International Journal of Current Engineering and Technology
E-ISSN 2277 – 4106, P-ISSN 2347 – 5161

Available at http://inpressco.com/category/ijcet

Research Article

An Improved LSB based Image Steganography for Grayscale and Color Images

Raju†* and Mohit Dhanda†

†Electronics and Communication Engineering Department, GNI, Mullana, India

Accepted 30 Sept 2015, Available online 02 Oct 2015, **Vol.5, No.5 (Oct 2015)**

Abstract

In this paper a LSB based technique is proposed for steganograpgy. This technique is targeted for digital images that are commonly used as a cover medium or carrier for hiding information. This technique is different from standard LSB technique that along with message hidden in LSB bits a part of message also resides at selective bits using a key. Also the key used for this selective implementation is used from the image itself. Finally the PSNRare computed to ensure the successful implementation of the proposed algorithm.

Keywords: *LSB, steganography, Steganalysis, stego-key, PSNR*

Introduction

In a steganographic system the factor responsible for security is the message encoding mechanism. In today's digital communication scenario the involvement of digital devices like smart phones, laptops and tablets have unlocked tremendous opportunities in this field. As less number of least significant bits of cover image is altered in comparison to plain LSB method, improving the PSNR of stego image (Akhtar N, 2013).With the growth of multimedia devices the steganography techniques are also improving. The steganographic system leaves unique patterns on the cover images and these patterns defeats the steganalyst (Vanmathi C, 2013). New algorithms are developed to make efficient steganography tools (Nag A, 2011). There are other methods for Information Hiding algorithm that are based on lifting wavelet transform image (Li C, 2011). Least significant bit based steganography technique is among one of the simplest and most commonly used technique (Karim, S, 2011). Various other techniques have also been developed to serve the purpose. The objective always remains the same to increase the security of secret message and increased payload capacity of the carrier medium. Digital images are always targeted as a carrier medium for the secret message, the reason being digital images are a very common method of information exchange. Both grayscale and colored images can be used as a carrier object. The reliability of a steganography algorithm depends on how data is inserted in the cover object (Chandramouli, 2004). It should be invisible to the eyes of an eavesdropper.

*Corresponding author: **Raju**

Methodology

Least significant bit (LSB) insertion is a common and simple approach to embed information in an image file (Chan C K, 2004). In this method the LSB of a byte is replaced with message bits. This technique proposed method is shown in fig-1. To the human eye, the resulting image will look identical to the cover object. The uniqueness in the algorithm is that the key is contained in the image itself and there is no need to send this key separately only the receiver knows this and he can decode the message.

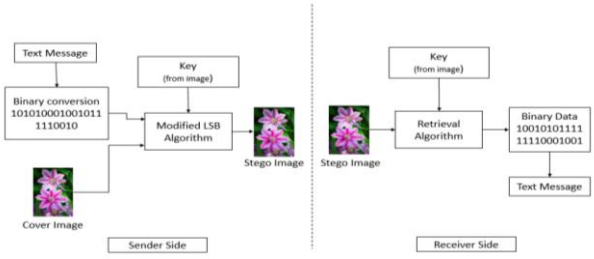


Fig.1 A model of proposed steganographic process

In this proposed method, the difference lies in the LSB replacement depending upon the key. The key used in the operation is derived from the cover image itself. The process remains same during the extraction of the image i.e. hiding and retrieving the text uses same rules. Steps used in proposed Improved LSB:

Hiding process

1. Find the pixel value of cover image.
2. Convert the image into binary data.

3. Find the value LSB of each pixels of cover image.
4. Obtain the secret text message.
5. Find the binary value of message to be hidden.
6. Select a valid key from the cover image data.
7. Generate the resultant *stego*-image.

Extracting process

1. Find the pixel value of *stego*-image.
2. Convert the image into binary extract the value of LSB from the *stego*-image.
3. Retrieve the LSB bits using the valid key generated from the cover image. .
4. Convert the binary data into text form to obtain the secret message.

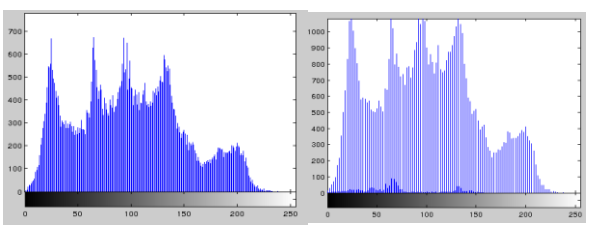
All the figures must be placed in the column wise, however the authors can use single column to place big figures provided that the template formatting must not change. The title of the figure is to be placed below the figures as shown.

Results

Least significant bit based steganography is among one of the commonly used methods for hiding data in images and other file formats. Proposed Algorithm was developed and implemented on a number of images. To analyze the changes introduced in the original image and the produced *stego*-image their histogram is generated. Further standard performance evaluation parameters like PSNR and MSE are also obtained and analyzed. Visually inspecting and comparing the stego-image with the original image there is no significant difference in both images. To judge the performance of the developed algorithm was first applied on grayscale image and the RGB images are also tested.

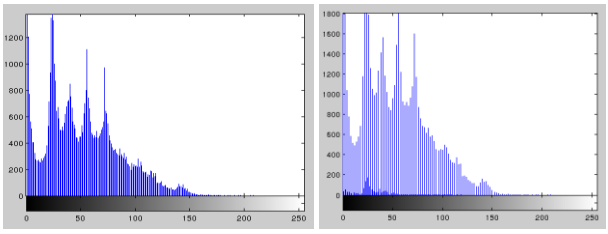
Grayscale and Color Image Results

(a) Original_leena (b) stego_leena



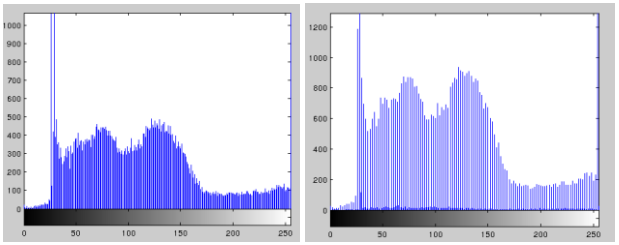
(a) Hist_Original_leena (b) Hist_stego_leena

(a) Original_movie (b) stego_movie

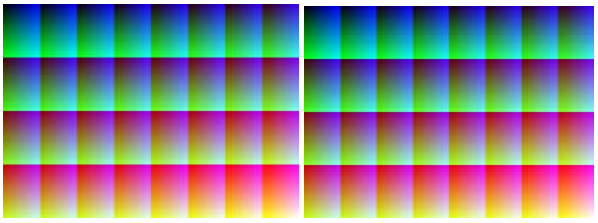


(a) hist_movie (b) hist_stego_movie

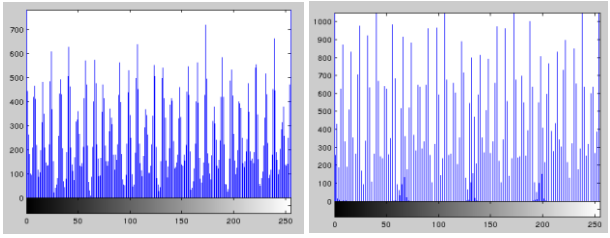
(a) Original_house (b) stego_house



(a) Hist_Original_house (b) Hist_stego_house



(a) Original_colours (b) stego_colours



(a)Hist_Original_colours (b) Hist_stego_colours

Table 1 MSE and PSNR

Sr. No	Cover Image	Secret Message	Stego Image	PSNR (dB)
1.	Leena	Text Message	leena_stego	48.996
2.	Movie	Text Message	Movie_stego	46.246
3.	Home	Text Message	Home_stego	39.534
4.	Colours	Text Message	Colours_stego	41.874

Conclusion

The proposed method has a unique feature that the key is contained in the image itself. The sender and the receiver are aware of this key. The developed algorithm is successfully applied on grayscale and RGB image sets. The results obtained are satisfactory. The output stego image is visually similar to the original image. Steganography using digital images is proposed due to the fact that, with the introduction of portable multimedia devices and smart phones exchange of digital images have increased tremendously. These digital images are best suitable for concealing information. The LSB based steganography technique is suitable for the covert communication when digital images are used as carrier object. The developed LSB method is capable of hiding text message in a cover object. The proposed system aims to overcome the shortcomings of the existing systems which aim at developing a more secure environment to carry out Image Steganography. This technique will provide the users a key that is already present in the original and steganographic image to encode and decode the secret message.

References

Akhtar N, (2013)PragatiJohri, Shahbaaz Khan, Enhancing the Security and Quality of LSB based Image Steganography, 5th *International Conference on Computational Intelligence and Communication Networks*, 978-0-7695-5069-5, pp-385-390.

Vanmathi C,(2013)Prabu S, A Survey of State of the Art techniques of Steganography, *International Journal of Engineering and Technology*, Vol 5, ISSN: 0975-4024.

Nag A, Singh,(2011) A Weighted Location Based LSB Image Steganography Technique, *Advances in Computing and Communications (ACC-2011), Conference Communications in Computer and Information Science*, Vol. 191, Springer-Verlag, Berlin, pp. 620–627.

Karim, S, (2011) M. I, A new approach for LSB based image steganography using secret key, *Computer and Information Technology (ICCIT)*, pp. 286-291.

Li C, (2011), Realization of a LSB Information Hiding algorithm Based on Lifting Wavelet Transform Image, *International Conference on Mechatronic Science, Electric Engineering and Computer*, pp.1015-1018.

Martin A, (2005), Is Image Steganography Natural, *IEEE transactions on Image Processing*, Vol.14, pp.2040-2050.

Hala Farouk, (2004), Design and implementation of a secret key steganographic micro architecture employing FPGA, Design, *Automation and Test in Europe Conference and Exhibition*, Proceedings, Vol.3, ISSN: 1530-1591, ISBN: 0-7695-2085-5, pp. 212-217.

Chandramouli,(2004), Image steganography and steganalysis: Concepts and practice, in *International Workshop on Digital Watermarking*, T. Kalker et al. (Eds.) LNCS Vol. 2939, Springer-Verlag, Berlin, pp. 35–49.

Chan C K, (2004), Hiding data in images by simple LSB substitution, *Pattern Recognition*, vol. 37, issue 3, pp 469-474.