International Journal of Applied Engineering and Technology ISSN: 2277-212X (Online)
An Open Access, Online International Journal Available at http://www.cibtech.org/jet.htm
2017 Vol. 7 (2) April-June, pp.1-6/Singh and Kaur

Research Article

IMPROVED LSB TECHNIQUE FOR IMAGE STEGANOGRAPHY IN TRUE COLOR

***Prabhjot Singh and Maninder Kaur**
Department of Diet, Kharar, Mohali Punjab India
**Author for Correspondence*

ABSTRACT

Information embedding in red, green and blue color channel in an image has found enormous potential in image steganography. As the three channels increase the image embedding capacity three folds by virtue of three image color matrix, therefore, the image entropy and PSNR are improved a lot. In the presented work, the secret message is embedded in all three color component part of the host image. The secret message is converted into binary sequence and each bit is xored with R-component pixel value. The resultant xor value is used to manipulate the R-, G- and B-component images for binary sequence insertion. The inverse of the process is used to extract the inserted code from the stego image. The PSNR, entropy, standard deviation and variance are used to evaluate the performance of the algorithm.

Keywords: *Entropy, PSNR, MSE, SD*

INTRODUCTION

Steganography is an ancient art of hiding information. Digital technology gives us new ways to apply steganography techniques, including one of the most intriguing that of hiding information in digital images.

Steganography and encryption are both used to ensure data confidentiality. This is the same case as we have some ornaments hiding in our house so that it is out of reach of theft. However, when the ornaments are stored in a lock room, they are protected declared. And when there is some tag over the ornaments, then it is claimed to be possessed. Steganography and cryptography bear very thin line difference in the spy craft family. Cryptography scrambles a message so it cannot be understood. Steganography hides the message so it cannot be seen. A message in cipher text, for instance, might arouse suspicion on the part of the recipient while an “invisible” message created with steganography methods will not.

Modern steganography goal is to keep its mere presence undetectable, but steganography systems because of their invasive nature leave behind detectable traces in the cover medium. Even if secret content is not revealed, the existence of it is: modifying the cover medium changes its statistical properties, so eavesdroppers can detect the distortions in the resulting stego medium’s statistical properties. The process of finding these distortions is called statistical steganalysis. There are different techniques for image steganography and includes Simple Watermarking, LSB Least Significant Bit Hiding (Image Hiding), Direct Cosine Transformation and Wavelet Transformation. Simple watermarking inserts the watermark image into host image with option of visible and invisible viewing. LSB uses the manipulation of least significant bit of the host image pixels in order to embed the message. DCT and wavelet transform uses frequency domain coefficients for embedding the secret messages.

Data is hidden in all three cases whether it is steganography, cryptography or encryption. However, in case of steganography, the data is hidden in the given host platform., in case of encryption, the data is made secured so that unauthorised person could not access the same and in case of water marking, the host material is of claiming nature by possessing the carrying watermark inside the host.

Related Works

There is continuous development in the area of image steganography for the last three decades and the new and efficient algorithms as per the application requirements were developed by different researchers. Bedi *et al.*, (2013) proposed that steganography techniques which are efficient, required to enhance the privacy for the information in digital format for the purpose of providing private data transmission. Moon and Raut (2013) introduced with main objective to hide an image and text behind a file. Suitable algorithm as 1 LSB, 2 LSB and 4 LSB method seem to be good for hiding more secret information. Hmood *et al.,* (2010) aimed for the purpose of evaluating the distortion occurring at the time of embedding. Yang and Weng (2008) told about a technique LSB that provides imperceptible stego images, along with the capacity at greater scale. Johnson (2003) focused on the place of Steganography in security. By using various Steganography methods, for hiding a message the likelihood of the private content to get noticed. In case, encryption is done, an extra protected layer is foreseen. Al-Hammami (2011) intended not only to analyse the hidden information, but also to detect it. Gutub *et al.,* (2010) aimed for presenting a method to hide small arabic texts within 2 covers: in the foremost there exhibits Arabic wording, in the later there exists an image. Zheng (2007) conveyed about the data that has been embedded into the host. It was suggested about the procedures which are adopted for achieving various sorts of discipline. Al-Ataby and Al-Naima (2010) stated the concept as the ability by which the private content that is sent from a source for some intention. Ibrahim *et al.,* (2011) proposed algorithm for hiding the information inside an image by using a technique named as Steganography. The advantage of having zip file can be considered prior to the conversion that is done for maximizing data storage in an image. Fazio *et al.,* (2014) specified that the steganography extension to the multi-recipient setting is foreseen. Broadcast Steganography enables a sender to communicate covertly with a dynamically designated set of receivers, such that the original information file was retrieved by the desirable recipient or user, and also the unauthorized users and outsiders remain unaware of the communication being performed. Jana *et al*., (2013) proposed a new approach by the use of a 2-d Cellular Automata image steganography for reliable information content. Singh and Singh (2015) suggested the least significant bit method for image steganography based on modifications in green and blue color channel by taking red color channel lsb.

Proposed Steganography Algorithm

The proposed algorithm for hiding secret message in an input image (JPEG format) is implemented in following steps:

- Read Input Image (host image) and Secret message file
- Decomposition of input image into red, green and blue color component images
- Conversion of secret message into binary form
- Sequencing each character (binary form) of message in single column matrix (array)
- Get the length of the binary array (character) or no. of bits to be embedded in Host image
- Generate the random locations in host image equal in no. of bits to be embedded.
- Generate the two LSBs of first location pixel from
- red component image and XOR with first bit of image to be embedded.
- If the XOR result is '00' or '11', then exchange the red component pixel with bits to be embedded.

If XOR (R_{LSB} , MB) = 00
OR
If XOR (RLSB , MB) = 11
Then, R_{LSB} = MB
Where, MB = Message Bit.

- If the XOR result is '01', then, exchange the green component pixel with bits to be embedded.

If XOR (R_{LSB} , MB) = 01
Then, G_{LSB} = MB
Where, MB = Message Bit.

- If the XOR result is '10', then exchange the blue component pixel with bits to be embedded.

If XOR (R_{LSB} , MB) = 10
Then, B_{LSB} = MB
Where, MB = Message Bit.

- Concatenate the R-, G- and B-component images to get stego image.

Stego Image = CAT (3, R, G, B)

- Evaluate the performance indices mean square error, peak signal to noise ratio, entropy, standard deviation, variance and mean intensity.

Code Extraction

The inserted code is extracted by taking the stego image as input image. The same is spitted into its R-, G- and B-color constituents. The key file is used to get the stego coordinates and xor value. The stego coordinates and xor value are used to get the R-, G-, and B-constituents color information to get back the least significant bit (LSB) in order to convert the binary sequence into ASCII code. This is the message that was embedded using least significant bit.

RESULTS AND DISCUSSION

The proposed algorithm has been tested using RGB or jpeg format image as the host image and the binary bits extracted from text file. The experiment was taken by using three different code word length as 10, 20 and 30. The three different host images were used for insertion of the code word. The embedding process in red, green and blue color channel gives strong image steganography degree. The results are summarized in blow tables and show a fair performance while embedding the code word.

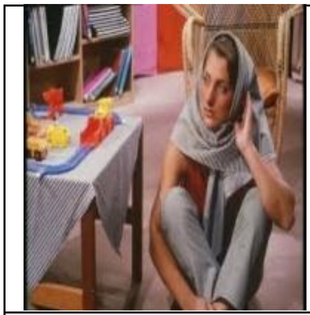
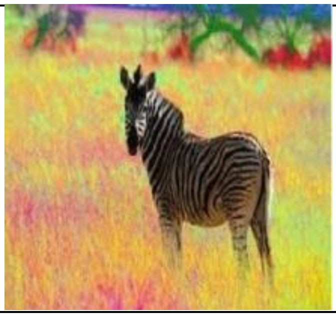
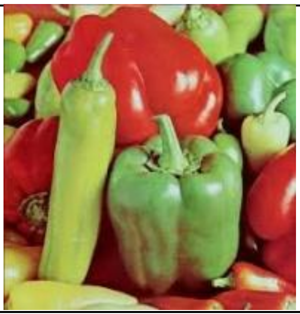
		

Figure 1	**Figure 2**	**Figure 3**

(Figure 1 to 3 - Host Images)

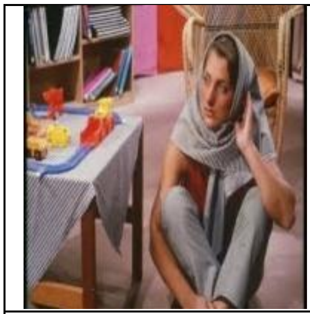
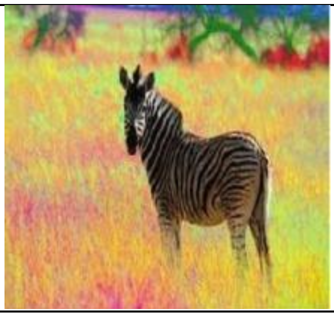
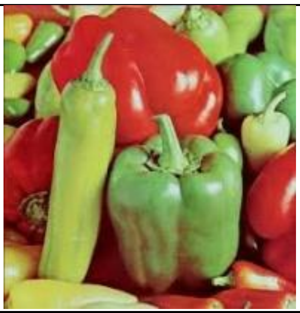
		

Figure 4	**Figure 5**	**Figure 6**

(Figure 4 to 6 - Stego Images at Message Length = 10)

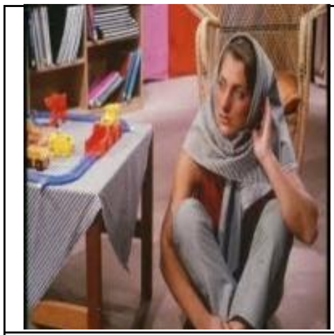
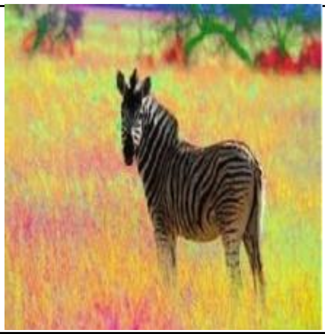
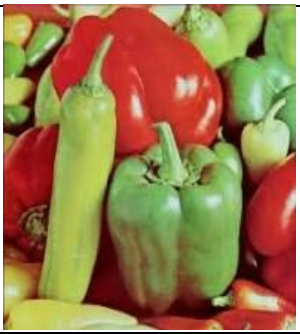
		

Figure 7	**Figure 8**	**Figure 9**

(Figure 7 to 9 - Stego Images at Message Length = 20)

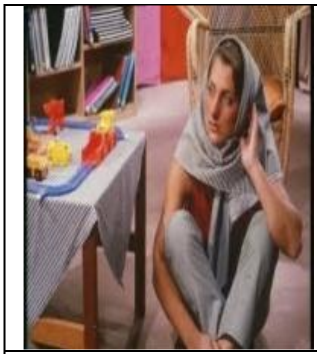
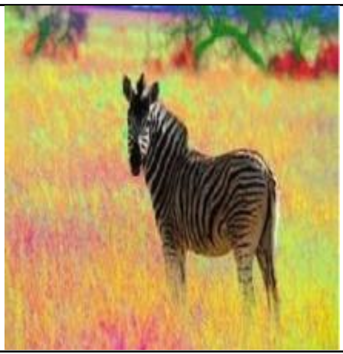
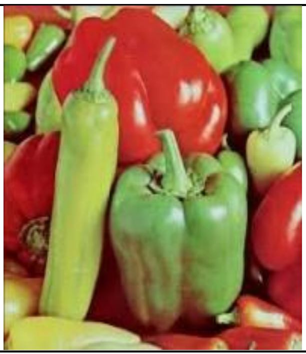
		

Figure 10	**Figure 11**	**Figure 12**

(Figure 10 to 12 - Stego Images at Message Length = 30)

Message Length = 10

Figure No.	**Steganography using Proposed Algorithm**			
	MSE	**PSNR**	**Entropy**	**Mean I.**
Figure 1	0.001023	77.966	7.561	120.592
Figure 2	0.000242	85.777	6.326	108.341
Figure 3	0.001300	77.873	7.087	123.098

Message Length = 20

Figure No.	**Steganography using Proposed Algorithm**			
	MSE	PSNR	Entropy	Mean I.
Figure 1	0.000778	80.320	7.335	118.902
Figure 2	0.000166	85.114	6.825	83.601
Figure 3	0.000889	80.204	7.009	131.223

Message Length = 30;

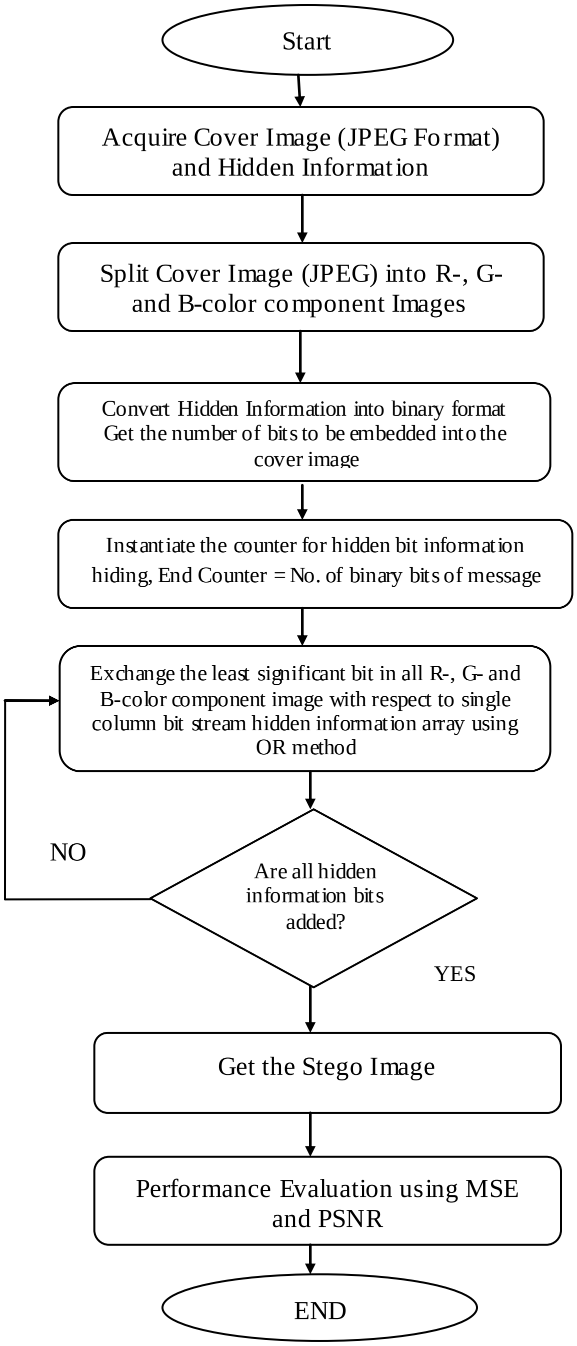
Figure No.	**Steganography using Proposed Algorithm**			
	MSE	PSNR	Entropy	Mean I.
Figure 1	0.000514	80.241	7.627	119.888
Figure 2	0.000112	83.600	6.908	121.983
Figure 3	0.000609	81.213	7.221	132.267

Conclusion

The least significant bit modification in host image in order to embed the message bits in red, green and blue channel using the xor method has been proved to be an effective tool for image steganography. Different images with different codes and lengths are used for robust testing of the algorithm.

The result table shows the performance of the algorithm in terms of MSE, PSNR, Entropy and means intensity.

The performance measures are evaluated using the PSNR and entropy of the stego image. Higher is PSNR, better is the secret code embedding. However, lesser is the difference in entropy of stego and host, better is the secret code embedding.


Start
Acquire Cover Image (JPEG Format) and Hidden Information
Split Cover Image (JPEG) into R-, G- and B-color component Images
Convert Hidden Information into binary format Get the number of bits to be embedded into the cover image
Instantiate the counter for hidden bit information hiding, End Counter = No. of binary bits of message
Exchange the least significant bit in all R-, G- and B-color component image with respect to single column bit stream hidden information array using OR method
Are all hidden information bits added?
NO
YES
Get the Stego Image
Performance Evaluation using MSE and PSNR
END

REFERENCES

Al-Ataby A and Al-Naima F (2010). A Modified High Capacity Image Steganography Technique Based on Wavelet Transform. *International Arab Journal of Information Technology* **7**(4).

Al-Htammami M (2011). A proposed Modified Data Encryption Standard algorithm by using Fusing Data Technique. *World of Computer Science and Information Technology Journal* **1**(3) 88-91.

Bedi P, Bansal R and Sehgal P (2013). Using PSO in a spatial domain based image hiding scheme with distortion tolerance. *Computers and Electrical Engineering* **39** 640-654.

Fazio N, Nicolosi AR and Perera IM (2014). Broadcast Steganography. In: Benaloh J. (edition) *Topics in Cryptology-CT-RSA 2014. CT-RSA 2014, Lecture Notes in Computer Science,* **8366** Springer, Cham.

Gutub AAA, Al-Alwani W and Mahfoodh AB (2010). Improved method of arabic text steganography using the extension 'Kashida' character. *Bahria University Journal of Information and Communication Technologies* **3**(1).

Hmood AK, Kasirun ZM, Jalab HA, Alam GM, Zaidan AA and Zaidan BB (2010). On the accuracy of hiding information metrics. *International Journal of the Physical Sciences* **5**(7) 1054-1062.

Ibrahim R (2011). Steganography Algorithm to hide Secret Message inside an image. *Computer Technology and Application* **2** 102-108.

Jana B, Giri D, Mondal SK, Pal P (2013). Image Steganography based on Cellular Automata. *International Journal of Pure and Applied Mathematics* **83**(5) 701-715.

Johnson N (2003). Eliminating Steganography in Internet Traffic with active wardens", In *Proceedings of the 5th International Workshop on Information Hiding, Noordwijkerhout, Netherlands,* Springer.

Moon SK and Raut RD (2013). Analysis of Secured Video Steganography Using Computer Forensics Technique for Enhance Data Security. *IEEE Second International Conference on Image Information Processing (ICIIP 2013).*

Singh AP and Singh H (2015). An Improved LSB based Image Steganography Technique for RGB Images. *IEEE International Conference on Electrical, Computer and Communication Technologies (ICECCT)* 1-4.

Yang C-H and Weng C-Y (2008). Adaptive Data Hiding in Edge Areas of Images with Spatial LSB Domain Systems. *IEEE Transactions on Information Forensics and Security* **3**(3).

Zheng L (2007). Ingemar J Cox, "JPEG based conditional entropy coding for correlated steganography. *IEEE International Conference on Multimedia and Expo*.