JCSE International Journal of Computer Sciences and Engineering Open Access

Review Paper Vol.-7, Issue-2, Feb 2019 E-ISSN: 2347-2693

Blind Image Steganalysis: A Review

Sindhav Bhumika A[1*], N. M. Patel[2], U. K. Jaliya[3]

[1,2,3]Department of Computer Engineering, BVM, VVnagar, Anand, Gujarat, India

[*]*Corresponding Author: bhumikasindhav028@gmail.com*

DOI: https://doi.org/10.26438/ijcse/v7i2.511514 | Available online at: www.ijcseonline.org

Accepted: 21/Feb/2019, Published: 28/Feb/2019

Abstract— Internet has become a vital source of communication through that data is transmit, receive and share in style of emails, text, speech, images, videos, audios etc. currently a day's JPEG pictures are wide utilized in our everyday life.. Communication between end user can be secure by using Cryptography. Such kind of communication can be embedded by using Steganography. However Steganography will use in digital carries like text, image, audio or video document for hide secrets documents. Now a day Steganalysis is a new approach to find and analyse the important information which is hiding using the steganography method. The steganalysis for JPEG kind pictures becomes important and important. Steganalysis in pictures supported DCT remodelled region, able to acknowledge the foremost widespread steganography algorithms occurring on the net. However performance of any algorithmic program depending on sensitivity of options and quantity of information hidden in a picture. This paper is provides an overview about steganography techniques and steganalysis techniques for digital images to find cue against to where to look for hidden data in images, discussion about different steganalysis algorithmic programs, steganalysis classification methods, limitation and characteristics of different steganalysis method.

Keywords: Steganography, Universal Steganalysis, Steganalysis, Multimedia documents, Cryptography, Cover Image, Stego Image, Classification, DCT.

I. INTRODUCTION

Steganography is the process to hide important information and all the information are appended with cover [1]. There are some different between Steganography and cryptography. But in cryptography the message are converted into some another language, so that the receiver can't directed understand. Process of Steganography is totally different then cryptography, in Steganography number of techniques are used for hind the important information like hide the information behind the image, audio, and etc. By analysis different steganography techniques and steganalysis techniques for digital images to find cue against to any kind of hidden data in images.

In Steganography there are two varieties:
1) Message and
2) Carrier.
Important information are store in message and message are in hidden form, this message are appended with the carrier.

1.1 IMAGE STEGANOGRAPHY

Steganography is the process of hiding data into public digital medium for secret communication over the communication channels. An image with a secret message within will simply be cover the globe Wide net or in Newsgroups. However, the sensible use of steganography still looks to be restricted. These techniques are often used with varied degrees of success on differing kinds of image files.

- ➢ Least Significant Bits
- ➢ Masking and filtering
- ➢ Transformations

1.2 IMAGE STEGANALYSIS

Important information are concealing by Steganography. Inside the image presence of the message are conceals. In Steganography extraction and modification techniques are used for detection but in steganalysis the stego object and non stego object are refer in blind steganalysis method. While not previous data of method used to cover the info [3].The image in which the secret data is hidden is known as stego image. The detection of hidden embedded data in the image without prior knowledge about data hiding algorithm is the main aim for blind image Steganalysis. A large number of steganalysis techniques are available for the detection of steganography in the image [11].

II. METHODOLOGY

Steganalysis method can be divided into 2 different categories as per the detecting presence of any hidden messages:

1. Feature based steganalysis
2. Statistical steganalysis
   - Spatial domain
   - Transform domain

2.2.1 Type of Steganalysis

Some situation the steganalysis method is depended on Steganographic algorithm. But in some situation Steganalysis use own method for detecting presence of hidden message bases on that Steganalysis are classified in two different categories.

1) Target / Specific steganalysis.
2) Universal / Generic / Blind steganalysis

Specific steganalysis:

In specific steganalysis method if the Steganalysis algorithm is known then the designer of detector is detect the hidden information from carrier base on the SA .Analysing and statistical properties are based on the Specific steganalysis method. When we use specific steganalysis method for detecting hidden information we can get the accurate result compare to other method. We cannot detect the hidden information by using the embedding algorithm, so it is a main disadvantage of this method.

Blind / Universal steganalysis:

Everyone does not know the Steganalysis algorithm, so Universal steganalysis is the best method to detect the presence of the important message. With the use of Universal steganalysis anyone can developed the detector of message on SA. Universal steganalysis is power full method compare to the specific steganalysis because SA is work as individual. Universal steganalysis is mainly focus on 2 phases.

a. Feature Extraction.
b. Classification.

2.2 The Flowchart for image Steganalysis system

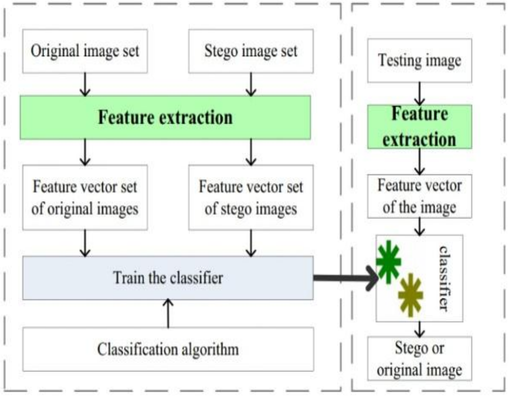

Fig. The framework of learning based steganalysis [4].

III. LITERATURE REVIEW

Yiqin Zhang and Fenlin Liu, et.al [1] in their paper proposes a feature improvement methodology for wealthy model options supported the improved Fisher criterion. Supported the principle that "The within-class variance ought to be smaller and between-class variance ought to be larger". Within the experimental analysis wealthy model SRM that may be won't to find typical fashionable steganography Victor-Marie Hugo.

Madhavi B. Desai the author describe et.al [2] in their paper proposes based Fisher Criterion and multivariate analysis techniques. This method s are dimensional unified feature set for universal image steganalysis victimisation Fisher Criterion and multivariate analysis techniques. The planned algorithmic rule achieves overall ninety seven detection accuracy against numerous steganography strategies.

Punam Bedi, et.al [3] in their paper proposes a feature proposes work for a unique feature choice algorithmic rule (FS-SDS) for steganalysis. FS-SDS may be a wrapper-type feature choice algorithmic rule that selects reduced feature set mistreatment random Diffusion Search.

Z. X. &. X. W, et.al [4] in their paper proposes the models for the messages embedded by spatial least vital bit (LSB) matching as freelance noises to the duvet image, and divulges that the bar chart of the variations between element grey values is smoothened.

Zhihua Xia, et.al [5] in their paper proposes the models for the learning-based steganalysis/detection technique to attack patial domain least vital bit (LSB) matching steganography in grayscale pictures.

Xiao feng Song et.al [6] in their paper describe about the 2D Gabor filters have bound optimum joint localization properties within the spatial domain and within the spatial frequency domain. The experimental results show that the detection error EOOB is given for quality factors seventy five and ninety five.

Madhavi B. Desai, et.al [7] in their paper describe about the value the performance of DWT feature based mostly steganalysis algorithms against varied state-of-art steganography ways and variable message embedding rates. This paper additionally presents the comparative performance of individual algorithms against totally different classification ways.

Yi Zhang, et.al [8] in their paper describe about strategies to boost the detection performance for content-adaptive JPEG steganography. The planned technique generates filtered pictures comprising wealthy texture and edge data victimization Gauss partial filter bank, and histograms of absolute values of filtered sub pictures.

Daniel Majercak et.al in their paper proposes Feature-based Steganalysis strategies method. [9] The objective is performance testing of Feature-based Steganalysis strategies for detection of steganography tools that area unit used for activity a secret message in still pictures. Feature extraction during this paper was applied in spatial domain and conjointly directly in transformation domain of DCT in JPEG files what helps to obtained relevant applied mathematics information.

Oswaldo Juarez-Sandoval et.al in their paper discuss about strategies proposes Feature-based Steganalysis strategies method. [10] The author propose a compact image steganalysis technique for the LSB-matching steganography, during which a feature vector composed by solely twelve parts is extracted from the image. By practical they Achieving 99.626% steganalyzer sensitivity on 0.25bpp stego images of the dataset by only two analysis dimensions.

IV. DATASET DESCRIPTION

Create dataset of 550 labelled image for training and testing phase. Create a stego image using multiple steganography tool like:

1. VSL steganography tool (Virtual Steganography Laboratory) generates stego image of F5 and LSB stego image [2], [7], [13]. Using a VSL steganography tool (Virtual Steganography Laboratory) generates stego image of F5 and LSB stego image. In VSL steganography tool you can hide image or any text file into image.

2. Digital Invisible Ink Toolkit 1.5 is generates stego image with DBS, DFF, and Blind Hide, hide Seek steganography methods.

3. OpenStego Tool is the free steganography tool. It can hide any kind of data or message within a cover file.

4. 1-2- Free Steganography Tool: This has allowed us to encryption and hidden files in other files using a specified password, which are not suspect of encryption (JPG, PNG, BMP).

V. SUMMARY

Detecting the presence of hidden information binary similarity measure is the most effective method in image steganalysis. At BSM we have to work with big plans. If we have a tendency to implant something into an image. Eighteen completely different BSM were obtained for every image of dataset to construct feature vector. Then this vector is used to train and take a look at the classifier. CF Moments area unit sensitive to varied knowledge concealing strategies and provides a helpful cue against the existence of any hidden messages into image [7]. Use of BSM in Desecrate Cosine Transform improved the performance of the domain against numerous JPEG steganography strategies [19]. Stego image will generate victimization multiple steganography tools like VSL, Digital Invisible Ink Toolkit, OpenStego Tool, 1-2- Free Steganography Tool.

VI. CONCLUSION

In this paper, we review the fundamental concepts and notions about multiple steganalysis techniques, so we can say that steganalysis is meant to reverse of steganography. In the steganalysis, feature extraction and classification process plays an important role. So by Identify a minimum number of features. It will give an efficient classification result. Blind image steganalysis has an advantage over Specific steganalysis, because in blind image steganalysis there is no need of any prior knowledge about data hiding methods. And also its applicable to any type of image and file format. After finding the number of features we can use them in different classification techniques like Bayesian, ANN. By comparing the results, we will know that which methods are given high accuracy.

REFERENCES

[1] H. j. J. L. a. C. Y. Yiqin Zhang and Fenlin Liu, "*Compact Image Steganalysis for LSB-Matching Steganography*", *International Conference on Advanced Computational Intelligence (ICACI),* pp. 187-192, 2018.

[2] S. V. P., B. P. Madhavi B. Desai, "*ANOVA and Fisher Criterion based Feature Selection for Lower Dimensional Universal Image Steganalysis", IJIP,* 2016.

[3] V. B. N. M. a. T. C. Punam Bedi, "*FS-SDS: Feature Selection for JPEG Steganalysis using Stochastic Diffusion Search*", *IEEE,* pp. 3797-3802, 2014.

[4] Z. X. &. X. W. &. X. S. &. Q. L. &. N. Xiong, "*Steganalysis of LSB matching using differences between nonadjacent pixels*", *Springer,* 2014.

[5] f. l. C. Y. Xiaofeng Song, "*Steganalysis of Adaptive JPEG Steganography Using 2D Gabor Filters, IJRITCC,* 2015.

[6] S. V. P. Madhavi B. Desai, "*Performance Analysis of Image Steganalysis against Message Size, Message Type and Classification Methods*", *IEEE,* 2016.

[7] F. L, C. Y, X. L. X. S. J. L. Y. Yi Zhang, "*Steganalysis of content-adaptive JPEG steganography based on Gauss partial derivative filter bank*",*Journal of Electronic Imagin* , 2017.

[8] Daniel Majercak, Vladimir Banoci, Martin Broda, Gabriel Bugar, Dusan Levicky"*Performance Evaluation of Feature-based Steganalysis in Steganography*", Conference Radioelektronika 2013, April 16-17.

[9] M. C.-H. Oswaldo Juarez-Sandoval, "*Compact Image Steganalysis for LSB-Matching Steganography", IEEE,* 2015.

[10] J.Anita christaline, R.Ramesh, D.Vaishali "*Steganalysis with classifier combinations*",ARPR-2014, pg. no-2858-2863

[11] S.K.Sabnisa,R.N.Awaleb" *Statistical Steganalysis of High Capacity Image Steganography with Cryptography*",Elsevier-2016,321-327

[12] Zohaib Khan, Atif Bin Mansoor “*An Analysis of Quality Factor on Image Steganalysis*” ,IEEE-Conference Paper · April 2010

[13] Sruthi Das N1, Rasmi P S”*A Survey on Different Image Steganalysis Techniques*”,IJMTER-2015,533-536

[14] S.Geetha, shiva s.shivtha sandhu, N. kamraj”*blindimagesteganalysis based on contentindependentstatisticalmeasures maximizing the specificity and sensitivity of system”*, Elsevier-2006, pg N0-683-697.

[15] Ismail Avcıbas¸Mehdi Kharrazi,Nasir Memon,B¨ulent Sankur”*Image Steganalysis with Binary Similarity Measures*”,EURASIP Journal on Applied Signal Processing 2005:17, 2749–2757

[16] Yi Zhang, Fenlin Liu ,Chunfang Yang ,Xiangyang Luo,Xiaofeng Song, Jicang Lu”*Steganalysis of content-adaptive JPEG steganography based on Gauss partial derivative filter bank*”,Journal of Electronic Imaging-2017.

[17] Manisha Saini, Rita Chhikara ”*performance Evaluation of DCT and DWT Features for Blind Image Steganalysis using Neural Networks*” International Journal of Computer Applications- March 2015 (0975 – 8887)

[18] Dr. Monisha Sharma1 and Mrs. Swagota Bera” *a review on blind still image steganalysis techniques using features extraction and pattern classification method*”, International Journal of Computer Science, Engineering and Information Technology (IJCSEIT), Vol.2, No.3. Vol.2, No.3.June 2012,

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

[20] K. Nandhini1, B. Gomathi” Implementation of LSB Based Steganography Algorithms in FPGA”, IJSRNSC, Volume-6, Issue-5, June 2017.

[21] Rajesh Shah , Yashwant Singh Chouhan “Encoding of Hindi Text Using Steganography Technique”, ISROSET- Int. J. Sci. Res. in Computer Science & Engineering Vol-2, Issue-1, PP (22-28), Feb 2014.

Authors Profile

Miss Sindhav Bhumika A. pursued Bachelor of Engineering in Information Technology from Lukhdhirji Engineering College(LEC)-Morbi-2, Gujarat, India in 2017.She is currently pursuing in Master of Technology in course of computer engineering (Software engineering) from Birla Vishvakarma Mahavidhyalaya (BVM), VVnagar, Anand, Gujarat, India. Her main research work focuses on image processing, steganalysis techniques.

Mr. N. M. Patel pursued Bachelor of Engineering in Electronics Engineering and Master of Engineering in Microprocessor & its application. He is also pursued Ph.D. in Computer Engineering and currently working as Associate Professor in Department of computer engineering, in Birla Vishvakarma Mahavidhyalaya (BVM), VVnagar, Anand, Gujarat, India. He has published more than 74 research papers in reputed international journals and national journals conferences including IEEE and it’s also available online.. He has 24 years of teaching experience . He also Guided more than 63 Project of master level . He is also registered as a PhD supervisor at GTU.

Mr. Udesang K Jaliya pursued Bachelor Engineering in Computer Engineering and Master of Engineering in computer engineering. He is also pursued Ph.D. and currently working as Assistant Professor in Department of Computer Engineering, in Birla Vishvakarma Mahavidhyalaya (BVM), VVnagar, Anand, Gujarat, India. He has published more than 35 research papers in reputed international journals and national journals conferences including IEEE and it’s also available online.. He also Received Best Paper Award in IEEE Sponsored International Conference on Data Mining and Advanced Computing. He has 15 years of teaching experience . He also Guided more than 20 Project of master level .He also published 2 Books related their field area. He is also registered as a PhD supervisor at GTU.