IOSR Journal of Computer Science (IOSR-JCE)
e-ISSN: 2278-0661, p-ISSN: 2278-8727
PP 40-46
www.iosrjournals.org

Improving Blind Image Steganalysis using Genetic Algorithm and Fusion Technique

Sarita R. Visavalia[1], Dr. Amit Ganatra[2]
[1]*Department of Information Technology, CHARUSAT, India*
[2]*Dpartmentof Computer Engineering, CHARUSAT, India*

ABSTRACT : *The Steganography is the science of communication of secret information using carrier/s between two or multiple entities. The secret information can be embedded into an existing image, audio or video or even as a complex combination of all three. In case the secret feature is visible, attention & attack is inevitable & evident, our primary goal is to creatively engineer concealment of the secret information/data on or within a given subject. Steganalysis is a creative art, a process of discovering hidden secrets and successfully extracting the information. In short, steganography is the harbinger of Steganalysis. The recent past has reported a large number of innovative & powerful steganalysis techniques. To make things simple, these techniques could be broadly categorized under two streams, specific-base or universal-base. Each category of techniques has a set of advantages and disadvantages. In real life situations, the steganalyst will not be able to know what or which steganographic technique is used. Here in this paper, we propose a novel method that enables identification of the steganographic technique used to introduce/embed secret information on a conventional item and also offer scalability.*

Keywords -*Steganography, Image Steganalysis, Information Fusion*

I. INTRODUCTION

Steganography is the art of passing information through apparently innocent files in a manner that the very existence of the message is unknown. The term steganography in Greek literally means, "Covered Writing". The files can be referred to as cover text, cover image, or cover audio as appropriate. After embedding the secret message it is referred to as stego-medium. A stego-key is used (optional) to control the hiding process so as to restrict detection and/or recovery of the embedded data. While cryptography is about protecting the content of messages, steganography is about hiding the message so that intermediate persons cannot see the message. Steganalysis is the process of detecting the existence of the steganography in a cover medium. The messages embedded into an image are often imperceptible to human eyes, but there exists some detectable artifacts in the images depending on the steganographic algorithm used [2, 5]. The steganalyst uses these artifacts for the detection of the steganography.

Blind Image Steganalysis techniques detect the existence of secret messages embedded in digital media when the steganography embedding algorithm is unknown. Essentially there are two approaches to the problem of steganalysis; one is to come up with steganalysis techniques that are specific to a particular steganographic technique. The other is developing universal techniques that are effective over a wide variety of steganographic techniques. Specific steganalysis attacks concentrate on image features which are directly modified by the embedding algorithm. Universal steganalysis techniques operate by extracting some inherent features of cover images that are likely to be modified when an image undergoes steganographic embedding process. These features are then used to classify the image as either a cover or stego image.

IOSR Journal of Computer Science (IOSR-JCE)
e-ISSN: 2278-0661, p-ISSN: 2278-8727
PP 40-46
www.iosrjournals.org

II. PROCEDURE FOR BLIND IMAGE STEGANALYSIS

Blind Image Steganalysis techniques detect the existence of secret messages embedded in digital media when the steganography embedding algorithm is unknown. Essentially there are two approaches to the problem of steganalysis; one is to come up with steganalysis techniques that are specific to a particular steganographic technique. The other is developing universal techniques that are effective over a wide variety of steganographic techniques. Specific steganalysis attacks concentrate on image features which are directly modified by the embedding algorithm. Universal steganalysis techniques operate by extracting some inherent features of cover images that are likely to be modified when an image undergoes steganographic embedding process. These features are then used to classify the image as either a cover or stego image. There have been a number of universal steganalysis techniques proposed in the literature which are describes in literature survey in section II. These techniques differ in the feature sets they utilize for capturing the characteristics of images.

First, Blind Image detection for steganography is two-class classification, either stego or original image. Some existing blind image steganalysis methods first extract some features from images, then select or design a classifier, and train the classifier using the features extracted from training image sets, and at the last, classify the features. A general structure of blind steganalysis, which consists of four parts: 1) feature extraction; (2) Train the classifier; (3) Test the classifier; and (4) Detection of image. Unfortunately, to date, there is no detailed framework to describe how to detect images steganography blindly. Here, it is provided a more rounded framework of blind steganalysis tentatively, which consists of the following major parts as shown in Fig 1.

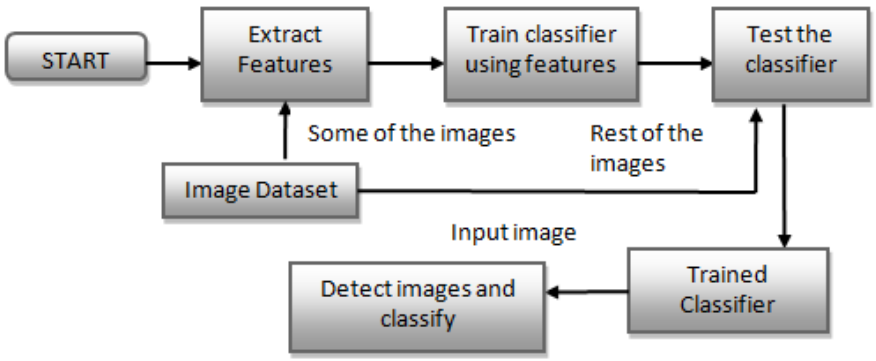

Fig. 1. Structure of Blind Image Steganalysis

III. COMPARATIVE ANALYSIS

Features are extracted or Image Quality Measures are calculated from the stego image. These features are considered in the relative techniques such as BSM, FBS, WBS, and RD. The comparison is shown in Table I.

TABLE I. COMPARISION OF UNIVERSAL STEGANALYSIS TECHNIQUES

Features Extracted in Universal Blind Image Steganalyzer	No of Features	Classifier Used	Format of Image
DCT Coefficients [10]	23	SVM	JPEG
Image Quality Measures [8]	10	Multivariate Regression	-
Rate Distortion Characteristics [9]	3	Bayesian	TIFF
Color wavelet statistics [6]	72	Non linear OC-SVM	JPEG
Higher Order Statistics [7]	72	Three Class SVM	JPEG, GIF, TIFF
Binary Similarity Measure [5]	-	SVM	-

Table II shows the comparison of some of these universal steganographic techniques as well as the extra functionality regarding the specific steganographic technique.

TABLE II. COMPARISION OD UNIVERSAL STEGANALYSIS TECHNIQUE FOR DETECTION

Techniques →	**BSM**	**FBS**	**WBS**	**RD**	**Proposed Method**
Detect Message?	**Yes**	**Yes***	**Yes***	**Yes***	**Yes**
Identify Technique?	**No**	**No**	**No**	**No**	**Yes**

IV. PROPOSED SYSTEM

Features are extracted or Image Quality Measures are calculated from the stego image. These features are considered in the relative techniques such as BSM, FBS, WBS, and RD. The comparison is shown in Table I. Table II shows the comparison of some of these universal steganographic techniques as well as the extra functionality regarding the specific steganographic technique.

Algorithm : Complete Rule Set using Fusion

Input : Image Dataset of specific steganographic techniques

Output: Set of classification rule

Method:

Step 1: For I = 1 to no_of_steganographic techniques

[For image dataset of every steganographic technique]

Calculate IQM between image and its denoised version.

Generate rules for classification using Genetic Algorithm by applying crossover and mutation.

End For

Step 2: For I = 1 to no_of_steganographic techniques

[For rest of the image from respective image dataset]

Perform testing on generated classification rules.

Perform testing for Original Images.

End For

Select Best rules after optimization.

Step 3: Apply information fusion for all classification rule.

As shown in step 2 and step 3 in above algorithm, it is very simple to add new classification rules for specific steganographic technique to the set of classification rules for identification of steganographic techniques. Only one has to derive the rules for pure or stego image for the technique for which one wants to identify the steganographic technique. How the rule can be derived that is shown in below algorithm named as "Rule Set Generation using GA"

To generate the classification rule we have used Genetic Algorithm. Steganalysis of digital images using GA is relatively unexplored. GA is chosen because of some of its nice properties. E.g. robust to noise, no gradient information is required to find a global optimum or sub-optimal solution, self learning capabilities etc. The proposed system uses the selected 11 image quality measures as mentioned in Encoding.

V. EXPERIMENT TERMINOLOGY

A. Data Source

In our experiment we have tested with overall two different data hiding algorithms, i.e.,Stegmark and Jsteg. The image samples from [14] are broadly used to evaluate the steganalyzer. In order to conduct an experimental setting, different sets of 36 JPEG images of 512 X 512 are used. By embedding separately with each steganographic technique, we got an overall of 108 marked records. For each individual method, a mixture containing 24 embedded records and 24 original records are used for training, while 12 original and 12 embedded records is kept for testing purposes.

B. Denoising

All the 108(24 X 3 training and 12 X 3 testing) records are denoised using "wavelet Toolbox - wavemenu" by haar 4 wavelet transform technique. The eleven image quality metrics are evaluated for the respective pair of the image file and its denoised version. Each record of the datasets consists of 11 IQMs and one manually assigned record type i.e., "0 for pure" or "1 for stegotype".

C. Encoding

Sample encoding is like: {MSE, PSNR, LabPE, NE, CC, SPE, SPME, BSME, BSPE, BSPME, L2, 0/1}; Image quality measures used for steganographic technique are different for all. But we have taken superset of image quality measures which are important for different steganographic techniques. For example, spectral phase error, spectral phase magnitude error and block spectral magnitude error are most affected measures for Stegmark while L*a*b Perceptual Error and Neighborhood Error are most affected measures for Jsteg.

VI. EXPERIMENTAL RESULTS

Two experiments have been conducted with images of type JPEG of 512 X 512. The size of the file which we want to hide is maximum 7 – 8% payload of the carrier image file for Jsteg is allowed. The actual steganographic capacity of a given image is dependent on the content of the image as well as the embedding technique used. In the first experiment, the system was trained with the training dataset, and the default fitness function and the GA parameters were used, i.e., with weight 0.2 and 0.8, 100 generations, crossover rate of 0.5, two-point crossover. When the training process was finished, the top best matching quality rules were taken as the final classification rules.Some of the sample rules generated by the GA-Based steganalyzer are:

Rule 1: *if (Spectral Phase Error< "17474931" and Spectral Phase-Magnitude Error< "608"and Block Spectral Magnitude Error < "987") then (image file = "pure");*

Rule 2: *if (Spectral Phase Error > "21794105" and Spectral Phase-Magnitude Error> "761" and Block Spectral Magnitude Error > "1312") then (image file = "StegMark");*

Rule 3: *if (L*a*b Perceptual Error< "145" and Neighborhood Error < "138" then image file = "Jsteg");*

The rules were then used to classify the training data and the testing data respectively. The detection rate with w1=0.2 and w2=0.8 are presented in Table IV.The experiment was repeated for two kinds of weight settings: 1) w1=0, w2=1; and 2) w1=1, w2=0.

TABLE III. DETECTION RATE OF EXPERIMENT1 AND EXPERIMENT2

Record Type	Detection Rate for Training Set in % for Experiment 1	Detection Ratein %	Detection Rate for Training Set in % for Experiment2
Pure	92 %	100 %	100 %
Stegmark	83 %	92 %	100 %
Jsteg	67 %	75 %	83 %

As shown in Fig.2, results are compared with different steganographic techniques tested in 'Steganalysis using Binary Similarity Measure' and 'Steganalysis using Color Wavelet Statistics'.

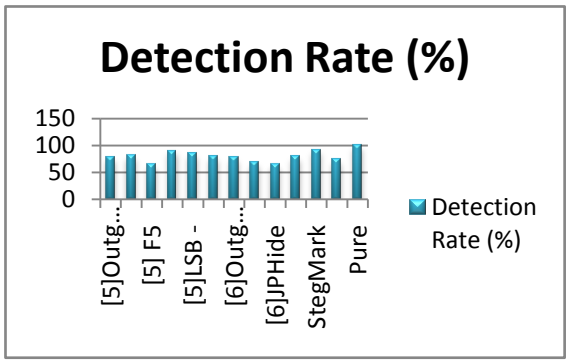

Fig. 2. Detection Rate for specific Steganographic Technique

VII. CONCLUSION

Proposed method for improving Blind Image Steganalysis using fusion technique is an efficient method to improve the performance of image steganalysis. The intension of proposed algorithm is to identify the steganographic technique which is used to hide a secret image into cover image when many steganographic techniques are available and receiver do not know about this. The proposed system is capable to upload and update new rules to the systems, as the new techniques become known. Therefore, it is cost effective and adaptive.

REFERENCES

[1] Mehdi Kharrazi, Husrev T. Sencar, Nasir Memon, "Image Steganography: Concepts and Practice", Lecture Note Series, Institute for Mathematical Sciences, NationalUniversity of Singapore (2004

[2] Abbas Cheddad, Joan Condell, Kevin Curran and Paul Mc Kevitt, "Digital Image Steganography: Survey and analysis of current methods", Signal Processing, March 2010, Pages 727-752

[3] Xiang-Yang Luo, Dao-Shun Wang, Ping Wang, Fen-Lin Liu, "A review on blind detection for image steganography", Signal Processing, Volume 88, Issue 9, September 2008, Pages 2138-2157

[4] Mehdi Kharrazi, Husrev T. Sencar, Nasir Memon, "Benchmarking steganographic and steganalysis technique", Proceedings of the SPIE, Volume 5681, pp. 252-263 (2005)

[5] Ismail Avcibas, Mehdi Kharrazi, Nasir Memon, Bulent Sankur, "Image Steganalysis with Binary Similarity Measure-s", EURASIP Journal on Applied Signal Processing**,** January 2005, Pages 2749 - 2757

[6] Siwei Lyu. Hany Farid, "Steganalysis Using Color Wavelet Statistics and One-Class Support Vector Machines", SPIE Symposium on Electronic Imaging, Volume 5306, Pages 35-45,January 2004

[7] Siwei Lyu. Hany Farid, "Detecting Hidden Messages Using Higher-Order Statistics and Support Vector Machines"

[8] Ismail Avcibas, Nasir Memon, Bulent Sankur, "Steganalysis Using Image Quality metrics", IEEE Trans. on Image Processing, vol. 12, no. 2, pp. 221–229, Feb. 2003.

[9] Mehmet U. Celik, Gaurav Sharma, A. Murat Tekalp, "Detecting Universal Image Steganalysis Using Rate-Distortion Curve", Lecture notes in Computer Science, Volume 2578/2003, Pages 340-354

[10] Tomas Penvy, Jessica Fridrich, "Multi-class Blind Steganalysis for JPEG Images", Proc. SPIE, Volume 6072, 60720O (2006)

[11] Mehdi Kharrazi, Husrev T. Sencar, Nasir Memon, "Improving Steganalysis by Fusion Techniques: A case study with Image Steganography", Proc. Of SPIE, Volume 6072, Pages 607205.1-607205.8

[12] S. Geetha, Siva.S.Sivatha Sindhu, Dr. N. Kamraj, "Evolving GA Classifier for breaking the Steganographic Utilities: Stools, Steganos and Jsteg", Proceedings of the International Conference on Computational Intelligence and Multimedia Applications (ICCIMA 2007) - Volume 04,Pages 230-234

[13] Ismail Avcibas, Bulent Sankur, Khalid Sayood, "Statistical Evaluation of Image Quality Measures", Journal of Electronic Imaging (April 2002) – 11(2), Pages 206-223

[14] Image samples available at: http://www.cl.cam.ac.uk/~fapp2/watermarking/benchmark/image_database