Indian Journal of Science and Technology, Vol 9(47), DOI: 10.17485/ijst/2016/v9i47/106446, December 2016
ISSN (Print) : 0974-6846
ISSN (Online) : 0974-5645

Review on Image Steganography

Ch. Yashwanth Roy* and Mohit Kumar Goel

Department of Electronics and Communications Engineering, Lovely Professional University, Phagwara - 144411, Punjab, India; yashwanthroy.ch@gmail.com, mohit.16907@lpu.co.in

Abstract

In this modern world of emerging technologies day by day, as the technology advances the need for secure communication over the internet also arises as a major need. Steganography is the technique that provides the base for secure communication. It is the art of hiding information in some other means of false medium for making a possible secure communication. The information to be hidden can be of any form such as image, text and video etc. and so the cover medium. Unlike cryptography, in steganography after the data is successfully hidden it is not even visible to the eavesdropper or the intruder which makes this technique safer and secure to follow. This review includes all about the major steganography techniques in spatial and transformational domain keeping the main focus on image steganography

Keywords: Cover Image, Frequency Domain, LSB, Stego-Image, Spatial Domain

1. Introduction

Steganography is the word derived from two Greek words "steganos" and "graphie" meaning "concealed writing". It is the art of hiding any kind of digital information in any other cover medium. This technique isn't a modern one, it was used from the ancient times. The cover medium can be any such as text, image or video. In ancient times people used wax tablets as a cover medium, used invisible inks, or encrypt the information with some codes and many more ancient techniques were used those days. In this digitalized era techniques have changed but the purpose always remained the same. So the cover mediums were also changed to digital mediums like image, video etc. In general any digital means can be used to hide the information, but at the same time the digital means with high degree of redundancy is more suitable. Here redundancy is with respect to the redundant bits that can be altered without being noticed.

This need is served by a digital image which has high redundancy. An image can be a color image, black and white image or a grayscale image. A color image comprises of three planes and are red, green, and blue and each plane is composed of M x N pixels and with pixel values of 0-255, whereas a grayscale image consists of only one plane with pixel values ranging from 0-128.

Video is another digital medium that supports steganography. Videos are considered more than images for hiding due to their high degree of spatial and temporal redundancy. Generally a video can be visualized a sequence of images running per second. A normal video consists of 25 frames per second. When compared with image steganography the probability of detection of hidden data in a video is less, but however there are also different attacks that can be applied on each single frame of a video like changing frame rates, lossy compression, interchanging the formats and addition or deletion of the frames during video processing. In case of video the hiding capacity is much higher than that of an image. Using videos for hiding provides a new dimension for hiding the data such as hiding in the motion components of the video or in the audio components of the video.

There are two more technologies that are similar to that of steganography but are very different and their purpose is far different from that of steganography. Cryptography is the art of encrypting the data and making it very difficult to understand, in this case the message is in scrambled form or encrypted form that is not

*Author for correspondence

understandable but the existence of message is visible to everyone unlike steganography. This technology although is used for secure communication purpose but since it is visible the intruder may get an idea of whether communication is taking place or not. The second technology is watermarking, this is done to protect the intellectual property of a customer and is used such that to find out false customers who break the license of any product and supply them to third parties.

2. Basic Steganography Model

A basic steganography model consists of secret information to be hidden, a cover image, stego-key and stego-image and of course algorithms for embedding the secret information and to extract the same from the stego-image. Let us say M represents the secret information to be hidden or the secret message and X be the cover image and K be the stego-image. Then the stego-image Y with the secret information in it can be represented as,

Y = F (M, K, X), where F is embedding algorithm.

For extracting the message again from stego-image Y the same can be represented as,

M=G (Y, K), where G is extraction algorithm. The same can be visualized with the help of figure below.

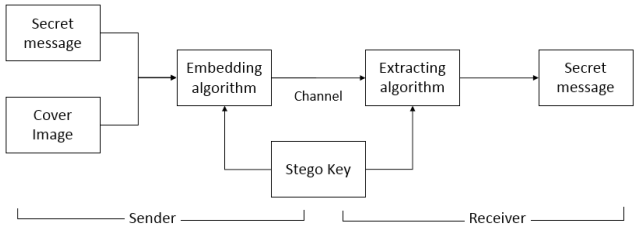

Figure 1. A basic steganography model.

3. Basic Methodology of Hiding the Data - LSB Technique

The basic technique of hiding the data in an image is the least significant method technique in which the data to be hidden is converted into binary form and each bit then is hidden or replaced by the LSB bit of pixel value. Not only one least significant bit but also two or three LSB bits can be used for hiding depending upon the embedding capacity and the quality required by the stego-image after hiding process is done.

For example if the data to be hidden is 'Y'. First the data is converted to binary format which is the ASCII value of the character 'Y' (ASCII - 89 – 01011001) now take a pixel say it as following values in binary.

```
( 00101100   01011111   01111110 )
( 00111010   00001110   11100110 )
( 01001111   11010000   01110010 )
```

Figure 2. Three pixel values in binary.

```
( 00101100   01011111   01111110 )
( 00111011   00001111   11100110 )
( 01001110   11010001   01110010 )
```

Figure 3. Three pixel values after hiding data in LSB.

As in Fig. 3, the values of the pixel are changed at LSB according to the data. The LSB bit with green color indicated that the value of the pixel hasn't changed even after hiding the data since the data bit and the LSB bit of the pixel are same. And the red color indicates that the pixel value has changed because of the data bit is not equal to that of the LSB bit of the pixel value.

4. Parameters to Measure Performance of a Steganography Technique

The performance of any steganography technique can be calculated or measured with some parameters and they are 1) security 2) capacity and 3) imperceptibility, these three are main parameters and two more parameters recently joined the list and they are 4) computational complexity and 5) temper resistance. Capacity is that how many data bits that can be hidden in the cover medium. Security is how secure the data is from the transformations done on the stego image such as cropping, filtering, scaling, addition of noise, and on steganalysis (art of identifying images with data).

There are various kinds of attacks that can be performed in order to get the hidden message from the stego-image. This process is of identifying the stego-images with hidden message is called as Steganalysis. Although steganalysis is not considered about extracting the image but identifying the stego-image with hidden message and then trying to extract the hidden message from it by applying various decoding algorithms. The different kind of attacks of steganalysis are 1) steganography-only attack, 2) known

carrier attack, 3) chosen steganography attack, and 4) known steganography attack. Only the stego-image is available with the intruder in "steganography-only attack" for steganalysis. In "known carrier attack" both the cover image and the stego-image are available for steganalysis. In "chosen steganography attack" the steganographic algorithm is available for steganalysis and in "known steganography attack" all the three sources, the cover image, stego-image and the steganographic algorithm is available for steganalysis.

The term imperceptibility refers to the perceptual transparency and temper resistance is the endurance of your secret message when an attempt is done to change it. The change in the cover image before and after the data has been hidden i.e. the distortion can be calculated with some parameters like peak signal-to-noise ratio (PSNR), mean square error (MSE), and correlation (r).

If X is an image of size M x N and Y be the image after hiding data bits in X i.e. stego-image and let X_{ij} and Y_{ij} are the pixel values at i^{th} row and j^{th} column. Then the formulas to calculate distortion parameters can be given as,

$$MSE = \frac{1}{M \times N} \sum_{i=1}^{M} \sum_{j=1}^{N} \left(X_{ij} - Y_{j} \right)^2 \quad (1)$$

$$PSNR = 10 \times \log_{10} \frac{C_{\max}^2}{MSE} \quad (2)$$

Where C_{max} is actual maximum pixel value in the cover image.

5. Classification of Steganography Techniques

Steganography techniques are broadly classified into two domains, one is steganography in spatial domain and the other is steganography in transformational (frequency) domain. Both the domains have their own pros and cons and any one of them can be selected depending on the performance parameters required by the technique. There are many techniques proposed in both the domains respectively.

6. Spatial Domain Techniques

In this domain the least significant bits (LSB's) of the pixel values of the cover image are used to hide the message bits without any transformation directly. In this techniques the security thereby depends on the pattern in which we are hiding the bits. In comparison with the transformational domain techniques the spatial domain techniques can embed high capacity of data into the cover image.

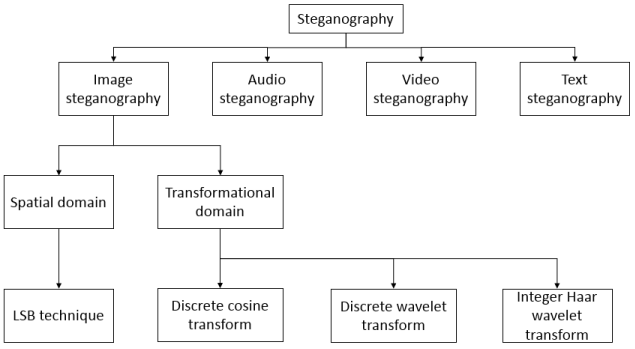

Figure 4. Classification of steganography techniques and their basic methodologies.

M. Radhika et al. have proposed a technique for an innovative approach for pattern based image steganography in which the message data is hidden in the cover image according to some pattern[1]. The pattern in this method goes like, first the cover image is divided into non-overlapping blocks of size 25x25 and within each 25x25 block the block is further divided into 5x5 non-overlapping sub blocks. Now the 25x25 blocks are selected by a pattern letter 'Z' and the 5x5 blocks within the 25x25 block are selected by the pattern ∝ and then LSB technique is used to hide the data. The two patterns can be used as two keys which improves security.

Nadeem Akhtar et al. have proposed a technique for an improved inverted LSB image steganography to improve the quality of the stego image[2]. In this method the LSB's of some of the pixels of the cover image are inverted if they occur with a particular pattern, by this way less number of pixels are changed thereby improving the quality of the stego image.

P Sandeep Reddy et al. have proposed a technique for hiding image in video in which the algorithm uses gray codes and secret keys for hiding the data securely[3]. The algorithm takes any input image of any format like .jpg, .png, .tiff, .bmp etc. and this input image is converted to bmp format because of the reason bmp file format uses lossless compression so that the compression of .bmp image does not lose any information.

7. Transformational Domain Techniques

In transformational domain, firstly some transformation methods like Discrete wavelet transform (DWT), Discrete cosine transform (DCT), Integer wavelet transform (IWT), Fractional Fourier transform (FrFT) or Discrete

curvelet transforms (DCVT) are used to transform the cover image to frequency domain and then the data bits are embedded onto it. This method is more secure as compared to spatial techniques but has less capacity. The basic LSB technique used in spatial domain has weak resistance to attacks, so as to overcome this problem many other techniques and algorithms were found by the researchers. The cover image can be transformed to frequency domain using many methods like Discrete cosine transform (DCT), Discrete wavelet transform (DWT), Integer wavelet transform (IWT), Fractional Fourier transform (FrFT) and Discrete curvelet transforms (DCVT).

K B Shiva Kumar et al. have proposed a method for bit length replacement steganography based on DCT coefficients[4]. In this method the cover image is converted to frequency domain using 2D - Discrete cosine transform (DCT). After performing 2D-DCT and getting the coefficients a coherent bit length is calculated which determines the number of LSB bits of the each DCT coefficients can be used for hiding the MSB bits of data or message. And then the data is hidden and finally the IDCT is performed on the stego image which is in the transform domain.

Barnali Gupta Banik et al. have proposed a technique for image steganography algorithm using scrambled image and quantization coefficient modification in DCT[5]. In this method the secret image is scrambled by Arnold transform before embedding. DCT is performed on the cover image and the DCT coefficients are modified according to the scrambled message data and then inverse DCT is applied to get the stego image.

Neda Raftari et al. have proposed a technique for digital image steganography based on assignment algorithm and combination of DCT-IWT[6]. In this method DCT is applied on the secret image and 2D Haar integer wavelet transform on the cover image and the DCT coefficients of the secret image. Now for embedding the data, best matched blocks are found using the root mean square error technique and Munkres' assignment algorithm. After this apply inverse Haar integer wavelet to get the stego-image. So this method is towards the improvement of the security.

Prajanto Wahyu Adi et al. have proposed a technique for a high quality image steganography by integer Haar wavelet transform using modulus function[7] in which a random 8 bit unsigned key is used to scramble the message or encrypt the message. Now IHWT – integer Haar wavelet transform on the cover image is performed and modulus operation is used to embed the data. After the embedding is done perform inverse integer Haar wavelet transform to obtain the stego image. Therefore by this proposed method the quality of the image is increased which improves the imperceptibility of the image.

Mohammad Reza Dastjani Farahani et al. have proposed a technique for a DWT Based Perfect Secure and High Capacity Image Steganography[8]. In this a same level DWT is applied to the cover image and the message data. For embedding the data most similar blocks are found using root mean square error (RMSE) pattern matching distance criterion and numbers of these blocks are saved as keys. According to this there is no combination or replacement between the message or the cover image DWT coefficients, therefore the cover image will remain unchanged. Hence the reason this method is called as perfect square method. This method has high capacity and also security is enhanced.

Sudhir Keshari et al. have proposed a technique for Weighted Fractional Fourier Transform based Image Steganography in which the secret image to be sent is hidden in intermediate domain between spatial and frequency of the cover image by weighted fractional Fourier transform (WFRFT)[9]. In this method WFRFT is performed on cover image with a transform order *a*. For embedding the data LSB technique is used. In this method the key is the transform order *a* which the intruder does not know with what transform order WFRFT is performed and this is also an advantage over conventional Fourier transform. So here only security is enhanced.

Reba Mostafa et.al have proposed a technique for Hybrid curvelet transform and least significant bit for image steganography in which curvelet denoising is applied on the image as a pre-processing step to remove the noise from the cover image[10]. The cover image is then transformed into the frequency domain using curvelet transform. The message data to be hidden in the cover image is embedded in the curvelet coefficients without making any changes that can be noticeable in the cover image. Therefore in this method only quality is been improved.

8. Conclusion

Throughout this paper a brief introduction to steganography and different steganography techniques are reviewed, by which a basic ideology is provided on steganography. In spatial domain although there is a high payload or high capacity to embed the data this method is more prone to

attacks as it has weak resistance while the transformational domain techniques are less prone to attacks and other transforms on data especially when the data hidden is small but are of less payload or low capacity for embedding the data also these methods have less distortion of cover image and is more secure than spatial domain techniques. Steganography is not only for secure communication of data but can also be used for a secure storage system such as storing any valuable information in the database, e.g. e-commerce companies like flipkart, amazon and many more who store many customers valuable data in their databases can use steganography for hiding those information safely from intruders.

9. References

1. Radhika Mani M, Lalithya V, Swetha Rekha P. An innovative approach for pattern based image steganography. IEEE, presented at the Int Conf Signal Processing, Informatics, Communication and Energy Systems. 2015 Feb. p. 1–4.
2. Akhtar N, Khan S, Johri P. An improved inverted LSB image steganography. IEEE, Int Conf on Issues and Challenges in Intelligent Computing Techniques (ICICT), 2014 Feb. p. 749–55.
3. Sandeep Reddy P, Reddy K. Hiding image in video. International Journal of Research Sciences and Advanced Engineering (IJRSAE) TM. 2014 Oct – Dec; 2(8):87–91.
4. Shiva Kumar KB, Raja KB, Chhotaray RK, Pattanaik S. Bit length replacement steganography based on DCT coefficients. ResearchGate, International Journal of Engineering Science and Technology. 2010; 2(8):3561–70. ISSN: 0975-5462.
5. Banik BG, Bandyopadhyay SK. Implementation of image steganography algorithm using scrambled image and quantization coefficient modification in DCT. IEEE Int Conf on Research in Computational Intelligence and Communication Networks (ICRCICN). 2015 Nov. p. 400–5.
6. Raftari N, Eftekhari Moghadam AM. Digital Image Steganography Based on Assignment Algorithm and Combination of DCT-IWT. IEEE Fourth Int Conf on Computational Intelligence, Communication Systems and Networks. 2012 Jul. p. 295–300.
7. Adi PW, Rahmanti FZ, Abu NA. High Quality Image Steganography on Integer Haar Wavelet Transform using Modulus Function. IEEE Int Conf on Science in Information Technology (ICSITech). 2015 Oct. p. 79–84.
8. Dastjani Farahani MR, Pourmohammad A. A DWT Based Perfect Secure and High Capacity Image Steganography Method. IEEE Int Conf on Parallel and Distributed Computing, Applications and Technologies. 2013 Dec. p. 314–7.
9. Keshari S, Modani SG. Weighted Fractional Fourier Transform based Image Steganography. IEEE Int Conf on Recent Trends in Information Systems. 2011 Dec. p. 214–7.
10. Mostafa H, Ali AF, EI Taweal G. Hybrid curvelet transform and least significant bit for image steganography. IEEE Seventh Int Conf on Intelligent Computing and Information Systems (ICICIS'15). 2015 Dec. p. 300–5.