EUROPEAN ACADEMIC RESEARCH
Vol. II, Issue 10/ January 2015

Impact Factor: 3.1 (UIF)
DRJI Value: 5.9 (B+)

ISSN 2286-4822
www.euacademic.org

Comparison Study of LSB Steganography for JPEG and GIF Images

ELAF JABBAR ABDUL RAZZAQ AL-TAEE
Kufa University, Iraq

Abstract:

The main purpose of steganography in current paper is to hide secret image using the Least Significant Bit (LSB) technique inside cover image so that the human eye would be unable to notice the hidden image in the cover file and it became difficult for attacker to detect it. This paper introduced comparing study between two types of images format (Gif and JPEG) used as a cover. The effectiveness of the comparison based on quality measures were done by computing RMSE, SNRrms, SNRpeak, and MAE. The results showed that the LSB steganography in JPEG images is better than GIF images.

Key words: Steganography, LSB, JPEG, GIF, BMP,DCT, Quality Measures

1. Introduction

In this modern era, computers and the internet are major communication media that connect different parts of the world as one global virtual world. As a result, people can easily exchange information and distance is no longer a barrier to communication. However, the safety and security of long-distance communication remains an issue [1].

Cryptography and Steganography are the ways to provide the security to the information. Cryptography is used to encrypt the message so that it is protected from any third

parties. Steganography is a method that is used to hide information in a cover so that nobody can guess it [2].

The word steganography is derived from Greek words Steganos and graphia. Steganos means covered and graphia means writing. Thus steganography means covered writing which is an art of covert communication. The word steganography is invented by the Trithemium who done an explicit work on cryptography [3].

The goal of steganography is to hide data inside cover medium in such a way that does not allow any "enemy" to even detect that there is a secret data present in cover medium. Steganography attempts to hide the existence of communication. The cover medium can be image, text, audio/video, or protocol [4].

Images are ideal for information hiding because of the large amount of redundant space is created in the storing of images. Secret images are transferred through unknown cover carriers in such a manner that the very existence of the embedded images is undetectable [5].

2. Related Works

Gurmeet et al. present a comparative analysis to demonstrate the effectiveness of the proposed methods. The effectiveness of the proposed methods has been estimated by computing Mean square error (MSE) and Peak Signal to Noise Ratio (PSNR), Processing time, security. The analysis shows that the BER and PSNR is improved in the LSB Method but security sake DCT is the best method **[**6].

Ravinder et al. introduce analyzing to the various steganography algorithms and stenographic application such that it provides good security. The proposed approach provides higher security and can protect the message from stego attacks [7].

Eltyeb. compares and analyses Least Significant Bit algorithm using the cover object as an image with a focus on two types: BMP and JPEG. The comparison and analysis are done with respect to a number of criteria to understand their strengths and weaknesses. [8].

3. The LSB Technique

Least significant bit (LSB) insertion is a common and simple approach to embed information in an image file. This technique works good for image steganography. The human eye the stego image will look identical to the cover image. For hiding information inside the images, the LSB (Least Significant Bit) method is usually used. The least significant bit i.e. the eighth bit is used to change to a bit of the secret image. When using a 8-bit image, one can store 1 bit in each pixel by changing a bit of each of the gray scale components. Suppose that we have eight adjacent pixels (8 bytes) with the gray scale encoding

10010101 00001100 11001001 10010110 00001111 11001011 10011111 00010000

When the number 200, can be which binary representation is 11001000 embedded into the least significant bits of this part of the image. If we overlay these 8 bits over the LSB of the 8 bytes above we get the following (where bits in bold have been changed)

10010101 00001101 11001000 10010110 00001111 11001010 10011110 00010000

Here the number 200 was embedded into the grid, only the 4 bits needed to be changed according to the embedded image. On average, only half of the bits in an image will need to be modified to hide a secret image using the maximum cover size.

3.1 LSB in GIF

Graphics interchange format also known as GIF is one of the machine independent compressed formats for storing images. We can used GIF images for LSB steganography, although extra care should be taken. After convert cover image and secret image to binary, calculate the least significant bit of each pixels of cover image to embed one bit of secret image to finally produce the GIF stego image. During the extraction process, calculate LSB of each pixels of the GIF stego image. Retrieve bits and convert each 8 bit into pixel. The main issue with the palette based approach is that if one changes the least significant bit of a pixel, it could result in an entirely different color since the index to the color palette gets modified. One possible solution to this problem is to sort the palette so that the color differences between consecutive colors are minimized. The strong and weak points regarding embedding information in GIF images using LSB is that since GIF images only had a bit depth of 8, the total amount of information that could be embedded will be less. GIF images are vulnerable to statistical as well as visual attacks, since the palette processing which has to be done on the GIF image leaves a clear signature on the image. This approach was dependent on the file format as well as the image itself, since a wrong choice of image could results in the image being visible. Fig 1 shows applying LSB technique on GIF images.

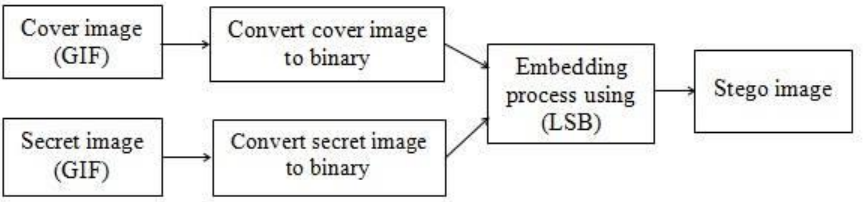

Fig 1: Applying LSB technique on GIF images

3.2 LSB in JPEG

The most commonly used method to embed a bit is LSB embedding, where the least significant bit of a JPEG coefficient is modified in order to embed one bit of secret image. Once the required secret image bits have been embedded, the modified coefficients are compressed using entropy encoding to finally produce the JPEG stego image. By embedding information in JPEG coefficients, it is difficult to detect the presence of any hidden data since the changes are usually not visible to the human eye in the spatial domain. During the extraction process, the JPEG file is entropy decoded to obtain the JPEG coefficients, from which secret image bits are extracted from the LSB of each coefficient.

LSB embedding is the most common technique to embed secret image bits DCT coefficients. This method has also been used in the spatial domain where the least significant bit value of a pixel is changed to insert a zero or a one. A simple example would be to associate an even coefficient with a zero bit and an odd one with a one bit value. In order to embed a secret image bit in a pixel or a DCT coefficient, the sender increases or decreases the value of the coefficient/pixel to embed a zero or a one. The receiver then extracts the hidden secret image bits by reading the coefficients in the same sequence. And decoding them in accordance with the encoding technique performed on it. The advantage of LSB embedding is that it has good embedding capacity and the change is usually visually undetectable to the human eye. If all the coefficients using the frequency domain technique. Fig 2 shows applying LSB technique on JPEG images.

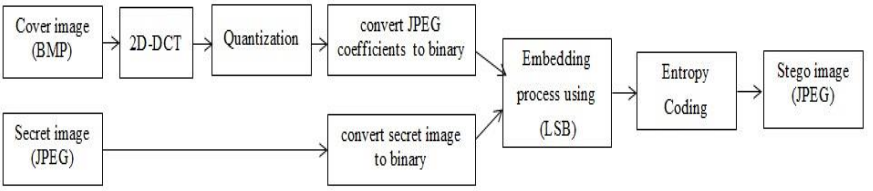

Fig 2: Applying LSB technique on JPEG images

4. Results and Discussions

Following experimental results highlights on 8 bit LSB Steganography, as shown in figures (3 and 4).

Fig 3: LSB technique results on GIF images

Fig 4: LSB technique results on JPEG images

For comparing g(r,c):stego image with I(r,c):cover image results requires a measure of image quality, this measures are defined by the following relations, and are applied to ten images (GIF-JPEG) as shown in figures (5, 6, 7, and 8).

1. Root-Mean-Square Error

$$RMSE = \sqrt{\frac{1}{N^2}\sum_{r=0}^{N-1}\sum_{c=0}^{N-1}[g(r,c) - I(r,c)]^2}$$

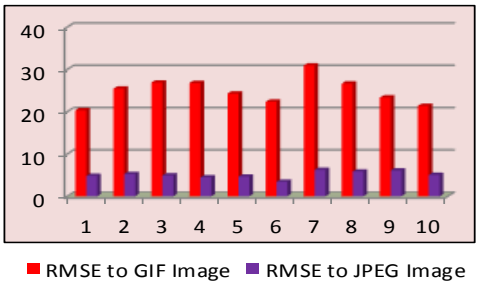

Fig 5: Root-Mean-Square Error to (GIF-JPEG) images

2. Root-Mean-Square Signal-to-Noise- Ratio

$$SNR_{RMS} = \sqrt{\frac{\sum_{r=0}^{N-1}\sum_{c=0}^{N-1}[g(r,c)]^2}{\sum_{r=0}^{N-1}\sum_{c=0}^{N-1}[g(r,c)-I(r,c)]^2}}$$

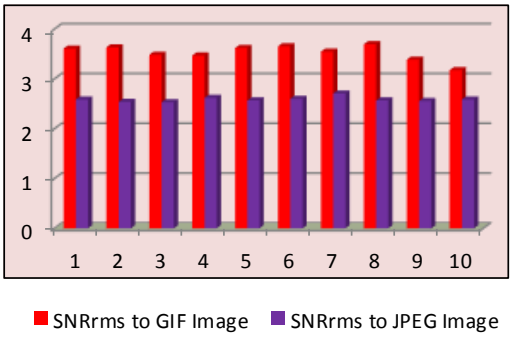

Fig 6: Root-Mean-Square Signal-to-Noise- Ratio to (GIF-JPEG) images

3. Peak Signal-to-Noise- Ratio

$$SNR_{PEAK} = 10\log_{10}\frac{(L-1)^2}{\frac{1}{N^2}\sum_{r=0}^{N-1}\sum_{c=0}^{N-1}[g(r,c)-I(r,c)]^2}$$

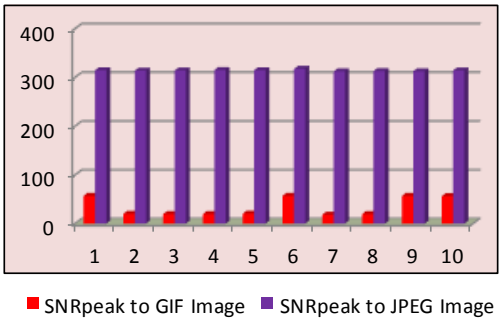

Fig 7: Peak Signal-to-Noise- Ratio to (GIF-JPEG) images

4. Mean Absolute Error

$$MAE = \frac{1}{N^2}\sum_{r=0}^{N-1}\sum_{c=0}^{N-1} abs[g(r,c) - I(r,c)]$$

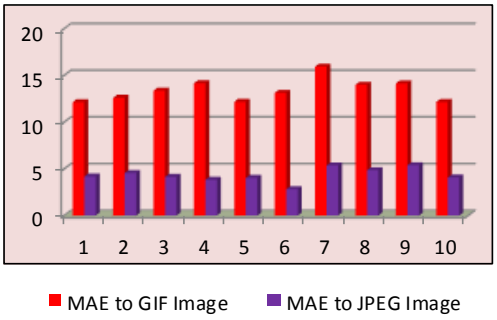

Fig 8: Mean Absolute Error to (GIF-JPEG) images

It is clear from the above measurements that the LSB steganography in JPEG images is better than GIF images.

5. Conclusion

Steganography is an effective way to embed secret image in cover image. In this paper the LSB technique is implemented

for GIF and JPEG image formats. From the quality measuring which including computing RMSE, SNRrms, SNRpeak, and MAE, it found that LSB in JPEG is more better than LSB used in GIF, as showed in figures (5, 6, 7, and 8).

The size of embedding data in GIF image format is less than the size of embedded data in JPEG image format.

When the hiding data increased in cover of type GIF format, this leads to distorted the cover and make sign to detect the exists of embedding data.

REFERENCES

[1] Nagham H., Abid Y., R. B., and Osamah M., 2012. "Image Steganography Techniques: An Overview", International Journal of Computer Science and Security (IJCSS), Volume (6) : Issue (3).

[2] Shivani K., and Nishi M., 2014." A Comparative Study of Image Steganography Techniques", International Journal of Science and Research (IJSR), Volume 3 Issue 4, April.

[3] T.V., S. Varadarajan, and T. Ravi, 2013." Improved Quality of Image Steganography Using POLPA",International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering, Vol. 2, Issue 12.

[4] Shilpa G., Geeta G., and Neha A., 2012." Enhanced Least Significant Bit algorithm For Image Steganography", IJCEM International Journal of Computational Engineering & Management, Vol. 15 Issue 4.

[5] V. Lokeswara, A. Subramanyam, and P. Chenna, 2011." Implementation of LSB Steganography and its Evaluation for Various File Formats", Int. J. Advanced Networking and Applications, Volume: 02, Issue: 05.

[6] Gurmeet K., and Aarti K., 2012."A Steganography Implementation based on LSB & DCT", international Journal

for Science and Emerging Technologies with Latest Trends.

[7] Saeed A., Kabirul I., and Baharul I., 2013." A Novel Approach for Image Steganography Using Dynamic Substitution and Secret Key", American Journal of Engineering Research (AJER), Volume-02, Issue-09.

[8] Eltyeb E., 2013."Comparison of LSB Steganography in BMP and JPEG Images", International Journal of Soft Computing and Engineering (IJSCE), Volume-3, Issue-5.