Grey Scale Image Hiding Method Based on Decomposition Operation

S.M. Wadi[1,2], N. Zainal[1], A. Abdulgader[1]
[1]Dept. of EE&S Eng., Universiti Kebangsaan Malaysia, UKM Bangi 43600, Malaysia
[2]Com. Eng. Dep., Najaf Technical College, Foundation of Technical Education, South Street, Najaf 472, Iraq.

***Abstract*- Capacity is one of the importance factors in the hiding techniques. The challenge facing of the concealment techniques is the inverse relationship between the capacity and quality of stego-image. The least-significant-bit (LSB)-based approach is a popular hiding technique in the spatial domain. Number of methods (PVD, OPAP, LSBM, LSBMR,) was proposed to enhance the performance of LSB method. However, the capacity of most hiding approaches especially in spatial domain was little and not enough to hide image in image with same size and type. New disguise algorithm based on decomposition and LSB is proposed in this paper. Distorted image as cover image used in this paper to decrease the effect of increase the capacity. Secret image decomposed by binary bit planes and hide 5 bit most significant bit planes from 8. Bit planes are change in order to avoid the appearance of the scene of secret image in stego-image ordering. Experimental results show that the capacity of proposed method is perfect with high quality of recovered image and strong against statistical analysis.**

key words: image hiding; image decomposition; hiding capacity; modified AES; HD image.

I. INTRODUCTION

Generally, hidden data is classified into two major types based on domain of host image. First type is the spatial domain methods where the secret data directly embedded in host pixels. Second type is transform domain method which based on hide the secret data on host image after transform it to frequency domain [1-2].

The popular and effective technique for hiding data in spatial domain is Least Significant Bit (LSB) which based on changing the LSB of each pixel value of host image with one bit secret data. However, LSB technique suffers from disadvantages such as low capacity. Numbers of methods were proposed to enhance the performance of LSB technique[3].

T. Sharp [4] proposed modified method to LSB named as LSB matching where the author suggests to add or subtract one randomly from host pixel if secret bit does not equal to LSB of host pixel. LSB matching technique is weak against detectors specially detecting operation proposed in [5, 6]. J. Mielikainen [7] suggested a modification to LSB matching by reducing the changes of host image in percentage from 0.500 to 0.375 bits/pixel (bpp) with same amount of data hiding. W. Luo et al. [8] used an edge adaptive method with LSB matching revisited, where new scheme based on the size of secret data and the difference between two neighboring pixels was proposed to determine the embedding areas. C. K. Chan et al [9] applied optimal pixel adjustment process (OPAP) on stego-image to improve the quality of stego-image. M. H. Lin et al [10] proposed a novel hiding image technique focus on colour secret and host images that preserved host image quality which loaded with a large quantity of secret information. To reduce the amount data of secret image, the author proposed to convert it to indexed image and then decrypt it using DES and then hide the encrypted data in RGB host image. Y.H. Yu et al [11] enhanced the operation of hiding operation proposed in [9]. The authors proposed hiding method to colour, palette, and grey scale secret image in true colour image based on method of [9] by modification of the palette construction operation. C. M. Wang et al. [12] suggested on controlling of the rest of two consecutive pixels to enhance the stego-image quality. N. I. Wua et al. [13] proposed hiding method based on pixel-value differencing (PVD) method and base decomposition. New range table were suggested with five regions to specify the host image and determine the smooth and edge areas as in PVD method [14]. To use the base decomposition scheme for reducing the stego-image distortion, authors selected two integers as a base pair to each range table. Coefficient pair will determine depend on the size of hidden data which specify from range table, then embedding coefficient pair in pixel pair.

The capacity of most hiding methods which based on (LSB, LSBM, LSBMR, PVD, OPAP, etc.) did not exceed 4 bit/pixel to keep the stego-image from distortion. This capacity is not enough to hide image in image with same size and type (for example, grey scale in grey scale or RGB in RGB with same size), where at least need five high significant bit planes to reconstruct an image. New hidden data method proposed in this paper based on LSB replacement. Instead of natural or known scene image, the distorted image like jamming appears in TV used as cover image. The quality of host image scene is not important because it is originally distorted. This will give flexibility to increase the hidden data capacity until 5 bpp or more. Another advantage is often the scene of encrypted image similar jamming in TV, therefore this camouflaged the adversary the stego-image is encrypted image not stego-image and then increases the security level.

The rest of this paper is Section 2 shows the proposed method. Experimental results explains in Section 3. Conclusion appears in Section 4.

II. PROPOSED METHOD

The goal of this paper is to propose hiding method with high capacity (5 bpp or more) to get high quality hiding image operation. The problem of most methods in spatial domain was its capacity smaller than 5 bpp, therefore, cannot hide

image in image with same size. Hidden image in image in spatial domain means replacement some bits of host image pixel with bits of secret image pixel. Now the question is how many bits needed in acceptance of reconstructed image?. To answer this question an test image (Lena) is decomposed to binary bit planes depend on (1), and then reconstruct it with lose 1, 2, 3, and 4 LSBs as shown in Fig. 1. At least 5 bit planes are used to reconstruct an image with accepted scene and PSNR where PSNR should be more than 30 dB because the human eyes distinguish differences between the original and reconstructed image if the PSNR smaller than 30 dB.

$$D = \sum_{i=0}^{n-1} a_i 2^i = a_0 2^0 + a_1 2^1 + \cdots + a_{n-1} 2^{n-1} \qquad (1)$$

where binary code (a_(n-1),…,a_1,a_0) is the binary representation of non-negative decimal number D.

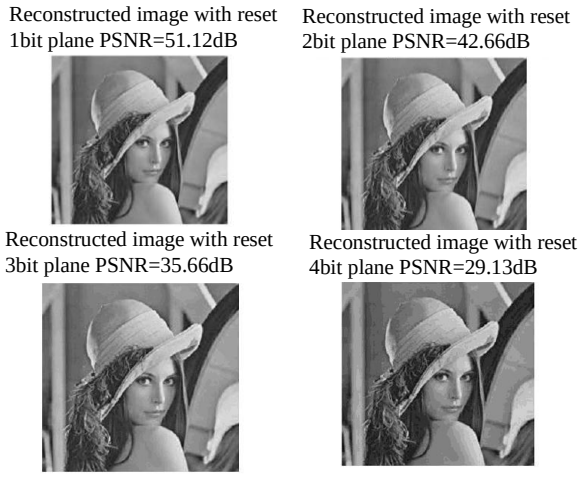


Fig. 1. Reconstructed of decomposed image with different number of lose bit planes.

Therefore, to hide an image decomposed by binary bit plane should be hidden at least 5 MSBs of secret image in host image. This capacity is high and lead to distorted the host image. Furthermore, distorted image as host image was used in proposed method. Modified AES method proposed in [15] used to produce the cover image. The steps of proposed method shown below:

1- Encrypt host image before hidden operation to get distorted image as host.

2- Decompose the host and secret image to binary bit planes based on (1).

3- Replace five least significant bit planes of host image with five most significant bit planes of secret image according to (2) below:

$$BP_h(9 - i) = BP_s(i) \qquad (2)$$

where BP_h, BP_s is Bit planes of host and secret images respectively, [i=8, 7,…,3].

III. Experimental Results

HD GS images (three images) are used to test proposed method as shown in Figs. 2-7. One image is used for all tests images as a cover image after distorted it by using encryption method shown in [15] as shown in Fig. 2, where the histogram of cover image shown in Fig. 2(c). Three tests as secret image are shown in Fig. 3. Fig. 4 clearly shows the stego-image is very similar to cover image that mean the distorted image protect its scene after hiding operation with high capacity. Three bit planes were wasted from secret image after reconstruct it from hiding operation where this not enough to distorted the secret image as in Fig. 6. Set of factors are used to evaluate the performance of proposed method.

A. PSNR

PSNR is a pixel-based evaluation of image quality after change pixels values of this image [11]. PSNR is commonly used as image quality measure in most image processing evaluation. PSNR is calculated depends on Mean Square Error (MSE) as in (3) and (4) below:

$$MSE = \frac{1}{MN} \sum_{i=1}^{M} \sum_{j=1}^{N} (x_{ij} - y_{ij})^2 \qquad (3)$$

where M and N denote the images dimensions, $x_{i,j}$ and $y_{i,j}$ stand for the value of pixel (i, j) in the original and the processed images, respectively. Now, PSNR is calculated as in (4):

$$PSNR = 10 \times log_{10}(\frac{255^2}{MSE}) \qquad (4)$$

Cover image in proposed method is distorted image (unknown sense image) therefore our comparison in term of PSNR only to reconstructed image. Table 1 shows the values of PSNR to reconstructed image, where the value of PSNR for all tests are within the acceptance range.

B. Q Index

The universal quality index, Q is used to measure the changes in host image because of the hiding operation. Q factor is in range (-1,1), where if Q factor is equal to 1 that means the host image is not distorted by hiding operation which is ideal case. Results of Q factor shown in Table I demonstrated that the proposed method can achieve high precision between the cover image and the stego- image for more details about Q index as in [16].

TABLE I
Q Index and PSNR for Reconstructd Image

Image reconstructed	PSNR	Q Factor
Test1	33.54dB	0.9991
Test2	32.09dB	0.9998
Test3	33.10dB	0.9984
Test4	33.43dB	0.9995

C. Histogram Analysis

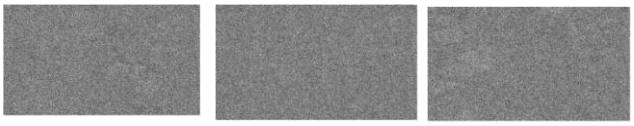
One of the important factors for hiding techniques is the stego-image histogram information. Histogram gives a significant indicator to statistical analyzer about the nature of stego-image and distribution of pixels [6]. Generally, a good hiding technique has identical distributed histogram in other words (the pixels evenly distrusted on grey levels). Fig. 5 clearly shows that the histogram of stego-image is equally distributed and that mean the stego-image is very strong against the statistical analyses hackers. Therefore, the proposed method has high security.

a b c

Fig. 2. OI a- Original image b- Cover image c- Histogram of CI

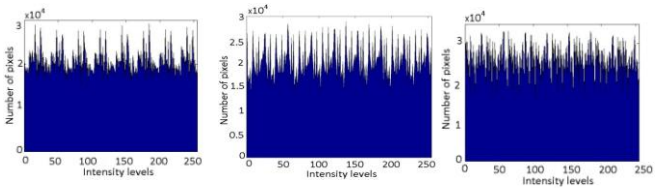
a b c

Fig. 3. Secret image (a-Test1, b-Test2, c-Test3)



a b c

Fig. 4. Stego-image (a-Test1, b-Test2, c-Test3)



a b c

Fig. 5. Histogram of stego-image (a-Test1, b-Test2, c-Test3)

a b c

Fig. 6. Reconstructed image (a-Test1, b-Test2, c-Test3)

D. Capacity

The important factor in proposed method is the capacity with preserve the other factors as shown in previous sub sections. Our aim is to achieve the capacity equal to 5 bpp and to hide image in image with same size and type. Table II shows the comparison between proposed scheme and number of hiding methods. The results that appear in Table II is in percentage of hiding data with respect to size of cover image. The capacity of proposed method is better compared to all other methods.

TABLE II
CAPACITY COMPARSION
(DATA HIDING SIZE TO COVER IMAGE SIZE)

Method	Capacity
Method in [7]	0.38
Method in [9]	0.50
Method in [12]	0.22
Method in [14]	0.21
Method in [17]	0.51
Method in [18]	0.17
Proposed method	**0.63**

IIII. CONCLUSION

In this paper, new high capacity image hiding method based on simple LSB approach is proposed. The problem in data hiding operations is the inverse relationship between hiding capacity and stego-signal quality, therefore the capacity is determined and not to exceed 4bpp in most hiding techniques based LSB substitution. The aim of proposed method is hidden image in image with same size and type (GS in GS). In order to achieve this task, the capacity should reached at least 5bpp to hide at least five bit planes of the secret image as shown in sub-section 2-1. In proposed method, distorted image used as cover image which minimize influenced the stego-image by the capacity increasing. Set of parameters (such as PSNR, histogram, and Q index) used to show the effectiveness of proposed method. Capacity of our method is compared with [7, 9,12, 14, 17, 18] to show that the capacity of proposed method higher than most LSB substitution based methods. The experimental results clearly show the proposed method has high capacity and high level of security.

ACKNOWLEDGEMENT

The authors would like to thank staff of Department of Electrical, Electronic and Systems Engineering in Faculty of Engineering and Built Environment, Universiti Kebangsaan Malaysia for assist in the completion of this work and also UKM for DPP-2013-013 fund.

REFERENCES

[1] C. C. Chang,T. S. Chen, and L. Z. Chung, "A steganographic method based upon JPEG and quantization table modification," *Information Sciences*, . Vol. 141, No. 2 p.p. 123-138, 2002.

[2] M. Iwata, M. K. Shiozaki, "A Digital Steganography Utilizing Features of JPEG Images," *IEICE Trans Fundam Electron Commun Comput Sci (Inst Electron Inf Commun Eng)*, Vol. E87, No., 4 p.p. 929-936, 2004.

[3] Y. Linde, A. Buzo, and R. M. Gray, "An Algorithm for Vector Quantizer Design," *Communications, IEEE Transactions on*, Vol. 28, No. 1, p.p. 84-95, 1980.

[4] T. Sharp, "An Implementation of Key-Based Digital Signal Steganography" *Proc. of 4th International Workshop on Information Hiding*, p.p. 13-26, 2001.

[5] J. J. P. Harmsen, A. William, "Steganalysis of additive-noise modelable information hiding" *Proc. of the SPIE*, p.p. 131-142, 2003.

[6] A. D. Ker, "Steganalysis of LSB matching in grayscale images," *Signal Processing Letters, IEEE*, Vol. 12, No, 6, p.p. 441-444, 2005.

[7] J. Mielikainen, "LSB matching revisited," *Signal Processing Letters, IEEE*, Vol, 13, No 5, p.p. 285-287, 2005.

[8] L. Weiqi, H. Fangjun, and H. Jiwu, "Edge Adaptive Image Steganography Based on LSB Matching Revisited," *Information Forensics and Security, IEEE Transactions on*, Vol. 5, No. 2, p.p. 201-214, 2010.

[9] C. K.Chan, and L.M. Cheng, "Hiding data in images by simple LSB substitution," *Pattern Recognition*, Vol. 37, No. 3, p.p. 469-474, 2004.

[10] M. H. Lin, Y. C. Hu, and C. C. Chang, "Both color and gray scale secret images hiding in a color image," *international journal of pattern recognition and artificial intelligence*, Vol. 16, No. 6, p.p. 697-713, 2002.

[11] Y. H. Yu, C. C. Chang, and I. C. Lin, "A new steganographic method for color and grayscale image hiding," *Computer Vision and Image Understanding*, Vol. 107, No. 3, p.p. 183-194, 2007.

[12] C. M. Wang, "A high quality steganographic method with pixel-value differencing and modulus function" *Journal of Systems and Software*, Vol. 81, No. 1, p.p. 150-158, 2008.

[13] N. I. Wu, K. C. Wu, and C. M. Wang, "Exploring pixel-value differencing and base decomposition for low distortion data embedding," *Applied Soft Computing*, Vol. 12, No. 2, p. p. 942-960, 2012.

[14] D. C. Wu, and W. H. Tsai, "A steganographic method for images by pixel-value differencing," *Pattern Recognition Letters*, Vol. 24, No, 9, p.p. 1613-1626, 2003.

[15] S. M. Wadi, and N. Zainal, "Rapid Encryption Method Based on AES Algorithm for Grey Scale HD Image Encryption," *Proc. of the 4th International Conference on Electrical Engineering and Informatics (ICEEI 2013)*, Vol. 8C, p.p. 52-57, 2013.

[16] W. Zhou, and A.C. Bovik, "A universal image quality index," *Signal Processing Letters, IEEE*, Vol. 9, No. 3, p.p. 81-84, 2002.

[17]H. Y. Cheng, "Adaptive Data Hiding in Edge Areas of Images With Spatial LSB Domain Systems," *Information Forensics and Security, IEEE Transactions on*, Vol. 3, No. 3, p.p. 488-497, 2008.

[18] M. B. O. Medeni, and E.M. Souidi, "A novel steganographic method for gray-level images with four-pixel differencing and LSB substitution" *Proc. in Multimedia Computing and Systems International Conference (ICMCS)*, 2011.