Indian Journal of Science and Technology, Vol 9(45), DOI: 10.17485/ijst/2016/v9i45/106483, December 2016
ISSN (Print) : 0974-6846
ISSN (Online) : 0974-5645

Image Steganography in RGB Color Components using Improved LSB Technique Image Pattern Compression using Weighted Principal Components Algorithm

Pooja Jain* and Navdeep Kanwal

Punjabi University, Patiala – 147002, Punjab, India; poojajain6556@gmail.com, navdeepkanwal@gmail.com

Abstract

Steganography is age old method employed to send/share secret information or message to/with the recipient. The hidden information is extracted at the recipient end by using some key. With the advent of internet as communication media, steganography has appeared in the form of digital image steganography with wide spread advancements. Hiding information in Least Significant Bit (LSB) of the host image pixels is one of the most popular methods. In the presented work, an improved LSB technique for textual message embedding is discussed. All three color channels space is used to embed the secret code. Simply manipulating only Least Significant Bit of the pixel is not safe for information hiding and vulnerable to attacks. Therefore, the information is embedded in all three color channels i.e. red, green and blue of the host image by ex-oring of the information bit and pixel bit. The secret message is converted into binary sequence and each bit is xored with R-component pixel value of host image. The resultant xor value is used to manipulate the R-, G- and B-component images for binary sequence insertion to get the stego image. The inverse of the process is used to extract the inserted code from the stego image. The PSNR, entropy, standard deviation and variance for host and stego images are used to evaluate the performance of the algorithm. Utilizing the three color channel enhances the hiding area for the host image three folds. The presented work allows three folds space in host image to embed as many textual information.

Keywords: Entropy, MSE, PSNR, SD

1. Introduction

1.1 Steganography

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[1].

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 wills not[2]. The hidden data can be detected by using the inverse algorithm with even accuracy and repeatability.

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

*Author for correspondence

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[3]. 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 unauthorized 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.

2. 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[1]. It was proposed that the techniques which are efficient, required to enhance the privacy for the information in digital format for the purpose of providing private data transmission. It was introduced with main objective to hide an image and text behind a file. Suitable algorithm as LSB method seems to be good for hiding more secret information[2–4]. Told about a technique LSB that provides imperceptible stego images, along with the capacity at greater scale. The place of steganography in security was focused in length here 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[5]. The algorithm was intended not only to analyze the hidden information, but also to detect it[6]. It is 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[7]. They conveyed about the data that has been embedded into the host[8]. It was suggested about the procedures which are adopted for achieving various sorts of discipline[9]. It was stated the concept as the ability by which the private content that is sent from a source for some intention[10]. They 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[11]. It was 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[12]. They discussed a new approach by the use of a 2-d Cellular Automata image steganography for reliable information content[13]. The Least Significant Bit method was described for image steganography based on modifications in green and blue color channel by taking red color channel LSB.

3. 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) = 10.
OR
If XOR (R_{LSB}, 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) = 00.
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.

4. 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.

5. 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 lengths 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.

Message Length = 10;
Respective Stego Images: Figures 4, 5 and 6.
Message Length = 20;
Respective Stego Images: Figures 7, 8 and 9.
Message Length = 30;
Respective Stego Images: Figures 10, 11 and 12.


Figure 1.


Figure 2.


Figure. 3.

(Figures 1 to 3 → Host images).


Figure 4.


Figure 5.


Figure 6.

(Figures 4 to 6 →Stego images at message length = 10).


Figure 7.


Figure 8.


Figure 9.

(Figures 7 to 9 →Stego images at message length = 20).


Figure 10.


Figure 11.


Figure 12.

(Figures 10 to 12 →Stego images at message length = 30).

Table 1. Results at message length = 10

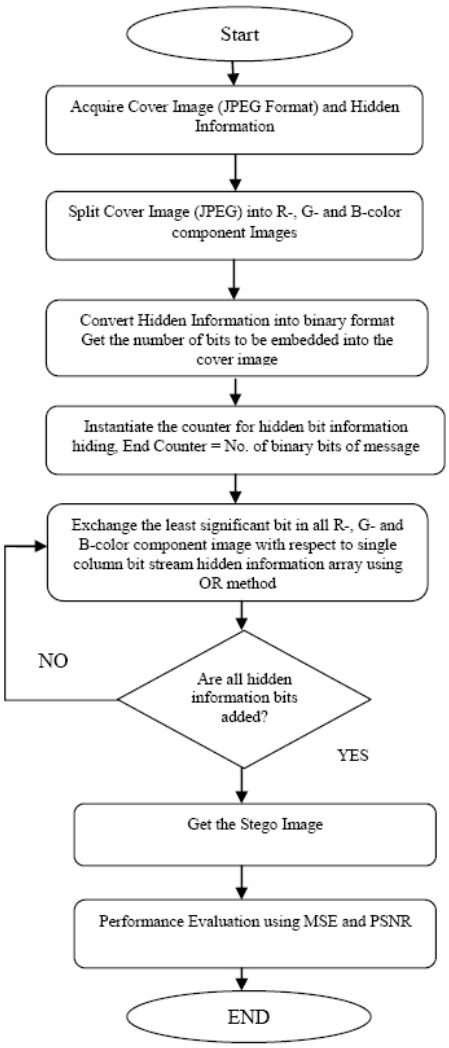
Figure No.	Steganography using Proposed Algorithm			
	MSE	PSNR	Entropy	Mean I.
Figure 1	0.001323	76.956	7.607	119.522
Figure 2	0.000222	84.697	6.926	84.621
Figure 3	0.001200	77.371	7.152	130.248

Table 2. Results at message length = 20

Figure No.	Steganography using Proposed Algorithm			
	MSE	PSNR	Entropy	Mean I.
Figure 1	0.000756	79.380	7.607	119.523
Figure 2	0.000163	86.044	6.926	84.621
Figure 3	0.000989	78.214	7.152	130.248

Table 3. Results at message length = 30

Figure No.	Steganography using Proposed Algorithm			
	MSE	PSNR	Entropy	Mean I.
Figure 1	0.000504	81.141	7.607	119.523
Figure 2	0.000104	84.621	6.926	119.523



6. 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. The PSNR more than 70 proves the efficiency of the algorithm when tested at different word length message 10, 20 and 30. 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 and Entropy and mean 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. There is almost no change in entropy between the host and stego image and hence secure is the hidden text message.

7. References

1. Bedi P, Bansal R, Sehgal P. Using PSO in a spatial domain based image hiding scheme with distortion tolerance. Elsevier Springer. 2013 Feb; 39(2):640–54.
2. Moon SK, Raut RD. Analysis of secured video steganography using computer forensics technique for enhance data security. IEEE; 2013.
3. Hmood AK, Kasirun ZM, Jalab HA, Alam GM, Zaidan AA, Zaidan BB. On the accuracy of hiding information metrics: Counterfeit protection for education and important certificates. International Journal of the Physical Sciences. 2010 Aug; 5(7):1054–62.
4. Yang CH, Weng CY. Adaptive data hiding in edge areas of images with spatial LSB domain systems. IEEE Transactions on Information Forensics and Security. 2008 Sep; 3(3):488–97.
5. Johnson N. Eliminating steganography in internet traffic with active wardens. Springer; 2003.
6. Al-Htammami M. A proposed modified data encryption standard algorithm by using fusing data technique. WCSIT. 2011; 1(3):88–91.
7. Gutub AAA, Al-Alwani W, Mahfoodh AB. Improved method of Arabic text steganography using the extension Kashida' character. BUJICT. 2010 Dec; 3(1):68–72.
8. Zheng L, Cox IJ. JPEG based conditional entropy coding for correlated steganography. IEEE; 2007.
9. Al-Ataby A, Al-Naima F. A modified high capacity image steganography technique based on wavelet transform. International Arab Journal of Information Technology. 2010 Oct; 7(4):358–64.
10. Ibrahim R. Steganography algorithm to hide secret message inside an image. Computer Technology and Application. 2011 Feb: 102–8.
11. Fazio N, Nicolosi AR, Perera IM. Broadcast steganography. Springer. 2014; 8366:64–84.
12. Jana B, Giri D, Mondal SK, Pal P. Image steganography based on cellular automata. IJPAM. 2013; 83(5):701–15.
13. Singh AP, Singh H. An improved LSB based image steganography technique for RGB images. IEEE; 2015. p. 1–4.