International Journal Of Engineering Research And Development
e-ISSN: 2278-067X, p-ISSN: 2278-800X, www.ijerd.com
Volume 13, Issue 9 (September 2017), PP.07-11

Review on Universal Steganalysis Techniques Based on the Feature Extraction in Transform Domain

[1*]Mr. Yadvendra Prasad Dwivedi,[2]Mrs. Swagota Bera,[3]Mrs. Monisha Sharma
[1,2,3]*Dept. of E & Tc*
*Corresponding Author: *Mr. Yadvendra Prasad Dwivedi*

ABSTRACT: Steganography and steganalysis are important topics in information hiding. Steganography refers to the technique of hiding secret messages into media such as audio, video, image and text with maximum stealthiness, while in steganalysiswe recover back the secret data hidden in the stegoimages.Steganography and steganalysis both have received a lot of attention from law enforcement and media. Steganalysis can be classified on the basis of the techniques used such as classified statistical techniques, pattern classification techniques and visual detection techniques etc. In this paper an extensive review report is presented for steganalysis. This paper provides a survey on steganalysis for digital images, mainly covering the fundamental concepts, the progress of steganographic methods for images in spatial representation and in JPEG format, and the development of the corresponding steganalytic schemes. Some commonly used strategies for improving and enhancing steganalytic capability are summarized and possible research trends are discussed.

General Terms

Information Hiding, Steganography, Steganalysis.

Keywords: Steganography, Steganalysis, Cover Image, Stegoimage,Transform Domain,Spatial Domain,Universal Steganalysis.

I. INTRODUCTION

Steganalysis is the art of Science which deals with the detection & destruction of the secretimage.Steganography can be used as both legally and illegally. Like civilians may use it for protecting privacy while terrorists may use it for transmitting terroristic information.Passivesteganalysis attempts to destroy the trace of secret communication without bothering to detect the secret message by changing image format, flipping all LSBs, JPEG compression etc., while active steganalysis uses specialized algorithms that detect the existence of stego-image. Steganalysis can be classified into two categories: signature steganalysis and statistical steganalysis. Both categories can be either specific or universal. Specific steganalysis is designed for a particular steganographic embedding algorithm, while universal steganalysis is a general class steganalytic technique, which can be implemented with any steganographic embedding algorithm, even an unknown algorithm. Steganography is used for Cyber-crime which is believed to benefit attackers as reported in USA TODAY and by other media. Secret data are hidden in the images, videos, c.ds, text and in any digital media and even in a simpler form such as in HyperText Markup Language (HTML), executable files and Extensible Markup Language (XML).

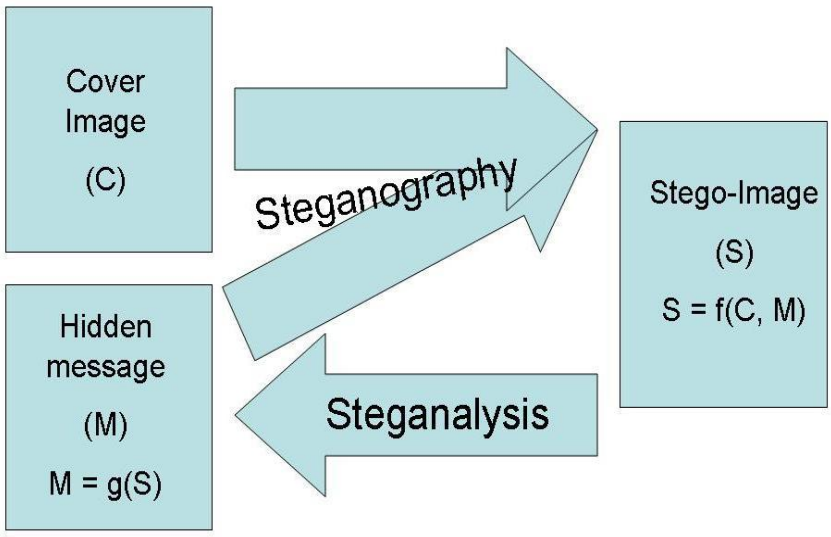

Figure 1 Complete process of steganography and steganalysis

From the block diagram of complete process of steganography and steganalysis which is shown in figure 1. In brief we say that the message (M) is hiding in cover images (C), which gets converted into stego- images (S), stego-images are the function of both C and M. The whole process is called steganography. when we recovering back the hidden message (M) from stego-image called as steganalysis.

Current steganalysis aims to focus more on detecting statistical anomalies in the stego images which are based on the features extracted from typical cover images without any modifications.Steganalysis can be classified into two broad categories based on prior information

a) Specific/Targeted steganalysis

b) Blind/Generic/Universal steganalysis

A) specific/targeted steganalysis:

Specific steganalysis, also called as targeted steganalysis, it is designed to attack one particular type of steganography algorithm. The steganalyst is aware of the embedding methods and statistical trends of the stego image if it is embedded with a known algorithm. This attack method is most effective when tested on images with the known embedding techniques, whereas it might fail considerably if the algorithm is unknown to the steganalyst.

B)blind/generic/universal steganalysis:

The more general class of steganalysis techniques independently can be designed to work with any steganographic embedding algorithm, even an unknown algorithm. Such techniques have been called as Universal Steganalysis techniques or Blind Steganalysis Techniques. Blind steganalysis also known as universal steganalysis is the modern and more powerful approach to attack a stego media. Since this method does not depend on knowing any particular embedding technique. This method can detect different types of steganography content even if the algorithm is not known. However, this method cannot detect the exact algorithm used to embed data if the training set is not trained with that particular stego algorithm. The method is based on designing a classifier which depends on the features or correlations existing in the natural cover images. The most current and popular methods include extracting statistical characteristics also known as features from the given set of images.

2. Various approaches are discussed by the different researchers in the area of steganalysis:

In **2003** Lyu S. and FaridH.proposed Detecting Hidden Messages using Higher-Order Statistics and Support Vector Machines in which 1800 JPEG images were used as data size. Feature extracted were mean, variance, skewness and kurtosis from 3-level DWT coefficients and SVM classifier was used for classification. Detection Accuracy is evaluated for the various steganographictechniques such as Outguess, Jsteg, Ezstego and LSB substitution. The feature dimension was 72[1]. In **2005** Jessica Fridrich proposed Feature-Based Steganalysis for JPEG Images and its Implications for Future Design of Steganographic Schemes in which data base used where 1814 Green spun Images. The DCT features were used as statistical features from intra block difference DCT Coefficient matrices with SVM classifier for evaluating detection accuracy for F5, Outguess and MB1. The feature dimension was 23[2].

In **2007** Yun Q. Shi, Chunhua Chen, Wen Chen Proposed A Markov Process Based Approachto Effective Attacking JPEG Steganography in which used data base was 7560 JPEG images. The one step Markov's features were used as statistical features from intra block difference DCT Coefficient matrices with SVM classifier for evaluating detection accuracy for F5, Outguess and MB1. The feature dimension was 324[3]. In **2007** Tomas Penvy, Jessica FridrichproposedMerging Markov and DCT Features for Multi-Class JPEG Steganalysis(CCPEV) in which used data base was 3400 JPEG images. The one step Markov's features and DCT features were used as statistical features from intra block difference DCT Coefficient matrices with SVM classifier for evaluating detection accuracy for F5, Outguess and MB1. The feature dimension was 274[4].

In **2011** Jan Kodovský and Jessica FridrichproposedSteganalysis in high dimensions: Fusing classifier built on random subspaces(CC-C300) in which used data base was 6500 JPEG images. The Markov's features were used as statistical features from intra block difference DCT Coefficient matrices with Ensemble classifier for evaluating detection accuracy for nsF5 and spatial domain stego images. The feature dimension was 1234[5]. In **2012** Jan Kodovský and Jessica FridrichproposedSteganalysis of JPEG Images using Rich Models (CC-JRM) in which 6500 camera images were taken and statistical features were extracted using intra and inter block co-occurrence (JRM) from the DCT coefficients of the imageswith the ensemble classifier. Further feature selection was done by ITERARIVE BEST strategy. The performance parameter was probability of error for evaluating detection accuracy for nsF5, MBs, YASS, MME and BCH. The feature dimension was 22510[6].

In **2012** Jan Kodovsky, Jessica Fridrich and VojtěchHolub proposed Ensemble Classifiers for Steganalysis of Digital Media(CF) in which 6500 camera images were taken and statistical features were extracted using Block DCTandIntra and inter block Difference DCT coefficient matrix. The feature extraction method used are co-occurrence Matrix. The classifier used are ensemble classifier implemented as random forests,

FLD. The performance parameter was probability of error and Training time error for evaluating detection accuracy for nsF5, MBs and YASS. The feature dimension was 7850[7].

In **2013**Fengyong Li, Xinpeng Zhang, Bin Chen and Guorui Feng proposed JPEG Steganalysis with High-Dimensional Features and Bayesian Ensemble Classifier in which BOSSbase 5000 images were taken and statistical features were extracted using Block DCT and Intra and inter block Difference matrix. The feature extraction method used are co-occurrence Matrices of DCT coefficients and coefficient differences. The classifier used are Majority VotingEnsemble Classifier (SVM, FLD). The performance parameter wasprobability of error. The feature dimension was15700. The detected steganography is nsF5 andMBs [8]. In **2013**Gökhan Gul, FatihKurugollu proposed JPEG Image Steganalysis using Multivariate PDF Estimates With MRF Cliques in which used data base was 20,000 JPEG images. The Markov Random Field (MRF) cliques and K-variate p.d.f estimates were used for features extraction with SVM classifier for evaluating detection accuracy for nsF5, JPEG hide & Seek, Outguess, YASS and MB1. The feature dimension was 363[9].

In **2014**Pritesh Pathak, S. Selvakumar proposed Blind Image Steganalysis of JPEG images using featureextraction through the process of dilation in which used data base was BSD-300 images. The extended DCT features, mean, variance, skewness and kurtosis from wavelet coefficients were used as statistical features with SVM classifier for evaluating detection accuracy for F5, Outguess, steghide and hide and seek. The feature dimension was 108 frequency domain, 21 spatial domains and 48 wavelet domain[10]. In **2014**GharehMohammadi,M.SanieeAbadeh proposed Image steganalysis using a bee colony based feature selection algorithm in which usedBOSSbsae 10,000images were taken and statistical features were extracted using SPAM and CCPEV. The artificial Bee Colony (ABC) feature selection method is used.The performance parameter was feature accuracy. The feature dimension was 250[11].

In **2014**Bin Chen Guorui Feng , Xinpeng Zhang and Fengyong Li proposed Mixing high-dimensional features for JPEG steganalysis in which BOSSbase 10,000 images used as data basewith ensemble classifier.Markov'sfeature,Extended DCT feature,Co-occurrences are used as a feature extraction in which the feature selection as to decrease its dimensionality accordingto the correlation coefficient among different features parts. The performance parameter is probability of error time cost function. The Feature Subclass includes SHI-648, 548-extended DCT, 7850-PEV, 1034-PS and 4784-PSC.The detected steganography wasnsF5, MB[12].

In **2015**VojtechHolub and Jessica Fridrich proposed Phase-Aware Projection Model for Steganalysis of JPEGImages(PHARM) in which BOSSbase 10,000 images used as database for this model with FLD ensemble classifier.First Order Statistics are used as feature extraction technique withPhase Aware Projection Model(PHARM) as a pre-processing method. Detection accuracy is evaluated for nsF5, J-UNIWARD and S-UNIWARD.The feature dimension was 12600[13]. In **2015**HassanKarimi, Mahrokh G. Shayesteh, Mohammad Ali Akhaee proposed Steganalysis of JPEG images using enhanced neighbouring joint density features in which BOSSbase 4,000 images are used as data base.The pre-processor used are Block DCT, Pth power of DCT Coefficient, Inter & inter block difference matrices with ensemble classifier. The feature extraction technique used areabsNJ(Absolute Value of neighbouring joint matrix from abs DCT coefficient&differential DCT coefficient. The performance parameter was F-test Statistics of ANOVA, Median testing error using ensemble class for evaluating detection accuracy for F5,Jsteg, MB1, nsF5 and YASS. The feature dimension usedwas 800[14].

In **2015**VojtěchHolub, Jessica Fridrich proposed Low-Complexity Features for JPEG Steganalysis Using Undecimated DCT(DCTR) in which BOSSbase 10,000 images used as a data size with FLD ensemble classifier. The feature extraction technique used areundecimatedDCT,Discrete Cosine TransformResidual(DCTR).The performance parameter wasProbability of error, Detection error EOOBfor evaluating the detection accuracy ofJUNIWARD, UED and nsF5[15]. In **2016**TomášDenemark Den, Mehdi Boroumand, Jessica Fridrich proposed Steganalysis Features for Content-Adaptive JPEG Steganography in which BOSSbase 10,000 images used as a database with FLD ensemble classifier. DCTR,PHARM and GFR are used as a feature extraction. The performance parameter are Probability of error and detection error for evaluating the detection accuracy of JUNIWARD and UED[16]. In **2016**DinaBashkirova proposed Convolutional Neural Networks for Image Steganalysis in which BOSSbase 10,000 images used as database with Image segmentation and calibration as a pre-processor with CNNclassifier.The performance parameters were ROC and Detection accuracy for evaluating the detection accuracy of nsF5. The feature dimension was 800[17].

In **2016**Rita Rana Chhikara, Prabha Sharma, Latika Singh proposed An improved dynamic discrete firefly algorithm for blind image steganalysisin which 2000 images taken from http://www.photobucket.com andhttp://www.1000pictures.com.data for data base. The pre-processor used are DCT with SVM as a classifier. CCPEV and SPAM technique was used for feature extraction and feature selection was done by Improved Firefly Algorithm DyFAFitnessfunction-SVM for evaluating the detection of nsF5, Outguess, PQ and Steghide with Detection Accuracy was used as performance parameter having dimension 686[18].

In **2016** Xiaofeng Song, Fenlin Liu, ZhenguiZhang ,Chunfang Yang ,Xiangyang Luo and Liju Chen proposed2D Gabor filters-based steganalysis of content-adaptiveJPEG steganography(GRF)in which BOSSbase 10,000 images used as a data base with image decompression as a pre-processor. Inter block & intra block Co-occurrence are used for feature extraction. The feature selection of 2-D Gabor filter on the basis of highest detection performance for evaluating the detection of UED, JUNIWARD and S-UNIWARD. The performance parameter was detection errors EOOB andExtraction Time with 17000dimension[19].

In **2017**LakhdarLaimeche, Hayet Farida MerouaniandSmaineMazouziproposedA new feature extraction scheme in wavelet transform for stego image classification in which uses UCID 1338as a data size with Random Forest as a classifier. The pre-processor used are DWT. Zipf's law used as statistical features for evaluating the detection of outguess and YASS.The feature selection used are ANOVA. The performance parameter was detectionAccuracyROC[20].

II. CONCLUSIONS

In the present paper, the research papers are discussed from year 2003 to 2017 obtained from various reputed journals published by IEEE, Springer, Elsevier and SPIE. In all the papers the universal steganalysis technique based on feature extraction and classification is implemented. The researches from year 2014 includes feature selection which further reduces the feature dimension by selecting the important features only for the classification of stego images and cover images.

REFERENCES

[1]. Lyu S. and FaridH., Detecting Hidden Messages using Higher-Order Statistics andSupportVector Machines, Information Hiding, vol.2578, pp340-354,Springer 2003.

[2]. Fridrich.J., Feature-based steganalysis for JPEG Images and its Implications forFutureDesign of Steganographic Schemes, International Workshop on Information Hiding, pp 67-81, Springer 2005.

[3]. ShiY.Q., ChenC.,andChenW.,A Markov Process Based Approach to Effective Attacking JPEG Steganography,Lecture Notes in Computer Science , InformationHiding,vol. 4437, pp 249-264, Springer 2006.

[4]. PevnyT.andFridrichJ.,Merging Markov and DCT features for Multiclass JPEG Steganalysis,Steganography, and watermarking of Multimedia Contents,vol. 6505, pp1-13,Springer 2007.

[5]. J. Kodovsky and J. Fridrich, Steganalysis in high dimensions: Fusing classifiers built on random subspaces, Proc. SPIE, Electronic Imaging, Media, Watermarking, Security and Forensics XIII, San Francisco, C.A., vol. 7880, pp. 23-26, January 2011.

[6]. J.Kodovsky, J. Fridrich, and V. Holub, Ensemble Classifiers for Steganalysis of Digital

[7]. Media,IEEE Transactions on Information Forensics and Security, vol. 7, Issue 2,pp 432 - 444, April 2012.

[8]. Li F., ZhangX.,andChen B., JPEGSteganalysisWith High Dimensional Features and Bayesian Ensemble Classifier, IEEE Signal Processing Letters, vol. 20, Issue 3, pp. 233-236,IEEE 2013.

[9]. Gul G. and Kurugollu F., JPEGImageSteganalysisUsing Multivariate PDF Estimates With MRF, IEEE Transactions on Information Forensics and Security, vol. 8, Issue. 3, pp. 578-587, IEEE2013.

[10]. MohammadiF. GharehandSanieeM.,Image Steganalysis Using a Bee Colony Based Feature Selection Algorithm, Engineering Applications of Artificial Intelligence, vol. 31, pp. 35-43, ELSEVIER 2014.

[11]. Pathak P. and Selvakumar S., Blind Image Steganalysis of JPEG images using feature extraction through the process of dilation, Digital Investigation, vol. 11, Issue1, pp. 67-77, ELSEVIER 2014.

[12]. Chen B., Feng G., Zhang X., LiF.,Mixing High-Dimensional Features for JPEG Steganalysis with Ensemble Classifier, Signal, Image and Video Processing,vol.8, Issue -8, pp. 1475-1482, Springer 2014.

[13]. HolubV. and Fridrich J., Phase-Aware Projection Model for Steganalysis of JPEG Images,Media Watermarking, Security and Forensics. vol. 9409, SPIE 2015.

[14]. Karimi H., Shayesteh M. G. and Akhaee M. Ali,Steganalysisof JPEGimagesusing enhanced neighbouring joint density features,IETImageProcessing,vol.9,Issue7,pp.545-552, IEEE2015.

[15]. Holub V. andFridrichJ.,Low-Complexity Features for JPEGSteganalysisUsing UndecimatedDCT,IEEE Transactions on Information Forensics and Security,vol. 10,Issue 2, pp. 219-228,IEEE 2015.

[16]. Denemark T. D.,Boroumand M.,Fridrich J.,SteganalysisFeatures for Content-AdaptiveJPEGSteganography,IEEE Transactions on Information Forensics and Security, vol. 11, Issue 8, pp. 1736-1746, IEEE 2016.

[17]. Bashkirova, Convolutional Neural Networks for Image Steganalysis,BioNanoSciencevol. 6, Issue 3, pp. 246-248, Springer 2016.

[18]. Chhikara R. R., Sharma P., AnImproved Dynamic Discrete Firefly Algorithm for Blind Image Steganalysis, International Journal of Machine Learning Cybernetics, pp. 1-15, Springer 2016.

[19]. Song X., Liu F.andZhang Z., 2D Gabor filters-based steganalysis of content-adaptive JPEG steganography, Multimedia Tools and Applications, pp. 1-29, Springer2016.

[20]. Laimeche L., Merouani H. F.andMazouzi S., A New Feature Extraction Scheme in Wavelet Transform for Stego Image Classification in Steganalysis,Evolving Systems, pp. 1-14, Springer 2017.
[21]. Johnson N.F. and Jajodia S., Exploringsteganography: Seeing the unseen, IEEE Computer, vol. 31, Issue 2,IEEE1998.
[22]. Hosmer C., Discovering Hidden Evidence, Journal of Digital Forensic Practice, vol. 1, Issue 1, pp. 47-56, 2006.
[23]. Hermandez J.C. -Castro, Blasco I. -Lopez, Estevez J. M. -Tapaidor, Steganography in games: A general methodology and its application of the Game of Go, Computers and Security, vol. 25, Issue 1, pp. 64-71, ELSEVIER 2006.

*Mr. Yadvendra Prasad Dwivedi. "Review on Universal Steganalysis Techniques Based on the Feature Extraction in Transform Domain." International Journal of Engineering Research and Development, vol. 13, no. 09, 2017, pp. 07–11.