The Image Steganography Techniques to Improve the Security and the Stego Image Quality

R. K. Nithya
II M.E., Computer Science and Engineering, Vivekanandha College of Engineering for Women, Namakkal, India

Dr. J. Jennifer Ranjani
Associate Professor, Computer Science and Engineering, Vivekanandha College of Engineering for Women, Namakkal, India

T.Thenmozhi
Assistant Professor, Computer Science and Engineering, Vivekanandha College of Engineering for Women, Namakkal, India

Abstract - Steganography is the method of hiding a secret information in a specified medium like image, video, Audio. It can be used to carry out hidden exchanges of information and to provide privacy for the user. This can be achieved by taking any multimedia as a carrier. The secret information should be embedded in the carrier medium in such a way that the attackers could not be able to find the existence of it. The security of the secret data and stego image quality should be maintained in both the embedding and recovering process. In this paper, algorithms under reversible Steganography and Least Significant Bit mechanism are discussed. These algorithm aims to achieve more security and to improve the stego image quality.

Keywords: PSNR, Reversible Data Hiding, DCT coefficient, Inpainting Algorithm, PVD

I. INTRODUCTION

Steganography means "Covered Writing" which is derived from the Greek language. The main purpose of steganography is to send secret or confidential message under the cover of a carrier signal. Two main properties of any steganographic technique are good imperceptibility and sufficient data capacity. Good imperceptibility ensures that the embedded message is difficult to detect. Steganography and cryptography are mainly used for security, but both are different. The main goal of cryptography is to communicate securely by changing the data into a form that an attacker cannot understand. The steganography techniques are used to hide the presence of the message and make it difficult for attackers to find the occurrence of the message. The research on steganography concentrates on images, audio, and video as cover media [1]-[4]. An image in which data is embedded is called as a cover image and the image which is used for carrying secret data is termed as stego image. A good data hiding method should be capable of evading visual and statistical detection while providing an adjustable payload. Impossibilities of data hiding is commonly achieved by exploiting the weakness of the human auditory and visual systems, using the techniques, for example changing the least-significant bits of pixels of cover image to embed information[5], or shifting lines, words, or characters by a small amount in an image containing text[6]. Other works hide information by adding redundant data, or making use of alternative representations of electronic data. For example hidden information can be added in a text document by adding tabs and spaces at the end of the line. The different combinations of the color palette entries in a GIF image can be used to embed secret data into the image file. Sometimes the cover media will experience some distortion due to data hiding and cannot be inverted back to the original media. That is, after the hidden data have been extracted out some permanent distortion has been occurred to the cover media. Reversible Steganography scheme has the ability to embed the secret data into a host image and

then recover the host image without losing any information when the secret data is extracted. This should be overcome by using some techniques. Reversible steganography is also known as reversible data hiding. No modification is done in the digital representation of the cover image when reversible data hiding method is used. The Reversible data hiding is used in the field of medical, military, legal applications etc.

II. SURVEY

In this section different techniques for Reversible steganography and LSB Matching for data hiding are discussed.

A. Reversible Steganography

Reversible Steganography scheme has the ability to embed the secret data into a host image and then recover the host image without losing any information when the secret data is extracted. No modification is done in the digital representation of the cover image when reversible data hiding method is used. Some of the techniques used are Reversible data hiding [7], Sequential recovery and Multilevel Histogram modification [8], Steganographic techniques for JPEGs [9], Reference pixel distribution and Interpolation mechanism [10].

(i) Reversible Data Hiding :

A novel reversible data hiding algorithm [11], once when the hidden data have been extracted the original image is recover without any distortion from the marked image. To embed data into the image, the zero or the minimum points of the histogram of an image is utilized in this algorithm by modifying the pixel grey scale values. The original image with the peak signal-to-noise ratio (PSNR) of marked image constructed by this method is above 48 dB. The computational complexity of this is low and execution time is short.

(ii) Sequential recovery and Multilevel histogram modification :

This reversible data hiding technique is mainly used for natural images. The most differences between pairs of adjacent pixels are equal or close to zero because of the similarity of neighbor pixels values. Based on these difference statistics, the histogram is constructed. Multilevel histogram modification mechanism is used in the data embedding stage. Based on one or two level histogram modification [12], the hiding capacity is enhanced as more peak points are used for secret bits modulation. The distortions on the host image made by secret content embedding is reduced as the differences of having common center around zero is improved. Instead of the peak points and zero points, the embedding level is used in the data extraction and image recovery stage.

(iii) Steganographic techniques for JPEGs :

The detection is done by decompressing the JPEG [14] stego image, geometrically distorting and recompression. The quantized structure of DCT coefficients is modified due to the geometrical distortion during the recompression. The distorted images have many macroscopic statics nearly equal to those of the cover image. The macroscopic statics S that changes with the embedded message length is chosen. By comparing the values of S for stego image and the cropped/recompressed stego image, the unknown message length is estimated. This detection methodology can be done by the F5 algorithm and Outguess.

(iv) Reference Pixel Distribution and Interpolation mechanism:

To obtain the interpolation errors, an image interpolation algorithm [10] was used instead of the nearest neighbor interpolation techniques. Select the reference pixels in the cover image. Pixels other than the reference pixels are interpolated. By subtracting the interpolated pixels from the original image Interpolation errors are calculated. By modifying the interpolation errors the data bits are kept secret , since the reference pixels value were not changed in the embedding process. The same is done in decoding process to extract the embedded data bits. The number of reference pixels in the smooth regions is reduced and the number of reference pixels in the complex

regions is increased in this method. The number of reference pixels affects the payload and the stego image quality in many cases. Interpolation Techniques is less secure against image manipulations and steganalysis due to the presence of LSB replacement style asymmetry.

(v) Texture Image Inpainting and Simultaneous Structure :

Initially decompose the image into the sum of two functions with different basic characteristics. With structure and texture filling-in algorithms reconstruct each one of these functions. To represent the underlying image structure, the first function is used in decomposing of bounded variation. The texture and possible noise is captured by using second function. Using image inpainting algorithms, the region of missing information in the bounded variation image is reconstructed. Using texture synthesis techniques [14] the same region is filled-in. by adding these two sub-images the original images is reconstructed.

B. Least Significant Bit Mechanisms

Some of the techniques are Spatial LSB Domain Systems based on Adaptive Data Hiding in Edge Areas of Images (AE-LSB) [15], Modulus Function and Pixel Value Differencing, Adaptive Steganographic Schemes for Digital Images, Palette-Based Image Steganography, LSB Matching - Edge Adaptive Image Steganography.

(i) Spatial LSB Domain Systems based on Adaptive Data Hiding in Edge Areas of Images (AE-LSB) :

Here a new adaptive least-significant bit (LSB) steganographic method based on pixel-value differencing (PVD) [15] was proposed. The difference value of two consecutive pixels estimates how many secret bits to be embedded into the two pixels. Pixels located in the edge areas were embedded with more secret bits than that located in smooth areas. The range of difference values were adaptively divided into lower level, middle level, and higher level. The readjusting phase ensures that the two consecutive pixels belong to the same level both before and after embedding. The range [0, 255] of difference values was divided into different levels. For extracting data exactly, the difference values before and after embedding must belong to the same level. This scheme provides more capacity and better quality than the PVD and was an improved version of PVD. The main disadvantage with this scheme was that it was less tolerant to steganalysis.

(ii) *Modulus Function and Pixel Value Differencing* :

High Quality Steganographic method with PVD and Modulus function was an extension of PVD based approach. This technique first calculates the difference value between two consecutive pixels and then modulus operation was used to calculate their remainder. The secret data were embedded into the two pixels by modifying their remainder. The hiding capacity of the two consecutive pixels depends upon the difference value taken. Lesser the difference value smoother the area, so only less secret data could be embedded and vice versa. The strength of the scheme was that it could greatly reduce the visibility of the hidden data than the PVD [15] method. Since the scheme used the remainder of the two consecutive pixels it was more flexible. However, a loophole exists in the PVD method. Unusual steps in the histogram of pixel differences reveal the presence of a secret message. The modified pixels will be spread around the whole stego image and many smooth regions gets contaminated.

(iii) Adaptive Steganographic Schemes for Digital Images:

This is a practical method for optimizing the parameters of additive distortion functions to minimize statistical detectability. By defining a rich parametric model which assigns a cost of making a change at every cover element based on its neighborhood, apply the framework to digital images in both spatial and DCT domain. With respect to a chosen detection metric and feature space, a practical method is used for optimizing the parameters. The size of the margin between sup-port vectors in soft-margin SVMs lead to a fast detection metrics. The Nelder-Mead simplex-reflection algorithm is used for spatial and DCT-domain images.

(iv) Palette-Based Image Steganography:

To minimize the RMS error between an original image and its stego-image, palette-based image steganography [16] is used. This method is used to embed one message bit into each pixel in a palette-based image. The cost of removing an entry color in a palette and the benefit of generating a new one to replace it is calculated in each iteration. An Entry color is replaced when the maximal benefit exceeds the minimal cost. This reduces the distortion of the carrier images to other palette-based methods.

(v) LSB Matching - Edge Adaptive Image Steganography:

The least significant bit (LSB) based steganography is the most common type of steganographic approach. In most existing approaches, the choice of data hiding positions within the input cover image mainly depends on a pseudo random number generator (PRNG). Here the relationship between the image content and the size of the secret message to be embedded is not considered. Thus the smoother regions in the cover images will get modified after data hiding even at a low embedding rate which will lead to low quality images. Such images could be easily identified by steganalysis. In LSB Matching Revisited (LSBMR) [17] one can select the regions to embed data based on a threshold value. The threshold value will be calculated based on the size of secret message and the difference between two adjacent pixels in the cover image. For lower embedding rates, sharper edge regions are used while smoother regions are not modified. The sharper regions in the image will be less contaminated by data hiding. As the embedding rate increases, by adjusting the parameters more edge regions can be adaptively released. The new scheme generates the output image without any distortions. LSBMR can enhance the security significantly compared with typical LSB-based approaches as well as their edge adaptive ones. The technique preserves the statistical and visual features of the cover image and ensures higher visual quality of stego images.

III. CONCLUSION

From the above analysis of Reversible steganography and Least Significant Bit Mechanism the following are analyzed. PVD with modulus function provide lesser distortion to the stego image than the other PVD methods. Texture image inpainting produces the stego image with better quality. In multilevel histogram modification embedding level is used instead of peak point and zero point. By using interpolation mechanism payload and stego image quality is improved. By considering the PSNR value the stego image quality can be maintained. Adaptive data hiding provides the higher capacity of information hiding. Modulus function will embed the data in more secure manner. Loss of data is reduced using this.

REFERENCES

[1] W. Bender, D. Gruhl, N. Morimoto, and A. Lu, “Techniques for data hiding,” IBM Syst.J., vol. 35, no. 3-4, pp. 313-336,1996.

[2] F. A. P. Petitcolas, R. J. Anderson, and M. G. Kuhn, “Information hiding-A survey’” Proc.IEEE, vol.87, no. 7, pp.1062-1078, Jul. 1999.

[3] N. F. Johnson, Z. Duric, and S. Jajodia, Information Hiding: Steganography and Watermarking – Attacks and Contermeacures. Norwell, MA: Kluwer, 2001.

[4] R. Chandramouli, M. Kharrazi, and N. Memon,” Image Steganography and Steganalysis concepts and practice, “Digital Watermarking Lecture Notes in Computer Science 2939, pp. 35-49, 2004.

[5] D. C. Wu and W. H. Tsai, “ A Steganographic method for images by pixel-value differencing,” Pattern Recognit.Lett., vol. 87, no.9-10,pp-1613-1626, 2003.

[6] J. T. Brassil and N. F. Maxemchuk, “Copyright protection for the electronic distribution of text Documents,” proc.IEEE, vol. 87, no.7, pp.1181-1196. 1999.

[7] Zhicheng Ni, Yun-Qing Shi, Nirwan Ansari, and Wei Su “Reversible Data Hiding”, IEEE Transactions on circuits and systems for video technology, vol. 16, no. 3, march 2006.

[8] Zhenfei Zhao, Hao Luo, Zhe-Ming Lu, Jeng-Shyang Pan “Reversible data hiding based on multilevel histogram modification and sequential recovery”, International Journal of Electronics and Communications (AEÜ) 65 (2011) 814– 826.

[9] Jessica Fridrich, Miroslav Goljan, Dorin Hogea “Methodology for breaking steganographic techniques for JPEGs”, Electronic Imaging, Security, Steganography, and Watermarking of Multimedia Contents V, Santa Clara, California, pp. 143-155, 2003.

[10] Wien Hong, Tung-Shou Chen, “Reversible data embedding for high quality images using interpolation and pixel distribution mechanism” , www.elsevier.com , J.Vis Commun. Image R.22(2011) 131-140

[11] Hong Zhao, Hongxia Wang, Muhammad Khurram Khan," Statistical analysis of several reversible data hiding algorithms", Multimedia Tools and Applications, April 2011, Volume 52, Issue 2-3, pp 277-290.
[12] Thomas Filler and Jessica Fridrich "Design of adaptive steganographic schemes for digital images", Proc. SPIE, Electronic Imaging, Media Watermarking, Security, and Forensics XIII, vol. 7880, San Francisco, CA, January 23–26, pp. OF 1–14, 2011.
[13] Zhang, W,; Ma, K,; Yu, "Reversibility improved data hiding in encrypted images," N.Signal Processing vol.94 January, 2014, p. 118-127.
[14] Marcelo Bertalmio, Luminita Vese, Guillermo Sapiro, member, IEEE, and Stanley Osher "Simultaneous Structure and Texture Image Inpainting", IEEE transactions on Image Processing, vol. 12, no. 8, August 2003.
[15] Matus Jokay and Tomas Moravick, "Image-Based LPEG Steganography", Tatra Mt. Math. Publ. 45(2010), 65-74.
[16] Mei-Yi Wu, Yu-Kun Ho, Jia-Hong Lee, "An iterative methods of palette-based image Steganography", www.elsevier.com, Pattern Recognition Letters 25 (2004) 301-309.
[17] J.Mielikainen, "LSB matching revisited," IEEE Signal Process. Lett, vol.13, no.5, pp.285-287, May 2006.
[18] M. Sabha, P.Peers and P. Dutre, " Texture Synthesis using Exact Neighborhood Matching," Volume 26(2007), number 2 pp. 131-142.
[19] D.Wu and W.Tsai, " A steganographic method for images by pixel value differencing," Pattern Recognit Lett, vol 24, pp. 1613-1626, 2003.