Global Journals LaTeX JournalKaleidoscope™
Artificial Intelligence formulated this projection for compatibility purposes from the original article published at Global Journals. However, this technology is currently in beta. *Therefore, kindly ignore odd layouts, missed formulae, text, tables, or figures.*

Steganography Images Detection using Different Steganalysis Techniques with Markov Chain Features

Rajendraprasad K[1]

[1] Osmania University

Received: 15 April 2015 Accepted: 30 April 2015 Published: 15 May 2015

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.

1 Introduction

teganography 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.

2 II.

3 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. 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.

4 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.

5 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.

6 Image scanning patterns

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

7 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.

8 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.

9 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.

10 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.

11 c) Image Calibration

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

12 Global

13 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.

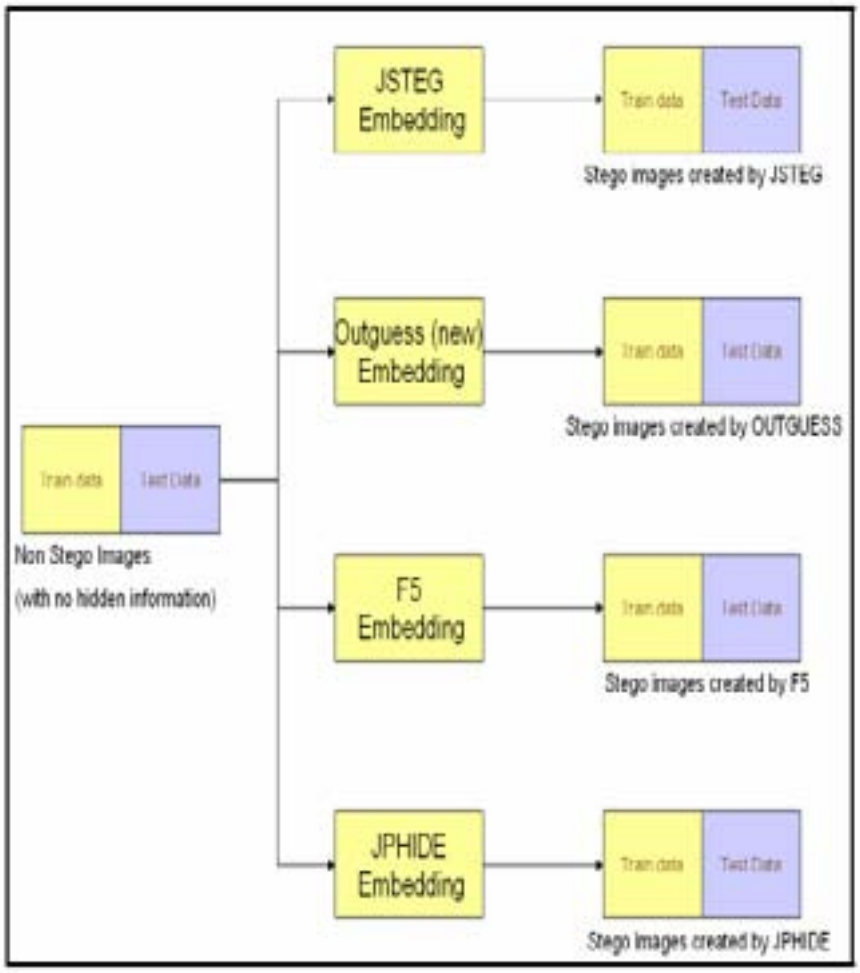
14 Conclusion and Future Work

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 [1]

1

Figure 1: Fig. 1 :

[1] © 2015 Global Journals Inc. (US)



2

Figure 2: Fig. 2 :

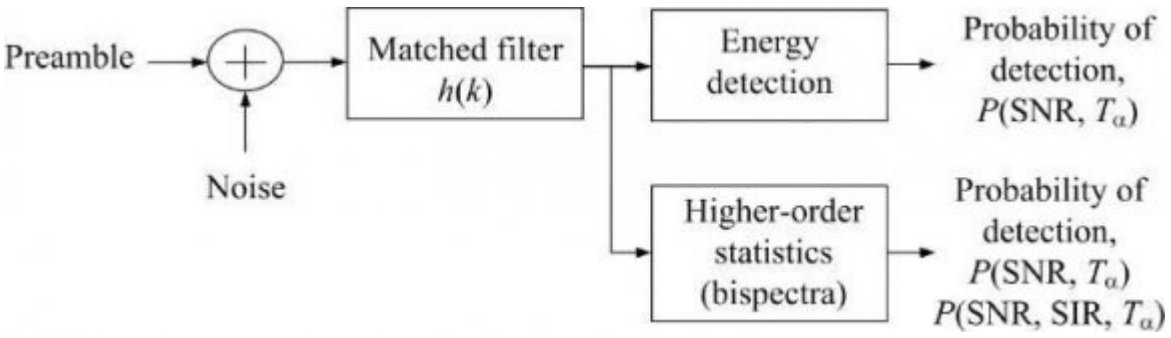


Figure 3:

3

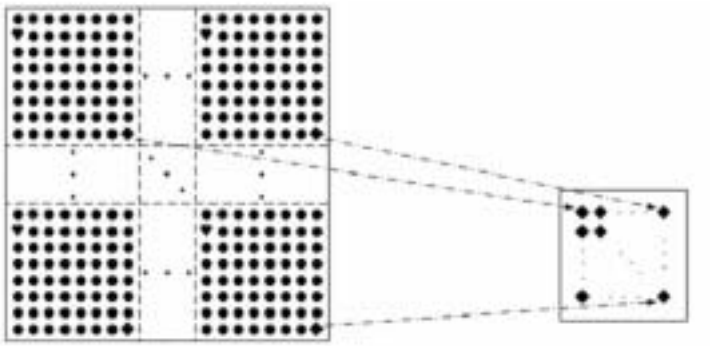


Figure 4: Fig. 3 :

1

Figure 5: Table 1 :

.1 Global Journals Inc. (US) Guidelines Handbook 2015

www.GlobalJournals.org

[Yun et al. ()] 'A Markov Process Based Approach to Effective Attacking JPEG Steganography'. Q Yun , S C Chen , W Chen . *Proceedings of the IEEE international Conference on Multimedia & Expo 2005. Amstenlam*, (the IEEE international Conference on Multimedia & Expo 2005. AmstenlamNetberlands) 2005. p. . (s.n.)

[Li et al. ()] 'Blind JPEG steganalysis based on multi-domain feature'. Z Li , J Chen , X Jiang , X Zeng , X.-Z Pan . *Journal of Zhejiang University (Engineering Science)* 2011. 45 (9) p. . (in Chinese)

[Huang and Huang ()] 'Calibration based universal JPEG steganalysis'. F Huang , J Huang . *Science in china series F: Information sciences*, 2009. 52 p. .

[Kodovsky and Fridrich ()] 'Calibration Revisited'. J Kodovsky , J Fridrich . *Proceeding of the 11th ACM Multimedia Security Workshop*, (eeding of the 11th ACM Multimedia Security Workshop) 2009. p. .

[Fridrich1 and Goljan1] Jessica Fridrich1 , Miroslav Goljan1 . *Dorin Hogea2, Steganalysis of JPEG Images: Breaking the F5 Algorithm*,

[Chen and Shi ()] 'JPEG Image Steganalysis Utilizing both Intrablock and Interblock Correlations'. C Chen , Y Q Shi . *IEEE international Symposium on Circuits and Systems*, (Seattle, Washington, USA) 2008. IEEE. p. .

[Chang and Lin] *LIBSVM: A library for Support Vector Machines*, C C Chang , C J Lin . `http://www.csie.ntu.edu.tw/~cjlin/libsvm`

[Pevny and Fridrich ()] 'Merging Markov and DCT features for multi-class JPEG steganalysis'. T Pevny , J Fridrich . *Proceedings of the 8th information Hiding Workshop*, (the 8th information Hiding WorkshopAlexandria, VA, USA) 2007. Springer-Verlag. p. .

[Li and Ping ()] 'Regional Correlation Based Blind Dection of JPEG Image Steganography'. K Li , X.-J Ping . *Journal of Information Engineering University* 2012. 13 (3) p. . (in Chinese)

[Pevny et al. ()] 'Steganalysis by subtractive pixel adjacency matrix'. T Pevny , P Bas , J Fridrich . *IEEE Transaction on Information Forensics and Security* 2010. 5 (2) p. .