A COMPREHENSIVE STUDY OF VARIOUS TECHNIQUES OF STEGANOGRAPHY : A SURVEY

Palak Keshwani[1]*, Rashmi Priyanka*[2]*, Lalita Nayak*[3]

[1][2][3]*Asst. professor , KITE, Raipur (CG), India*

Email:palakeshwani@gmail.com, rashmi.priya2@gmail.com , lalitanayak2010@gmail.com

ABSTRACT

Today, security is a very important concern in the data communication. Security of data is used in almost every field like education, e-commerce, industry and data warehouse. Firmly sending and receiving data in these areas is an important issue as the data is very crucial. Maintaining the security becomes tough as the data intrinsic features are also different. Hence, the main focal point of this paper is to study and discuss the trends which have already been proposed in the direction of steganography. The gap identification is provided by this study and based on the identification further suggestions are provided.

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

1. Introduction

With the rapid enhancement and the data swapping, a lot of apprehension have been brought up in the security of data transmitted over open channels, particularly at the level of text and picture information. There are 3 basic routines for secured communication, cryptography, steganography and watermarking. Cryptography , manages the improvement of procedures for changing over data in the middle of understandable and incomprehensible structures amid data trade. Steganography, then again, is a procedure for concealing and separating data to be passed on utilizing a transporter signal. Watermarking, is a method for creating legal strategies for concealing restrictive data in the perceptual information. The technique which I am analyzing is Steganography. The image into which a message is hidden is called a cover image and the result is stego-image. This is achieved by entrenching the secret data behind another media such as image, audio and video. In image steganography, the message is hidden behind an image. 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. Steganography is the method through which existence of the secret message can be kept secret. Steganography has various applications. The stegoimage must be undetectable and it should entrench more data. Two significant characteristics which should be considered while scheming a steganographic algorithm are undetectability and embedding capacity.

2. Literature Review

It inserts secret data by replacing x LSBs of a pixel by x secret data bits directly [1]. Zhang and Wang’s method and Mielikainen’s methods [3,4] had the limited capacity for embedding. In this scheme, only one pixel of n pixels into one group is increased or decreased by 1. A very well-known steganographic method is the Least Significant Bit (LSB) substitution method. In the past, several work has been done on steganography. In order to minimize the image distortion, Chan–Cheng gave a new LSB algorithm which based on optimal pixel adjustment [2] in 2004.Zhang and Wang gave an algorithm [3] which is represented in (2n + 1)-ary notation system. In 2006, Jarno Mielikainen [4] projected a new LSB matching algorithm for embedding secret message. The security in LSB-based techniques is not good because they only modify the LSB of the image pixels. Different steganalysis algorithms e.g. RS detector [5] can be applied to get the secret data easily. All the pixels in the cover image cannot bear equal amount of embedding without causing observable distortion. For this reason, it can be easily noticed by eavesdropper. To trounce these problems, adaptive techniques for embedding are proposed [6-12]. In these techniques, quantity of embedding data in pixels is uneven. These techniques give more unrevealed result than simple LSB and other non-adaptive methods. The adaptive techniques estimate the hiding capacity of the cover according to its local characteristics[13,14,15,16]. One of the adaptive technique proposed by Wu-Tsai utilizes the dissimilar values between two neighboring pixels to calculate the number of secret bits to be entrenched[17]. A steganographic technique given by Wu et al.[18] utilizes LSB and pixel values differencing(PVD) method. Within this algorithm, the pixels located in the edge areas hide the secret data using PVD algorithm and the pixels located in the smooth areas hide the secret data using 3-LSB algorithm[18]. In 2008, Yang et al. [19] gave a LSB matching adaptive steganography that utilizes the different values of 2 successive 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 given an adaptive image steganography using LSB matching revisited. In these algorithms, edge regions of cover image are changed and the smooth regions stayed remained stable. In 2013 [22], Yu and Wang gave an adaptive steganography technique in the sparse domain. In 2014 [23], Maleki et al. gave an adaptive and non-adaptive methods for grayscale images based on modulus function. Adaptive method utilizes average difference value of 4 neighbor pixels and modulus function. The average difference value of 4 neighbor pixels and a threshold secret key are utilized to find out the edge or smooth area. This adaptive technique can withstand the RS steganalysis attack. Non-adaptive method gives less distortion in the stego-image. The residual of the paper is organized as follows. First, I provide a small introduction to non-adaptive technique using LSB and integer wavelet transform. Then, I will discuss the adaptive technique using LSB and integer wavelet transform. Second, I will discuss the results; and then I will conclude the paper.

3. Methodology

There are 2 techniques for hiding the secret data inside the cover media. They are non-adaptive and adaptive techniques. Here I will analyze LSB using non-adaptive and adaptive steganography. Then I will review DWT using non-adaptive and adaptive steganography.

LSB with non-adaptive steganography

LSB replacement hides a secret message into the cover image by replacing the x LSBs of the cover image with x message bits to get the stego image. In various existing techniques, the selection of hiding places within a cover image depends on a pseudorandom number generator without taking into account the relationship between the image content itself and the size of the secret data. And, hence the smooth regions in the cover images will indubitably be contaminated after embedding data still at a less embedding rate, and this will give low visual quality and low security, especially for those images with lots of smooth areas. If we take a 24-bit color image, a bit of every of the three colors - red, green and blue can be used, so therefore a total of 3 bits can be stored in each pixel. For example, the given grid can be taken as 3 pixels of a 24-bit color image, using 9 bytes of memory:

(00101101 00011101 11011100)
(10100110 11000100 00001100)
(11010010 10101101 01100010)

If we take the number 204, which is represented in binary form as 11001100, is entrenched into the least significant bits of this part of the image, the resultant is as follows:

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

Even if the number was entrenched into the first 8 bytes of the grid, only the 3 underlined bits needs to be changed according to the embedded message. Therefore, on an average, only half of the bits in an image will need to be changed to entrench a secret message. Because, there are 256 possible intensities of each primary color, changing the LSB of a pixel results in small changes in the intensity of the colors. These changes cannot be apparent by the human eye and therefore the secret data is successfully hidden. Through a chosen image, one can even hide the message in the least as well as second least significant bit .

LSB with adaptive steganography

The least-significant-bit (LSB)-based technique is a very familiar steganographic technique in the spatial domain but this scheme will give poor visual quality and low security based on various analysis and experiments predominantly for those images having many smooth regions. Here I briefly explain the LSB matching revisited based on adaptive steganography. In 2010 Weiqi Luo et al. [20] gave an edge adaptive scheme which find the places for entrenching according to the size of secret data and the difference between 2 successive pixels in the cover image. For smaller embedding rates, sharper edge places are used while keeping the smoother places as they are. As the entrenching rate increases, more edge places can be released adaptively for hiding the data by changing a few parameters. LSB matching revisited (LSBMR)[4] takes a pair of pixels as an entrenching component, in which the LSB of the 1st pixel entrench 1 bit of secret message, and the relationship (odd–even combination) of the 2 pixel values carries another bit of secret message. The changing rate of pixels can reduce from 0.5 to 0.375 bits/pixel (bpp) in the case of a highest embedding rate, meaning less alterations to the cover image at the same payload compared to LSB replacement and LSB matching. It has been made known that this scheme can avoid the LSB replacement style asymmetry, and hence it should make the detection slightly extra difficult than the LSB matching scheme. This approach has 2 parts-embeddding and extraction. The embedding or entrenching part first initializes few parameters, that are used for successive data preprocessing and region selection, and then calculates the capacity of chosen places. If the places are large enough for entrenching the secret data , then data hiding is performed on the selected places. Then, it performs some postprocessing to arrive at the stego image. Or else,the scheme needs to revise the parameters, and then repeats place selection and capacity calculation until secret data can be entrenched completely. The extraction section first extracts the side data from the stego image. Based on this side information, it then does some preprocessing and know the places that have been utilized for data hiding. Last of all, it finds the secret message according to the equivalent algorithm. In[20] such a place adaptive method is applied to the spatial LSB domain. The absolute difference between 2 contiguous pixels is used as the measure for place selection, and the LSBMR is used as the data hiding algorithm. The experimental results calculated on huge figure of images using different steganalytic algorithms reveal that both visual quality and security of stego images are enhanced hugely as compared tol LSB-based approaches.

DWT using non-adaptive steganography

We have 2 familiar domains for hiding the secret data. They are spatial domain and transform domain. The Least Significant Bit (LSB) replacement is an example of the spatial domain .Thus far, LSB is the favorite method which is used for embedding the data because it is very easy to apply, offers high embedding capacity, and gives an easy way to organize the stego-image quality. But, it has little robustness to adjustments which can be made to the stego-image, for example -low pass filtering, compression and little imperceptibility. The other class of technique for entrenching the data is the transform domain that overcome the robustness and imperceptibility troubles found in the LSB substitution techniques. There are many different transforms existing for hiding the secret data. The normaly 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. Many current researches are proposed for the use of DWT as it is used in the new image compression format MPEG4 and JPEG2000, various examples of using DWT can be seen in [23]. In [23], the secret data is entrenched into the high frequency coefficients of the wavelet transform at the same time leaving the low frequency coefficients subband unaffected. A little mathematical operations are performed on the secret data before entrenching. These methods and a clever mapping table stay the messages away from destroying and stealing from intended users on the internet and therefore offer acceptable security. In [24], a novel distortionless image data hiding algorithm based on integer wavelet transform (IWT) that can turn around the stego-image into the original image without performing any distortion after extracting the hidden data is given. Integer Wavelet Transforms maps integer with integer. This technique embeds the data into one or more middle bitplane(s) of the integer wavelet transform coefficients in the middle and high frequency subbands. It can hide more data as compared to the existing distortionless data embedding techniques and it satisfy the imperceptibility criteria. The image histogram alteration is utilized to keep away from grayscales from probable overflowing. A secret key function is utilized that keeps the secret data secret still after the algorithm is revealed. And hence, the lossless recovery of original image is attained. Various benefits of transform domain methods are their large capacity to tolerate noises and some signal processing activities but they are computationally very complex and slower.

DWT using adaptive steganography

B.Lai and L.Chang [16] gave an adaptive embedding capacity function to determine how many bits of the secret message is to be entranched in each of the wavelet coefficients. The original image is separated into 8*8 sub-blocks. The method that used was Haar Discrete Wavelet Transform(HDWT).Each block is divided to obtain LL1,HL1,LH1and HH1 bands. Because human eyes are not sensitive to the edge area ,more data is entrenched when the band LL1 is complex. A data embedding capacity function is employed to find out the complexity of LH1,HL1and HH1 bands. If these 3 subbands are complex, the LL1 band is divided and additional data bits are entrenched in the further decomposed LH2,HL2 and HH2 bands. This method does better than other methods in data entrenching capacity and image quality. Wavelet domain allow us to embed data in those places that the human eyes is less perceptive to, for example, the high resolution detail bands (HL, LH and HH). Entrenching data in these areas let us to raise the robustness. It also keep good visual quality. Integer Wavelet Transform maps an integer data set into another integer data set. In the Discrete Wavelet Transform, wavelet filters have floating point coefficients so that when we entrench data in their coefficients any truncations of the floating point values of the pixels that should be integers may cause the loss of the entrenched data. This may direct to the breakdown of the data embedding system. In line to avoid the troubles 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 that doesn't allow perfect rebuilding of the input image. And in this case there will be no loss of data through forward and inverse transform. Because of this differentiation among Integer Wavelet Transform and Discrete Wavelet Transform, the LL sub band in the case of Integer Wavelet Transform appears to be a close copy with lesser level of the original image at the same time in the case of DWT the resulting LL subband is distorted. Lifting scheme is one of the technique which can be utilized to carry out integer wavelet transform. R.O.El Safy et al.[25] gave an adaptive data hiding method that is tied with the use of optimum pixel adjustment algorithm to entrench the data into the integer wavelet coefficients of the cover image so as to increase the data hiding capacity as much as possible. A particular pseudorandom generator function is utilized to pick the entrenching regions of the integer wavelet coefficients to increase the system security. The system entrench the secret data in a random order by utilizing a secret key that is only well-known to sender and receiver. This system entrenches different number of bits in every wavelet coefficient according to a entrenching capacity function so as to increase the entrenching capacity without giving up the visual quality of resultant stego image. The system also reduce the difference between the original coefficients values and modified values by using the optimum pixel adjustment algorithm. Experiments and the obtained results revealed that this system gives greater entrenching 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 except the system go through low robustness against different attacks like histogram equalization and JPEG compression.

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 technique embeds a secret message into the cover image by replacing the x LSBs of the cover image with x message bits to arrive at the stego image.	Easy and simple way of entrenching secret data.
2)Adaptive LSB	Image	In this method, the	Fine visual quality.

		entrenching of the secret data into the cover image is done by adapting any of the local characteristics of the image.	
3)Non-adaptive DWT	Image	In this method, the wavelets are used to entrench the secret data. The secret message is entrenched into the high frequency coefficients of the wavelet transform while leaving the low frequency coefficients subband unchanged.	It can entrench more data compared with the existing distortion less data hiding techniques and suit 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.	Entrenching capacity is maximized.

4. 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

The average Peak Signal-to-Noise ratio, PSNR of non-adaptive steganographic method with Least Significant Bit is 62.2. The average Peak Signal-to-Noise ratio of adaptive steganographic algorithm using Least Significant Bit is 61.9. The average PSNR of non-adaptive steganographic algorithm utilizing Discrete Wavelet Transform is 33.13 and that of adaptive steganographic algorithm using Discrete Wavelet Transform is 31.35 but both of them have very high hiding capacity.

5. Conclusions and Future Scope

Steganography is used in different applications. In some applications, non-adaptive steganography is used whereas in some applications, steganography is modified by adapting some of the local characteristics of the image leading to adaptive steganography. This paper gives a laconic overview of adaptive and non-adaptive LSB methods as well as adaptive and non-adaptive DWT method.

In future, adaptive and non-adaptive steganographic techniques can be fused together .This fused approach will give us greater security as trespasser will not be capable to perceive that what technique exactly we have used non-adaptive or adaptive.

6.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.