S.Shanmuga Priya, K.Mahesh, Dr.K.Kuppusamy/ International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622 www.ijera.com
Vol. 2, Issue 3, May-Jun 2012, pp.2632-2637

Efficient Steganography Method to Implement Selected Lease Significant Bits in Spatial Domain (SLSB – SD)

S.Shanmuga Priya[1]
Research Scholar
Alagappa University
Karaikudi

K.Mahesh[2]
Associate Professor
Alagappa University
Karaikudi

Dr.K.Kuppusamy[3]
Associate Professor
Alagappa University
Karaikudi

***Abstract*—** In order to improve the capacity of the hidden secret data and to provide an imperceptible stego-image quality, a novel steganographic method based on least-significant-bit (LSB) replacement method is presented. First, a different value from two consecutive pixels by utilising the PVD method the security level is the same as previous. In the LSB matching, the choice of whether to add or subtract one from the cover image pixel is random. The new method uses the choice to set a binary function of two cover pixels to the desired value. The embedding is performed using a pair of pixels as a unit, where the LSB of the first pixel carries one bit of information, and a function of the two pixel values carries another bit of information. we expand the LSB matching revisited image stegano graphy and propose an edge adaptive scheme which can select the embedding regions according to the size of secret message and the difference between two consecutive pixels in the cover image. For lower embedding rates, only sharper edge regions are used while keeping the other smoother regions as they are. When the embedding rate increases, more edge regions can be released adaptively for data hiding by adjusting just a few parameter the proposed method show better performance than traditional LSB matching in terms of distortion and resistance against existing steganalysis.

Keywords: Content-based steganography, least-signifi-cant-bit (LSB)-based steganography, pixel-value differencing (PVD), security, steganalysis.

I.INTRODUCTION

STEGANOGRAPHY is a technique for information hiding. It aims to embed secret data into a digital cover media, such as digital audio, image, video, etc. We can use digital images, videos, sound files, and other computer files that contain perceptually irrelevant or redundant information as covers or carriers to hide secret messages. After embedding a secret message into the cover image, we obtain a so-called stego-image. It's important that the stego-image doesn't contain any detectable artifacts due to message embedding. A third party could use such artifacts as an indication that a secret message is present. Once a third party can reliably identify which images contain secret messages, the stegano-graphic tool becomes useless. Obviously, the less information we embed into the cover image, the smaller the probability of introducing detectable artifacts by the embedding process. Another important factor is the choice of the cover image. The selection is at the discretion of the person who sends the message. Images with a low number of colors, computer art, and images with unique semantic content (such as fonts) should be avoided as cover images. Some stegano-graphic experts recommend grayscale images as the best cover images. They recommend uncom-pressed scans of photographs or images obtained with a digital camera containing a high number of colors and consider them safe for steganography. In previous work, we've shown that images stored previously in the JPEG format are a poor choice for cover images. This is because the quan-tization introduced by JPEG compression can serve as a watermark or unique fingerprint, and you can detect even small modifications of the cover image by inspecting the compatibility of the stego-image with the JPEG format. Pfitzmann and Westfeld introduced a method based on statistical analysis of pairs of values (PoVs) exchanged during message embedding. Pairs of colors that differ in the LSB only, for exam-le, could form these PoVs. This method provides reliable results when we know the message place-ment (such as sequential). However, we can only detect randomly scattered messages with this method when the message length becomes com-parable with the number of pixels in the image. Several steganographic programs cre-ate clusters of close palette color that can be swapped for each other to embed message bits. These programs decrease the color depth and then expand it to 256 by making small perturbations to the colors. This preprocessing, however, will cre-ate suspicious pairs (clusters) of colors that others can detect easily. Lossless data embedding In our previous work on lossless (or invertible) data embedding, LSB embed-ding in color and grayscale images originated by analyzing the capacity for lossless data embedding in the LSBs. Randomizing the

Thus, the lossless capacity became a sensitive measure for the degree of randomization of the LSB plane. Note that for most images the LSB plane is essentially random and doesn't contain any easily recognizable structure. Using classical statistical quantities constrained to the LSB plane to capture the degree of randomization is unreliable. The lossless capacity reflects the fact that the LSB plane—even though it looks ran-dom—is related nonetheless to the other bit planes. This relationship, however, is nonlinear, and the lossless capacity seems to measure this relationship fairly well. This is why we proposed it for steganography detection. LSB replacement is a well-known steganographic method. In this embedding scheme, only the LSB plane of the cover image is overwritten with the secret bit stream according to a pseudorandom number generator (PRNG). As a result, some structural asymmetry (never decreasing even pixels and increasing odd pixels when hiding the data) is introduced, and thus it is very easy to detect the existence of hidden message even at a low embedding rate using some reported steganalytic algorithms, such as the Chi-squared attack [2], regular/singular groups (RS) analysis [3], sample pair analysis [4], and the general framework for structural steganalysis [5], [6]. LSB matching (LSBM) employs a minor modification to LSB replacement. If the secret bit does not match the LSB of the cover image, then or is randomly added to the corre-sponding pixel value. Statistically, the probability of increasing or decreasing for each modified pixel value is the same and so the obvious asymmetry artifacts introduced by LSB replacement can be easily avoided. Therefore, the common approaches used to detect LSB replacement are totally ineffective at detecting the LSBM. Up to now, several steganalytic algorithms (e.g., [7]–[10]) have been proposed to analyze the LSBM scheme. In [7], Harmsen and Pearlman showed that LSBM works as a low-pass filter on the histogram of the image, which means that the histogram of the stego image contains fewer high-frequency components compared with the histogram of its cover.

Based on this property, the authors introduced a detector using the center of mass (COM) of the histogram characteristic function (HCF). In [8], Ker pointed out that the original HCF COM method in [7] does not work well on grayscale images and introduced two ways of applying the HCF COM method, namely utilizing the down-sampled image and the adjacency histogram instead of the traditional histogram, which are effective for grayscale im-ages that have been JPEG compressed with a low quality factor, say, 58. In a recent work [10], Li et al.proposed to calculate calibration-based detectors, such as Calibrated HCF COM, on the difference image. The experimental results showed that the new detector outperforms Ker's approaches in [8] and achievedacceptable accuracy at an embedding rate of 50%. In [9], Huang

II. RELATED WORKS

This letter proposes a modification to the least-significant-bit (LSB) matching, a steganographic method for embedding message bits into a still image. In the LSB matching, the choice of whether to add or subtract one from the cover image pixel is random. The new method uses the choice to set a binary function of two cover pixels to the desired value. The embedding is per-formed using a pair of pixels as a unit, where the LSB of the first pixel carries one bit of information, and a function of the two pixel values carries another bit of information. Therefore, the modified method allows embedding the same payload as LSB matching but with fewer changes to the cover image. The experimental results of the proposed method show better performance than traditional LSB matching in terms of distortion and resistance against existing steganalysis.
This paper introduces a new, principled approach to detecting least significant bit (LSB) steganography in digital signals such as images and audio. It is shown that the length of hidden messages embedded in the least significant bits of signal samples can be estimated with relatively high precision. The new steganalytic approach is based on some statistical measures of sample pairs that are highly sensitive to LSB embedding operations. The resulting detection algorithm is simple and fast. To evaluate the robustness of the proposed steganalytic approach, bounds on estimation errors are developed. Furthermore, the vulnerability of the new approach to possible attacks is also assessed, and counter measures are suggested

A. D. Ker, proposed a new technique that is a new framework of LSB steganalysis of digital media a general framework for the detection of the least significant bit (LSB) steganography using digital media files as cover objects. The new framework exploits high-order statistics of the samples. It can compute a robust estimate of the length of a secret message hidden in the LSBs of samples for a large class of digital media contents such as image, video, and audio, in which the underlying signals consist of correlated samples. A case study on the LSB steganalysis of natural grey-scale and color images and experimental results are reported.

Hiding a secret image in edges of images The purpose of steganography is covert communication - to hide the very existence of a message from a third party. The paper proposes a new least significant bit embedding algorithm for hiding secret messages in nonadjacent pixel locations of edges of images. It ensures a better security against eavesdroppers.

III. PROBLEM AND THE PROBLEM SOLVING APPROACHES

A. *EXISTING SYSTEM*

The least-significant-bit (LSB)-based approach is a popular type of steganographic algorithms in the spatial domain. However, we find that in most existing approaches, the choice of embedding positions within a cover image mainly depends on a pseudorandom number generator without considering the relationship between the image content itself and the size of the secret message. Thus the smooth/flat regions in the cover images will inevitably be contaminated after data hiding even at a low embedding rate, and this will lead to poor visual quality and low security based on our analysis and extensive experiments, especially for those images with many smooth regions. Steganographic method based on least-significant-bit (LSB) replacement and pixel-value differencing (PVD) method is presented. First, a different value from two consecutive pixels by utilising the PVD method is obtained. A small difference value can be located on a smooth area and the large one is located on an edged area. In the smooth areas, the secret data is hidden into the cover image by LSB method while using the PVD method in the edged areas. Because the range width is variable, and the area in which the secret data is concealed by LSB or PVD method are hard to guess. To estimate how many secret bits will be embedded into the two pixels. Pixels located in the edge areas are embedded by a k-bit LSB substitution method with a larger value of k than that of the pixels located in smooth areas.

The range of difference values is adaptively divided into lower level, middle level, and higher level. For any pair of consecutive pixels, both pixels are embedded by the k-bit LSB substitution method. However, the value k is adaptive and is decided by the level which the difference value belongs to. Most existing steganographic approaches usually assume that the LSB of natural covers is insignificant and random enough, and thus those pixels/pixel pairs for data hiding can be selected freely using a PRNG. However, such an assumption is not al-ways true, especially for images with many smooth regions.

B. *PROPOSED SYSTEM*

In this paper, we consider dig-ital images as covers and investigate an adaptive and secure data hiding scheme in the spatial least-significant-bit (LSB) domain. LSB replacement is a well-known steganographic method. In this embedding scheme, only the LSB plane of the cover image is overwritten with the secret bit stream according to a pseuo random number generator (PRNG). As a result, some structural asymmetry (never decreasing even pixels and increasing odd pixels when hiding the data) is introduced, and thus it is very easy to detect the existence of hidden message even at a low em-bedding rate using some reported steganalytic algorithms, such as the Chi-squared attack [2], regular/singular groups (RS) analysis [3], sample pair analysis [4], and the general framework for structural steganalysis [5], [6].

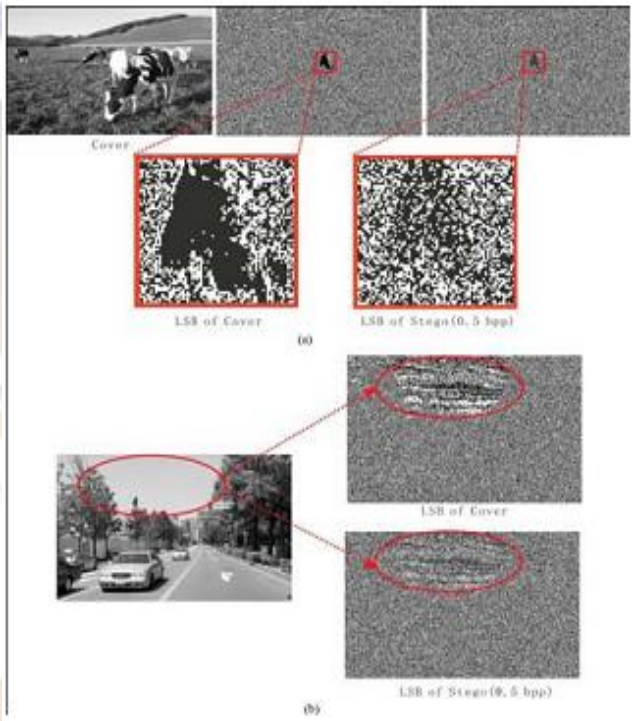

Figure 1.

This paper presents a novel steganographic algorithm based on the spatial domain: Selected least Significant Bits (SLSB). It works with the least significant bits of one of the pixel color components in the image and changes them according to the message's bits to hide. The rest of bits in the pixel color component selected are also changed in order get the nearest color to the original one in the scale of colors. This new method has been compared with others that work in the spatial domain and the great difference is the fact that the LSBs bits of every pixel color component are not used to embed the message, just those from pixel color component selected.

IV. PERFORMANCE ANALYSIS

In this section, we will present some experimental results to demonstrate the effectiveness of our proposed method com-pared with existing relevant methods as mentioned in

Section II. Three image datasets have been used for algorithm evaluation, UCID [22] including 1338 uncompressed color images with a size of 384 × 512 or 512 × 384, NJIT dataset including 3680 uncompressed color images with a size of either 512 × 768 or 768 × 512, which were taken with different kinds of camera, and our dataset SYSU including 982 TIFF color images with a size of 640 ×480. In all, there are 6000 original uncompressed color images including (but not limited to) landscapes, people, plants, animals, and buildings. All the images have been converted into grayscale images in the following experiments.

A. Embedding Capacity and Image Quality Analysis One of the important properties of our steganographic method is that it can first choose the sharper edge regions for data hiding according to the size of the secret message by adjusting a threshold . As illustrated in Fig. 5, the larger the number of secret bits to be embedded, the smaller the threshold becomes, which means that more embedding units with lower gradients in the cover image can be released (please refer to the definition of in Step 3 in data embedding). When is 0, all the embedding units within the cover become available. In such a case, our method can achieve the maximum embedding capacity of 100% (100% means 1 bpp on average for all the methods in this paper), and therefore, the embedding capacity of our proposed method is almost the same as the LSBM and LSBMR methods except for 7 additional bits.

From Fig. 5, it can also be observed that most secret bits are hidden within the edge regions when the embedding rate is low, e.g., less than 30% in the example, while keeping those smooth regions such as the sky in the top left corner as they are. Therefore, the subjective quality of our stegos would be improved based on the human visual system (HVS) characteristics. Table I shows the average PSNR, weight-PSNR (wPSNR is a better image quality metric adopted in Checkmark Version 1.2

The PSNR is less for non-adaptive steganography method than adaptive steganography method. The less MSE and more PSNR is the desirable condition for better performance. The adaptive steganography method satisfies this so, adaptive method is better choice for gray-scale images. For colored images the MSE is less and PSNR is more in non-adaptive steganography method than in adaptive steganography method. As

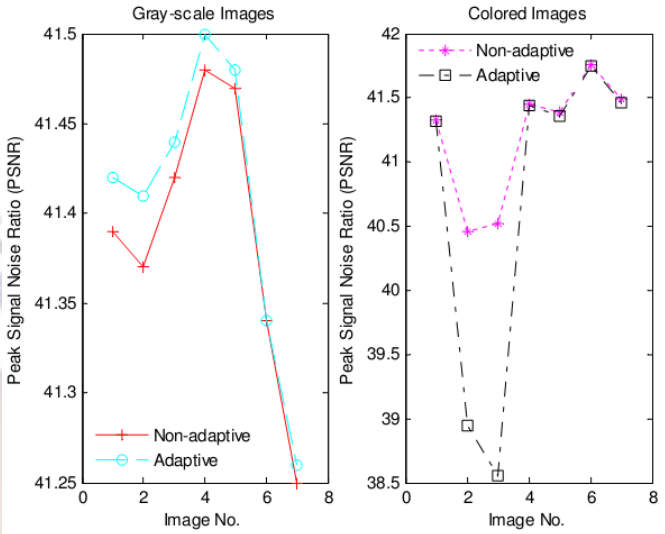

Fig. 4(a) Fig. 4(b)

Fig. 4(a) Comparison of PSNR of non-adaptive and adaptive method (gray-scale),
Fig. 4(b) Comparison of PSNR of non-adaptive and adaptive method (colored)

compared to adaptive method, the performance of non-adaptive method is better for colored images. For gray-scale images, a trend is observed that PSNR is higher and MSE is less in case of adaptive method, therefore adaptive method is better for gray-scale images. For colored images, a trend is observed that PSNR is higher and MSE is less in case of non-adaptive method, therefore non-adaptive is better for colored images. 100% recovery of original image is observed after extraction of secret data.

V. SYSTEM IMPLEMENTATION

A. Data Embedding

Step 1 : The cover image of size of is first divided into non overlapping blocks of pixels. For each small block, we rotate it by a random degree in the range of, as determined by a secret key. The resulting image is rearranged as a row vector by raster scanning. And then the vector is divided into non overlapping embedding units with every two consecutive pixels, where, assuming is an even number.

$$y_i = \begin{cases} x_i + 1 & \text{if } i \in \Lambda_1 \\ x_i - 1 & \text{if } i \in \Lambda_2 \\ x_i & \text{if } i \in \Lambda_3 \end{cases} \quad (1)$$

$$H_j : y_i = x_i + d_i, \quad j = 1, 2, 3 \tag{2}$$

$$P(d_1 = 1, l_1 = 1, \ldots, d_{|\Omega|}, l_{|\Omega|}) = (p_d p_l)^{|\Omega|} \tag{3}$$

$$H = \arg\max_j P(H_j) P(y_i | H_j) \tag{4}$$

where, is the size of the secret message , and denotes the total number of elements in the set of .

Since y_i is Gaussian the MAP detector becomes

$$H = \arg\max_j P(H_j) exp \frac{-(y_i - d_j)^2}{2\sigma^2} \tag{5}$$

Therefore, $u_i = H_j$, $j = 1, 2$ or 3. Using a minimum probability of error criterion we observe that hidden data is detected if,

$$P(H_1) \prod_{i=1}^{M} P(u_i|H_1) \begin{cases} > P(H_2) \prod_{i=1}^{M} P(u_i|H_2) & \text{and} \\ > P(H_3) \prod_{i=1}^{M} P(u_i|H_3) \end{cases} \tag{6}$$

or

$$P(H_2) \prod_{i=1}^{M} P(u_i|H_2) \begin{cases} > P(H_1) \prod_{i=1}^{M} P(u_i|H_1) & \text{and} \\ > P(H_3) \prod_{i=1}^{M} P(u_i|H_3) \end{cases} \tag{7}$$

Both these cases will have the same probability of error due to symmetry. So, we consider only the first case. We make another simplification. Only the detection of H_1 versus H_3 is considered because they are statistically *closer* than H_1 and H_2. So, the multiple hypothesis problem has been simplified to binary hypothesis testing. We now have,

$$\frac{\prod_{i=1}^{M} P(u_i|H_1)}{\prod_{i=1}^{M} P(u_i|H_3)} \begin{cases} > \frac{P(H_3)}{P(H_1)} & \text{decide Hidden Data} \\ \text{else} & \text{decide No Hidden Data} \end{cases} \tag{8}$$

which gives

$$\prod_{S_1} \frac{P(u_i = 1|H_1)}{P(u_i = 1|H_3)} \prod_{S_2} \frac{P(u_i = -1|H_1)}{P(u_i = -1|H_3)} \prod_{S_3} \frac{P(u_i = 0|H_1)}{P(u_i = 0|H_3)} \tag{9}$$

$$\begin{cases} > \frac{P(H_3)}{P(H_1)} & \text{decide Hidden Data} \\ \text{else} & \text{decide No Hidden Data.} \end{cases}$$

This in turn implies,

$$\prod_{S_1} \frac{p_{11}}{p_{31}} \prod_{S_2} \frac{p_{12}}{p_{32}} \prod_{S_3} \frac{p_{13}}{p_{33}} \begin{cases} > \frac{P(H_3)}{P(H_1)} & \text{decide Hidden Data} \\ \text{else} & \text{decide No Hidden Data} \end{cases} \tag{10}$$

Here, S_1, S_2, and S_3 denote the set of pixels where 1, -1, and 0 is detected, respectively. If $P_d = P(\text{decide } H_1 | H_1 \text{ true})$ is the probability of correct detection and $P_f = P(\text{decide } H_1 | H_3 \text{ true})$ denotes the false alarm probability of the steganalyst then we see from Eq. (10) that these quantities are functions of $|S_1|$ and $|S_2|$, the number of hidden bits. there are 2^{3^M} possible detection rules the second detector can employ. This includes the optimal detector also. Sometimes, computing the parameters of the global detection rule may be highly computationally intensive. Therefore, we sacrifice optimality for tractability. In this spirit, suppose the second detector uses a J-out-of-M detection rule (*i.e.*, if J or more out of M decisions favor Hidden Data the steganalyst decides Hidden Data) then

$$P_d = \sum_{k=J}^{M} \sum_{r=0}^{M-k} \frac{M!}{k!r!(n-k-r)!} p_{11}^k p_{12}^r p_{13}^{M-k-r} \tag{11}$$

$$P_f = \sum_{k=J}^{M} \sum_{r=0}^{M-k} \frac{M!}{k!r!(n-k-r)!} p_{31}^k p_{32}^r p_{33}^{M-k-r} \tag{12}$$

B.DATA EXTRATCION:

The reciever will need the Following
1. Stego-image (downloaded from web)
2. Stego Key

T, the Threshold Significant Value, to look for the coefficients below these values of Original Image. Then extract by subtracting the coefficients below T from Original coefficients and Inverse DCT. To date, DCT Algorithm can successfully extract a small Text Message and our algorithm also increasing the Payload (amount hidden data) Thus seeing how much hiding bandwidth can be used on different Images.

C. Selected Least Significant Bit Encoding

Selected Least significant bit (LSB) coding is the simplest way to embed information in a digital audio file. By substituting the least significant bit of each sampling point with a binary message, Selected LSB coding allows for a large amount of data to be encoded. In SLSB coding, the ideal data transmission rate is 1 kbps per 1 kHz. In some implementations of SLSB coding, however, the two least significant bits of a sample are replaced with two message bits. This increases the amount of data that can be encoded but also increases the amount of resulting noise in the audio file as well Thus, one should consider the signal content before deciding on the SLSB operation to use. For example, a sound file that was recorded in a bustling subway station would mask low-bit encoding noise. On the other hand, the same noise would be audible in a sound file containing a piano solo. To extract a secret message from an SLSB encoded sound file, the receiver needs access to the sequence of sample indices used in the embedding process. Normally, the length of the secret message to be encoded is

smaller than the total number of samples in a sound file. One must decide then on how to choose the subset of samples that will contain the secret message and communicate th at decision to the receiver. One trivial technique is to start at the beginning of the sound file and perform SLSB coding until the message has been completely embedded, leaving the remaining samples unchanged. This creates a security problem, however in that the first part of the sound file will have different statistical properties than the second part of the sound file that was not modified.

VI. CONCLUSION

In this paper, an edge adaptive image steganographic scheme in the spatial SLSB domain is studied. As pointed out in, there usually exists some smooth regions in natural images, which would cause the SLSB of cover images not to be completely random or even to contain some texture information just like those in higher bit planes. If embedding a message in these regions, the SLSB of stego images becomes more random, and according to our analysis and extensive experiments, it is easier to detect. In most previous steganographic schemes, however, the pixel/pixel-pair selection is mainly determined by a PRNG without considering the relationship between the characteristics of content regions and the size of the secret message to be embedded, which means that those smooth/flat regions will be also contaminated by such a random selection scheme even if there are many available edge regions with good hiding characteristics. To preserve the statistical and visual features in cover images, we have proposed a novel scheme which can first embed the secret message into the sharper edge regions adaptively according to a threshold determined by the size of the secret message and the gradients of the content edges. The experimental results evaluated on thousands of natural imagesusing different kinds of steganalytic algorithms show that both visual quality and security of our stego images are improved significantly compared to typical SLSB-based approaches and their edge adaptive versions. Furthermore, it is expected that our adaptive idea can be ex-tended to other steganographic methods such as audio/video steganography in the spatial or frequency domains when the embedding rate is less than the maximal amount.

Reference:

[1] J. Mielikainen, "LSB matching revisited," IEEE Signal Process. Lett. , vol. 13, no. 5, pp. 285–287, May 2006.
[2] A. Westfeld and A. Pfitzmann, "Attacks on steganographic systems," in Proc. 3rd Int. Workshop on Information Hiding , 1999, vol. 1768, pp. 61–76.
[3] J. Fridrich, M. Goljan, and R. Du, "Detecting LSB steganography in color, and gray-scale images," IEEE Multimedia, vol. 8, no. 4, pp. 22–28, Oct. 2001.
[4] S. Dumitrescu, X. Wu, and Z. Wang, "Detection of LSB steganography via sample pair analysis," IEEE Trans. Signal Process. , vol. 51, no. 7, pp. 1995–2007, Jul. 2003.
[5] A. D. Ker, "A general framework for structural steganalysis of LSB replacement," in Proc. 7th Int. Workshop on Information Hiding, 2005, vol. 3427, pp. 296–311.
[6] A. D. Ker, "A fusion of maximum likelihood and structural steganalysis," in Proc. 9th Int. Workshop on Information Hiding, 2007, vol. 4567, pp. 204–219.
[7] J. Harmsen and W. Pearlman, "Steganalysis of additive-noise modelable information hiding," Proc. SPIE Electronic Imaging, vol. 5020, pp. 131–142, 2003.
[8] A. D. Ker, "Steganalysis of LSB matching in grayscale images," IEEE Signal Process. Lett., vol. 12, no. 6, pp. 441–444, Jun. 2005.
[9] F. Huang, B. Li, and J. Huang, "Attack LSB matching steganography by counting alteration rate of the number of neighbourhood gray levels," in Proc. IEEE Int. Conf. Image Processing, Oct. 16–19, 2007, vol. 1, pp. 401–404.
10] X. Li, T. Zeng, and B. Yang, "Detecting LSB matching by applying calibration technique for difference image," in Proc. 10th ACM Work- shop on Multimedia and Security, Oxford, U.K., 2008, pp. 133–138.
11] Y. Q. Shiet al., "Image steganalysis based on moments of characteristic functions using wavelet decomposition, prediction-error image, and neural network," in Proc. IEEE Int. Conf. Multimedia and Expo , Jul. 6–8, 2005, pp. 269–272.
12] B. Li, J. Huang, and Y. Q. Shi, "Textural features based universal steganalysis," Proc. SPIE on Security, Forensics, Steganography and Watermarking of Multimedia , vol. 6819, p. 681912, 2008.
13] M. Goljan, J. Fridrich, and T. Holotyak, "New blind steganalysis and its implications," Proc. SPIE on Security, Forensics, Steganography and Watermarking of Multimedia, vol. 6072, pp. 1–13, 2006.
[14] K. M. Singh, L. S. Singh, A. B. Singh, and K. S. Devi, "Hiding secret message in edges of the image," inProc. Int. Conf. Information and Communication Technology, Mar. 2007, pp. 238–241.
[15] M. D. Swanson, B. Zhu, and A. H. Tewfik, "Robust data hiding for images," in Proc. IEEE on Digital Signal Processing Workshop , Sep. 1996, pp. 37–40.
[16] D. Wu and W. Tsai, "A steganographic method for images by pixel-value differencing," Pattern Recognit. Lett., vol. 24, pp. 1613–1626, 2003.
[17] X. Zhang and S. Wang, "Vulnerability of pixel-value differencing steganography to histogram analysis and modification for enhanced security," Pattern Recognit. Lett., vol. 25, pp. 331–339, 2004.