ISSN:2321-1156
International Journal of Innovative Research in Technology & Science(IJIRTS)

SPATIAL DOMAIN BIT PLANE STEGANOGRAPHY

MANSOUR ZUAIR, ABDULMALIK RAHHAL, WADOOD ABDUL, SANAA GHOUZALI*,EMAD-UL-HAQ QAZI**

Department of Computer Engineering, College of Computer and Information Sciences, King Saud University, Riyadh, Kingdom of Saudi Arabia.

* Department of Information Technology, College of Computer and Information Sciences, King Saud University, Riyadh, Kingdom of Saudi Arabia

** Department of Computer Sciences, College of Computer and Information Sciences, King Saud University, Riyadh, Kingdom of Saudi Arabia.

ABSTRACT: Steganography is the art of hiding a secret message in different types of multimedia (image, voice or video), such that the secret message is not detectable. In this paper, we propose a new spatial domain steganography algorithm where the host image is converted into blocks of bit-planes to insert the secret information. The proposed algorithm divides the image in to 8 bit planes and then the bit planes are further divided in to N x N blocks. The hidden message is inserted based on a chaotic sequence in to the blocks. We intend to find the most optimum bit plane to insert the hidden information, keeping high imperceptibility in terms of the human visual system. The algorithm shows relatively good PSNR (Peak Signal to Noise Ratio) and MSSIM (Mean Structural SIMilarity). In addition the proposed algorithm also shows resistance against attacks such as JPEG compression.

Keywords: *Steganography, Spatial Domain, Bit Plane.*

1 INTRODUCTION

Markus Kuhn defines steganography,as "steganography is the art and science of communicating in a way which hides the existence of the communication". Steganography is concerned with hiding the fact that communication is taking place whereas cryptography is concerned with encrypting the secret message where the adversary knows that secret communication is going on[1].

Stenographicalgorithmsare classified in to spatial domain and frequency domain algorithms [2]. For each domain there are many algorithms which have certainadvantages and drawbacks.

LSB (least significant bit) replacing is the most widely used data hiding method in the spatial domain.It is a simple method with high embedding capacitybut the hidden data are sensitive to image alteration and vulnerable toattacks[2,3,4,5,6]. In the frequency domain, the image is transformed in to frequency components by using transforms like the Discrete Fourier Transform (DFT), the Discrete Cosine Transform (DCT)[7,8]and the Discrete Wavelet Transform (DWT)[3],[9] and[10]. These components are modified according to the algorithm to insert the secret data. Hiding data in frequency domain has certain advantages over hiding in spatial domain; it provides higher robustness against changes and attacks, whichmeans more resistance to loss from image manipulation and increased difficulty to attacker. However, it is relatively costly in terms of complexity, [2] and [9], also the amount of secret data that can be hidden in the frequency domain is less than the LSB scheme [11].

In [2] authors proposed a 3-3-2 LSB(three, three and two least significant bits from the red, green and blue color components respectively) insertion method in an RGB pixel respectively. This pattern distribution is considered because human eye is more sensitive to changes in the blue color component than the red and green color components. In[2], The secret image is inserted into the cover image using chaotic sequence and XOR operation.

In [5], the authors use LSB insertion method using chaos in the spatial domain. The main advantage of chaos theory is simplicity of implantation, more randomness than traditional pseudo random generators, non-periodicity and confidentiality. In a similar way to [2] they generate chaotic binary sequence XORed with the secret message, each XORed bit is again XORed with LSB of the selected pixel of the cover image. The algorithm presented in [5] outperforms the one presented in [2]in terms of imperceptibility with regard to PSNR (Peak Signal to Noise Ratio).

In [4] Nag et al. proposed a new spatial domain method for image steganography using X-Box mapping. They generate four different X-Boxes (using XOR operation) andthen the image is encrypted based on X-Box values. Finally, the encrypted values are inserted in 4 LSB bits of the cover image. The basic advantage of this approach is that the stego key is not required. Experimental result shows good imperceptibility in terms of PSNR with insertion capacity equal to 25%.

Atallah mentioned that hiding directly in two LSB of an image reduces robustness of image in [6]. The secret message is divided into pairs of bits, then random pixels

of the cover image are chosen, where the algorithm searches for identical values to the secret message and saves the locations in a table. The algorithm can hide 6 bits of the secret message in one RGB pixel of the cover image. The identical values of secret message and cover image are sought to have high levels of imperceptibility.

In [12] X. Zhang proposed a reversible data hiding scheme for encrypted images. The proposed algorithm depends on encrypting the original uncompressed image using an encryption key to produce the encrypted image. Additional data is then embedded in to the encrypted image using a data hiding key. On the receiver side, the stego image is decrypted using an encryption key. Using data hiding key and decrypted image the embedded data is extracted and original image is recovered with the aid of spatial correlation of natural images.

In[13]Alam et al. extended the work of Chen et al. [14] to enhance the security of the algorithm. Edge detection is used to increase the capacity of the algorithm. A gray scale image is divided in to blocks of n pixels. The first pixel of each block is used to store the status of other pixels, the status is '1' if it is an edge pixel and status is set to '0' for a non-edge pixel. The secret information is then inserted through LSB substitution for edge and non-edge pixels using chaotic sequence. The experimental results show good imperceptibility and capacity.

In [15], Luo et al. expanded LSB matching revisited (LSBMR) image steganography algorithm and proposed an edge adaptive scheme which can select the embedding region according to the size of the secret image and the difference between consecutive pixels of the cover image. The host image is first divided into non-overlapping blocks and then each block is rotated based on a secret key. The rotation of the cover image improves the security and allows inserting the secret message in to both horizontal and vertical edges. In the next step, the blocks are rearranged as row vectors and then each vector is divided in to non-overlapping embedding units where each unit consists of two consecutive pixels. Then the embedding region is determined based on the given secret message size and the data hiding is done using a secret key. Finally, the stego image is rebuilt. The experiments show that the algorithm has improved security and imperceptibility.

Most of the algorithms proposed in the literature use LSB substitution of lower bits usually 1,2 and 3. This allows for a high level of imperceptibility but the hidden information inserted at these levels is vulnerable to the most common unintentional attacks. We are interested to find the most optimum locations to insert the hidden information, keeping high imperceptibility and also provide a certain level of resistance against common unintentional attacks such as JPEG compression.

The reset of the paper is organized as the follows. In Section 2, the proposed bit plane steganography algorithm is described. In Section 3,results are illustrated and the paper is concluded in Section 4.

2 PROPOSED BIT PLANE STEGANOGRAPHY ALGORITHM

The proposed bit plane steganography algorithm divides the image into N×N blocks of 8-bit planes for a gray scale image. The hidden information is inserted into random blocks based on a chaotic sequence. The insertion procedure takes into account the local mean L (block of N×N) and global mean G (whole image) according to Equation (1):

$$L'_{B(a,b)} = \begin{cases} (1+\partial)G_B, & if M_{(i,j)} = 1 \\ (1-\partial)G_B, & if M_{(i,j)} = 0 \end{cases} \quad \text{(Error! Bookmark not defined.)}$$

where $L'_{B(a,b)}$ is new mean value of block (a,b) in bit plane B, G_B is the mean of bit plane B, and ∂ is the force of insertion of the hidden information.

Now to change the local mean of the block ($L'_{B(a,b)}$), f randomly selected bits are flipped in the particular block. Where f is calculated using Equation (2):

$$f = \lceil L' - L \rceil N^2 \quad \text{(Error! Bookmark not defined.)}$$

The secret message insertion procedure is illustrated in Figure 1.

In the extraction phase, the local and global mean values are compared for blocks specified by the chaotic secret key and the decision of '1' or '0' is reached based on Equation (3):

$$M_{(i,j)} = \begin{cases} 1, & if L'_{B(a,b)} \geq G_B \\ 0, & if L'_{B(a,b)} < G_B \end{cases} \quad \text{(Error! Bookmark not defined.}$$

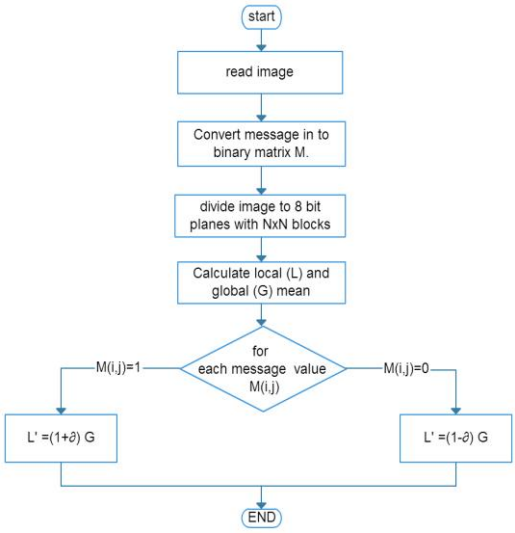


Fig. 1. Secret message insertion procedure.

3 EXPERIMENTAL RESULT:

We tested the algorithm for 5 images of size 512×512 shown in Figure 2.

Baboon Lenna Fabric

Window Thumb

Fig. 2. Tested images.

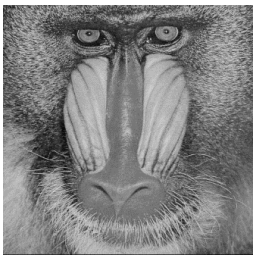
The capacity C for an X×Y image is given by Equation (4):

$$C \approx \frac{X \times Y}{2 \times N^2} \text{ bit} \qquad \text{(Error! Bookmark not defined.}$$

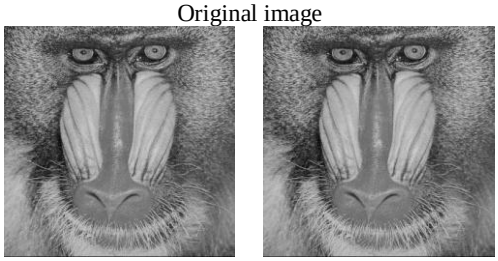
Where X×Y is image size and N×N is the block size.

4 IMPERCEPTIBILITY ANALYSIS

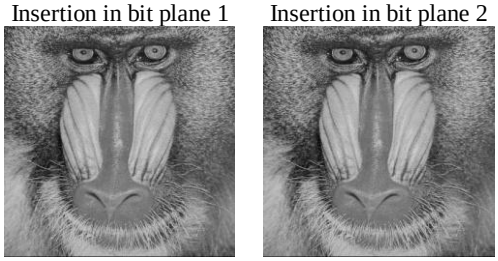
To find out the most optimal bit plane to insert the hidden information we inserted the hidden information in to each bit plane and carried out objective and subjective analysis of the stego images. We noticed that the hidden information is imperceptible in bit planes 1-4 when $\partial = 0.1$ as illustrated in Figure 3. There are some locations where the hidden information is not completely imperceptible for bit plane 5. For bit plane 6-8, there are several location where the changes in the image are visible.



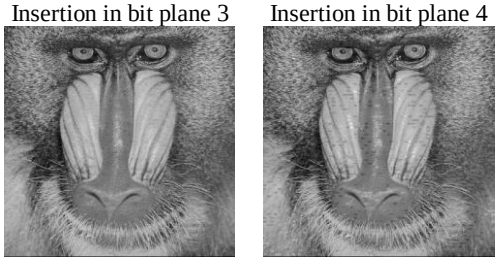
Original image



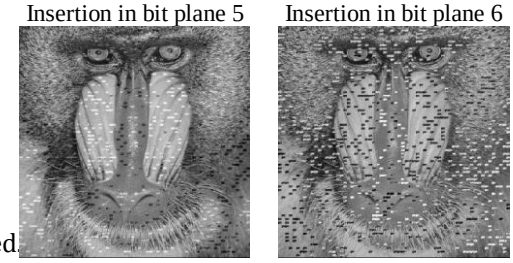
Insertion in bit plane 1 Insertion in bit plane 2



Insertion in bit plane 3 Insertion in bit plane 4



Insertion in bit plane 5 Insertion in bit plane 6



Insertion in bit plane 7 Insertion in bit plane 8

Fig. 3. Hidden information insertion into each bit plane of Baboon($\partial = 0.1$).

The Mean Square Error (MSE) and the Peak Signal to Noise Ratio (PSNR) are the two error metrics used to compare image quality. The MSE represents the cumulative squared error between the modified and the original image, whereas PSNR represents a measure of the peak error. The lower the value of MSE, the lower the error. MSE is calculated using Equation (5):

$$MSE = \frac{\sum_{XY}[I_1(x,y) - I_2(x,y)]^2}{X \times Y} \quad \text{(Error! Bookmark not defined.)}$$

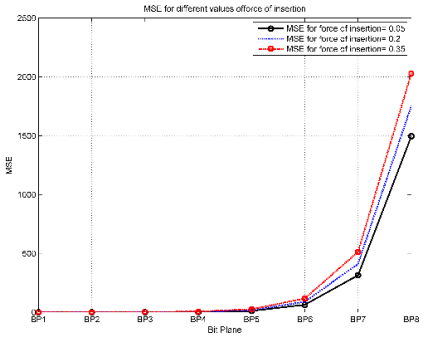


Fig. 4. Average MSE of all tested images for all bit planes-with $\partial = (0.05,0.2,0.35)$.

Figure 4 shows the average MSE for all tested images for all bit planes with different value of force insertion(∂). We noticed that MSE values for bit planes 1-5 are relatively lower than the bit planes 6-8 for all values of insertion force.

PSNR is calculated using Equation (6):

$$PSNR = 10 * \log_{10}\left(\frac{R^2}{MSE}\right) \quad \text{(Error! Bookmark not defined.)}$$

Where R is the maximum gray scale value of a pixel in the image under consideration.

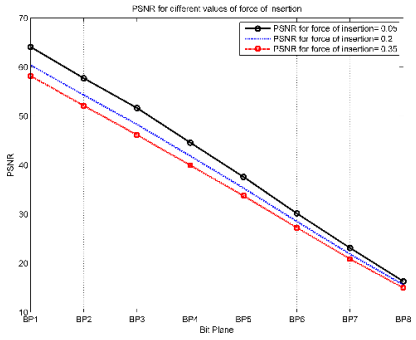


Fig. 5. Average PSNR of all tested image for all bit planes-with $\partial = (0.05,0.2,0.35)$.

Figure 5 shows the average PSNR values for all tested images for all bit planes with different values of force of insertion (∂). As high PSNR values indicate low distortion, we can conclude that bit planes 1-5 are the most suitable to insert the hidden information.

Table 1 shows the comparison between the proposed algorithm and similar algorithms found in the literature.The PSNR values for the proposed algorithm show higher imperceptibility when compared with these algorithms, especially for the optimal cases, i.e. bit planes 4 and 5.

Table 1: PSNR comparison.

Algorithm	PSNR dB
[1]	49 -59
[3]	34 35
[12]	41 - 40.79
Proposed algorithm As shown in Fig 5	18-64

Although MSE and PSNR are very simple and conventionally accepted tools to measure signal fidelity yet in practice, we observe that tools like the Structural SIMilarity (SSIM) index give a clearer understanding of imperceptibility specially when modeling the human visual system in applications like compression and data hiding.

Figure 6 shows the Mean SSIM (MSSIM) for all images and all bit planes with different value of force of insertion (∂). We observe very similar results to the ones shown in Figure 3. The MSSIM results confirm our initial analysis that bit planes 1-5 are the most suitable to insert the hidden information in terms of imperceptibility.

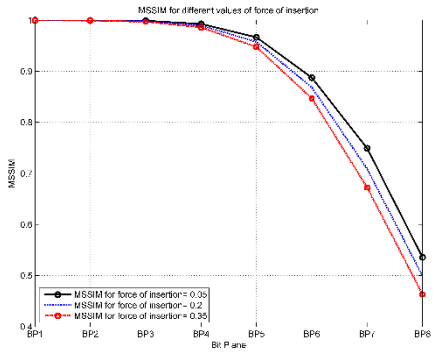
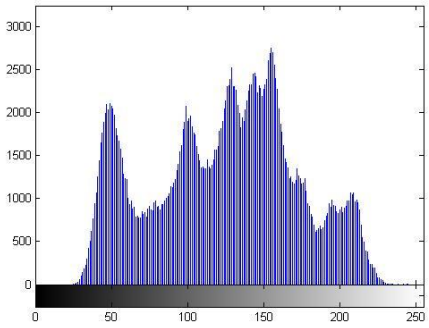
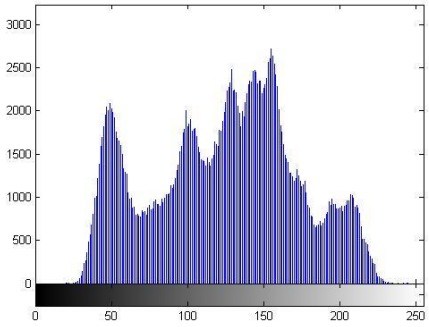


Fig. 6. Mean SSIM of all images and all bit planeswith $\partial = (0.05,0.2,0.35)$.

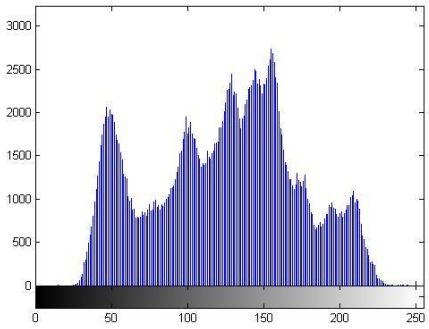
In the context of data hiding it is important to analyze the histograms of the image before and after the data hiding process. Figure 7 shows the histograms of original image and stego images after hiding data in bit planes 4, 5 and 6. We observe that bit planes 1-5 are suitable to insert the hidden information as the histogram before and after hiding the data resemble each other. The histogram after hiding data in bit plane 6 shows tell-tale signs of image manipulation.



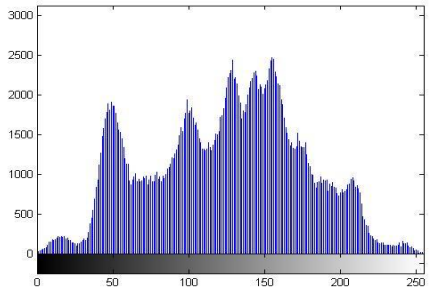
Histogram of original image



Hiding data in bit plane 4



Hiding data in bit plane 5



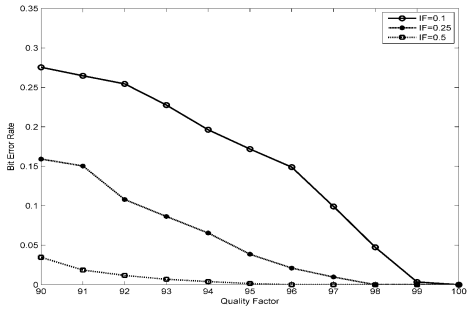
Hiding data in bit plane 6

Fig. 7. Histogram of original image and the histograms of stego images after hiding data in bit planes 4, 5 and 6($\partial = 0.1$).

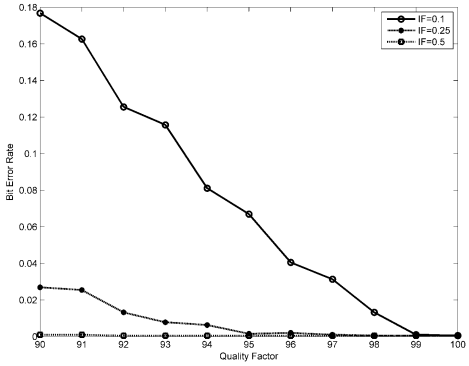
5 ROBUSTNESS AGAINST UNINTENTIONAL ATTACKS:

JPEG compression is a common unintentional attack in the context of image steganography. We tested the proposed algorithm against JPEG compression with compression quality 90-100.

Figure 8 shows that the proposed algorithm is able to resist this common unintentional attack to a certain level. It is also obvious here that algorithms that employ substitution of lower bits (1-3) will lose most of the hidden information under such unintentional attacks. Although it is important to have resistance againstcompression and other signal distortions, it is essential for a steganography application to have very good imperceptibility.



bit plane 4



bit plane 5

Fig. 8. JPEG compression for bit planes 4 and 5 for $(IF) = 0.1, 0.25$ and 0.5.

6 CONCLUSION

The art of hiding secret information requires selecting the optimal location to insert the secret information for a particular application. The current work is a step forward in the direction of finding the best bit planes to insert the hidden information in a chaotic manner. Bit plane 4 and 5are the most optimumaccording to our tests and analysis. The proposed algorithm shows good PSNR values when compared with similar approaches found in the literature. The algorithm is best suited for a scenario where high invisibility is sought with resistance to common unintentional attacks like JPEG compression.

7 REFERENCES:

[1] V. Nagaraj, V. Vijayalakshmi, and G. Zayaraz. In: Overview of Digital Steganography Methods and Its Applications. Int. J. Adv. Sci. Technol., vol. 60, pp. 45–58, 2013.

[2] D. Bandyopadhyay, K. Dasgupta, J. K. Mandal, and P. Dutta. In: A Novel Secure Image Steganography Method Based on Chaos Theory in Spatial Domain. Int. J. Secur., 2014.

[3] E. Ghasemi, J. Shanbehzadeh, and N. Fassihi. In: High capacity image steganography using wavelet transform and genetic algorithm. Proceedings of international multiconference of engineers and computer scientists, vol. 1, pp. 16–18, 2011.

[4] A. Nag, S. Ghosh, S. Biswas, D. Sarkar, and P. P. Sarkar. In: An image steganography technique using X-box mapping. International Conference on Advances in Engineering, Science and Management (ICAESM), pp. 709–713, 2012.

[5] B. S. and K. L. Sudha. In: Text Steganography using LSB insertion method along with Chaos Theory. ArXiv12051859 Cs, May 2012.

[6] A. M. Al-Shatnawi. In: A new method in image steganography with improved image quality. Appl. Math. Sci., vol. 6, no. 79, pp. 3907–3915, 2012.

[7] H.-W. Tseng and C.-C. Chang. In: High capacity data hiding in JPEG-compressed images. Informatica, vol. 15, no. 1, pp. 127–142, 2004.

[8] F. Li, X. Zhang, J. Yu, and W. Shen. In: Adaptive JPEG steganography with new distortion function. Ann. Telecommun. - Ann. Télécommunications, vol. 69, no. 7–8, pp. 431–440, Aug. 2014.

[9] S. Sarreshtedari and S. Ghaemmaghami. In: High Capacity Image Steganography in Wavelet Domain. in 2010 7th IEEE Consumer Communications and Networking Conference (CCNC, pp. 1–5), 2010.

[10] S. Hemalatha, U. D. Acharya, A. Renuka, and P. R. Kamath. In: A secure and high capacity image steganography technique. Signal Image Process. Int. J. SIPIJ Vol, vol. 4, pp. 83–89, 2013.

[11] D. E. Walia, P. Jain, and N. Navdeep. In: An Analysis of LSB & DCT based Steganography. Glob. J. Comput. Sci. Technol., vol. 10, no. 1, May 2010.

[12] X. Zhang. In: Reversible Data Hiding in Encrypted Image. IEEE Signal Process. Lett., vol. 18, no. 4, pp. 255–258, Apr. 2011.

[13] S. Alam, V. Kumar, W. . Siddiqui, and M. Ahmad. In: Key Dependent Image Steganography Using Edge Detection. Fourth International Conference on Advanced Computing Communication Technologies (ACCT), pp. 85–88, 2014.

[14] W.-J. Chen, C.-C. Chang, and T. H. N. Le. In: High payload steganography mechanism using hybrid edge detector. Expert Syst. Appl., vol. 37, no. 4, pp. 3292–3301, Apr. 2010.

[15] W. Luo, F. Huang, and J. Huang. In: Edge adaptive image steganography based on LSB matching revisited. Inf. Forensics Secur. IEEE Trans. On, vol. 5, no. 2, pp. 201–214, 2010.