Volume : 5 | Issue : 5 | May 2016 • ISSN No 2277 - 8179 | IF : 3.508 | IC Value : 69.48

Research Paper

Compare and Review of Various Steganalysis Security Techniques

Engineering

KEYWORDS : Steganalysis, PCA, CF, SURF.

Mr. Dinesh V. Patel C-201, HOMETOWN,NEAR SBI, NEW RANIP, AHMEDABAD- 382480

ABSTRACT

This paper provides the concepts of Steganalytic technique. Steganography is extensively used method in secure communication. In steganographic method one message is secretly embedded in an image so that the presence of this message is hidden from the viewers-users. Steganalysis is the technique of locating the existent of stego content in the image. A review and comparison of different steganalysis technique for different image formats embedded with stego content.

INTRODUCTION

Steganalysis is used to identify and evaluate the hidden information from mentioned data with less knowledge about the steganography algorithm. The idea of steganalysis is to fetch the sufficient evidence about the existence of embedded message. The use of Steganalysis is in terrorist activities, cybercrime, digital forensics and criminal activities over the internet. The aim of steganography is to hide data imperceptibly into a cover, so that the existence of hidden information cannot be identified. Steganalysis aims to exhibit the existence of hidden data.

It is complex problem because the original host information is not known. After finding the existence of hidden data in the image, it can be processed using various steganalysis methods. We can classified the steganalysis techniques in to two parts, Signature and statistical. Both can further divided into two parts, specific and universal. Universal steganalysis is also named as Blind steganalysis. Blind technique is uses to detect the existence of stego image without knowing the steganalysis method used to hide the image. Specific technique is also known as targeted steganalysis. It is used to crack message implant due to a particular steganographic technique. Generally, targeted steganalysis methods are more precise than the blind methods.

We have different image formats, the most important for cameras, printing, and scanning, are JPG images, Bitmap images, TIF images, PNG images, and GIF images. Bitmap and gif images are widely used formats. In bitmap image each pixel is assigned a specific bit to reflect a color. The resolution of the images is increase when increase the numbers of bits to represent the image. Bitmap images are created pixel-by-pixel so they can be easily edited. GIF images, Graphics Interchange Format, supports up to 8 bits per pixels for an image. GIF can have a palette of 24-bit colors and allows the image 256 colors. GIF is mostly used for logos and graphics.

B. BLIND IMAGE STEGANALYSIS TECHNIQUES

In this section we review and compare many different blind image steganalysis techniques for different types of images based on classification techniques.

1. A Universal Steganalysis to Steganographic Images on Frequency Domain[3]
The detection is accomplished based on the spectrum analysis of difference frequency histogram coefficient according to apparent spectrum difference between nonsteg and steg images. The physical frame of the algorithm is easy and the detection technique can be put into practice. Experiments show that the detection performance is good for detecting images of discrete cosine transform domain and discrete wavelet transform domain.

2. Characteristic Function Moments and PCA based image Steganalysis Method[4]
This scheme based on the characteristic function (CF) moments of three-level wavelet sub-bands including the further decomposition coefficients of the first scale diagonal sub-band. The first three statistical moments of each wavelet band of test images and prediction error image is selected to form 102 dimension features for steganalysis. PCA (Principal Components Analysis) is utilized to reduce the features and the support vector machine is adopted as the classifier.

3. Universal Steganographic Detection Algorithm in JPEG Image Using the Data Dependent Kernel[10]
This is a steganographic detection technique for JPEG image. It is based on the data dependent concept. In which first it get the beginning classifier by SVM training and the kernel function is changed with conformal modification by using the information of Support Vectors, retrain with the new kernel to increase the spacing around classification partition, loop until getting the best result.

4. Steganalysis Scheme Using the Difference Image of Calibrated Sub-sampling[9]
The steganalysis scheme use the various histogram and image calibration. The message embedding create the correlation with the adjacent pixels weakens and the random changes of the pixel values produce the block effects among the different pixels. The proposed technique crops a distrustful image by 1 pixel in a row or/and column direction and compares the difference histograms. Two distance measures (Manhattan and Euclidean distance) are engaged to assess the gap between the histograms and a SVM is used as classifier.

5. Comparison between Neural-Network, Steganalysis and Linear-Classification Method Steg detect[8]
Compared universal neural network classification and Steg detect - a linear classification tool. The results of this technique show that neural networks were better than the linear classification tool.

6. SURF: Steganalysis Using Random Forests[7]
SURF, Steganalysis using random forests, use HCS (Huffman Code Statistics) features and FR Index. FR index is the ratio of File size to Resolution. The SURF method proves random forest to be an efficient classifier for steganalysis.

7. Blind Detection for JPEG Steganography[6]
This method constructed 9 statistical models from the discrete cosine transform and decompressed spatial domain for a JPG image. By calculating the HCF (histogram characteristic function) and the COM (center of mass), the energy distribution of each model as one part of our feature set is calculated. Support vector machines are utilized to make classifiers.

8. Images Using Open Source Software[5]
Data mining tool developed in java. It used for comparing classification success and error rates. It also developed an application using Weka Java library for loading the data of the Images and categories the images.

Volume : 5 | Issue : 5 | May 2016 • ISSN No 2277 - 8179 | IF : 3.508 | IC Value : 69.48

9. Block-based Image Steganalysis algorithm[11]
This method classifies the image blocks into multiple classes on steganalysis results of decomposed image blocks. It finds a classifier for each class and decides whether a block is from a stego or cover image. Hence, the steganalysis of the whole image can be conducted through voting process by fusing steganalysis results of all image blocks.

REFERENCES

[1] "Network-Security-Essentials (Applications and Standards)", Pearson Education, William Stallings

[2] B. Schneier, Practical Cryptography, Wiley, 2003.

[3] A universal steganalysis to steganographic images on frequency domain Ping, Qian; Li-ya,Chen; Meng,Wu; 2011.

[4]. an image steganalysis method based on characteristic function moments and PCA Li Hui; S. Ziwen; Z.Zhiping; Control Conference (CCC)

[5] Statistical steganalyis of images using open source software Kaipa, B.; Robila, S. A.; LISAT, Long Island Systems, 2010.

[6] Blind detection for JPEG steganography W. Yu; Z.Li; L.Ping; ICNIT, International Conference,2010 , Page(s): 128 - 132 .

[7] SURF: Steganalysis using random forests Veena,H.B, Krishna,S, Shenoy.P.D., Intelligent Systems Design and Appli, 2010.

[8] Comparison between NeuralNetwork Steganalysis and Linear-Classification Method Stegdetect Holoska.J, Oplatkova.Z.; Zelinka.I,Senkerik,R, Conference 2010.

[9] Steganalysis scheme using the difference Image of Calibrated Sub sampling JC-Joo; TWOh; JHChoi; HK Lee; IIHMSP, 2010.

[10] Universal Steganographic Detection Algo in JPEG Image Using the Data-Dependent Kernel C.Qunjie; Z.Shangping; Electronic Commerce and Security (ISECS), 2010.

[11] Block-based image steganalysis:;Algorithm and performance-evaluation SCho; BHCha; JWang; Kuo,C.-C.J.; 2010