Literature Survey On Modern Image Steganographic Techniques

Priya Thomas
Department of Computer Science and Engineering
Nehru College of Engineering and Research Center, Kerala, India.

Abstract

Steganography is the method of storing information by hiding that information's existence. It can be used to carry out hidden exchanges and hence can enhance individual privacy. Steganography aims at communicating the secret data in an appropriate multimedia carrier. In this paper I have made an analysis of modern steganographic algorithms. Based on certain design criteria's such as security against RS steganalysis, invisibility, payload capacity, robustness against attacks, embedding scheme etc, different algorithms have been evaluated. This analysis explores the strengths and weaknesses of the modern image steganographic techniques which will enable us to design a better steganographic algorithm.

Key words - Image steganography, Hiding Behind Corners (HBC), Pixel-Value Differencing (PVD), steganalysis, statistical attacks.

1. Introduction

Steganography means "covered writing" which is derived from the Greek language. The main purpose of steganography is to send secret or confidential messages under the cover of a carrier signal. It is generally accepted that any steganographic technique must possess two main properties: good imperceptibility and sufficient data capacity. The first property ensures that the embedded messages are difficult to detect, and the second implies efficiency in hidden communication. Steganography and cryptography aims at security, but both are different. The goal of cryptography is to communicate securely by changing the data into a form that an eavesdropper cannot understand. Steganography techniques, on the other hand, tend to hide the presence of the message and make it difficult for an observer to figure out the possibility of occurrence of the message.

The rest of the paper is organized as follows: Section 2 gives a literature review on certain modern steganographic schemes highlighting its strengths and weaknesses. Section 3 compares the different schemes based on certain design criteria's. Finally concluding remarks are given.

2. Literature Review

In this section, we first give description of the typical LSB-based approaches including LSB in GIF [1], LSB replacement [6], EA-LSBMR [3], and some adaptive schemes including PVD with modulus function[10], difference expansion technique [2], hiding in edges [7], adaptive edges with LSB (AE-LSB) [11], hiding behind corners (HBC) [1] etc.

2.1. LSB in GIF [1]

Palette based images, such as GIF images, are popular image file format commonly used on the Internet. GIF images are indexed images where the colours used in the image are stored in a palette or a colour lookup table. GIF images can also be used for LSB steganography [5], although extra care should be taken. The main issue with the palette based approach is that if one changes the least significant bit of a pixel, it could result in an entirely different colour since the index to the colour palette gets modified. One possible solution to this problem is to sort the palette so that the colour differences between consecutive colours are minimized. The strong and weak points regarding embedding information in GIF images using LSB is that since GIF images only had a bit depth of 8, the total amount of information that could be embedded will be less. GIF images are vulnerable to statistical as well as visual attacks, since the palette processing which has to be done on the GIF image leaves a clear signature on the image. This approach was dependent

on the file format as well as the image itself, since a wrong choice of image could results in the message being visible.

2.2. Steganographic Method based on Difference Expansion Technique [2]

Difference Expansion (DE) is a simple and efficient reversible data-embedding method [8] used for digital images. Here the redundancy in the digital content is explored to achieve reversibility. In this method, one bit can be embedded into two consecutive pixels. So the maximum embedding capacity will be 0.5 bpp. The main advantage of this technique was that it discovers extra storage space by exploring the redundancy in the image content. Both the payload capacity limit as well as the visual quality of embedded images of the DE [2] method are the best along with a low computational complexity. The difference expansion technique was later generalized so that n -1 bits can be embedded into n pixels, resulting the maximum embedding capacity (n -1)/n bpp. However, the difference expansion based reversible data hiding methods could not gain much popularity as the method double the differences between pixels in successive iteration. The distortions were larger and hence DE was vulnerable to statistical attacks. DE based technique had low payload capacity. The technique could not be used for applications demanding high visual quality.

2.3. Hiding Behind Corners [3]

Certain digital techniques do not take into account the cover's original information thereby they leave certain marks on the stego image. In Hiding Behind Corners (HBC), this was avoided by taking the cover's original information. Two algorithms were used in HBC based on using image filters to determine the effective hiding places in an image. They were FilterFirst and BattleSteg. The strength of FilterFirst was that it eliminates the need to provide any additional information such as original image. It was also very effective in hiding information. Whereas the weakness of FilterFirst was that it was not secure, as an attacker can repeat the filtering process. It could be also much easier to retrieve the hidden information once the stego-image is identified. The strength of BattleSteg was that it requires a password to retrieve the message. Its weakness includes the absence of a random seed so it was impossible to know where to place the shots and also it was possible for BattleSteg to never have a hit. Hiding Behind Corners approach effectively utilizes edge areas but embedding capacity is less.

2.4. Hiding Secret Message in Edges of the Image (RELSB) [4]

Hiding Secret Message in Edges of the image introduced a new least significant bit embedding algorithm for hiding secret messages in non-adjacent pixel locations at the edges of images. Here the messages were hidden in regions which were least like their neighbouring pixels i.e. regions that contain edges, corners, thin lines etc so that an attacker will have less suspicion of the presence of message bits in edges, because pixels in edges of an image appears to be much brighter or dimmer than their neighbours. Edges can be detected by edge detection filters such as a 3x3 window Laplacian edge detector [5]. One common disadvantage of LSB embedding [6] was that it created an imbalance between the neighbouring pixels. Here this imbalance was avoided by flipping the gray-scale values among 2i-1, 2i and 2i+1. The various strengths of this scheme were that an attacker will have less suspicion to the presence of message bits in edges because pixels in edges appear to be either much brighter or dimmer than their neighbours and it was also secure against blind steganalysis. It also limits the length of the secret message to be embedded. The main disadvantage with this scheme was that the embedding capacity was relatively low. It could not make full use of edges during embedding.

2.5. Adaptive Data Hiding in Edge Areas of Images with Spatial LSB Domain Systems (AE-LSB) [7]

Here a new adaptive least-significant bit (LSB) steganographic method based on pixel-value differencing (PVD) [8] was proposed. The difference value of two consecutive pixels [9] 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 [6] and was an improved version of PVD. The main disadvantage with this scheme was that it was less tolerant to steganalysis.

2.6. Steganographic Method based on Pixel Value Differencing and Modulus Function [10]

High Quality Steganographic method with PVD and Modulus function was an extension of PVD [8] 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 [8] method. Since the scheme used the remainder of the two consecutive pixels it was more flexible. However, a loophole exists in the PVD [8] 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.

2.7. Data hiding method based on interpolation technique [11]

Reversible data hiding method based on Interpolation Technique (IT) concealed data into interpolation errors. Instead of using the nearest neighbour interpolation technique, an image interpolation algorithm was used to obtain the interpolation errors. The reference pixels are adaptively selected in the cover image and pixels other than the reference pixels are interpolated. Interpolation errors are obtained by subtracting the interpolated pixels from the original image. Data bits were concealed by modifying the interpolation errors. Because reference pixel values were not changed in the embedding process, the same set of interpolated pixels could be obtained in the decoding process and thus, the embedded data bits could be extracted and the original image was restored. In this technique, they reduced the number of reference pixels in smooth regions and increased the number of reference pixels in complex regions. But the distortions in the output image were much higher in histogram shifting method [12]. However, in most cases, the number of reference pixels affects the payload and the stego image quality. Interpolation Technique is less secure against image manipulations and steganalysis due to the presence of LSB replacement style asymmetry.

2.8. Edge Adaptive Image Steganography based on LSB Matching (EA-LSBMR) [13]

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 steganalysts. In LSB Matching Revisited (LSBMR) [14] 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.

3. Comparison of Steganographic Techniques

Algorithms for image steganography will have different advantages and disadvantages. It is important to ensure that one uses the most suitable algorithm for an application. All steganographic algorithms have to satisfy few basic requirements. The most important requirement of any steganographic algorithm is that it has to be imperceptible. Many steganographic algorithms leave a ‘signature’ when embedding information that can be easily detected through statistical analysis. A strong steganographic algorithm should not leave any such visible mark in the image and should be secure against all type of image manipulations. The table below compares different steganographic techniques discussed so far based upon various properties including payload capacity, security against steganalysis [5], robustness against statistical attacks, LSB replacement style asymmetry [14] etc. Based on the analysis concluding remarks are given.

Table 1. Comparison of Steganographic Techniques

Method / Aspects	LSB in GIF [1]	DE [2]	HBC [3]	RE-LSB [4]	AE-LSB [7]	PVD [10]	IT [11]	EA-LSBMR [13]
Invisibility	Low	Low	High	High	High	Low	Medium	High
Payload Capacity	High	Low	Low	Low	High	High	Medium	High
Robustness against statistical attacks	High	High	Low	Medium	High	Low	High	High
Tolerance to RS Steganalysis	Low	Low	Low	High	Low	High	Medium	High
Robustness against image manipulation	Low	High	Low	Medium	High	High	Low	High
LSB replacement style asymmetry	Yes	Yes	Yes	Yes	Yes	No	Yes	No
Utilization of edge areas	Low	Low	High	Medium	Low	Low	Medium	High

From the discussions above we get to know that LSB in GIF [1] images have high payload capacity but is vulnerable to steganalysis. DE [2] based approach is secure against image manipulation [5] but has lesser payload capacity. HBC [3] embeds the secret bits into edge regions as far as possible while keeping the smooth regions as they are, but it is vulnerable to RS steganalysis. RELSB [4] performs data hiding on the center pixels by detecting the edges in the image and is also secure against blind steganalysis. The disadvantage with this scheme is that payload capacity is relatively low. AE-LSB [7] provides better capacity but is vulnerable to attack by RS steganalysis. The average modification rate of the pixels is the least i.e. the average payload capacity of each single pixel is the largest among the other schemes, so only fewer pixels need to be modified at the same embedding rate. But here the less smooth regions would get contaminated due to its lesser modification rate. PVD with modulus function [10] reduces the visibility of the hidden data in an efficient manner and it is also secure against RS steganalysis. Interpolation Technique [11] based approach is secured against statistical attacks but it is highly vulnerable to image manipulation [5]. EA-LSBMR [13] utilizes the edge areas fully so is both visually and statistically invisible. It is also secure against RS steganalysis. From the above analysis done in TABLE 1 we can arrive at the conclusion that EA-LSBMR [13] is secure against all type of attacks. HBC [3] and EA-LSBMR [13] utilizes the edge areas fully. But HBC [3] is vulnerable to RS steganalysis as LSB replacement style asymmetry is present in it. EA-LSBMR [13] provides high payload capacity and is highly secure.

4. Conclusion

From the above analysis we have seen that HBC [1] even though utilizes the edge areas fully is not secure against statistical attacks and RS steganalysis. PVD [10] with modulus function provides lesser distortion to the stego image than the other PVD methods but doesn't utilize the edge areas fully so is more visually visible than EA-LSBMR [3]. AE-LSB [6] provides higher capacity but this can lead to contamination of the less smooth areas. EA-LSBMR [3] is both visually and statistically invisible and is secure against image manipulations. It has high payload capacity and it utilizes the edge areas fully compared with the other methods. The research in the field of steganography is an ongoing process. By analysing

the recent trends in the field of image processing new steganographic algorithms could be developed. By such analysis we can arrive at a perfect steganographic algorithm in the coming future.

References

[1]. W. Bender, D. Gruhl, N. Morimoto, & A.Lu, "Techniques for data hiding", *IBM Systems Journal*, 35, PP 210-224, 2002

[2]. J. Tian, "Reversible data embedding using a difference expansion." **IEEE** *Transactions on Circuits and Systems for Video Technology*, 13, 8, PP 890–896, 2003.

[3]. K. Hempstalk, "Hiding behind corners: Using edges in images for better steganography," *Proceedings of the IEEE*, Hamilton, New Zealand, 2006.

[4]. K. M. Singh, L. S. Singh, A. B. Singh, and K. S. Devi, "Hiding secret message in edges of the image," *Proceedings of International Conference on Information and Communication Technology,* PP 238–241, 2007.

[5]. J. Fridrich, M. Goljan, and R. Du, "Detecting LSB steganography in color, and gray-scale images," *IEEE Multimedia*, vol. 8, no. 4, pp. 22–28, Oct. 2001.

[6]. Z. Ni, Y.Q. Shi, N. Ansari, W. Su, "Reversible data hiding" , *IEEE Transactions on Circuits and Systems for Video Technology* , 16 , 3 ,PP 354–362,2006.

[7]. C. H. Yang, C. Y. Weng, S. J. Wang, and H. M. Sun. "Adaptive data hiding in edge areas of images with spatial LSB domain systems," *IEEE Transactions on Information Forensics Security*, 3, 3, PP 488–497, 2008.

[8]. D. Wu and W. Tsai, "A steganographic method for images by pixel value differencing," *Pattern Recognit. Lett.*, vol. 24, pp. 1613–1626, 2003

[9]. X. Li, T. Zeng, and B. Yang, "Detecting LSB matching by applying calibration technique for difference image," in *Proc. 10th ACM Workshop on Multimedia and Security*, Oxford, U.K, pp. 133–138, 2008.

[10]. Chung-Ming Wang, Nan-I Wu, Chwei-Shyong Tsai, Min-Shiang Hwang, " High quality steganographic method with pixel-value differencing and modulus function," *Science Direct The Journal of Systems and Software*, 2007.

[11]. L. Luo, Z. Chen, M. Chen, X. Zeng, Z. Xiong, "Reversible image watermarking using interpolation technique," *IEEE Transactions on Information Forensics and Security* , 5 ,1, PP 187–193, 2010

[12]. L.M. Marvel, C.G. Boncelet , & C. Retter, "Spread Spectrum Steganography", *IEEE Transactions on image processing*, 8,8, PP 160-178, 2007.

[13]. Weiqi Luo, Fangjun Huang, and Jiwu Huang, "Edge adaptive image steganography based on LSB matching revisited," in *IEEE Transactions on Information Forensics and Security*, vol.5, no.2, June 2010..

[14]. J. Mielikainen, "LSB matching revisited," *IEEE Signal Process. Lett.*, vol. 13, no. 5, pp. 285–287, May 2006.

[15]. D. Artz, "Digital Steganography: Hiding Data within Data", *IEEE Internet Computing Journal***,** 4, 2, PP 127-135, 2001.