5LSB Steganogaraphyusing Monotonic RGB Color Image as Cover Medium

Sahib Khan[#], Tawab Khan[*], Muhmmad Ismail[#], Muhmmad Haseeb Zafar[#], Rehan Ashraf[+], Nasir Ahmad[#]
[#] University of Engineering and Technology Peshawar, Peshawar, Pakistan
[*]Department of Mathematics, Abdul Wali Khan University Mardan, Mardan, Pakistan
[+] University of Engineering and Technology Taxila, Pakistan
engrsahib_khn@yahoo.com

***Abstract*—This work presents new least significant bits based steganography technique to embed secret information in the five least significant bits of single channel out of three primary channels of RGB color image, at a time. The 5 least significant bits (5LSB) substitution technique make use of these individual channels as cover media and hide secret information in either red (R), green (G) or blue (B) channels of color image, taking one at time and leaving other channels unaltered. It has been observed that data hiding in the 5LSB of these channels doesn't create any visually significant distortion and doesn't attract the attention of eavesdroppers. The experimental results show that hiding information in blue channel provides significantly good visual quality of stego images than other two channels. While, hiding data in green channel create more distortion. The 5LSB steganography result in PSNR values larger than the threshold value of 30 dB for R and B channels of RGB color image, while, PSNR value for G channel is below the threshold of 30dB.**

Keywords—4 LSB Steganography; RGB;Color Image; HVS; Steganalysis.

I. INTRODUCTION

The traces of the use of Steganography can be found back in 440 BC, when the tablet and a tattoo on the shaved head of slave were used to send tale of Demaratus, as mentioned by Herodotus in the Histories of Herodotus [1], [2]. Data hiding also called Steganography is the area of information security used to hide secret messages in cover media i.e. image, audio, video etc. Due to the presence of high level of redundant bits image got more attraction and are greatly experimented for information hiding [3]. The main aim of Steganography is to conceal secret information in such a way that their existences remain blind. For this to achieve information are usually hidden by replacing the least significant bits (LSB) of cover image with secret message bits. 4 least significant bits (4LSB) is one such technique used to substitute the 4LSB of each pixel of cover with secret message bits [4].

Data hiding in images faces a variety of challenges that arise due to the modification in cover image. The human visual system (HVS) is very sensitive to the change made in cover image especially to the changes in smooth regions. The other challenge is the limited hiding capacity; each cover image has capability of hiding a limited message data. To enhance hiding capacity and keeping distortion in acceptable range is the main aim of each Stegnaographer to achieve.

Various researchers proposed different Steganographic techniques; exploiting images (color and gray scale) for data hiding both in spatial domain and transform domain. To hide message in gray scale image various Steganographic method were implemented. These methods include 4 LSB Steganography [4], VLSB Steganography [5, 6], Data hiding in Edges [7, 8] and others. Along with spatial domain technique, researchers also made use of different transform for data hiding [9]. Discrete Cosine Transform (DCT) [10, 11] and wavelet transform [12, 13]. While, using color images as cover, Liu and Liao [14], proposed a high-performance JPEG Steganographic method capable to resist statistical attacks. Tong and Ding [15] implemented a quantized based color image Steganographic method. Crandall investigated that coding technique can improve the hiding efficiency and proposed a matrix coding [16]. Fridrich and Soukal [17] proposed an enhanced payload matrix embedding technique. The relation of covering and Steganographic codes was studies in [18]. It revealed that covering code define the stego code [18].

In this paper color image channels are experimented for data hiding and the effect of LSB substitution on each is analyzed. This paper is arranged further in different sections. Section II, discusses the implementation of proposed scheme of data hiding. Section III, presents the experimental results and discusses the effects of data hiding in each channel. Final section concludes the proposed work.

II. IMPLEMENTATION

A color image, 24bits format, consists of three individual channels i.e. red, green and blue. To form a color with RGB, three light beams (one red, one green, and one blue) must be superimposed. To hide secret data in the individual channels of RGBcolor using 5LSB steganography, the cover image is separated in its three basic channels, each represented in 8bits, with 255 different shades of each primary color.

To hide data in R-channel of RGB color image, the R channel is extracted at the first. Then, R-channel is subjected to LSB substitution, using 5LSB steganography the five least significant bits of R-channel elements are replaced with 5bits of secret message. While, the G-channel and B-channel are lift unaffected. The modified R-channel and the unaltered G and B channels are combined to make a colorstego image. The quality of stego image is compared with the original cover image by calculating mean square error (MSE) and peak signal to noise ratio (PSNR).

978-1-5090-2000-3/16/$31.00 ©2016 IEEE

To use G-channel for embedding secret information, the G-channel is separated from R and B channels of original cover image. Then, G-channel is processed to hide information using LSB substitution. The 5LSB steganography technique replaces the five least significant bits of G-channel elements with 5bits of secret message. While, the R-channel and B-channel remain unaltered. The modified G-channel with hidden information and the unchanged R and B channels are united to make a colorstego image.

In the similar way, B-channel is used ft embedding secret message in its five least significant bits using 5LSB steganography. The data hiding in least significant bits create some variations in the image. The quality of image should not distort enough to attract the attention of eavesdropper. To measure the quality of resulted stego image MSE and PSNR are used as measuring parameters. The implementation process of 5LSB steganography using single channel of RGB image as cover media is shown here in Fig 1.

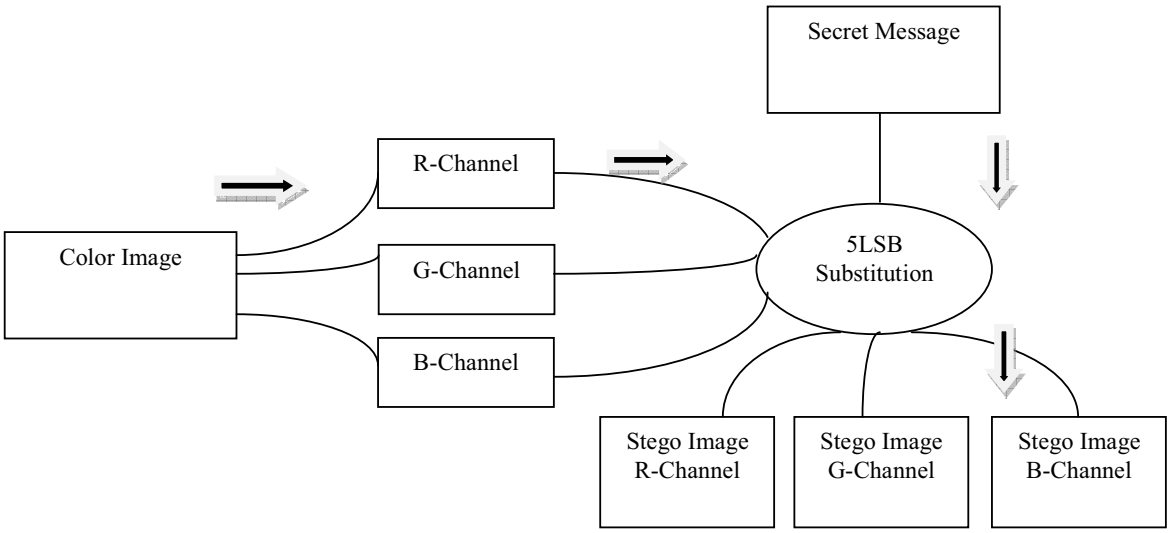


Fig. 1. Data hiding in R, G and B channels of color image

III. Experimental Results

TheAs color image consist of three primary colors i.e. red, green and blue, all the channels can be used as cover to hide secret message. To hide secret message in red, green and blue channel a color image is used as cover as shown in Fig 2. The color cover image is divided in its primary color components as show in Fig 3. Then each color channel is exposed to 4LSB substitution individually. The 4 least significant bits of each element of color channel under process are replaced with 4 bits of message bits. The stego images are obtained for each modified channels. The Fig 4(a), (b) and (c) show the stego image of hiding message in R-channel, G-channel, and B-channel respectively. The MSE and PSNR are used to determine the quality of stego-image as given by expression (1) and (2), respectively.

$$\text{MSE} = \frac{\sum_{i=1}^{r}\sum_{j=1}^{c}(\text{Cover}(i,j)-\text{Stego}(i,j))^2}{r*c} \quad (1)$$

$$\text{PSNR} = 10\log_{10}\frac{255^2}{\text{MSE}} \quad (2)$$

The MSE, SNR, PSNR and hiding capacity for each channel is listed in Table I.

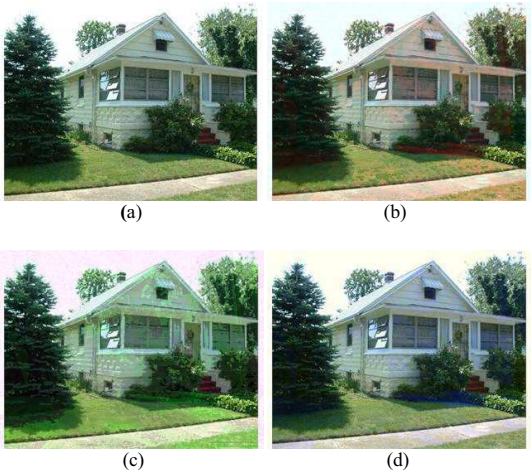
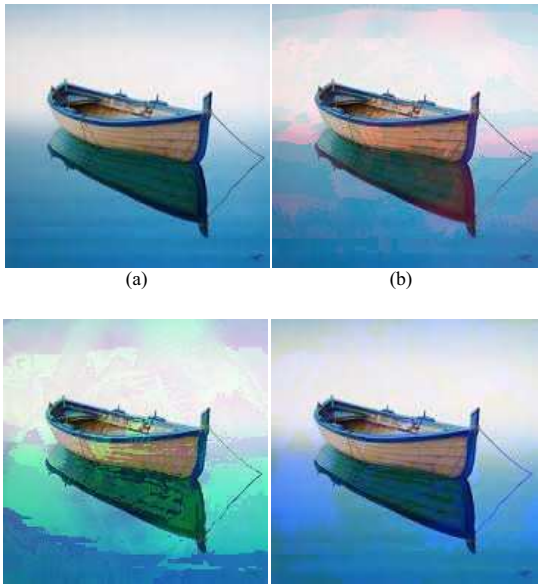


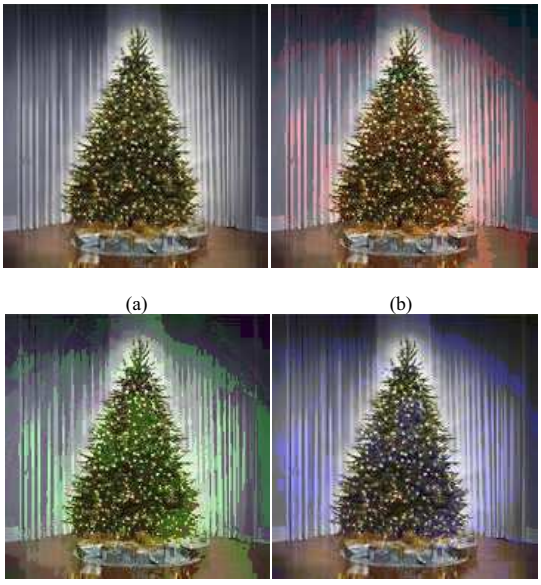
Fig. 2. House (a) Cover Image, (b) Red channel Stego Image, (c) Green channel Stego Image, (d) Blue channel Stego Image



(a) (b)

(c) (d)

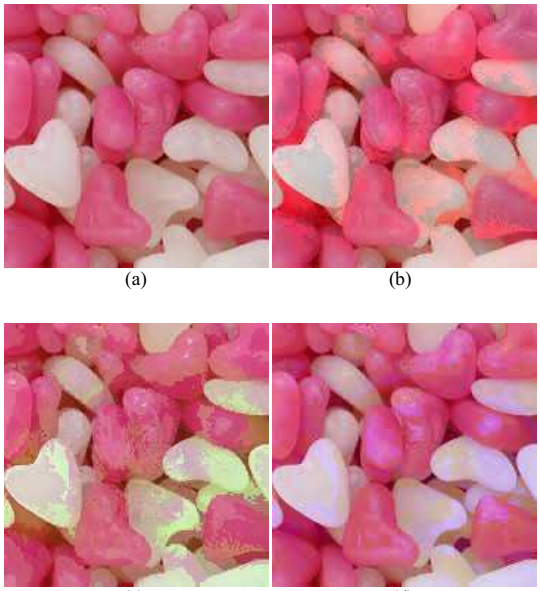
Fig. 3. Boat (a) Cover Image, (b) Red channel Stego Image, (c) Green channel Stego Image, (d) Blue channel Stego Image



(a) (b)

(c) (d)

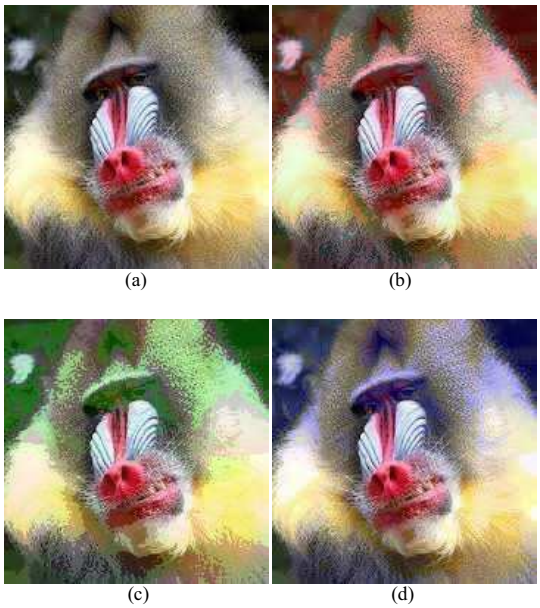
Fig. 4. Tree (a) Cover Image, (b) Red channel Stego Image, (c) Green channel Stego Image, (d) Blue channel Stego Image



(a) (b)

(c) (d)

Fig. 5. Jelly bean (a) Cover Image, (b) Red channel Stego Image, (c) Green channel Stego Image, (d) Blue channel Stego Image



(a) (b)

(c) (d)

Fig. 6. Mandrill (a) Cover Image, (b) Red channel Stego Image, (c) Green channel Stego Image, (d) Blue channel Stego Image

The experimental results shows that hiding information in the least significant bits using 5LSB steganography generate significant results for R and B channels. Stego images of both these channels display high quality and give PSNR value above the threshold value i.e. 30dB. While the G-channel produces visually significant distortion in stego images and the PSNR is also very low i.e. below 30dB.

Table I. PSNR, SNR, MSE of 5LSB Steganography for R, G and B channels

S. No	Cover Image	Hiding Capacity (%)	MSE R-Channel	PSNR (dB) R-Channel	MSE G-Channel	PSNR (dB) G-Channel	MSE B-Channel	PSNR (dB) B-Channel
1	House	20.83	60.3215	30.3326	739.4608	19.4417	23.6445	34.3935
2	Boat	20.83	50.6143	31.0881	292.2293	23.4736	12.4839	37.1673
3	Tree	20.83	64.6916	30.0223	252.0380	24.1161	8.6584	38.7565
4	Jelly bean	20.83	62.7524	30.1545	291.4282	23.4855	17.5680	35.6836
5	Mandrill	20.83	64.5700	30.0305	276.5333	23.7133	10.5355	37.9043

IV. CONCLUSION

The 5LSB steganography is an efficient hiding technique using 5 least significant bits of one individual channels of RGB color image at a time as cover medium. This creates a high quality stego images with peak signal to noise ratio value up to 38dB for B-channel and 30dB for R-channel. While, G-channel is affected badly and creates visually significant distortion. Hence, 5LSB steganography is not applied suitable to apply on G-channel for information hiding. Comparing the effect of 5LSB substitution on individual channels, it is observed that blue channel is less sensitive to bits substitution mechanism and create less distortion in stego image than the other two channels. An overall hiding efficiency of 20.83% has been achieved by replacing the 5 LSB of one primary channel of RGB image. The changes made in stego images of all the channels are not detectable to human visual system (HVS) except G channel, which is affected significantly. In short targeting one channel of a color image for information hiding, using the proposed method, is good choice to be adopted and it can be used for application where the required hiding capacity is equal to or less than 20.83%.

REFERENCES

[1] R. J. Anderson, and F. A. Petitcolas, “On the limits of steganography,” Selected Areas in Communications, IEEE Journal on, 16.4 (1998): 474-481.

[2] N. F. Johnson, and S. Jajodia, "Exploring steganography: Seeing the unseen," Computer 31.2 (1998): 26-34.

[3] A. D. Ker, “Improved detection of LSB steganography in grayscale images,” In Information Hiding, (2004): 97-115. Springer Berlin Heidelberg.

[4] S. Khan, M. H. Yousaf, and J. Akram, “Implementation of Variable Least Significant Bits Stegnography using DDDB Algorithm,” International Journal of Computer Science Issues(IJCSI), 8.6 (2011): 292-296.

[5] S. Khan, and M. H. Yousaf, "Implementation of VLSB Stegnography Using Modular Distance Technique," Innovations and Advances in Computer, Information, Systems Sciences, and Engineering. Springer New York, (2013): 511-525.

[6] S. Khan, N. Ahmad, and M. Wahid, “Varying index varying bits substitution algorithm for the implementation of VLSB steganography,” Journal of the Chinese Institute of Engineers, 39.1 (2016): 101-109.

[7] S. Khan, et. al., "A secure true edge based 4 least significant bits steganography," in Emerging Technologies (ICET), 2015 International Conference on, (Dec. 2015): 1-4 doi: 10.1109/ICET.2015.7389227

[8] W. Luo, F. Huang, and J. Huang, “Edge adaptive image steganography based on LSB matching revisited,. Information Forensics and Security, IEEE Transactions on, 5.2 (2010): 201-214.

[9] S. Khan, et. al., “Implementation of Variable Tone Variable Bits Gray-Scale Image Stegnography Using Discrete Cosine Transform,” Journal of Signal and Information Processing, 4.4 (2013): 343-350.

[10] N. Kafri, and H. Y. Suleiman, “Bit-4 of frequency domain-DCT steganography technique,” In Networked Digital Technologies, 2009. NDT'09. First International Conference on (2009): 286-291, IEEE.

[11] D. Singla, and R. Syal, “Data Security Using LSB & DCT Steganography in Images,” International Journal Of Computational Engineering Research, 2 (2012: 359-364.

[12] K. B. Raja, K. R. Venugopal, and L. M. Patnaik, “High capacity lossless secure image steganography using wavelets,” In Advanced Computing and Communications, 2006. ADCOM 2006. International Conference on (2006): 230-235, IEEE.

[13] N. Cvejic, and T. Seppänen, “A wavelet domain LSB insertion algorithm for high capacity audio steganography,” In Digital Signal Processing Workshop, 2002 and the 2nd Signal Processing Education Workshop. Proceedings of 2002 IEEE 10th (2002): 53-55, IEEE.

[14] C. L. Liu, and S. R. Liao, “High-performance JPEG steganography using complementary embedding strategy,” Pattern Recognition, 41.9 (2008): 2945-2955.

[15] L. Tong, and Q. Zheng-Ding, “A DWT-based color image steganography scheme,” In Signal Processing, 2002 6th International Conference on, Vol. 2, (2002): 1568-1571, IEEE.

[16] R. Crandall, “Some notes on steganography,” Posted on steganography mailing list, (1998).

[17] J. Fridrich, and D. Soukal, “Matrix embedding for large payloads,” In Electronic Imaging, International Society for Optics and Photonics (2006): 60721W-60721W.

[18] J. Bierbrauer, and J. Fridrich, “Constructing good covering codes for applications in steganography,” In Transactions on data hiding and multimedia security III (2008): 1-22, Springer Berlin Heidelberg.