Monika Sahu al. International Journal of Recent Research Aspects ISSN: 2349-7688, Vol. 2, Issue 2, June 2015, pp. 21-25

Review of Image Steganography Techniques in Cloud Security

Monika Sahu

Assistant Professor, Tek Chand Mann College of Engineering, Sonipat, Haryana (India)

***Abstract*— Steganography is art of hiding secret information in a cover media in such a way that it is not detectable to anyone. Owing to their easy availability and popularity on internet, digital images are most commonly used coverage medium in steganography. There exist a number of image steganography techniques for hiding secret information in image. Some techniques are more complex than others and each of these have its own strong and weak points. Depending upon the need of a particular application, different steganography techniques are used for different applications. This paper intends to give an overview of different image steganography techniques along with its advantages and disadvantages**

***Keywords*— Neural Network, Forecasting, Machine learning.**

I. INTRODUCTION

In past few decades, due to several advancements in network and digital technology, it has become very popular & suitable to transmit the digital data from one end to another end over internet. This communication of information needs to be secure and thus the importance of information security has been significantly increased. Information security can be achieved by using cryptography and steganography (information hiding) techniques. Steganography is often confused with Cryptography, though they are really different terms. Cryptography deals with privacy while steganography deals with secrecy. Cryptography protects the contents of message by transforming them into cipher text via some cipher algorithm with/without using a key. Yet it gives the output that is scrambled and unreadable, but suspicious enough to attract interceptors' attention. To overcome this problem, a new security approach called "Steganography" came into existence. The word Steganography is taken from two Greek words "stegos" meaning "cover" and "grafia" meaning "writing", defining it as "covered writing" [10]Steganography is the art of hiding secret messages within another seemingly innocuous message, or carrier [9]. ". People have been using various forms of hiding information since ages. The steganography technique is now extremely used in computers files with digital data as the carrier and networks as high-speed communication channels.

Steganography deals with embedding secret information in a given media (called cover media) without making any visible changes to it. The goal is to hide a message within the cover media such that the existence of the secret message is concealed [6].

Commonly used terms in steganography field are: cover media, this is the media that will hold the confidential information. Secret message, this may be text, image or any type of data that we want to hide in the cover media. Stego media, this is the cover media with secret message embedded into it. This is actually what any casual observer can see. Stego-key optional), this is needed to hide and extract the secret message from the stego-media.

Formally, steganographic technique can be written in form of a formula:

Cover_media+Secret_message=Stego_media

The graphical view of Steganographic system is shown in fig.1.

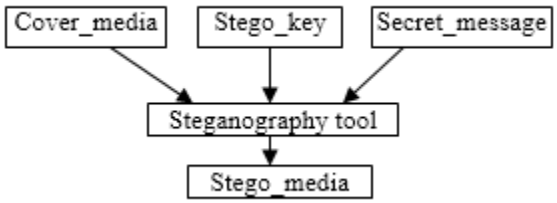

Fig.1 Graphical view of Steganographic system

The hidden message may be simple text, image or other multimedia that can be represented in the form of a bit stream. In steganography, possible cover media could be an image, audio, video, text or some other digital means which can hide the secret information. Images are most popular cover media used for information hiding. The reason behind this is that the human visual system (HVS) cannot detect the difference between an original image and a stego image when secret information is properly embedded in cover image.

In this paper, main focus is on digital image hiding. This paper intends to provide an overview of the different techniques used for image steganography.

In this paper, main focus is on digital image hiding. This paper intends to provide an overview of the different techniques used for image steganography.

II. IMAGE STEGANOGRAPHY

Images are most popular digital file format used in steganography. In image steganography, a secret message is embedded in a digital image which is referred to as cover image with the help of an embedding algorithm, using an

optional secret key. The resulting stego image is then transmitted to the receiver. At the receiver end, secret image is retrieved from the stego image by the extraction algorithm using the same secret key.

In a computer, an image file is represented as a collection of numbers which corresponds to the light intensity values in different parts of the image file. This numeric illustration forms a grid and the single points are termed as pixels. For a typical Gray Scale Image, 8 bits/pixel are used to represent it. For a digital color image, 24 bits/pixel, and RGB color model is used, also known as true color. Almost, all the color variations for the pixels of a 24-bit image are derived from three primary colors: red, green, and blue, and each of these colors is represented by 8 bits. Thus in any given pixel, 256 different shades of red, green and blue color are possible adding up to more than 16 million possible combinations that finally results into 16 million different colors[7].

Several techniques can be used to reduce the size of an image file so that file can be sent over internet in a practical amount of time. All of these techniques make use of some mathematical formulas to compress an image file. Two types of compression techniques used for image files are: lossless compression & lossy compression.

In Lossless compression, no information is removed from the original image. The original image's integrity is preserved and original image can be easily recreated from the compressed image. Image formats that use lossless compression are GIF (Graphics Interchange Format) and BMP (bitmap file).

In Lossy compression, smaller files are created by discarding the points that are too small for human eyes to discriminate. This results into an image which is something similar to the original image, but not the same as the original. This compression technique is used by JPEG file format [7].

A number of different steganographic techniques exist for different image file formats being used, each of which allow us to hide confidential data in an image file format.Image steganographic techniques are basically categorized as:

Spatial domain techniques;

Transform domain techniques;

Masking and Filtering.

The next section gives brief idea about each of these image steganographic techniques.

III. IMAGE STEGANOGRAPHY TECHNIQUES

Spatial Domain Techniques

In this approach, secret messages are directly embedded into pixel values of cover image. The most popular and simplest Steganography method used to hide secret message in cover image is the least significant bits (LSB) insertion technique. In the LSB insertion technique, Least Significant Bits of some or all of the pixels of cover image are replaced by the bits of the secret data. Pixels of cover image are selected either sequentially or randomly. If the LSB bits which have minimum weighting are changed, the image distortion caused is not observable by a human naked eye. Considering the eye imperceptions LSB technique is extensively used to hide the secret data. Sometimes key is also embedded in the image itself, thus making it more difficult for the intruder to extract the hidden message from the image.

If a 24-bit image is used to hide the secret data, a bit of each of the red, green and blue colour channels of a pixel can be used, as each of these channels is represented by a byte. So, one can store 3 bits per pixel. A 128X128 pixel image, can thus store a total amount of 49152 bits or 6144 bytes of secret data. Let us take an example of a grid for 3 pixels of a 24-bit image which can be represented as follows:

(00100111 11101001 11001000)
(00100111 11001000 11101001)
(11001000 00100111 11101001)

The binary value for A is 10000001. When this binary value of A is inserted, resulting three pixels would be:

(00100111 11101000 11001000)
(00100110 11001000 11101000)
(11001000 00100111 11101001)
(01101100 10001111 01101011)

While the number is embedded using the first 8 bytes of the grid, only the 3 underlined and highlighted bits needs to be changed. Therefore on an average, only half of the bits in a cover image will need to be changed to hide a covert message [1]. Since there are 256 possible intensity values of each primary colour, modifying the LSB of a pixel would result into a small change in the intensity of the colour. Such changes cannot be easily noticed by a human naked eye, and results into successfully hiding of the secret message. With a carefully-chosen image, it is possible to hide the information in the least and second or even up to third to least significant bit and still the difference cannot be visible [10].

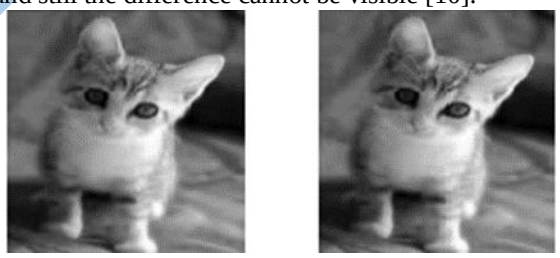

Fig. 2 (a) Cover Image (b) Stego Image (after inserting A)

In the above specified example, consecutive bytes of the cover image i.e. from the first byte to the last byte of the cover message are used to hide the secret information. This technique is very easy to detect. More security can be added to the system if sender and receiver share a secret key that specifies some technique by which only certain pixels to be changed.

In general, LSB uses images of BMP file format, as they use lossless compression. However, to be able to hide a secret data inside a BMP file format, a very large cover image is required. Nowadays, BMP images of 800 × 600 pixels are not commonly used on the Internet and might cause a doubt in mind of an observer. Due to this reason, LSB steganography has also been developed to be used with other image file formats [10].

This method has several implementation versions that provide improvisation to the algorithm in various aspects. Though this method is simpler, but has a larger impact as compared to the other method.

A better steganographic method to hide secret information into a RGB color cover image was proposed by Ankita Gangwar and Vishal Shrivastava. They proposed a method for Least Significant Bit (LSB) based on image steganography that improves the existing LSB substitution techniques to enhance the security level of hidden information [2]. It is a new approach for substituting LSB of RGB color image. The proposed algorithm hides the secret data within the LSB of the image where a secret key encrypts the secret data to protect it from illegitimate users. In their paper, secret data is embedded into different position of LSB of image depending on the secret key. Accordingly, it is difficult to recover the hidden information knowing the retrieval methods. The use of the secret key provides an extra way to secure the information from illegal user.

Several spatial domain techniques were also proposed utilizing edge features of an image for hiding secret information. One such technique was proposed by Xin Liao, Qiao-yan Wen and Jie Zhang. Their steganographic method was based on four-pixel differencing and modified least significant bit (LSB) substitution [11]. Their method considers the features of edge, so the pixels in edge areas can tolerate much more changes without making visible distortion. The average difference value of a four-pixel block is used to categorize the block either as a smooth area or an edge area. Every pixel hides the secret data by using k-bit modified LSB substitution method, where k is decided by the level into which the average difference value falls. Readjustment is executed to make sure that the average difference value belongs to the same level before and after embedding, as well as to minimize the distortion. By showing that the readjustment procedure works, a theoretical proof has been provided to validate that the method succeeded in embedding and extracting. Experimental results show that the proposed method has an acceptable image quality as well as provides a large hiding capacity. However method lacks in attack-resistance capability a little in order to provide good imperceptibility and capacity. In 2012, Amitava Nag, Saswati Ghosh, Sushanta Biswas, Debasree Sarkar and Partha Pratim Sarkar, also proposed an Image steganography technique based on LSB using X-box mapping where some X-boxes having unique data are used [1]. The 8-bit greyscale secret image is embedded in greyscale cover image using this Steganography algorithm, where four unique X-boxes with 16 different values (expressed by 4- bits) are used and each value is mapped to the four LSBs of the cover image. Such mapping provides enough security to the secret information because without any information of mapping rules, it is not possible for anyone to extract the secret information.

However simple LSB insertion is easy to implement and good for steganography, but we can try to minimize one of its drawbacks: the ease of extraction. This drawback can be improved by developing modified LSB insertion techniques that makes use of several features and properties of images as well with help of some form of secret key, thereby providing more security and imperceptibility.

Transform Domain Techniques

In this approach, secret information is embedded in the transform coefficients of the cover image, i.e. cover image is first transformed and then secret information is embedded. The transformation may be either Discrete Cosine Transform (DCT), or Discrete Wavelet Transform (DWT).

The more complex way of hiding a secret data inside a cover image makes use of discrete cosine transformations. LSB insertion technique for images does not provide good results if any type of compression is done on the resulting stego-image e.g. JPEG, GIF etc. Discrete cosine transformations (DST)), are used by the JPEG images to attain compression. DCT transforms successive 8 x 8 pixel blocks of the image into 64 DCT coefficients each. Each of such DCT coefficients Sij of an 8 x 8 block of image pixels is given by:

$$Sij=1/(4\ CjCi \sum_{x=0}^{7}\sum_{y=0}^{7}(Pxy \cos[(2x+1)j\pi/16]\ \cos[(2y+1)i\pi/16]))$$

where Ci, Cj = $1/\sqrt{2}$ when i, j equals 0 and Ci, Cj = 1 otherwise. After the coefficients have been calculated, quantizing operation is performed.

Even though a change of a single DCT affects all 64 image pixels, the LSB of the quantized DCT coefficient can be used to hide information [3].

DCT is a lossy compression transform because the cosine values cannot be calculated accurately, and repetitive calculations using limited precision numbers gives rounding errors into the final result. Further, difference between original data values and restored data values depend on the mode used to calculate the DCT [5]. This technique is widely used because of its independency over the image formats. Transform domain works well for both lossy and lossless compression images.

At ARES 2010, Zahra Toony and Mansour Jamzad, proposed a new image hiding scheme based on seam carving method in which, the secret image is first classified on basis of image complexity measure [13]. Then image is resized to an appropriate smaller size while preserving the important contents of the image using seam carving method. The resultant smaller size image is then embedded in a cover image. Hiding a smaller image causes less distortion in the cover-image and hence a higher quality stego image is obtained. The proposed method provides higher embedding rate and enhanced security. Future work included comparing proposed method with others by considering several quality measurement methods. YongHong ZHANG, also proposed an image hiding scheme by using the curvelet transform [12]. First of all, Arnold transform is applied to the secret image and the image is gained. Digital curvelet transform is then applied to the secret image and cover image and their coefficients are obtained; thereafter their respective curvelet

coefficients are interpolated. Finally, the stego image is constructed by using Inverse digital curvelet transform. Original secret image can be extracted from stego image by applying reverse of above specified procedure. This scheme gives better speed and security.

Masking and Filtering Method

Masking and filtering is a steganography technique which is mainly used on images with 24 bits per pixel. This technique can be applied on color as well as grey scale images. It hides information in much similar way to that of placing watermarks on an image and are every so often used as digital watermarks. Masking images involves changing the luminance of the masked area. Lesser the change in luminance, lesser is the chances that it can be perceived. Masking is stronger than LSB insertion in respect of compression, cropping, and some image processing. These techniques insert information in significant areas and thus are more suitable with, lossy JPEG images.

Fig.3 demonstrates how masks and filters can be embedded into images without harming the original quality of the image. The whole image has been watermarked. This prevents image from being illegitimately copied, edited or used in any other application for which it was not planned to be used. Slightly varying the luminosity and opacity of the watermark layers provide different results. The image on the left side has opacity of zero percent. The opacity is steadily increased until the watermark layer becomes visible [8]. Thus, using masks and filters preserves the original image quality, but forbids anyone from using the image for any unintentional purpose.

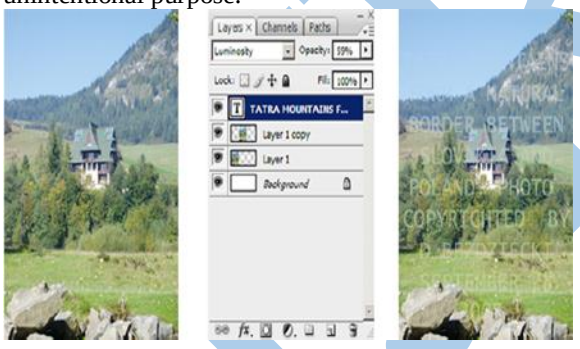

Fig.3 Masking and Filtering Method

IV. PERFORMANCE ANALYSIS METRICS

Three common parameters namely imperceptibility, capacity, and security, are used to analyse the performance of steganographic techniques.

PSNR (Peak Signal-to-Noise Ratio) is used as a parameter to measure the amount of imperceptibility and is expressed in decibels. It is the measurement of the quality between the cover image and stego-image. The larger PSNR value means there is only little differentiation between the cover-image and the stego-image. On the other hand, a smaller PSNR value means there is enormous distortion among the cover-image and the stego-image. Steganographic algorithm aims at providing a large PSNR value. PSNR is given by:

PSNR = 10*log10 (255*255/MSE).

where MSE stands for mean squared error. It gives the difference between the stego image and its original image. The better the stego image quality is, the lower the MSE value will be. MSE is given by:

MSE= 1/H*W {sum (square [M1 (i, j)-M2 (i, j)])}

where H and W are the number of rows and number of columns respectively of the cover image, M1 (i, j) stands for the pixel of cover image at (i, j) position and M2 (i, j) stands for the pixel of stego image at (i, j) position.

The second parameter is hiding capacity. The hiding capacity specifies the most number of bits that can be hidden in the cover image with an acceptable quality of resultant stego-image. A scheme is futile if the resultant stego-image is too much distorted as compared to original image regardless of the fact that it can hold a large amount of secret data. The hiding capacity (H.C.) is calculated for each image as a percentage of the cover image size.

Each of the above steganographic techniques with its advantages and disadvantages is listed in the table 1.

Sr. No	Name of Technique	Advantages	Disadvantages
1	Spatial domain technique	i) Image quality is not changed for any algorithm that uses spatial method. Less degradation of Original Image. ii) The large capacity of data can be stored.	i) Editing the image leads the image to lose its secret data. Less robust.
2	Masking and Filtering	i) Even though the image is compressed data is not affected. ii) The information hiding done in visible parts of the image.	These techniques can be applied only to gray Scale images and restricted to 24 bits.
3	Transform Domain Technique	i) To hide data in most significant areas of the cover-image, it makes them more robust from attack.	These method types are computationally very complex to implement.

		ii) It can be applied changes for the whole image.	

Table 1 Comparison of Image Steganographic Techniques [4]

V. CONCLUSION

This paper reviewed the major steganographic techniques. All of these techniques try to satisfy the three most important factors of steganographic design (imperceptibility, capacity, and security). We have seen that each of above discussed techniques can be applied, with a varying degree of success. Though spatial domain techniques have large data hiding capacity but these techniques often fail to prevent statistical attacks. On the other hand, DCT based domain techniques are less prone to attacks than the spatial domain methods, but they provide a small hiding capacity.

Thus we can conclude that some techniques are more complex than others and each of these have its own strong and weak points. Depending upon the need of a particular application, different steganographic techniques are used for different applications.

REFERENCES:

[1]. Amitava Nag, Saswati Ghosh, Sushanta Biswas, Debasree Sarkar, Partha Pratim Sarkar 2012, "An Image Steganography Technique using X-Box Mapping", IEEE Xplore Digital Library, International Conference On Advances In Engineering, Science And Management (ICAESM - 2012) March 30, 31, 2012.

[2]. Ankita Gangwar, Vishal Shrivastava, "Improved RGB -LSB Steganography Using Secret Key", International Journal of Computer Trends and Technology- volume4Issue2- 2013.

[3]. B.Swathi, K.Shalini, K. Naga Prasanthi, "A REVIEW ON STEGANOGRAPHY USING IMAGES", Asian Journal of Computer Science and Information Technology 2: 8 (2012) 234 – 237.

[4]. C.Gayathri, V.Kalpana, "Study on Image Steganography Techniques", International Journal of Engineering and Technology (IJET), Vol. 5 No 2 Apr-May 2013.

[5]. Johnson, N. F. and Jajodia, S., "Exploring steganography: Seeing the unseen. Computer", 1998, 31(2):26–34.

[6]. MOHAMMAD TANVIR PARVEZ, ADNAN ABDUL-AZIZ GUTUB" Vibrant Color Image Steganography using Channel Differences and Secret Data Distribution" Kuwait Journal of Science and Engineering (KJSE), vol. 38, issue 1, 2011.

[7]. Nagham Hamid, Abid Yahya, R. Badlishah Ahmad, Osamah M. Al-Qershi, 2012, "Image Steganography Techniques: An Overview", IJCSS, Vol. 6, Issue 3.

[8]. Pradeep Kumar Saraswat, Dr. R. K. Gupta, "A Review of Digital Image Steganography", Journal of Pure and Applied Science & Technology, Vol. 2(1), Jan 2012, pp. 98-106.

[9]. Richerd A. Mllin "An Introduction to Cryptography" Second Edition Discrete Mathematics and its application Series Editor Kenneth H. Rosen 2007 by Taylor & Francis Group, LLC www. copyright.com (http://www.copyright.com/).

[10]. T. Morkel, J.H.P. Eloff , M.S. Olivier, 2005, "An Overview of Image Steganography," in Proceedings of the Fifth Annual Information Security South Africa Conference (ISSA2005), Sandton, South Africa.

[11]. Xin Liao, Qiao-yan Wen, Jie Zhang, "A steganographic method for digital images with four-pixel differencing and modified LSB substitution", J. Visual Communication and Image Representation 22(1): 1-8 (2011).

[12]. YongHong ZHANG, 2011, "Digital Image hiding using curvelet transform", IEEE Xplore Digital Library, International Conference on Computer Science and Automation Engineering (CSAE 2011).

[13]. Zahra Toony, Mansour Jamzad, 2010, "A Novel Image Hiding Scheme Using Content Aware Seam Carving Method", IEEE Xplore Digital Library, International Conference on Availability, Reliability and Security (ARES 2010)Journal of Wildfire,15:121—135,200

