International Journal of Multidisciplinary Informative Research and Review
2020; 1(3): 118-126
Published online November 30, 2020 (https://agribusinessedu.com/ijmirr-journal/)
DOI: 10.5281/zenodo.4309803
ISSN: 2709-6289 (Online)

A Steganalysis Techniques Based on Characteristic Function of three level Wavelet Decomposition

Md. Abdullah Al Mamun[1*], Tashrifa Shahid[2], Md. Rafiuzzaman Sarkar[3], Masud Ibn Afjal[4], Md. Fazle Rabbi[5]

[1] Lecturer, Dept. of Computer Science and Engineering, Prime University, Dhaka-1216.
[2] Lecturer, Dept. of Computer Science and Engineering, Prime University, Dhaka -1216.
[3] Lecturer, State College, Dinajpur, Bangladesh.
[4] Assistant Professor, Dept. of Computer Science and Engineering, Hajee Mohammad Danesh Science and Technology University (HSTU), Dinajpur-5200, Bangladesh.
[5] Associate Professor, Dept. of Computer Science and Engineering, Hajee Mohammad Danesh Science and Technology University (HSTU), Dinajpur-5200, Bangladesh.

Email address:

* Corresponding author: mamuncse.40@gmail.com (M. A. A. Mamun)
tashrifashifa@gmail.com (T. Shahid), rafiuzzamanshourav76@gmail.com (M.R. Sarkar), masud@hstu.ac.bd (M.I. Afjal), rabbi@hstu.ac.bd (M.F. Rabbi).

To cite this article:

Md. Abdullah Al Mamun, Tashrifa Shahid, Md. Rafiuzzaman Sarkar, Masud Ibn Afjal, Md. Fazle Rabbi. A Steganalysis Techniques Based on Characteristic Function of three level Wavelet Decomposition . *International Journal of Multidisciplinary Informative Research and Review.* Vol. 1, No. 3, 2020, pp. 118 -126.

Abstract: *Steganalysis technique is the way of detecting stego and cover image which satisfies the needs of individuals and public security communication. But now a days it has become a powerful tool for criminals engaged in crime activities. So steganalysis is required for preventing these crime activities and also to measure the performance level of various steganography tools. In this paper, a modified steganalysis method is proposed for detecting stego image and cover image through prediction error image generation, transformation, feature extraction and classification process. During the generation of prediction error image a GAP(Gradient Adjusted predictor) is used to getbetter detection rate. Then three order haar wavelet transform is performed on the image itself and its prediction error image to get twelve wavelet subbands. Moreover, decomposition of first scale diagonal subband is also applied to get four extra subbands. In feature extraction process, first three order moments of characteristic function of wavelet subbands (including image itself & its prediction error image) are selected to form the feature vectors. Finally, the classification task is performed to classify into cover and stego images using ANN. The method is evaluated for various steganography tools such as StegJ, Openstego, Image Steganography and invisible Secret. The detection rate of the propose steganalyzer is 75-90% and improvement is 5-20.3% using ANN. It also show that the detection rate of the propose steganalyzer is 60-87% and improvement is 1-19.7% using SVM.*

Keywords: *steganalysis; haar wavelet transform; wavelet subbands; moments of characteristic function; prediction error image.*

1. Introduction

Nowadays, the exchange of digital information has grown statistically through home, enterprise, governmental or open networks. In order to assure the information fidelity and to improve the security of communication, the steganography technology is used (Sandal, 16) as it is the art of invisible communication achieved by hiding information inside a carrier file like image, audio, video and protocol. It is known to us that electronic documents such as images contain perceptual irrelevant or redundant information, so that it can be used as cover to hide the secret messages. The image that is used to hide message bits is called the cover image and after embedding the message bit it is called the stego image (Steganalysis: Seminar Report, 2015). Some steganography techniques are spatial domain techniques; transform domain techniques, distortion techniques, masking & filtering techniques. In spatial domain techniques, some bits of images' pixel values are changed directly in data hiding and transform domain embedding can be termed as a domain of implanting techniques for which a number of algorithms have been proposed. Presently, most of the powerful steganography techniques operate in transform domain techniques since it has an advantage over spatial domain techniques as it hides information in areas of the images which are less exposed to compression, cutting and image processing (Manmade, 2015). However, steganalysis is the counterpart of steganography which is used to determine whether a digital file contains hidden information or not. Steganalysis is also momentous for the steganography in order to improve the implementing steganography algorithms. By exposing the deficiency of the algorithm, the user can further elevated the algorithm so that the intruders cannot detect the presence of hidden data inside the image. Thus, steganalysis is especially important in security aspects, namely monitoring a user's communication with the outside world. On the other hand, it is also very important to international security, as terrorist organizations use stenographic techniques to communicate with each other. So it has received a great deal of attention from law enforcement and the media for its significance. According to theoretical categorization various types of steganalysis attacks are chosen stego attack, stego only attack, known cover attack, known message attack, chosen message attack, known stego attack, visual attack, chi-square attack etc. In this way, steganalysis method can be divided into three categories according to more practical categorization. The first one is targeted steganalysis which works on a specific type of stego-system and sometimes limited on image format. The second is blind steganalysis which is designed to work on all types of embedding techniques and image formats and the third one is semi-blind steganalysis that works on a specific range of different stego-system (Bhome, 2010).

In this paper, a steganalysis technique is presented that uses a modified prediction algorithm for getting the prediction error image from the input image. In addition, a comparative study of using various predictors is also shown in this paper according to the detection rate.

2. Literature Review

Steganalysis is relatively new research discipline with few articles that was appeared before late-1990s. However, there are several works done for steganalysis where a few works are available on Blind steganalysis. For instance, the authors of the paper described in (Sun, 2009) proposed a blind steganalysis method based on three order statistical moments of characteristic function. This moment are selected as feature to classify between cover & stego images. It is a wavelet based steganalysis technique where total 102 features are extracted from 34 wavelet subbands. In the paper (Harmsen, 2003) the author indicates that the histogram of a stego images has less high frequency power than cover images. The center of gravity of the histogram will decrease after LSB matching embedding. They proposed a targeted steganalysis algorithm based on the fact that after LSB matching, the local maxima of an image gray level or color histogram decrease and the local minima increase. Consequently, the sum of the absolute differences between local extrema and their neighbors in the intensity histogram of stego images will be smaller than for cover images. One limitation of this method is that it performs poorly on LSB matching in grayscale images. Another paper in (Fridrich, 2005) the author use high pass filter to recover approximate message length using maximum likelihood estimator. This method is used for estimating the number of embedding changes in images. The method uses a high-pass filter and then recovers an approximate message length using a Maximum Likelihood Estimator on those stego image segments where the filtered samples can be modeled using a stationary Generalized Gaussian random process. The limitation of this method is that is not effective for never compressed images.

Next in (Holotyak, 2005) a blind statistical steganalysis of additive steganography is presented using wavelet higher order statistics. This method based on classifying higher order statistical features. Again (Zhang, 2016) the author proposed a region segmentation pre-processing method. The method is based on absolute difference of gray intensity. The entire image is divided into three different regions roughly and then features are extracted according to these regions. This is a blind steganalysis method which uses RS analysis. They propose a new region segmentation algorithm based on absolute difference of image gray (RSADIG) which is mainly used for those steganography algorithms which put BMP format image as carrier. Further in (Zhang, 2007) the author proposed method is a targeted steganalysis algorithm that uses the fact that after LSB matching, Local maxima of images gray level or color histogram decreases Local minima increases The sum of absolute differences between local extrema and their neighbors in the histogram of stego image < cover image. The method is superior to others for never compressed imagery and inferior for decompressed imagery. A blind steganalysis method to cope with the twin difficulties of unknown image statistics and unknown stenographic codes is proposed in (Fridrich, 2002).He showed how a statistical model based on image first-order and high-order magnitude statistics moments derived from high-frequency wavelet subbands could be used to detect steganography in grayscale images. Another method in (Farid, 2002) the author proposed is a steganalysis method based on histogram character function (HCF). By HCF and center of mass (COM) they proposed a method to attack spread spectrum steganalysis in raw images. In (Harmsen, 2004) the author proposed a steganalysis technique for LSB matching in grayscale images. He apply histogram characteristic function based on,

- ❖ Calibrating the output using a down sampled image
- ❖ Computing the adjacency histogram instead of the usual intensity histogram.

An improved version of (Fridrich, 2005) is proposed by author using absolute moments of the noise residua which performs well, it is the histogram extrema method and use GFH algorithm. Main drawback of this method is that if the datasets are JPEG compressed with a quality factor of 80 the high frequency noise is removed then this method performs worse. In this paper, the feature extraction process described in (Sun, 2009) have been improved by using a GAP(Gradient Adjusted predictor). A comparison on the detection rate by using three different predictors is also shown in the paper. In (Y Q Shi, 2011) author first decomposed test image and its prediction-error image into 13 subbands by three-level DWT respectively, then selected 78-dimension vector which are the first three CF moments of these wavelet subbands as features, then select stego image from cover image. The author proposed (David Salomonm, 2013) a steganalysis method based on histogram character function (HCF). By HCF and center of mass (COM) they proposed a method to attack spread spectrum steganalysis in raw images.

3. Proposed Technique

As discussed in the previous section, the author of the paper described in (Sun, 2009) presented a steganalysis technique for detecting steganography based on first three order moments of characteristic function of wavelet subbands that has lower detection rate for some steganography tools. An improvement of that Steganalysis technique has been proposed in this paper. In this proposed technique, a modified prediction algorithm issued. The same haar wavelet transform and feature extraction steps such as, formation of characteristic function, calculation of moments, classification (Sun, 2009), (Salomonm, 2000) are used in this proposed technique as well. Before applying wavelet transform, each input image is converted from RGB to Gray and a GAP (Gradient Adjusted predictor) is used to get the predicted error image from the input image. Then three level haar wavelet transform is applied on each input & its prediction error image. Further decomposition of first scale diagonal subband is performed on both of them. Thus total 34 wavelet subbands are obtained. In the feature extraction process, first three order moments of characteristic function are calculated according to (Salomonm, 2000) to form feature vectors. Total 102 features are selected where, first 51 are selected from input image and last 51 from its predicted error image. These feature vectors of 102 dimensions are used to obtain the dataset. Finally, the classification task is performed using back propagation feed-forward ANN which detect the presence of hidden information inside an input image. The proposed method is evaluated for various steganography tools such as StegJ, Openstego, Image Steganography and invisible Secret and the simulation results show that the detection rate of the propose steganalyzer is 60-90% and the improvement is up to 20% . It also shows the comparison on the detection rate by using different predictors.
The discussed working steps of the proposed steganalysis technique are illustrated in the following flowchart of Fig. 1.

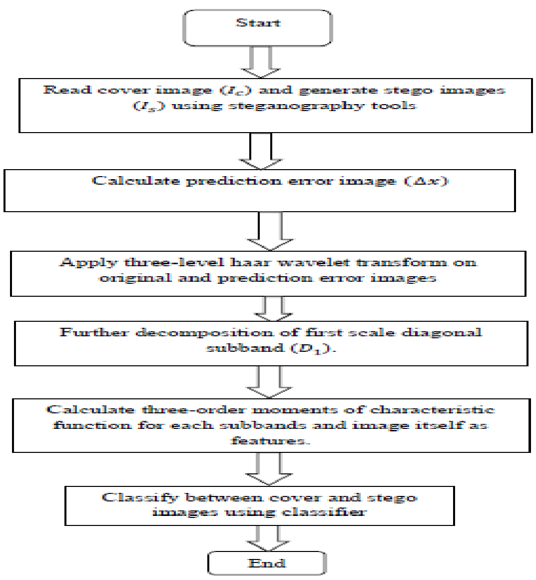


Figure. 1. A Steganalysis Technique

The steps of the proposed method are discussed here in detail:

3.1 Prediction Error Image

In steganalys is we should concern about implicit changes caused by the embedding. This change is so small that it is likely to be concealed by the noise or because of the continuity of the various nature images. If we extract the feature of an image directly, then the ability to distinguish between cover and stego images will be impacted by the image content itself. Therefore in order to enhance the noise introduced by data hiding, it is proposed to predict each pixel grayscale value in the original cover image from its neighboring pixels grayscale values and to obtain the prediction error image by subtracting the predicted image from the test image (Sun, 2009). In the proposed method we have used the following Fig.2 prediction method from which we obtain the prediction error image,

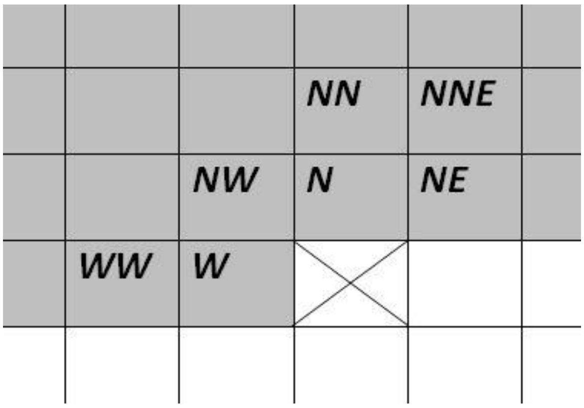


Figure. 2. Causal pixels for GAP predictor

Gradient Adjusted Predictor (GAP) is embedded in CALIC algorithm, one of the representative linear prediction lossless image codes. Most important advantage of the GAP predictor is high adaptability, because GAP recognizes weak, regular and sharp horizontal and vertical edges, as well as smooth areas. To detect edges, predictor uses local gradient testimation and three heuristic defined thresholds. Vertical and horizontal gradients are estimated as follows:

$$g_v = | W - WW | + | N - NW | + | N – NE |$$

$$g_h = | W - NW | + | N - NN | + | NE – NNE |. \quad (3)$$

Labels for causal neighbor pixels are marked on Figure. 3.3. A prediction is further made according to:

If gv – gh > 80, P = W
else if gv – gh < - 80, P = N
else P = (W + N) / 2 + (N E + NW) / 4
If gv – gh > 32 , P = (P + W) / 2
else if gv – gh > 8 , P = (3P + W) / 4
else if gv – gh < - 32 , P = (P + N) / 2
else if gv – gh < - 8 , P = (3P + N) / 4.(4)

GAP achieves smaller error image entropy than MED, but it is far more complicated and uses three heuristic thresholds.
let X is the predicted pixel and P is obtained predicted form, So predicted error image is obtained by E = X - P.

Image 3.2 Feature Extraction

In the feature extraction process, at first the first three CF moments of coefficients of the three level wavelet subbands are taken for the image itself and its prediction error image. Similarly, moment’s are taken from four extra subbands which are obtained by further decomposition of first scale diagonal subbands. These 102 moments are used to construct the feature vector for an input image.

3.2.1 The Statistical Moment of Characteristic Function

The statistics of samples of a random process are completely described by the joint probability distributions: by the probability distribution function (PDF) for a continuous valued random process and by the probability mass function (PMF) for a discrete valued random process. The CF of the image is simply the Fourier transform of the PDF h(X) defined as follows:

$$h(t) = E[e^{jtx}] = \int_{-\infty}^{+\infty} h(x)e^{jtx}\,dx \quad (4)$$

For the CF *h(t)*, its nth moment is defined by:

$$M_n = \int_{-\infty}^{+\infty} h(t)t^n\,dt \quad (5)$$

And its nth absolute moment is given in (4)

$$M_n^A = \int_{-\infty}^{+\infty} |h(t)||t|^n\,dt \quad (6)$$

$|h(t)|$is weighted by $|t|^n$,any change in the tails of $|h(t)|$,which correspond to the high frequency components of h(x), is thus polynomially amplified. The statistical moment of CF,

Mn and M_n^A are related to nth derivation of h(x) at x=0; by

$$M_n = j^n 2\pi \frac{d^n}{dx^n} h(x)|_{x=0} \quad (7)$$

and

$$M_n^A \geq |M_n| = 2\pi|\frac{d^n}{dx^n} h(x)|_{x=0} \quad (8)$$

If a CF h (t) has heavy tails and M_n is large, then the corresponding PDF h(x) is peaky.

CF is defined as

$$\text{h (k)}=\sum_{m=0}^{M-1} h(m)\exp\{\frac{j2\pi mk}{K}\}, 0 \leq k \leq K-1 \quad (9)$$

Ziwen Sun and Hui Li (Sun, 2009) defined the nth absolute moment of the discrete CF by:

$$M'^A_n = \sum_{k=0}^{K-1} |h(k)| sin^n \frac{\pi k}{K} \quad (10)$$

We use the following nth moment of the discrete CF,

$$M'_n = \sum_{k=0}^{K} |h(k)|k^n \quad (11)$$

M'^A_n Provides an upper bound on the discrete derivatives of the histogram$\{h(m)\}_{m=0}^{M-1}$.

In this paper, image and its prediction error image are first decomposed into three level through haar wavelet transform to obtain nine detail subbands. These subbands are horizontal H_i , vertical V_i and Diagonal D_i(I =1, 2, 3).The further decomposition of the first-scale diagonal subband D_1 is used here to improve the performance as described in (Salomonm, 2000). As a result four additional subbands are L_2',H_2' ,V_2' and D_2'.Then we calculate CF moments of these subband coefficients which are three first three order moments of the image itself and the nine detail subbands(horizontal H_i,vertical V_ior Diagonal D_ii=1,2,3),three approximate subbands L_i (i=1,2,3)and also L_2' ,H_2' ,V_2',D_2'.The same CF moments can be obtained for the prediction-error image. so we obtain 102 dimension.

3.2.2The Illustration of the Selected Feature

According to (Sun, 2009), the effectiveness of selected feature is illustrated here, The D-dimensional feature vector$x_k^{(i)}$, $x_k^{(j)}$ are the k'th sample of class ω_i and the l'th sample of class ω_j respectively and$\delta(x_k^{(i)}, x_l^{(j)})$ is the distance between feature vectors of various classes is:

$$J_d = \frac{1}{2}\sum_{i=1}^{c} p_i \sum_{j=1}^{c} p_j \frac{1}{n_i n_j} \sum_{k=1}^{n_i} \sum_{l=1}^{n_j} \delta(x_k^{(i)}, x_l^{(j)}) \quad (12)$$

Where c is the number of classes, n_i and n_j are the number of samples of class ω_i and ω_j respectively, P_i and P_j are priori probability of corresponding classes. The selected feature vector x should enable the largest average distance between samples,

$$\text{J(x)} = \max(J_d(x)) \quad (13)$$

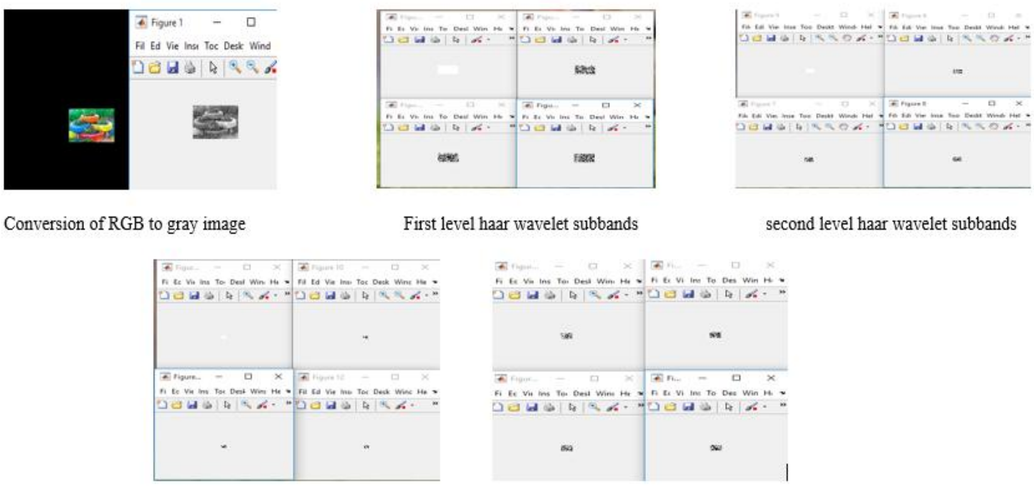
Various distance measure can be used to compute $\delta(x_k^{(i)}, x_l^{(j)})$.

3.3 Classification

After completing feature extraction process the classification task is performed using ANN classifier and SVM classifier. For giving database as input to the ANN need to be processed. Every input image in dataset has the resolution as 80×60×3 for RGB images. Images are then converted to grey images. We have randomly selected 10(5 cover & 5 stego) images for four different steganography tools. For each tool, the processed data matrix dimension is 10×102, where 10 is the number of rows and 102 is the number of columns. For ANN each row is the example image and columns are the features. Each feature of single image is goes to the hidden layer of the ANN and the ANN updates its weights both hidden layer an output layers. The target matrix dimension of the ANN is, No of selected image (For separate tools)×2. No of selected image (For separate tools) is the number of examples. The ANN is trained using training function gradient decent.

4. Experiment and Result Analysis

Let us consider an input image to be classified as shown in Figure. 3. According to this paper, the original images and its prediction error images are first decomposed into three level using haar wavelet transform. We have also used some other wavelet methods instead of using haar wavelet transform for comparison of detection rates. From this comparison, we have seen that there is no change of moments among cover and stego images if other wavelets (like daubechies, Symlet or others) are used instead of haar wavelet. So, the use of haar wavelet is good choice for steganalysis. Through this transform we obtain nine detail subbands including horizontal (H_1, H_2, H_3) vertical (V_1, V_2, V_3) and diagonal (D_1, D_2, D_3). Decomposition of the first scale diagonal subband was proposed to improve the performance of the learning system as in (Ker, 2005). So, four extra subbands are obtained. The reason of doing so is as follows: D_1 is the finest detail subband in the haar wavelet transform and each of its co-efficient involves diagonal differences in a four pixel block.



Conversion of RGB to gray image — First level haar wavelet subbands — second level haar wavelet subbands

Third level haar wavelet subbands — Decomposition of first scale diagonal subbands

Figure. 3. wavelet subbands obtained from input image

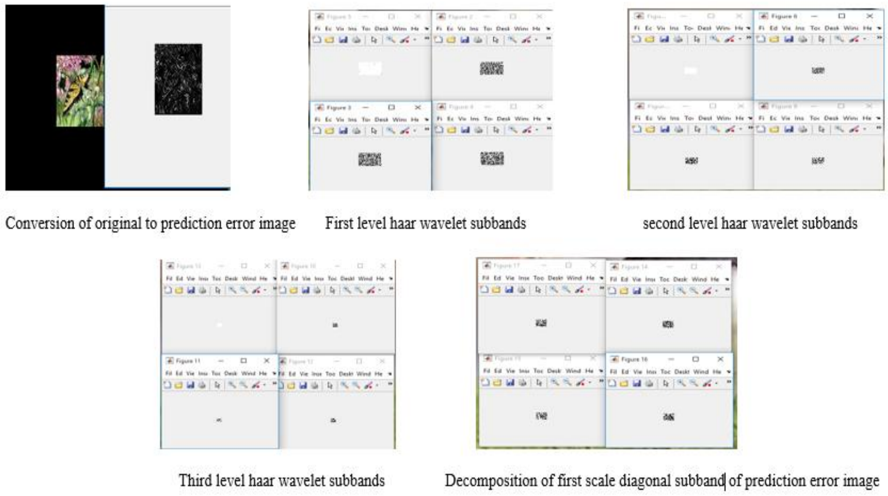


Figure. 4. Wavelet subbands obtained from prediction error image

After that first three order moments of CF are calculated as features: image itself and nine detail subbands, three approximation subbands and also four extra subbands from further decomposition of first scale diagonal subband. The same CF moments can be obtained for prediction error image. So, we obtain 102 dimension features shown in Fig. 5. The whole process is done for all input images.

The above experiment takes four parameter while using ANN classifier. These are Steganography Tools, Image Format, Detection Rate and Improvement. It has also been considered the number of hidden layers while using ANN.

Table 1: The experimental results using ANN

Steg. Tools	**Image Format**	**No. of Hidden layer**	**Detection Rate**			**Improvement using proposed method %**
			Ziwen sun et al. methods	**Using Seven predictor**	**Proposed Method**	
Invisible Secret	JPG	10	65.%	80%	71%	15
Image Steganography	PNG	10	70%	60%	81%	11
OpenStego	PNG	10	75%	90%	80%	15
StegaJ	BMP	10	83.3%	85%	80%	1.7

Table 2: The experimental results using SVM

Steg. Tools	**Image Format**	**Detection Rate**			**Improvement using proposed method %**
		Ziwen sun *et al.* methods	**Using Seven predictor**	**Proposed Method**	
Invisible Secret	JPG	50%	50%	50%	0
Image Steganography	PNG	52%	50%	50%	2
OpenStego	PNG	55.5%	61%	61%	5.5
StegaJ	BMP	70%	81%	81%	11

It is clearly seen that the detection rate and the improvement of this modified steganalysis technique is greater than the existing technique for the mentioned steganography tools.

Table 3: The experimental ratio of dataset

Dataset	No. of cover	No. of stego	Total	Ratio %
Training	7	7	14	54
Testing	6	6	12	46

5. Conclusion

In this paper, a steganalysis technique is presented which classify between cover and stego images. It can detect stego images without having knowledge about the embedding algorithm. The method is developed based on three order CF moments of wavelet subbands. However, it has previously been noted that the addition of noise to an image has a low-pass filtering effect on the intensity histogram of the image and the distortion caused by data hiding may be rather weak and hence covered by other types of noise. The effectiveness of the proposed technique is improved in comparison to the existing solutions because of using a modified predictor which gives the better detection rate. Selected 102 features from each image and its prediction error image are used to obtain feature vectors. Then Classification is performed to classify cover and stego images using ANN. Some steganography tools such as Invisible Secret, Image Steganography, OpenSteg, and StegJ are used to produce stego images. The simulation results show that the detection rate of the propose method is 60-90% and the improvement is upto20% using ANN. Our future work is to develop a fusion based method where fusion will be applied to a set of classifiers.

Copyright

References

[1] Bhme, R. (2010). *Advanced statistical steganalysis*. Springer Publishing Company, Incorporated.

[2] Fridrich, J., Soukal, D., & Goljan, M. (2005, March). Maximum likelihood estimation of length of secret message embedded using±k steganography in spatial domain. In *Security, steganography, and watermarking of multimedia contents VII* (Vol. 5681, pp. 595-606). International Society for Optics and Photonics.

[3] Farid, H. (2002, September). Detecting hidden messages using higher-order statistical models. In *Proceedings. International Conference on Image Processing* (Vol. 2, pp. II-II). IEEE.

[4] Fridrich, J., & Goljan, M. (2002, April). Practical steganalysis of digital images: state of the art. In *Security and Watermarking of Multimedia Contents IV* (Vol. 4675, pp. 1-13). International Society for Optics and Photonics.

[5] Holotyak, T., Fridrich, J., & Voloshynovskyy, S. (2005). Blind statistical steganalysis of additive steganography using wavelet higher order statistics. In *9th IFIP TC-6 TC-11 Conference on Communications and Multimedia Security (CMS 2005)* (pp. 273-274). Springer.

[6] Harmsen, J. J., & Pearlman, W. A. (2003, June). Steganalysis of additive-noise modelable information hiding. In *Security and Watermarking of Multimedia Contents V* (Vol. 5020, pp. 131-142). International Society for Optics and Photonics.

[7] Harmsen, J. J., Bowers, K. D., & Pearlman, W. A. (2004, June). Fast additive noise steganalysis. In *Security, Steganography, and Watermarking of Multimedia Contents VI* (Vol. 5306, pp. 489-495). International Society for Optics and Photonics.

[8] Juarez-Sandoval, O., Cedillo-Hernandez, M., Nakano-Miyatake, M., Perez-Meana, H., & Toscano-Medina, K. (2016, June). Image-adaptive steganalysis for LSB matching steganography. In *2016 39th international conference on telecommunications and signal processing (TSP)* (pp. 478-483). IEEE.

[9] Hong, J; Hu,J; & Zhang,H.(2016). A Study on Preprocessing Method for Steganalysis Feature Extraction", Department of Information Science and Technology Xiamen University, Xiamen, China. In 2016, *10th IEEE*

International conference on Anti-counterfeiting, Security, and Identification(ASID). Doi:10.1109/ICASID.2016.7873886.

[10] Ker, A. D. (2005). Steganalysis of LSB matching in grayscale images. *IEEE signal processing letters*, *12*(6), 441-444.

[11] Li, B., Shi, Y. Q., & Huang, J. (2008, October). Detecting doubly compressed JPEG images by using mode based first digit features. In *2008 IEEE 10th Workshop on Multimedia Signal Processing* (pp. 730-735). IEEE.

[12] Sun, Z., Li, H., Wu, Z., & Zhou, Z. (2009, November). An image steganalysis method based on characteristic function moments of wavelet subbands. In *2009 International Conference on Artificial Intelligence and Computational Intelligence* (Vol. 1, pp. 291-295). IEEE.

[13] Manwade, N., & Nigam, S. (2015). LSB image steganography with DES cryptography. *International Journal of Advanced Research in Computer Science and Software Engineering*, *5*(7), 761-764.

[14] Salomon, D. (2004). *Data compression: the complete reference*. Springer Science & Business Media.

[15] Steganalysis: Seminar Report, PPT, PDF for ECE Students(2015, 23 November), retrieved from http://www.seminarsonly.com/electronics/steganalysis-seminar.php