Scientific Journal Impact Factor (SJIF) : 1.711
International Journal of Modern Trends in Engineering and Research
ISSN (ONLINE) : 2349 - 9745
ISSN (PRINT) : 2393 - 8161

A Survey on Different Image Steganalysis Techniques

Sruthi Das N[1], Rasmi P S[2]
[1]*Computer Science & Engineering , TIST*
[2]*Information Technology, TIST*

Abstract— Steganography is a data hiding technique used to hide secret message within cover media. Steganography does not attract unnecessary attention compared to cryptography. In cryptography a message is encrypted for security. The information about the secret message is not hidden here, instead encryption is carried out. This is the reason steganography is very difficult to detect compared to the cryptography. The aim of steganalysis is to detect the presence of steganography. There are a number of steganalysis techniques are present for the detection of steganography. A survey on different steganalysis techniques for images is presented in this paper.

Keywords- Steganography, Steganographer, Stego image, Steganalysis, Steganalytic features, Large-scale steganalysis

I. INTRODUCTION

Nowadays steganography become very popular with the wide use of internet. Many steganographic tools are available easily and are very easy to understand and use. Today Steganography has been largely misused for illegal purposes. An article reported that terrorists groups are using steganography for secret communication.

For rating the performance of steganographic techniques some criteria can be used. One of the important criteria is the security. Steganography is susceptible under various attacks. These attacks include active and passive attacks. A steganographic technique is said to have security if and only if the secret message hidden using that particular steganographic technique can only be detected with a random guess. Otherwise that steganographic technique is said to be insecure.

Another important criterion is the capacity. Capacity of a steganographic technique means how much data can be hidden in steganographic medium using that particular technique. A steganographic technique with low capacity is not very efficient. The capacity should be high for a good steganographic technique. Different steganographic algorithms are F5 [1], [2], OutGuess [3], [4], StegHide [5], [6], BlindHide [7], BattleSteg [7], JPHide&Seek [8] etc.

Steganalysis [9], [10], [11] is a branch of science which deals with the detection of secret message hidden in a steganalysis medium using steganography. The first step in steganalysis is to detect the hidden message and when the hidden message is discovered it is a successful attack on steganography. It is very important to detect the steganographic communication since steganography is misused for illegal purposes.

The rest of the paper is organized as follows. An overview on existing steganalysis techniques and some of the problems associated with these techniques are presented in section II. Concluding remarks are given in section III.

II. TYPES OF STEGANALYSIS

The identification of whether or not a secret message id hidden in a suspected medium (image, file, audio, video, etc) is the main aim of steganalysis. Steganalysis is classified into two main categories. They are specific steganalysis and universal steganalysis [12]. The different type steganalysis techniques are shown in Figure 1.

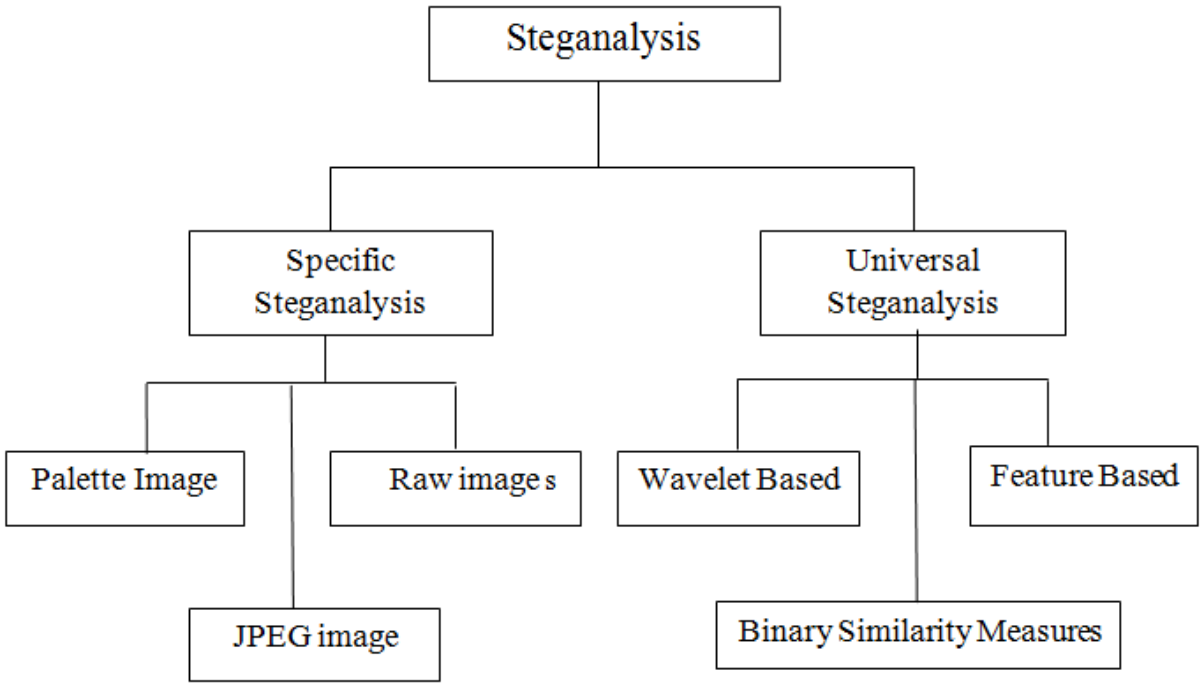

Figure 1: Classification of steganalysis

2.1. Specific Steganalysis

Specific steganalysis method is fully dependent on the steganographic algorithm that is being used for hiding secret data into the image. The success rate for detecting the hidden data is very high for this type steganalysis. GIF, BMP and JPEG files are the most commonly used image formats for hiding secret data. The different specific steganalysis algorithms are [13],

- ***Palette Image Steganalysis*** **-** mainly used for GIF image
- ***Raw image Steganalysis*** **-** mainly used for BMP images
- ***JPEG image Steganalysis*** **–** popular for image steganalysis

2.2. Universal or Generic or Blind Steganalysis

Universal steganalysis [14], [15], [16] is mostly preferred than specific steganalysis because universal methods are independent of the underlying steganographic algorithms. The goal of universal steganalysis is to identify the cover image and stego image. The statistical artifacts; a result of the embedding process; are used to differentiate between cover image and stego image. Selection image's right feature is an important factor for accuracy. Different blind steganalysis algorithms are,

- ***Wavelet Based Steganalysis:***

  In wavelet based steganalysis decompose an image by using wavelet, calculate the co-occurrence matrix of the adjacent wavelet coefficients, and apply Laplace transform to the co-occurrence matrix.

- ***Feature Based Steganalysis:***

  Feature based steganalysis uses a set of different features that are obtained from DCT and spatial domain [17], [18].

- ***Binary Similarity Measures (BSM):***

  Binary similarity measure steganalysis capture statistical artifacts & determine the presence of hidden data.

Image steganalysis and pattern recognition are similar to each other. Both of these techniques are based on classifying the images as stego image and normal image. Blind steganalysis or universal steganalysis aims at this classification without the prior knowledge of steganalysis algorithm used. Universal image steganalysis has a general structure with two stages. They are feature extraction and classification. After extracting the features from the stego image, the preprocessing of the features are carried out for improving the classification. These preprocessing include conversion of RGB image into gray scale, cropping and compression of the image etc. In feature extraction informative features are extracted. These selected features should be sensitive to steganography.

There is also another broad classification of steganalysis in terms of its performance capacity. They are large scale steganalysis and small scale steganalysis. Small scale steganalysis means steganalysis is performed on individual images. Most of the existing systems use small scale steganalysis. Nowadays terrorist are using social media to communicate secretly by transferring stego images. Social media application has many users all over the world and these users share millions of images per day. So it is practical to use small scale steganalysis in such scenarios.
In large scale steganalysis, steganalysis is performed on large number of images simultaneously. So it is very suitable for real world scenarios where large numbers of images are shared. This area of steganalysis is not fully developed, many research have been still conducting [19]. Large scale steganalysis uses universal steganalysis for better efficiency.

III. CONCLUSION

In this paper a brief description about steganography and its performance criteria are discussed. And also there are some discussions about some steganographic algorithms. Mainly the paper presents a detailed description on steganalysis, requirements, and different types of steganalysis. Difference between small scale steganalysis and large scale steganalysis is also mentioned in this paper. Overall this paper gives an idea about steganography, steganalysis and different techniques, small scale steganalysis and large scale steganalysis.

REFERENCES

[1] A. Westfeld, "F5—A steganographic algorithm," in Proc. 4th Inf. Hiding Workshop, vol. 2137. 2001, pp.289-302.

[2] A. Westfeld, "Implementation of the F5 Steganographic Algorithm", [Online]. Available: http://code.google.com/p/f5-steganography. Apr.2012.

[3] N. Provos, "Defending against statistical steganalysis," in Proc. 10th Conf. USENIX Security Symp., vol. 10. 2001,pp.323-335.

[4] N. Provos, "Implementation of the OutGuess Algorithm ver. 2.0", [Online]. Available: http://www.outguess.org/, Oct.2001.

[5] S. Hetzl, "Implementation of the Steghide Algorithm ver. 0.5.1", [Online]. Available: http://steghide.sourceforge.net/, Oct. 2003

[6] S. Hetzl and P. Mutzel, "A graph–theoretic approach to steganography," in Proc. 9th Int. Conf. Commun.Multimedia Security, 2005, pp.119-128.

[7] K. Hempstalk, University of Waikato, "Digital Invisible Ink Toolkit", [Online]. Available: http:// http://diit.sourceforge.net/, 2005.

[8] A. Latham, "Implementation of the JPHide and JPSeek Algorithms ver 0.3", [Online]. Available: http://linux01.gwdg.de/ , Aug 1999.

[9] J. Fridrich, M. Goljan, R. Du, Detecting LSB steganography in color and gray-scale images, IEEE Multimedia Magaz., Special Issue on Security, 22-28, Oct-Nov 2001.

[10] N.F. Johnson, S. Jajodia, Steganalysis of images created using current steganography software, in: Lecture Notes] in Computer Science, vol. 1525, Springer-Verlag, Berlin, 1998, pp.273-298.

[11] N.F. Johnson, S. Jajodia, Steganalysis: The investigation of hidden information, in: Proc. IEEE Information Technology Conference, Syracuse, NY, 1998.

[12] Manveer Kaur and Gagandeep Kaur, "Review of Various Steganalysis Techniques", (IJCSIT) International Iournal of Computer Science and Information Technologies, Vol.5 (2), 2014.

[13] Natarajan Meghanathan and Lopamudra Nayak, ''Steganalysis Algorithms For Detecting The Hidden Information In Image, Audio And Video Cover Media '', in International Journal of Network Security & Its Application (IJNSA), Vol.2, No.1, January 2010.

[14] H. Farid, Detecting hidden messages using higher-order statistical models, in: Proc. IEEE Int. Conf. Image Process, Rochester, NY, vol. 2, pp. 905-908, Sep 2002.

[15] Xiaochuan Chen, Yunghong Wang, Tieniu Tan, Lei Guo, Blind image steganalysis based on statistical analysis of empirical matrix, IEEE, ICPR, 2006.

[16] Patricia Lafferty, Farid Ahmad, Texture based steganalysis: Results for color images, in: Proc. of SPIE, vol. 5561, 2004.

[17] Qingxiao Guan, Jing Dong and Tieniu Tan, " Evaluation of FeatureSsets for Steganalysis of JPEG Image", IEEE Youth Conference on Information Computing and Telecommunications (YC-ICT), Nov. 2010.

[18] Rita Chhikara and Latika Singh," A Review on Digital Image Steganalysis Techniques Categorised by Features Extracted", in International Journal of Engineering and Innovative Technology (IJEIT) Volume 3, Issue 4, October 2013.

[19] Andrew D. Ker and Tomáš Pevný, "The stegnographer is the outlier: Realistic Large-Scale Steganalysis", IEEE Trans. Inf. Forensics Security, vol.9, no. 9, Sep. 2014.

