http://ansinet.com/itj

ITJ

ISSN 1812-5638

INFORMATION TECHNOLOGY JOURNAL

ANSInet
Asian Network for Scientific Information
308 Lasani Town, Sargodha Road, Faisalabad - Pakistan

Information Technology Journal 10 (8): 1601-1607, 2011
ISSN 1812-5638 / DOI: 10.3923/itj.2011.1601.1607

Detection of LSB Matching Steganography using Neighborhood Node Degree Characteristics

[1]Bin Xia, [1,2]Xingming Sun, [1]Lingyun Xiang, [1]Haijun Luo and [3]Hengfu Yang
[1]College of Information Science and Engineering, Hunan University, Changsha, 410082, China
[2]College of Computer and Software, Nanjing University of Information Science and Technology, Nanjing, 210044, China
[3]Department of Information Sciences and Engineering, Hunan First Normal University, China

Abstract: This study presented a method to detect Least Significant Bit (LSB) matching steganography in gray images based on the neighborhood node degree characteristic. Natural images have a strong correlation between adjacent pixels and it's disturbed by LSB matching. Accordingly the effects of LSB matching steganography on neighborhood node degree were examined at first. Then features were extracted from neighborhood node degree histogram. A new calibration algorithm based on neighborhood node degree was proposed to get more effective features. Support Vector Machine (SVM) was used as classifier. Experimental results demonstrated that the proposed method was efficient to detect the LSB matching steganography and had superior results compared with other recently proposed algorithms on compressed images and low embedding rate uncompressed images.

Key words: Information hiding, steganalysis, LSB Matching, neighborhood node degree histogram, neighborhood calibration, calibration histogram

INTRODUCTION

Steganography is the art of invisible communication. Its purpose is to hide the very presence of communication by embedding messages into cover objects. Digital images contain much redundant information which helps to conceal the presence of secret messages. Thus, Digital images are well suited for serving as covers object and have been the most widely used media to transmit secret message (Berg *et al*., 2003; Zaidan *et al*., 2010). To accommodate a secret message in a digital image, the original cover image is slightly modified by the embedding algorithm. As a result the stego image is obtained.

LSB steganography is the most popular, frequently used scheme for its high payload, good visual imperceptibility and extreme ease of implementation. There are two kinds of LSB steganography: LSB replacement and LSB matching (Hmood *et al*., 2010a, b). LSB replacement embeds a secret message into the cover image by replacing the LSB with message bit. LSB matching does not simply replace the LSB of the cover image, if the bit must change, ±1 is added to the pixel value. Whether to use '+' or '-' is chosen randomly and has no effect on the hidden message. The extraction of the secret message for both LSB replacement and LSB Matching work the same way: the LSB for each selected pixel is the hidden bit (Sharp, 2001).

The research of steganalysis which is a counter technology of steganography aimed at detecting the presence of secret message in cover objects. Recently, a lot of image steganalysis techniques have been developed by Qin *et al*. (2010). Consider the proposed algorithm, LSB replacement can be uncovered relatively easily (Ker, 2004; Fridrich and Goljan, 2002; Dumitrescu *et al*., 2003) but fewer and weaker detectors have been proposed for LSB matching. Harmsen and Pearlman (2003) proposed a steganalysis method using the Histogram Characteristic Function (HCF) for distinguishing between cover and stego images. Assuming that the histogram of stego image is a convolution process for the noise probability mass function and the original histogram, they found that the embedding method is a low-pass filtering of histogram which is quantified by a decrease in the HCF Center of Mass (COM). While good results were reported in color images but performed poorly in grayscale images, to improve the method in grayscale images (Ker, 2005) extended Harmsen's method by two novel ways: calibrating the output using a down sampled image and computing the adjacency histogram instead of the usual

Corresponding Author: Xingming Sun, College of Information Science and Engineering, Hunan University, No. 252, Lushan South Road, Yuelu District, Changsha, 410082, China
Tel: 86-731-88821341 Fax: 86-731-88821780

histogram. Significant improvements in detection of grayscale images were achieved. Also based on the observation that LSB matching steganography is equivalent to low-pass filtering the intensity histogram, Zhang *et al.* (2007) and Cancelli *et al.* (2008) proposed a steganalysis algorithm based on the Amplitude of Local Extreme. Yu and Babaguchi (2008) used the fusion of run length histogram and HCF to detect the LSB matching steganography. Qin *et al.* (2009) used the difference statistics of neighboring pixels to improve the detect result. Fridrich *et al.* (2005) and Holotyak *et al.* (2005) presented some new methods for attacking the ±k steganography which was efficient in detecting the LSB matching using decompressed JPEG (Joint Photographic Experts Group) image. There are also exist blind techniques, Goljan *et al.* (2006) extracted features from the wavelet domain to train classifiers. Liu *et al.* (2008) exploited the correlation of least and second significant bit plane to attack LSB matching and revealed that the accuracy of the classifier degenerates as the image complexity increases. Pevny *et al.* (2010) argued that the dependence between neighboring pixels were disturbed by message embedding and utilized Markov model to extract sensitive features.

In this study, a new method using Neighborhood Node Degree Characteristic against LSB matching steganography is proposed. Firstly, by analyzing the effects of LSB matching on neighorhood node degree, neighborhood Node Degree Histogram Characteristic Function (NDHCF) is selected as features. Secondly, a new calibration algorithm based on neighborhood node degree is proposed to get other features. Finally features are used to train Support Vector Machine (SVM). Experimental results demonstrate that the proposed method is efficient to detect the LSB matching steganography.

NEIGHBORHOOD NODE DEGREE ANALYSIS

Consider the cover and stego images are grayscale with the intensity in the range 0…255. The previously mentioned LSB matching algorithm can be formally described as Table 1, the distortion due to LSB matching embedding is modeled as an additive i.i.d. noise signal η with the following Probability Density Function (Fridrich *et al.*, 2005) with ρ∈[0, 1].

$$\begin{aligned} p(\eta=0) &= 1-\rho/2 \\ p(\eta=1) &= p(\eta=-1)=\rho/4 \end{aligned} \qquad (1)$$

Table 1: LSB matching embedding operation

	To embed bit b, modify x to	
Pixel value x	b = 0	b = 1
2i, 0<2i<255	2i	2i+1 or 2i-1
2i+1, 0<2i+1<255	2i or 2i+2	2i+1
0	0	1
255	254	255

Neighborhood node degree: Let P (i, j) for the intensity of the image at location (i, j). The neighborhood node degree of 9 = (i, j) is defined as:

$$d(i,j)=|\{(i+u, j+v)\,|\,P(i+u, j+v)=P(i,j)\}| \qquad (2)$$

where, -k≤u≤k, -k≤v≤k and u, v can not both be zero. k is the neighborhood size parameter, k = 1, 2 denote 3×3 neighborhood and 5×5 neighborhood, respectively. Node degree d (i, j) indicates the number of neighboring pixels which intensity equals the center pixel P (i, j). The neighborhood node degree can be considered as an indicator to the pixel dependence in the corresponding neighborhood. To be more specifically, the larger the degree is, the greater dependence that is held by the neighborhood.

Effects of LSB matching on neighborhood node degree: Consider the effects of LSB matching steganography with embedding ratio ρ on neighborhood node degree. Basically the neighborhood node degree is changed after LSB matching steganography if the pixel value or the neighboring pixels are modified. Simply we analyze the changes in a neighborhood through the alter of the center pixel and the neighboring pixel to illustrate the effects for the neighborhood node degree. Let P_c is the intensity of the center pixel in the neighborhood and symbol np denote the neighboring pixels of the center pixel in the neighborhood, P_{np} is the neighboring pixel's intensity, due to LSB matching steganography the center pixel's value changed to {P_c-1, P_c, P_c+1}. So only the np which the absolute difference between the center pixel is 0, 1 or 2 may lead the neighborhood node degree changed. Let:

$$NP_0=\{np\,\|P_c-P_{np}|=0\}$$

be the np that the intensity is equal to the center pixel,

$$NP_1=\{np\,\|P_c-P_{np}|=1\}$$

for the neighboring pixels where the absolute difference between the center pixel is 1 and:

$$NP_2=\{np\,\|P_c-P_{np}|=2\}$$

for the neighboring pixels where the absolute difference between the center pixel is 2. Figure 1 is an example of 3×3 neighborhood, p_c is the center pixel, p_1, p_2, p_3, p_1, p_4, p_5, p_6,

$P_1 = 128$	$P_2 = 122$	$P_3 = 123$
$P_4 = 126$	$P_c = 125$	$P_5 = 125$
$P_6 = 127$	$P_7 = 124$	$P_8 = 125$

Fig. 1: An example of 3×3 neighborhood

Table 2: The 3×3 neighborhood node degree statistic result for Fig. 2 and the corresponding stego image

Node degree	d = 0	d = 1	d = 2	d = 3	d = 5	d = 6	d = 7	d = 8
Cover image	37656	17460	6755	2030	84	13	1	0
Stego image	38107	17687	6488	1786	59	4	0	0

p_7, p_8 are the neighboring pixels, since the intensity of p_5, p_8 is 125 equal to p_c, so p_5, $p_8 \in NP_0$ and p_4, $p_7 \in NP_2$. The neighborhood node degree of p_c is 2.

When p_c is not modified, the original neighboring pixels in NP_0 may be changed resulting in node degree reduction in the probability $\rho/2$. And the np in NP_1 due to a modification change to the same with node degree increase probability $\rho/4$.

When p_c is modified, the original np in NP_0 do not change as the node degree reduction with the probability $1-\rho/2$ and due to change into different result with a reduction probability $\rho/4$. The np in NP_1 may not change with node degree increase probability

$$\frac{(1-\rho/2)}{2}$$

and the np in NP_2 may changes into the same with probability $\rho/8$.

In a neighborhood, let the probability that the neighboring pixel in NP_0 is r_0, neighboring pixel belong to NP_1 in probability r_1 and r_2 is the probability that neighboring pixel in NP_2. d_c denotes the neighborhood node degree of cover image and d_s is the stego image's node degree. Base on the analysis above:

$$\begin{aligned} d_s &= d_c + 8\left\{\left(1-\frac{\rho}{2}\right)\left(-\frac{\rho}{2}r_0+\frac{\rho}{4}r_1\right)+\frac{\rho}{2}\left[-\left(1-\frac{\rho}{2}\right)r_0-\frac{\rho}{4}r_0+\frac{(1-\frac{\rho}{2})}{2}r_1+\frac{\rho}{8}r_2\right]\right\} \\ &= d_c + 8\left\{\left(1-\frac{\rho}{2}\right)\frac{\rho}{4}(r_1-2r_0)+\frac{\rho}{2}\left[\frac{(1-\frac{\rho}{2})}{2}(r_1-2r_0)+\frac{\rho}{8}(r_2-2r_0)\right]\right\} \end{aligned} \tag{3}$$

Since the correlation of image adjacent pixels have close intensity and the number of pixels in NP_0, NP_1, NP_2, is close, r_0,r_1,r_2 are little difference. The observation is that, in 8,515 uncompressed images the 3×3 neighborhood statistic result is $r_0 = 0.10$, $r_1 = 0.14$ and $r_2 = 0.10$, in 10,408 compressed images the 3×3 neighborhood statistic result is $r_0 = 0.20$,$r_1 = 0.17$ and $r_2 = 0.15$. Base on the facts that $r_1<2r_0$, $r_2<2r_0$ and:

$$\left(1-\frac{\rho}{2}\right)\frac{\rho}{4}(r_1-2r_0)+\frac{\rho}{2}\left[\frac{(1-\frac{\rho}{2})}{2}(r_1-2r_0)+\frac{\rho}{8}(r_2-2r_0)\right]<0 \tag{4}$$

Fig. 2: The cover image

so $d_s<d_c$. That the image's neighborhood node degree decrease after LSB matching steganography and it is expected that statistically for cover image the number of pixels with great node degree is larger than the number of pixels of stego image. Figure 2 shows a cover image with size 256×256 and Table 2 is the 3×3 neighborhood node degree statistic result for the cover image and corresponding stego image with embedding rate $\rho = 100\%$.

As it's shown, the number of pixels of cover image when $d>1$ is larger than the number of pixels of stego image.

FEATURES EXTRACTION

Feature extraction is a key step for classification. In this session, the eight effective f features from neighborhood node degree are extracted.

Center of mass (COM) of NDHCF: First define the neighborhood Node Degree Histogram (NDH):

$$h(x)=|\{(i,j)\,|\,d(i,j)=x\}|$$

and use h_c (x) for cover image's NDH, h_s (x) for stego image. The COM of NDHCF:

$$C(h(x)) = \frac{\sum_{x=0}^{n} xh(x)}{\sum_{x=0}^{n} h(x)} \qquad (5)$$

where, n is the maximum of the NDHCF, n = 8 when k = 1, n = 24 when k = 2. Due to the LSB matching embedding process, the neighborhood node degree is decreased, that C (h_s (x))>C (h_s (x)). Figure 3 is the C (h (x)) for 100 randomly selected grayscale cover images and corresponding stego images with embedding ratios ρ = 25, 50, 75 and 100%. That C (h_c (x)) is larger than C (h_s (x)) and the higher embedding rate in steganography, the more the C (h (x)) decreased.

Calibration using neighborhood node degree: Consider the facts that steganography disturb the dependence between neighboring pixels and decrease the neighborhood node degree, so the 3×3 neighborhood can be used to calibrate image, after calibration it's expected to get a strong dependence cover image.

In a 3×3 neighborhood, pixels are divided into two classes: Sensitive pixel and Normal pixel, a Sensitive pixel that $d_{sp}\leq 3$ and other pixels belong to Normal pixel. If a pixel after modification (±1) change from Normal Pixel to Sensitive pixel that it is called Recoverable pixel.

The calibration algorithm is as follows:

- **Step 1:** Given an image calculates all pixels' neighborhood node degree
- **Step 2:** Find all recoverable pixels and record the values
- **Step 3:** Modify the recoverable pixels' value

Compute the COM of NDHCF for calibration images C (h′ (x)) and denote the alteration rate of NDHCF COM as:

$$R = \frac{C'(h(x)) - C(h(x))}{C(h(x))} \qquad (6)$$

Figure 4 shows the alteration rate of NDHCF COM for 100 randomly selected grayscale cover images and corresponding stego images with embedding ratios ρ = 25, 50, 75, 100%. Due to LSB matching steganography the stego image's alteration rate is greater than the cover image's thus R_s>R_c. Compared with NDHCF COM (Fig. 3) the alteration rate between the cover image and the stego images is more evident, also higher embedding rate has greater alteration rate. Now there are three features C (h (x)), C (h' (x)) and R calculated through Eq. 5 and 6. Additionally for a given image, compute these features twice using 3×3 and 5×5 neighborhood, respectively (Fig. 4).

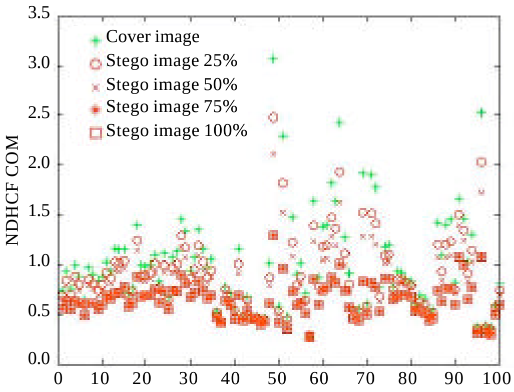

Fig. 3: Values of C(h (x)) before and after embedding for 100 randomly selected images

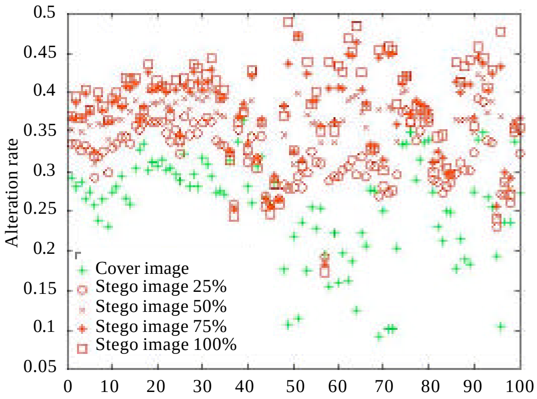

Fig. 4: Values of R before and after embedding for 100 randomly selected images

To value the calibration process the calibration Change Ratio (CR) is useful:

$$CR = \frac{\text{Recoveralbe pixels}}{\text{Total pixels}} \qquad (7)$$

According to the calibration algorithm, the CR of an image increase after LSB matching, i.e., CR_c<CR_s.

Base on the fact that LSB matching also smoother the histogram, the sum of Difference of the Calibration Histogram (DCH) is calculated to characterize this effect as follows:

$$DCH = \frac{\sum_{i\in Rp} |H(i) - H(i+1)| + |H(i) - H(i-1)|}{\sum_{j=0..255} H(j)} \qquad (8)$$

where, R_P is the pixel value changed in the calibration. H (n) is the calibration image 's histogram thus define as $H(n) = |p(i, j)|p(i, j) = n|$. After LSB matching, the DCH is likely to decrease, namely $DCH_c > DCH_s$.

According to present observation CR and DCH are two effective features, can be added to the feature vector. Totally an 8-D feature vector is used for classify.

EXPERIMENTS AND PERFORMANCE ANALYSIS

Experimental results are given here to demonstrate the performance of the proposed method on both compressed and uncompressed image sets. In addition, other methods were implemented to facilitate performance comparisons.

Image sets: The accuracy of steganalysis varies significantly across different image sources, so two image were used sets to test our algorithm and compare with other methods. The experiments were conducted separately on two sets with uncompressed and compressed images, respectively.

- **Set#1, NRCS:** 3,162 uncompressed images download from NRCS Photo Gallery at http://photogallery.nrcs.usda.gov, all the images in NRCS were downloaded as very high resolution uncompressed digital TIFF files with size 2100×1500 or 1500×2100. For testing, the images were resampled to 640×418 and converted to grayscale
- **Set#2, FreeFOTO:** 10, 408 compressed JPEG images download from http://www.freefoto.com at quality factor 75 with size 600×400 or 400×600, the images were converted to grayscale before use

Classifier: Support Vector Machine (SVM) was choosed as classifier in experiments for its efficient classification performance for large scale learning. Before classification features were normalized at first. For a feature f, find its maximum value f_{max} and minimum value f_{min} from all of the training images. For any training or test image the feature f is scaled as:

$$F = \frac{f - f_{min}}{f_{max} - f_{min}} \qquad (9)$$

where, F is the normalized value, for all of the training image $F\in[0,1]$, for most test images, it is expected that F will also between 0 and 1. This scaling step prevents features with large numerical ranges from dominating those with small numerical ranges, avoids numerical ill conditioning and dramatically improves classification accuracy (Hsu *et al*., 2003), non-linear kernel: rbf was adopt in classification.

Performance evaluation: Receiver Operation Characteristic (ROC) curves was choosed to show the detection probability in terms of the false positive probability. And to evaluate the overall goodness of the ROC curve, the area under the ROC curve (AUC) was used, (Shapiro, 1999; Wang and Moulin, 2007).

Detection performance: With embedding ratios 25, 50, 75 and 100%, secret message was embedded into all images randomly using LSB matching steganography to obtain the stego images. Each image set above was divided into parts: training and testing set. The 40% original images and their stego images was selected randomly for training, the rest for testing. For example Set#1, the training set contains 1,264 cover images and 1,264 corresponding stego images for each message lengths total 5056 stego images. The rest 1,898 cover images and 7,592 (1898×4) stego images are for test. The proposed method was compared with Ker (2005), Liu *et al*. (2008) and Cancelli *et al*. (2008) method. Some of the ROC curves of detection performances are presented in Fig. 5. The AUC for all methods is listed in Table 3.

As it's shown in Table 3, The proposed method give high detection accuracy on compressed image with average AUC 0.9968 but on uncompressed image our method is a little weaker compare to Cancelli's ALE method average AUC 0.8556 against 0.8620. But on low embedding rate (25%) the detection result 0.7584 is best compare above methods, that the calibration algorithm has special effect on low embedding rate. At last the experimental results also show that our method is reliable for both uncompressed images and compressed images.

Table 3: AUC for all methods AUCs for each method

		AUC			
Image set	Embeding rates (%)	Ker' s	Liu' s	Cancelli' s	The propose method
Set#1	25	0.7084	0.6855	0.7308	0.7584
	50	0.8232	0.8274	0.8330	0.8265
	75	0.8942	0.9035	0.9242	0.9008
	100	0.9183	0.9210	0.9600	0.9366
	Average	0.8360	0.8343	0.8620	0.8556
Set#2	25	0.5673	0.9011	0.8827	0.9939
	50	0.7923	0.9804	0.9584	0.9974
	75	0.9526	0.9943	0.9823	0.9979
	100	0.9688	0.9965	0.9912	0.9981
	Average	0.8203	0.9681	0.9536	0.9968

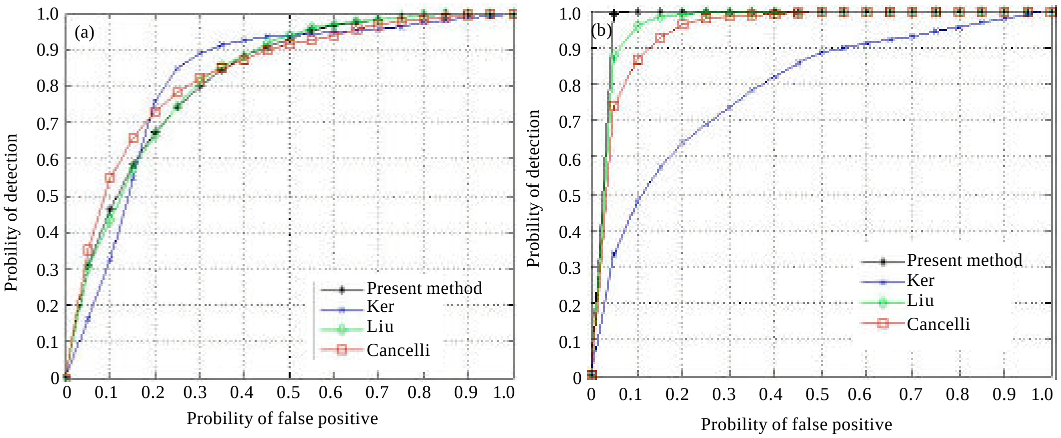

Fig. 5 (a-b): ROC curve samples, the embedding rate is 50% (a) The detection of image Set#1 and (b) The detection of image Set#2

Compare all the mentioned methods on different image set: uncompressed images (set#1) and compressed images (set#2) the best result on set#1 is Cancelli's 0.8620 but on set#2 Liu's (0.9681) and present method (0.9968) are higher than other method, that Cancelli's and Ker's mainly features extract from image's histogram give better result on uncompressed images and Liu's and present method mainly use image's adjacent pixels' correlation show better result on compressed image. It can be found that histogram features are suitable for images with large noise and features use neighboring pixels' correlation are more useful in compressed image. Overall the detection results on compressed image are much better than uncompressed image, in other word, compressed image is not suitable for LSB matching Steganography and Steganalysis should pay more attention on uncompressed image which contain much noise. Additionally compare Ker's with other methods; the trained classifiers outperform the detectors use single feature.

CONCLUSION

A learning-based Steganalysis method using image neighborhood node degree characteristic has been presented to detect LSB matching steganography in gray images. An 8-D feature vector is obtained by neighborhood node degree histogram and image calibration algorithm. Due to the large differences among the cover images, SVM is used for classification. Experimental results show that neighborhood node degree is an effective feature and our method provides more reliable detection results than other proposed methods, especially in lower embedding rate. In addition, features extract on image's histogram or neighboring pixels' dependence has its own advantages, an ideal Steganalysis should increase the dimensionality of feature set and contain both the features mentioned above.

The present method give a high accuracy on compressed image but it still not good enough on the detection of uncompressed image. Our future studies will focus on how to improve the low embedding rate of uncompressed image's detection result.

ACKNOWLEDGMENT

This study was supported in part by National Natural Science Foundation of China (No. 60736016, No. 60973128, No. 60973113, No. 61073191, No. 61070195 and No. 61070196) and in part by National Basic Research Program of China (No. 2009CB326202, 2010CB334706).

REFERENCES

Berg, G., I. Davidson, M.Y. Duan and G. Paul, 2003. Searching for hidden messages: Automatic detection of steganography. Proceedings of the 15th Conference on Innovative Applications of Artificial Intelligence, Aug. 12-15, Acapulco, Mexico, pp: 51-56.

Cancelli, G., G. Doerr, I.J. Cox and M. Barni, 2008. Detection of steganography based on the amplitude of histogram local extrema. Proceedings of 15th IEEE International Conference on Image Processing (ICIP), Oct. 12-15, San Diego, CA, pp: 1288-1291.

Dumitrescu, S., X. Wu and Z. Wang, 2003. Detection of LSB steganography via sample pair analysis. Inform. Hiding, 2578: 355-372.

Fridrich, J. and M. Goljan, 2002. Practical steganalysis of digital images State of the art. Proc. SPIE, 4675: 1-13.

Fridrich, J., D. Soukal and M. Goljan, 2005. Maximum likelihood estimation of length of secret message embedded using ±K steganography in spatial domain. Proc. SPIE, 5681: 595-606.

Goljan, M., J. Fridrich and T. Holotyak, 2006. New blind steganalysis and its implications. Proc. SPIE, 6072: 1-13.

Harmsen, J.J. and W.A. Pearlman, 2003. Steganalysis of additive-noise modelable information hiding. Proc. SPIE, 5020: 131-142.

Hmood, A.K., B.B. Zaidan, A.A. Zaidan and H.A. Jalab, 2010a. An overview on hiding information technique in images. J. Applied Sci., 10: 2094-2100.

Hmood, A.K., H.A. Jalab, Z.M. Kasirun, B.B. Zaidan and A.A. Zaidan, 2010b. On the Capacity and security of steganography approaches: An overview. J. Applied Sci., 10: 1825-1833.

Holotyak, T., J. Fridrich and D. Soukal, 2005. Stochastic approach to secret message length estimation in ±k embedding steganography. Proc. SPIE., 5681: 673-684.

Hsu, C.W., C.C. Chang and C.J. Lin, 2003. A practical guide to support vector classification. Technical report, Department of Computer Science and Information Engineering, National Taiwan University, http://www.csie.ntu.edu.tw/~cjlin/papers/guide/guide.pdf.

Ker, A., 2004. Quantitative evaluation of pairs and RS steganalysis. Proc. SPIE, 5306: 83-97.

Ker, A.D., 2005. Steganalysis of LSB matching in grayscale images. IEEE Signal Process. Lett., 12: 441-444.

Liu, Q., A.H. Sung, B. Ribeiro, M. Wei, Z. Chen and J. Xu, 2008. Image complexity and feature mining for steganalysis of least significant bit matching steganography. Inform. Sci., 178: 21-36.

Pevny, T., P. Bas and J. Fridrich, 2010. Steganalysis by subtractive pixel adjacency matrix. IEEE Trans. Inform. Forensics Security, 5: 215-224.

Qin, J., X. Sun, X. Xiang and Z. Xia, 2009. Steganalysis based on difference statistics for LSB matching steganography. Inform. Technol. J., 8: 1281-1286.

Qin, J., X. Xiang and M.X. Wang, 2010. A review on detection of LSB matching steganography. Inform. Technol. J., 9: 1725-1738.

Shapiro, J.H., 1999. Bounds on the area under the ROC curve. J. Optical Soc. Am., 16: 53-57.

Sharp, T., 2001. An implementation of key-based digital signal steganography. Inform. Hiding, 2137: 13-26.

Wang, Y. and P. Moulin, 2007. Optimized feature extraction for learning-based image steganalysis. IEEE Trans. Inform. Forensics Security, 2: 31-45.

Yu, X.Y. and N. Babaguchi, 2008. Run length based steganalysis for LSB matching steganography. Proceedings of the IEEE International Conference on Multimedia and Expo, June 23-April 26, Hannover, Germany, pp: 353-356.

Zaidan, B.B., A.A. Zaidan, A.K. Al-Frajat and H.A. Jalab, 2010. On the differences between hiding information and cryptography techniques: An overview. J. Applied Sci., 10: 1650-1655.

Zhang, J., I.J. Cox and G. Doerr, 2007. Steganalysis for LSB matching in images with high-frequency noise. Proceedings of the IEEE 9th Workshop on Multimedia Signal Processing, Oct. 1-3, Piscataway, New Jersey, USA., pp: 385-388.