A Secure and Lossless Adaptive Image Steganography with Mod-4 LSB Replacement Methods Using Image Contrast

N.Santoshi, B.Lokeswara Rao, B.Lokeswara Rao

Abstract: An adaptive Steganography scheme is proposed in this paper. The adaptive quantization embedded is introduced and employed by block-wised fashion. We also constructed contrast-correlation distortion metric to optimally choose quantization steps for image blocks to guarantee more data being embedded in busy areas. Deferent form existing methods, our scheme embeds the AQE parameters together with message bits into the cover image by deference expanding algorithm. Simulation experiments show the proposed scheme can provide a good trade-o® between the perceptibility and the capacity.

Keywords: Steganography, Adaptive quantization embedded, Construct-correlation distortion, Deference expanding

1 INTRODUCTION

1.1 Steganography

Steganography means to hide secret information into innocent data. Digital images are ideal for hiding secret information. An image containing a secret message is called a cover image. First, the difference of the cover image and the stego image should be visually unnoticeable. The embedding itself should

draw no extra attention to the stego image so that no hackers would try to extract the hidden message illegally. Second, the message hiding method should be reliable. It is impossible for someone to extract the hidden message if she/he does not have a special extracting method and a proper secret key. Third, the maximum length of the secret message that can be hidden should be as long as possible.

“Steganography is the art of hiding information in ways that prevent the detection of hidden messages,”

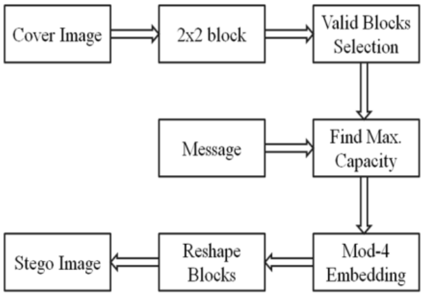
Imperceptibility and capacity are the two important properties of any Steganography schemes, the former ensures that the embedding is imperceptible (can not be detected by human eyes), and the latter indicates the efficiency of covert communication. There have been lots of techniques proposed to balance the trade-o® between them. Wang et al. [6] developed a technique to hide secret data by LSB substitution and a genetic algorithm (GA). Chang et.al. [1] used dynamic programming strategy to replace GA in [6]. In [2], Chan et. al. proposed a simple LSB substitution with an optimal pixel adjustment process(OPAP). These techniques can all be concluded as LSB-like methods, which realized optimal data embedding in meanings of mean square error(MSE). It is known for us that MSE is not a good metric for measuring the image degradation caused by information hiding, so the above methods cannot provide famous performance. Therefore lots of en devours have been made for performance improvements. Wu [4] proposed a Steganography method for images by pixel-value differencing, which divided the image into two-pixels block, and embed ded information into the deference value of each two pixels. BPCS [5]divided the image into regions and performed complexity measurement using a binary complexity measure on the individual bit planes to embed data in these regions. In [8], Zhangn proposed to convert data into a series of symbols in a notation system with multiple bases, and the speci¯c bases were obtained by the degree of local variations of the neighboring pixels in the stego image. In [3], Yang and Lin proposed a base-oriented hiding algorithm, which classed each block of the host image according to the base value, and make data embedding according some pre determinative parameters. After reviewing them, we can ¯nd it without hard that different from LSB-like methods, they all adopt the adaption mechanism(i.e. different quantization steps for different pixels). Despite that the adaption mechanism can achieve good per formance in experimental meanings, there is not a proper framework to tell us why those chosen quantization steps are suitable and how to obtain them. In this paper, we propose a new Steganography method to hide data in gray images via adaptive quantization-embedded(AQE). In the scheme, we construct a new distortion metric called contrast- correlation distortion, the message bits are embed ded into image blocks via an optimally searched quantization step under a given distortion con strain. The remainder of the paper is organized as following. Section 2 introduces the principles of adaptive quantization-embedded. Section 3 discusses the new construct distortion metric. Section 4 discuss the application of reversible data hiding algorithm in our scheme. Section 5 details the im plementation of the whole algorithm. Section 6 gives the simulation experiments. Section 7 con cludes the whole paper.

1.2 Existing Techniques Introduction to LSB

Maintaining the secrecy of digital information when being communicated over the Internet is presently a challenge.

Given the amount of cheap computation power available and certain known limitations of the encryption methods it is not too difficult to launch attacks on cipher-text. An ideal Steganography technique embeds message information into a carrier image with virtually imperceptible modification of the image. Adaptive Steganography comes closer to this ideal since it exploits the natural variations in the pixel intensities of a cover image to hide the secret message. The objective of steganography is a method of embedding an additional information into the digital contents, that is undetectable to listeners. We are investigating its embedding, detecting, and coding techniques. The idea behind the LSB algorithm is to insert the bits of the hidden message into the least significant bits of the pixels. As the application domain of embedding data in digital multimedia sources becomes broaden, several terms are used by various groups of researchers, including steganography, digital watermarking, and data hiding. 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 detailed algorithm is presented along with results of its application on some sample images.

BlockDiagram



2 PROPOSED ADAPTIVE STEGANOGRAPHY

Cover data, steganography key and the embedding function are basic components of steganographic algorithms. In order to achieve an adaptive steganographic algorithm, the following features of the embedding function are considered

- Pixel selection
- Message bits representation\
- . Cover modification

Franz and Schneidewind proposed an algorithm called Condith which selects the pixels for embedding based on their characteristics [1]. The algorithm calculates the difference between a pixel and its neighbors. If the difference exceeds a minimum threshold then pixel can be used to embed a message bit.

To select the areas with greater diversity of grayscale levels, Dulce *et al*. analyze the grayscale space distribution of regions and proposed the ConText algorithm [2]. In our method, we employ an adaptive mechanism in both pixel selection and message bits representation. We use 4 pixels to represent two bit of the message.

2.1 Adaptive Steganography Using Filtering

Adaptive Steganography reduces modifications to the image, and adapts the message embedding technique to the actual content and features of the image. In general, to keep a good degree of stealth ness, Adaptive methods embed message bits into certain random clusters of pixels (avoiding areas of uniform color) selecting pixels with large local standard deviation or image blocks containing a number of different colors. The main advantage of adaptive steganography is that the changes made to the cover image take into account the sensitivity of the human visual system and also various statistical parameters generally being used by steg-analysis algorithms. The main challenge posed to existing adaptive steganography techniques [3,4,5,6] is that the methods so far developed doesn't seem to have a way to control the amount of information that is to be hidden, for a given cover image. This problem is overcome in the method presented in this paper.

The proposed approach utilizes the sensitivity of the human visual system to adaptively modify the intensities of some pixels in a high frequency components spatial image (HFSI) of the cover image. The modification of pixel intensities depends on the magnitude of the pixels in HFSI and also on the local features of the cover image. If the contrast of the image is large (e.g., an edge), the intensities can be changed greatly without introducing any distortion to human eyes. On the other hand, if the contrast is small (e.g., a smooth), the intensities can only be tuned slightly. In this method, first the cover image is passed through a filter to separate the high and low frequency components of the image. The inverse transform of both the images is computed. Now the pixels values of HFSI are modified depending on the magnitude of the pixel i.e. more the magnitude more the Least Significant Bits (LSB's) of that pixel are changed and also the local features of cover image are considered. Now both the LFSI (Low Frequency components spatial image of cover image) and HFSI are added to form the stego - image. At the receiver the reverse process is to be done to recover the message.

The payload is embedded into the cover image by segmentation, DCT and coherent bit length *L* is shown in the Figure1.
Fig.1 Block Diagram of BSLDCT Embedding Technique
Cover Image:
The cover image is color or gray scale of any size and format. If the cover image is color then convert into grayscale image and corresponding pixel intensity values.
Pixel Management:
The gray scale cover image pixel intensity vary from *zero* to *255*. During the payload embedding process the intensity values of cover image may exceed lower and higher level limits which results in difficulty to retrieve the payload at the destination. Hence the cover image pixel intensity values are limited to lower *15* and upper *240* instead of *zero* and *255*.
Segmentation:
The cover image is segmented into 8x8 matrices. The DCT is applied on each 8x8 block to get DCT coefficients which are used to hide the payload Most Significant Bit (MSB) based on the DCT coefficient values of the cover image
2D-DCT:
Transform each 8x8 matrix into frequency domain using 2D-DCT. Using DCT on 8*8 sub blocks has an advantage of less computation time for embedding as well as security to payload increases compared to applying DCT to

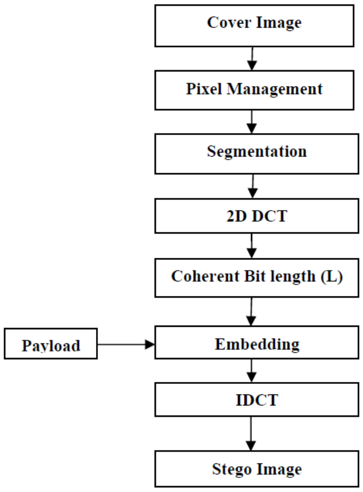


Fig.1 Block Diagram of BSLDCT Embedding Technique

2.2 Least Significant Bit Insertion

Usually 24-bit or 8-bit files are used to store digital images. The former one provides more space for information hiding; however, it can be quite large. The colored representations of the pixels are derived from three primary colors: red, green and blue. 24-bit images use 3 bytes for each pixel, where each primary color is represented by 1 byte. Using 24-bit images each pixel can represent 16,777,216 color values. We can use the lower two bits of these color channels to hide data, then the maximum color change in a pixel could be of 64-color values, but this causes so little change that is undetectable for the human vision system. This simple method is known as *Least Significant Bit insertion.* Using this method it is possible to embed a significant amount of information with no visible degradation of the cover image..

Several versions of LSB insertion exist. It is possible to use a random number generator initialized with a stego-key and its output is combined with the input data, and this is embedded to a cover image. For example in the presence of an active warden it is not enough to embed a message in a known place (or in a known sequence of bits) because the warden is able to modify these bits, even if he can't decide whether there is a secret message or not, o r he can't read it because it is encrypted. The usage of a stego-key is important, because the security of a protection system should not be based on the secrecy of the algorithm itself, i nstead of the choice of a secret key. *Fig.* 3 shows this process. The LSB inserting usually operates on bitmap images. 'Steganos for Win dows' and 'Wbstego' are LSB inserting software products which are able to embed data (in clear or encrypted format) in a bitmap image. The embedded data cannot be considered as a watermark, because even if a small change occurs in a picture (cropping, lossy compression and color degradation) the embedded information will be lost – although the change which is occurred during the embedding process is invisible.

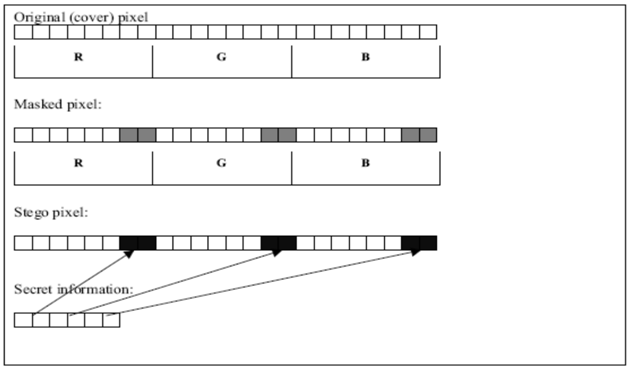


Fig. 2.

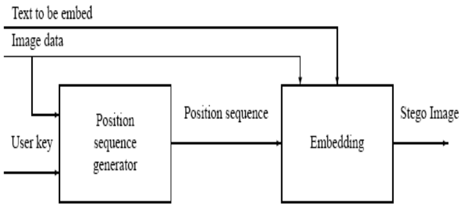


Fig. 3.

3 ALGORITHM

Step 1: Let the cover image is represented by c(x,y).

It is then passed through a filter with transfer function h(x,y) to separate high and low frequency components.

$F[c(x, y)] = C(X, Y)$

Where C(X, Y) represents Fourier Transform of the cover image. In this paper capital letters representation for pixel is used for frequency domain and small letters for spatial representation.

$C(X, Y)H(X, Y) = LO(X, Y) + HI(X, Y)$

Where LO(X, Y), HI(X, Y) represent low frequency and high frequency components of cover image respectively, obtained after passing through the filter with cut off as stated above.

Step 2: Inverse transform of both the frequency

Components is found out, known as HFSI (High Frequency components Spatial Image) and LFSI (Low Frequency Components Spatial Image) separately.

$F1[LO(X, Y)]= lo(x, y)$ and

$F-1\ [HI(X, Y)] = hi(x, y)$

Where lo(xy) and hi(x,y) are the spatial components of low and high frequencies in the cover image respectively.

Step 3: Now message is embedded into HFSI image.

The number of bits modified in a pixel is made to depend up on its magnitude and also on the local features of the cover image. Let the message is represented as m(x,y) and the embedding function as M[].

$mlo(x, y) = M[lo(x, y) + m(x, y)]$

Step 4: Both the modified HFSI and unmodified LFSI are added to form stego - image.

$Steg(x, y) = mlo(x, y) + lo(x, y)$

Step5: At the receiver LFSI is subtracted from stego image leaving modified HFSI image.

$mhi(x, y) = steg(x, y) - hi(x, y)$

Step 6: Now the message is decoded from the Modified HTSI image using the stego - key

$m(x, y) + lo(x, y) = M\ '[mhi(x, y)]$

4 Spatial domain reversible steganography :

This type of reversible steganography directly modifies image pixels in the spatial domain to achieve reversibility. Since this technique is easy to implement, offer a relatively high hiding capacity, and the quality of the cover image can be easily controlled, it has become a popular method for reversible steganography.

Introduction:

REVERSIBLE data embedding, which is also called lossless data embedding, embeds invisible data (which is called a payload) into a digital image in a reversible fashion. As a basic requirement, the quality degradation on the image after data embedding should be low. An intriguing feature of reversible data embedding is the reversibility, that is, one can remove the embedded data to restore the original image. From the information hiding point of view, reversible data embedding hides some information in a digital image in such a way that an authorized party could decode the hidden information and also restore the image to its original, pristine state. The performance of a reversible data-embedding algorithm can be measured by the following.

1) *Payload capacity limit:* what is the maximal amount of information can be embedded?

2) *Visual quality:* how is the visual quality on the embedded image?

3) *Complexity:* what is the algorithm complexity?

The motivation of reversible data embedding is distortion-free data embedding . Though imperceptible, embedding some data will inevitably change the original content. Even a very slight change in pixel values may not be desirable, especially in sensitive imagery, such as military data and medical data. In such a scenario, every bit of information is important. Any change will affect the intelligence of the image, and the access to the original, raw data is always required. From the application point of view, reversible data embedding can be used as an information carrier. Since the difference between the embedded image and original image is almost imperceptible from human eyes, reversible data embedding could be thought as a covert communication channel. By embedding its message authentication code, reversible data embedding provides a true self authentication scheme, without the use of metadata.

In this paper, we present a high-capacity, high visual quality, reversible data-embedding method for digital images. Our method can be applied to digital audio and video as well. We calculate the differences of neighboring pixel values, and select some difference values for the difference expansion (DE). The original content restoration information, a message authentication code, and additional data (which could be any data, such as date/time information, auxiliary data, etc.) will all be embedded into the difference values. In this paper we will consider grayscale images only. For color images, there are several options. One can decorrelate the dependence among different color components by a reversible color conversion transform, and then reversibly embed the data in the decorrelated components. Or one can reversibly embed each color component individually. Please note that reversible data embedding is a fragile technique When the embedded image is manipulated and/or lossy compressed, the decoder will find out it is not authentic and thus there will be no original content restoration.

4.1 Reversible Data Hiding

DATA HIDING is referred to as a process to hide data (representing some information) into cover media. That is, the data hiding process links two sets of data, a set of the embedded data and another set of the cover media data. The relationship between these two sets of data characterizes different applications. For instance, in covert communications, the hidden data may often be irrelevant to the cover media. In authentication, however, the embedded data are closely related to the cover media. In these two types of applications, invisibility of hidden data is an important requirement. In most cases of data hiding, the cover media will experience some distortion due to data hiding and cannot be inverted back to the original media. That is, some permanent distortion has occurred to the cover media even after the hidden data have been extracted out. In some applications, such as medical diagnosis and law enforcement, it is critical to reverse the marked media back to the original cover media after the hidden data are retrieved for some legal considerations. In other applications, such as remote sensing and high-energy particle physical experimental investigation, it is also desired that the original cover media can be recovered because of the required high-precision nature. The marking techniques satisfying this requirement are referred to as *reversible*, *lossless*, *distortion-free*, or *invertible* data hiding techniques. Reversible data hiding facilitates immense possibility of applications to link two sets of data in such a way that the cover media can be loss Lesley recovered after the hidden data have been extracted out, thus providing an additional avenue of handling two different sets of data.

Obviously, most of the existing data hiding techniques are not reversible. For instance, the widely utilized spread-spectrum based data hiding methods are not invertible owing to truncation (for the purpose to prevent over/underflow) error and round-off error. The well-known least significant bit plane (LSB) based schemes and are not lossless owing to bit replacement without “memory.” Another category of data hiding techniques, quantization-index-modulation (QIM) based schemes and , are not distortion-free owing to quantization error. Recently, some reversible marking techniques have been reported in the literature. The first method is carried out in the spatial domain. It uses modulo 256 addition (assuming here that eight-bit grayscale images are considered) to embed the hash value of the original image for authentication. The embedding formula is $Iw = (I + W) \bmod (256)$, in which I denotes the original image, Iw the marked image, and $W = W(H(I), K)$ the watermark, where $H(I)$ denotes the hash function operated on the original image I, and K the secret key. Because of using modulo 256 addition, the over/underflow is prevented and the reversibility is achieved. Some annoying salt-and-pepper noise, however, is generated owing to possible grayscale value flipping over between 0 and 255 in either direction during the modulo 256 addition. The second reversible marking technique was developed in the transform domain, which is based on a lossless multire solution transform and the idea of patchwork. It also uses modulo 256 addition. Note that no experimental results about this technique have been reported. Another spatial domain technique was reported in that losslessly compresses some selected bit plane(s) to leave space for data embedding. Because the necessary bookkeeping data are also embedded in the cover media as an overhead, the method is reversible. Since these techniques aim at authentication, the amount of hidden data is limited. The capacity of method, which is based on the idea of patchwork and modulo 256 addition, is also limited except that the hidden data exhibit some robustness against high quality JPEG compression. Since it uses modulo 256 addition, it also suffers from salt-and-pepper noise. As a result, the technique cannot be utilized in many applications. This observation is valid to all lossless data hiding algorithms that use modulo 256 addition to achieve reversibility. The first reversible marking technique that is suitable for a large amount of data hiding was presented. This technique first segments an image into non overlapping blocks, and then introduces a discriminating function to classify these blocks into three groups: R(regular), S(singular), and U(unusable). It further introduces a flipping operation, which can convert an R-block to an S-block and vice versa. A U-block remains intact after the flipping operation. By assigning, say, binary 1 to an R-block and binary 0 to an S-block, all R- and S-blocks are scanned in a chosen sequential order, resulting in a biased (meaning that the binary numbers of 1 and 0 are not balanced) binary sequence. This biased binary sequence is loss lessly compressed to leave space for data embedding and the compressed bit sequence is embedded into the cover media as an overhead for later reconstruction of the original image. In data embedding, the R- and S-blocks are scanned once again and the flipping operation is applied whenever necessary to make the changed R- and S-block sequence coincident with the to-be-embedded data followed by the overhead data mentioned above. While it is novel and successful in reversible data hiding, the payload is still not large enough for some applications. Specifically, the embedding capacity estimated by authors ranges from 3 to 41 kb for a 512 × 512 × 8 cover grayscale image when the embedding amplitude is 4 (the estimated average PSNR of the marked image versus the original image is 39 dB) .

Another problem with the method is that when the embedding strength increases in order to increase the payload, the visual quality of the marked image will drop severely due to annoying artifacts. To increase the payload dramatically, a new lossless data hiding technique based on integer wavelet transform (IWT) (a second generation wavelet transform, which has avoided round-off errors) was developed recently. Because of the superior de correlation capability of wavelet transform, the selected bit plane compression of IWT coefficients in high frequency sub bands creates more space for data hiding, resulting in a two to five times payload as large. Specifically, its payload ranges from 15 to 94 kb for a 512 × 512 × 8 grayscale image at the same (39 dB) PSNR of the marked images compared with the original images. To achieve reversible data hiding, a histogram modification is applied in its pre-processing to prevent over/underflow. This histogram modification causes, however, a relatively low PSNR of the marked image versus the original image though there are no annoying artifacts. It is noted that reversible data hiding has attracted increasing attention recently, and more algorithms are being developed. Then the authors adopt the CALIC lossless image compression algorithm, with the quantized values as side information, to efficiently compress the quantization residuals to create high capacity for the payload data . The compressed residual and the payload data are concatenated and embedded into the host signal via generalized-LSB modification method. The payload of this technique is from 15 to 143 kb for a 512 × 512 × 8 grayscale image while the PSNR is 38 dB. Even though the payload is high, the PSNR is still not high enough. In this paper, we propose a new reversible data embedding

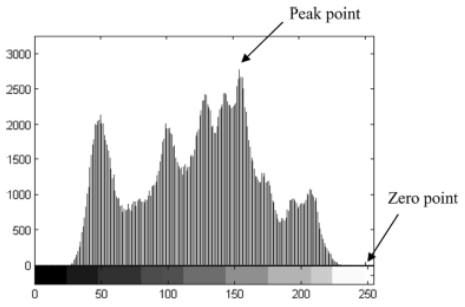


Fig. 1. Histogram of Lena image.

technique, which can embed a large amount of data (5–80 kb for a 512 × 512 × 8 grayscale image) while keeping a very high visual quality for all natural images, specifically, the PSNR of the marked image versus the original image is guaranteed to be higher than 48 dB. It utilizes the zero or the minimum point of the histogram (defined below) and slightly modifies the pixel grayscale values to embed data. This technique can be applied to virtually all types of images. Up to now, it has been successfully tested on different types of images, including some commonly used images, medical images, texture images, aerial images, and all of the 1096 images in CorelDraw database. The computation of our proposed technique is quite simple and the execution time is rather short. Although the proposed lossless data hiding technique is applied to still images, it is also applicable to videos which consist of a sequence of images.

4.2 Drawbacks of Existing Techniques:

1. In LSB Technique only you are going to hide in least significant only. So, any one can easily retrieve the secret information.
2. Compressed domain reversible steganography often suffers from high computational cost, low hiding capacity, and low stego-image quality.
3. After hiding the data in image by using LSB algorithm, if someone takes the Image and compress the image means definitely lsb value will be change.
4. So we can't get the original data what we hided

5 EXPERIMENTAL SIMULATION

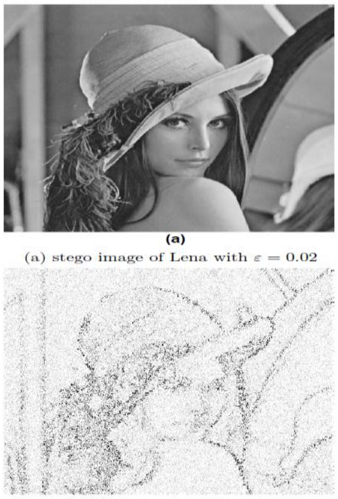
Using a 512 £ 512 8-bit gray image "lena" as the cover image and choosing ″ = 0:02,n = 5, a total of5:57 £ 105 secret bits are embedded, so the capacity is equal to 0.25. The stego images are shownin Also shown is the error image, which has been enhanced by a 35-time gray-level stretchfor the purpose of display. The similar experimental results are shown in Fig.2 for the cover image baboon. We can see that the modification were mainly in busy areas and on edges, which means less perceptual distortion is achieved. Three quality metrics are used to measure the distortion induced by data embedding: wPNSR,the Watson metric, and SSIM[10]. The wPNSRand Watson metric are all designed in [7] by using characteristics of HVS and measure the total perceptual error. Four standard test images, lena baboon, peppers and boat are used to make the second experiment.

(a) Cover Image (b) Stego Image

Figure 2. Block diagram for the proposed steganographic system.

Table 1 lists the value of apcity,wPSNR,Waston metrics and SSIM under ″ = 0:01and ″ = 0:03.

It can be seen from Table.1 that the imageswith more edges and textures can carry more information than the °at one, and given the larger ″,the AQE can provides more space to carry messagebits. So the propose method can be *daptive* withthe di®erent image region and di®erent image.



(a)
(a) stego image of Lena with $\varepsilon = 0.02$

(b)
(b) Enhanced error image of Lena

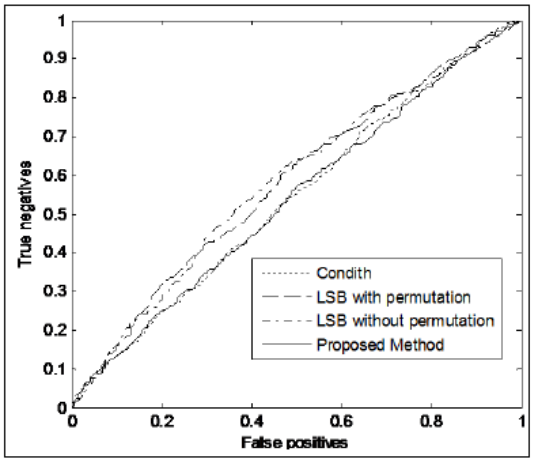


Figure 6. ROC curve (Embedded message size obtained by T=10).

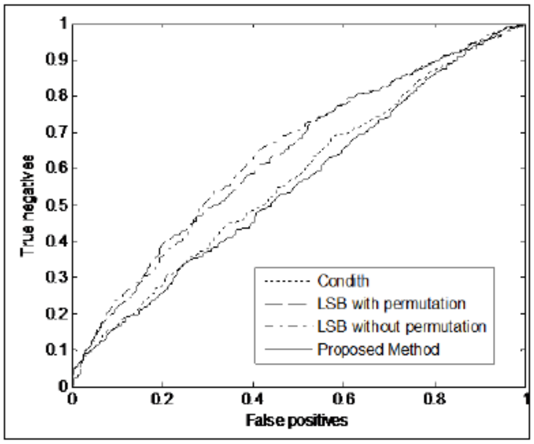


Figure 7. ROC curve (Embedded message size obtained by T=5).

In order to evaluate the detection accuracy quantitatively, we use the 'detection reliability' ρ, defined as

Where A is the area under the ROC curve. The accuracy is scaled to obtain ρ = 1 for a perfect detection and ρ = 0 for no detection case. The detection reliability values for the proposed and the reference methods are shown in steganography is used in the covert communication to transport secrete information.

TABLE III. THE DETECTION RELIABILITY

Method	ρ (T=5)	ρ (T=10)
LSB with permutation	0.2657	0.1596
No-permutation LSB	0.2804	0.1661
Condith	0.1466	0.0802
Proposed Method	0.112	0.0789

6 CONCLUSION

The proposed method based on image contrast has been shown to be capable of improving the embedding capacity and imperceptibility of stego images and reducing the detection probability. The existing adaptive steganographic methods have been reviewed and compared to the proposed algorithm. Bit Length Replacement Steganography using Segmentation and DCT is proposed. The cover image is segmented into smaller matrix of size 8x8 and converted to DCT domain. The MSB bits of payload in spatial domain are embedded into each DCT coefficients of cover image based on the coherent length *L* which is determined by the DCT coefficient

values. The performance results in terms of PSNR for different kinds of images and dimensions are better in the proposed algorithm compared to the existing algorithm. In future the technique can be verified for robustness. Approach has been verified to be superior to the selected wellknown steganography methods.

REFERENCES

[1] E. Franz, and A. Schneidewind, "Adaptive steganography based ondithering," in Proceedings of the 2004 workshop on Multimedia and security, Magdeburg, Germany, 2004, pp. 56-62.

[2] R. H. M. Dulce, R. C. Raul, and F. U. Claudia, "Adaptive Steganography based on textures," in Proceedings of the 17th International Conference on Electronics, Communications andComputers, 2007, pp. 34-39.

[3] C. H. Yang, C. Y. Weng, S. J. Wang et al., "Adaptive Data Hiding in Edge Areas of Images With Spatial LSB Domain Systems," IEEE
Transactions on Information Forensics and Security, vol. 3, no. 3, pp.488-497, 2008.

[4] D. C. Wu, and W. H. Tsai, "A steganographic method for images bypixel-value differencing," Pattern Recognition Letters, vol. 23, pp.1613–1626, 2003.

[5] H. C. Wu, N. I. Wu, C. S. Tsai et al., "Image steganographic schemebased on pixel-value ifferencing and LSB replacement methods," in
Proc. Inst. Elect. Eng., Vis. Images Signal Process, 2005, pp. 611–615.

[6] X. Qi, and K. Wong, "An Adaptive DCT-Based MOD-4 SteganographicMethod," in International Conference on Image Processing (ICIP'05),
Genova, Italy, 2005, pp. 297-300.

[7] M. Ramezani, and S. Ghaemmaghami, "Towards Genetic FeatureSelection in Image Steganalysis," in 6th IEEE International Workshopon Digital Rights Management, Las Vegas, USA, 2010.

[8] Raja K B, C R Chowdary, Venugopal K R, L M Patnaik. (2005) :"A Secure Steganography using LSB, DCT and Compression Techniques on Raw Images," *IEEE International Conference on Intelligence Sensing and Information processing,* pp.171-176.
[9] Kumar V and Kumar D. (2010): "Performance Evaluation of DWT Based Image Steganography," *IEEE International Conference onAdvance Computing,* pp. 223-228.
[10]Weiqi Luo, Fangjun Huang, and Jiwu Huang. (2010): "Edge Adaptive Image Steganography Based on LSB Matching Revisited," *IEEE Transactions on Information Forensics and Security,* no. 2, vol. 5, pp. 201-214.
11]R O El Safy, H H Zayed and A El Dessouki (2009): "An Adaptive Steganographic Technique Based on Integer Wavelet Transform," *International Conference on Networking and Media Convergence*, pp.111-117.
[12] Mathkour H, Al-Sadoon B and Touir A. (2008): "A New Image Steganography Technique. :" *International Conference on Wireless Communications, Networking and Mobile Computing,* pp.1-4.
[13] V Vijaylakshmi,G Zayaraz and V Nagaraj. (2009):"A Modulo Based LSB Steganography Method," *International Conference on Control,Automation*,Communication *and Energy Conservation*, pp. 1-4.
[14] Wien Hong, Tung-Shou Chen and Chih-Wei. (2008):"Lossless Steganography for AMBTC-Compressed Images," *Congress on Image and Signal Processing,* pp.13-17.
[15] A W Naji, Teddy S Gunawan, Shihab A Hameed, B B Zaidan and A A Zaidan. (2009): "Stego-Analysis Chain, Session One," *International Spring Conference on Computer science and Information Technology,* pp. 405-409.
[16] M Hassan Shirali-Shahreza and Mohammad Shirali-Shahreza. (2008): "A New Synonym Text Steganography," *International Conference on Intelligent Information Hiding and Multimedia Signal Processing*, pp. 1524-1526.

- *N Santoshi is currently pursuing masters degree program in Digital Elecronics And Communication system in CIST affiliated to JNTU KAKINADA, INDIA, PH-9441820617. E-mail: santoshineelamsetty@gmail.com*
- *B.Lokeswara rao is HOD in Electronics And Communication engineering in CIST, INDIA, PH-08790325618. E-mail: blokeswararao@gmail.com*