Image Steganalysis Based on Co-Occurrences of Integer Wavelet Coefficients

M. Abolghasemi[i *], H. Aghaeinia[ii] and K. Faez[iii]

ABSTRACT

We present a steganalysis scheme for LSB matching steganography based on feature vectors extracted from integer wavelet transform (IWT). In integer wavelet decomposition of an image, the coefficients will be integer, so we can calculate co-occurrence matrix of them without rounding the coefficients. Before calculation of co-occurrence matrices, we clip some of the most significant bitplanes of the coefficients. By this preprocessing, in addition to reducing the dimension of feature vector the effects of the embedding are also preserved. We test our algorithm for different embedding rats using Fisher linear discrimination (FLD) classifier and by comparing it with the current state-of-the-art steganalyzers; it is shown that the proposed scheme outperforms them by significant margin.

KEYWORDS

Integer wavelet transform (IWT), LSB matching, Steganography, Steganalysis

1. INTRODUCTION

Information hiding has become the focus of many researchers in the recent years. This is the art of hiding a message signal into a host signal, such as audio, video and still images without any imperceptible distortion of the host signal. To embed a message, the host signal is slightly modified by embedding techniques. Many steganography software algorithms can be downloaded freely from the Internet. Especially with the expanding use of internet and ease of digital communication, steganography have been developed in recent decade. Because the detailed changes of an image cannot be understood by human vision, it is the most interesting media for steganography, especially on the internet. Many steganography methods are introduced which embed the message based on kinds and structure of an image. None of these algorithms can completely provide immunity. Many steganalysis algorithms also have been proposed to detect the presence of hidden message [1, 2].

The steganalysis techniques proposed in the literature can be classified into two categories: the specific steganalysis, which is designed to attack a specific steganography technique, and the universal steganalysis, which is designed to detect the hidden message embedded with various data embedding algorithms. The steganalysis and detection is based on getting the characteristic difference between the normal images and stego images concealed the secret message. In other view, steganalysis techniques can be broadly divided into two groups, a) Passive steganalysis: Detects the presence or absence of a secret message in an observed media and b) Active steganalysis: Extracts an approximate version of the secret message or estimates some parameters such as the embedding key, message length, etc. using a stego media [3].

In the next section we briefly review LSB matching embedding. Previous works which presented for steganalysis of it are introduced in section 2. Features extraction algorithm for proposed method (we called it IWBS) is discussed in Sec. 4. In Sec. 5, the experimental results in comparison with state-of-the-arts LSB matching steganalysis methods are presented. Finally, the conclusions are drawn in Sec. 6.

2. LSB MATCHING

Many different steganography algorithms proposed to embed a message in an image. Some of these methods work based on least significant bits (LSBs) of image pixels and the others use transform domain to embed a message. For LSB matching, first one converts the secret data into a stream of bits then he/she takes each pixel of the cover image possibly in a pseudo-random order generated by a shared secret key. If the embedding bit is

i* Corresponding Author, M. Abolghasemi is with the Department of Electrical Engineering, Amirkabir University of Technology, Tehran, Iran (e-mail: mo_abolghasemi@aut.ac.ir).

ii H. Aghaeinia is with the Department of Electrical Engineering, Amirkabir University of Technology, Tehran, Iran (e-mail: aghaeini@aut.ac.ir).

iii K. Faez is with the Department of Electrical Engineering, Amirkabir University of Technology, Tehran, Iran (e-mail: kfaez@aut.ac.ir).

the same as LSB bit it remains unchanged. Otherwise the pixel value is added randomly to 1 or -1 [4]. Steganalysis of this method is more difficult in comparison with simple LSB embedding especially in gray level images. Mathematically it can be shown as follows:

$$I_s = \begin{cases} I_c + 1, & if\ b \neq LSB(I_c)\ and\ \ (r > 0\ or\ I_c = 0) \\ I_c - 1, & if\ b \neq LSB(I_c)\ and\ \ (r < 0\ or\ I_c = 255) \\ I_c, & if\ b = LSB(I_c) \end{cases} \quad (1)$$

Where I_s and I_c respectively denote a pixel value in the stego and cover image, b is the message bit to be hidden, and r is an i.i.d random variable with uniform distribution on $\{-1,+1\}$. Steganalysis of this method is *more* difficult in comparison with simple LSB replacement especially in gray level images and fewer detectors have been proposed for LSB matching.

3. PREVIOUS WORKS

Harmsen and Pearlman presented a steganalysis method based on modeling steganography as a type of noise [4]. They noted that this operation affects the histogram characteristic function (HCF), by shifting it slightly toward zero. They then measured this effect using the center of mass (COM), or geometric mean of the HCF. For a color image, the addition of noise to the HCF has a well-defined behavior. While theoretically, this logic applies to a grayscale image, practically it is not very useful. The addition of noise changes the number of colors present in an image to greater than what is naturally present, causing the HCF to shift from a "reasonable" value to an "unreasonable" one. But in grayscale images, the number of grayscale tones used in the image is very large compared to the number of possible tones; in many natural images all grayscale tones can be used. Simply adding noise no longer shifts the HCF to a value beyond what is naturally found in clean images. Ker noted this and extended Harmsen's method by adding a "calibration" step [5]. Instead of simply computing the COM of the HCF, Ker also computed the HCF-COM of a downsampled version of the image. This new COM is used to give a reference point from which to measure an "abnormal" deviation. By experiment, Ker showed that the noise added by steganography caused a bigger shift from the downsampled image than a non-stego image.

Xuan et al. presented a steganalysis method based on co-occurrence matrix [6]. They consider different directions for gray-level co-occurrence matrix calculation and obtained the mean of them (We called it gray-level co-occurrence based steganalysis or GCBS). For feature reduction, they considered the main diagonal elements and three diagonals above it as features and also used class-wise non-principal components analysis (CPNCA) algorithm for decreasing feature dimensionality. They used these features for steganalysis of SS, QIM, and LSB replacement data hiding.

Goljan *et al.* [7] presented wavelet absolute moment (WAM) algorithm for steganalysis of LSB matching. They calculate the features from the noise component of an image in wavelet domain. They extract 27 moments for steganalysis purpose. In [8] Zhang *et al.* proposed Amplitude of Local Extrema (ALE) method for detection of LSB matching that based on the statistics of the amplitudes of local extrema in gray level histogram. He showed that the performance is comparable or superior to other state-of-the-art algorithms. Cancelli *et al.* improved this method with reducing the noise associated with border effects in the histogram and extended the analysis to amplitudes of local extrema in 2D adjacency histogram [9]. They also compared the performance of previous three steganalysis methods for detection of LSB matching steganography [10].

In the previous work, we presented a scheme based on the co-occurrence matrix of pixel values for LSB matching data hiding method [11] and provided some insights that have motivated our steganalysis method to test it for wavelet lifting scheme coefficients. In this paper, we focus on image steganography which is performed in the spatial domain (LSB embedding). Indeed we extend our method based on integer wavelet transform, and it is shown that the proposed steganalysis scheme improves the results and outperforms the existing methods by a significant margin under all embedding bit rates. We obtain integer wavelet coefficients of an image based on lifting scheme and then calculate the co-occurrences of them as features and use it for steganalysis of LSB matching.

4. PROPOSED STEGANALYSIS SCHEME

The co-occurrence matrix of the image and (IWT coefficients) tends to be diagonally distributed because the gray-levels of the neighbor pixels in natural images are often highly correlated. After the data embedding, however, the high-concentration along the main diagonal of gray-level co-occurrence matrix spreads because the high-correlations between the pixels in the original image have been reduced. We obtain co-occurrence of the integer wavelet coefficients to attack LSB matching steganographic technique. The process of proposed algorithm is depicted in Fig.1. First we use one level for integer wavelet transform for decomposition of an image using lifting scheme, and obtain four subbands of wavelet coefficients, i.e C_A, C_V, C_H, C_D. Using integer wavelet, we don't need round the wavelet coefficients and stego message due to steganography method was remained in these coefficients. After integer wavelet decomposition, the features of each subband are calculated with co-occurrence & wavelet (C&W) algorithm, which is illustrated in Fig. 1b. Therefore we obtain feature vectors corresponding to each subband, i.e F_A, F_V, F_H, F_D. We will report the result of steganalysis for each feature vector and fused vectors in the next section. The C&W algorithm are described at four steps.

Step 1: We take absolute values of the coefficients of each subband. After that we delete some of the most significant bitplanes of the coefficients before obtaining co-occurrence matrix of them. In the other word, we consider only four least significant bitplanes of the coefficients and clip the other most significant bitplanes. By this preprocessing, in addition to obtaining feature vector with lower size, also we highlight the effects of embedding process. Because LSB matching steganography changes the least significant bits and the most significant bits have little or no changes, thus with clipping some of the most significant bitplanes of integer wavelet coefficients, stego signal isn't removed. Also because the nature of an image is lowpass, most information of an image is in the most significant bitplanes, so the deletion of these bitplanes makes the features calculated from remaining parts more sensitive to embedding and less sensitive to image content especially for detail subbands. Indeed this technique increases SNR between the stego signal and cover image. Also clipping the most significant bitplanes has greatly reduced dimensionality of feature vectors to a manageable extent.

Step 2: The co-occurrence matrix, similar to the empirical matrix can be recognized as a matrix form the two-dimensional normalized histogram. We consider the asymmetry of the co-occurrence matrix and considering all elements of co-occurrence matrix, construct the feature vector. This matrix is defined over integer wavelet coefficients to be the distribution of co-occurring values at a given offset. Mathematically, a co-occurrence matrix $\mathbf{M}$ is defined over a $n \times m$ matrix C, parameterized by an offset (dx, dy) as [12]:

$$\mathbf{M}_d(m,n) = \#\{(x,y) | C(x,y) = m, C(x+dx, y+dy) = n\} \quad (1)$$

We consider the four directions i.e., $\theta = 0^\circ, 45^\circ, 90^\circ, 135^\circ$, $dx = dy = d = 1,2,3$, and calculate four co-occurrence matrices, $\mathbf{M}_d^1, \mathbf{M}_d^2, \mathbf{M}_d^3, \mathbf{M}_d^4$ respectively.

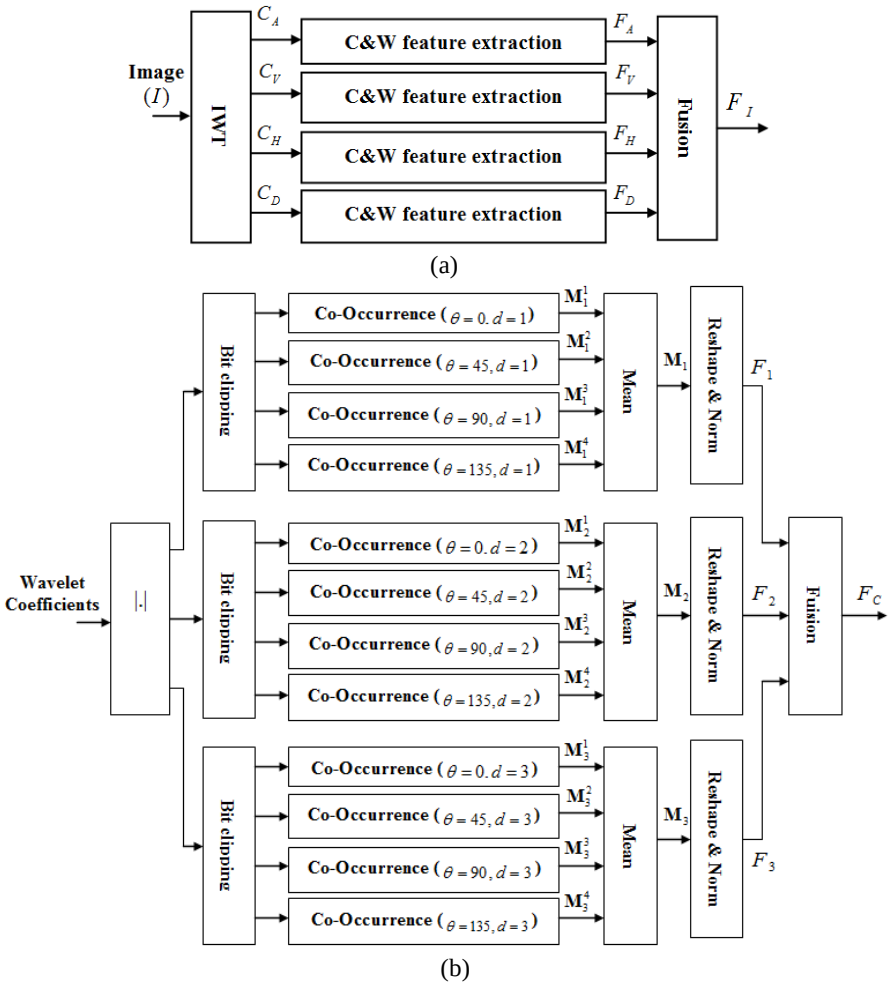

Figure 1: a) Block diagram of proposed scheme for steganalysis, b) C&W algorithm for feature extraction

Step 3: After calculation of the co-occurrence matrices for different directions, we calculate the resultant co-occurrence matrix as following:

$$\mathbf{M}_d = (\mathbf{M}_d^1 + \mathbf{M}_d^2 + \mathbf{M}_d^3 + \mathbf{M}_d^4)/4 \quad (2)$$

Therefore we have three co-occurrence matrices, i.e $\mathbf{M}_1, \mathbf{M}_2, \mathbf{M}_3$. Then we generated the following resultant feature vectors:

$$F_d' = \mathrm{Re}\,shape(\mathbf{M}_d) = \{r_1 \mid r_2 \mid ... \mid r_{2^p}\} \quad (3)$$

Where $p = 4$ and *Reshape* is converting of the matrix to vector with concatenating the rows of the matrix together. So the size of the feature vector F_d will be 256. Finally the feature vectors elements are normalized:

$$F_d(i) = \frac{F_d'(i)}{\sum_j |F_d'(j)|^2} \quad (4)$$

Step 4: At this stage we have three feature vectors F_1, F_2, F_3 related to different distances, i.e $d = 1,2,3$. We can fuse them with different methods. We combine them by concatenating them:

$$F_C = \{F_1 \mid F_2 \mid F_3\} \quad (5)$$

Fusion at this stage would be best in an information theoretical sense, since the features are incorporated without any processing. The size of resulted feature vector will be 768.

5. Experimental Results

We test carefully our algorithm for Camera database which used in [7] and utilized it to generate different stego images for evaluation of our method. The images have been converted to gray scale with 8 bit-depth and centrally cropped with size of 512×512 pixel. The Camera database includes 3,164 images captured using 24 different digital cameras (Canon, Kodak, Nikon, Olympus and Sony) previously used in [7]. They include photographs of natural landscapes, buildings and object details. All images have been stored in a raw format i.e. the images have never undergone lossy compression.

We generated stego-images with LSB matching algorithm for different embedding rates between 0.05 bpp to 1 bpp. These test images contained a variety of images. Then we extracted feature vectors F^c and F^s corresponding to cover and stego images. We randomly selected half of vectors of cover and the corresponding vectors of stego-images for training and the rest for testing. We used FLD classifier and obtain receiver operating curves (ROC) and area under ROC curves (AUR) for evaluation of our algorithm [13]. In our experimental work, we extracted feature vectors for different subbands of wavelet coefficients, F_A, F_V, F_H, F_D for different embedding rates 0.01-0.5 bpp (Camera database), and obtain corresponding AUR values. The results are depicted in Fig. 2. For combination of these feature vectors, we obtain the fused vector as following:

$$F_{Fused} = aF_A + bF_V + cF_H + dF_D \quad (6)$$

Where, a, b, c, d are constant factors for combining the feature vectors. From Fig. 2, it can be seen that features which were extracted from detail subband, i.e F_D, have more AUR value against the other subbands, so we consider more gain for F_D. We test different values for these factors, and experimentally, consider $a = b = c = 0.005$ and $c = 0.6$. Details of the AUR values are summarized in table I.

We carefully compare our results with the current steganalyzers such as KER [5], GCBS [6], WAM [7], ALE [9], and CBS [4]. We obtained feature vectors of each algorithm for three databases with different embedding rates.

The ROC curves of KER, GCBS, ALE, WAM, CBS schemes and proposed method (we called it IWBS) steganalysis are shown in Fig. 3-5 for 0.1, 0.25, and 0.5 bpp embedding rates, respectively. It was clear from these results, that our algorithm outperforms the state-of-the-arts steganalyzers for detecting LSB matching steganographic method for gray scale images. The AUR values also are depicted in these figures. It is seen from these figures, he AUR values for IWBS method are 0.1 more than the other steganalysis schemes approximately for all embedding rates.

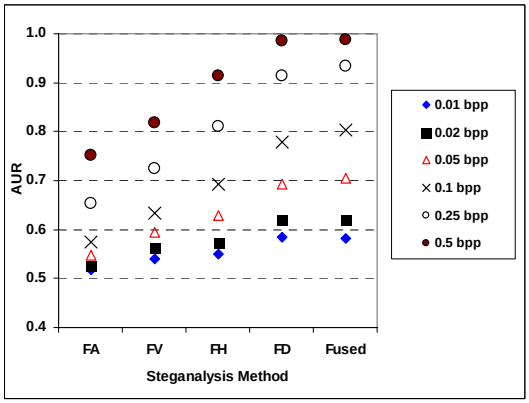

Figure 2: AUR values for $F_A, F_V, F_H, F_D, F_{Fused}$ vectors, embedding rates between 0.01 to 0.5

TABLE 1
THE RESULTS FOR $F_A, F_V, F_H, F_D, F_{Fused}$ VECTORS, EMBEDDING RATES BETWEEN 0.01 TO 0.5

Embedding Rate (bpp)	F_A	F_V	F_H	F_D	F_{Fused}
0.01 bpp	0.518	0.539	0.55	0.584	0.582
0.02 bpp	0.527	0.561	0.573	0.618	0.62
0.05 bpp	0.548	0.595	0.628	0.693	0.704
0.1 bpp	0.575	0.633	0.692	0.779	0.804
0.15 bpp	0.606	0.664	0.735	0.832	0.852
0.2 bpp	0.631	0.698	0.772	0.878	0.897
0.25 bpp	0.654	0.725	0.81	0.915	0.933
0.5 bpp	0.751	0.819	0.914	0.984	0.989

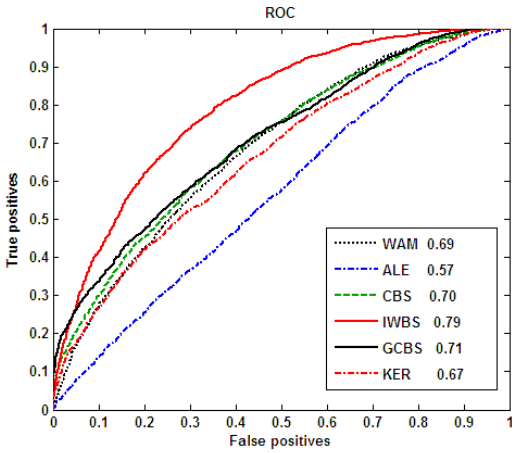

Figure 3: ROC curves for steganalysis methods, GCBS, ALE, WAM, CBS, and IWBS, embedding rates is 0.1 bpp

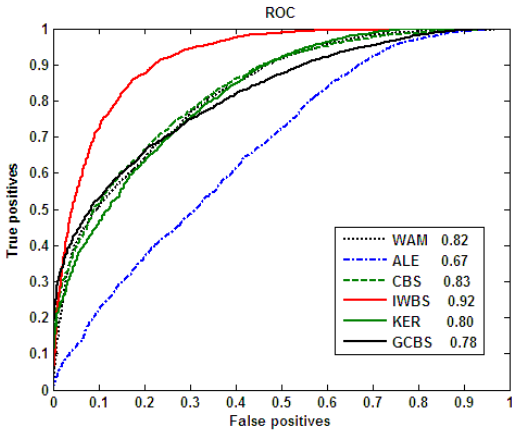

Figure 4: ROC curves for steganalysis methods, GCBS, ALE, WAM, CBS, and IWBS, embedding rates is 0.25 bpp

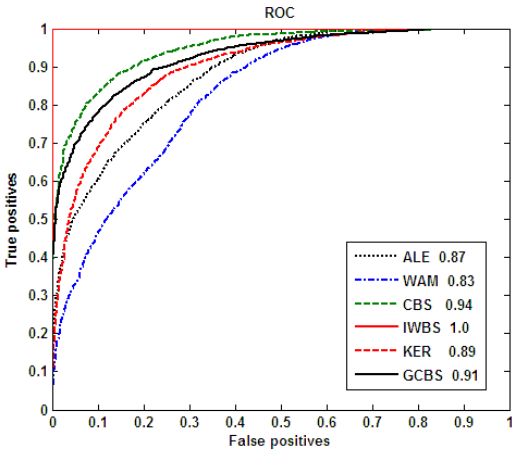

Figure 5: ROC curves for steganalysis methods, GCBS, ALE, WAM, CBS, and IWBS, embedding rates is 0.5 bpp

6. CONCLUSION

This paper has discussed a new steganalysis method based on features which were extracted from co-occurrence matrices of integer wavelet coefficients which some of its most significant bitplanes are deleted. We investigated different IWT subbands for feature extraction, and it was shown that the features which were extracted from IWT detail coefficients, F_D can greatly detect LSB matching embedding method. The tests were done carefully on different databases and compared with current steganalysis methods. It was shown that our algorithm (IWBS) outperforms the state-of-the-art steganalyzers with significant margin for detecting LSB matching steganographic method.

7. ACKNOWLEDGMENTS

The authors would like to thank J. Fridrich and M. Goljan for providing the source code of the WAM steganalyzer and also G. Cancelli and G. Döerr for providing a good website, including the standard databases and the source code of the ALE steganalyzer.

8. REFERENCES

[1] Mehdi Kharrazi, Husrev T. Sencar, and Nasir Memon, “Image Steganography: Concepts and Practice” WSPC/Lecture Notes Series, April 22, 2004.

[2] Mehdi Kharrazi, Husrev T. Sencar, Nasir Memon, "Performance study of common image steganography and steganalysis techniques" Journal of Electronic Imaging 15(4), 041104 (Oct–Dec 2006).

[3] R. Chandramouli, "A mathematical framework for active steganalysis", Multimedia Systems © Springer-Verlag, Vol. 9, pp. 303–311, 2003.

[4] J. J. Harmsen, W. A. Pearlman, “Steganalysis of additive noise modelable information hiding” In E. J. Delp and P. W. Wong, editors, Proceedings SPIE, Electronic Imaging, Security, Steganography,and Watermarking of Multimedia Contents V, vol. 5020, pp. 131-142, Santa Clara, CA, January, 2003.

[5] A. Ker, "Steganalysis of LSB Matching in Grayscale Images" IEEE Signal Process. Lett., vol. 12, no. 6, pp. 441–444, June, 2005.
[6] G. Xuan, Y. Q. Shi, C. Huang, D. Fu, X. Zhu, P. Chai, J. Gao, "Steganalysis Using High-Dimensional Features Derived from Co-occurrence Matrix and Class-Wise Non-Principal Components Analysis (CNPCA)" IWDW, pp. 49-60, 2006
[7] M. Goljan, J. Fridrich, and T. Holotyak, "New blind steganalysis and its implications," In E. J. Delp and P. W. Wong, editors, Proceedings SPIE, Electronic Imaging, Security, Steganography, and Watermarking of Multimedia Contents VIII, vol. 6072, pp. 1-13, January, 2006.
[8] J. Zhang, I. J. Cox, and G. Do¨err, "Steganalysis for LSB matching in images with high-frequency noise," in Proceedings of the IEEE Workshop on Multimedia Signal Processing, October 2007.
[9] G. Cancelli, G. Doërr, I. J. Cox, and M. Barni, " Detection Of ±1 LSB Steganography Based On The Amplitude Of Histogram Local Extrema", International Conference on Image Processing (ICIP) 2008.
[10] G. Cancelli, G. Doërr, I. J. Cox, and M. Barni, "A comparative study of ±1 steganalyzers," In Proceedings IEEE, International Workshop on Multimedia Signal Processing, pp. 791-794, Queensland, Australia, October 2008.
[11] M. Abolghasemi, H. Aghainia, K. Faez, M. A. Mehrabi, "Detection of LSB±1 steganography based on co-occurrence matrix and bit plane clipping", SPIE and IS&T. Journal of Electronic Imaging, vol. 19(1), pp. 1-9, March 2010.
[12] Haralick, R.M. "Textural features for image classification" IEEE Trans. Systems Man Cybernetics. SMC-3 (1973).
[13] T. Fawcett, "ROC graphs: Notes and practical considerations for researchers," HP Laboratories, Tech. Rep., March 2004.