IMAGE STEGANOGRAPHY USING MODIFIED LSB

Abhijeet Bhaskar
abhibhas6@gmail.com
Student (B.Tech.), Department of ECE
Galgotia's College of Engineering & Technology
Gr. Noida, UP-201306

Under the supervision of
Mr. Upendra Kumar Acharya
Upendra.acharya@galgottiacollege.edu
Asst. Proff., Dept. of ECE,
Galgotias College of Engineering & Technology
Gr. Noida, UP-201306

ABSTRACT

The proposed method is a quite useful technique for secure communication over the web. In steganography, the hidden message is invisible. This paper depicts methods to implement encryption and decryption techniques on the secret information to be hidden into other images, this will provide confidentiality to the secret information. The sender and the receiver only know the techniques to hide and retrieve the secret message. No third party person will even suspect that there is a hidden message inside the image file. The sender and the receiver only have the knowledge of the instructions to hide and retrieve.

Keywords— *Steganography; Data-hiding; Cover Image; Stego Image; LSB; PSNR; Encryption Key; MSE; UIQI; SSIM;*

1. INTRODUCTION

Steganography is the art of concealing the fact that communication is going on, by hiding secret message into other files. Many types of carrier files are used, but the most popular are digital images because of their massive usages on the internet. To hide data in digital images, there are a number of steganography methods. Each one of them has their strong and weak points. Many applications require complete confidentiality of the secret data, while others may need a large text message to be hidden. Presented method intends to provide a new technique of image steganography and its uses.

Steganography is more important as many people are engaging with the internet. Steganography means hiding secret data in such a way that no third party can detect the hidden data. The difference between steganography and cryptography is that the information is visible in cryptography but is still undeciphered but in steganography, the information is hidden.

2. LITERATURE SURVEY

The word steganography is derived from the Greek word "Seganos", means covered or secret and – "graphy" meaning writing or drawing. Therefore, literally, the meaning of steganography is covered writing. It is the technique of making information invisible such that its presence cannot be sensed by a third party that communication is going on. A secret message is encoded such that even the presence of the data is hidden. Along with other communication techniques, steganography can be used to transmit secret messages.

The main target of the presented technique is to transmit message securely in a completely unnoticeable way and to avoid any kind of suspicion to the transmission of a hidden information. In the modern world, the interest in steganography has been increased very rapidly primarily because of two reasons:

- The publishing & broadcasting sector needs steganography technique for hiding copyright related piecess of informations and serial numbers in digital films, audio, and video recordings, books, articles and multimedia products.
- Due to rapidly increasing cases of data theft throughout the whole world, people have been self-motivated to study and implement methods by which personal information can be hidden secretly within the cover images.

The basic steganography model have Carrier Image, Secret Message and Encryption Key. Carrier Images are also known as cover-image, inside which the secret data is hidden. Thus it serves the purpose to hide the very existence of the secret messages.

Secret Information is the message that the sender wants to transmit with confidentiality. It is of many types like plain text, cipher-text, or anything that can be embedded in a stream of bits such as a copyright logo, a secret communication, or any kind of serial number. Encryption Key ensures that only the intended receiver who knows the decoding technique will be able to retrieve the message from a cover-image. The cover-image with the embedded secret information is called the Stego-image.

Retrieving the secret information from a stego-image needs the cover-image itself and the Encryption Key which was used during the process of encoding. The best part is that the original image is not even required in the presented method to retrieve the hidden data.

3. PROPOSED METHODOLOGY

Least significant bit (LSB) insertion is a simple yet efficient approach for embedding data into a digital image. The simplest steganography technique inserts the bits of the data directly into the least significant bits, i.e. LSB of the cover-image in a particular sequence.

Digital images are used as cover images. They are mainly of two types- 24-bit images and 8-bit images. In 24-bit images, we can insert up to three bits of data into each pixel. In 8-bit images, one bit of data can be hidden into each pixel. After applying the LSB method, the output image within which the secret message is embedded is called stego-image. LSB technique, as the name suggests replaces the least significant bit of each pixel with the data that is to be hidden. Since LSB is replaced, there is no major or any noticeable effect on the cover image and hence third party users will not be able to even suspect that any information is embedded inside the cover-image. However, obviously, there will be a minor unnoticeable change in the intensity level of original and stego image, but it is almost impossible to be detected by naked eyes.

Following example shows how the letter A is embedded into the 3 pixels, i.e. 8 bytes of a 24-bit image.

Pixels: (00100111 11101011 11001010)

(00100111 11011000 10101001)

(11001000 00110111 11011001)

A: 01010011

Result: (0010011**0** 11101011 11001010)

(00100111 11011000 1010100**0**)

(1100100**1** 00110111 11011001)

One of the best advantages of LSB technique is easy to implement and large message capacity. Also, there is very small chance of change in the quality of the cover image.

Changing the least significant bits does not result in any kind difference which is noticeable to the human eye because the amount of the change is almost negligible. In the presented method, the hiding capacity can be increased, as per need by using two or three least significant bits, but we have kept it to only one bit to keep the quality of the stego-image.

3.1 Encoding

Steps for Encoding:

1. Read the Secret Message.
2. Count the length of Secret Message.
3. Create a Final Message which is Length of Secret message added before the Secret Message.
4. Read Encryption Key.
5. Encrypt the Final Message with the Encryption Key and name it (say Embed Message).
6. Read Cover Image.
7. Access Cover Image in a particular RGB and replace each bit of Embed Message in the LSB of each color component of every pixel until each message bit is hidden.
8. Reorganize the pixels of the Cover Image.
9. Name the resultant Stego-Image.
10. Save the Stego image.

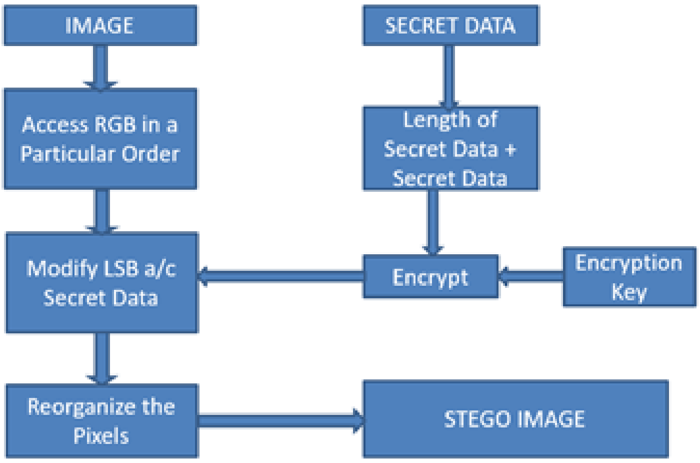
IMAGE
SECRET DATA
Access RGB in a Particular Order
Length of Secret Data + Secret Data
Modify LSB a/c Secret Data
Encrypt
Encryption Key
Reorganize the Pixels
STEGO IMAGE

Fig -1: Block Diagram of Encoding

3.2 Decoding

Steps for Decoding:

1. Read the Stego-Image.
2. Access the Stego-Image in a particular order and retrieve first 8 bits of the Stego-Image.
3. Find the length of the Secret Message from the retrieved first 8 bits.
4. Start count.
5. Access the Stego-Image in the particular order and retrieve the LSB of each pixel until the count is less than the length of the Secret Message.
6. Read the Decryption Key.
7. Decrypt the Secret Message and Convert it to Char format.
8. Create a Text File in .txt format.
9. Store the decrypted messages in the text file.

10. Save the TXT file, which contains the Secret Message.

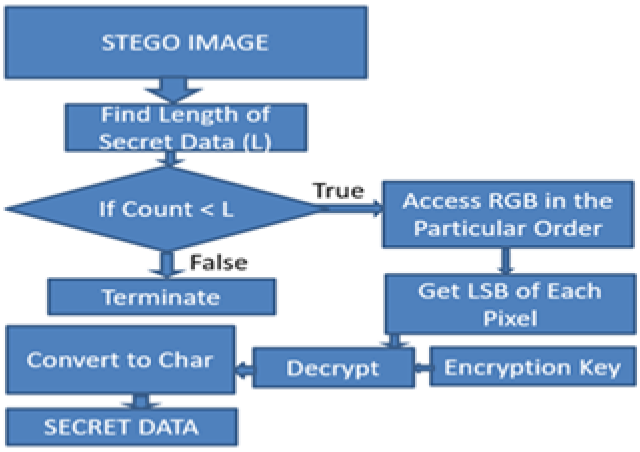

Fig -2: Block Diagram of Decoding

4. RESULT & ANALYSIS

A. Mean Squared Error (MSE)

It measures the average of the squares of the errors—that is, the average squared difference between the estimated values and what is estimated.

$$MSE = \left[\frac{1}{M*N}\right] \sum_{i=1}^{M}\sum_{j=1}^{N}\left(X_{ij} - X'_{ij}\right)^2$$

B. Peak Signal to Noise Ratio (PSNR)

It is the ratio between the maximum possible power of a signal and the power of corrupting noise that affects the fidelity of its representation.

$$PSNR = 10log_{10}\frac{255^2}{MSE}\ dB$$

C. Universal Image Quality Index (UIQI)

It breaks the comparison between original and distorted image into three comparisons: luminance, contrast, and structural comparisons.

$$l(x,y) = \frac{2\mu_x\mu_y}{\mu_x^2\mu_y^2}$$

$$c(x,y) = \frac{2\sigma_x\sigma_y}{\sigma_x^2+\sigma_y^2}$$

$$s(x,y) = \frac{2\sigma_{xy}}{\sigma_x+\sigma_y}$$

Where $\mu_x\mu_y$ denotes the mean values of original and distorted images. And σ_x σ_y denotes the standard deviation of original and distorted images, and σ_{xy} is the covariance of both images. Based on the above three comparisons the UIQI is:

$$UIQI(x,y) = l(x,y).c(x,y).s(x,y) = \frac{4\mu_x\mu_y\mu_{xy}}{(\mu_x^2+\mu_y^2)(\sigma_x^2+\sigma_y^2)}$$

UIQI is a simple measure that counts only on the first and second-order statistic of the original and distorted images.

D . Structural Similarity Index (SSIM)

The Structural Similarity (SSIM) index is a method for measuring the similarity between two images.

The SSIM index can be viewed as a quality measure of one of the images being compared, provided the other image is regarded as of perfect quality.

Fig -3: Cover Image

Fig -4: Stego Image

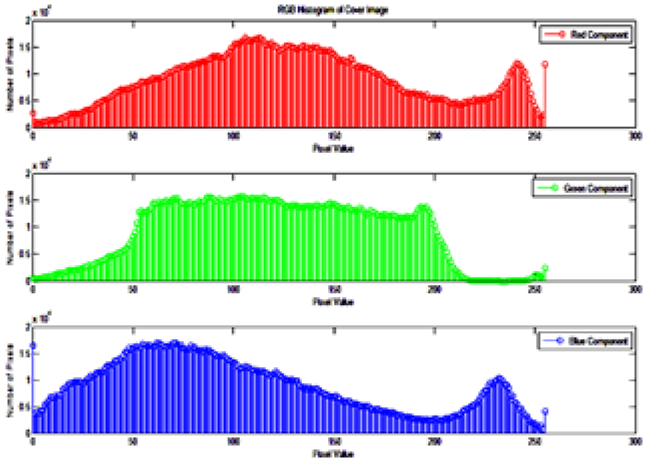

Fig -5: RGB Histogram of Cover Image

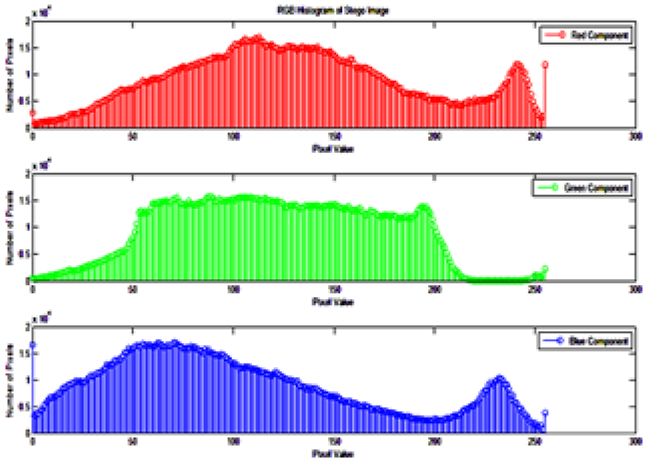

Fig -6: RGB Histogram of Stego Image

Table -1: PSNR and MSE comparison

IMAGES	MSE (Ref.)	PSNR (Ref.)	MSE (Proposed)	PSNR (Proposed)
Colored Chips	7.6294 e-04	79.3059	9.7101 e-05	88.2586
Iron	0.0058	70.4807	6.6021 e-05	89.9340
Nasa	0.0115	67.5406	2.9861 e-05	93.3797
Car	1.6022 e-04	86.0837	1.1338 e-05	97.5855
Ballon	0.0034	72.8664	1.1042 e-05	97.7005

Fig -8: Cover Car

Fig -7: Stego Car

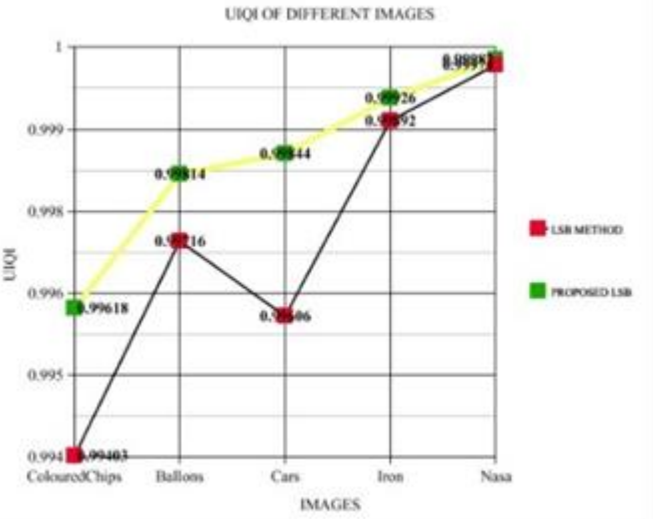

Fig -9: UIQI of different images

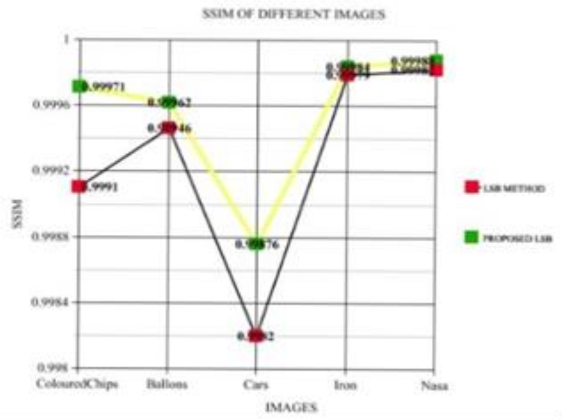

Fig -10: SSIM of different Images

5. KEY POINTS OF PROPOSED METHOD

- More information can be hidden in a single image file.
- A pre-decided particular RGB order of LSB Modification, which serves as the second password.
- Requires Passkey to decode.
- Double Layer Security, thus more secure.
- Only one bit LSB modification, thus no considerable effect on the Image.
- No need to decode all pixels to get the required message. The Header is used to terminate the decoding.
- No change in Image Shape.

6. CONCLUSION

The advantage of LSB technique lies in its simplicity and ease of implementation. LSB method also allows high embedding capacity. The LSB technique uses encryption key and thus is more secure. Hiding secret data using Steganography method lowers the chances of secret data being detected. LSB technique for digital image Steganography works smoothly for 8 bits and 24 bits BMP, GIF and PNG image formats.

Using this encoding and decoding algorithms, one can retrieve the secret message exactly as original data without altering the cover image.

7. REFERENCES

[1] Al-Shatnawi, A.M., 2012. A new method in image steganography with improved image quality. Applied Mathematical Sciences, 6(79), pp.3907-3915.

[2] Gupta, S., Goyal, A. and Bhushan, B., 2012. Information hiding using least significant bit steganography and cryptography. International Journal of Modern Education and Computer Science, 4(6), p.27.

[3] Mandal, J.K. and Das, D., 2012. Colour image steganography based on pixel value differencing in spatial domain. International journal of information sciences and techniques, 2(4).

[4] Emam, M.M., Aly, A.A. and Omara, F.A., 2016. An improved image steganography method based on lsb technique with random pixel selection. International Journal of Advanced Computer Science and Applications, 7(3), pp.361-366.

[5] Kaur, G. and Kochhar, A., 2012. A steganography implementation based on LSB & DCT. International Journal for Science and Emerging Technologies with Latest Trends, 4(1), pp.35-41.

[6] Thenmozhi, M.J. and Menakadevi, T., 2016. A New Secure Image Steganography Using Lsb And Spiht Based Compression Method. International Journal of Engineering Research & Science (IJOER), 2(3), pp.81-85.

[7] Shabnam, S. and Hemachandran, K., 2016. LSB based Steganography using Bit masking method on RGB planes. IJCSIT) International Journal of Computer Science and Information Technologies, 7(3), pp.1169-1173.

[8] Datta, B., Mukherjee, U. and Bandyopadhyay, S.K., 2016. LSB Layer Independent Robust Steganography using Binary Addition. Procedia Computer Science, 85, pp.425-432.

[9] Pandit, A.S. and Khope, S.R., 2016. Faculty Student." Review on Image Steganography.". International Journal of Engineering Science, 6115.

[10] Artz, D., 2001. Digital steganography: hiding data within data. IEEE Internet computing, 5(3), pp.75-80.

[11] Jamil, T., 1999. Steganography: the art of hiding information in plain sight. IEEE potentials, 18(1), pp.10-12.

[12] Wang, H. and Wang, S., 2004. Cyber warfare: steganography vs. steganalysis. Communications of the ACM, 47(10), pp.76-82.

[13] Johnson, N.F. and Jajodia, S., 1998, April. Steganalysis of images created using current steganography software. In International Workshop on Information Hiding (pp. 273-289). Springer, Berlin, Heidelberg.

[14] Provos, N. and Honeyman, P., 2003. Hide and seek: An introduction to steganography. IEEE security & privacy, 99(3), pp.32-44.

[15] Pavani, M., Naganjaneyulu, S. and Nagaraju, C., 2013. A survey on LSB based steganography methods. International Journal of Engineering and Computer Science, 2(8), pp.2464-2467.

[16] Baby, D., Thomas, J., Augustine, G., George, E. and Michael, N.R., 2015. A novel DWT based image securing method using steganography. Procedia Computer Science, 46, pp.612-618.