Available online at www.elixirpublishers.com (Elixir International Journal)

Digital Processing

Elixir Digital Processing 76 (2014) 28523-28526

ISSN: 2229-712X

Image steganography practices classification by object oriented approach: a review

Ashwani Kumar Singh* and Jaya Sharma
Department of Computer Science and Engineering, ASET, Noida.

ARTICLE INFO

Article history:
Received: 12 May 2014;
Received in revised form:
7 November 2014;
Accepted: 17 November 2014;

Keywords
Stego object, MSE,
Payload capacity,
Image error Management,
PSNR.

ABSTRACT

This paper focuses on reviewing the various Steganography techniques that have been reported by researchers and scientists in the literature. The motivation of this paper is to overview the past and current Steganography techniques to embed the Stego image which bypass the human visual system without being detected. The techniques which operate both on text and image are considered. The focus is also given for the use and future scope of these techniques. The techniques are reviewed on the parameters of security, peak signal to noise ratio of stego image, mean square error and the capacity of data that can be carried out on the network without being detected. The paper is divided in three major sections which are the implementation in spatial domain, frequency domain, adaptive or mixed technique

Introduction

With the advancement of internet and extensive use of online communication, the need of security and confidentiality is increased. This led to the requirement of secure communication techniques that are easy to use but is difficult to breach. Cryptography is one of the most widely used technique to solve this problem of secure communication. The problem with cryptography is that the message is sent in encrypted form possibly gather the attention of hackers. For this the solution is Steganography. It is being interpreted as the study and implementation of invisible communication, It differs from cryptography in the way that the aim is to protect the information on communication channel from eavesdropper .It focuses on hiding the presence of message from the observer[1]. Steganography is not the replacement of the cryptography rather it is the technique which increases the power of cryptography. Steganography has been evolved from ancient time when Greeks used to hide the message of high importance on the scalp of the secret message carrier. The concept of Steganography system can be explained as let data embedding method is "M" which is used to hide the message "MSG" in the cover image "IMG".The new message formed is the combination of "MSG+IMG" and this is extracted on the receivers end without any change in the integrity of the message. A good steganographic algorithm is that which produce minimum entropy change e[2] .With the advancement of the digital world this technique is used to solve the famous "prisoners problem" given by simmons [20,1]. In this problem two prisoners have to communicate securely, so that the warden is unaware about the message passed between them. so they agreed on a technique which uses cover text to hide the message. The introduction of digital images in various formats the Steganography system uses images as the cover objects. The power of images is exploited in the Steganography technique. This paper describes the techniques related to images on an object oriented approach. Here the object is considered as the region, dimension and quality of image which is exploited to hide the message (MSG) securely.

Rest of the paper is organized as: - Section II discusses related work, Section III sets out the comparison of steganography techniques on the basis of security, payload and PSNR .The comparative analysis is concluded in secion IV.

Related Work

Steganography in spatial domain

This category broadly defines the data encapsulation applied on pixel value of image. This method uses payload which can be carried out is the least significant bit (LSB) plane of the image. In the 8 bits across the plane of an 8*8 image the LSB is exploited for inserting the data .The concept used is explained by following equation:

$$X_n' = X_n - X_n \bmod 2^k + M_i \qquad \text{..........(1)}$$

In the above equation X_n' is representing the nth value of the embedded image , X_n stands for the original image used for embedding the text and k stands for the number of bits used to hide the data, Where M_i is the nth place value of the embedded data in the image. After embedding the data it can be easily extracted by the mathematical formulation which is given as:

$$X_i' = X_i - \bmod 2^k \qquad \text{.......(2)}$$

This is done in such a way that the above process of embedding does not affect the image pixel value. If it destroys the original features of the image it can be easily detected.

Hideki Noda [4] presented a method which uses a lossy compression image method to exploit the cover image characteristics. In this method the image is divided in a block of size N×N. Here the complexity is set to $0.3A_{max.}$ The object used in this technique is the JPEG2000. The object is used to hide the data in the LSB [2, 18] plane. By this method the payload capacity achieved is 25% of the size of fresh image. The PSNR obtained is 48db.

K.B Raja [5] given a model for Steganography which operates only on raw formats of images. Two dimensional DCT is used in this technique. The LSB of the fresh image is considered for embedding the image. The stego [5] object is created by compressing the image using quantization and length of the fresh image. The object is considered to be the bits of less importance in the fresh image, which is not needed for the description of image after the extraction of image. In this

Tel:
E-mail address: singhashwani1989@gmail.com

method last two digits were replaced with the first two most significant bits of the hidden images. The author succeed to obtain a low MSE which result to satisfactory PSNR.

Rig Das [6] presented a Steganography technique in which main focus is done on Huffman encoding. In this technique the gray level value of the both image object is stored and calculation of the size of the secret data image is done. It consider size of image is N bit then the image is multiplied with N. After multiplying the size of image should be smaller in size of the cover object image ,then only be the embedding is possible. It is not possible to hide a larger image in smaller but vice versa is only possible. The next step comprise of obtaining the Huffman coding of the secret image to embed it in LSB of the fresh image .This technique is complex then the previous techniques . In this technique the author claims full recovery of the secret image which shows that the high PSNR [4] and low MSE [4] as both are inversely proportional to each other. The formula given by the author used for calculation is:

$$\text{PSNR} = 10\times\log(255^2/\text{MSE}) \quad ....(3)$$

In which, $$MSE=\sum_{x=0}^{n-1}\sum_{y=0}^{n-1} (f(x,y)-g(x,y))^2/N^2 \quad ....(4)$$

The unit of PSNR is db and it indicates the quality of the image obtained, smaller the MSE means minimum error and higher the PSNR means better image quality of the recovered image. In this paper it is clearly stated that for successful embedding PSNR should be greater than 57db. The images are almost identical which are founded in the result. In this technique the use of Huffman coding results in to satisfactory results. This makes the image more secure and prevent it from destroying by hacker. The object used to hide the data is the result of Huffman coding [6].

Monoj Kumar Ramaiya [7] proposed a improved technique based on the mapping through the use of S- box tool and DES. In this paper a combination of nPr and substitution is used to obtain the stego image. The XOR operation is used to find the final stego image. The encoding algorithm separates 8×8 image in to 4 parts there for embedding these pixel in LSB of the fresh image. The last two LSB bits are used to embed and s-box integration makes it more effective .The capacity of data to be embedded is restricted to 25% of the original image. In this technique the gray value of less important pixel is changed which are needed for the security of the image. All the operation were performed on 64×64 images. The difference between the pixel values is calculated to be 0-3. The base for this technique is data encryption standards and the object used in the technique is the last two LSB of the fresh image which results to more promising results.

B. Steganography in frequency domain

Frequency domain methods comprise of the techniques which first convert the image into the frequency domain and then the embedding of data takes place. The data in this technique is less in payload but is more secure and robust than the spatial domain techniques. There is no such standard procedure to determine the amount of data which can be embedded in the frequency sub bands.

Nedal M.S. Kafri and Hani Y.Suleiman[8] proposed an algorithm to embed the image with more security and to make stego image more robust to attacks. The main focus is done on finding the method to bypass the steganalysis process (detection of presence of secret data in cover image) [1]. This is achieved by transforming the image in frequency domain. The data embedded in the non zero coefficient obtained by the Discrete cosine transform. Inverse discrete cosine transform is applied to obtain the required stego image [8]. The output of the above process results in the bmp image [3]. In this technique the 4th bit is exploited of the discrete cosine transform. The author show better result than the spatial domain techniques which comes to the average value of PSNR as 47.58db. The object taken for embedding the secret data is the discrete cosine transform coefficient which give more refined results.

Sachin.A.Thanekar[9] defined a new technique in frequency domain named OCTA PVD. This technique used the concept of generating the pixel pair of 3×3 rather than 2×2 image blocks for embedding the secret data. In this method the algorithm states that the 3×3 pair of pixel value differencing is used. The embedding algorithm is then implemented in the plane. The extraction process at the receiver end divides the image in the 3×3 pixel block to locate the range of extraction. This is being done by making the histogram of the concerned images. The author reached the PSNR of 37.90 [9].

Amrita Khamrui and J K Mandal [17] introduced a genetic algorithm using the discrete cosine transform. DCT is used to obtain the frequency bands and two bits of the image are embed in sub bands leaving the first bit. To create the population of bits initial sub mask of the image is taken. To increase the security the new generation of bits followed by crossover is done. The object taken for embedding is the crossover bits of the image mask. This technique gives PSNR of 44.92db but works only for gray scale images.

Po-Yueh Chen and Hung-Ju Lin[18] proposed a method where high frequency bands of image are obtained by discrete wavelet transform. These high bands are considered for embedding the secret data. Low frequency bands are preserved so that the maintain the integrity and quality of image. The object taken to embed the image is is the high frequency bands of the fresh image. The algorithm is designed for variable payload and image quality. The PSNR obtained is 54.94db which falls under the satisfactory range. However the algorithm is not compatible with JPEG format.

Adaptive Steganography techniques

These techniques are the implementation of the combined features of spatial domain methods and frequency domain methods. These are called adaptive because these techniques target particular part in an image by making statistical calculation on the image before transforming the image in DCT plane.

Anjali,A.shejul [10] proposed an adaptive Steganography technique by using feature of (Hue, saturation, value) color space only for embedding the secret data in images. Followed by performing DWT to transform the image in to four sub bands. Only the high frequency bands are selected to embed the secret data as they are less prone to the histogram attacks. The author measures the efficiency of the algorithm on the basis of invisibility by human visual system and capacity of the data which the cover object can carry. The author experimented two states of image firstly by embedding the data in fresh image and secondly by embedding the data in cropped part of image. The resulting payload of both the operation is satisfactory but the fresh image contains 15% payload as stated by the author. The object used by the author to hide the MSG is the YCbCr plane [10] which is found to be the more promising towards the protection of histogram attacks.

Abbas cheddad [11] came up with a new approach in which the use of biometrics is done . The algorithm used to identify the skin of human and by forming the subset of skin region the data embedding is applied. The author used a skin probability map (SPM) [11] which makes the clusters around the upper and lower boundaries of the skin. Then the DWT of the clustered image is created. As the human face image is an ellipse it has two dimensions they are used to determine the region. The data is then embedded in the upper and lower region of image graph which is extracted by applying inverse of it. The technique although provide less space for the embedding but on the cost of more security towards the blind histographic attacks[9]. The object used in the technique is the human skin on gray images only .

An adaptive technique is given by Nidhi Grover [12] in this technique the edge detection came into picture. The LSB [2] is used with combination of edge detection of the images resulting in to adaptive scheme of Steganography. The algorithm is divided into two modules .The first module is for embedding the information .which deals with detecting the edges of the grayscale image and then by converting the secret text in 0, 1 form is embedded to form stego image. The binary values are saved in two groups one with edge detection and other one without edge detection. The stego image is then saved in .png format and the reverse process is done for the extraction of image at the reciever's end. The result of this approach is satisfactory value of PSNR i.e. 49.74db.The object selected for hiding the secret message is obtained by edge detection of the fresh image.

Lifang Yu and Yao Zhao[13] proposed an adaptive algorithm for JPEG image. The algorithm implements the adaptive data hiding by preserving the first order values of the image. The data bits are randomly mixed and are selected by a genetic algorithm. The mixing of bits to overcome the problem of dissymmetry is applied in this method. To minimize the modification less modification rules are used. The ranking of the bits obtained by crossover is done and the high ranking bits are taken for embedding. The PSNR obtained is 44.32db. Object considered for embedding the data is the high ranking bits of the image.

COMPARITIVE ANALYSIS

A number of parameters could be defined for comparing the performance of various steganography techniques. In this paper we have identified parameters like Security, maximum payload and PSNR. Security is defined as the robustness of the algorithm towards the steganoanalysis techniques. Maximum payload gives the amount of data that can be embedded without destroying the essential properties of image. PSNR value measures the quality of the image after restoration, higher the PSNR value better will be the quality of stego image

.

Technique Used	**Security**	**Maximum Payload**	**PSNR value**
Spatial Domain Technique	Low	25% of the fresh Image	57db
Frequency Domain Techniques	Medium	15% of the fresh image	54.94db
Adaptive Domain Techniques	High	12.5% of the fresh image	49.74db

Table 1: Comparision of Steganography Techniques

The levels at which the algorithm satisfy security of application is taken as low, medium and high .The low levels indicates weakness in terms of providing security and hence are susceptible to attacks. Medium level defines that the security result depend on outside influence i.e High level states that the technique completely fulfill the security requirements. Thus it is considered robust in terms of security. Payload is expressed in terms of percentage of data of the fresh image used forn for embedding. The PSNR value is used to state the quality of stego image. Higher the PSNR better will be the quality of stego image. From the above table it is clear that there is been tradeoff between security,payload and PSNR value of the image. Spatial domain techniques are suitable for high payload and low security requirement application .While Adaptive domain techniques should be used in high security and comparatively low payload conditions. The frequency domain techniques are suitable for medium security and payload applications.

Conclusion

In this paper the evolution of major techniques of image Steganography being reviewed on the basis of the security, payload carried by the image and quality of the image in terms of PSNR. An object oriented scheme is used to deduce the embedding region of each technique. The discussed techniques have various tradeoffs as the techniques in spatial domain are more prone to attacks as compared to adaptive domain techniques. while the techniques of frequency domain are not prone attack only in the condition when the amount of data to be embed is small in size. Embedding secret data using DWT produce more uniform results. The adaptive method of Steganography is complex but produce more promising results and robust to the various types of statistical and histogram attacks. Even though there are various techniques but there is scope of research of Steganography techniques on various image formats .

References:

[1] Rajarathnam Chandramouli , Mehdi Kharrazi and Nasir Memon ,"Image Steganography and Steganalysis: concept and practice" Springer-Verlag Berlin Heildelberg,pp 35 - 49, 2004.

[2] R.Chaundramouli and Nasir Memon ,"Analysis of LSB based Image Steganography Techniques",*Image Processing ,International conference (volume 3)*,pp 1019-1022, June2001.

[3] Ross J. Anderson, Fabien A.P Perititcolas "On the Limits of Steganography" in proceeding of the IEEE signal processing letters,pp 474-482, May 1998.

[4] Hideki Noda, Jeremiah Spaulding, Mahdad N Shirazi , and Eiji Kawaguchi "Application of Bit-Plane Decomposition Steganography to JPEG2000 Encoded Images" signal processing Letters, IEEE(Volume 9,issue 12) ,pp 410-413,Dec 2002.

[5] K.B.Raja, C.R Chowdary, Venugopal K R, L.M.Patnaik "A Secure Image Steganography using LSB, DCT and Compression Techniques on Raw Images" Intelligent Sensing and Information processing.Third International Conference on 14-17,pp- 171-176, Dec 2005 .

[6] Rig Das and Themrichon Tuithung "A Novel Steganography Method for Image Based on Huffman Encoding" Emerging Trends and Applications in Computer Science (NCETACS) ,3rd International Conference on 30-31 March,pp 1092-1097, December 2012.

[7] Manoj kumar Ramaiya , Naveen Hemrajani ,Anil Kishore Saxena "Security Improvisation in Image Steganography using DES"*Advance Computing Conference (IACC), 3rd International Conference* on 22-23),pp 1094 – 1099, Feb 2012.

[8] Nedal M. S. Kafri and Hani Y .suleiman "Bit-4 of Frequency Domain – DCT Steganography Technique", *Networked Digital Technologies, International Conference on 28-31*,pp 299-304 ,July 2009.

[9] Sachin.A. Thanekar , Ms. Soudamini S. pawar "OCTA (STAR) PVD A Different Approach of Image Steganography" *Computational Intelligence and Computing Research (ICCIC) ,IEEE conference on* 26-28,pp 1-5, Dec 2013.

[10]Anjali A.Shejul and PROF. U.L Kulkani "A DWT based Approach for Steganography using Biometrics" *Data Storage and Data Engineering (DSDE), International Conference on* 9-10 Feb, pp 10 39 – 43,feb 2010.

[11]Abbas Cheddad , joan Condell , Kevin Curran , Paul Mc Kevitt "A skin tone detection algorithm for an adaptive approach steganography" Elsevier B.V,pp 2465- 2478 ,July 2009.

[12]Nidhi Grover and A.K. Mohapatra "Digital Image Authentication Model Based on Edge Adaptive Steganography",*Advanced Computing ,Networking and Security (ADCONS), International Conference on* 15-17, pp 238 - 248, 2013.

[13]Lifang Yu, Yao Zhao, Rongrong Ni , Ting Li "Improved Adaptive LSB Steganography Based On Chaos and Genetic Agorithm" EURASIP Journal on Advances in Signal Processing volume 10,pp 1-6, May 2010

[14]Neil F. Johnson and Sushil Jajodia "Exploring Steganography: seeing the Unseen". in proceeding of the IEEE signal processing letters vol9 26 - 34, 1998.

[15]T.Morkel, J.H.P. Eloff, M.S. Oliver "An Overview Of Image Steganography, " *in proceedings of the Fifth Annual Information Security South Africa Conference*, July 2005.

[16]Anjali A .Shejul, Umesh L. Kulkarni "A Secure Skin Tone Based Steganography Using Wavelet Transform*" IJCTE,* pp 16 - 22, july 2011.

[17]Amrita Khamruia,, J K Mandalb "A Genetic Algorithm Based Steganography Using Discrete Cosine Transform" *International Conference on Computational Intelligence: Modeling Techniques and Applications(CIMTA)* pp 105-111,Dec 2013.

[18]Po-Yueh Chen, Hung-Ju Lin"A DWT Based Approach for Image Steganography" International Journal of Applied Science and Engineering pp 275-290,Dec 2006.

[19]Chi-Kwong Chan and L.M. Cheng "Hiding data in images by simple LSB substitution" *Elsevier international conference, pp* 469 – 474, 2004.

[20]G. Simmons, "The prisoners problem and the subliminal channel" In Advances in Cryptology CRYPTO, pp 51 –67, 1983.