Steganography in Colored Images Using Information Reflector with 2^k Correction

Manish Mahajan
Lecturer, CSE Deptt, RIMT-IET, Mandi Gobindgarh

Akashdeep Sharma
Lecturer, CSE Deptt, BBSBEC, Fatehgarh Sahib

ABSTRACT

Steganography is a process that involves hiding a message in an appropriate carrier for example an image or an audio file. The carrier can then be sent to a receiver without anyone else knowing that it contains a hidden message. The aim of this study was to investigate the various steganograhy methods & how they are implemented .LSB is a very well known method in this field. In binary images we are very much restricted in the scope as there are only 4 bits or 8 bits to represent a pixel so we are very much restricted to most popular LSB methods .But in colored images there are generally up to 24 bits images with three different RGB channels, if using RGB color space .So, we can explore a lot many new methods which can manipulate or use various channels of colored images in regular or arbitrary pattern to hide the information. Using this concept we have explored the various existing methods of data hiding in colored images & taken an intersection between the arbitrary pixel manipulation & LSB method to propose our work which uses arbitrary channel of a pixel to reflect the presence of data in one or two other channels. Finally we have used the 2k correction method to improve the stego image so as to assure the maximum security against the visual attacks. We have proved that this work shows an attractive result as compared to the other present algorithms on the various parameters like security, imperceptibility capacity & robustness.At the end the new steganography technique is also compared with the available techniques.

Keywords: Steganography,,information reflector

1. INTRODUCTION

The word steganography means "covered or hidden writing" [9]. The object of steganography is to send a message through some innocuous carrier (to a receiver while preventing anyone else from knowing that a message is being sent at all. Computer based stenography allows changes to be made to what are known as digital carriers such as images or sounds. The changes represent the hidden message, but result if successful in no discernible change to the carrier. The information may be nothing to do with the carrier sound or image or it might be information about the carrier such as the author or a digital watermark or fingerprint [7,8,9].

Cryptography and steganography are different. Cryptographic techniques can be used to scramble a message so that if it is discovered it cannot be read. If a cryptographic message is discovered it is generally known to be a piece of hidden information (anyone intercepting it will be suspicious) but it is scrambled so that it is difficult or impossible to understand and de-code. Steganography hides the very existence of a message so that if successful it generally attracts no suspicion at all[3]. Using steganography, information can be hidden in carriers such as images, audio files, text files, videos and data transmissions [7,8,9]. When the message is hidden in the carrier a stego-carrier is formed for example a stego-image. Hopefully it will be perceived to be as close as possible to the original carrier or cover image by the human senses. Images are the most widespread carrier medium [10]. They are used for steganography in the following way. The message may firstly be encrypted. The sender (or embedder [12]) embeds the secret message to be sent into a graphic file [11] (the cover image [12] or the carrier). This results in the production of what is called a stego-image. Additional secret data may be needed in the hiding process e.g. a stegokey. The stego-image is then transmitted to the recipient [11]. The recipient (or extractor [12]) extracts the message from the carrier image. The message can only be extracted if there is a shared secret between the sender and the recipient. This could be the algorithm for extraction or a special parameter such as a key [11] (the stegokey). One of the commonly used techniques is the LSB where the least significant bit of each pixel is replaced by bits of the secret till secret message finishes [2,4,5,6]. The risk of information being uncovered with this method as is very much prone to 'sequential scanning' based techniques [1], which are threatening its security. The random pixel manipulation technique attempts at overcoming this problem, where pixels, which will be used to hide data are chosen in a random fashion based on a stego-key. However, this key should be shared between the entities of communication as a secret key. Moreover, some synchronization between the entities is required when changing the key [1]. This will put key management overhead on the system. Another technique is the Stego Color Cycle (SCC). This SCC technique uses the RGB images to hide the data in different channels. That is, it keeps cycling the hidden data between the Red, Green and Blue channels, utilizing one channel at a cycle time. The main problem of this technique is that, hiding the data in the channels is done in a systematic way. So, being able to discover the data in the first few pixels will make the discovery of the technique easy. StegoPRNG is also a different technique that uses the RGB images. However in this technique, a pseudo random number generator (PRNG) is used to select some pixels of the cover image. Then, the secret will be hided in the Blue channel of the selected pixels. Again this technique has the problem of managing the key, and problem of capacity since it uses only the Blue channel out of the three channels of their available channels [6]. Our suggested technique tries to solve the

problem of the previous techniques by using an arbitrary channel of a pixel to act as an information reflector which reflects the presence of data in one or two other channels.

The flow of this paper is as follows: Section 2 represents the various parameters that should be taken into consideration while designing a technique for steganograhy. Section 3 gives as outline about the proposed method. Section 4 gives the comparisons & results with a conclusion of the work in section 5.

2. PARAMETERS

Imperceptibility: (security or transparency) The unauthorized user should not be even able to percept that data is being transferred in image i.e. by message hiding in image there should not be any changes in images that are easily visible to human eye. This should be as much a high as possible.

Capacity: By capacity we mean how much data or how much length of message a cover image can carry. For efficient transmission this parameter should also be as higher as possible.

Stoutness: By stoutness we mean that how much the stego image can withstand with the accidental or intentional changes for e.g. compression. We mean that there should be no change in hidden data.

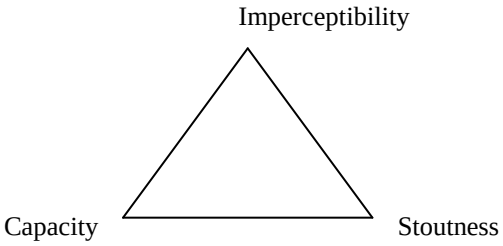


Fig 1 Stego Parameter Triangle

The above outlined fig 1 shows the various parameters that are responsible for deciding the strength of some steganography technique. These 3 parameters are not independent rather they are very much dependent upon each other .For e.g. if we want to increase the imperceptibility of a stego image then we will choose some random pixels to store the secret message but due to this the capacity of stego image will definitely be decreased & the stoutness will also increase to some extent. In this way we can say that these 3 parameters are interdependent & change in one will definitely change the value of other two parameters to some extent.

3. ARBITRARY CHANNEL REFLECTOR METHOD

In this paper we are representing a technique that is based upon using arbitrary channel of a pixel as an information reflector. Here we use one of the RGB channels of a pixel of a coloured image as a reflector to represent whether the hidden information bits are present in one or both of the other channels. In this method firstly we check the 2 least significant bits of the reflector channel, if it is 11 it means the secret text is in both the other channels so we can insert or retrieve the least 2 significant bits of both the channels in the order Ist channel followed by 2nd channel. But if the least significant bit of reflector channel is 00, it means that the pixel does not contain any secret data. On the other hand if the value of 2 LSBs of reflector channel is 01 or 10 it means that the secret text is only in one of the other channels. If the value is 01 then the data is in IST channel & if the value is 10 then the data is in 2nd channel in accordance to table1.Then we check the decimal value of actual data carrier channel if it is less than certain threshold value (i.e. 90 in our case) then the least 3 significant bits of data carrier channel will be replaced by secret data else if the value is greater then threshold value then the least two significant bits will be replaced by secret data. The information about the fact that the data carrier channel is having 2 bits of data or 3 bits of data is stored in channel other than reflector & data carrier channel according to table 1 by modifying the least significant bit of that channel ,that is if data carrier is having 2 bits of information then the value of LSB of that channel should be 0 but if data carrier channel carries 3 bits of secret data then the value of LSB of that channel should be 1.So accordingly we retrieve or insert the 2 or 3 LSBs of Ist or 2nd channel as our secret data. The Ist or 2nd channel will be two channel other than the reflector channel in the order red, green and blue as shown in table 1.For choosing the reflector channel we will use the pseudo random number generator which should be in synchronization at both transmitter & receiver ends.Also we will use the first 8 bytes of cover image as header to carry the information about the message like size of secret message in bytes or may be some other relevant information. In addition to this while inserting as well as while extracting the secret message we will maintain a special pointer that will be incremented according to the length of total message. One important thing that we need to take care is that at the end of insertion if we are left with less no of bits as permitted by the reflector channel then we will use the LSBs of data carrier channel .For e.g. if we are left with one bit of secret data & we are permitted to use 2 bits of both the channel then we will insert or retrieve the1 bit from LSB of IST channel in accordance to table 1. To assist this we are using the special pointer for secret message.

Relation between reflector & first –second channel is clear from table 1.

REFLECTOR	IST CHANNEL	2ND CHANNEL
RED	GREEN	BLUE
GREEN	RED	BLUE
BLUE	RED	GREEN

Table 1. Relation between reflector & other two channels.

LSB OF REFLECTOR	DECIMAL VALUE OF DATA CHANNEL	SECRET DATA
00 No channel is data channel	DON'T CARE	NO SECRET DATA
01 Means IST channel is data channel	<=Threshold value	3 LSBs OF IST CHANNEL
01 Means IST channel is data channel	>Threshold value	2 LSBs OF ISTCHANNEL
10 Means 2nd channel is data channel	<=Threshold value	3 LSBs OF 2nd CHANNEL
10 Means2nd channel is data channel	>Threshold value	2 LSBs OF 2nd CHANNEL
11 Both channels are data channels	TAKE CARE	2 or 3 bits in a channel depending upon threshold value

Table 2. Relation showing the secret information channel

After inserting the secret message in each channel we can also improve the stego image by applying the 2k correction to data carrier channel of the pixel (where k is no of bits relaced by secret data)as suggested by Jae-Gil-Yu[13]. This paper proposed the steganograhy technique based upon edge detection & 2k correction using MSB3 algorithm. But the problem with this technique is that while applying the 2k correction we need to take care that 3MSBs of data channel should not be changed because we need these MSBs to retrieve the message at receiver's end so the scope of 2k correction remains very limited & we cannot take the full advantage of this technique. But in our technique limitation has been eliminated & we can apply the 2k correction without any restriction.

Example of 2^k correction

Actual pixel value (APV)175=10101111

Stego pixel value (SPV) 169=10101001

Error value |175-169| = 6

If Error value<=2k-1

No need to change

Else //if error value is>2k-1 then

New stego pixel value = Either SPV - 2k OR SPV + 2k whichever is close to APV

In our case Error value =6 > (23-1 = 4) So

New stego pixel value= Either SPV – 23 OR SPV + 23 whichever is close to APV

= (169-8 =161) OR (169+8 =177) whichever is close to 175

= 177 (10110001)

In this way the 2k correction makes the intensity of the channel nearer to the actual pixel value without affecting the secret data.

3.1 ALGORITHM FOR HIDING THE SECRET MESSAGE

1) Take the secret message, path of cover image & path of output image from the user.
2) Now encrypt the secret message using certain suitable encryption algorithm. Also convert the secret message in 8 bit binary code for each character. Then read the cover image in a 3 dimensional array.
3) Find the total length of message in bytes considering 8 bit code for every character.
4) Use the first 4 bytes of the cover image as header & store the length of the message in this header & set the pointer at the first bit of message. Also add the secret key in the header. The pixels after the 4th byte will be used for hiding information.
5) Use the pseudo random number generator to generate the numbers which will be used to choose the information reflecting channel.
6) If the 2LSBs of reflecting channel is 00 then this pixel will not contain any secret data & go to step 3 for next pixel.
7) If the 2LSBs of reflecting channel is 01 then check the decimal value of first channel & go to step 10.
8) If the 2LSBs of reflecting channel is 10 then check the decimal value of 2nd channel & go to step 10.
9) If the 2LSBs of reflecting channel is 11 then check the

decimal value of both channels & go to step 10.

10) If the decimal value is less than equal to the threshold value then hide the three bits of secret data in this channel according to table 1 & table 2. For 01 & 10 case of reflecting channel also modify the LSB of other channel (other than data carrier Channel) as 1 so as to reflect that data is 3 bits in carrier channel. For 11 case of reflecting channel set the 4^{th} & 3^{rd} LSB bit of reflecting channel for first & 2^{nd} data channel respectively as 1 to reflect that data is 3 bits in carrier channel & go to step 12 else go to step 11
11) If the decimal value is greater than the threshold value then hide the two bits of secret data in this channel according to table 1 & table 2. For 01 & 10 case of reflecting channel also modify the LSB of other channel (other than data carrier channel) as 0 so as to reflect that data is 2 bits in carrier channel. For 11 case of reflecting channel set the 4^{th} & 3^{rd} LSB bit of reflecting channel for first & 2^{nd} data channel respectively as 0 to reflect that data is 2 bits in carrier channel & go to step 12.
12) 2k correction: - Apply the 2k correction as described above to the channels in which you have recently hidden the data. Also increment the pointer by 2, 3,4,5 or 6 as per situation.
13) Now check the pointer value if it is equal to the no of bits of message length then go to step14 else take the next pixel of image & go to step 4.
14) Exit.

3.2 ALGO FOR EXTRACTING THE SECRET MESSAGE

1) First of all take the path of the stego image from the user & then read the stego image in 3 dimensional array.
2) Secondly read the header of stego image & get the hidden message length in bytes & read the secret key for pseudo random number generator. Also set the pointer to 1.
3) Use the pseudo random number generator synchronized with transmitting end to generate the numbers which will tell the information reflecting channel.
4) If the 2LSBs of reflecting channel is 00 then this pixel does not contain any secret data & go to step 3.
5) If the 2LSBs of reflecting channel is 01 then the secret data is in first channel. See the value of LSB of 2^{nd} channel if it is 1 then retrieve 3 LSB bits from first channel else if it is 0 then retrieve 2 LSB bits from IST channel & go to step 8.
6) If the 2LSBs of reflecting channel is 10 then the secret data is in 2^{nd} channel. See the value of LSB of first channel if it is 1 then retrieve 3 LSB bits from 2^{nd} channel else if it is 0 then retrieve 2 LSB bits from 2^{nd} channel & go to step 8.
7) If the 2LSBs of reflecting channel is 11 then retrieve 2 or 3 bits from both channels depending upon the value of 4^{th} & 3^{rd} LSB bit of reflecting channel for first & 2^{nd} channel respectively. If the value of corresponding LSB bit is 1 then retrieve 3 bits from that channel else retrieve 2 bits from the corresponding data channel & go to step 8.
8) Increment the pointer by 2, 3, 4, 5 or 6 as per situation & go to step 9.
9) Now check the pointer value if it is equal to the no of bits of message length then go to step 10 else take the next pixel of image & go to step 3.
10) Convert the message bits into characters & decrypt them with the suitable decryption algorithm.
11) Exit.

4. RESULTS & COMPARISONS

It is clear from table 3 that in our technique the quality of stego image is very impressive that is above 99% in all that cases which clear reflects the strength of or proposed technique. Besides finding the value of MSE, PSNR & quality parameter we have also calculated the value of bits per pixel(BPP), capacity, number of secret message bits hidden & percentage of pixels used parameters in case of all the 16 image sets as shown in table 3.

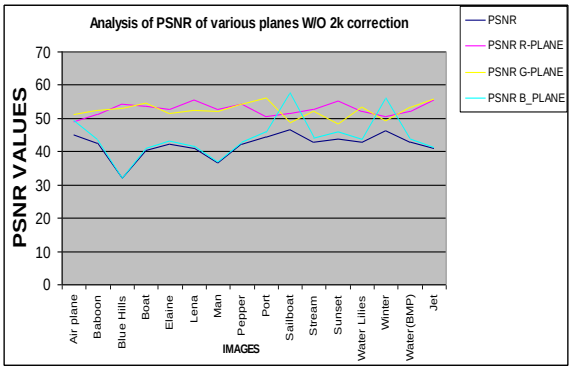
Image	Resolution (m x n)	Bits per pixel (Bpp)	Quality factor (Q)	Percent capacity (%ge)	Percent pixels used (%ge)
Air plane	150 x 100	2.68504	0.999762	11.1877	9.673300
Baboon	131 x 131	2.25463	0.999753	9.39429	10.06930
Blue Hills	800 x 600	3.68531	0.999988	15.3555	0.219792
Boat	127 x 88	2.03659	0.999577	8.48580	17.11700
Elaine	105 x 135	2.27703	0.999879	9.48763	12.07050

Table 3 Results of Various Parameters on Different Image Sets

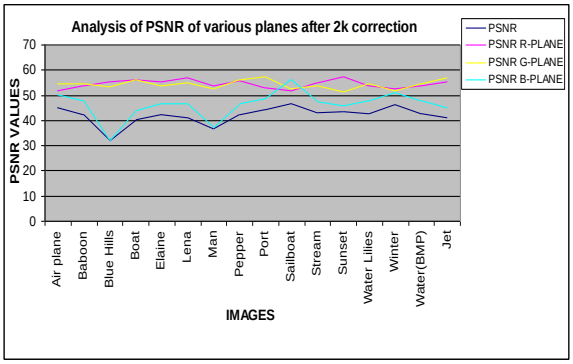
We have constantly hidden the 3896 bits in various images of various resolutions & we found that bits per pixel, capacity & quality parameters are almost independent from the resolution of the image.

When we have analyzed the values of PSNR parameter of various planes we have found that the PSNR value of blue plane is very dominating in deciding the overall PSNR value of cover as well as stego image. It is clear from the fact that the image of Blue Hills & Man has very low PSNR values because the PSNR value of blue is very low in both the images. Also both of these images are blue component dominating. It is clear from the following GRAPH1 & GRAPH2 that the role of blue component is very dominating in deciding the PSNR value of image before & after 2k correction.

We are very much concerned about PSNR value parameter because this is one of the major parameter which ultimately decides the imperceptibility & robustness parameter. If the imperceptibility will be more then there will be obviously less visual attacks. So PSNR is deeply analyzed.



Graph 1 PSNR values of various planes of images without 2k correction



Graph 2 PSNR values of various planes of images with 2k correction

Comparisons With Other Techniques:

We have compared our proposed technique with famous LSB substitution technique, Tseng Cheng technique & NPI technique [14] on the very important parameter of PSNR for four famous image sets of lena, pepper, baboon & jet of different sizes as shown in table 4 below.

Image	NPI Technique (PSNR)	Tseng Cheng Technique (PSNR)	LSB Technique (PSNR)	Proposed Technique (PSNR)
Lena	42.590	40.055	41.005	45.829
Pepper	43.924	39.897	42.374	45.760
Baboon	38.364	31.384	33.988	46.111

Jet	42.505	38.287	39.383	44.579

Table 4 Comparison of proposed technique with previous techniques for PSNR

5. CONCLUSION

This work is designed & implemented for hiding the secret information into some RGB image using one of the channel of image as reflector which will give information about the secret data carrier channel. This reflector channel is not fixed rather chosen randomly for every pixel due to which the imperceptibility factor is increased a lot. This imperception also gives a great relief against visual attacks. The PSNR & MSE values are also better in this technique as compared to previous techniques. Besides 2k correction applied to the proposed technique has improved the stego image up to great extent. This technique uses the 2k correction up to full of its strength which was not possible in the previous techniques. Also the histogram analysis of cover & stego image indicates that the proposed method with 2k correction will generate stego images in which the intensity distributions will be almost same as original cover image so there will be less chances of any kind of attack on secret message which is accountable for the imperceptibility & robustness factor. We have tried to check this method on basic goodness criteria of any steganography algorithm i.e. capacity, imperceptibility & stoutness. Basically the technique is proposed by keeping in mind about the safe capacity rather than about capacity which is justified with the improved values of MSE & PSNR.

REFERENCES

[1] S. Venkatraman, A. Abraham, M. Paprzycki, "Significance of Steganography on Data Security", International Conference on Information Technology: Coding and Computing (ITCC'04), Las Vegas, 5-7 April 2004.

[2] Kathryn Hempstalk, "Hiding Behind Corners: Using Edges in Images for Better Steganography", Proceedings of the Computing Women's Congress, Hamilton, New Zealand, 11- 19 February 2006.

[3] N.F. Johnson, S. Jajodia, "Exploring Steganography: Seeing the Unseen", IEEE computer, Vol. 31, No. 2, pages 26-34, February 1998.

[4] G.C. Kessler, "An Overview of Steganography for the Computer Forensics Examiner", Forensic Science Communications, Vol. 6, July 2004.

[5] D. Artz, "Digital Steganography: Hiding Data within Data", IEEE Internet Computing: Spotlight, pages 75-80, May-June 2001.

[6] K. Bailey, K. Curran, "An Evaluation of Image Based Steganography Methods", Multimedia Tools & Applications, Vol. 30, No. 1, pages 55-88, July 2006.

[7] A. Gutub, L. Ghouti , A. Amin, T. Alkharobi, M.K. Ibrahim, "Utilizing Extension Character 'Kashida' With Pointed Letters For Arabic Text Digital Watermarking", Inter. Conf. on Security and Cryptography - SECRYPT, Barcelona, Spain, July 28 - 31, 2007.

[8] A. Gutub, M. Fattani, "A Novel Arabic Text Steganography Method Using Letter Points and Extensions", WASET International Conference on Computer, Information and Systems Science and Engineering (ICCISSE), Vienna, Austria, May 25-27, 2007.

[9] Johnson Neil F., Zoran Duric, Sushil Jajodia, Information Hiding, and Watermarking - Attacks & Countermeasures, Kluwer 2001.

[10] Westfield Andreas and Andreas Pfitzmann, Attacks on Steganographic Systems. Third International Workshop, IH'99 Dresden Germany, October Proceedings, Computer Science 1768. pp. 61- 76, 1999.

[11] Zollner J., H. Federrath, H. Klimant, A. Pfitzmann, R. Piotraschke, A. Westfeld, G. Wicke, G. Wolf, Modelling the Security of Steganographic Systems, Information Hiding, 2nd International Workshop, IH'98 Portland, Oregon, USA, Computer Science 1525. pp. 344-354, April 1998.

[12] Pfitzmann Birgit. Information Hiding Terminology. First International Workshop, Cambridge, UK, Proceedings, Computer Science 1174. pp. 347-350, May -June

[13] Jae-Gil Yu1, Eun-Joon Yoon2, Sang-Ho Shin1 andKee-Young Yoo, Dept. of Computer Engineering, Kyungpook National University Daegu, Korea," A New Image Steganography Based on 2k Correction and Edge-Detection", Fifth International

Conference on Information Technology: New Generations 978-0-7695-3099-4/08 © April 2008 IEEE

[14] Ali Shariq Imran, M. Younus Javed, and Naveed Sarfraz Khattak "A Robust Method for Encrypted Data Hiding Technique Based on Neighborhood Pixels" Information International Journal of Computer Science and Engineering 1;3 © www.waset.org Summer 2007