Frame Adaptive Picture Steganography Based on LSB Identical Revisited

[1]Puligundla Rajyalakshmi, [2]R. Ravi Kumar
[1,2]Dept. of CSE, Swarna Bharathi Institute of Science and Technology, Khammam, AP, India

Abstract

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. 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. In this paper, we expand the LSB matching revisited image steganog- raphy 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 parameters. The experimental results evaluated on 6000 natural images with three specific and four universal steganalytic algorithms show that the new scheme can enhance the security significantly compared with typical LSB-based approaches as well as their edge adaptive ones, such as pixel-value-differencing-based approaches, while preserving higher visual quality of stego images at the same time.

Keywords

?????????? IS MISSING ????????

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., without being suspicious.

On the other side, steganalysis aims to expose the presence of hidden secret messages in those stego media. If there exists a steganalytic algorithm which can guess whether a given media is a cover or not with a higher probability than random guessing, the steganographic system is considered broken. In practice, two properties, undetectability and embedding capacity, should be carefully considered when designing a steganographic algorithm. Usually, the larger payload embedded in a cover, the more detectable artifacts would be introduced into the stego. In many applications, the most important requirement for steganography is undetectability, which means that the stegos should be visually and statistically similar to the covers while keeping the embedding rate as high as possible. 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 PseuDorandom Number Generator (PRNG).

-1LSB matching (LSBM) employs a minor modification to LSB replacement. If the secret bit does not match the LSB of the cover image, then $+1$ 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.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 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, 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 and achieved acceptable accuracy at an embedding rate of 50. The experimental results demonstrated that the method was more effective on uncompressed grayscale im- ages. Besides those specific detectors, some universal steganalytic algorithms such as [11-13] can also be used for exposing the stego images using LSBM and/or other stegano- graphic methods with a relatively high detection accuracy.Unlike LSB replacement and LSBM, It is also shown that such a new scheme can avoid the LSB replacement style asymmetry, and thus it should make the detection slightly more difficult than the LSBM approach based on our experiments.The typical LSB-based approaches, including LSB replace- ment, LSBM, and LSBMR, deal with each given pixel/pixel- pair without considering the difference between the pixel and its neighbors. Until now, several edge adaptive schemes such as [14–19] have been investigated. In, Hempstalk proposed a hiding scheme by replacing the LSB of a cover according to the difference values between a pixel and its four touching neighbors. Although this method can embed most secret data along sharper edges and can achieve more visually impercep- tible stegos (please refer to Fig. 1(g) and Table I), the security performance is poor. Since the method just modifies the LSB of image pixels when hiding data, it can be easily detected by existing steganalytic algorithms, such as the RS analysis (please refer to Section IV-C. Furthermore, the threshold θ is predetermined and thus it cannot change adap- tively according to the image contents and the message to be embedded. The pixel-value differencing (PVD)-based scheme. Usually, PVD-based approaches can provide a larger embedding capacity (on average, larger than 1 bpp). Based on our extensive experiments, however, we find that the existing PVD-based approaches cannot make full use of edge informa- tion for data hiding, and they are also poor at resisting some statistical analyses.One of the common characteristics of most the stegano- graphic methods mentioned above is that the pixel/pixel-pair selection is mainly determined by a PRNG while neglecting the relationship between the image content and the size of the secret message. By doing this, these methods can spread the secret data over the whole stego image randomly even at low embedding rate. However, based on our analysis and extensive experiments, we find that such embedding schemes do not perform well in terms of the security or visual quality of the stego images.

we should preferentially use those subimages with good hiding characteristics while leaving the others unchanged. Therefore, deciding how to select the regions is the key issue of our proposed scheme. Generally, the regions located at the sharper edges present more complicated statis- tical features and are highly dependent on the image contents. Moreover, it is more difficult to observe changes at the sharper edges than those in smooth regions.

In this paper, we propose an edge adaptive scheme and apply it to the LSBMR-based method. The experimental results evaluated on thousands of natural images using different kinds of steganalytic algorithms show the superiority of the new method. The rest of the paper is arranged as follows. Section II analyzes the limitations of the relevant steganographic schemes and proposes some strategies. Section III shows the details of data embedding and data extraction in our scheme. Section IV presents experimental results and discussions. Finally, concluding remarks and future work are given in Section V.

II. Analysis of Limitations of Relevant Approaches and Strategies

In this section, we first give a brief overview of the typical LSB-based approaches including LSB replacement, LSBM, and LSBMR, and some adaptive schemes including the original PVD scheme [17], the improved version of PVD (IPVD) [18], adaptive edges with LSB (AE-LSB) [19], and hiding behind corners (HBC) [14], and then show some image examples to expose the limitations of these existing schemes. Finally we propose some strategies to overcome these limitations.

~±In the LSB replacement and LSBM approaches, the embedding process is very similar. Given a secret bit stream to be embedded, a traveling order in the cover image is first generated by a PRNG, and then each pixel along the traveling order is dealt with separately. In such a way, the LSB of pixels along the traveling order will match the secret bit stream after data hiding both for LSB replacement and LSBM. There- fore, the extracting process is exactly the same for the two ap- proaches. It first generates the same traveling order according to a shared key, and then the hidden message can be extracted correctly by checking the parity bit of pixel values.

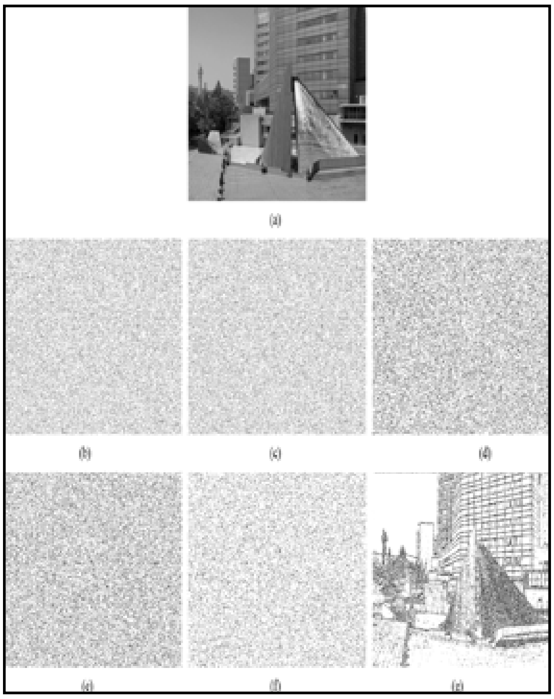

Fig. 1. (a) Cover Image. (b)–(g) Differences Between Cover and Stego Images Using the Six Steganographic Approaches with the Same Embedding Rate of 30%. The Black Pixels Denote that those Pixel Values in the Corresponding Positions have been Modified After Data Hiding. (a) Cover Image. (b) LSBM. (c) LSBMR. (d) PVD. (e) IPVD. (f) AE-LSB. (g) HBC.

Table 1:
Average PSNR, WPSNR, and the Modification Rate Over 6000 Stego Images With Different Steganographic Algorithms and Embedding Rates. The Numbers in Brackets Denote the Best Values in the Corresponding Cases

Embedding Rate	Steganographic Algorithms		Average PSNR	Average wPSNR	Avg. rate of Modification
10%	LSB-Based	LSBM	61.1	63.1	0.0500
		LSBMR	(62.2)	64.1	0.0375
	Edge-Based	PVD	51.5	56.3	0.0488
		IPVD	53.8	58.8	0.0490
		AE-LSB	52.0	56.1	(0.0277)
		HBC	61.1	(68.9)	0.0500
	Our Proposed		61.9	(68.9)	0.0386
30%	LSB-Based	LSBM	56.4	58.4	0.1500
		LSBMR	(57.4)	59.4	0.1125
	Edge-Based	PVD	46.8	51.5	0.1465
		IPVD	49.0	54.0	0.1471
		AE-LSB	47.2	51.3	(0.0831)
		HBC	56.4	(61.0)	0.1500
	Our Proposed		56.8	60.8	0.1187
50%	LSB-Based	LSBM	54.2	56.1	0.2500
		LSBMR	(55.2)	57.1	0.1875
	Edge-Based	PVD	44.5	49.3	0.2441
		IPVD	46.8	51.8	0.2452
		AE-LSB	45.0	49.1	(0.1384)
		HBC	54.2	(57.4)	0.2500
	Our Proposed		54.1	56.8	0.2022

where the function denotes the LSB of the pixel value and are the two secret bits to be embedded.

By using the relationship (odd–even combination) of adja- cent pixels, the modification rate of pixels in LSBMR would decrease compared with LSB replacement and LSBM at the same embedding rate. What is more, it does not introduce the LSB re- placement style asymmetry. Similarly, in data extraction, it first generates a traveling order by a PRNG with a shared key. And then for each embedding unit along the order, two bits can be extracted. The first secret bit is the LSB of the first pixel value, and the second bit can be obtained by calculating the relation- ship between the two pixels as shown above.

Our human vision is sensitive to slight changes in the smooth regions, while it can tolerate more severe changes in the edge regions. Several PVD-based methods such as [17–19] have been proposed to enhance the embedding capacity without in- troducing obvious visual artifacts into the stego images. The basic idea of PVD-based approaches is to first divide the cover image into many nonoverlapping units with two consecutive pixels and then deal with the embedding unit along a pseudo- random order which is also determined by a PRNG. The larger difference between the two pixels, the larger the number of secret bits that can be embedded into the unit. To a certain extent, existing PVD-based approaches are edge adaptive since more secret data is embedded in those busy regions.

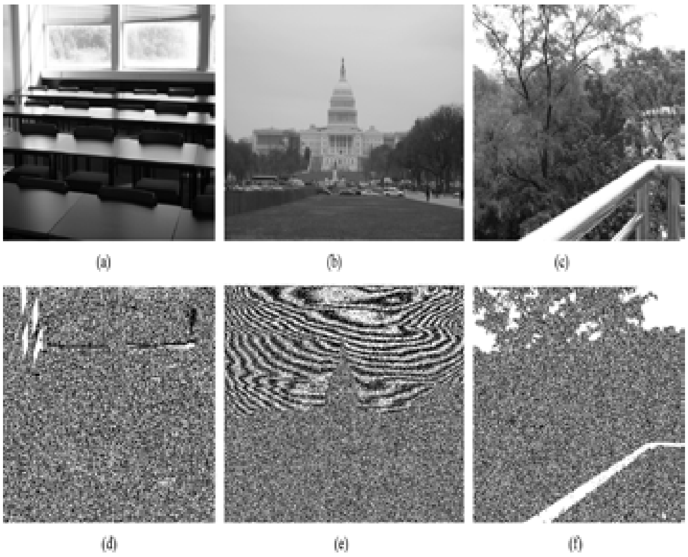

Fig. 2: LSB of Three Cover Images. It can be Observed that the LSB is not Completely Random. Some of the LSB Planes Would Even Present Texture Information Just Like those in the Higher Bit Planes (a) Example 1. (b) Example 2. (c) Example 3. (d) LSB of Example 1. (e) LSB of Example 2. (f) LSB of Example 3

However, sim- ilar to the LSBM and LSBMR approaches, pixel pair selection is mainly dependent on a PRNG, which means that the modified pixels will still be spread around the whole stego image as illustrated in fig. 1(b)–(f). It is observed that many smooth re- gions will be altered inevitably after data hiding even when the difference between two consecutive pixels is zero (meaning the subimages are located over flat regions), while many available sharp edge regions have not been fully exploited.

×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. Based on extensive experiments, we find that uncompressed natural images usually contain some flat regions (it may be as small as 5 5 and it is hard to notice), and the LSB in those regions have the same values (1 or 0). Therefore, if we embed the secret message into these regions, the LSB of stego images would become more and more random, which may lead to visual and statistical differ- ences between cover (contains flat regions/texture information) and stego images (appearing as a noise-like distribution) in the LSB plane as illustrated in fig. 3. Compared with smooth regions, the LSB of pixels located in edge regions usually present more random characteristics, and they are statistically similar to the distribution of the secret message bits (assuming a 1/0 uniform distribution). Therefore, it is expected that fewer detectable artifacts and visual artifacts would be left in the edge regions after data hiding. Furthermore, the edge information (such as the location and the statistical moments) is highly dependent on image content, which may make detection even more difficult. This is why our proposed scheme will first embed the secret bits into edge regions as far as possible while keeping other smooth regions as they are. As shown in fig. 1(g), we found that the HBC method [14] has this property. However, the HBC method just modifies the LSBs while keeping the most significant bits unchanged; thus it can be regarded as an edge adaptive case of LSB replacement, and the LSB replacement style asymmetry will also occur in their stegos. We will show some experimental evidence to expose the limitation of the HBC method in Section IV-C1. Please note that we do not evaluate the security of JPEG images in this paper. The reason is that all the nonoverlapping 88 blocks within JPEG images are arranged regularly due to lossy JPEG compression,namely the additional secret message would destroy the unique fin- gerprints introduced by the previous JPEG compression with a given quantization table. We can even potentially detect a hidden message as short as one bit from the JPEG stegos.

III. Proposed Scheme

The flow diagram of our proposed scheme is illustrated in fig. 4. In the data embedding stage, the scheme first initializes some parameters, which are used for subsequent data prepro- cessing and region selection, and then estimates the capacity of those selected regions. If the regions are large enough for hiding the given secret message , then data hiding is performed on the selected regions. Finally, it does some postprocessing to ob- tain the stego image. Otherwise the scheme nee

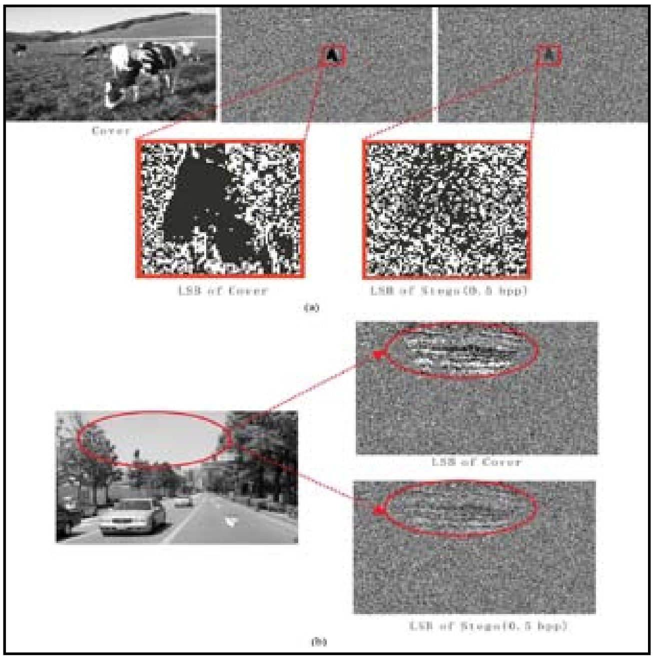

Fig. 3: LSB Before and After Random Contamination by LSBM (a) Randomization in the Small Flat Region (b) Randomization in the Large Texture Region

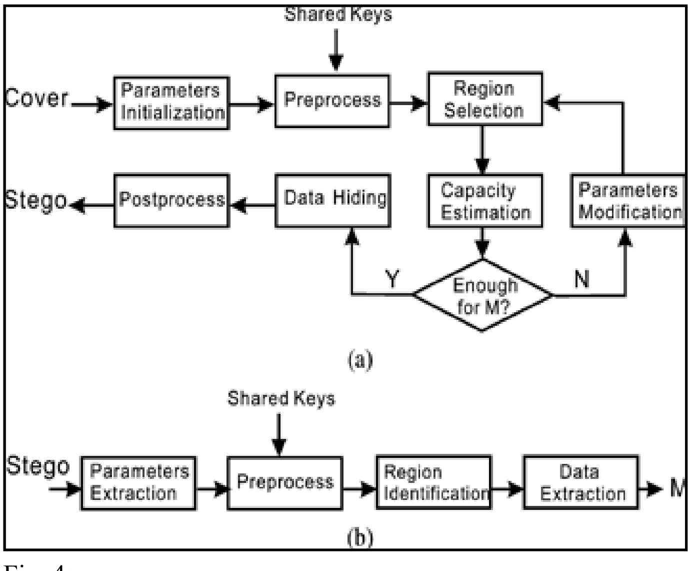

Fig. 4:

A. Data Embedding

$m{\times}nBz{\times}Bz$• Step 1: The cover image of size of is first divided into nonoverlapping blocks of pixels. For each small block, we rotate it by a random degree in the range of $\{0, 90, 180, 270\}$, as determined by a secret key

key_1. The resulting image is rearranged as a row vector $V(x_i, x_{i+1})i{=}_1n$by raster scanning. And then the vector is divided into nonoverlapping embedding units with every two consecutive pixels , where $1, 3, \ldots, mn$, assuming is an even number.

key_1Two benefits can be obtained by the random rotation. First, it can prevent the detector from getting the correct embedding units without the rotation key , and thus security is improved. Furthermore, both horizontal and vertical edges (pixel pairs) within the cover image can be used for data hiding.

$MTE^{U(t)}t$

- Step 2: According to the scheme of LSBMR, 2 secret bits can be embedded into each embedding unit. Therefore, for a given secret message , the threshold for region selection can be determined as follows. Let be the set of pixel pairs whose absolute differences are greater than or equal to a parameter

$\{0, 1, \ldots, 31\}$

$t{\in}|M||M$ | $E^{U(t)}|E^{U(t)}$where is the size of the secret message , and denotes the total number of elements in the set of .

$T{=}0$Please note that when , the proposed method becomes the conventional LSBMR scheme, which means that our method can achieve the same payload capacity as LSBMR (except for 7 bits).

- Step 3: Performing data hiding on the set of

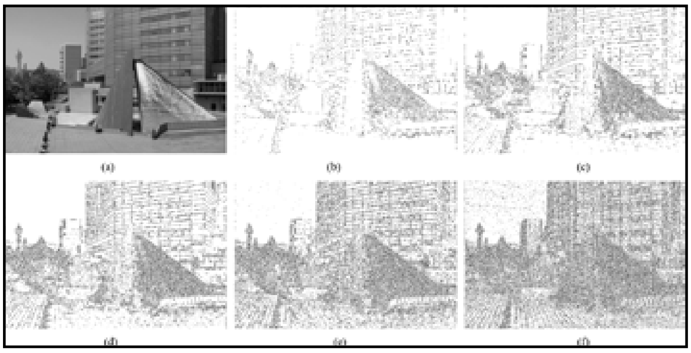

Fig. 5. (a) Cover image. (b)–(f) Positions of those modified pixels (black pixels) after data hiding using our proposed method with embedding rates of 10%, 20%, 30% , 40%, and 50%, respectively. It is observed that at lower embedding rates, e.g., 10%–40%, only sharper edges (such as the edge regions in the buildings etc.) within the cover image are used, while keeping those smooth regions (such as the smooth sky in the top left corner) as they are. When the embedding rate increases, more regions can be released adaptively by decreasing the threshold T . For instance, in the case of 50%, many embedding units in the sky are also used for data hiding. (a) Cover image. (b) 10%, T = 21. (c) 20%, T = 9. (d) 30%, T = 5. (e) 40%, T = 3. (f) 50%, T = 2.

B. Data Extraction

$BzTBz{\times}Bzkey_1$To extract data, we first extract the side information, i.e., the block size and the threshold from the stego image. We then do exactly the same things as Step 1 in data embedding. The stego image is divided into blocks and the blocks are then rotated by random degrees based on the secret key . The resulting image is rearranged as a row vector V'. Finally, we get the embedding units by dividing V' into nonoverlapping blocks with two consecutive pixels.

$Tkey_2(x'_i, x'_{i+1})x'_{i+1}_Tm_i, m_{i+1}$We travel the embedding units whose absolute differences are greater than or equal to the threshold according to a pseudorandom order based on the secret key , until all the hidden bits are extracted completely. For each qualified

embedding unit, say, , where $x'_i| \geq$, we extract the two secret bits as follows:

$$\mathrm{LSB}(x''_i), m_{i+1}{=}\mathrm{LSB}{+}\, x'_{i+1}\Big).m_i$$

$(x'_i, x'_{i+1})_T{=}19$For instance, we are dealing with the unit $(63, 83)$ with . We eventually get the secret bits by

$$\mathrm{LSB}(63)\_1\,m_{i+1}{=}\mathrm{LSB}{+}\ 83\Big){=}0.m_i$$

IV. Experimental Results and Analysis

In this section, we will present some experimental results to demonstrate the effectiveness of our proposed method compared 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

$TTE^{U(T)}T$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

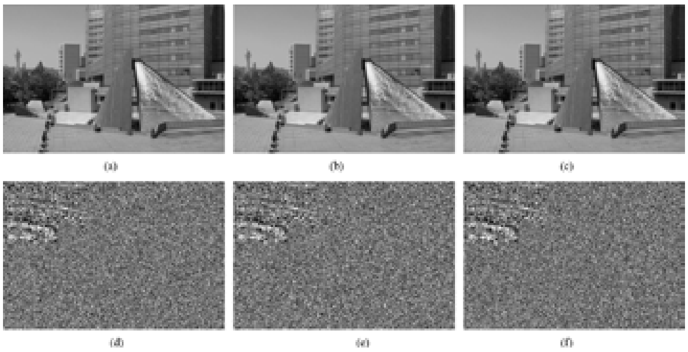

Fig. 6: LSB planes of the cover image and its stego images using our proposed method. It is observed that there are no obvious visual traces leaving along the embedded content edges [please refer to Fig. 5(d) and (f)] after data hiding. Furthermore, most texture information in smooth regions (upper-left corner) can be well preserved. (a) Cover image. (b) Stego with 30%. (c) Stego with 50%. (d) LSB of cover. (e) LSB of stego with 30%. (f) LSB of stego with 50%.

$\max(x)^2$[23]. It takes into account HVS characteristics and improves the classical PSNR by

$\mathrm{wPSNR}^{10\log_{10}=}$

–

$x$where is the cover image and x' is the stego image. NVF denotes the noise visibility function [24]) and the average modification rate over 6000 images with different embedding rates for the seven steganographic methods.

±For the average PSNR, it is observed that the LSBMR method performs best since it employs the 1 embedding scheme and its modification rate is lower than the others except for the AE-LSB method. Please note that the value of PSNR is independent of the location of the modified pixels. Thus the average PSNR of our proposed method will be slightly lower than that of LSBMR since some embedding units need to be readjusted to guarantee the correct data extraction (please refer to the Appendix for more details) in the proposed method.

For the average wPSNR, the performances of the HBC and our proposed methods are very similar and usually outperform the others. The reason is that the modified pixels using both methods always locate at the sharper edges within covers while preserving the smoother regions after data hiding [please refer to Figs. 1(g) and 5(b)–(f)]. According to the NVF in [24], the weighting for the changes in sharper regions is smaller than those in smoother regions, which means the values of wPSNR should become higher than those of stegos with the random em- bedding scheme.

For the average modification rate, the AE-LSB method is always the lowest. The reason is that according to the embedding procedure of AE-LSB, the average payload capacity for each single pixel is the largest among the schemes, which means that fewer pixels need to be modified at the same embedding ca- pacity. Please note that the average modification rates of LSBM

and HBC are the same and equal to one half of the embedding rate or 4/3 of the modification rate of LSBMR.

On the whole, the object qualities including PSNR and wPSNR of our stegos are nearly the best among the seven steganographic methods (please compare the underlined values and those values in brackets).

B. Visual Attack

Although our method embeds the secret message bits by changing those pixels along the edge regions, it would not leave any obvious visual artifacts in the LSB planes of the stegos based on our extensive experiments. Fig. 6 shows the LSB of the cover and its stegos using our proposed method with an embedding rate of 30% and 50%, respectively. It is observed that there is no visual trace like those shown in Fig. 5(d) and (f); also, most smooth regions such as the sky in the upper-left corner are well preserved. While for the LSBM, LSBMR, and some PVD-based methods with the random embedding scheme, the smooth regions would be inevitably disturbed and thus be- come more random. Fig. 7 shows the LSB planes of the cover and its stegos using the seven steganographic methods with the same embedding rate of 50%, respectively. It is observed that the LSB planes of stegos using the LSBM, LSBMR, PVD, and IPVD methods (especially for the LSBM due to its higher modification rate) look more random compared with others. On zooming in, these artifacts are more clearly observed, as illustrated in Fig. 3. Please note that the smooth regions can also be preserved for HBC, and less smooth regions will be contaminated for AE-LSB due to its lower modification rate as shown in Table I.

C. Statistical Attack

1) RS Analysis: RS steganalysis [3] is one of the famous methods for detecting stegos with LSB replacement and for es-

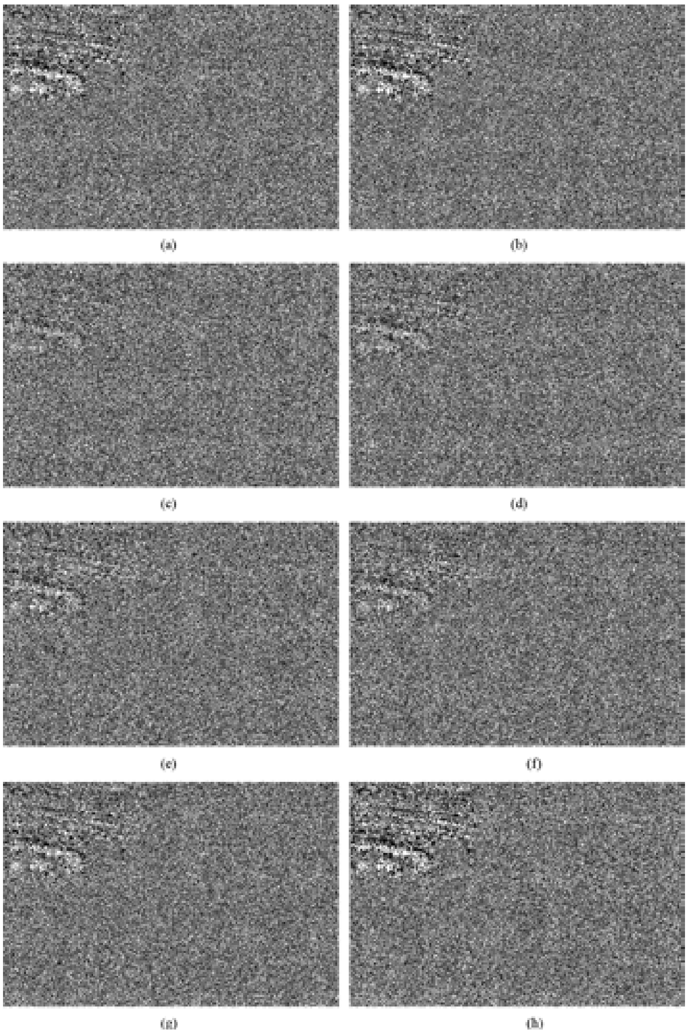

Fig. 7. LSB planes of cover [Fig. 6(a)] and stego images with the seven steganographic methods at the same embedding rate of

50%. (a) LSB of cover. (b) LSB of our stego. (c) LSB of LSBM stego. (d) LSB of LSBMR stego. (e) LSB of PVD stego. (f) LSB of IPVD stego. (g) LSB of stego with AE-LSB. (h) LSB of stego with HBC.

timating the size of the hidden message. In this test, we employ this steganalysis to evaluate the security of our proposed method and HBC method.

Since the HBC can be regarded as a special case (edge adap- tive) of LSB replacement, the structural asymmetry artifacts introduced by LSB replacement can be reflected in the corresponding RS diagram. As shown in Fig. 8(a), the difference between $R_M(S_M)$ and $R_{-M}(S_{-M})$ will become larger with in- creasing the embedding rates. While our proposed method is actually an LSBM-based scheme, these LSB replacement style artifacts will be easily avoided and thus the RS steganalysis is ineffective at detecting our stegos. As shown in Fig. 8(b), the difference between $R_M(S_M)$ and $R_{-M}(S_{-M})$ remains close even with an embedding rate of 100%.

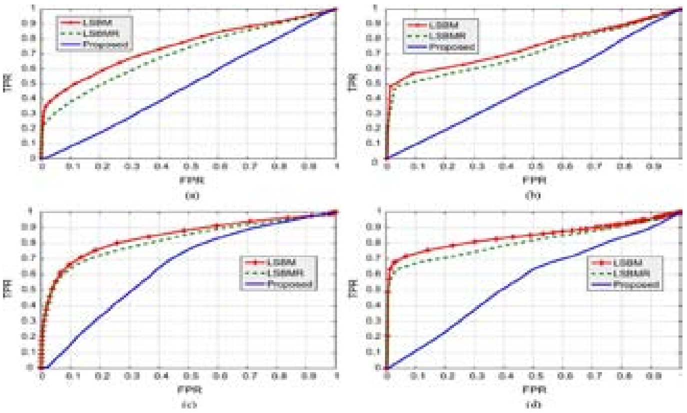

Fig. 9: ROC Curves for Three LSBM-based Steganographic Methods with Two Specific Steganalytic Algorithms. The x-Coordinate and y-Coordinate Denote the FPR (False Positive Rate) and TPR (True Positive Rate), Respectively. (a) 50% using Li-1D [10]. (b) 50% using Huang-1D [9]. (c) 75% using Li-1D [10]. (d) 75% using Huang-1D [9].

Li-110D [12]. Steganalytic features are extracted from the normalized histogram of the local linear transform coeffi- cients [27] of the image. The experimental results in [12] show that these features can capture certain changes of the local textures before and after data embedding, and thus can detect the presence of a hidden message, espe- cially for some adaptive steganographic algorithms, such as MBNS [28], MPB [29], and JPEG2000 BPCS [30], ef- fectively even with low embedding rates, for instance 10% (110 Dimension).

In the experiments, we first create the stego images using the seven steganographic methods with different embedding rates ranging from 10% to 50% with a step of 10%. And then extract those image features as mentioned above both for the cover and stego images. The FLD classifier is also used for the classifica- tion. Table III shows the detection accuracy which is averaged over the results of a ten-fold cross-validation just as it did in Section IV-C1. From Table III, it can be observed that our pro- posed method outperforms the other six relevant methods nearly for all the situations, especially for the stegos with lower embed- ding rates, e.g., less than 30%.

For example, when the embedding rate is 20%, our maximum accuracy is 59.29%, that is around 20% improvement on the typical LSB-based methods including LSBM and LSBMR. When the embedding rate increases, say 50%, our results will get closer to the performance of the LSBMR method. The reason is that the sharper edge regions within cover images are not numerous enough for hiding a secret message of such a large size; the method has to decrease the threshold to release more smooth/flat regions. For instance, the embedding units whose absolute differences are larger than or equal to 2 of the image as shown in Fig. 5(f) have been used for data hiding, which would lead to poor security based on our extensive experiments. Please note that unlike the digital watermarking or fingerprinting hiding techniques, the steganographer has the freedom to select the cover image and/ or steganography to carry the message [20]. In practice, we can select those cover images with good hiding characteristics, namely the covers with more edge regions using our proposed scheme. Therefore, for a given secret message, the threshold can be used as a blind criterion for cover image selection. Usually the larger the threshold , the larger the number of sharp edges within the selected cover, and thus the higher the security achieved.

*TTT*Based on experiments, we also observe that the performances of the first three edge-based schemes, i.e., PVD, IPVD, and AE-LSB, are poorer than the LSB-based approaches. For the HBC method, its performance is similar to our method although it can be easily detected by the RS analysis (please refer to Table II), which indicates that it is more difficult to detect those pixel changes that along the edges regions using the four uni- versal feature sets.

Table 3: Average Accuracy (%) Of Each Feature Set On Fld With Different Embedding Rates. Values With An Asterisk (*) Denote The Minimum Accuracy Among the Seven Steganographic Algorithms

Embedding Rate	Steganographic Algorithms		Shi 78-D	Farid 72-D	Moulin 156-D	Li 110-D	Max. Accuracy
10%	LSB-Based	LSBM	69.39	55.04	57.61	74.11	74.11
		LSBMR	68.01	56.83	57.51	72.90	72.90
	Edge-Based	PVD	83.96	77.68	86.21	84.93	86.21
		IPVD	75.58	68.86	75.97	80.42	80.42
		AE-LSB	80.90	68.17	77.91	82.18	82.18
		HBC	54.31	50.68	**51.23 ***	54.61	54.61
	Our Proposed		**52.56 ***	**50.56 ***	51.39	**52.94 ***	**52.94 ***
20%	LSB-Based	LSBM	77.05	59.29	65.22	79.21	79.21
		LSBMR	75.30	60.68	63.61	78.01	78.01
	Edge-Based	PVD	91.15	85.68	90.95	88.15	91.15
		IPVD	84.54	75.27	83.74	84.85	84.85
		AE-LSB	88.19	74.25	86.46	87.86	88.19
		HBC	62.15	52.25	53.74	59.24	62.15
	Our Proposed		**59.29 ***	**51.84 ***	**53.26 ***	**56.59 ***	**59.29 ***
30%	LSB-Based	LSBM	80.92	63.14	69.91	82.05	82.05
		LSBMR	79.78	63.50	67.72	81.01	81.01
	Edge-Based	PVD	94.31	89.58	92.85	89.86	94.31
		IPVD	88.29	78.41	86.89	86.96	88.29
		AE-LSB	90.62	77.12	89.75	89.36	90.62
		HBC	70.80	55.44	57.72	65.92	70.80
	Our Proposed		**67.48 ***	**54.59 ***	**57.49 ***	**63.16 ***	**67.48 ***
40%	LSB-Based	LSBM	83.90	66.05	73.40	83.86	83.90
		LSBMR	83.09	65.90	71.40	83.30	83.30
	Edge-Based	PVD	95.84	91.87	94.15	90.78	95.84
		IPVD	90.47	80.41	88.61	88.61	90.47
		AE-LSB	91.88	79.10	91.36	89.97	91.88
		HBC	78.48	60.10	**62.45 ***	73.58	78.48
	Our Proposed		**76.62 ***	**58.96 ***	63.80	**71.01 ***	**76.62 ***
50%	LSB-Based	LSBM	86.08	68.20	77.23	85.13	86.08
		LSBMR	85.13	67.70	75.29	84.46	85.13
	Edge-Based	PVD	96.80	93.13	94.99	91.79	96.80
		IPVD	91.97	82.16	89.42	89.59	91.97
		AE-LSB	92.98	80.50	92.29	90.49	92.98
		HBC	84.00	64.26	**68.95 ***	79.92	84.00
	Our Proposed		**83.24 ***	**63.99 ***	69.63	**77.05 ***	**83.24 ***

V. Concluding Remarks

If embedding a message in these regions, the LSB of stego images becomes more random, and according to our analysis and extensive experiments, it is easier to detect. In this paper, an edge adaptive image steganographic scheme in the spatial LSB domain is studied. As pointed out in Section II, there usually exists some smooth regions in natural images, which would cause the LSB of cover images not to be completely random or even to contain some texture information just like those in higher bit planes. In most previous steganographic schemes, however, the pixel/pixel-pair selection is mainly determined by a PRNG without considering the relationship between the char- acteristics 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 images using different kinds of steganalytic algorithms show that both

$$f(a,b) = f(a, b+2k_2)$$

$$f(a,b) = f(a+4k_1, b), \forall b, k_1, k_2 \in Z. \quad (2)$$

visual quality and security of our stego images are improved significantly compared to typical LSB-based approaches and their edge adaptive versions.

Furthermore, it is expected that our adaptive idea can be extended 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.

APPENDIX

$+1)$

$\{0, 1, 2, \ldots, 31\}$

$(x_i, x_i T (x_i'', x_i''$ $_{+1})(*) d = \_ x_{i+1} | T$ In the Appendix, we prove that for every embedding unit in the cover image, where $|x_i$ $\geq$,

$\in$, our proposed algorithm can modify it as

$\mathrm{LSB}(x_i'') | x_i'' x_i'' m_i, f(x_i'', x_i''{}_{+1})_{+1} | T ==$ a new pair with the least distortion according to for- mula , under conditions that

$m_{i+1} 0 x_i'', x_i''{}_{+1} 255 \_ T$, and $\leq$ $\leq$, $\geq$. This is very important in order to guarantee that we can distinguish the same selected regions before and after data embedding with the same threshold .

$= \mathrm{LSB}(\lfloor a/2 \rfloor$ Proof: First, we show some important properties of the bi- nary function $f(a,b)$ $+ b)$ as follows:

$$f(a,b) \neq f(a, b \pm 1), f(a-1, b) \neq f(a+1, b), \in Z. \forall a, b \quad (1)$$

Then we have

$$f(a,b) \_ f(a, b + 2k_2) \in Z. (2)$$

Since , then d $\leq$ $|R_l| + d + |R_r| \max(T) 31 = 256 = 256 - |R_l| - |R_r| |R_r| 25631 R_l = T = | R_l | + \_ = 225.$, then we have $\geq$ $|R_l| 64 |R_r| 2 |R_l| + |R_r| < 4 + 2 =$ Therefore, there must exist a region or R_r which satisfies $\geq$ or $\geq$. Otherwise, we have , get contradiction.

$f(a,b) \_ f(a + 4k_1, b), \forall b, k_1, k_2$ We formulate the four cases as described in Section III-A Step 3 as follows:

- If $\geq$, then we let $\leq$

$|R_r| 255 (k_1 T 12 = x_i'' \; d'' x_i', x_i'' d' + \overset{+1}{2} == x_i' T + \_ \overset{+1}{1} + 2 == 1) = 2 = \geq T.$ $0, k_2$, then

$+$

$= x_i + r_1, x_{i+1}' = x_{i+1} + r_2 |R_l| 0, x_i'' T \_ \overset{+1}{1} + 4 |R_r| x_{i+1}' (k_1 T + < 2 = \overset{x_i''}{d''}$

x_i'
$= d' + 4 x_i'$ •

If $\geq$ & , then we let $\geq$ $=== 0) 4 = -1, k_2$, then $r_1, r_2 \in \{0, -1, +1\}, +1$.where $|r_1|$ $|r_2| \leq$

(x_i', x_{i+1}') Based on the embedding process and the formula (1), it is easy to verify that the modified pixel pair satisfies

$+1)$

$\mathrm{LSB}(x_i') \_ m_i, f(x_i', x_{i+1}') \_ m_{i+1} (x_i', x_i' | x_i' x_{i+1}' | < = (3)$ If $\mathrm{\dot{s}}$ out of range $[0, 255]$, or the new difference d' $\_ T$, then we need to readjust them as follows. To preserve the property (3), we limit

$= x_i' + 4k_1, x_i''{}_{+1} = x_{i+1}' + 2k_2, \forall k_1, k_2 \in Z. x_i''$

$\mathrm{LSB}(x_i'') \_ m_i, f(x_i'', x_i''{}_{+1}) \_ m_{i+1}$. Based on formula (2), we have:

In the following, we are going to show that there always exists $\in Z k_1, k_2$, s.t.

$\leq x_i'', x_i''{}_{+1} \leq 255 | x_i'' \_ x_i''{}_{+1} | \geq T. 0$

$0 x_i < x_{i+1}$ Without loss of generality, assume that $\leq$ $\leq$

$255 (x_i', x_{i+1}')$. Then we need to readjust in the following two cases.

x_{i+1}' Case #1. x_i' or is out of range $[0, 255]$, then only one of the following two subcases would happen.

$x_i === 0.$ • Case #1.1. $0, r_1$ $-1, r_2$

$= x_i \_ 1 = 0 \_ 1 = -1, x_i''{}_{+1} = x_{i+1}). (x_i'$

$= | x_{i+1}' \_ = x_{i+1} \_ \_ = d + 1$ Then d' $x_i' |$ $(x_i$ $1)$ $\geq$ $+1. T$

$34 x_i' + 4 = 0 = \overset{+1}{3}, x_i''{}_{+1} d'' = d' = d + + d x_i' \overset{\leq}{1}^{+1} \geq 34 = \overset{x_i''}{38} (k_1$ — If $d \leq$, then , we let

$x_i' 1, k_2 = -1 = + 4 \leq = + 4$
$2)$
$= 34 T.$, then

$d > x_i' == \overset{+1}{3}, x_i''{}_{+1} x_i'' \lfloor = | x_i''{}_{+1} max(T) \geq T. 255, r_1 = 0, r_2 0 + d > 34 =$ —

If , then , we let x_i''

$x_i' + 4 = -1 + 4 = x_{i+1}' (k_1 (x_i \_ = 0) 4) = = \_ x_{i+1} \_ \_ 1 + 1, k_2$, then d'' $\_ 3 > 31 = d$

x_{i+1}==• Case #1.2. $+1$.

$=x_i, x'_{i+1}=x_{i+1}+1=255+1=256).(x'_i$

The analysis is similar to Case #1.1.

$d=T, d' x'_i=|x'_i x'_i{}^{+1} +1\_=d\_1=T\_1<T. R_l=[0, x'_i).R_r=(x'_{i+1}, 255]$.

Case #2. $x'_i|$ In such a case, both and must be in the region of $[0, 255]$. We let $\geq$.
$4=3T$

VI. Acknowledgment

The authors would like to thank Prof. Yun Q. Shi at New Jersey Institute of Technology, New Jersey, USA, for providing us the test images, thank Dr. Xiaolong Li at Peking University, Beijing, China, for providing us the source code in [10] and thank the anonymous reviewers for their valuable comments.

References

[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, 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, 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 funsion of maximum likelihood and structural steganalysis", in Proc. 9th Int. Workshop on Information Hiding, 2007, Vol. 4567, pp. 204–219.

[7] J. Harmsen, W. Pearlman,"Steganalysis of additive-noise mode- lable 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, 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, 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. Shi et 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, Y. Q. Shi,"Textural features based universal steganalysis", Proc. SPIE on Security, Forensics, Steganography and Watermarking of Multimedia, Vol. 6819, pp. 681912, 2008.

[13] M. Goljan, J. Fridrich, 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. Hempstalk,"Hiding behind corners: Using edges in images for better steganography", in Proc. Computing Women's Congress, Hamilton, New Zealand, 2006.

P. Rajya lakshmi received M.sc degree in the year of 2007 from OSMANIA UNIVERSITY and her M.Tech (CSE) from JNT University, Hyderabad in 2010-12. At Present working as Assistant Professor in CSE department at sree kavitha engineering college karepally skhammam (D), Andhra Pradesh, India.

R. Ravi Kumar received his MCA degree in the year of 2001 from KAKATIYA UNIVERSITY CAMPUS, Warangal and his M.Tech(CSE) from JNT University, Hyderabad in 2008-10. He worked as In-Charge HOD at Kakatiya University Post-Graduate College, Khammam. At Present working as Assistant Professor in CSE department at Swarna Bharati Institute of Science and Technology, Khammam, Andhra Pradesh. His research interest includes Network Security, Data Mining and Parallel Algorithms.