International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2013): 4.438

A Survey and Analysis on Adaptive and Non-adaptive Methods of Steganography

Palak V. Keshwani[1] , Rakesh K. Khare[2]

[1]M.Tech Scholar , Computer Science & Engineering, RIT Raipur, CSVTU Bhilai, India
palakeshwani@gmail.com

[2]Associate Prof. & Head (IT), RIT Raipur, CSVTU Bhilai, India
rakesh_khare2001@yahoo.com

Abstract: ***Steganography means secret communication. It can also be defined as the study of invisible communication that is used to hide the existence of the communicated data in such a way that it remains confidential. In steganography, secret data can be communicated in an appropriate multimedia carrier such as image, audio and video files. Steganography can be classified into two types- Adaptive steganography and Non-adaptive steganography. Each has its strengths and weaknesses. In this paper, we review some adaptive and non-adaptive methods of steganography.***

Keywords: Steganography, Adaptive steganography, Non-adaptive steganography, LSB, PVD, DWT, PSNR.

1. Introduction

The word steganography is derived from the Greek words “stegos” means “cover” and “grafia ”means “writing” defining it as “covered writing”. Steganography is the method through which existence of the secret message can be kept secret. This is achieved by hiding secret message behind another media such as image, audio and video. In image steganography, the message is hidden behind an image. The image into which a message is hidden is called a cover image and the result is stego-image. Two important properties that should be considered while designing a steganographic algorithm are undetectability and embedding capacity. The stego-image must be undetectable and it should embed more data. Steganography has various applications. It can be used in military, commercial and anti-criminal applications, transmission of confidential documents between international governments, e-commerce, media, database systems, digital watermarking etc.

2. Literature Review

In the past, several work has been done on steganography. A very well-known steganographic method is the Least Significant Bit (LSB) substitution method. It embeds secret data by replacing x LSBs of a pixel with x secret bits directly [1]. To minimize the image distortion, Chan–Cheng proposed a simple LSB algorithm based on optimal pixel adjustment [2] in 2004.Zhang and Wang proposed an algorithm [3] which is represented in (2n + 1)-ary notation system. In this scheme, only one pixel of n pixels into one group is increased or decreased by 1. In 2006, Jarno Mielikainen [4] proposed LSB matching algorithm for embedding secret message. Zhang and Wang’s scheme and Mielikainen’s schemes [3,4] had the limited capacity for embedding.

The level of security in LSB-based methods is poor because they just modify the LSB of the image pixels. Various steganalysis algorithms e.g. RS detector [5] can be used to detect the secret data easily. Also, all the pixels in the cover image cannot tolerate equal amount of embedding without causing visible distortion. Hence, it can be easily noticed by eavesdropper. To overcome these problems, adaptive methods for embedding have been proposed [6-12].In these methods, amount of embedding data in pixels is variable. These methods gives more imperceptible result than simple LSB and other non-adaptive methods. Adaptive methods calculate hiding capacity of the cover according to its local characteristics[13,14,15,16]. One adaptive method proposed by Wu-Tsai uses the different values between two neighboring pixels to calculate the number of secret bits to be embedded[17]. A novel steganographic method proposed by Wu et al.[18] uses LSB and pixel values differencing(PVD) method. In this algorithm, the pixels located in the edge areas embed the secret data using PVD algorithm and the pixels located in the smooth areas embed using 3-LSB algorithm[18].In 2008, Yang et al. [19] proposed a LSB matching adaptive steganography which uses the different values of two consecutive pixels based on n bit modified LSB method to distinguish between edge and smooth areas. Weiqi et al. in 2010 [20] and Sivaranjani et al. in 2011 [21] have proposed an adaptive image steganography using LSB matching revisited. In these algorithms, edge regions of cover image have changed and the smooth regions remained stable. In 2013 [22],Yu and Wang proposed an adaptive steganography algorithm in the sparse domain. In 2014 [23], Maleki et al. proposed an adaptive and non-adaptive methods for grayscale images based on modulus function. Adaptive method uses average difference value of four neighbor pixels and modulus function. The average difference value of four neighbor pixels and a threshold secret key are used to determine the edge or smooth area. Also, this adaptive method can resist against the RS steganalysis attack. Non-adaptive method provides minimum distortion in the stego-image. The remaining of the paper will be organized as follows. Firstly, we will provide a brief introduction to non-adaptive method using LSB and integer wavelet transform. Then we will describe the adaptive method using LSB and integer wavelet transform. Secondly, we will discuss the results; and finally we will conclude the paper.

3. Methodology

There are two methods for embedding secret data inside any cover media : non-adaptive and adaptive.Here we will review LSB using non-adaptive and adaptive steganography. Then we will review DWT using non-adaptive and adaptive steganography.

3.1 LSB using non-adaptive steganography

LSB replacement embeds a secret message into the cover image by replacing the k LSBs of the cover image with k message bits to arrive at the stego image. In most existing methods, the choice of embedding places inside a cover image depends on a pseudorandom number generator without considering the relationship between the image content itself and the size of the secret message. Hence the smooth regions in the cover images will indisputably be contaminated after hiding data even at a low embedding rate, and this will give poor visual quality and low security, especially for those images with many smooth regions. When taking a 24-bit color image, a bit of each of the three colors - red, green and blue can be used, so a total of 3 bits can be stored in each pixel. For example, the following grid can be considered as 3 pixels of a 24-bit color image, using 9 bytes of memory:

(00101101 00011100 11011100)
(10100110 11000100 00001100)
(11010010 10101101 01100010)

When the number 201, which is represented in binary form as 11001001, is embedded into the least significant bits of this part of the image, the resulting grid is as follows:

(0010110**1** 0001110**1** 1101110**0**)
(1010011**0** 1100010**1** 0000110**0**)
(1101001**0** 1010110**1** 01100010)

Though the number was embedded into the first 8 bytes of the grid, only the 3 underlined bits needed to be changed according to the embedded message. On an average, only half of the bits in an image will need to be changed to hide a secret message. Since, there are 256 possible intensities of each primary color, modifying the LSB of a pixel results in miniature changes in the intensity of the colors. These changes cannot be perceived by the human eye and hence the message is successfully hidden. With a chosen image, one can even hide the message in the least as well as second to least significant bit and still not see the difference. In the above example, successive bytes of the image, from the first byte to the end of the message, are used to embed the information. This method is very simple to detect.

3.2 LSB using adaptive steganography

The least-significant-bit (LSB)-based scheme is a very common steganographic algorithms in the spatial domain but this scheme will lead to poor visual quality and low security based on various analysis and experiments particularly for those images with many smooth regions. Here we briefly describe the LSB matching revisited based on adaptive steganography. In 2010 Weiqi Luo et al. [20] proposed an edge adaptive scheme which select the regions for embedding according to the size of secret message and the difference between two successive pixels in the cover image. For lesser embedding rates, simply sharper edge regions are used while keeping the other smoother regions as they are. When the embedding rate enhances, more edge regions can be released adaptively for data hiding by modifying just a few parameters. LSB matching revisited (LSBMR)[4] considers a pair of pixels as an embedding component, in which the LSB of the first pixel embeds one bit of secret message, and the relationship (odd–even combination) of the two pixel values carries another bit of secret message. The modification rate of pixels can decrease from 0.5 to 0.375 bits/pixel (bpp) in the case of a maximum embedding rate, meaning lesser changes to the cover image at the same payload compared to LSB replacement and LSB matching. It has been shown that such a scheme can avoid the LSB replacement style asymmetry, and thus it should make the detection slightly more difficult than the LSB matching scheme. The approach consist of two parts- embeddding and extraction. The embedding part first initializes some parameters, which are used for successive data preprocessing and region selection, and then estimates the capacity of selected regions. If the regions are big enough for hiding the secret message , then data hiding is performed on the selected regions. Then, it does some postprocessing to get the stego image. Otherwise the scheme needs to revise the parameters, and then repeats region selection and capacity estimation until secret message can be embedded completely. The extraction part first extracts the side information from the stego image. Based on this side information, it then does some preprocessing and recognize the regions that have been used for data hiding. Lastly, it obtains the secret message according to the analogous extraction algorithm. In[20] such a region adaptive scheme is applied to the spatial LSB domain. The absolute difference between two adjacent pixels is used as the criterion for region selection, and the LSBMR is used as the data hiding algorithm. The experimental results calculated on large number of images using various steganalytic algorithms show that both visual quality and security of stego images are improved drastically compared to typical LSB-based approaches.

3.3 DWT using non-adaptive steganography

We have two popular domains for hiding data - spatial domain and transform domain. The Least Significant Bit (LSB) substitution is one of the example of spatial domain techniques. So far, LSB is the preferred technique used for hiding data because it is easy to implement, offers large hiding capacity, and provides a very easy way to control stego-image quality. But it has low robustness to adjustments made to the stego-image such as low pass filtering and compression and also low imperceptibility. The another type of method for hiding data is the transform domain techniques which overcome the robustness and imperceptibility problems found in the LSB substitution techniques. There are various transforms available for hiding data. The generally used transforms are: the discrete cosine transform (DCT) which is used in the image compression format MPEG and JPEG, the discrete wavelet transform (DWT) and the discrete Fourier transform (DFT). Most recent researches are intended for the use of DWT because it is used in the new image compression format MPEG4 and JPEG2000, examples of using DWT can be found in [23]. In [23], the secret message is embedded into the high frequency coefficients of the wavelet transform while leaving the low frequency coefficients subband unchanged. Some mathematical operations are done on the secret messages before embedding. These procedures and a well-made mapping table keep the messages away from stealing, destroying from unintended users on the internet and hence provide agreeable security. In [24], a novel distortionless image data hiding algorithm based on integer wavelet transform(IWT) that can reverse the stego-image into the original image without making any distortion after extracting the hidden data is proposed. IWT maps integer to integer. This algorithm hides data into one or more middle bitplane(s) of the integer wavelet transform coefficients in the middle and high frequency subbands. It can embed more data compared with the existing distortionless data hiding techniques and satisfy the imperceptibility condition. The image histogram modification is used to avoid greyscales from possible overflowing. A secret key function is used which keeps the secret data secret even after the algorithm is revealed. Therefore, the lossless recovery of original image is achieved. The advantages of transform domain techniques over spatial domain techniques are their high ability to bear noises and some signal processing operations but they are computationally very complex and slower.

3.4 DWT using adaptive steganography

B.Lai and L.Chang[16] proposed an adaptive hiding capacity function to determine how many bits of the secret message is to be embedded in each of the wavelet coefficients. The original image is divided into 8*8 sub-blocks. The technique used was Haar Discrete Wavelet Transform(HDWT).Each block is decomposed to obtain LL1,HL1,LH1and HH1 bands. Because human eyes are insensitive to the edge region ,more data is embedded when the band LL1 is complex. A data hiding capacity function is utilized to calculate the complexity of LH1,HL1and HH1 bands. If these three subbands are complex, the LL1 band is decomposed and additional data bits are embedded in the further decomposed LH2,HL2 and HH2 bands. This method do better than other methods in both data hiding capacity and image quality. Wavelet domain let us to hide data in those regions that the human eyes is less sensitive to, such as the high resolution detail bands (HL, LH and HH). Hiding data in these areas allow us to increase the robustness. It also maintains good visual quality. IWT maps an integer data set into other integer data set. In DWT, the wavelet filters have floating point coefficients so that when we hide data in their coefficients any truncations of the floating point values of the pixels that should be integers may cause the loss of the hidden information.This may lead to the breakdown of the data hiding system. In order to avoid the problems of floating point precision of the wavelet filters when the input data is integer as in digital images, the output data will no longer be integer which doesn't allow ideal rebuilding of the input image and in this case there will be no loss of data through forward and inverse transform. Because of the above difference between IWT and DWT the LL subband in the case of IWT appears to be a close copy with smaller scale of the original image while in the case of DWT the resulting LL subband is distorted. Lifting scheme is one of the technique which can be used to perform integer wavelet transform. R.O.El Safy et al.[25] proposed an adaptive data hiding technique tied with the use of optimum pixel adjustment algorithm to hide data into the integer wavelet coefficients of the cover image so as to maximize the hiding capacity as much as possible. A pseudorandom generator function is used to select the embedding places of the integer wavelet coefficients to increase the system security. The system embeds the secret data in a random order using a secret key which is only known to sender and receiver. This system embeds varying number of bits in each wavelet coefficient according to a hiding capacity function so as to maximize the hiding capacity without sacrificing the visual quality of resulting stego image. The system also minimizes the difference between original coefficients values and modified values by using the optimum pixel adjustment algorithm. Experiments and the achieved results showed that this system achieve high hiding capacity up to 48% of the cover image size with sound image quality and high security because of using random insertion of the secret message. But the system suffers from low robustness against various attacks like histogram equalization and JPEG compression.

4. Analysis of adaptive and non-adaptive methods of steganography

Table 1: Adaptive and Non-adaptive methods

Steganographic Techniques	*Cover Media*	*Description*	*Advantages*
1)Non-adaptive LSB	Image	This method embeds a secret message into the cover image by replacing the k LSBs of the cover image with k message bits to arrive at the stego image.	Simple & easy way of hiding secret data.
2)Adaptive LSB	Image	In this method, the embedding of secret data into the cover image is done by adapting any of the local characteristics of the image.	Good visual quality.
3)Non-adaptive DWT	Image	In this method, the wavelets are used to embed the secret data. The secret message is embedded into the high frequency coefficients of the wavelet transform while leaving the low frequency coefficients subband unchanged.	It can embed more data compared with the existing distortionless data hiding techniques and satisfy the imperceptibility condition.

4)Adaptive DWT	Image	A function is used to select the embedding regions of the integer wavelet coefficients. The integer wavelet coefficients are used to hide the secret data	Hiding capacity is maximized

5. Results

Table 2: Study of Results

Sr. No.	*Steganographic Algorithms*	*Average PSNR*
1	Non-adaptive LSB	62.2
2	Adaptive LSB	61.9
3	Non-adaptive DWT	33.13
4	Adaptive DWT	31.35

Average PSNR of non-adaptive steganographic algorithm using LSB is 62.2 and of adaptive steganographic algorithm using LSB is 61.9. Average PSNR of non-adaptive steganographic algorithm using DWT is 33.13 and of adaptive steganographic algorithm using DWT is 31.35 but both of them have very high hiding capacity.

6. Conclusions and Future Scope

The steganography has been used for a wide variety of applications in a number of different fields. For some applications the non-adaptive steganography is used whereas for some applications steganography is modified by adapting some of the local features of the image giving rise to adaptive steganography. The above paper gives a succinct overview of non-adaptive and adaptive LSB method as well as non-adaptive and adaptive DWT method

In future, non-adaptive and adaptive steganographic techniques can be fused.This fused approach will give us more security as intruders will not be able to detect that what approach exactly we have used adaptive or non-adaptive.

References

[1] Bender DW, Gruhl NM, Lu A. Techniques for data hiding. IBM Syst J 1996;35:313–6.
[2] Chan CK, Cheng LM. Hiding data in images by simple LSB substitution. Pattern Recognit 2004;37(March):469–74.
[3] Zhang X, Wang S. Efficient steganographic embedding by exploiting modification direction. IEEE Commun Lett 2006;10(11): 781–3.
[4] Mielikainen J. LSB matching revisited. IEEE Signal Process Lett 2006;13(5):285–7.
[5] Fridrich J, Goljan M, Du R. Reliable detection of LSB steganography in color and grayscale images. In: Proceedings of ACM workshop on multimedia and security; 2001. p. 27–30
[6] Wu DC, Tsai WH. A steganographic method for images by pixel value differencing. Pattern Recognit Lett 2003;24:1613–26.
[7] Chang CC, Tseng HW. A steganographic method for digital images using side match. Pattern Recognit Lett 2004;25:1431–7.
[8] Zhang X, Wang S. Steganography using multiple-base notational system and human vision sensitivity. IEEE Signal Process Lett 2005;12:67–70.
[9] Wu HC, Wu NI, Tsai CS, Hwang MS. Image steganographic scheme based on pixel-value differencing and LSB replacement methods. Proc Inst Elect Eng, Vis Images Signal Process 2005;152(5):611–5.
[10] Yang CH, Weng CY, A steganographic method for digital images by multi pixel differencing. In: Proceedings of international computer symposium, Taipei, Taiwan, R.O.C.; 2006. p. 831–6.
[11] Wang CM, Wu NI, Tsai CS, Hwang MS. A high quality steganography method with pixel-value differencing and modulus function. J Syst Software 2008;81:150–8.
[12] Yang CH, Weng CY, Wang SJ, Sun HM. Adaptive data hiding in edge areas of images with spatial LSB domain systems. IEEE Trans Inf Forensics Security 2008;3(3):488–97.
[13] K.Changa, C. Changa, P. S. Huangb, and T. Tua, "A Novel image Steganographic Method Using Tri-way Pixel-Value Differencing,"Journal of Multimedia, Vol. 3, No.2, June 2008.
[14] A. Westfeld, "F5a steganographic algorithm: High capacity despite better steganalysis," 4th International Workshop on Information Hiding, pp.289-302, April 25-27, 2001.
[15] P. Chen, and H. Lin, "A DWT Approach for bnage Steganography," International Journal of Applied Science and Engineering 2006. 4, 3: 275:290.
[16] B. Lai and L. Chang, "Adaptive Data Hiding for bnages Based on Harr Discrete Wavelet transform," Lecture Notes in Computer Science, Volume 4319/2006.
[17] Wu DC, Tsai WH. A steganographic method for images by pixelvalue differencing. Pattern Recognit Lett 2003;24:1613–26.
[18] Yang CH, Weng CY, A steganographic method for digital images by multi pixel differencing. In: Proceedings of international computer symposium, Taipei, Taiwan, R.O.C.; 2006. p. 831–6.
[19] Yang CH, Weng CY, Wang SJ, Sun HM. Adaptive data hiding in edge areas of images with spatial LSB domain systems. IEEE Trans Inf Forensics Security 2008;3(3):488–97.
[20] Luo Weiqi, Huang Fangjun, Huang Jiwu. Edge adaptive image steganography based on LSB matching revisited. IEEE Trans Inf Forensics Security 2010;5(2).
[21] Sivaranjani Mrs, Semi Sara mani Ms. Edge adaptive image steganography based on LSB matching revisited. J Comput Appl (JCA) 2011;IV(1):1–3.
[22] Yu C, Wang J. An image adaptive steganography algorithm based on sparse representation and entropy. Sci Computer Appl 2013.
[23] Najme Maleki, Mehrdad Jalali , Majid Vafaei Jahan. Adaptive and non-adaptive data hiding methods for grayscale images based on modulus function. Egyptian Informatics Journal (2014) 15, 115–127
[24] Guorong Xuan, Jiang Zhu, Jidong Chen, Yun Q. Shi, Zhicheng Ni and Wei Su. Distortionless data hiding based on integer wavelet transform. ELECTRONICS LETTERS 5th December 2002 Vol. 38 No. 25
[25] R.O. EI Safy et al. An Adaptive Steganographic Technique Based on Integer Wavelet Transform.978-1-4244-3778-8/09 ,2009 IEEE.