IJCSE International Journal of Computer Sciences and Engineering Open Access
Research Paper Volume-4, Issue-10 E-ISSN: 2347-2693

Improved Random Area Selective Image Steganography with LSBMR

Neethan Elizabeth Abraham[1*], Reshm Chandran[2], Jyothisree[3], Sunu Ann Thomas[4]

[1,2,3,4]Department of ECE, Mangalam College of Engineering, Kerala

Available online at: www.ijcseonline.org

Received: 23/Sep/2016 Revised: 29/Sep/2016 Accepted: 22/Oct/201 Published: 31/Oct/2016

Abstract -Image steganography is the art of hiding secret message in grayscale or color images. Easy detection of secret message for any state-of-art image steganogra- phy can break the stego system. To prevent the breakdown of the stego system data is embedded in the selected area of an image which reduces the probability of detection. Most of the existing adaptive image steganography techniques achieve low embedding capacity. In this paper a high capacity Predictive Edge Adaptive image steganography technique is proposed where selective area of cover image is predicted using Modified Median Edge Detector (MMED) predictor to embed the binary payload (data). The cover image used to embed the payload is a grayscale image. Experimental results show that the proposed scheme achieves better embedding capacity with minimum level of distortion and higher level of security. The proposed scheme is compared with the existing image steganography schemes. Results show that the proposed scheme achieves better embedding rate with lower level of distortion.

Keywords - Edge adaptive ·High level bit plane ·Low level bit plane ·Predictive image

I. Introduction

Image steganography is used to hide secret information within an image [4]. Two major approaches used are reversible and irreversible image steganography.

In reversible image steganography [1, 9, 12, 16, 17, 19, 23, 27, 28, 33] the cover image can be reconstructed accurately while extracting the payload from the stego image. The stego image is the image obtained after embedding the secret message in cover image. Most of the existing reversible image steganography schemes are very complex and achieve small em- bedding capacity [1, 13, 26, 27]. Embedding capacity can be increased by adaptive embedding of payload near sharper edges. More bits can be accommodated in sharper edges using adaptive selection.

Irreversible image steganography schemes achieve higher embedding capacity with minimum computation time. Detection of hidden information in stego image resulting from irreversible stego system is straightforward. Many steganalytic schemes [7, 10, 14] have been proposed in literature, which can accurately detect the presence of secret information embedded using irreversible image steganography. These methods are prone to easy detection of the embedded information. Even though irreversible image steganography schemes achieve low computation time, low level of security degrades the performance of such system. Encryption of secret information could be one of the solutions. However, inclusion of encryption spoils the use of steganography as the fundamental need of image steganography is to eradicate the suspicion of hidden data.

In this paper an adaptive image steganography technique which bears high embedding rate is proposed. Adaptive nature of the embedding process increases the embedding rate without increasing the detectability. Binary payload is embedded in edge area of a grayscale cover image. Grayscales of the cover image are used to embed binary payload in selected area based on some threshold which determines the number of bits to be embedded.

II. Related work

There are many reversible image steganography schemes proposed in the literature which employ encryption to achieve higher level of security. Wu et al. proposed a reversible image steganography scheme [32], where the secret message is encrypted using either AES or DES. The encrypted bits are then embedded in a code tree computed from the frequency of absolute error values. Error values are computed using MED predictor [32].

Scheme proposed in [29] generates an intermediate image by converting a pair of pixel values of secret image into four hexadecimal values and then four hexadecimal values are converted to three decimal values. This intermediate image is then distributed and embedded into n cover images. To recover the secret image one has to gather all n stego images. The steganography scheme used in this method is straightforward. Detection of hidden information is so trivial that any steganalysis scheme can detect the presence of hidden information with more than 80 % accuracy.

A data hiding based on side-match vector quantization (SMVQ) has been proposed by Chang et al. [3]. For each block of cover image codeword is generated using SMVQ. These codeword are used to embed the secret data. If secret bit is equal to 0,the closest codeword generated by SMVQ is encoded. For a secret bit 1 the approx- imation of the first closest codeword and the second closest

codeword is computed to replace the closest codeword. Even though the proposed scheme effectively encodes the secret message, for a large payload the size of transformed index table can increase the space complexity of the steganography system. Moreover, the embedding capacity of the scheme is low compared to other existing image steganography schemes.

High embedding rate of irreversible image steganography draws researchers to work in this area. Level of security is a concern in irreversible image steganography. Easy detection of hidden data is possible with some powerful steganalytic tools.

Least Significant Bit (LSB) replacement is the most common irreversible steganog- raphy scheme. The binary bits of the secret data are hidden in the cover image by replacing the LSBs of the cover image with the secret binary bits [31]. The method is so trivial that an attacker can easily detect the presence of hidden information.

Modification rate is further reduced in LSB matching revisited (LSBMR) [11, 22]. A pair of pixel is used to embed the secret bits. A secret bit is added to the first pixel of the pair and another bit is embedded using the relationship of the pair of pixels. As only one pixel of the pair is modified to embed two secret bits the modification rate reduces to 0.375 bit per pixel (bpp) [22]. General asymmetry introduced in LSB does not exist in LSBMR hence detection of the presence of secret bits is difficult. There are some edge adaptive methods proposed in literature such as hide behind corner (HBC) [8]. Edge adaptive irreversible image steganography proposed by Lou et al.

[20] embeds secret data adaptively in the selected regions of the cover image. Method proposed in [20] extends LSBMR [22] and embeds secret data in edge areas of the cover image baring smoother areas. To embed the secret data cover image is first rotated using a specific key. Edge areas of the modified cover are identified to embed the secret information adaptively. This method is highly secure as percentage accuracy of detection of most of the statistical analysis used on the stego images, generated using the method proposed by Luo et al. [20], is less. The method proposed in [20] identifies an edge as the difference between two consecutive pixels. Data is embedded only in those areas where a vertical edge exists. A single bit is embedded in two consecutive pixels. Even though this method selects edge area adaptively it is done using a single threshold value. Hence the method proposed in [20] is not at all adaptive when it comes to embedding. The proposed method tries to identify vertical as well as horizontal edges to embed the secret data, which intern increases the embedding capacity of the proposed scheme. MMED effectively predicts horizontal as well as vertical edges. Edges are classified into three categories using three levels of threshold. More bits are embedded in sharper edges, which again increase the embedding rate. Result analysis shows that the proposed method achieves better results with respect to embedding rate and lesser percentage accuracy of detection compared to most of the state of the art steganography methods.

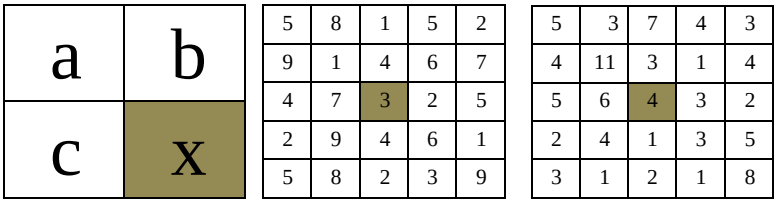
III. Proposed method

Proposed method has two major phases; embedding and recovery as shown in Fig. 1. To embed the secret message S, MMED predictor is used to compute the edge image from the cover image. Region selector divides the edge image into nonoverlapping Z × Z blocks. Predicted error greater than a particular threshold, are selected from each block for capacity estimation. Capacity of each block is measured by computing the number of bits that can be embedded into a particular block. In each block for a particular predictive error one, two or three bits of the secret message can be embedded into the corresponding grayscale of the original cover depending on the threshold. Capacity is computed by adding the number of bits that can be embedded in a particular grayscale of a block. If the capacity of the block is not enough to accommodate the secret data region selector re-computes the region for embedding. There are certain additional information required for extraction of the secret data such as block size (Z) and threshold (T_k) which are embedded in those regions which are not used for data embedding.

III.1 Embedding process

The cover image C of size m × n is first converted to predictive error image of same size using MMED predictor. A template shown in Fig.2a is used to compute the predictive error image. Predictive error image is computed asA sample sub image is shown in Fig. 2b and its corresponding MMED predictive error image is shown in Fig. 2c. Shaded pixel in Fig.2b is has a = 1, b = 4 and c =7 and 1 ≤ min (4,7), hence the corresponding MMED value is MMED(3) = |3− max(4, 7)| = 4. This MMED value corresponding to 3 is the shaded pixel shown inFig. 2c. It is evident from Fig. 2c that the predictive error image contains the horizontal as well as vertical edges of the sample sub image.

Predictive error image computed using MMED predictor is divided into non-overlapping blocks of Z × Z pixels.Secret message S is divided into three subparts namely S_1, S_2 and S_3 such that$|S_1|$ = 60 percent of |S|, $|S_2|$ = 30 percent of |S|, $|S_3|$ = 10 percent of |S| and |S|= $|S_1|$+ $|S_2|$+ $|S_3|$. Threshold T_k for region selector is computed using a threshold selection parameter p_k. $M(p_k)$ is the set of MMED values defined as $M(p_k)$= {MMED(x_{ij})|p_k ≤ MMED(x_{ij})< 2^{3+k}, ∀x_{ij}∈ C} where k ∈ {1, 2, 3}. Threshold parameters are defined as p_1∈ {0, 1, 2 … 15},p_2∈ {16, 17, 18 … 31} and p_3∈ {32, 33, 34 … 63}. Threshold values are computed using threshold selection parameters as T_k ¼ argmax_{pk} fjMðp_k Þj≥j$S_k$jg where k ∈ {1, 2, 3}.Number of bits embedded in a particular pixel x_{ij}∈ C depends upon T_k. Embedding is performed on cover image C as follows



(a) (b) (c)

Fig. 1 (a) Template for MMED, (b) Sample sub image and (c) Corresponding MMED predictive error image

Pixels belonging to smoother edges are used to embed one or two bits of the secret message. Secret bits are used to replace either single LSB of the pixels belonging to the smoother edge area or two LSBs of the pixel belonging to the smoother edge area. Three bits are embedded in the pixels belonging to sharper edge area.Extraction is performed on stego image based on threshold (T_k) as Pixels from the stego image are selected using raster scan. MMED values are compared with threshold to decide on the number of bits to be extracted from each pixel of the stego image.

III.2 Complexity analysis

To compute the MMED at most 7 fundamental operations are required per pixel. As the size of the image is m × n the total number of operations required to compute MMED is 7 × (m × n). $M(p_k)$ is computed for each block of size Z × Z using 2 fundamental operations (≤, <) per pixel, hence the total operations required to compute $M(p_k)$ per block is 2 × (Z × Z). As there are $\frac{m \times n}{}$ blocks, hencethe number of comparisons required to compute M(p) over entire image is 2 × (m x n). Similarlythreshold selection requires at most 6 × (m × n) operations. So, parameter selection process requires at most 15 × (m × n) operations. Embedding and extraction process requires (2 × 7 × S) operations. Hence the computation complexity of the proposed method is O((m × n) + S).

IV. Experimental results

Proposed scheme has been analyzed using 500 images from USC-SIPI image database. Qualitative as well as quantitative analysis of the proposed scheme have been done using these images. The proposed scheme has been compared with Reversible as well as irreversible image steganography methods. Quantitative measures such as embedding rate, embedding capacity and peak signal to noise ratio (PSNR) are used. Performance of the proposed method has been evaluated using different steganalysis techniques.

IV.1 Qualitative and quantitative analysis

Embedding rate is measured as the total number of bits embedded in a particular cover image. Percentage embedding is used to measure as well as compare the embedding rate of the proposed scheme.

It is the ratio of the square of maximum grayscale intensity I_{max} to the mean square error (MSE) of the original cover and the corresponding stego image. MSE is defined asis the quality of stego image [24]. Figure 3 shows some of the cover images for which Table 1 illustrates the embedding capacity and corresponding PSNR of the proposed scheme and some of the existing reversible image steganography schemes.

Table 1 shows that the proposed scheme achieves higher embedding capacity than most of the reversible image steganography methods. Embedding region selected for different embed- ding rate is shown in Fig. 4. It is visually clear from Fig. 4 that embedding is done mostly in edge areas, if the embedding rate is low. Hence maximum visual quality can be achieved instego images with lower embedding rate. Even though embedding rate is increased to 50 %, embedding is confined to edge area of the cover image as shown in Fig. 4. With higher embedding rate the proposed scheme tends to keep smoother regions intact, which increases the visual quality of the stego images even for higher embedding rates.

(a) (b) (c) (d) (e)

Fig. 3 Cover images for which embedding capacity and corresponding PSNR are Computed. a Elaine, b Boat, cPepper, d Baboon, e Barbara

Table 1 Comparison of maximum payload (bits) and corresponding PSNR (dB)

Method	Elaine		Boat		Pepper		Baboon		Barbara	
	Payload	PSNR	Payload	PSNR	Payload	PSNR	Payload	PSNR	Payload	PSNR
Ni et al. [23]	4878	48.2	11,441	48.2	5415	48.2	5432	48.22	5836	47.08
Tasi et al. [28]	25,462	48.9	25,788	48.92	32,186	48.99	12,983	48.8	36,361	49.63
Luo et al. [19]	27,687	49.7	28,041	49.74	33,783	49.8	14,544	49.59	49,338	49.92
Kim et al. [16]	21,965	49.6	22,480	49.63	27,045	49.68	11,279	49.5	30,764	49.22
Hong et al. [9]	27,194	49.7	28,739	50.11	34,758	49.87	13,024	51.24	49,475	50.77
J. Tian [27]	28,658	48.2	28,875	49.53	35,767	46.72	14,457	48.52	37,568	49.46
Proposed	37,012	50.3	32,623	51.83	38,657	50.29	30000	53.02	61,656	53.84

Figure 5 shows the capacity distortion curves of different steganography techniques for two images namely Barbara and Eline. Secret bits are embedded in images of size 100 × 100. Method proposed by Thodi et al. [26] has been implemented using prediction error expansion with histogram shifting and flag bits (i.e. P3 version [26]) to compare the results with our proposed method. Proposed method achieves better PSNR even with higher embedding rates as shown in Fig. 5. Proposed scheme is analyzed and compared with existing irreversible steganography methods using embedding rate, average PSNR and average modification rate. Modification rate is defined as the number of bits flipped in a cover image to embed the secret data. We have implemented theses steganography schemes to compute the stego images for 500 grayscale images taken from the database. Different embedding rates are used to compute PSNR and modification rate of all images. Averages of PSNR and modification rate computed

Visual attack is the most commonly used tool to detect the presence of the hidden data [20, 25]. Visual distortion introduced into the low level bit planes of the stego image reveals the regions

Table 2 Comparison of embedding rate and average PSNR (dB)

Embedding Rate	Method	Average PSNR	Average modification rate
10 %	LSBM	61.1	0.0500
	LSBMR	62.2	0.0375
	HBC	61.1	0.0500
	Luo et al. [20]	61.6	0.0369
	Proposed	65.7	0.0700
20 %	LSBM	57.7	0.0900
	LSBMR	59.02	0.0600
	HBC	58.4	0.1000
	Luo et al. [20]	59.46	0.1035
	Proposed	63.73	0.1200
30 %	LSBM	56.4	0.1500
	LSBMR	57.4	0.1280
	HBC	56.7	0.1500
	Luo et al. [20]	56.73	0.1164
	Proposed	61.5	0.1730
50 %	LSBM	54.2	0.2500
	LSBMR	55.5	0.1875
	HBC	54.3	0.2500
	Luo et al. [20]	54.57	0.2205
	Proposed	59.8	0.3026

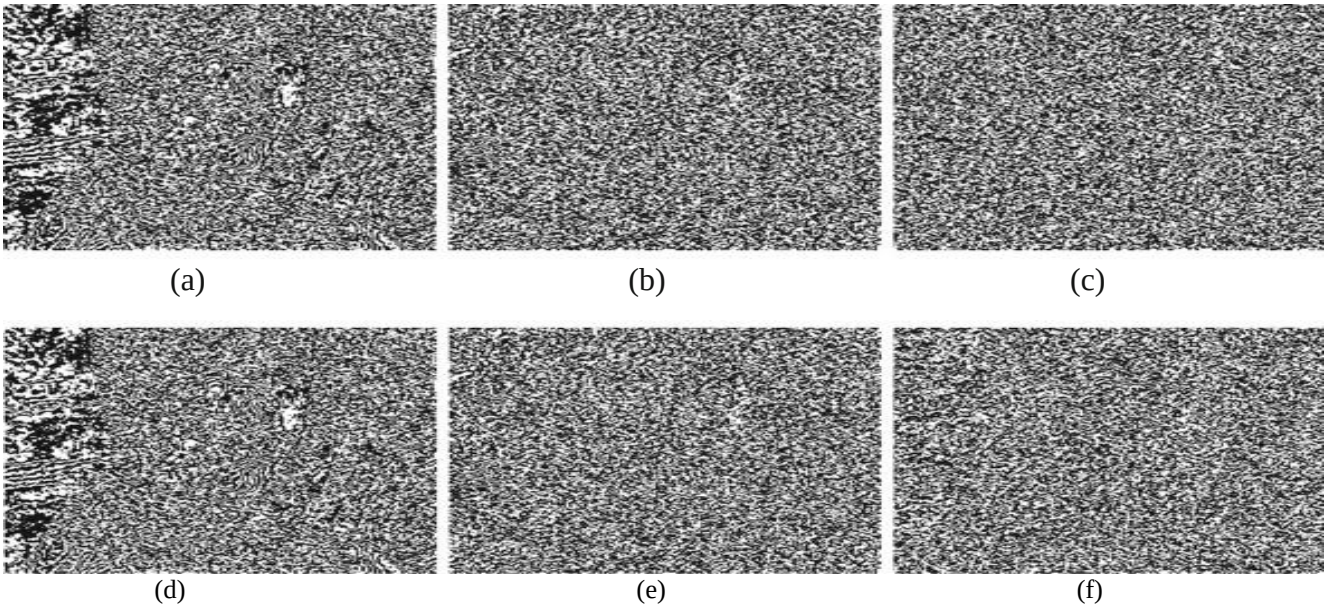
where the secret data has been hidden. Proposed scheme embeds secret data in LSBs of the cover image. Depending upon the sharpness of the edge three or two or single least significant bit plane is used to embed the secret data. Visually bit planes obtained after embedding the secret data are not different from the least significant bit planes of the original cover as shown in Fig. 6. Least significant bit planes of the stego image Barbara shown in Fig. 6, are obtained using 30 % embedding rate. Please note that the proposed scheme does not leave any visual artifacts in the resulting stego image even for higher embedding rates. As steganography methods such as LSBM and LSBMR use random embedding, visual artifacts bound to creep into smooth regions of the resulting stego image. As edge areas are used in the proposed scheme to embed the secret data, it tends to leave smooth regions in a cover. Hence better quality stego images are obtained.

IV.2 Statistical attack

Steganalysis is a method to detect the presence of hidden secret information in an image. Different statistical tools are used to extract the features of the cover and stego images to test the robustness of the steganography technique against the possible statistical attacks. Steganalysis schemes can be broadly classified as

1. Steganalysis specific to a steganography method.
2. Blind Steganalysis.

Specific steganalysis schemes accurately detect the presence of secret information embed- ded into the stego images [18]. These schemes are so powerful that they can even estimate the embedding ratio of the steganography scheme. There are some steganalysis schemes which can reliably detect the presence of secret message for LSB based steganography methods. Regular Singular (RS) analysis is one of the most popular steganalysis schemes used to detect the presence of secret message for LSB replacement algorithms [2, 4, 6, 15, 20].



(a) (b) (c)

(d) (e) (f)

Fig. 6 a–c three least significant bit planes of cover image Barbara. d–f three least significant bit planes of stego image of Barbara

Blind steganalysis schemes tend to classify the images into categories namely cover and stego images. These schemes first extract the features of cover as well as stego images. A classifier is selected and trained using the features extracted from the training sets of cover and the stego images. The test images are then classified into cover and stego images using the classifier. Features are extracted from the images to construct the feature vector of optimal dimensions to differentiate the stego images from the cover.

4.3.1 RS analysis

RS analysis classifies pixels into either regular or singular groups. Regular and singular groups are identified with respect to a mask m. Mask m is a set of −1, 0 and 1 which captures the flipping of pixels of the cover image. General idea of the RS analysis is to detect the change in regular and singular groups with increasing embedding rates. To avoid detection of the presence of secret message in stego images difference between regular groups R_m, R_{-m} and singular groups S_m, S_{-m} should be restricted to minimum. As HBC and Luo et al. [20] are edge adaptive image steganography methods based on LSB the proposed scheme is compared with HBC and Luo et al. [20] using RS analysis. Figure 7 shows RS diagram for Luo et al. [20], HBC and the proposed scheme. Relative percentage of regular and singular groups of different embedding rates computed for the image Barbara. Please note that for proposed scheme the differences between R_m, R_{-m} and S_m, S_{-m} do not increase substantially with increasing embedding rates. Hence the detection probability is less. Difference values for HBC start to expand from 25 % embedding rate where as for the proposed scheme the difference values start to increase beyond 30 % embedding rate. The performance of the proposed scheme is comparable with the steganography scheme proposed by Luo et al. [20]. However the embedding rate of the proposed scheme is better than Luo et al. [20].

V. Conclusion

Proposed method is an edge adaptive irreversible image steganography. A modified edge predictor is proposed to identify the edge areas of a cover image. An adaptive method is also proposed to identify the sharper edges, which can be used to embed more secret message bits. Adaptive nature of the proposed approach increases the embedding capacity and reduces the detection probability. Result analysis shows that the proposed scheme is robust enough to foil most of the powerful steganalysis schemes.

References

[1]. Alattar M (2004) Reversible watermark using the difference expansion of a generalized integer transform. IEEE Trans Image Process 13(8):1147–1156

[2]. Böhme R (2010) Principles of modern steganography and steganalysis. In: Böhme R (ed) Advanced statistical steganalysis, 1st edn. Springer, Berlin Heidelberg, pp 11–77

[3]. Chang CC, Tai WL, Lin CC (2006) A reversible data hiding scheme based on side-match vector quantiza- tion. IEEE Trans Circuits Syst Video Technol 16(10):1301–1308

[4]. Cheddad, Condell J, Curran K, McKevitt P (2010) Digital image steganography: survey and analysis of current methods. Signal Process 90:727–752

[5]. Farid H (2002) Detecting hidden messages using higher-order statistical models. IEEE Image Process IntConfProc 2:905–908

[6]. Fridrich J, Goljan M, Du R (2001) Reliable detection of LSB steganography in color and grayscale images. In: Proceedings of the 2001 workshop on Multimedia and security, pp 27–30. doi:10.1145/1232454.1232466

[7]. Harmsen J, Pearlman W (2003) Steganalysis of additive-noise modelable information hiding. SPIE Electron Imaging ConfProc 5020:131–142

[8]. Hempstalk K (2006) Hiding behind corners: using edges in images for better steganography. In: Computing Women's Congress Proceedings, Hamilton, New Zealand

[9]. Hong W, Chen TS (2011) Reversible data embedding for high quality images using interpolation and reference pixel distribution mechanism. J Vis Commun Image Represent 22:131–140

[10]. Huang F, Li B, Huang J (2007) Attack LSB matching steganography by counting alteration rate of the number of neighborhood gray levels. IEEE Image Process ConfProc 1:401–404

[11]. Huang F, Zhong Y, Huang J (2014) Improved algorithm of edge adaptive image steganography based on LSB matching revisited algorithm. Digital-forensics and watermarking. Lect Notes ComputSci 8389:19–31

[12]. Hwang J, Kim JW, Choi JU (2006) A reversible watermarking based on histogram shifting. Lect Notes ComputSci 4283:348–361

[13]. Kamstra L, Heijmans HJAM (2005) Reversible data embedding into images using wavelet techniques and sorting. IEEE Trans Image Process 14(12):2082–2090

[14]. Ker D (2005) Steganalysis of LSB matching in grayscale images. IEEE Signal Process Lett 12(6):441–444

[15]. Khosravi MJ, Naghsh-Nilchi AR (2014) A novel joint secret image sharing and robust steganography method using wavelet. Multimedia Systems 20(2):215–226

[16]. Kim K, Lee M, Lee H, Lee H (2009) Reversible data hiding exploiting spatial correlation between sub-sampled images. Pattern Recogn 42(11):3083–3096

[17]. Lin CC, Tai WL, Chang CC (2008) Multilevel reversible data hiding based on histogram modification of difference images. Pattern Recogn 41(12):3582–3591

[18]. Luo XY, Wang DS, Wang P, Liu FL (2008) A review on blind detection for image steganography. Signal Process 88:2138–2157

[19]. Luo L, Chen Z, Chen M, Zeng X, Xiong Z (2010) Reversible image watermarking using interpolation technique. IEEE Trans Inf Forensics Secur 5(1):187–193

[20]. Luo W, Huang F, Huang J (2010) Edge adaptive image steganography based on LSB matching revisited. IEEE Trans Inf Forensics Secur 5(2):201–214

[21]. Luo W, Huang F, Huang J (2011) A more secure steganography based on adaptive pixel value differencing scheme. Multimed Tools Appl 52(2–3):407–430

[22]. Mielikainen J (2006) LSB matching revisited. IEEE Signal Process Lett 13(5):285–287

[23]. Ni Z, Shi YQ, Ansari N, Su W (2006) Reversible data hiding. IEEE Trans Circuits Syst Video Technol 16(3):354–362

[24]. Ou D, Sun W (2014) High payload image steganography with minimum distortion based on absolute moment block truncation coding. Multimed Tools Appl. doi:10.1007/s11042-014-2059-2

[25]. Roy R, Changder S, Sarkar A, Debnath NC (2013) Evaluating image steganography techniques: future research challenges. In: Proceedings of International Conference on Computing, Management and Telecommunications (ComManTel), pp 309–314. doi:10.1109/ComManTel.2013.6482411

[26]. Thodi M, Rodríguez JJ (2007) Expansion embedding techniques for reversible watermarking. IEEE Trans Image Process 16(3):721–730

[27]. Tian J (2003) Reversible data embedding using a difference expansion. IEEE Trans Circuits Syst Video Technol 13(8):890–896

[28]. Tsai PY, Hu YC, Yeh HL (2009) Reversible image hiding scheme using predictive coding and histogram shifting. Signal Process 89(6):1129–1143

[29]. Ulutas G, Ulutas M, Nabiyev VV (2012) Secret image sharing with reversible capabilities. International Journal of Internet Technology and Secured Transactions 4(1):1–11

[30]. Vetterli M (1987) A theory of multirate filter banks. IEEE Trans Acoust Speech Signal Process 35(3):356– 372

[31]. Walton S (1995) Image authentication for a slippery new age. Dr Dobbs J Softw Tools Prof Program 20:18–26

[32]. Wu HC, Wang HC, Tsai CS, Wang CM (2010) Reversible image steganographic scheme via predictive coding. Displays 31:35–43

[33]. Zhang L, Wu X (2006) An edge-guided image interpolation algorithm via directional filtering and data fusion. IEEE Trans Image Process 15(8):2226–2238

