ResearchGate

See discussions, stats, and author profiles for this publication at: https://www.researchgate.net/publication/313809353

An improved color image steganography technique in spatial domain

Conference Paper · December 2016

DOI: 10.1109/ICECE.2016.7853987

CITATIONS
5

READS
108

3 authors, including:

Saikat Mondal
Khulna University
11 PUBLICATIONS **23** CITATIONS
SEE PROFILE

Rameswar Debnath
Khulna University
25 PUBLICATIONS **275** CITATIONS
SEE PROFILE

Some of the authors of this publication are also working on these related projects:

Academic Thesis View project

PredictRisk View project

All content following this page was uploaded by Saikat Mondal on 17 July 2018.

The user has requested enhancement of the downloaded file.

An Improved Color Image Steganography Technique in Spatial Domain

Saikat Mondal, Rameswar Debnath, Borun Kumar Mondal
Computer Science and Engineering Discipline, Khulna University
Khulna-9208, Bangladesh
saikatcsebd@gmail.com

Abstract—**Steganographic techniques are used to transmit secret information using a carrier file without visibility during communication. In this paper, we proposed an improved RGB image steganographic technique for secured communication between two authorized parties. This technique embeds the information within 2nd to 8th bit position of blue (B) or green (G) component or both of a pixel throughout the blue and green channels; one bit hidden information is placed in one byte. The insertion bit-position is determined by using a hash function, which has a random nature to select the bit position within 2nd to 8th. The method is secure and not vulnerable to intentional attack. The experimental result shows that the high capacity with better peak signal-to-noise (PSNR) ratio is obtained by our proposed method than that of the existing methods.**

Index Terms—**steganography, spatial domain, hash function, robustness.**

I. INTRODUCTION

Data security in the last few decades has gained a wider audience for the growing possibilities of communication of huge data in the computer network. But the problem of unauthorized copying now-a-days is of great concern especially to the music, film, book and software publishing industries. Thus, we need a secured and trust-worthy communication way for transmitting confidential data. Cryptography is one of effective solution to protect data from the unauthorized users. Many cryptographic techniques have been developed in order to secure the information. But cryptography suffers from a number of drawbacks- notably the fact that the mere presence of an encrypted message might be cause for suspicion in itself [11], [12]. Another drawback of cryptography is the limitations that have been enforced by certain governments, which is particularly significant when cryptography is to be used by remote users. Many governments have created laws to either limit the strength of cryptographic systems or to prohibit it altogether [13], [14]. Primarily due to law enforcement's fear of not being able to gain intelligence by information interception [14], the use of cryptography and sometimes even the possession of a cryptographic algorithm are illegal in certain countries [15].

Steganography is the art and science of writing hidden messages in such a way that no one apart from the intended recipient knows the existence of the message. The purpose of steganography is to conceal the presence of message within seemingly harmless carriers or cover during communication [1]. There are various kinds of carrier-file formats have been used for message concealment, but digital images are the most prominent and famous because of their regularity on the internet.

Several methods have been proposed based on LSB [4], [5], [6] substitution methods. These methods cannot provide high security since the insertion of hidden data in LSB is easily predictable and extractable. Several methods have been proposed where embedding is carried out some higher order bits [8], however, the robustness of the methods is still poor.

In [9], Khalaf and Sulaiman established a technique, known as the segmenting and hiding data method. In this method, the message is concealed into two RGB channels depending on the third channel. Every part is hiding individually in two channels of a RGB image. One of the channels is utilized as index path to the subsequent two channels by calculating the number of the digits of 1 within that index path. However, this index path is not applied in a proficient way.

An RGB channel based image steganography technique is proposed in [10]. In this method, a bit of hidden information is inserted within 3rd to 8th bit position of either blue component or green component or red component of a pixel. A hash function and a secret key are used to select the data embedding position inside the color byte. In this method, only a single bit can be inserted into a color byte by changing two LSBs of both the blue and green components. Even if data is not inserted into a pixel, both LSBs of blue and green components are changed. The payload capacity as well as the PSNR is lower because two lower significant bits are changed when secret data is inserted.

In our technique, we proposed a modification of the method in [10] and some other extensions that increase data capacity and computational complexity. In this method, we insert a bit of hidden information within 2nd to 8th bit position of either green or blue component or both of a pixel. We also use a hash function and a secret key to select the insertion bit position. In every insertion, LSB of either blue component or green component is changed whereas the method in [10] changes two LSBs of both blue and green components. Although two LSBs of both blue and green components of a pixel are changed when data is not inserted but these cases are fewer than that of the method in [10].

The rest of this paper is organized as follows: Section II describes our methodology in details. Experimental results are described in Section III. In Section IV, we conclude this paper.

II. METHODOLOGY

A pixel of a color image is a combination of three components (R, G and B) of 8 bits each in a 24-bits color scheme and the message is a bit stream of its ASCII value. Insertion position inside a color component depends on the value of a hash function. The bit stream is inserted in the blue channel and green channel. After inserting the hidden

978-1-5090-2963-1/16/$31.00 ©2016 IEEE

information in the cover image which is called stego-image is passed to the recipient by unsecured communication network. After receiving the stego-image, the recipient will retrieve the secret information from the stego-image. The overview of the proposed image steganography technique is shown in the Figure 1.

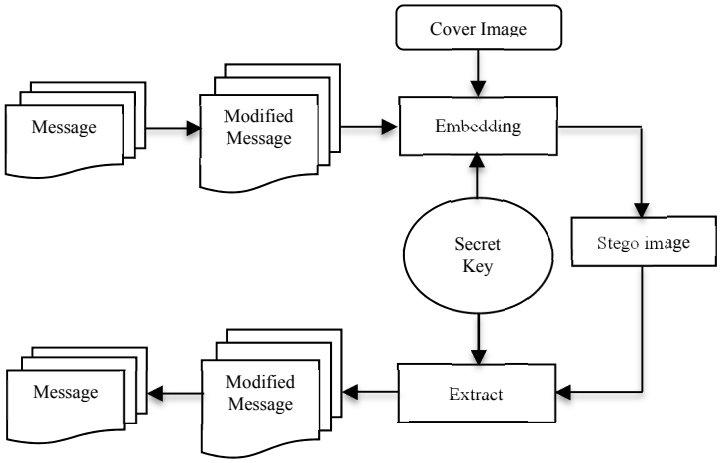

Fig. 1: Overview of the proposed system

A. Data Insertion Technique

For each byte of data from the confidential message we interchange 1st bit with 8th bit, 2nd with 7th, 3rd with 6th and 4th with 5th. Then each bit of the bit stream is inserted one after another into the blue and green channels from the beginning to the end. The inserted location of blue and green components (bytes) is determined randomly within 2nd to 8th position a hash function. If the value of the calculated location (by hash function) in blue component and the bit that has to insert are same then '0' is set to the LSB position of that blue component. Otherwise, '1' is set to the LSB position of that blue component. The process is run until the bit stream is finished or the blue components are finished. If the blue components are finished but message bit stream still remained to embed then same embedding process is run on green channel. Embedding into blue channel gets priority as the change of LSBs of the blue channel is not detectable by human eye.

Data Embedding Algorithm

//**M** = Bit Stream of Message, $\mathbf{I_Z}$ = Image Size, $\mathbf{S_K}$ = Secret //Key, **B** = Binary matrix of the blue channel of the cover //image, **G** = Binary matrix of the green channel of the //cover image, **R** = Binary matrix of the red channel of the //cover image

Step-1: Convert the message into 1D binary matrix, **M**
Step-2: **For** each byte of **M**
Interchange 1st bit with 8th bit, 2nd with 7th, 3rd with 6th and 4th with 5th
After finishing the interchange, a modified bit stream ($\mathbf{M_M}$) is found to embed
Step-3: Calculate, $\mathbf{R_0}$ = No of 0s in Red channel of the current pixel of cover image and $\mathbf{R_1} = \mathbf{S_K} - \mathbf{R_0}$
Step-4: Calculate, $\mathbf{P_B} = ((Iz + \mathbf{R_1}) \%7) + 1$
Step-5: **If** the bit value of $\mathbf{P_B}$ position of the current pixel in blue component and current bit of $\mathbf{M_M}$ to embed are equal **then**
0 is set to the LSB position of that blue component
Else
1 is set to the LSB position of that blue component
Step-6: Repeat the steps 3 to 5 until the bit stream is finished or the blue components are finished
Step-7: **If** the blue components are finished but message bit stream still remained to embed **then** go to the starting pixel of cover image
Step-8: Calculate, $\mathbf{R_2}$ = No of 1s in Red channel of the current pixel of cover image and $\mathbf{R_3} = \mathbf{S_K} - \mathbf{R_2}$
Step-9: Calculate, $\mathbf{P_G} = ((Iz + \mathbf{R_3}) \%7) + 1$
Step-10: **If** the bit value of $\mathbf{P_G}$ position of the current pixel in green component and current bit of $\mathbf{M_M}$ to embed are equal **then**
0 is set to the LSB position of that green component
Else
1 is set to the LSB position of that green component
Step-11: Repeat the steps 8 to 10 until the bit stream is finished

B. Data Extracting Technique

Extracting is the reverse process of embedding technique. In order to recover the secret information from stego-image, LSBs of blue and green components will determine the existence of hidden bit on those components.

Data Extracting Algorithm

//**M** = Bit Stream of Message, $\mathbf{I_Z}$ = Image Size, $\mathbf{S_K}$ = Secret //Key, **B** = Binary matrix of the blue channel of the stego //image, **G** = Binary matrix of the green channel of the // stego image, **R** = Binary matrix of the red channel of the // stego image, $\mathbf{M_M}$ = Modified bit stream

Step-1: **If** the LSB of blue component of the current pixel is 0 then
Calculate, $\mathbf{R_0}$ = No of 0s in Red channel of the current pixel of stego image and $\mathbf{R_1} = \mathbf{S_K} - \mathbf{R_0}$
Calculate, $\mathbf{P_B} = ((Iz + \mathbf{R_1}) \%7) + 1$
Pick the bit from the current blue component of the position $\mathbf{P_B}$ and insert into $\mathbf{M_M}$
Else
Go to the next pixel
Step-2: Repeat the above step until the bit stream is finished to extract or the blue components are finished
Step-3: **If** the blue components are finished but message bit stream still remained to extract **then** go to the starting pixel of stego image
Step-4: **If** the LSB of green component of the current pixel is 0 then
Calculate, $\mathbf{R_2}$ = No of 1s in Red channel of the current pixel of stego image and $\mathbf{R_3} = \mathbf{S_K} - \mathbf{R_2}$
Calculate, $\mathbf{P_G} = ((Iz + \mathbf{R_3}) \%7) + 1$
Pick the bit from the current green component of the position $\mathbf{P_G}$ and insert into $\mathbf{M_M}$
Else
Go to the next pixel
Step-5: Repeat the above step until the bit stream is finished to extract
Step-6: Get the modified bit stream, $\mathbf{M_M}$
Step-7: **For** each byte of $\mathbf{M_M}$
Interchange 1st bit with 8th bit, 2nd with 7th, 3rd with 6th and 4th with 5th

After finishing the interchange, bit stream **M** is found

Step-8: Get the confidential message from bit stream **M**

III. EXPERIMENTAL RESULTS

In this paper, we have shown experimental results of our proposed method and compared with the method in [10]. Here, three benchmark RGB images are used named Lena, Baboon and Pepper for experimental result analysis. The size of each image is 512 X 512. MATLAB R2010a is used to implement the proposed method and the method in [10]. Table 1 shows the PSNR values and percentage of pixels of the cover image required for embedding a message of size 15064 bytes. In general, the value of PSNR below 30dB shows the low quality and more than 40 dB shows high quality stego-image. From Table I, we see that high quality of stego-images is obtained by our proposed method for all images and the average PSNR value is 67.87.

For measuring the Peak-Signal-to-Noise Ratio (PSNR) the following formula is used:

$$\mathrm{PSNR} = 10\log_{10}\left(\frac{C^2{}_{\max}}{\mathrm{MSE}}\right)$$

Where, Cmax holds the maximum possible pixel value in the cover image and MSE denotes Mean Square Error which is defined as:

$$\mathrm{MSE} = \frac{1}{mn}\sum_{i=1}^{m}\sum_{j=1}^{n}(S_{ij} - C_{ij})^2$$

Where, i and j are the image co-ordinates, m and n are the dimensions of the image, S and C are stego image and cover image respectively.

TABLE I
PSNR VALUES OF PROPOSED SYSTEM AND EXISTING SYSTEM [10]

Images of Size 512X512	Data Embedded (bytes)	PSNR of proposed System(dB)	PSNR of existing System[10] (dB)
Lenna	15064	66.36	53.77
Baboon	15064	67.98	53.76
Pepper	15064	69.29	53.80
Average	15064	67.87	53.78

TABLE II
CAPACITY COMPARISON BETWEEN PROPOSED SYSTEM AND EXISTING SYSTEM [10]

Cover Image	Data Embedded (bytes)	Pixel holds data of proposed System (%)	Pixel holds data of existing System [10] (%)
Lena	15064	91.45	85.07
Baboon	15064	97.32	85.66
Pepper	15064	89.94	83.05
Average	15064	92.90	84.59

From the results in Table 2, it is found that greater percentages of pixel are used for information concealing that shows the data capacity. Sometimes steganography suffers from active or some passive attack as well. A steganographic technique is required to secure it from both the attacks. The proposed method is extremely safe as it introduces message in variable position in the color components and data is less susceptible to accidental attack. The selection process of channel, pixel and position by our proposed method adds to the complexity of steganalysis. Moreover, message is modified by bitwise operation before embedding which is very fast but also added computational complexity. From Fig. 2, we can observe the fact that there is no visual artifact in the stego-images; they look same as the corresponding original cover images from they are generated. Fig. 3 and 4 show the comparison of our proposed methods and the method in [10].

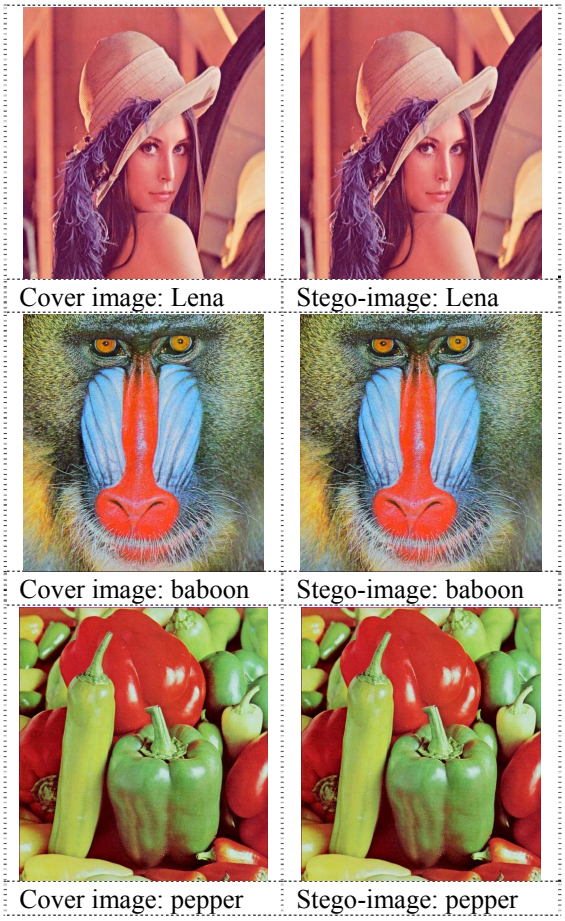

Fig 2: Cover images and their Stego-images

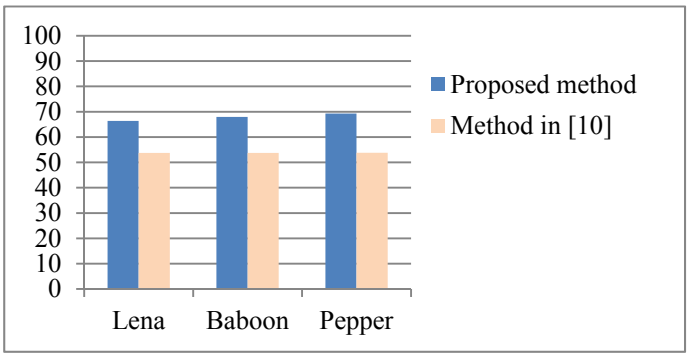

Fig. 3: Comparison of PSNR values of the proposed method and the method in [10]

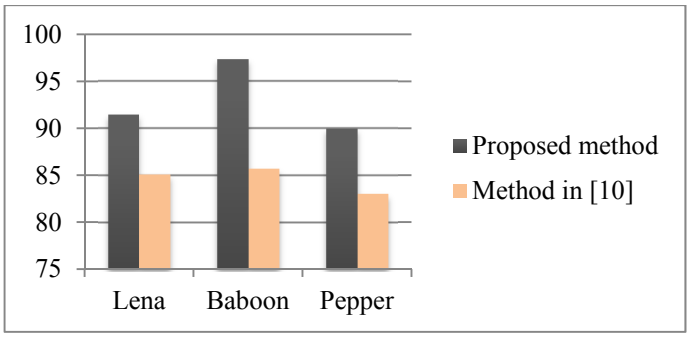

Fig. 4: Comparison of PSNR values of the proposed method and the method in [10]

IV. CONCLUSION

Steganography establishes the secrete communication between two authorized parties hiding the existence of information using a carrier file. In this paper we proposed an improved steganography technique in spatial domain where hidden bits are embedded into variable position within 2^{nd} to 8^{th} bit position of blue then green (if necessary) components of pixels of the cover image. The proposed method is safe against intentional and unintentional attacks as it modifies the raw message to distort the meaning of the secret message and inserts the modified message bits into blue channel mostly and green channel making very low image distortion. High PSNR value ensures that it is awfully difficult for the unlawful users to recognize the changes in stego-image.

REFERENCES

[1] Ramanpreet Kaur, Prof. Baljit Singh "Survey and analysis of various steganographic techniques," International Journal of Engineering Science & Advance Technology. Vol. 2 , issue 3, pp. 561 – 566, May-June 2012.

[2] N.F. Johnson and S. Jajodia, "Exploring steganography: Seeing the unseen ," Computer, vol. 31, no. 2, pp. 26-34 Feb 1998.

[3] F.A.P Peticolas, R.J. Anderson and M.G.Kuhn, "Information hiding –A survey," Proceedings of IEEE, pp. 1062-1078, July 1999.

[4] Na-I Wu, "A study on data hiding/or gray-level and binary images ," Accessed on March 2009.

[5] Junija M. and Sandhu P.S., "Designing of robust stegangraphic technique based on LSB insertion and encryption," Proceedings of International Conference on Advances in Recent Technologies in Communication and Computing, pp. 302-305, 2009.

[6] Juneja M. and Sandhu P. S., "An improved LSB based steganograhy technique for RGB color images," International Journal of Computer and Communication Engineering, vol. 2, no. 4, July 2013.

[7] Adnan Gutub, Mahmoud Ankeer, Muhammad Abu- Ghalioun, Abdulrahman Shaheen, and AleemAlvi, "Pixel indicator high capacity technique for RGB image based steganography," WoSPA 2008 – 5th IEEE International Workshop on Signal Processing and its Applications, University of Sharjah, Sharjah, U.A.E. March 2008.

[8] Kaur M, Gupta S., Sandhu P. S. and Kaur J., "A dynamic RGB intensity based steganography scheme," World Academy of Science, Engineering and Technology, vol. 67, pp. 833-838, 2010.

[9] Emad T. Khalaf, NorrozilaSulaiman,"Segmenting and hiding data randomly based on index channel," International Journal of Computer Science Issues, vol. 8, no. 1, issue 3, May 2011.

[10] Anupam K. Bairagi, Saikat Mondal and Rameswar Debnath, "A robust RGB channel based image steganography technique using a secret key," Proceedings of the 16th International Conference on Computer and Information Technology, pp. 81-87, Khulna, Bangladesh, March, 2014.

[11] M. Shirali-Shahreza, "Stealth Steganography in SMS," Proceedings of IFIP International Conference on Wireless and Optical Communication Network, pp. 316-321, 2006.

[12] E. Kawaguchi and R. O. Eason, "Principles and applications of BPCS steganography," Proceedings of SPIE International Society for Optical Engineering, pp. 464-473, 1999.

[13] J. Krinn,"Introduction to steganography," 2000, http://rr.sans.org/covertchannels/steganography.php.

[14] F. S. Grodzinsky, K. Miller and M. J. Wolf, "The ethical implications of the messenger's haircut: Steganography in the digital image. In: Himma K. E. (ed.) Internet Security: Hacking, Counter Hacking and Society," Jones and Bartlett Publishers, pp. 205, 2007.

[15] B. Dunbar, "A detailed look at steganographic techniques and the use in an open-system environment," SANS Institute, Information Security Reading Room, pp. 3.

View publication stats