International Journal of Latest Trends in Engineering and Technology
Special Issue SACAIM 2017, pp. 468-470
e-ISSN:2278-621X

DESIGN AND IMPLEMENTATION OF EFFICIENT STEGANOGRAPHY ALGORITHM

Geethesh P. B[1], Cynthia Fernandes[2] & Mr Santhosh B[3]

Abstract- Steganography is an art of composing concealed messages such that nobody, aside from the sender and planned beneficiary the presence of the message, a type of security through indefinite quality. In this paper we have proposed modified LSB algorithm. The proposed algorithm is efficient in terms of security of the messageand degradation is minimum compared to LSB algorithm.
Keywords- LSB, Steganography, pixel

1. INTRODUCTION

The art and science of hiding information by embedding messages inside other, apparently harmless messages. Steganography works by replacing bits of useless or unused informationin regular computer files (such as graphics, sound, text, HTML, or even floppy disks) with bits of different, invisible information. This hidden information can be plain text, cipher text, or even images.Ordinarily, be that as it may, steganography is composed in characters including hash stamping, however its use inside pictures is additionally normal. At any rate, steganography shields from pilfering copyrighted materials and also supporting in unapproved seeing.

Calculation of LSB strategy for steganography.There may be two distinct periods of LSB technique, inserting stage and separating stage. A portion of the methods utilized as a part of steganography are area apparatuses or basic framework, for example, minimum critical piece (LSB) inclusion and commotion control, and change space that include control calculations and picture change, for example, discrete cosine change and wavelet transformation. However there are systems that offer the characteristic of both of the picture and space instruments, for example, interwoven, design piece encoding, spread range meth-ods and covering.

2. LEAST SIGNIFICANT BIT TECHNIQUE

Least significant bit (LSB) insertion is a common and simple approach to embed information in an image file. In this method the LSB of a byte is replaced with an M‟s bit. This technique works good for image steganography. To the human eye the stego image will look identical to the carrier image.. For hiding information inside the images, the LSB (LeastSignificantByte) method is usually used. To a computer an image file is simply a file that shows different colors and intensities of light on different

areas of an image. The best type of image file to hideinformation inside is a 24 Bit BMP (Bitmap) image.When an image is of high quality and resolution it is a easier to hide information inside image. Although24 Bit images are best for hiding information due to their size. Some people may choose 8 Bit BMP‟s or possibly another image format such as GIF . The reason being is that posting of large images on the internet may arouse suspicion. The least significant bit i.e. the eighth bit is used to change to a bit of the secret message. When using a 24-bit image, one can store 3 bits in each pixel by changing a bit of each of the red, green and blue colour components. Suppose that we have three adjacent pixels (9 bytes) with the RGB encoding [3]

10010101 00001101 11001001
10010110 00001111 11001011
10011111 00010000 11001011

When the number 300, can be which binary representation is 100101100 embedded into the least significant bits of this part of the image. If we overlay these 9 bits over the LSB of the 9 bytes above we get the following (where bits in bold have been changed)

10010101 0000110**0** 1100100**0**
1001011**1** 0000111**0** 11001011
10011111 00010000 1100101**0**

[1] Department of MCA, AIMIT, St. Aloysius College, Mangaluru– 575022, Karnataka, India
[2] Department of MCA, AIMIT, St. Aloysius College, Mangaluru– 575022, Karnataka, India
[3] Department of MCA, AIMIT, St. Aloysius College, Mangaluru– 575022, Karnataka, India

Here the number 300 was embedded into the grid, only the 5 bits needed to be changed according to the embedded message. On average, only half of the bits in an image will need to be modified to hide a secret message using the maximum cover size.

3. NEW PROPOSED ALGORITHM

LSB algorithm inserts insert plain text in the last two bits of each byte. The proposed modified LSB algorithm generates pseudo random number r and in the next r th byte inserts the plain text. Some of the advantages of proposed method is since plaintexts are not inserted in the carrier image sequentially degradation of the image is minimum compare to the LSB algorithm. In the LSB method if the hacker knows message is embedded, he can extract the message easily. Since in the proposed method randomly next new rth byte is selected, it makes hacker impossible to extract the message even if he knows message is hidden.

Proposed modified LSB Steganography algorithm

Encoding Text

```
 r= next_Su_Rand(initalize);
while((data=inputmsg.read()) != -1)
                    {
                              carrier.write((source.read(r) & 252) | ( data & 3 ));
                               r= next_Su_Rand();
                              carrier.write((source.read(r) & 252) | ( (data & 15) >>> 2 ));
                              r= next_Su_Rand();
                              carrier.write((source.read(r) & 252) | ( (data & 63) >>> 4 ));
                              r= next_Su_Rand();
                              carrier.write((source.read(r) & 252) | ( data >>> 6));
                               r= next_Su_Rand();
                    }
```

Decoding Text

```
r= next_Su_Rand(initalize);
for(i = 0; i< size; i++ )
                    {
                              data = in.read(r);
                              output = data & 3;
                               r= next_Su_Rand();
data = in.read(r);
                              output |= (data & 3) << 2;
r= next_Su_Rand();
data = in.read(r);
                    output |= (data & 3) << 4;
                                r= next_Su_Rand();
data = in.read(r);
                                        output |= (data & 3) << 6;
                                        out.write(output);
                          }
```

4. IMPLEMENTATION& EXPERIMENTAL RESULTS

The algorithm is implemented using java. Fig 1 shows the original image and Fig 2 is the Stegano image using LSB algorithm. Fig 3: is theStegano image using modified LSB algorithm.

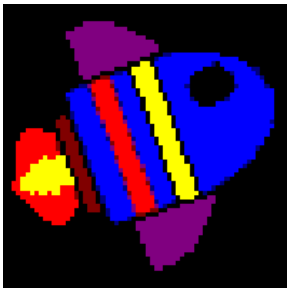

Fig 1:Original Image

Fig 2: Stegano Image (LSB algorithm)

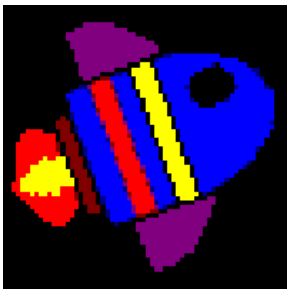

Fig 3: Stegano Image (modified LSB algorithm)

The Experimental results shows that there is no difference with respect to the size of the image. And degradation due to embedding the message is negligible and human eye cannot differentiate. When the message is embedded in, the there is a degradation and it is minimized in modified LSB algorithm. Since the hacker does not know about the order in which plain texts are stored it more efficient than existing LSB algorithm.

5. CONCLUSION

The proposed method is more efficient than existing LSB algorithm. Compare to the LSB degradation of the images is very minimum. And because of the randomness in the bye value makes Modified LSB algorithm is more efficient.

6. ACKNOWLEDGEMENT

The authors would like to thank the dedicated research group in the area of Stegnography, networks at the Dept of Computer Science, AIMIT, St Aloysius College, Mangalore, India, for many discussions for further improvement and future aspects of the Paper. Lastly but not least the author would like to thank everyone, including the anonymous reviewers.

7. REFERENCES

[1] J. Bieniasz and K. Szczypiorski, "SocialStegDisc: Application of steganography in social networks to create a file system," 2017 3rd International Conference on Frontiers of Signal Processing (ICFSP), Paris, France, 2017, pp. 76-80.

[2] Ö. Çataltaş and K. Tütüncü, "Comparison of LSB image steganography technique in different color spaces," 2017 International Artificial Intelligence and Data Processing Symposium (IDAP), Malatya, Turkey, 2017, pp. 1-6.

[3] C. Vaske, M. Wecksten and E. Jarpe, "Velody — A novel method for music steganography," 2017 3rd International Conference on Frontiers of Signal Processing (ICFSP), Paris, France, 2017, pp. 15-19.

[4] S. N. Gowda, "An intelligent fibonacci approach to image steganography," 2017 IEEE Region 10 Symposium (TENSYMP), Cochin, India, 2017, pp. 1-4. doi: 10.1109/TENCONSpring.2017.8070030

[5] D. Shehzad and T. Dag, "A novel image steganography technique based on similarity of bits pairs," 2017 IEEE 8th Control and System Graduate Research Colloquium (ICSGRC), Shah Alam, 2017, pp. 99-104