www.ijecs.in
International Journal Of Engineering And Computer Science ISSN:2319-7242
Volume 4 Issue 1 January 2015, Page No. 10065-10067

A Survey on Different Methods for Hiding Information behind an Image

Deepali G. Singhavi[1], *Dr. P. N. Chatur*[2]

[1]M.Tech Scholar, Department of Computer Science and Engineering,
Government College of Engineering,Amravati,India
deepalisinghavi@gmail.com

[2]Head of Department, Department of Computer Science and Engineering,
Government College of Engineering, Amravati,India
chatur.prashant@gcoea.ac.in

Abstract: ***In recent years data hiding has been proposed as a likely technique for the purpose of information security.Hiding data is the process of embedding information into digital content without causing perceptual degradation. In data hiding, pieces of information represented by some data are hidden in a cover media like image. The main intention of data hiding is to prevent the detection of hidden information.The most commonly used algorithm for data hiding is Least Significant Bit algorithm apart from these various algorithms have been proposed for data hiding in last few years. This paper consists of survey of different methods and techniques available for data hiding.***

Keywords: Data hiding, least significant bit, Information security.

1. Introduction

Since the rise of the internet, the important factorthat is to be considered in the field of information technology and communication has been the security of information. Data privacy issues can be found in various range of sources such as healthcare records, criminal justice investigations and proceedings, financial institutions and transactions, biological traits, residence and geographic records and ethnicity. As more and more systems are connected to the Internet today providing security to data and data privacy has become increasingly important. Thus, hiding the data behind some media such as within an image, video, music or any other computer file is vital to protect important data. Data hiding has become a most common technique for the purpose of authentication, security, and copyright protection, etc. It helps to keep not only the contents of a message secret, but also keep the existence of the message secret.Hiding data is the process of embedding information into digital content without causing perceptual degradation. The main intention of data hiding is to prevent the detection of hidden information. In data hiding, pieces of information represented by some data are hidden in a cover media like image. The data hiding process link two data set i.e. cover media and embedding secret information. The relationship between this data set characterizes different applications such as covert communication and authentication. The application in which the hidden data may be irrelevant or unrelated to the cover media is covert communications and the application in which the embedded data are closely related to cover media is authentication. In this paper we focus on various methods that are used to hide important behind an image file. The most common and easiest method that is used for data hiding is least significant bit algorithm apart from this reversible data embedding were proposed for data hiding and some variations of least significant bit algorithm are also there for data embedding. This paper consists of survey of different method and algorithm for hiding information behind an image.

2. Different methods

In last few years different types of hiding algorithm are proposed. The most common algorithm or method that is used for data hiding is least significant bit algorithm. Because it is very easy to understand and simple to implement.Apart from least significant bit algorithm there are some variations of least significant algorithm that have been proposed for data hiding. And also some reversible watermarking algorithm has been proposed for data hiding. This section consists of different method and algorithm which are available for hiding information behind an image.

2.1 Least Significant Bit Technique [1]

Least significant bit is a steganography algorithm; steganography is anart that hides information in other carrier to hide the fact that communication is actually taking place. Least significant bit insertion method is a simple method that is used to embed information behind an image. The method use the LSB of a byte of cover image to hide M bits of secret message. The resultant stegano image will look identical to the carrier image to human eyes. The best image for hiding information is 24 bit RGB image. It is easier to hide information in an image if it is of high quality and good resolution. Although the most common image file is 24 bit image but to avoid posting of large image on internet some people also choose 8 bit image for data hiding. In most commonly used least significant bit method the last bit of image is replaced by secret message. So we can store 1 bit in a pixel of 8 bit image and 3 bits in a pixel of 24 bit image file that is 1 bit in each of the red, blue and green component. This method works well for image steganography. Image steganography is a simple and secure way to transfer information over the internet.

2.2Reversible Data Embedding Using A Difference Expansion [2]

Another method that is used for data hiding is reversible data embedding which is also called as lossless data embedding. Reversible data embedding ensures distortion-free data embedding. Reversible data hiding can hide secret data behind an image in reversible fashion. The method allows authorized party to decode the hidden information and also allow restoring the image to its original form as it is. The main aim of this method is to ensure that the resultant degradation on the image after data embedding should be low.Three factors that can be used to measure the performance of reversible data embedding are payload capacity, visual quality, and algorithm complexity. Reversible data embedding can be used for covert communication channel since the difference between the embedded image and original image is almost imperceptible from human eyes. In reversible data embedding using difference expansion, difference of the neighboring pixel values is used for the difference expansion. In digital image, one can select some expandable difference values of pixels and embed one bit into each of them. To extract the embedded data and for restoring the original values and we need to embed some location information to help decoder to know which difference values have been selected for the difference expansion for information retreival. For embedding this location information we have to create and embed a location map, which contains the location information of all selected expandable difference values. To decode the information first we require calculating difference value. For an image, using the same pairing as in embedding, and applying integer transform to each pair to decode hidden information. The problem with reversible data embedding is that it is a fragile technique. The decoder will not able to restore the original content restoration if the embedded image is manipulated and/or lossy compressed. The important feature or advantage of reversible data embedding is its reversibility.

2.3 Simple LSB Substitution With An Optimal Pixel Adjustment Process[3]

In data hiding method by using simple LSB method we simply replace least significant bits of cover media by secret message. The method is very simple and most commonly used but problem with this method is it reduces the resultant stegano-image quality and in some application it is required to maintain the resultant stegano image quality. To improve the resultant image quality a simple LSB algorithm with an optimal pixel adjustment is proposed. In this method first a simple LSB substitution is applied on cover image then the WMSE between the cover-image and the stegano-image is derived and used to improve the image quality. The difference δ i.e. the embedding error between the stegano image and cover image is used for optimal pixel adjustment process to improve image quality. The visual quality of stegano image obtained by optimal pixel adjustment process is much better than that of stegano image obtained by the simple LSB substitution method. The WMSE obtained by this method could be less than ½ of that obtained by LSB substitution method.

2.4 Reversible Data Hiding[4]

In data hiding method we modify the pixel values of cover media to embed secret message, this will leads to some distortion in cover image and so cover media cannot be inverted back to the original media. That is even after the hidden message is extracted out the cover media will experience some permanent distortion. In some application it is critical to retrieve the original media for some legal consideration after the hidden data have been extracted out. Application such as medical diagnosis and law enforcement has this requirement. Reversible, lossless, distortion-free, or invertible data hiding techniques satisfy this requirement. Reversible data hiding method hides data in such a way that after extracting secret data we can losslessly recovered the cover image. A reversible data hiding method by using histogram can embed large amount of data and at the same time maintain a very high image visual quality. In this method we first generate histogram for given cover image then we determine zero or minimum point of histogram to embed data, where zero point refer to gray scale value which no pixel in the given image assumes and a peak point corresponds to the gray scale value which the maximum number of pixels in the given image assumes. The gray scale value between zero point and peak point is used to embed secret data.The peak point is calculated with an objective to increase the embedding capacity, because the number of bits that can be embedded into an image is equals to the number of pixels associated with the peak point. The given image is scanned in sequential order to find out pixels whose gray scale value lies between zero and peak point and then the gray scale value of all this pixels are incremented by 1 that is the range of histogram is shifted to the right side by one. Again the image is scanned in the same sequential order. When the pixel with gray scale value equal to peak point is encountered the embedding bit is checked if the corresponding bit in the embedding sequence is 1 the pixel gray scale value is incremented by 1 otherwise the pixel gray scale value remains the same.The limitation of this method is that it is applicable only to gray scale images.

2.5 Very Fast Watermarking By Reversible Contrast Mapping[5]

Most of the reversible watermarking techniques require some manipulation on image prior to data embedding stage such as lossless data compression; the lossless compression increases the mathematical complexity of watermarking technique. So a watermarking technique is proposed that can hide secret data without performing any prior compression. Very fast watermarking by reversible contrast mapping achieves high-capacity data embedding without performing any compression. In reversible contrast mapping a simple integer transform is defined on pairs of pixels and then watermarking is used to substitute the LSB of transform pair by secret message. At detection each transformed pair should be correctly identified to extract the watermark and to restore the original pixels. The

LSB of first pixel of each pair indicates whether the pair is transformed or not, 1 indicates it is transformed and 0 for non-transformed pair. The main benefit of this method is that even if the least significant bits of transformed pair are lost, it is inevitable.

2.6 Reversible Image Watermarking Based On Integer-To-Integer Wavelet Transform [6]

In reversible watermarking even though the embedding distortion is inevitable it can be resolved and the original data can be reconstructed from the watermarked image as it is. In reversible watermarking based on integer to integer wavelet transform an input image is first divided into non overlapping blocks, and the watermark is embedded into the high-frequency wavelet coefficients of each block by using simple LSB algorithm. That is an image block consisting of integer-valued pixels is transformed into a wavelet domain, It maps integers to integersand does not cause any loss of information through forward and inverse transforms. The advantage of this method is it allows higher embedding capacity while maintaining distortion at lower level.

2.7 Enhanced Least Significant Bit Algorithm[1]

In simple least significant bit algorithm the LSB of pixel values of cover image is replaced by secret message i.e. the least significant bit of each color i.e. RGB of the carrier image is used to embed secret message. The problem with simple LSB method can be easily stated from the fact that modifying the three colors of a pixel produces a major distortion in the resulting color so a method that introduces less distortion in the resulting image is required. The enhanced LSB algorithm improves performance of simple LSB by hiding information in only one color that is blue color of the carrier image. This minimizes the distortion level which is negligent to human eye.

3. Conclusion

In this survey the aim has been to study differentmethods of data hiding for hiding information behind an image.Every model discussed in this paper has different requirement and different level of applicability.Each methodhas some advantage and disadvantages as well. The future research is directed towards developing methods or techniques that will improve the stegano image quality, can embed large amount of information behind an image and will able to restore the carrier image back to its original form.

References

[1] J. Tian, “Reversible data embedding using a difference expansion,” IEEE Trans. Circuits Syst. Video Technol., vol. 13, no. 8, pp. 890–896, Aug. 2003

[2] C. K. Chan and L. M. Cheng, “Hiding data in images by simple LSB substitution,” Pattern Recognit.., vol. 37, pp. 469–474, Mar. 2004.

[3] Z. Ni, Y. Q. Shi, N. Ansari, and W. Su, “Reversible data hiding,” IEEE Trans. Circuits Syst. Video Technol., vol. 16, no. 3, pp. 354–362, Mar.2006.

[4] D. Coltuc and J.-M. Chassery, “Very fast watermarking by reversible contrast mapping,” IEEE Signal Process. Lett., vol. 14, no. 4, pp. 255–258, Apr. 2007.

[5] S. Lee, C. D. Yoo, and T. Kalker, “Reversible image watermarking based on integer-to-integer wavelet transform,” IEEE Trans. Inf. Forens. Secur., vol. 2, no. 3, pp. 321–330, Sep. 2007.

[6] S. Gupta, G. Gujral, and N. Aggrawal, “Enhanced Least Significant Bit algorithm For Image Steganography,” IJCEM International Journal of Computational Engineering & Management, Vol. 15 Issue 4,pp. 40-42, July 2012.

[7] Artz, D, “Digital Steganography: Hiding data within Data‟, IEEE Internet Computing, May/June 2001.

Author’s Profile

Deepali G. Singhavihas received her B.E.degree in Computer Engineering from Bapurao Deshmukh College of Engineering Sewagram, wardha,India in 2012 and now pursuing M.Tech in Computer Science and Engineering from Government college of Engineering Amravati, india. Her area of research includes image processing, network security, and Data Mining.

Dr. Prashant N. Chatur has received his B.E. degree in Electronics Engineering from V.Y.W.S College of Engineering, Badnera, India, in 1988, the M.E. degree in Electronics Engineering from Government College of Engineering, Amravati, India, in 1995, and the Ph.D. degree in Artificial Neural Network from Amravati University, India, in 2002. He was a lecturer with department of Computer Science & Engineering, in GovernmentPolytechnic, Amravati, in 1998. He was a lecturer, assistant professor, associateprofessor, with Department of Computer Science & Engineering, in Government College of Engineering, Amravati, in 1991, 1999 and 2006 respectively. His research interest includes Neural Network, Data Mining, Image Processing. At present, he is the Head of Computer Science and Engineering department at Government College of Engineering, Amravati,India.