IMAGE STEGANOGRAPHY USING LSB TECHNIQUE

[1]Jeevesh Pasrija, [2]Shikha Gupta

[1]UG Student, [2]Assistant Professor
[1,2]Department of Information Technology,
[1,2]Maharaja Agrasen Institute of Technology, Rohini, Delhi-110086, India.

Abstract- Steganography is the art of hiding the fact that communication is occurring by concealing data in some other data. A wide range of carrier file formats can be used, yet digital images are the most prominent because of their high frequency on the web. For hiding secret information in images, there exist a large variety of steganography techniques. This paper addresses the challenges and devises the implementation of LSB technique used for hiding data inside an image.

I. Introduction

It is very important to secure any important information that has to be transferred from a sender to a receiver. Intruders can disclose the information to others, change it to misrepresent an individual or organization, or use it for an attack. This problem can be solved through the use of steganography. Steganography is technique of hiding information in the digital media. In contrast to cryptography, it is not to encrypt the information so that attackers may not get it, but it is used to hide the existence of the information itself. Steganography is an art of concealing information in the ways that prevents detection of hidden information. Steganography includes secret communication methods that hide the information from being seen or discovered. [4]

Digital images are widely used to cover objects for steganography. An image is a collection of bytes containing different light intensities in different areas of image. When dealing with the digital images for use with Steganography, 8-bit and 24-bit per pixel image files are generally used. Both have some advantages as well as disadvantages. 8-bit images are of great format because of their relatively small size. The drawback is that only 256 possible colors can be used that can be potential problem during its encoding. Usually a gray scale color palette is used while dealing with 8-bit images because its gradual change in color would be harder to detect after the image has been encoded with the secret message provided. 24-bit images offer more flexibility when used for Steganography. The large numbers of colors that can be used go well beyond the human visual system, which makes it very hard to detect once the secret message has been encoded. [6]

This paper depicts method to implement encryption and decryption technique on the secret information that has to be hidden into other images which will provide confidentiality to the secret information. Steganography is the technique of hiding information in digital media. In contrast to cryptography, it is not to keep others from knowing hidden information but it is to keep others from thinking that information even exists.

Steganography is art of concealing information in ways that prevents the detection of hidden messages. The growing possibilities of modern communications need special means of security especially on computer network. The network security is important as number of data being exchanged on internet increases. Therefore, confidentiality and data integrity are required to protect against unauthorized access and use. This has resulted in explosive growth of field of information hiding. [8]

The basic steganography model has three things Carrier Image, Secret Message and Encryption Key. Carrier Image is also known as cover-image, inside which secret data is hidden. Thus it serves purpose to hide very existence of secret messages. Secret information is message that sender wants to transmit with confidentiality.

The graphical representation of this system is given below:

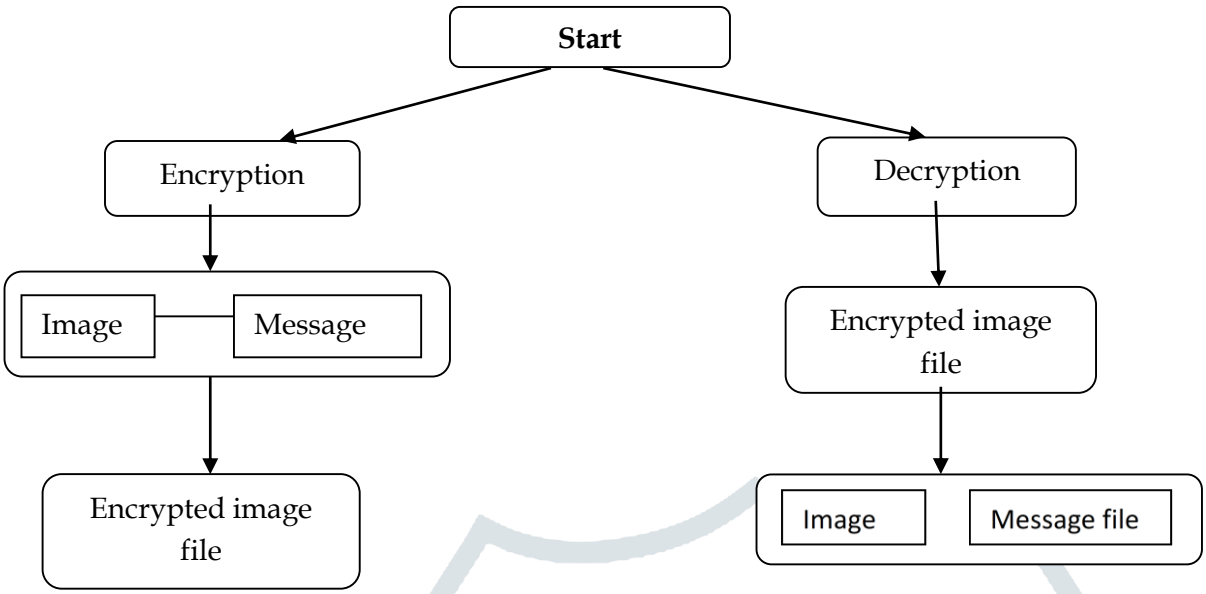

Figure 1: Graphical Representation of Proposed System

II. Related Work

In the year 2015, G. Prashanti and K. Sandhyarani [2] have done survey on recent achievements of LSB based image steganography. In this survey, there are improvements that enhance steganographic results such as high robustness, high embedding capacity and un-detectability of hidden information.

In 2014, Kazem Qazanfari and Reza Safabakhsh [3] proposed an improved version of LSB++ approach. In this improved LSB++ they make distinction between sensitive pixels and allow protecting them from the embedding of extra bits, which results in the lower distortion in co-occurrence matrices.

In the year of 2013 Akhtar, N., Johri, P., Khan, S., [11] implemented a variation of plain LSB (Least Significant Bit) algorithm. The stego-image quality has been improved by using bit-inversion technique. LSB method improves the PSNR of stego-image. Through storing the bit patterns for which LSBs are inverted, image may be obtained correctly.

In the year 2013, M. R. Modi et al [5]. proposed a novel steganography technique to embed secret information of LSBs of the cover image. In their method least two significant bits of edges are utilized to store the secret message as edge regions are very good areas to embed the secret information than other smooth regions of cover image.

In 2012, S. Gupta, G. Gujral and N. Aggarwal [7] proposed an enhanced LSB algorithm for image steganography in which they only embed secret information in blue component of RGB color space. In their technique the first M×N size cover image is selected. After the selection of cover image only the blue component is used for embedding the secret information.

In the year 2009, S. Channalli and A. Jadhav "Steganography an Art of Hiding Data" [9] Authors proposed new LSB based method in which common bit pattern is used to hide data.

III. Methodology:

3.1 RGB Color Model

Pixels are smallest individual element of an image. So, each pixel is sample of an original image. It means more samples provide more accurate representations of original. The intensity of each pixel is a variable. In color imaging systems, color is typically represented by three or four component intensities. Here, we will work with RGB color model.

The RGB color model is an additive color model in which red, green and blue light are added together in various ways to reproduce broad array of colors.[10] The name of model comes from the initials of three additive primary colors, red, green, and blue. The main purpose of RGB color model is for sensing, representation and display of images in electronic systems, though it has also been used in conventional photography.

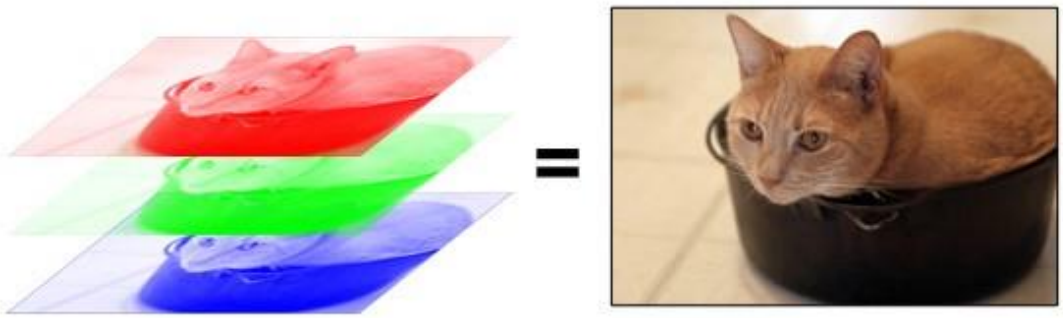

Figure 2: Image formation using RGB colors

3.2 LSB Technique

While working with binary codes, we have more significant bits and less significant bits, as you can see in the image below.

The leftmost bit is the most significant bit. If we change the leftmost bit it will have a large impact on the final value. On the other hand, rightmost bit is less significant bit. If we change rightmost bit, it will have a less impact on final value. [13] The rightmost bit will change only 1 in a range of 256 (i.e. less than 1%).

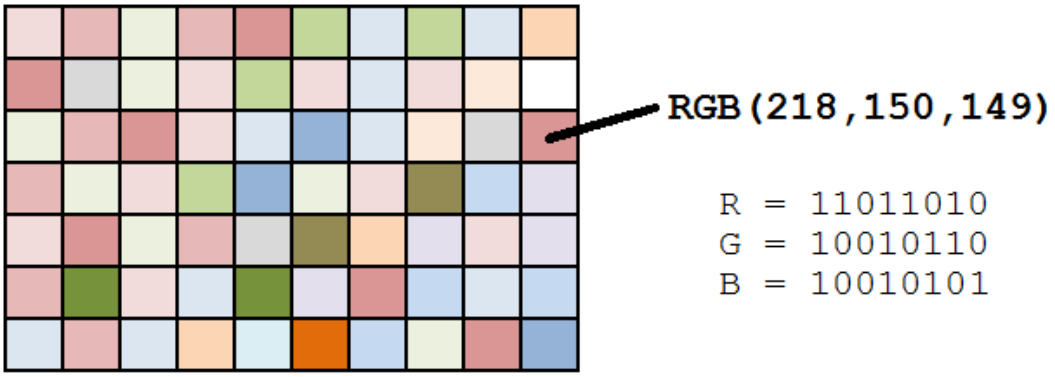

Figure 3: Different RGB value for different colors

Each pixel has three values, each RGB value is 8-bit and the rightmost bits are less significant. So, if we change rightmost bits, it will have a very small visual impact on final image. This is steganography key to hide an image inside another and for this, change less significant bits from an image and include most significant bits from the other image.

Figure 4: Merging the pixels of two images to form new image

In past few years, various steganography techniques that embed hidden messages in multimedia objects have been proposed. Modulating least significant bit does not result in human perceptible difference because amplitude of change is small. [1] In this, the embedding capacity can be increased by using two or more least significant bits.

IV. Results

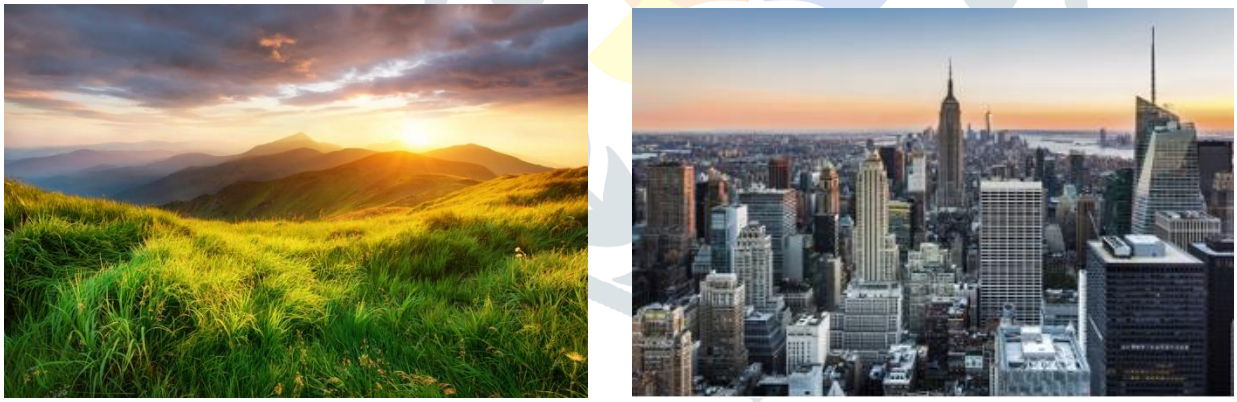

Figure 5: Inputs- (a) Cover Image, (b) Message Image

Figure 6: Outputs- (a) Encrypted Image, (b) Decrypted Message Image

V. Conclusion

The advantage of the LSB technique lies in its ease of implementation and simplicity. The LSB method allows high embedding capacity and uses encryption key and thus is more secure. Hiding the secret data using Steganography lowers the chances of the secret data being detected. LSB technique for the digital images work smoothly for 8 bits and 24 bits BMP, JPG and PNG image formats. Using these algorithms (encoding and decoding), one can retrieve secret message exactly as the original data without altering the cover image.

VI. References

[1]. K. Neeraja, "A Novel Steganographic Approach: Embedding Secret Text In Video", International Journal of Pure and Applied Mathematics, 2018.

[2]. G. Prashanti, K. Sandhyarani, "A New Approach for Data Hiding with LSB Steganography", Emerging ICT for Bridging the Future - Proceedings of the 49th Annual Convention of the Computer Society of India CSI, Springer 2015.

[3]. K. Qazanfari and R. Safabakhsh, "A new Steganography Method which Preserves Histogram: Generalization of LSB++", Elsevier International Journal of Information Sciences, Sept. 2014.

[4]. Shivangi Baranawal, Aparna Gupta,Arti Tiwari ,Amit Pratap Singh, "Steganography Using LSB Algorithm", International Journal of Electronics, Electrical and Computational System, 2014.

[5]. M. R. Modi, S. Islam and P. Gupta, "Edge Based Steganography on Colored Images", 9th International Conference on Intelligent Computing (ICIC), July 2013.

[6]. https://towardsdatascience.com/steganography-hiding-an-image-inside-another-77ca66b2acb1

[7]. S. Gupta, G. Gujral and N. Aggarwal, "Enhanced Least Significant Bit Algorithm for Image Steganography", International Journal of Computational Engineering & Management, July 2012.

[8]. B.B. Zaidan, A.A. Zaidan, A.K. Al-Frajat and H.A. Jalab, On the Differences between Hiding Information and Cryptography Techniques: An Overview. Journal of Applied Sciences, 2010.

[9]. S. Channalli and A. Jadhav, "Steganography an Art of Hiding Data", International Journal on Computer Science and Engineering (IJCSE), 2009.

[10]. https://en.wikipedia.org/wiki/RGB_color_model

[11]. Akhtar, N.; Johri, P.; Khan, S., "Enhancing the Security and Quality of LSB Based Image Steganography," Computational Intelligence and Communication Networks (CICN), Sept. 2013.

[12]. Abhijeet Bhaskar, "Image Steganography using Modified LSB", International Journal of Scientific and Engineering Research (IJSER), 2019

[13]. Ramadhan J. Mstafa, Christian Bach, "Information Hiding in Images Using Steganographic Techniques", March 2013.