Global Journal of Computer Science and Technology: G Interdisciplinary
Volume 15 Issue 3 Version 1.0 Year 2015
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals Inc. (USA)
Online ISSN: 0975-4172 & Print ISSN: 0975-4350

Steganography Images Detection using Different Steganalysis Techniques with Markov Chain Features

By Rajendraprasad K & Dr. V. B. Narasimha
Osmania University, India

Abstract- Steganography is the art of covered or hidden writing. It is used for criminal activities applications environment. In this paper we focus on implementation of effective detection technique is an essential task in digital images. Previously many number of detection techniques are available for steganography images. After implementation of all approaches also again some challenges are available. This paper presents comparative study in between different steganalysis techniques. Different techniques are providing different results. Analyze of all techniques detection and embedding performance results. Finally we can decide one best steganalysis technique. It saves time and increases accuracy compare to all previous methods.

Index Terms: *steganography, steganalysis technique, digital images, markov chain features.*

GJCST-G Classification: *H.2.8, I.3.3*

Strictly as per the compliance and regulations of:

Steganography Images Detection using Different Steganalysis Techniques with Markov Chain Features

Rajendraprasad K[α] & Dr. V. B. Narasimha[σ]

Abstract- Steganography is the art of covered or hidden writing. It is used for criminal activities applications environment. In this paper we focus on implementation of effective detection technique is an essential task in digital images. Previously many number of detection techniques are available for steganography images. After implementation of all approaches also again some challenges are available. This paper presents comparative study in between different steganalysis techniques. Different techniques are providing different results. Analyze of all techniques detection and embedding performance results. Finally we can decide one best steganalysis technique. It saves time and increases accuracy compare to all previous methods.

Index Terms: steganography, steganalysis technique, digital images, markov chain features.

I. Introduction

Steganography is sometimes referred to as data hiding. Steganalysis technique is opposite to steganography. Steganalysis technique focuses on detecting the presence of hiding data. Steganalysis approaches are two types. Those are

1. Target approach
2. Blind steganalysis

Target approaches provide high accurate detection and reliable results compare to previous other steganalysis techniques. Previously many number of steganalysis techniques are design. Those techniques are steganography detectors, rich model detection scheme, statistics based approach, and movement based approaches. All existing approaches are not efficient under detection and reliable results generation.

In this paper design of new detection scheme using feature set. Feature set consist of different dimensions of input content. Combine of all dimensions of features display as a highly efficient detection results. Comparision study with other techniques also discuss in the remaining sections also. After completion of comparative study which technique is considerable that is also we can decide here.

Author α : Research Scholar, Dept. of Informatics, Osmania University, Hyderabad, Telangana, India.
e-mail: k.rajendraprasad.mca@gmail.com
Author σ : Asst. Prof, Dept. of CSE, Osmania University, Hyderabad, Telangana, India.

II. Related Work

Counter technique of image stenography is known as steganalysis. It's identifies the artifacts that existing in stenography images. Steganalysis provides analysis results from hidden information. Different steganalysis approaches information described below here.

Image stenography detectors contain two parts. Those two parts are image model and machine learning tool. Image model chosen training set of stego and cover images. Primary here we focus on detection accuracy from image model. Stenographic embedding operation image insensitive content converts into sensitive information. We can capture as many dependencies among individual image elements. Observation of all dependencies some of the disturbances are available here. Now here we can calculate the measurement features using spatial and frequency domain. These are DCT (Discrete Cosine Transform) coefficients. All domains of features we can extract with different iterations. Different iterations of features store into different matrices. Combine of all matrices display improved detection accuracy. This kind of process we can call as machine learning from all dimensions.

Here one richer model of JPEG images has different number of sub models. 1. Here capture the DCT coefficients using parallel channels. 2. Joint operation applies on parallel channels DCT coefficients. 3. Finally improved DCT statistical coefficients values are displayed here. Statistical coefficients are useful for construction of image models and steganalysis. Steganalysis results are improved and enhanced in the form robustness and scalability. Finally again we observed some more accuracy related issues.

Next other steganalysis approaches are introduced for increased statistical robustness values and scalability. New steganalysis approaches we can apply on low dimensional and high dimensional environment also. Collection of all dimensions features information and create feature set.

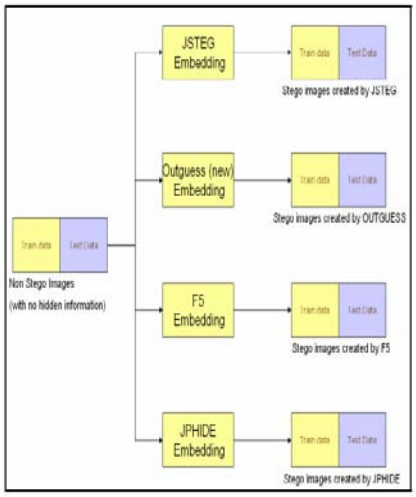

Fig. 1: Steganalysis Procedure

Using higher order statistics in digital images detects stenographic images information. Here we can use quardrature mirror filters for separable of decomposition values in stenographic images. Here two types of separable filters are available. Those are vertical and horizontal filters. Filtering operation can perform subsequently. After filtering operation then we can calculate the statistics using mean, variance and skewness parameters. Finally here we can calculate error statistics also. Statistical features based detection gives effective steganalysis accuracy results compare to previous methods.

After training operation on images using steganographic scheme next apply universal blind detection scheme. Here we can use optimal linear predictor for wavelet coefficients. All wavelet coefficients information collects and display statistical clustering results. Here we can apply threshold operation for separation of stego image from cover image. These kinds of operations are possible limited images database only. This method is not scale well and show low performance results.

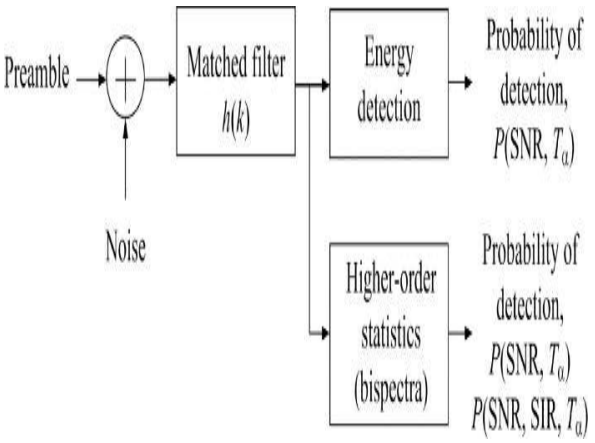

Fig. 2 : probability detection ratio

III. Problem Statement

Previous no single steganalysis technique is not work efficiently. Blindly all steganalysis techniques apply on stego images. All previous steganalysis techniques have take more time and resources.

The main goal of this paper was to the performance analysis of three different steganalysis techniques. Using three steganalysis results next we can perform detection accuracy comparison results. We test on various test images and performance calculation performs based on detected area. Comparison was made based on the number of negatives, positives and misclassified results.

IV. Implementation Details

Steganalysis techniques analyzed are listed below for detection of steganography images. Those techniques are

1. Discriminant analysis based Linear Discriminant Classification.
2. Support vector machines based classification.
3. Image scanning patterns

In all above steganalysis techniques are using logic and features are same. Only the major difference is classification technique only.

Detection technique Procedure

We shall present the new feature set for steganalysis on historical images. Feature set have scanning patterns, markov transition probability matrix, local and global calibrations and classification techniques.

a) Image Scanning Patterns

Image is divided into non overlapping blocks. Scan of each and every block of row and column and other Hibert directions also. We can observe all possible paths of correlations information also its better.

b) Intra and Inter Block Features

i. *Intra Block Features*

We can extract intra block features and store into matrix. Matrix contains DCT coefficients content information. All adjacent coefficients update into matrix. Next apply markov chain operations calculate transition probability features. Here we can perform different orders of markov probability matrix value.

ii. *Inter Block Features*

All orders of probability matrix features are rearrange then store into new matrix. Calculate the average of all orders transition probability value finally. Finally original image features set content display here.

c) Image Calibration

Image calibration is used for accurate statistics. Decompress and finally we can display original image.

d) Classification procedure

Extraction of features and calculate metrics of detection features information as a final output.

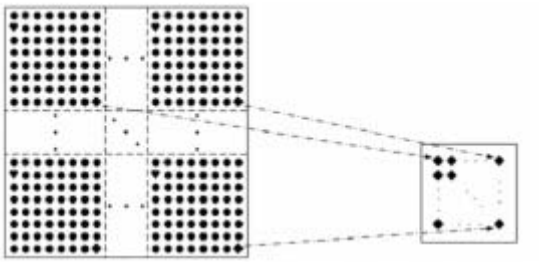

Fig. 3 : Block Feature Set Diagram

V. Experimental Results

Each approach has different features and working with different image databases, it's very complex. Following table have an aim to recapitulate the three approaches information.

Papers / Characteristics	Neural Network Based Steganalysis in Still Images	Steganalysis Based on Moments of Characteristic Functions Using Wavelet Decomposition, Prediction-Error Image, and NN	Texture based steganalysis
Type of steganalysis	Passive	Passive	Passive
Features	Transform domain includes : DFT, DCT, DWT	Moments of characteristics function, Prediction error-image.	LBP(Local Binary Pattern)
Type of Neural Network	Back-Propagation Neural Networks	Feed forward NN with back-propagation.	Not mentioned
Use of ANNs	For classifying	For classifying	For selecting
Number of data hiding methods	One " Brain Chen's quantization (3)	Five " Cox et al. SS, Piva et. al's blind SS , Huang and Shi's block SS, generic QIM and a generic LSB"	One " Blindside"
Images used	Each image is divided into 8x8 sub-block	1096 sample images included in the CorelDRAW (www.corel.com)	1000 clean color JPG images and 1000 stego-images
Results	Hidden images: 85.4% No hidden images: 75.0%	Five methods combined: 98.7 %	Hidden images: 68.5% No hidden images: 99.1%

Table 1: Comparative Study

VI. Conclusion and Future Work

We have proposed scanning patterns based approach for detection of JPEG steganography. Here we utilized feature set approaches for improving detection accuracy. Finally proposed approach compare with existing approaches. Proposed approach gives enhanced performance results, that's why proposed markov chain features approach is best

References References Referencias

1. Jessica Fridrich1, Miroslav Goljan1, Dorin Hogea2, Steganalysis of JPEG Images: Breaking the F5 Algorithm.
2. Z. Li, J. Chen, X.-n. Jiang, X.-t. Zeng and X.-z. Pan, "Blind JPEG steganalysis based on multi-domain feature", Journal of Zhejiang University (Engineering Science), vol. 45, no. 9, (2011), pp. 1528-1538 (in Chinese).
3. Q. Yun, S. C. Chen and W. Chen, "A Markov Process Based Approach to Effective Attacking JPEG Steganography", Proceedings of the IEEE international Conference on Multimedia & Expo 2005. Amstenlam, Netberlands:[s.n.], (2005), pp. 269-272.
4. C. Chen and Y. Q. Shi, "JPEG Image Steganalysis Utilizing both Intrablock and Interblock Correlations", IEEE international Symposium on Circuits and Systems. Seattle, Washington, USA: IEEE, (2008), pp. 3029-3032.
5. T. Pevny and J. Fridrich, "Merging Markov and DCT features for multi-class JPEG steganalysis", Proceedings of the 8th information Hiding Workshop. Alexandria, VA, USA: Springer-Verlag, (2007), pp. 249-264.
6. J. Kodovsky and J. Fridrich, "Calibration Revisited", Proceeding of the 11th ACM Multimedia Security Workshop, (2009), pp. 63-74.
7. F. Huang and J. Huang, "Calibration based universal JPEG steganalysis", Science in china series F: Information sciences, vol. 52, no. 2, (2009), pp. 260-268.
8. K. Li and X.-j. Ping, "Regional Correlation Based Blind Dection of JPEG Image Steganography", Journal of Information Engineering University, vol. 13, no. 3, (2012), pp. 306-311 (in Chinese).
9. T. Pevny, P. Bas and J. Fridrich, "Steganalysis by subtractive pixel adjacency matrix", IEEE Transaction on Information Forensics and Security, vol. 5, no. 2, (2010), pp. 215-224.
10. C. C. Chang and C. J. Lin, "LIBSVM: A library for Support Vector Machines", http://www.csie.ntu.edu.tw/~cjlin/libsvm.

Global Journals Inc. (US) Guidelines Handbook 2015

www.GlobalJournals.org