

[7] S. Dumitrescu, X. Wu, and Z. Wang, "Detection of LSB Steganography via Sample Pair Analysis", Proceedings of 2003 IEEE Transaction on Signal, vol.51, 2003.

[8] T. Zhang and X. Ping, "Reliable detection of LSB steganography based on the difference histogram", Proceedings of 2003 IEEE, vol. 3, pp. 545-548, 2003.

[9] L. Zhi, S. A. Fen and Y. Y. Xian,"A LSB steganography detection algorithm", Proceedings of 2003 IEEE ISPIMRC, pp. 2780-2783, 2003.

[10] Maroney, C. Hide and Seek 5 for Windows 95, computer software and documentation, originally released in Finland and the UK.

[11] Katzenbeisser. S,Fabien, Petitcolas. A.P., "Information hiding techniques for steganography and digital watermarking*"*,Artech House, Norwood, MA 02062, USA, 1999.

[12] Kathryn Hempstalk, "Hiding Behind Corners: Using Edges in Images for Better Steganography", Proceedings of the Computing Women's Congress, 2006.

[13] R. Chandramouli, N.D. Memon and G. Li, "Adaptive Steganography," Proceedings on Security and Watermarking of Multimedia Contents III, Special session on Steganalysis, SPIE Photonics West, pp. 69-78, 2002.

[14] Karen Bailey, Kevin Curran and Joan Condell, "An Evaluation of Pixel based Steganography and Stego detection Methods," The Imaging Science Journal, vol. 52, pp. 131 - 150, 2004.

[15] Elke Franz and Antje Schneidewind, "Adaptive Steganography Based on Dithering," Proceedings Of the 2004 workshop on multimedia and security, ACM, Magdeburg, Germany, 2004.

[16] M. M. Amin, M. Salleh, S. Ibrahim, M. R. K.Atmin and M. Z. I. Shamsuddin, "Information Hiding using Steganography," 4th national Conference on Telecommunication Technology, NCTT 2003, IEEE, pp. 21 – 25, 2003

[17] Santosh Arjun, N. and Atul Negi, "A Filtering Based Approach to Adaptive Steganography," 10th Conference, TENCON 2006, IEEE, pp. 1-4, 2006.

[18] Manglem Singh, Birendra Singh and Shyam Sundar Singh, "Hiding Encrypted Message in the Features of Images," IJCSNS, vol. 7, 2007.

[19] H. C. Wu, N. I. Wu, C. S. Tsai, and M. S. Hwang, "Image steganographic scheme based on pixel-value differencing and LSB replacement methods," Proceedings of 2005 Instrument Electric Engineering, Vis. Images Signal Process, vol. 152, pp. 611–615, 2005.

[20] Cheng-Hsing Yang, Chi-Yao Weng, Shiuh-Jeng Wang, Hung-Min 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.

[21] D. C. Wu and W. H. Tsai, "A Steganographic method for images using pixel value differencing," Pattern Recognition Letters, vol. 24, pp. 1613-1626, 2003.

[22] Hossain, M. Al Haque and S. Sharmin, F., "Variable rate Steganography in gray scale digital images using neighborhood pixel," 12th International Conference Dhaka, Information Computers and Information Technology, ICCIT '09, 2009.

[23] J. Canny, "A Computatinal Approach to Edge Detection," IEEE Tranaction on Pattern Analysis and Machine Intelligence, vol. 8, pp. 679-687, 1986.

[24] Wen-Jan Chen a, Chin-Chen Chang, T. Hoang Ngan Le, "High payload steganography mechanism using hybrid edge detector," Expert Systems with Applications, vol. 37, pp. 3292–3301, 2010.

[25] Hussain, M. and Hussain, "Embedding data in edge boundaries with high PSNR," Proceedings of 7th International Conference on Emerging Technologies (ICET 2011), pp.1-6, 2011.

[26] Youssef Bassil, "Image Steganography Based on a Parameterized Canny Edge Detection Algorithm," International Journal of Computer Applications (0975 – 8887), vol. 60, 2012.

[27] Specification for the Advanced Encryption Standard (AES), Federal Information Processing Standards Publication 197, 2001.

[28] Mamta Juneja and Parvinder S. Sandhu, "A New Approach for Information Security using an Improved Steganography Technique," J Inf Process Syst, vol. 9, 2013.

