ISSN(Online) :2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 10, October 2015

Improved Spatial Domain Image Steganography using LSB & MSB

Himanshi Sharma[1], Sharad Chauhan[2], Kamal Sharma[3]

M.Tech Student, Department of CSE, E-Max Group of Institutions, Ambala, Kurukshetra University, India[1]

Assistant Professor, Department of CSE, E-Max Group of Institutions, Ambala, Kurukshetra University, India[2]

Professor, Department of CSE, E-Max Group of Institutions, Ambala, Kurukshetra University, India[3]

ABSTRACT: In this paper, an improvement in 3-3-2 approach is proposed and implemented with the purpose of security enhancement and quality maintenance. In this approach, instead of using the same method for whole message, we proposed two different techniques 2-1-1 and 1-2-1. Both are based on the LSB & MSB of red, green and blue color. These are used in combination to hide the whole byte in a single pixel. According to the results, it is observed that security is improved as compared to existing 3-3-2 approach with reasonable PSNR value.

KEYWORDS: Steganography, Modified 3-3-2 approach, High security, RGB images, LSB & MSB**.**

I. INTRODUCTION

Steganography is the practice of concealing a secret message such as text file, image, or video within cover media (image, audio or video). The main aim of steganography is to hide the presence of hidden messages in the cover medium. So that no one gets any idea about the secret information transmission. In short, we can say that Steganography is one such technique in which presence of secret message cannot be detected and we can use it as a tool for security purpose to transmit the confidential information in a secure way [6].

The main two problems of steganography is the amount of data that is hidden and the quality of cover medium. In this work we focus on image steganography in spatial domain. Spatial domain techniques allow direct dealing with image pixels. The most common method for image steganography is LSB technique. The simplest LSB technique hides the secret information directly into the spatial domain by modulating the least significant bits of the cover image. Besides simplicity, the other limitation of this technique is the amount of data hidden inside it. It hides only one bit in one pixel.

To increase the capacity of this technique Shahzad Alam, S M Zakariya, and M Q Rafiq proposed two techniques named 3-3-2 and 4-4-4 modifies LSB technique [1]. Among which 3-3-2 modifies LSB gives better result and improve the capacity of image for data hiding. For this it hides one byte of data per pixel in the ratio of 3:3:2 in red, green and blue color. The other advantage of this technique is that no limitation on the type of cover image used. But this technique does not improve the security of hidden data.

In this work we used the advantage of this technique and try to improve its security by proposing two techniques 2-1-1 and 1-2-1 LSB technique. The next section describes the existing 3-3-2 approach. Section III describes proposed method. In section IV, we present our results.

II. RELATED WORK (EXISTING 3-3-2 APPROACH)

In the field of image steganography different algorithms and techniques has been proposed to share the information secretly.The 3-3-2 LSB approach is advancement over simple least significant bit algorithm. In this approach, the problem of sensitivity of the blue color can be overcome by using two bits while using three bits of each other colors green and blue [1].

ISSN(Online) :2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 10, October 2015

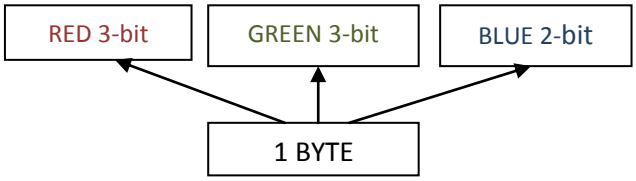

Figure 1: Schematic of 3-3-2 approach [1]

This means, has been able to hide byte in each pixel of true color image (24-bit), as shown in Figure 1, and so is to increase the proportion of suppression by 33.33% from the size of file cover, without suspected to the suppression, even if they were chosen at random file cover. The standard pictures of 800*600 pixels may have 1 byte for each pixel. Meaning that 800*600=480000 byte, which means there will be 480000 characters

On the other hand, second approach named 4-4-4 modified LSB approach [1] improved the capacity of hidden data by hiding 12 bits in a single pixel as compare to 8 bits in 3-3-2 approach. But that also leads maximum MSE, so we choose 3-3-2 LSB approach over 4-4-4 LSB technique to maintain quality of stego image.

This 3-3-2 approach focussed only on capacity and quality of image. It gives not much importance to the security of hidden data. The limitation of this technique is that secret message bit is directly embedded at corresponding LSB and for that same technique is used. This will make it easy for intruders to detect and extract the original message.

III. IMPROVED 3-3-2 APPROACH

The outer working of this proposed work is similar to the existing 3-3-2 work i.e the final stego image has data hiding in the ratio of 3:3:2 for each pixel. To improve the 3-3-2 approach, we proposed two different techniques. The first technique is known as 2-1-1 LSB technique and second is known as 1-2-1 LSB technique. They both are used in combination to hide the complete message as shown in Figure 2 for one pixel.

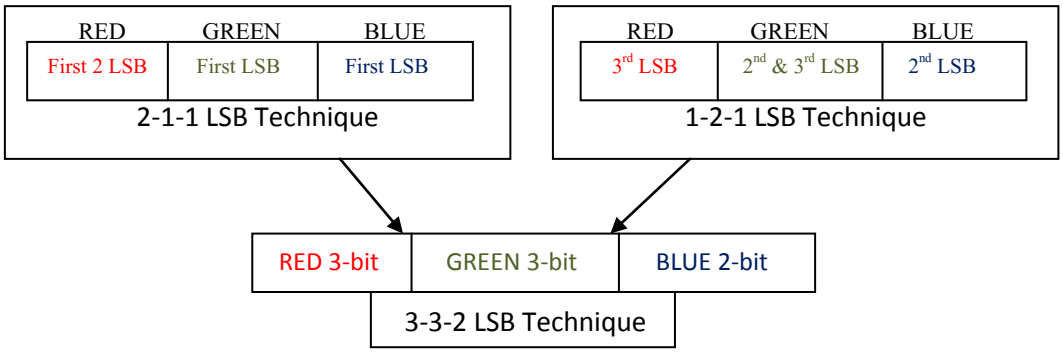

Figure 2: Formation of one pixel in improved 3-3-2 approach after data hiding

The modified algorithm for 3-3-2 approach is described below:

A. Algorithm for Embedding

Inputs: RGB cover image, secret message
Output: Stego image with secret data embedding in it
Step1: Begin
Step2: Calculate message length (length) and size of image (img_size);
Step 3: (i) If (length>img_size) then error ("message is too long to fit in image");
(ii)Else goto step 4.
Step4: store message in byte array.
Step 5: For i =1 to length repeat steps 6 to 9
Step 6: (i) Read 1st byte (b) from byte array and convert into bits.
(ii)Read 1st pixel (p) from image.
Step7: Hide half bits using 1st technique (2-1-1 LSB technique).

ISSN(Online) :2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 10, October 2015

Step8: Hide next half bits using 2nd technique (1-2-1 LSB technique).
Step9: p++; b++;
Step10: Save resulting image as a stego image.
Step11: Exit.
The main advantage of this technique is that the message bits will not directly hide at least significant bit. They will first convert to some other form and then that resultant bits will be hide at corresponding least significant bit. Without applying both techniques we can't get a single character because it hides in two parts each with different techniques. To extract the original message from the stego image we first need to convert these resultant bits back to original form by using the rules of 2-1-1 and 1-2-1 LSB techniques. That will make the process complex for intruders by enhancing its security.

B. 2-1-1 LSB TECHNIQUE

To hide the half bits of byte we proposed 2-1-1 LSB technique. This technique will hide the bits of red, green and blue colour in the ratio of 2:1:1 as shown in figure 3.

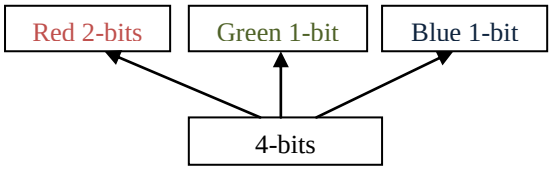

Figure3. LSB technique 2-1-1

To remove the limitation of existing 3-3-2 approach, this technique will not directly hide the bits to the LSB of RGB color. Instead, this will use two different color bits in combination with secret message bit and apply some rules, shown in table1.That resultant bit will be embedded at corresponding LSB of RGB colors and makes it difficult for intruders to detect and extract the original message. The process is described below and rules1 is shown in table1:

1. Two bits embedded in red colour:
   (i) Take 3rd lsb of blue, 3rd msb of red and 1 bit of character, Apply rules and resultant bit is stored at 1st lsb of red color.
   (ii) Take 4th lsb of blue, 4th msb of red and 1 bit of character, apply rules and resultant bit stored at 2nd lsb of red color.
2. One bit embedded in green color:
   (i) Take 2nd msb of green, 1st msb of blue and 1 bit of character, Apply rules and resultant bit is stored at 1st lsb of green color.
3. One bit embedded in blue color:
   (i) Take 1st msb of green, 2nd msb of blue and 1 bit of character, Apply rules and resultant bit is stored at 1st lsb of blue color.

Table 1: Rules for 2-1-1 LSB Technique

1st bit	2nd bit	3rd bit	Resultant bit
0	0	0	1
0	0	1	0
0	1	0	0
0	1	1	1
1	0	0	0
1	0	1	1
1	1	0	1
1	1	1	0

The complete schematic of this proposed technique is shown in figure 4 with the hidden bit position in RGB images.

ISSN(Online) :2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 10, October 2015

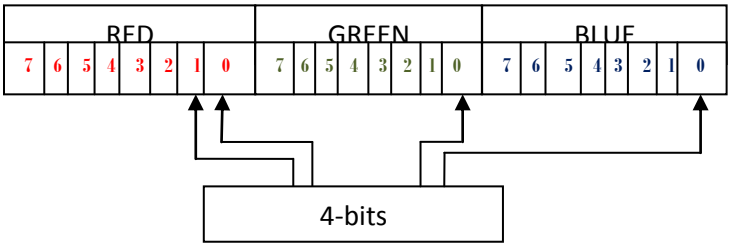

Figure 4: Schematic of 2-1-1 Technique

C. 1-2-1 LSB TECHNIQUE

To hide the remaining half bits of byte we proposed 1-2-1 LSB technique. This technique will hide the data in the ratio of 1:2:1. That means two bit will hide in green color and one bit in each other color red and blue as shown in Figure 5. The extra security layer that we add in this technique is that the data bits are not directly replaced by LSB of pixel.

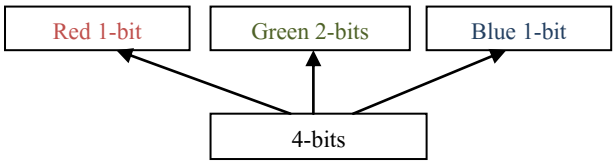

Figure 5: LSB technique 1-2-1

This technique will used single different colour bit in combination with secret bit and then apply some rules for that. The resultant bit is stored at corresponding LSB. The process of this technique is described below and rules2 is shown in table2:

1. One bit embedded in red color:
   (i) Take 4th msb of green and 1 bit of character, apply rules2 and resultant bit is stored at 3rd lsb of red color.
2. Two bits embedded in green color:
   (i) Take 3rd msb of blue and 1 bit of character, apply rules2 and resultant bit is stored at 2nd lsb of green color.
   (ii) Take 2nd msb of red and 1 bit of character, apply rules2 and resultant bit is stored at 3rd lsb of green color.
3. One bit embedded in blue color:
   (i) Take 3rd msb of green and 1 bit of character, apply rules2 and resultant bit is stored at 2nd lsb of blue color.

Table2: Rules for 1-2-1 LSB Technique

1st bit	2nd bit	Resultant bit
0	0	1
0	1	0
1	0	0
1	1	1

IV. RESULTS AND ANALYSIS

We have tested this technique on distinct type of images like Lena, baboon etc. To check the quality of stego image we used two parameters, mean square error (MSE) and PSNR (Peak signal to noise ratio) value. PSNR [7] is most commonly used to measure the quality of reconstruction of lossy compression codecs (e.g., for image compression). The signal in this case is the original data, and the noise is the error introduced by compression. When comparing compression codecs, PSNR is an approximation to human perception of reconstruction quality. Although a higher PSNR generally indicates that the reconstruction is of higher quality, in some cases it may not. PSNR is most easily defined via the mean squared error (MSE). Given a noise-free m×n monochrome image I and its noisy approximation K, MSE is defined as [7]:

ISSN(Online) :2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 10, October 2015

$$MSE = \frac{1}{m\,n}\sum_{i=0}^{m-1}\sum_{j=0}^{n-1}[I(i,j) - K(i,j)]^2$$

The PSNR value in db is defined as:

$$\begin{aligned} PSNR &= 10 \cdot \log_{10}\left(\frac{MAX_I^2}{MSE}\right) \\ &= 20 \cdot \log_{10}\left(\frac{MAX_I}{\sqrt{MSE}}\right) \\ &= 20 \cdot \log_{10}(MAX_I) - 10 \cdot \log_{10}(MSE) \end{aligned}$$

Here, MAX_I is the maximum possible pixel value of the image. When the pixels are represented using 8 bits per sample, this is 255. For color images with three RGB values per pixel, the definition of PSNR is the same except the MSE is the sum over all squared value differences divided by image size and by three. Alternately, for color images the image is converted to a different color space and PSNR is reported against each channel of that color space. Typical values for the PSNR in lossy image and video compression are between 30 and 50 dB, provided the bit depth is 8 bits, where higher is better. For 16-bit data typical values for the PSNR are between 60 and 80 dB. Acceptable values for wireless transmission quality loss are considered to be about 20 dB to 25 dB. In the absence of noise, the two images I and K are identical, and thus the MSE is zero. In this case the PSNR is infinite. So in the proposed results less MSE and high PSNR value shows better quality of stego image.

As the proposed improved 3-3-2 LSB approach allow to choose any type of image for steganographic technique i.e. no limitations on the type of image chosen. So we tested this work on different type of images such as lena, baboon etc.

Table 3: Values obtained by improved 3-3-2 Approach for Lena image (size 258*258, type- .bmp)

Data in bytes	Image name	MSE	PSNR
100	000	0.0118	67.4356
300	100	0.0349	62.7398
600	200	0.0649	60.0440
1000	300	0.1107	57.7219
3000	400	0.3297	52.9833
6000	500	0.6521	50.0214
10000	600	1.0893	47.7932
24000	700	2.7527	43.7673
34000	800	3.8970	42.2575
60000	900	6.8645	39.7987

Table 3 shows the mean square error and PSNR values which are obtained by applying improved 3-3-2 approach for Lena image. To get these performance values we used Lena image with different size of hidden data.

ISSN(Online) :2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 10, October 2015

Table 4: Values obtained by improved 3-3-2 Approach for baboon image (size 225*225, type- .jpg)

Data in bytes	Image name	MSE	PSNR
300	100	0.0464	61.4984
500	200	0.0794	59.1684
1000	300	0.1569	56.2077
3000	400	0.4708	51.4364
5000	500	0.7873	49.2036
10000	600	1.5389	46.2926
24000	700	3.7024	42.4799
35000	800	5.4071	40.8351
50000	900	7.7456	39.2742

Table 4 shows the mean square error and PSNR values which are obtained by applying improved 3-3-2 approach for baboon image. From the above both observations, it is clear that the proposed work gives reasonable values in terms of quality for all type of images i.e. jpg, bmp etc.

Table 5: Comparison of three approaches on the basis of PSNR value for Lena image

Data in Byte	Existing 3-3-2 approach	4-4-4 approach	Improved 3-3-2 approach
100	50.24	60.97	67.44
300	50.26	57.02	62.74
600	50.06	54.41	60.04
1000	50.08	52.34	57.72
3000	49.01	47.42	52.98
6000	47.60	44.55	50.02
10000	46.13	42.34	47.79
24000	43.35	38.52	43.76
34000	42.03	37.04	42.25

Table 5 shows the comparison of PSNR performance between existing 3-3-2, 4-4-4 and improved 3-3-2 approaches for Lena image. It is clear from the above observation that improved 3-3-2 approach gives better values than other existing approaches.

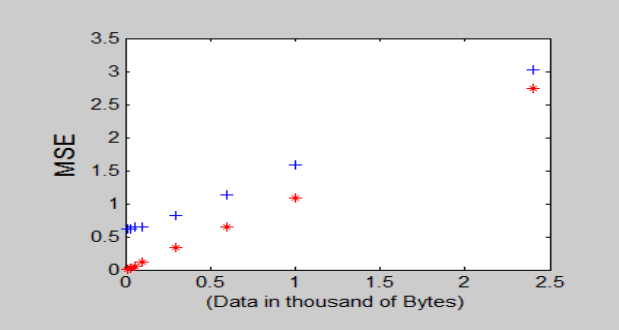

Figure 6: Comparison of MSE between existing 3-3-2 and improved 3-3-2 approach.

ISSN(Online) :2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 10, October 2015

The comparison between mean square errors (MSE) of existing 3-3-2 modified LSB approach and improved 3-3-2 LSB approach is shown graphically in Figure 6 for Lena image. The MSE of existing approach shown by blue color plus sign and of improved 3-3-2 LSB approach shown by red color multiply sign. It is clear from the above observation that proposed method gives reasonable quality values and improves security.

V. CONCLUSION

In this work, we implemented improved 3-3-2 approach with similar outer structure to the existing work but its internal working is completely different and more secure. This approach is based on a combination of two techniques 2-1-1 and 1-2-1 LSB approach that allow indirect data hiding in cover image by providing two security layers. The first layer that we used is the dependency of each hidden bit on other color value. The second layer is the addition of rules in that dependency on other color value. It's clear that the hidden bit in stego image is not the original data bit but it is the resultant bit generated from the rules (used in 2-1-1 or 1-2-1 LSB technique). The use of these two techniques for hiding a single byte or a character makes it strong as compare to existing 3-3-2 modify LSB approach. By using the advantages of existing 3-3-2 approach this improved method allows data hiding of 1 byte per pixel. It also provides no limitation on the type of image use. The major advantage of proposed work is that without applying both proposed technique we even can't get a single character. It enhances the security of hidden data from outside attackers. From the above results we concluded that this approach is more secure than existing 3-3-2 LSB approach and provides reasonable PSNR value. In future we can use this method in other steganography techniques. We can also enhance this method to get better PSNR values.

REFERECES

[1] Shahzad Alam, S M Zakariya, and M Q Rafiq, "Analysis of Modified LSB Approaches of Hiding Information in Digital Images", IEEE 5th International Conference on Computational Intelligence and Communication Networks (IEEE CICN 2013), pp. 280-285, 2013.

[2] Johri, P. ,Khan, S., Akhtar, N., "Enhancing the Security and Quality of LSB Based Image Steganography", 5th International Conference on Computational Intelligence and Communication Networks (IEEE CICN 2013), pp. 385-390, 2013.

[3] Zheng Zhiwei , Tao Shun , Ding Shilei, Yang Ren-er, "Image Steganography Combined with DES Encryption Pre-processing", IEEE Sixth International Conference on Measuring Technology and Mechatronics Automation (IEEE ICMTMA 2014), pp. 323-326, 2014.

[4] Roy, R. ; Changder, S., Gupta, P.K., "A secure image steganography technique with moderately higher significant bit embedding", IEEE International Conference on Computer Communication and Informatics (IEEE ICCCI 2014), pp. 1-6, 2014.

[5] Altaay, A.A.J.; bin Sahib, S. ; Zamani, M., "An Introduction to Image Steganograpy Techniques", IEEE International Conference on Advanced Computer Science Applications and Technologies (IEEE ACSAT 2012), pp. 122-126, 2012.

[6] Bansal, S. ; Bansal, R.K.; Kaur, S., "Steganography and classification of image steganography techniques", IEEE International Conference on Computing for Sustainable Global Development (IEEE INDIACom 2014), pp. 870-875, 2014.

[7] V Chayapathi , Sharath B , Dr G S Anitha, "Improvement of Image Quality by Adding White Gaussian Noise", International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering(IJAREEIE), vol. 2, issue 10, 2013.

[8] T.R. Devi, "Importance of Cryptography in Network Security", IEEE International Conference on Communication Systems and Network Technologies (IEEE CSNT), pp. 462-467, 2013.