ISSN:0975-9646

Survey on Universal Image Steganalysis

Madhavi B. Desai[#1], Dr. S.V. Patel[*2]

[1#]*Ph.D. Student,Computer Engineering Department,Uka Tarsadia University,*
Maliba Campus,Gopal Vidyanagar, Dist: Surat, Tarsadi – 394345, Gujarat, India

[*]*Professor, Computer Science Department,*
Veer Narmad South Gujarat University, Surat, Gujarat, India.

***Abstract*— Ooverwhelming growth in communication technology and usage of internet has greatly facilitated transfer of data. The threat of unauthorized data access is increasing along with it. Since last decade, too many data hiding methods have been proposed. Because of large number of redundant bits, image has become popular carrier for data hiding techniques. The advancement in image steganography has put forward many security threats like: unauthorized data transmission and reception, commercial spy and terrorist activities etc. To overcome these problems, researchers have started working on development of a method that can detect the existence of hidden message. Broadly speaking these steganalysis techniques are classified in two categories: specific and universal steganalysis. This paper describes various methods proposed by researchers for universal steganalysis. As it is not possible to know which method was used by transmitter, we need to work towards universal approach. This paper analyzes useful contribution made by various researchers in the field of universal steganalysis.**

***Keywords*— Universal Steganalysis, Cover-Image, Stego-Image, Classifier.**

I. Introduction

Information hiding has been a hot research area now a days. Cryptography was used mostly in early days, for secure communication. But, only encrypted information is not secure enough, and that’s why hidden information came in existence, which is known as steganography. Steganography is the art of hiding and transmitting data through carrier such as text, images, audio, video etc. Among this digital images are most popular carrier for data hiding. As digital images has more redundant information and most popular on internet.

Always new technology may also have some negative impacts. Steganography can be misused by criminals for planning and coordinating criminal activities. By embedding messages in images and posting them on public sites, it is difficult to identify the message. It can harm personal privacy, industry or military also. To overcome these types of threats steganalysis came in existence. Steganalysis is science of breaking steganography. The aim of steganalysis is to identify image as cover or stego image. Some may even think of conveying a computer virus via steganography methods. Thus it raises the concerns of developing steganalysis techniques to detect these negative effects. On other side, steganalysis can also serve as a measure of performance for steganographic technique.

Now a day’s many steganography tools are available to hide the data like JSTEG, F5, EzStego, JPHide etc. LSB based tools are also available.

Rest of the paper is organized as follows. Section 2 describes the structure of universal image steganalysis. Section 3 describes the categorization of different methods for feature extraction based on previous work. Comparisons of some popular methods are described in section 4. Section 5 describes about performance evaluation methods and finally in last section 6 summary and conclusions are discussed about the work done by different authors.

II. Structure of Universal Image Steganalysis

Image steganalysis is actually similar to pattern recognition, which centers on two class-classifications: original image and stego image. Blind detection aims at classifying into cover and stego images without prior knowledge of data hiding method. Some existing methods first extracts some features from images, then select or design a classifier, and train the classifier using the features extracted from images and classify it. A general structure of blind image steganalysis, which consists of two main stages: (1) Feature Extraction (2) Classification. In addition, after extracting features, a feature preprocessing may be used to enhance the efficiency of classification. Framework of image steganalysis is as shown in Fig 1.

- **Image Preprocessing:** Some operations are performed on images before feature extracting, such as converting RGB image into grayscale, cropping, JPEG compression, DCT or DWT transformation etc to improve classification.
- **Feature Extraction:** Extract informative features, which are sensitive to data embedding. Features should be low dimension, which will decrease the computation complexity of training.
- **Classifier Design:** selection and design of the classier is performed, on the basis of extracted features. Large set of image database is used for training of the classifier.
- **Classification:** Testing image set is passed to the train classifier deduced in step 3. Classifier will classify image into stego and original image.

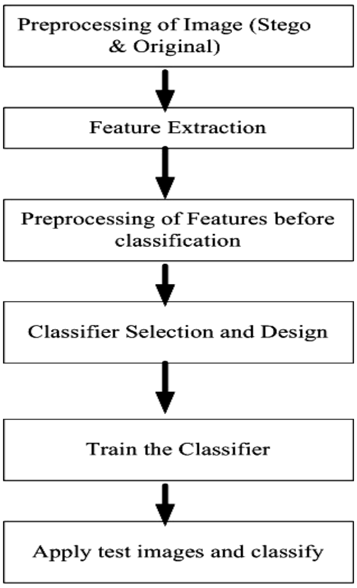
Preprocessing of Image (Stego & Original)
Feature Extraction
Preprocessing of Features before classification
Classifier Selection and Design
Train the Classifier
Apply test images and classify

Fig. 1 Framework of Universal Image Steganalysis

III. Algorithms Used For Feature Extraction

Based on whether an image contains hidden message or not, images can be classified into two classes: cover image and stego image. As per pattern recognition basic task of pattern recognition is features selection. Features should be sensitive to data hiding method. Features should be different for original image and stego image. Larger feature difference means better feature selection. Features should be general i.e. features should be sensitive to all data hiding methods. There can be multidimensional feature vector. Classifier design issue is the second step of steganalysis same as pattern recognition. The following section describes various feature extraction algorithms.

A lot of research work is going on towards development of universal steganalysis method can break all the popular steganography methods. Feature extraction is important part of steganalysis method. Fig. 2 categorizes various features used by the researchers.

A. Image Quality Metrics

A good IQM should reflect the distortion on the image well due to, blurring, compression, additive noise and sensor inadequacy. A good IQM should be accurate, consistent and monotonic in predicting quality. In 2000, Avcibas et. al. [1] conducted a statistical analysis on the sensitivity and consistency behavior of objective IQMs. Twenty six image quality metrics are categorized into six groups according to the type of information they use. The measures are categorized into pixel difference, correlation, edge spectrum, context and HVS-based measures. Their sensitivity and consistency to coding as well as additive noise and blur were investigated by ANOVA. It was found that measures based on HVS, Phase spectrum and edge stability measures are most sensitive to coding and blur artifacts, while the mean square error remains the best for additive noise.

The selection of IQMs decides the accuracy of detection; however the choice of IQMs in existing references is experimental. In practice, it is hard to choose the optimum one due to the existing large numbers of metrics standard. In addition, selection of multiple measures will increase the implement complexity of feature extraction.

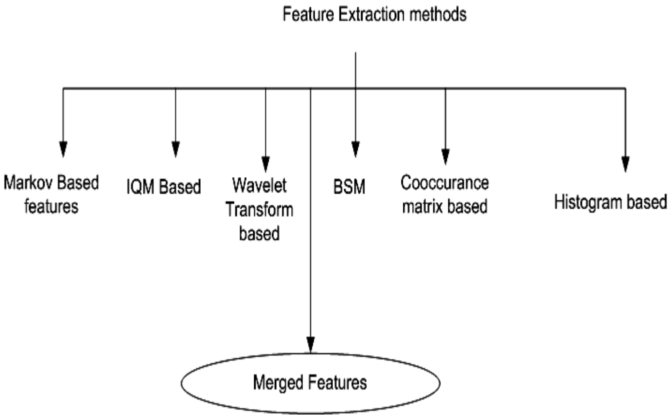

Fig 2 Classification of Various Feature Extraction Methods

B. Markov Based Features

A Steganalysis method by Shie and Chen Et. al. [2] was presented, to effectively detect the advanced JPEG Steganography. Difference JPEG 2-D Arrays along horizontal, vertical and diagonal directions are used and then Markov process is applied to model these difference JPEG 2-D arrays to utilize second order statistics for steganalysis. After this thresholding technique is applied to reduce the feature dimensions. Support Vector Machine (SVM) with polynomial kernel is used as classifier. This method is checked against F5, Outguess and MB1 Steganography.

Zou et. al [3] extracted the markov features from prediction image. Image pixels are predicted with their neighboring pixels and prediction error image is generated by subtracting the prediction value from the pixel value and then thresholded with a predefined threshold. The empirical transition matrix along the horizontal, vertical and diagonal directions serve as features for classifier. For classification SVM with linear and non-linear kernel are used as classifier. SVM with non-linear kernel performed better than SVM with linear kernel. Proposed method is checked against Cox et al, Piva et al, QIM and LSB with different embedding rates. It has been reported by author that proposed method outperforms than K. Suvilian et al[4] method.

Markov features are further extended by Wing and Zhi-Min [5] to original, difference and second difference JPEG arrays. The Markov features based on the original JPEG array capture the characteristics of the distribution of DCT coefficients while Markov feature based on difference and second difference JPEG arrays capture differences among neighboring coefficients. According to author these three merged Markov features improves the performance of steganalysis system. RBFNN (Radial Basis Neural network) is used as a classifier. The experimental results in the paper show that the generalization capability for different image database of proposed method outperforms the methods of Fridrich [6] and Shi and Chen [2].

Markov Features are further expanded to modified markov approach by R. Lakhmi Priya et al. [7]. They have extracted the features from intra block - DCT domain and inter block – DCT domain. Author has finally extracted the features from horizontal and vertical difference arrays along DWT approximation sub-bands. To increase the detection accuracy calibrated features are also calculated from the calibration method. Author has used L-GEM based RBFNN classifier for the classification. Algorithm is tested against MB1, MB2, JSTEG and F5 steganographic method. Author has mentioned that proposed method gives better results than Wing and Zhi-Min [5].

C. Wavelet Transform Features

Farid [8] used a different approach for feature extraction from grayscale images. The decomposition employed is based on separable quadrature mirror filters (QMFs). A statistical model is build which is composed of mean, variance, kurtosis, skew of sub-band coefficients and error statistics from an optimal linear predictor of coefficient magnitudes. A Fisher Linear Discriminant analysis is then used to discriminate between untouched and adulterated images.

Lyu and Farid [9] extended the statistical model to first and higher order color wavelet statistics and exploits the color statistics. A one-class support vector machine (OC-SVM) is employed for detection of secret messages in digital images. This method is tested against JSteg, Outguess, F5, Jphide and Steghide steganography methods. This method has used only JPEG image database.

Lyu and Farid [10] further extended the statistical model to include phase statistics in addition to first and higher order magnitude statistics to extract 432-D feature vector. SVM is used to classify the images. The experiments and results show that this method is more reliable in detecting steganography.

A steganalysis technique based on multiple features is given by Xuan et al [11]. He has taken first three moments and three level Haar wavelet decomposition resulted in 39-D feature vectors. Bayes classifier is used to classify the testing images. Author has used the 1096 CorelDraw images. Method is tested against Cox et al, Piva et al, generic LSB method and generic QIM steganography method. The success classification rate is average 86%.

Wen-Nung and Guo-Siang [12] proposed a set of two image features; the gradient energy and the statistical variance of the Laplacian parameters. The proposed system is effective in detecting any steganography embedding technique and has been shown to give 90% positive detection rate.

For a given gray scale image Shuang - Huan Zhan and Hong-Bin Zhang[13] performed four-order discrete 2-D wavelet decomposition to capture statistical model based on mean, variance, skewness and kurtosis to obtain 36-D feature vector. Another set of 36 elements were obtained from log error statistics of an optimal linear predictor. All 72 elements were further processed by ANOVA (Analysis of variance) to find the sensitivity of these wavelet statistics to hidden message. Steghide, Hide4pgp and S-tools are used to hide message in images. Compared to Farid‘s[8] method testing rate based on ANOVA showed improvement.

The proposed method [14] takes 1-level wavelet decomposition of the image with Haar QMF and divides it in horizontal, vertical and diagonal subbands into overlapping windows. It then constructs an over determined equation system for each window which is solved using Moore-Penrose pseudo-inverse of matrix. Thereafter a linear predictor error for all sub-bands is calculated. The features are extracted from the error vectors obtained from the sub-bands and classified using Linear Support Vector Machine. The experiments confirm that this method is superior to Lyu‘s[10] and Glojan‘s method[15].

Xiangyang Luo and Fenlin Liu[16] firstly, decompose image into three scales through WPT (wavelet packet transformation) to obtain 85 coefficient sub bands together, and extract the multi-order absolute characteristic function moments of histogram from them as features. And then, normalize these features and combine them to a 255-D feature vector for each image. They adopt a back-propagation (BP) neural network to classify cover and stego images. This method has higher average detection accuracy compared to Xuan et al. [11] and Wang method [17] as indicated by experiment results.

Ziwen Sun and Hui Li[18] also classifies using BP neural network on features extracted from characteristic function moments of three-level wavelet sub bands including the further decomposition coefficients of the first scale diagonal sub band. He extends his work by analyzing effectiveness of feature vectors using the Euclidean distance to get better performance. Li Hui, Sun Ziwen et al. [19] utilizes PCA (Principal component analysis) to reduce the features and SVM is adopted as classifier. The detection accuracy improves with reduced feature set.

D. Binary Similarity Measures

Ismail Avcibas [20] developed a steganalysis technique based on binary similarity measures. The basic idea behind this technique was that, the strong correlation between 7th and 8th bit planes as well as the binary texture characteristics within the bit planes will differ if, steganography is applied to an image. This difference was taken as input to SVM classifier to distinguish between stego and cover images. 1800 natural image database was taken for experimental purpose. The steganography algorithms like LSB, LSB +/- where pixel values are incremented or decremented by 1 instead of flipping their least significant bits and JPEG domain algorithms like F5 and Outguess were used.18 different binary similarity measures were obtained for each image to construct 18-D feature vector. These vectors were then used to train and test the SVM classifier. This method provided better results for LSB like methods compare to method proposed by Farid **[8]** in which higher order statistics of wavelet components are used for detecting hidden messages. The Farid methods proved better result for JPEG steganography methods.

Jing-Qu Lin et. al[21] captured the seventh and eighth bit planes of the non-zero DCT coefficients from JPEG images as opposed to bit planes in Avcibas‘s method[20] which are derived from spatial domain. 14 features of each image based on binary similarity measures are computed. C-Support Vector Classification and RBF kernel function is used for classification. This method has close detecting accuracy compared to Fridrich‘s [6] method, but average time is 25 times faster than [6] as no calibration image is generated.

E. Co-occurrence Matrix

Kodovsky et al. [22] designed 7850-dimensional features that are produced from the co-occurrence matrices of DCT coefficient pairs and called as CF features. Since both the intra-block and inter-block dependencies are represented by the features, the steganalysis method can effectively detect the hidden data in JPEG images. An ensemble classifier mechanism is presented to solve the problem, in which the individual Fisher Linear Discrimination (FLD) classifiers are trained in a random feature subspaces with low dimensions, and the final decision on a suspicious medium is made by fusing the individual FLD decisions with majority voting strategy. This way, both the good classification performance and the satisfactory computational complexity are ensured.

The steganalysis scheme by Fengyong Li and Xinpeng Zhang [23] is comprised of two parts : feature extraction and Bayesian ensemble classifier. The features are extracted in two parts: one part is generated from the coefficient co-occurrence matrices, which are 7850 features proposed by Kodovsky[22], while another part is derived from the co-occurrence matrices of coefficient differences. Cartesian calibration method is used to produce other 7850 features; hence a total of 15700 high dimensional feature set is used for steganalysis. The extracted features firstly are to used train a number of sub-classifiers, which are integrated as an ensemble classifier with a Bayesian mechanism. In construction of each sub classifier *d* features from 15700 are used to train FLD (Fisher linear discriminate) classifier. Around 201 sub classifiers are obtained with different subset of features. Embedding method employed is nsF5 and Model based steganography. Merging the two features improves performance by 2%.

Ziwen Sun and Maomao Hui [24] calculates the forward difference in three directions, horizontal, vertical and diagonal, towards adjacent pixels to obtain three-directional differential images for a natural image. Then the differential images are thresholded with a pre-set threshold to remove the redundant information. The co-occurrence matrixes of thresholded differential images are used as features for steganalysis. The performance of this method is evaluated on 3 steganographic methods Cox‘s Spread Spectrum (SS), +-1 method and generic LSB‘s with data embedding rate of 0.3, 0.2 and 0.1 bpp resp. Support vector machine (SVM) with RBF kernel are applied as classifier.

F. Histogram Features

Deng Qian-lan [25] proposed a feature vector as 18 2-D histograms obtained from a given color image, 9 are the 2-D adjacency histogram of the three direction differential image and the other 9 are the 2-D histograms among the differential images of three color plane. After this, 2-D DFT histograms are calculated , resulting in a set of 54 features. Support vector machine with RBF kernel is applied as a classifier.

Deng Qian-lan [26] further extracted features from the DFT of the histogram of differential image. Four histograms are obtained from a given image , 1 from the histogram of image itself and 3 histograms of the difference in three directions, horizontal, vertical and diagonal towards adjacent pixels to obtain three-directional differential images for a natural image. The features are then divided into low and high frequency bands. Support vector machine (SVM) with RBF kernel is applied as classifier.

The run length features proposed by Dong and Tan [27] uses the histogram characteristic function. They take the first three HCF moments for each histogram. Using three different images; quantized image, difference image and original image with four directions; horizontal, vertical, minor and major diagonals, they get a 36-D feature vector which outperforms [28] and [29].

In 2009, T. H. Manjuladevi et. al[30] presented a blind steganalysis method using histogram and DFT of an image. 24-D feature vector was obtained and then SVM classifier was used to differentiate between original and stego versions of images. This method was tested for steganography method S-Tool. The method provided very good detection rate even for embedding rate less than 5%.

G. Merged Features Based Universal Steganalysis

A neural network based steganalysis is given by Shaohui Liu and Yao Hongnun[31]. The digital images, cover as well as stego, are analysed in DCT, DFT and DWT transform domains using neural network. Results indicate that the method is promising.

Penvy and Fridrich [32] proposed a new set of features for steganalysis of JPEG images which is obtained by merging 193 DCT feature set that captures inter-block dependencies among DCT coefficients and Markov features which capture intra-block dependencies. Calibration is applied to Markov features and their dimensionality is further reduced by a factor of 4 hence obtaining 81 Markov features. The resulting feature sets are merged, producing a 274-dimensional feature vector. The new feature set is then used to construct a Support Vector Machine multi-classifier capable of assigning stego images to six popular steganographic algorithms—F5, OutGuess, Model Based Steganography without , and with deblocking, JP Hide&Seek, and Steghide. The new feature set provides significantly more reliable results however the images undergoing double compression have a high probability of misclassification.

Multi-domain features are used for universal steganalysis by Yan et. al.[33]. Features were extracted from gradient energy difference in spatial domain, correlation coefficient in DCT domain and the mean and standard deviation of difference value matrix in DWT domain. This proposed method gives better reliability when embedding capacity is above 2 KB compared to Wnnung Lie et al [34] method. This author has used only BMP images in database.

Xianting Zeng, Xuezeng Pan[35] combine the concepts of image calibration[6] and COM (centre of mass) of HCF (Histogram Characteristic Function) to collect thirteen statistics in the DCT domain and spatial domain, 82-dimensional feature vector for each image is calculated by using the characteristic function and the COM for each statistic. Support vector function (SVM) is utilized to construct the blind classifier. It outperforms Shi et al[29] when spread spectrum steganography method Cox is used. It also gives comparable result with their method when F5, Jsteg, Jphide & seek, Outguess and Steghide is used for embedding.

Shaohui Liu; Lin Ma; Hongxun Yao; Debin Zhao[36] showed that proper reorganization of block based DCT coefficients can have similar characteristics to wavelet transforms. The test and the predicted-error images are decomposed using block-based DCT to generate 228 features. SVM is used as a classifier because of its comparable and efficient classification performance. They have embedded data using LSB (Least Significant Bit), QIM(Quantization Index Modulation) and SS(Spread Spectrum) technique. The method outperforms Farid‘s[8] and shi et al’s method[29].

IV. Summary of Different Universal Steganalysis Methods

Table 4.1summarizes various approaches used by the researches for the detection of various steganography methods. The comparison is shown with respect to type of classifiers used, feature extraction method, feature reduction method, performance evaluation methods adopted to outperform various popular steganography methods. Key points regarding each method are also highlighted in remarks column.

TABLE I
Summary of Various Steganalysis Methods

					Steganography Method										
Paper	Features	Classifier	Feature Reduction Method	Image Type	LSB	F5	Jsteg	Out Guess	MB1	MB2	Jphide &Seek	Steg Hide	SS	Different embeddin	Comment
[1]	IQM	Multivariate Regression Analysis	ANOVA	JPEG Bmp	V		V						V	NO	
[2]	Markov	SVM		JPEG		V		V	V					YES	
[3]	Markov	SVM with Linear and Nonlinear kernel		BMP JPEG	V								V	YES	Non Linear kernel give better result than linear
[5]	Markov	RBFNN		JPEG		V		V	V	V		V		NO	Performance is better than [2]
[7]	Markov	RBFNN		JPEG		V	V		V	V				YES	Performance is better than [5]
[8]	Wavelet	FLD		BMP JPEG	V		V	V						YES	
[9]	Wavelet	SVM		JPEG		V	V	V				V		YES	Tested only with JPEG database
[11]	Wavelet	Bayes		BMP JPEG	V	V	V	V					V	NO	Outperforms [8]
[16]	Back-propogation			BMP JPEG	V	V	V						V	YES	Outperforms [11]
[18]	Wavelet	Backprogation	Euclidean Distance	BMP JPEG	V	V	V	V			V			YES	
[20]	BSM	SVM		BMP JPEG	V	V		V						YES	Better Performance in Spatial Domain than transform domain
[21]	BSM	SVM		JPEG		V		V	V	V				YES	Jpeg only

Paper	Features	Classifier	Feature Reduction Method	Image Type	LSB	F5	J	Out Guess	MB1	MB2	Jphide &Seek	Steg Hide	SS	Different embedding	Comment
[22]	Co-occurrence	Bayesian Ensemble		JPEG		V			V					YES	
[25]	Histogram	SVM		BMP JPEg	V								V	NO	Performance is better against spatial domain steganography
[26]	Histogram	SVM		BMP	V								V	NO	Performance is better against spatial domain steganography
[32]	Merge	SVM		JPEG		V		V	V	V	V	V		Yes	Original Image features better against JPHide&Seek, Calibrated features good against F5
[33]	Merge	SVM		BMP	V									NO	Author has used only BMP image database
[36]	Merge	SVM		Not specified	V								V	YES	Method outperforms [8]

V. Performance Evaluation Methods

Researchers have used various parameters for quantitative evaluation of steganalysis method. Performance of steganalysis method is evaluated against all the steganography methods using three parameters: True Positive (TP), True Negative (TN) and Average.

- True Positive (TP) means stego medium is correctly classified as stego.
- False Negative (FN) means stego medium is wrongly classified as cover.
- True Negative (TN) means cover medium is correctly classified as cover
- False Positive (FP) means cover medium is wrongly classified as stego.

When applying testing data set on classifier generally confusion matrix is define for evaluation [37] is as shown in Fig 3.

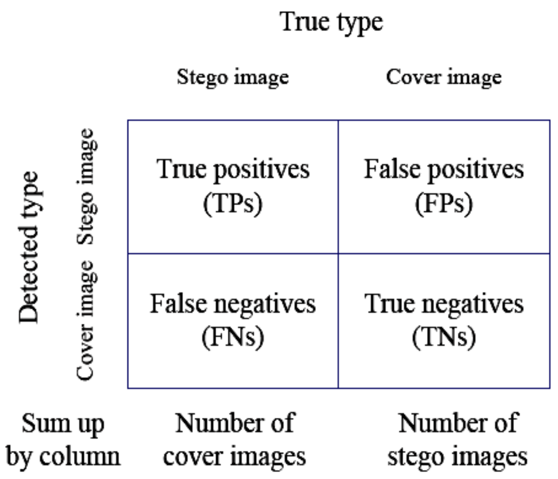

Fig 3 Confusion Matrix[37]

Based on this Confusion matrix,

$$TP\_rate = \frac{TP}{TP + FN} \quad (1)$$

$$FP\_rate = \frac{FP}{TN + FP} \quad (2)$$

$$Accuracy = \frac{TP + TN}{TP + FN + TN + FP} \quad (3)$$

$$\Pr ecision = \frac{TP}{TP + FP} \quad (4)$$

Performance also can be measured by ROC curve.

A. ROC Curve

In this, True Positive Rate is plotted on vertical axis and False Positive Rate is plotted on horizontal axes. If the area under ROC curve is larger, performance of steganalysis method is better.

Some authors have evaluated the performance of steganalysis methods against various embedding rates. The method which can detect stego images with less embedding rate is desired. To obtain a database with various embedding rates various approaches can be used. In one of the paper by Farid [8], message is hidden in the central region of an image with size n x n pixels. Second approach is to take constant length messages say 100, 500 or 1000 bits. Another approach can be: assume that p bits could be embedded in each pixel value, regardless of the depth of the pixels i.e. 8 or 24 bits/pixel. Thus the message length consists of a percentage point of the total number of pixels and the length is independent of the type of image format, bmp or jpeg, but proportional to the size of image.

VI. Summary and Conclusion

Universal steganalysis are more robust as they are designed to detect messages embedded using any steganogrphy method and without knowledge of embedding method. In this report we have categorized the study based on various features extracted and it has been found that features extracted from wavelet coefficients give better results than spatial domain or DCT (Discrete Cosine Transform) coefficients. Because of correlation capability of DWT coefficients of each subband at same level, features generated are independent of each other, which is suitable for steganalysis. Moments of characteristic function of wavelet coefficients provide better efficiency. However the detection accuracy improves when combination of these features extracted from spatial domain and frequency domain is used as shown in merged features.

The performance of steganalysis method also varies with choice of classifiers. Various classifiers used in literature are SVM, Bayesian, Artificial Neural Network, Fisher Linear Discriminator, Linear Discriminant Analysis. Feature Selection Techniques in steganalysis can effectively reduce the cost of recognition by reducing the number of features and can also provide a better classification accuracy due to finite sample size effects. Various feature selection techniques given in the literature survey are ANOVA, Euclidean Distance, Principle Component Analysis and respective authors has claimed that detection accuracy has improved noticeably when these techniques are applied to capture the most relevant features prior to classification.

As new embedding algorithms are being designed now and then, there is still an utmost need for universal steganalysis. Dimensionality being a curse and as can be seen in literature survey features have increased from 23-D features of Fridrich to 15700 given by Fengyong Li, hence future scope lies in universal steganalysis in fusion with feature selection.

References

[1] I. Avcibas, N. Memon, B. Sankur, “Steganalysis of watermarking techniques using image quality metrics,” In Proceedings of the SPIE, Security and Watermarking of Multimedia Contents II, vol. 4314, 2000, pp. 523–531.

[2] Y.Shi, C.Chen, W.Chen, “A Markov process based approach to effective attacking JPEG steganography,” In: Proceedings of the 8th International Workshop, Springer, Berlin, 2006, pp.249–264.

[3] Dekun Zou, Yun Q. Shi, Wei Su, Guorong Xuan, “Steganalysis based on Markov model of threshold prediction-error image,” IEEE, ICME, 2006, pp.1365-1368.

[4] K. Sullivan, U. Madhow, S. Chandrasekaran, and B.S. Manjunath, “ Steganalysis of spread spectrum data hiding exploiting Cover Memory”, SPIE2005, vol. 5681, pp 38-46.

[5] Wing W. Y NG, Zhi-Min He, Patrick P.K Chan, Daniel S. Yeung, “Blind Steganalysis with High Generalization Capability for different Image Databases L-GEM,” Proceedings of the 2011 International Conference on Machine Learning and Cybernetics, Guilin, 10-13 July, 2011, pp. 1690-1695.

[6] J. Fridrich, “Feature-based steganalysis for JPEG images and its implications for future design of steganographic schemes,” In Proceedings of Information Hiding Workshop, Lecture Notes in Computer Science, vol. 3200, Springer, 2004, pp. 67–81.

[7] R. Lakshmi Priya, P.Eswaran, S.L Ponnambli Kamakshi,” Blind Steganalysis with Modified Markov Features and RBFNN,” IJERT, Volume 2, Issue 5, May 2013, e-ISSN 2278-0181.

[8] H. Farid, “Detecting hidden messages using higher-order statistical models,” In Proceedings of IEEE Int. Conf. Image Process., Rochester, NY, vol. 2, September 2002, pp 905–908.

[9] S. Lyu, H. Farid, “Steganalysis using color wavelet statistics and one-class vector support machines,” In Proceeding of SPIE, Security, Steganography, Watermarking of Multimedia Contents, vol. 5306, 2004, pp. 35–45.

[10] S. Lyu, H. Farid, “Steganalysis using higher order image statistics,” In Proceedings of IEEE Trans. Inform. Forensics and Security,vol 1, no.1, 2006 , pp 111-119.

[11] G. Xuan, “Steganalysis based on multiple features formed by statistical moments of wavelet characteristic functions,” In Lecture Notes in Computer Science, vol. 3727, Springer-Verlag, Berlin,2005, pp. 262–277.

[12] Wen-Nung Lie, Guo-Shiang Lin, “A feature based classification technique for blind image steganalysis, IEEE Trans. Multimedia,” December 2005, pp. 1007–1020.

[13] Shuang-Huan Zhan, Hong-Bin Zhang, “Blind Steganalysis using Wavelet Statistics and ANOVA” Machine Learning and Cybernetics, International Conference on Volume 5, August 2007, pp.2515 – 2519.

[14] Anahita Shojaei-Hashemi, Shahrokh Ghaemmaghami, Hamid Soltanian-Zadeh, “Universal Steganalysis based on Local Prediction Error in Wavelet Domain,” Seventh International Conference on Intelligent Information Hiding and Multimedia Signal Processing, 2011, pp. 165-168.

[15] M.Goljan, J.Fridrich and T.Holotyak, “New Blind Steganalysis and its implications,” In Proceedings of Security, Steganography and Watermarking of Multimedia Contents VIII, SPIE vol 6072, 2006, pp 1-13.

[16] Xiangyang Luo, Fenlin Liu, Jianming Chen, Yining Zhang,” Image universal steganalysis based on wavelet packet transform,” Multimedia Signal Processing, IEEE 10th Workshop on Digital, 2008, pp 780 – 784.

[17] Y.Wang and P.Moulin ,"Optimized feature extraction for learning based image steganalysis," IEEE Trans Inf Forensics Security, vol 2, no 1, 2005, pp 262-277.

[18] Ziwen Sun; Hui Li; Zhijian Wu; Zhiping Zhou, "An Image Steganalysis Method Based on Characteristic Function Moments of Wavelet Subbands," Artificial Intelligence and Computational Intelligence, 2009, pp 291 – 295.

[19] Li Hui, Sun Ziwen, Zhou Zhiping, "An image steganalysis method based on characteristic function moments and PCA," Control Conference (CCC), 30th Chinese Publication, 2011, pp 3005 – 3008.

[20] Ismail Avcıbas¸ Mehdi Kharrazi, NasirMemon, B¨ulent Sankur, "Image Steganalysis with Binary Similarity Measures," EURASIP Journal on Applied Signal Processing 2005, pp. 2749–2757.

[21] Jing-Qu Lin, Shang-Ping Zhong, "JPEG Image Steganalysis Method Based on Binary Similarity Measures," Proceedings of Eighth International Conference on Machine Learning and Cybernetics, Baoding, 12-15 July 2009, pp. 2238-2243.

[22] J. Kodovsky, J. Fridrich, and V. Holub, "Ensemble classifier for steganalysis of digital media," IEEE Trans. Inf. Forensics Security, vol. 7, no. 2, April 2012, pp. 432–444.

[23] Fengyong Li, Xinpeng Zhang, Bin Chen, and Guorui Feng, "JPEG Steganalysis With High-Dimensional Features and Bayesian Ensemble Classifier," IEEE signal processing letters, Vol. 20, No. 3, March 2013, pp. 233-236.

[24] Ziwen Sun, Maomao Hui, Chao Guan, "Steganalysis Based on Co-occurrence Matrix of Differential Image", Intelligent Information Hiding and Multimedia Signal Processing, Aug. 2008 pp.1097 – 1100.

[25] Deng Qian-lan, "The blind detection of information hiding in color image," Computer Engineering and Technology (ICCET), Volume: 7,2010, pp.346-348.

[26] Deng Qian-lan, Lin Jia-jun, "A Universal Steganalysis Using Features Derived from the Differential Image Histogram in Frequency Domain, " Image and Signal Processing, 2009, pp. 1 – 4.

[27] Jing Dong and Tieniu Tan, "Blind Image Steganalysis Based on Run-Length Histogram Analysis," National Laboratory of Pattern Recognition, Institute of Automation, Chinese Academy of Sciences, ICIP 2008, pp. 2064-2067.

[28] Xiaochuan Chen;Yunhong Wang; Tieniu Tan; Lei Guo; "Blind Image Steganalysis Based on Statistical Analysis of Empirical Matrix," ICPR , Volume 3, 2006, pp. 1107 – 1110.

[29] Shi Y.Q., Xuan G.r., Zuo D.K.," Steganalysis Based on Moments of Characterstic Functions using Wavelet Decomposition, Prediction-Error Image and Neural Network," Proceedings of IEEE ICME, 2005, Page(s) 269-272.

[30] T. H. Manjula Devi1, H.S.Manjunatha Reddy,2 K. B. Raja3Venugopal K. R3 and L. M. Patnaik4, "Detecting Original Image Using Histogram, DFT and SVM, "International Journal of Recent Trends in Engineering Vol. 1, No. 1, May 2009.

[31] Shaohui Liu, Yao Hongnun, Wen Goa, "Neural network based steganalysis in still images," in: Proc. Int. Conf. on Multimedia and Expo, ICME2003, vol. 2, pp. 509–512, July 2003.

[32] Pevny, T., Fridrich, J., " Merging markov and dct features for multi-class jpeg steganalysis," IS and T/SPIE EI 2007, Lecture Notes in Computer Science, vol.6505, January 29th - February 1st 2007.

[33] Yan et. al , " Universal Steganalysis method based on Multi-Domain Features," Journal of Information & Computational Science, May 2013,pp. 2177-2185.

[34] Y. Wang et. al, "Optimized feature extraction for learning based image steganalysis," IEEE Trans Inf Forensics Secur, Vol 2,No.1, pp. 31-34, 2007.

[35] Zhuo Li, Kuijun Lu, Xianting Zeng, Xuezeng Pan,Feature-Based Steganalysis for JPEG Images 2009, pp. 76 - 80.

[36] Shaohui Liu, Lin Ma, Hongxun Yao, Debin Zhao, Universal Steganalysis Based on Statistical Models Using Reorganization of Block-based DCT Coefficients, 2009 Fifth International Conference on Information Assurance and Security, 2009, Page(s) 778-781.

[37] Bin Lie, Junhui He, Jiwu Huang, Yun Qing Shi, "A Survey on Image Steganography and Steganalysis", Journal of Information Hiding and Multimedia Signal Processing, Vol 2, Issue 2, April 2011,pp 142-172.