ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 4, Issue 2, pp: (308-313), Month: April - June 2016, Available at: www.researchpublish.com

Steganography in Color Image using ISB

[1]Smt. Renuka Mathapati, [2]Dr.Jagadeesh Pujari

[1]Department of Computer Science, JSS SMI College, vidyagiri, Dharwad
[2]Department of ISE, SDMCET, Davalgiri Dharwad

Abstract: **This paper discusses a novel technique for implementing Steganography in a bitmap color image in RGB plane using ISB techniques. The three planes are used for embedding text and also provide additional authentication for reconstruction.**

Keywords: **Steganography, RGB planes, Signature, Encoding, Decoding, ISB.**

I. INTRODUCTION

In the field of Communication, security-issues have got the highest priority. Classical cryptography is one of the ways to secure plain text messages. Along with that at the time of data transmission, security is also implemented by introducing the concept of Steganography [1], etc. In this types of combined approach, there exits some drawbacks. Breaking of encrypted text message can be achieved by applying some technique [2]. So, there remains some probability of snooping of information. The work proposed here represents a way for securing the text [3]. The algorithm, that we have proposed here, will secure the text message Here, we have used the concept of Steganography using ISB [4] techniques were ISB technique works with the 2nd bit from last bit but before MSB and in this paper we have considered the image file format as our covering object [5].This work is specifically focused on protection of any information which is in the form of text [6]. The design of this technique is based on signature in two planes. A novel technique i.e ISB [7] is basically concentrates on any the bits other then 1st and last bit in which embedding of text is done without disturbing the image that leads to good quality of image and avoids detection of text within image.

II. PROPOSED WORK

This work involves encryption and decryption of secret message which is been embedded within an RGB [8] colored image in which all the three planes are used to hide the text on the bases of signature in respective two planes i.e R & B planes then the characters are embedded in G plane by creating an identifying pixel that is surrounded with neighboring pixel in the form of 8 bit then the character is hidden into it using ISB technique. The character can he hidden in a pixel which can be a part any three planes either R or G or B pattern. Once the candidate pixel is identified based on its value in any one region that region will be framed as embedding the character and remaining two region will be holding the signature this process continues till all the characters are hidden. Considering a color image for embedding the characters within it based on interval of 5 i.e 5th row and 5th column which is identified candidate pixel which can be on any region like R or G or B. Once we get the candidate pixel surrounding to it we have eight pixel in which the character gets embedded in the form of 8 bits without disturbing the image which gives rise to stego image nothing but text embedded image. This work is done using ISB techniques [9]. Intermediate Significant bit of neighboring pixel of candidate pixel is considered for embedding a character. The process continues for remaining 7 neighboring pixel values. Following are the images i.e FIG (A) which shows image without text and FIG (B) which shows image with text or hidden text under image.

ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 4, Issue 2, pp: (308-313), Month: April - June 2016, Available at: www.researchpublish.com

FIG. (A): IMAGE WITHOUT TEXT

FIG. (B): IMAGE WITH TEXT

III. ALGORITHM

1. Encoding:

Step 1: Read color image

Step 2: Read text file

Step 3: Read the character from text file

Step 4: Convert string to array of ASCII values

Step 5: Store 8 bits in bit array by Shifting and Anding

Step 6: Embed text in the Image column wise in the 8 bit neighbors of a pixel

Step 7: If we have reached end of rows in image (bottom of image),reset the row, increment column

Step 8: Select neighboring 8 pixel values

Step 9: Start clockwise from 12 o clock pixel

Step 10: Select candidate pixel

Step 11: Store RGB values of 8 neighboring pixels in ‘pix’

Step 12: Embed the corresponding text in that pixel value

Step 13: Each neighbor contains only one bit of the text

Step 14: Clearing last bit

Step 15: R Plane and B plane are indicators (Signature)(1 0 1 0 values)

Step 16: Only G Plane is used to store data

Step 17: ODD number, end with 1

Step 18: Else end with 0 by default (after clearing)

Step 19: Add nth bit

Step 20: Get the difference between encoded and original image which is a stego image

2. Decoding:

Step 1: Read the encoded color image

Step 2: Find the maximum row and column along with size of image

Step 3: Open the text file to write characters

Step 4: Final variable is used to hold the decoded character

Step 5: Shift the bit value

Step 6: If we have reached end of rows in image (bottom of Image), reset the row, increment column

Step 7: Select neighboring 8 pixel values

Step 8: Start Clockwise from 12 o clock pixel

Step 9: Select candidate pixel

Step 10: Store RGB values of 8 neighboring pixels in 'pix'

Step 11: Embed the corresponding text in that pixel value

Step 12: Each neighbor contains only one bit of the text

Step 13: Obtain 2nd bit from last bit

Step 14: R Plane and B plane are indicators (1 0 1 0 values)

Step 15: Only G Plane is used to store data

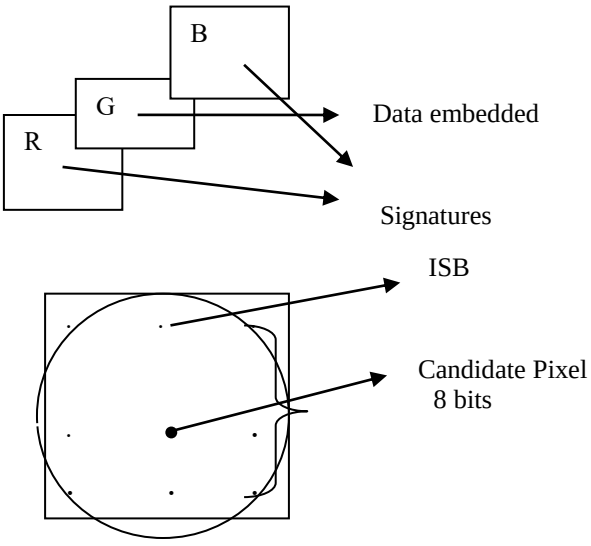
Step 16: ODD number, end with 1

Step 17: Else end with 0 by default (after clearing)

Step 18: If all conditions are true, obtain the embedded bit

Step 19: Separate image file and text file

3. Figures:



ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 4, Issue 2, pp: (308-313), Month: April - June 2016, Available at: www.researchpublish.com

IV. RESULTS

During our implementation phase, we have tested our algorithm for different sets of images as well as text messages. For each and every normal bitmap images the proposed technique is working fine. Different parameters are been applied to test the quality of the image like Mean Square Error (MSE),Peak Signal to Noise Ratio (PSNR) and Root Mean Square Error (RMSE) with their results when applied to the image. As the length of the text increases the results of these parameters also varies. Thus more number of characters can be embedded into the image depending upon its size.

IV a. Tabular representation of different parameters applied to image using ISB*:*

MSE vs. No. of Characters

No.of Characters	ISB
100	0.006245931
200	0.012430827
300	0.018330892
500	0.030141195
800	0.048436483
1000	0.060658773

PSNR vs. No. of Characters

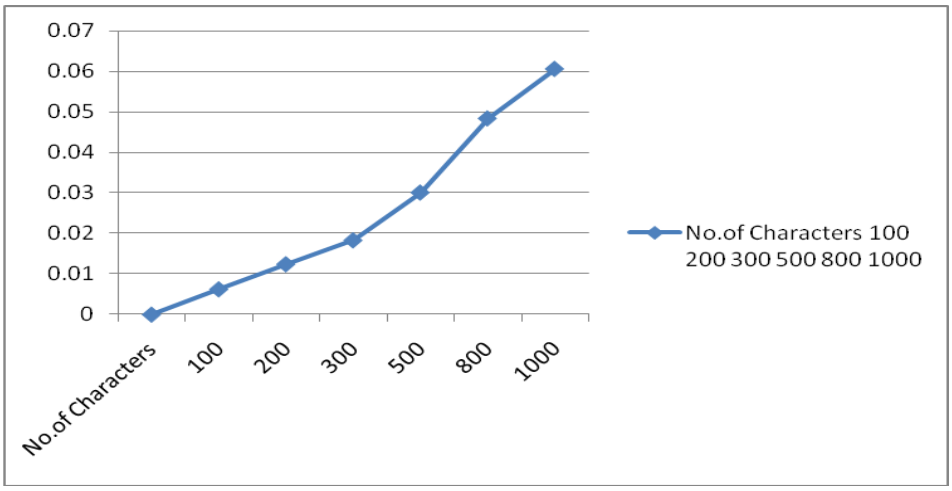
No.of Characters	ISB
100	70.20882749
200	67.21979914
300	65.53296334
500	63.37319469
800	61.31307332
1000	60.33586311

RMSE vs. No. of Characters

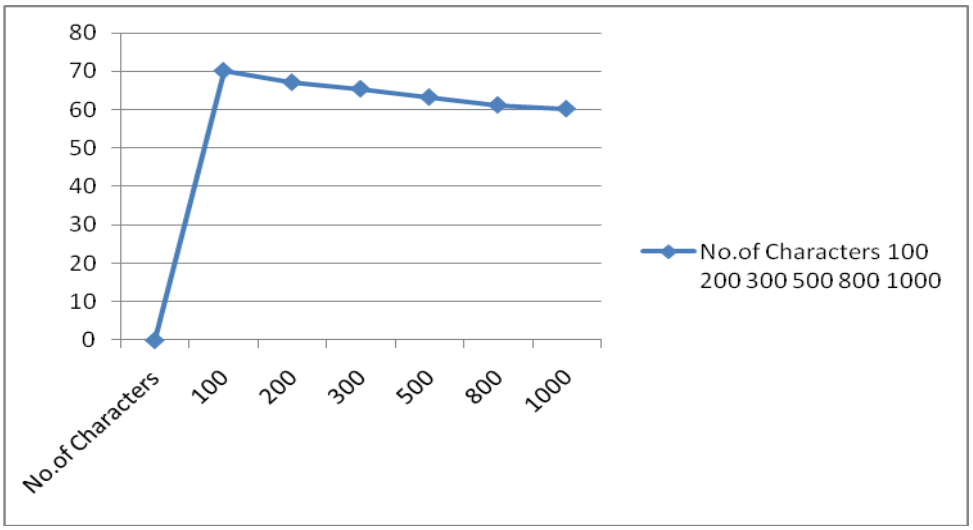
No.of Characters	ISB
100	0.0790312
200	0.11149362
300	0.13539162
500	0.1736122
800	0.2200829
1000	0.24629002

IV b. Graphical representation of different parameters based on results Using ISB:

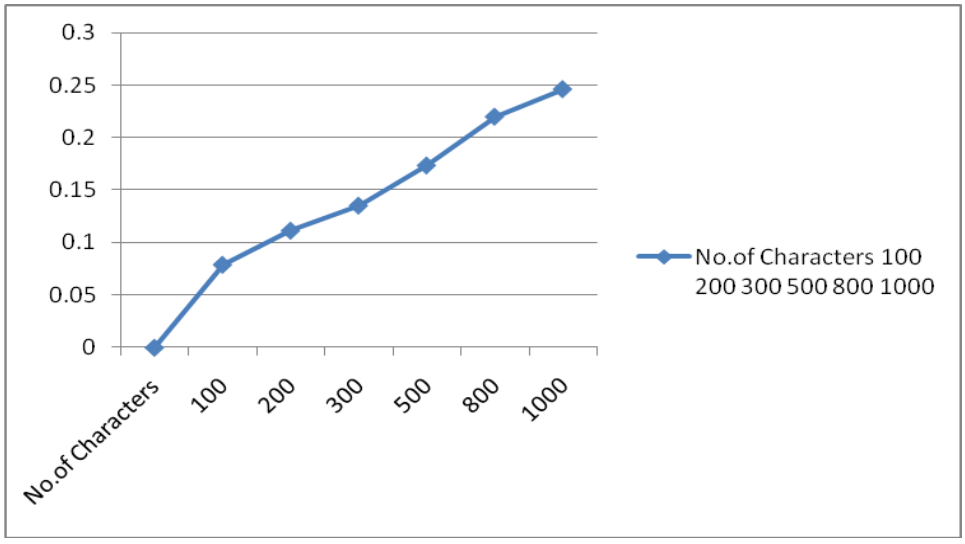
Mean Square Error:



Peak Signal to Noise Ratio:



Root Mean Square Error:



V. CONCLUSION

In this paper, the major importance is given on the secrecy as well as the privacy of information. So, to obtain privacy we have used the concept of steganography. This algorithm is supposed to be more efficient as here from the resultant image it is difficult to guess the actual data that is hidden behind it. The triplets play an important role for hiding the text in either of one triplet and remaining for identifying a pixel in the form signature. ISB is compared with different parameters like MSE, PSNR and RMSE which give the analysis of good quality of image that provide a clear idea about the best parameter. Since it is signature based whenever there is a corruption during transmission even then the data can be tracked as the signatures are present in two planes.

REFERENCES

[1] S. Channalli and A. Jadhav, "Steganography an Art of Hiding Data", International Journal on Computer Science and Engineering, IJCSE, vol. 1, no. 3, (2009)

[2] K.H. Jung, K.J. Ha and K.Y. Yoo, "Image data hiding method based on multi-pixel differencing and LSB substitution methods", Proc. 2008 International Conference on Convergence and Hybrid Information Technology (ICHIT '08), Daejeon (Korea), (2008) August 28-30, pp. 355-358.

[3] N. F. Johnson and S. Katzenbeisser, "A Survey of steganographic techniques. in Information Hiding Techniques for Steganography and Digital Watermarking,S.Katzenbeisser and F.Petitcolas, Ed. London: Artech House, (2000), pp. 43-78.

[4] Shabir A. Parah, Javaid A. Sheikh, G.M. Bhat, "Data Hiding in Intermediate Significant Bit Planes, A High Capacity Blind Steganographic Technique", International Conference on Emerging Trends in Science, Engineering and Technology , pp.192-197, July 2012

[5] S. C. Katzenbeisser. Principles of Steganography. in Information Hiding Techniques for Steganography and Digital Watermarking", S. Katzenbeisser and F. Petitcolas, Ed. London: Artech House, (2000), pp. 43-78

[6] P. Kruus, C. Scace, M. Heyman, and M. Mundy., A survey of steganography techniques for image files .Advanced Security Research Journal. [On line], 5(1), (2003), pp. 41-52.

[7] Bailey, K., and Curran, K.,"An Evaluation of Image Based Steganography Methods", Journal of Multimedia Tools and Applications, Vol. 30, No. 1, pp. 55 -88, 2006.

[8] Adnan Gutub, Ayed Al-Qahtani, Abdulaziz Tabakh, "Triple-A: Secure RGB Image Steganography Based on Randomization",International Conference on Computer Systems and Applications (AICCSA-2009), pp: 400-403, 10-13 May 2009.

[9] R. Amirtharajan, Sandeep Kumar Behera, Motamarri Abhilash Swarup, Mohamed Ashfaaq and John Bosco Balaguru Rayappan , "Colour Guided Colour Image Steganography " Universal Journal of Computer Science and Engineering Technology , 16-23, Oct. 2010, pp. 2219-2158.