# A Novel Steganalysis Method Based on Histogram Analysis

**Article** *in* Lecture Notes in Electrical Engineering · November 2015

DOI: 10.1007/978-3-319-07674-4_73

CITATIONS
6

READS
2,501

**3 authors:**

Bismita Choudhury
WVU Institute of Technology
**6** PUBLICATIONS **81** CITATIONS
SEE PROFILE

Rig Das
Technical University of Denmark
**22** PUBLICATIONS **798** CITATIONS
SEE PROFILE

Arup Baruah
Assam Don Bosco University
**19** PUBLICATIONS **168** CITATIONS
SEE PROFILE

# Chapter 73
# A Novel Steganalysis Method Based on Histogram Analysis

**Bismita Choudhury, Rig Das and Arup Baruah**

**Abstract** Steganalysis is the art of detecting hidden messages embedded inside Steganographic Images. Steganalysis involves detection of steganography, estimation of message length and its extraction. Recently Steganalysis receives great deal of attention from the researchers due to the evolution of new, advanced and much secured steganographic methods for communicating secret information. This paper presents a universal steganalysis method for blocking recent steganographic techniques in spatial domain. The novel method analyses histograms of both the cover and suspicious image and based on the histogram difference it gives decision on the suspicious image of being stego or normal image. This method for steganalysis extracts a special pattern from the histogram difference of the cover and . By finding that specific pattern from the histogram difference of the suspicious and cover image it detects the presence of hidden message. The proposed steganalysis method has been experimented on a set of stego images where different steganographic techniques are used and it successfully detects all those stego images.

**Keywords** Steganalysis · Steganography · Histogram · PSNR

B. Choudhury (✉) · A. Baruah
Department of Computer Science and Engineering and Information Technology,
Don Bosco College of Engineering and Technology, Guwahati 781017, Assam, India
e-mail: bismi.choudhury@gmail.com

A. Baruah
e-mail: arup.baruah@gmail.com

R. Das
Department of Computer Science and Engineering, National Institute of Technology,
Rourkela 769008, Orissa, India
e-mail: rig.das@gmail.com



H.A. Sulaiman et al. (eds.), *Advanced Computer and Communication Engineering Technology*, Lecture Notes in Electrical Engineering 315,
DOI 10.1007/978-3-319-07674-4_73

## 73.1 Introduction

The battle between Steganography and Steganalysis never ends. For hiding secret message or information, Steganography provides a very secure way by embedding them in unsuspicious cover media such as image, text or video [1]. As a counter action Steganalysis is emerging out as a process of detection of steganography. Steganalysis refers to the science of discrimination between stego-object and cover-object. Steganalysis detects the presence of hidden information without having any knowledge of secret key or algorithm used for embedding the secret message into the cover image [2].

In the general process of steganalysis, steganalyzer simply blocks the stego image and sometimes try to extract the hidden message. Figure 73.1 shows the block diagram of the generic steganalysis process. Generally, Steganalysis techniques are classified into two broad categories: specific and universal blind steganalysis. The targeted steganalysis process is designed for some specific steganographic methods where all features of that particular steganographic method are well known. On the other hand, universal blind steganalysis process uses combination of features to detect arbitrary steganographic methods [3, 4].

Steganalysis can be achieved by applying various image processing techniques like image filtering, rotating, cropping etc. Also it can be achieved by coding a program that examines the stego-image structure and measures its statistical properties, e.g., first order statistics (histograms) or second order statistics (correlations between pixels, distance, direction) [4].

This paper, presents a novel steganalysis method which uses histogram difference for detection of steganography in spatial domain. Here a special pattern in the histogram difference of suspicious image and cover image is utilized for the detection purpose.

This paper is organized as follows. Section 73.2 reviews some previous work done in steganalysis. The proposed novel steganalysis method is explained in Sect. 73.3. Simulation and results are shown in Sects. 73.4 and 73.5 concludes.

## 73.2 Related Work

Many research works have been carried out on steganalysis till now. Based on the domain of message embedding (Spatial or Frequency domain) different methods are employed to detect presence of steganography. Some of them are as follows.

### *73.2.1 RS Steganalysis*

Fridrich et al. described a reliable and accurate method for detecting Least Significant Bit (LSB) based steganography [5]. For performing RS Steganalysis they

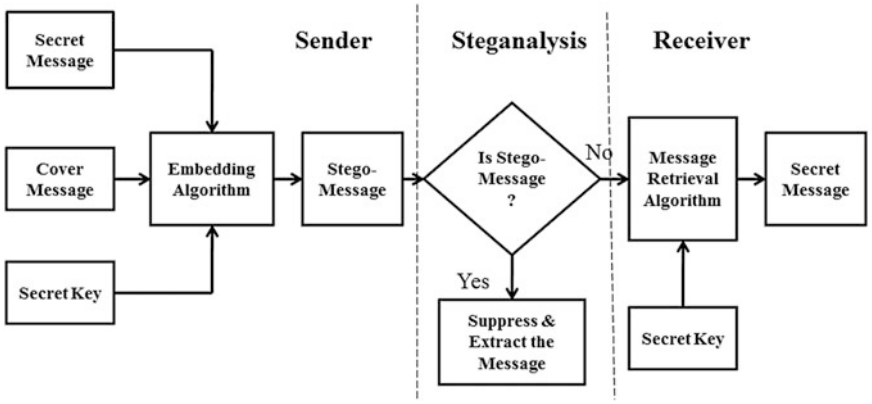


**Fig. 73.1** Block diagram of Steganalysis

divided the image pixels into three groups—Regular, Singular and Unchanged group. In normal image number of regular groups is greater than that of singular group. But after embedding any data in the image, Regular and Singular group of pixels have a tendency of becoming equal. Based on this characteristic they proposed RS steganalysis technique for attacking steganography. Here detection is more accurate for messages that are randomly scattered in the stego-image than for messages concentrated in a localized area of the image.

### *73.2.2 Breaking F5 Algorithm*

Fridrich et al. presented a steganalysis method to reliably detect messages (and estimate their size) hidden in JPEG images using the steganographic algorithm F5 [6]. The estimation of the cover-image histogram from the stego-image is the key point. This is done by decompressing the stego-image, cropping it by four pixels in both directions to remove the quantization in the frequency domain, and recompressing it using the same quality factor as the stego-image. The number of relative changes introduced by F5 is determined using the least square fit by comparing the estimated histograms of selected DCT coefficients with those of the stego-image.

### *73.2.3 Histogram Estimation Scheme for Defeating Pixel Value Differencing Steganography Using Modulus Function*

In this paper Jeong-Chun Joo Kyung-Su Kim and Heung-Kyu Lee presented a specific steganalysis method to defeat the modulus Pixel Value Differencing

(PVD) steganography [7]. By analyzing the embedding process they provided three blind Support Machines (SMs) for the steganalysis and each are used for checking three different features. SM1: the fluctuations around the border of the sub range, SM2: the asymmetry of the stego PVD histogram, and SM3: the abnormal increase of the histogram value. The Support Vector Machine (SVM) classifier is applied for the classification of the cover and stego images. Here Original histogram is estimated from the suspicious image using two novel histogram estimation schemes (HES): a curve-fitting method and a histogram reverse-tracing method those work without the cover image.

### *73.2.4 Steganalysis by Subtractive Pixel Adjacency Matrix*

Tomas Pevny and Patrick Bas and Jessica Fridrich presented a method for detection of steganographic method LSB matching [8]. By modeling the differences between adjacent pixels in natural images, the method identifies some deviations those occur due to steganographic embedding. For steganalysis a filter is used for suppressing the image content and exposing the stego noise. Dependences between neighboring pixels of the filtered image are modeled as a higher-order Markov chain. The sample transition probability matrix is then used as a vector feature for a feature-based steganalyzer implemented using machine learning algorithms.

## 73.3 A Novel Method for Steganalysis Using Histogram Analysis

In this paper we proposed a novel steganalysis technique for detection of steganography in spatial domain based on the histogram analysis of the cover and the suspicious image. The schematic diagram of the whole process is given in Fig. 73.2.

The main goal in here is to develop a steganalysis method which is able to block most of the recently developed steganographic algorithms with a good accuracy. The novel algorithm first finds the histograms of both the cover and suspicious image. Then it uses difference values of both the histograms to detect the stego-image.

### *73.3.1 Histogram Difference*

Image histogram proves to be one of a good feature for analyzing the difference between cover image and stego image. In general, histograms of cover image and stego image have some significant differences that help in discriminating between

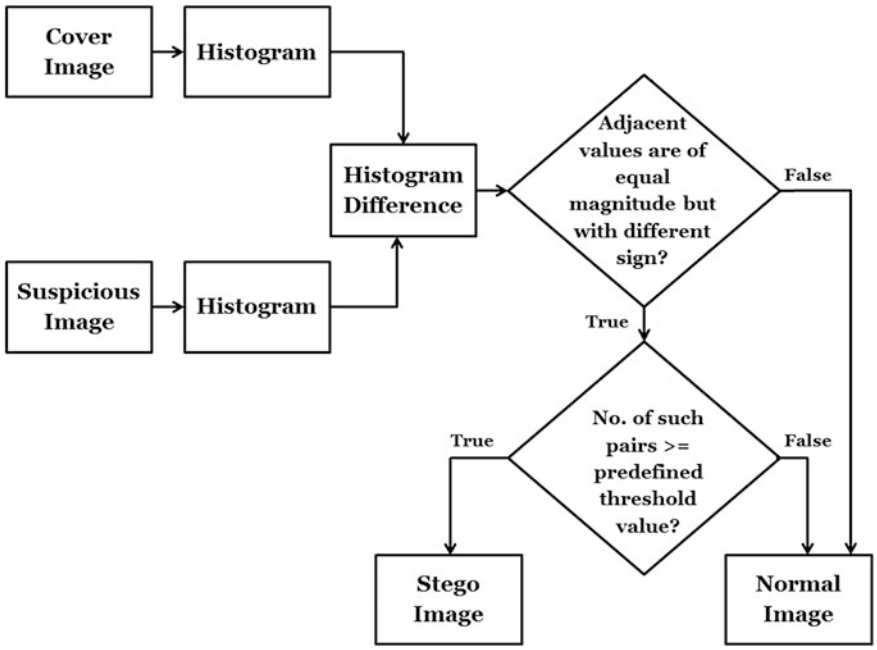


**Fig. 73.2** Block diagram of proposed steganalysis method

cover and stego image. In steganography, while embedding secret data in a cover image by modifying the Least Significant Bits (LSBs) of the cover image, some of the pixel values of the cover image get changed and thereby the histogram of the stego image acquires some variations from that of the cover image. If we find the histogram difference of both the cover and stego image we can observe that some of the difference values possess same magnitude to their adjacent values but of different signs (For e.g. 2, −2; −35, 35; … etc.). But this kind of pattern is not found in the histogram difference between cover and noisy image or any processed image.

The Table 73.1 shows the histogram difference values of the cover image with stego image (LSB embedding) and noisy image introduced with Gaussian noise tested on the Lenna image. From the table we can see that the most of the adjacent difference values are having same magnitude but with different sign only in case of stego image (For e.g. -2, 2; -48, 48; -132, 132), but not in case of noisy image. In this way the steganalysis method tries to find out such pairs in the histogram difference of the cover and the suspicious image and based on this characteristic stego images are detected.

**Table 73.1** Histogram difference of cover image with stego image and noisy image

| Histogram difference of cover and stego image | Histogram difference of cover and noisy (Gaussian noise) image |
|---|---|
| −2 | −37,079 |
| 2 | −2,101 |
| −9 | −2,180 |
| 9 | −2,204 |
| −48 | −2,179 |
| 48 | −2,048 |
| −58 | −1,747 |
| 58 | −1,662 |
| −152 | −1,454 |
| 152 | −1,088 |
| −132 | −711 |
| 132 | −383 |
| −266 | 120 |
| 266 | 601 |

### *73.3.2 Proposed Novel Algorithm for Steganalysis*

**Algorithm**

Input: M × N Suspicious Image and M × N Cover Image.
Output: Decision whether the Suspicious Image is a Stego Image or not.

Step-1: Read both the Cover and Suspicious Image and store their intensity values of different pixels in two different arrays.
Step-2: Find histograms of both the Cover and Suspicious Image.
Step-3: Plot both the histograms in a single plot and find the difference.
Step-4: In the different values, if there are adjacent values those are same in magnitude but different in sign then increment a counter.
Step-5: Repeat Step 4 until all the difference values are checked and the counter incremented accordingly.
Step-6: Set a threshold value of the counter and if the counter value goes beyond the threshold value then detect the Suspicious Image as the Stego Image else as the Normal Image.
Step-7: End.

## 73.4 Simulation and Results

Some experiments are carried out to check the capability and efficiency of the novel steganalysis process. This method is capable of detecting stego image where most of the newly developed steganographic algorithms are used. The proposed

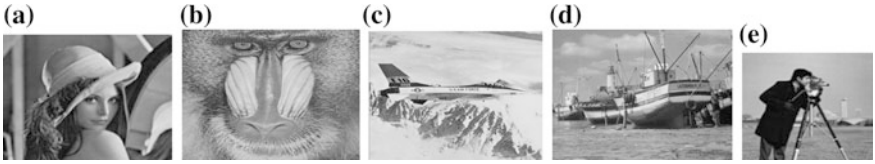


**Fig. 73.3** **a–d** Four cover images for training, **e** Secret image/message. **a** Lenna, **b** Baboon, **c** Airplane, **d** Boat, **e** Cameraman

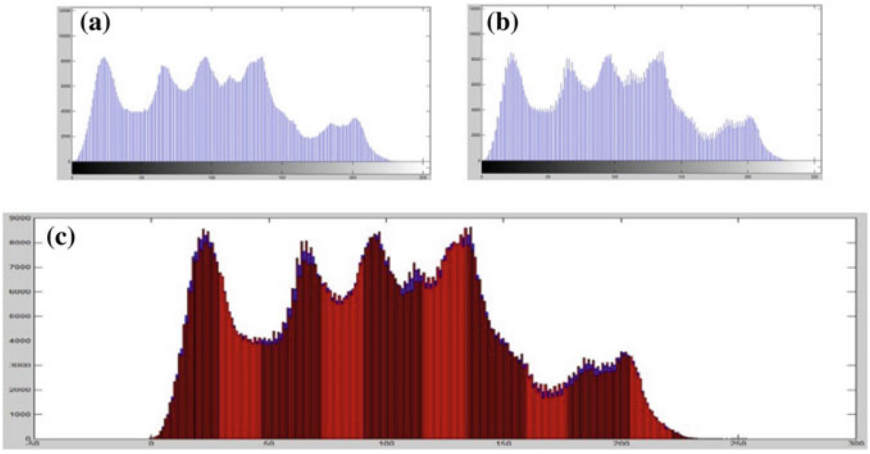


**Fig. 73.4** **a** Histogram of cover image of Lenna, **b** Histogram of stego image using LSB replacement, **c** Histogram difference of cover and stego image

steganalysis algorithm is tested on six steganographic algorithms in spatial domain, viz. Least Significant Bit (LSB) replacement, LSB matching, Steganography based on Huffman Encoding, Wavelet Obtained Weight (WOW), Universal Wavelet Relative Distortion for spatial domain (S_UNIWARD) and HUGO.

For the testing purpose, all the simulation has been done in MATLAB 2012 on Windows 7 platform. A set of 8-bit grayscale images of size 1024 $\times$ 1024 are used as cover-image and image of size 256 $\times$ 256 are used as the secret image to form the stego-image. Figure 73.3a–d shows the four original cover images (Here test results are shown only for Lenna Image) and Fig. 73.3e shows the secret image used to embed using LSB replacement [8], LSB matching [8] and Steganography based on Huffman Encoding [9]. For the steganographic algorithms S_UNIWARD [10], WOW [10] and HUGO [10] randomly generated message bits are used to create stego-image. The histogram of the cover image is used to compare with the histogram of the stego image created for testing the proposed steganalysis method. The novel steganalysis algorithm successfully detects the stego-image by analyzing the histogram difference of both suspicious and cover image.

Figure 73.4a shows the histogram of Lenna image, Fig. 73.4b shows histogram of Lenna image after using LSB replacement steganography in which LSBs of

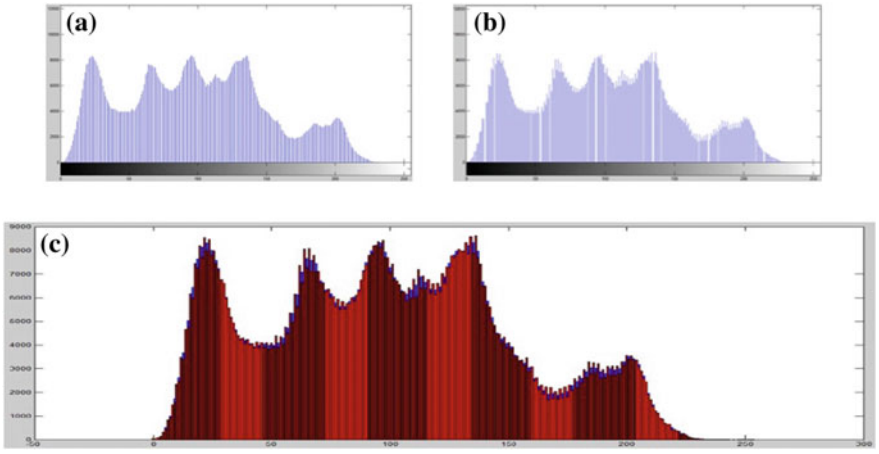


**Fig. 73.5** **a** Histogram of cover image of Lenna, **b** Histogram of stego image using LSB matching, **c** Histogram difference of cover and stego image

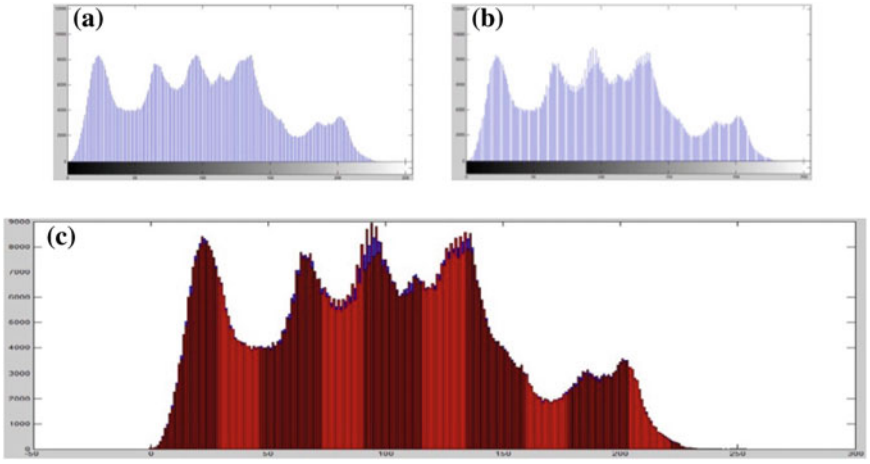


**Fig. 73.6** **a** Histogram of cover image of Lenna, **b** Histogram of stego image created by steganography based on Huffman encoding, **c** Histogram difference of cover and stego image

individual cover elements are replaced with message bits [8], Fig. 73.4c shows histogram difference of the cover and the stego image.

Figure 73.5a shows the histogram of Lenna image, Fig. 73.5b the histogram of Lenna image after using LSB matching steganography which randomly increases or decreases pixel values by one to match the LSBs with the communicated message bits [8], Fig. 73.5c shows histogram difference of cover and stego image. The recent Steganographic method based on Huffman encoding proposed by Das and Tuithung [9] is also a very much secured method and very few specific

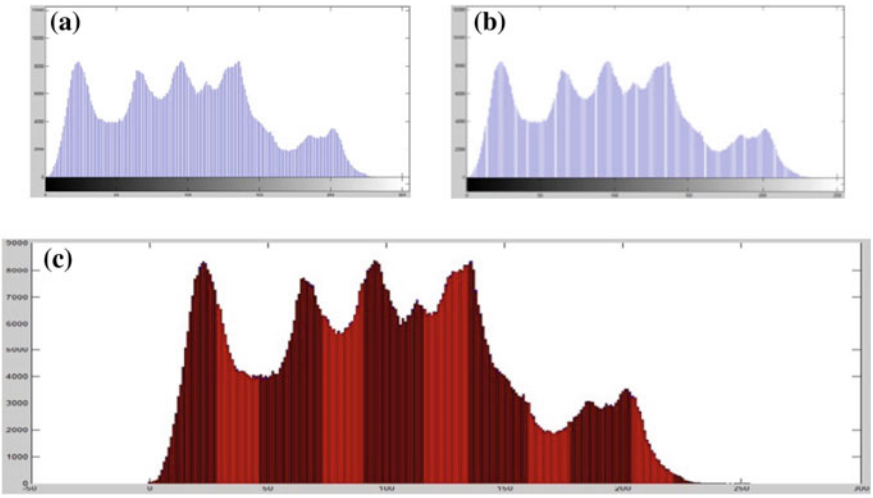


**Fig. 73.7** **a** Histogram of cover image of Lenna, **b** Histogram of stego image created using S_UNIWARD method, **c** Histogram difference of cover and stego image

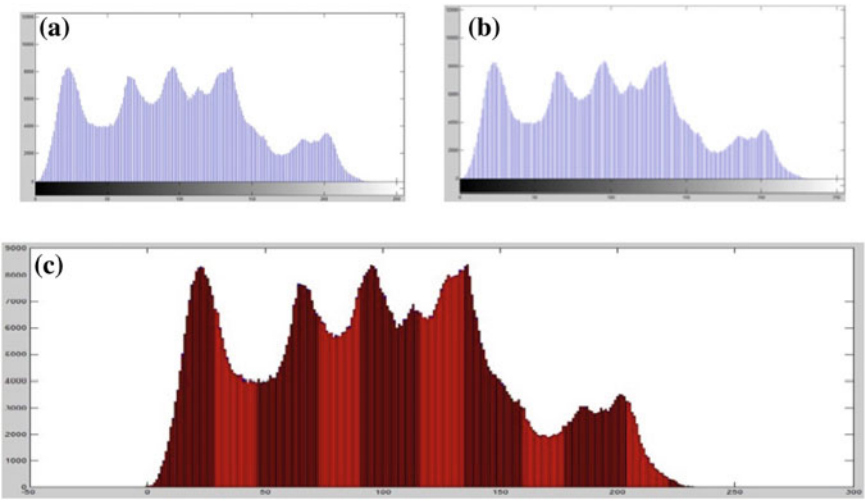


**Fig. 73.8** **a** Histogram of cover image of Lenna, **b** Histogram of stego image using steganographic method WOW, **c** Histogram difference of cover and stego image

patterns can be observed in the histogram difference. However, our proposed steganalysis algorithm is able to block it (Fig. 73.6a–c).

Three very recent and secure steganographic algorithms S_UNIWARD [11] (Fig. 73.7a–c), WOW [12] (Fig. 73.8a–c) and HUGO [13] (Fig. 73.9a–c), proposed by Fridrich et al., make a few modifications in the cover image to embed randomly generated message bits. The novel steganalysis method successfully detects those stego images even though they possess few artifacts.

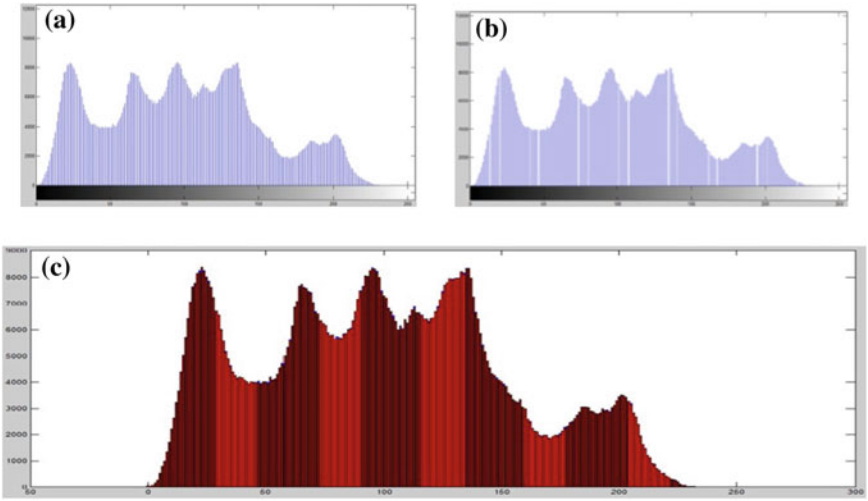


**Fig. 73.9** **a** Histogram of cover image of Lenna, **b** Histogram of stego image using steganographic method HUGO, **c** Histogram difference of cover and stego image

**Table 73.2** PSNR between the cover and the stego image

| Steganographic algorithms | PSNR value between the cover and the stego image (dB) |
|---|---|
| LSB embedding | +56.88 |
| LSB matching | +56.88 |
| Steganography based on Huffman encoding | +57.43 |
| WOW | +62.69 |
| S_UNIWARD | +62.21 |
| HUGO | +61.92 |

From the Peak Signal to Noise Ratio (PSNR) values, shown in Table 73.2, it can be seen that the most of the used steganographic methods have done less modification to the cover image which is very difficult to get noticed. However, the proposed steganalysis method successfully blocks the stego images where these steganographic techniques are applied.

## 73.5 Conclusion

In this paper, we have proposed a universal steganalysis method that checks the histogram difference of the suspicious image with that of the cover image to get adjacent difference values having same magnitude but of different sign. This method

has a great capability of detecting stego images even though very small changes are done in the cover image. Experimental results show that it can block from generic LSB modification techniques to much secured recent steganographic methods. The PSNR values, shown in the Table 73.2, for tested stego images using different steganographic methods depicts that the tested steganographic methods are efficient methods.

Most of the steganalysis algorithms are targeted methods to attack specific steganographic techniques. So in the small group of the universal blind steganalysis this novel algorithm provides a new addition. In future we will work on the steganalysis of the steganography in frequency domain. Then we would like to develop a universal steganalysis method to detect stego images irrespective of the data embedding domain.

## References

1. Johnson, F.N., Jajodia, S.: Exploring steganography: seeing the unseen. IEEE Computer Society Press. **31**(2), 26–34 (1998)
2. Fridrich, J., Goljan, M.: Practical steganalysis of digital images—state of the art. In: Proceedings of Electronic Imaging, SPIE, vol. 4675, pp. 1–13 (2002)
3. Lou, D.C., Hu, C.H., Chiu, C.C.: Steganalysis of histogram modification reversible data hiding scheme by histogram feature Coding. Int. J. Innov. Comput. Inf. Control **7**, 11 (2011)
4. Cheddad, A., Condell, J., Curran, K., Kevitt, M.P.: Digital image steganography: survey and analysis of current methods. Elsevier Signal Process. **90**, 727–752 (2010)
5. Fridrich, J., Goljan, M., Du, R.: Reliable detection of LSB steganography in grayscale and color images. In: Proceedings of ACM, Special Session on Multimedia Security and Watermarking, Ottawa, Canada, October 5 (2001)
6. Fridrich, J., Goljan, M., Hogea, D.: Steganalysis of jpeg images: breaking the F5 algorithm. In: Proceedings of the 5th Information Hiding Workshop, Springer, vol. 2578, pp. 310–323 (2002)
7. Joo, C.J., Kim, S.K., Lee, K.H.: Histogram estimation-scheme-based steganalysis defeating the steganography using pixel-value differencing and modulus function. Opt. Eng. **49**, 077001 (2010)
8. Pevny, T., Ba, P., Fridrich, J.: Steganalysis by subtractive pixel adjacency matrix. In: ACM Multimedia and Security Workshop, Princeton, NJ, September 7–8, pp. 75–84 (2009)
9. Das, R., Tuithung, T.: A novel steganography method for image based on huffman encoding. In: 3rd IEEE National Conference on Emerging Trends and Applications in Computer Science (NCETACS—2012), pp. 14–18 (2012)
10. Steganography codes for windows. http://dde.binghamton.edu/download/stego_algorithms/
11. Holub, V., Fridrich, J.: Digital image steganography using universal distortion. In: ACM Workshop on Information Hiding and Multimedia Security, June (2013)
12. Holub, V., Fridrich, J.: Designing steganographic distortion using directional filters. In: IEEE Workshop on Information Forensic and Security (WIFS), Tenerife, Spain, December (2012)
13. Filler, T., Fridrich, J.: Gibbs construction in steganography. IEEE Trans. Inf. Forensics and Security. **5**(4), 705–720 (2010)