Complete Study On Different Methods For Producing Stegoimage

NEHA SAXENA

mailnehasaxena@yahoo.co.in

ABSTRACT

Steganography refers to the technique of hiding secret messages into media such as text, audio, image and video without any suspicion, while steganalysis is the art and science of detection of the presence of steganography. It can be used for the benefit of the mankind to serve us as well as by terrorists and criminals for malicious purposes. Both steganography and steganalysis have received a lot of attention from law enforcement and media. In the past, different steganographic techniques with properties of imperceptibility, undetectability, robustness and capacity have been proposed. Newer and more sophisticated steganographic techniques for embedding secret message will require more powerful steganalysis methods for detection. The battle between steganography and steganalysis is never ending. In this paper, an extensive review report is presented for steganography and steganalysis.

1. Background On Steganography

Steganography, the study of data hiding with the intent of sending a secret message, has become increasingly important over the last few years as the use of digital media, which provides ample space to hide the message, has become more popular. Generally, methods of image steganography hide messages by using redundancy in the image. The message will be visually imperceptible as long as the insertion of the message does not cause any noticeable changes to the original image. Of course, it may be possible to detect the message using other means. The study of detecting secret messages is called Steganalysis.

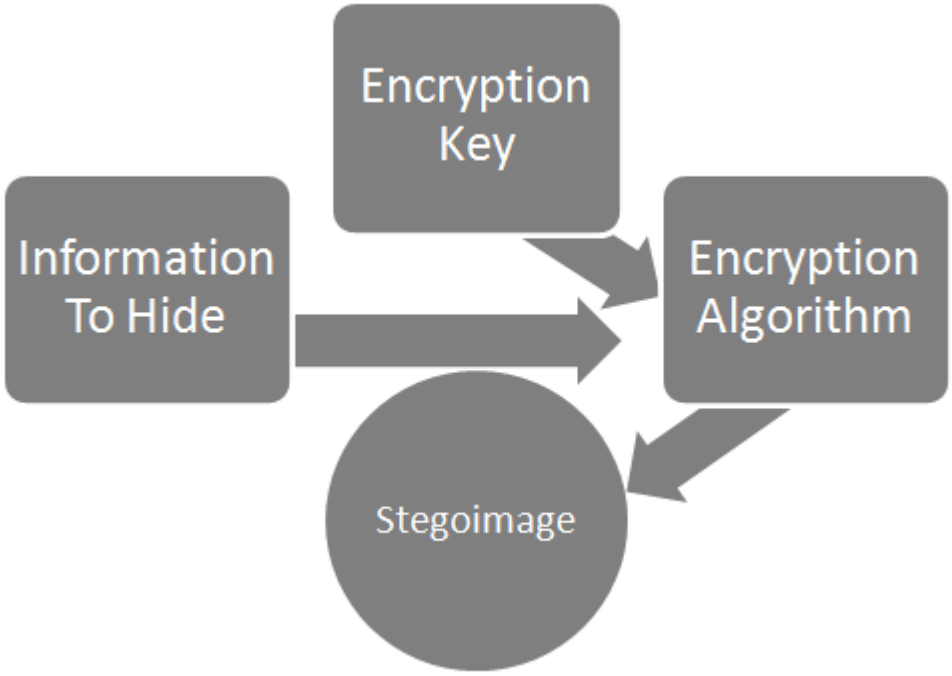
Of course cryptography already provides a means to send a secret message, but cryptography and steganography have different goals. Consider that the main goal of cryptography is to render a message unintelligible to a receiver who does not know the secret key required to decrypt the

message. This differs from the goal of steganography which is to conceal the fact that a message even exists. A common example to illustrate this difference, is that two prisoners Bob and Carl are conspiring to escape, but all their communications are being monitored by a warden Wendy. If Bob sends an encrypted message to Carl, Wendy will wonder what they are secretly discussing and cut off all communications between them. Obviously, Bob and Carl need to send messages to each other that will go undetected. If Bob and Carl have access to computers, they might choose to use an image from a website to hide their messages. Of course, Bob and Carl can still encrypt the message before hiding it in the image to ensure that if Wendy finds the hidden message she cannot read it.

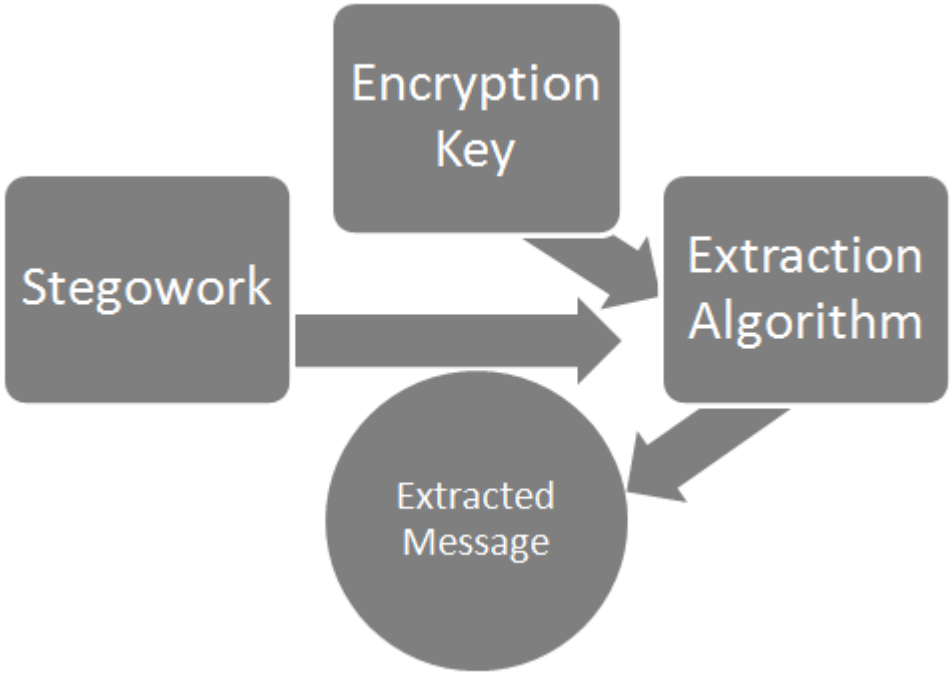
Digital data utilization along with the increased popularity of the internet has facilitated information sharing and distribution. Watermark, which is usually some information related to original data or the owner, is embedded in the original data; then the watermarked data is distributed throughout computer networks. Considering the applications of such systems, the watermark can be extracted from the media.

The Watermark and Steganography are similar but in different purpose. The main goal of watermarking is to embed information into image that cannot remove the information from image. The main goal of steganography is to embed information into image that cannot be detected. Hence the recent work that embed message into JPEG image does not consider the compression rate of JPEG image. However, the JPEG image is easily be compressed again such that the embed information will be destroy. The best way is to design a embed method between watermark and steganography, such that the cover image can resist the JPEG compression.

2.Digital Information Hiding Model



3. Digital Information Extraction model



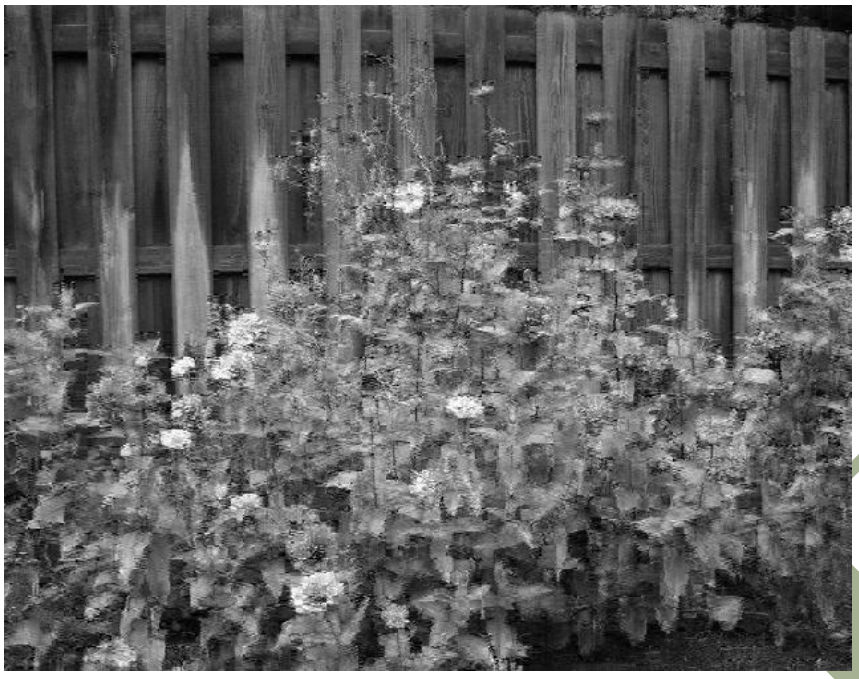
4. Classification Of Steganographic Techniques

There are three basic types of steganography: spatial steganography, transform steganography and adaptive steganography.

4.1 Spatial Steganography

There are many versions of spatial steganography, but all directly change some bits in the image pixel values in hiding data. Least significance bit (LSB)-based steganography is one of the simplest techniques that hides a secret message in the LSBs of pixel values without introducing many perceptible distortions. To our human eye, changes in the value of the LSB are imperceptible, thus making it an ideal place for hiding information without any perceptual change in the cover object. Embedding of message bits can be done either sequentially or randomly.

Original image



Stegoimage - 9x9 blocks, with the first column of each block preserved and message embedded in the other columns in the sign

4.2 Transform Based Steganography

4.2.1Discrete Cosine Transform

JPEG is based on DCT in lossy compression and it is the most common format of images produced by digital cameras, scanners and other photographic capture devices.

4.2.2 Discrete Fourier Transform-based Steganography

Fast Fourier transform is not suitable for hidden communication due to round-off errors .Johnson and Jajodia , and McKeon used DFT in Fourier-based steganography.

4.2.3 Discrete Wavelet Transform-based Steganography

DWT-based steganography is still in infancy. Bhattacharya et al develop a dual steganographic technique based on DWT and spread spectrum Two different secret images after converting into 1-D vectors are inserted into two high frequency components HL1 and HH1 of 1-level DWT of the cover images using pseudo random number generator and session key.

4.3 Adaptive Steganography

Some important requirements of a good steganographic scheme are undetectable, robustness against attacks, embedding capacity and imperceptibility. Adaptive steganography is a special case of the two former techniques and it tries to fulfill at least some or all requirements of a good steganographic scheme. LSB matching revisited (LSBMR) is another edge adaptive steganography technique, which can release more edge regions for embedding message bits. It can resist some of the steganalytic tools also.

The model-based method (MB1) generates a stego-image based on a given distribution model, using a generalized Cauchy distribution, which results in minimum distortion . This algorithm can be broken by the first-order difference .

5. Conclusions

This paper presents a background discussion on major algorithms of steganography and steganalysis for digital images. Some important algorithms of steganography in spatial domain are discussed in details with special emphasis so that researchers and steganalysts will have knowledge of how to develop such techniques. Different types of both specific and universal steganalytic techniques in spatial domain as well in transform are described in short in this paper.

6. References

1. U.C. Nirinjan, and D. Anand, Watermarking medical images with patient information, Proc. of 20th IEEE International Conference of Biological Society, pp. 703-706, 29 October – 1 November 1998.

2. Y. Li, C. Li and C. Wei, Protection of mammograms using blind steganography and watermarking, Proc. of IEEE ISIAS, pp. 496-499, 2007.

3. R. J. Anderson and F.A.P. Pettitcolas, On the limits of steganography, IEEE Journal on Selected Areas in Communication, vol. 16, no. 4, pp. 474-481, 1998.

4. H. Wang and S. Wang, Cyber warfare: Steganography vsSteganalysis, Communications of ACM, vol. 47, no. 10, pp. 76-82, 2004.

5. N. Provos and P. Honeyman, Hide and seek: An introduction to steganography, IEEE Security and Privacy, vol. 1, no. 3, pp. 32-44, 2003.

6. B. Lin, J. He, J. Huang and Y.Q. Shi, A survey on image steganography and steganalysis, Journal of Information Hiding and Multimedia Signal Processing, vol. 2, no. 2, pp. 142-172, April 2011.