Image Hiding using Improved Bit Inversion LSB Steganography Technique

Harsimran Singh Sekhon
Department of Computer Science Engineering
ASRA College of Engineering &Technology, Bhawanigarh, India
hsekhon1988@gmail.com

Sourav Garg
Faculty of Computer Science Engineering Department
ASRA College of Engineering &Technology, Bhawanigarh, India

Abstract- Steganography is an effective way to hide sensitive information. In this paper we have used the LSB steganography and improved bit inversion LSB steganography on images to obtain secure stego-image. Results shows that PSNR of improved bit inversion LSB stegnography is higher than PSNR of bit inversion LSB steganography and MSE of improved bit inversion LSB steganography is less than MSE of bit inversion LSB steganography. This paper focuses on the approach like increasing the security of the message and increasing PSNR and reducing the distortion rate.

Keywords – Steganography, Image, PSNR, MSE.

I. INTRODUCTION

Steganography [1] is the art of hiding information imperceptibly in a cover medium. The word “Steganography” is of Greek origin and means “covered or hidden writing”. The main aim in steganography is to hide the very existence of the message in the cover medium. Steganography includes a vast array of methods of secret communication that conceal the very existence of hidden information. Traditional methods include use of invisible inks, microdots etc. Modern day steganographic techniques try to exploit the digital media images, audio files, video files etc.

Steganography and cryptography are cousins in the spy craft family. Cryptography scrambles a message by using certain cryptographic algorithms for converting the secret data into unintelligible form. On the other hand, Steganography hides the message so that it cannot be seen. A message in cipher text might arouse suspicion on the part of the recipient while an “invisible” message created with steganographic methods will not. Anyone engaging in secret communication can always apply a cryptographic algorithm to the data before embedding it to achieve additional security. In any case, once the presence of hidden information is revealed or even suspected, the purpose of steganography is defeated, even if the message content is not extracted or deciphered. Steganography’s niche in security is to supplement cryptography, not replace it. If a hidden message is encrypted, it must also be decrypted if discovered, which provides another layer of protection.

II. IMAGE STEGANOGRAPHIC TECHNIQUES

There are several Steganographic techniques for image file format which are as follows[3]:

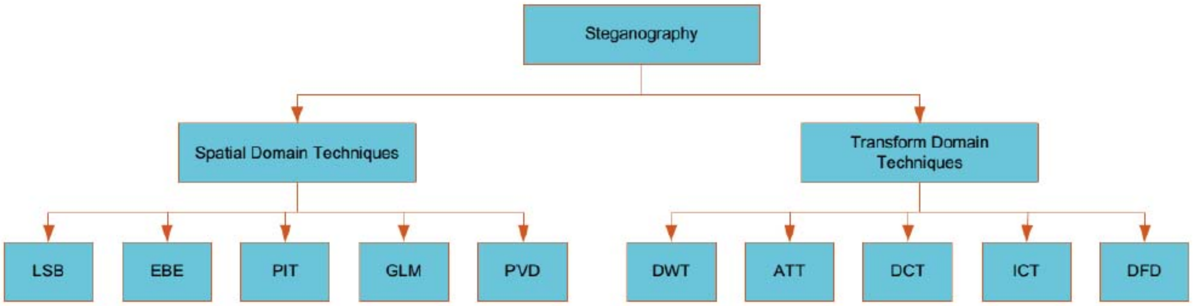


Figure 1. Classifications of steganographic techniques

1. Spatial Domain Technique

There are many versions of spatial steganography, all directly change some bits in the image pixel values in hiding data. Least significant bit (LSB)-based steganography is one of the simplest techniques that hides a secret message in the LSBs of pixel values without perceptible distortions. To our human eye, changes in the value of the LSB are imperceptible. Embedding of message bits can be done either simply or randomly. The least significant bit (in other words, the 8th bit) of some or all of the bytes inside an image is changed to a bit of the secret message. Digital images are mainly of two types (i) 24 bit images and (ii) 8 bit images. In 24 bit images we can embed three bits of information in each pixel, one in each LSB position of the three eight bit values. Increasing or decreasing the value by changing the LSB does not change the appearance of the image; much so the resultant stego image looks almost same as the cover image. In 8 bit images, one bit of information can be hidden.

A stego-image is obtained by applying LSB algorithm on both the cover and hidden images. The hidden image is extracted from the stego-image by applying the reverse process.

Advantages of spatial domain LSB technique are:

1.Degradation of the original image is not easy.

2.Hiding capacity is more i.e. more information can be stored in an image.

Disadvantages of LSB technique are:

1.Robustness is low

2.Hidden data can be destroyed by simple attacks.

In this paper, improved LSB inversion method to improve the quality of final image is proposed. Two schemes of the method are implemented.

2. Masking and Filtering

Masking and Filtering is a steganography technique which can be used on gray- scale images. Masking and filtering is similar to placing watermarks on a printed image. These techniques embed the information in the more significant areas than just hiding it into the noise level. Watermarking techniques can be applied without the fear of image destruction due to lossy compression as they are more integrated into the image.

Advantages of Masking and filtering Techniques:

This method is much more robust than LSB replacement with respect to compression.

Disadvantages:

Techniques can be applied only to gray scale images and restricted to 24 bits.

3. Transform Domain Technique

The Frequency domain the message is inserted into transformed coefficients of image giving more information hiding capacity and more robustness against attacks. Transform domain embedding can be termed as a domain of embedding techniques for which a number of algorithms have been suggested. Most of the strong steganographic systems today operate within the transform domain Transform domain techniques have an advantage over LSB techniques as they hide information in areas of the image that are less exposed to compression, cropping, and image processing. Some transform domain techniques do not seem dependent on the image format and they may outrun lossless and lossy format conversions.

Transform domain techniques are of different types:

- Discrete Fourier transformation technique (DFT).
- Discrete cosine transformation technique (DCT).
- Discrete Wavelet transformation technique (DWT).

Distortion Techniques

In this technique, store information by signal distortion and measure the deviation from the original cover in the decoding process. Distortion techniques need knowledge of the original cover image during the decoding process where the decoder functions to check for differences between the original cover image and the distorted cover image in order to restore the secret message. In this technique, a stego-image is created by applying a sequence of modifications to the cover image. This sequence of modifications is use to match the secret message required to transmit. The message is encoded at pseudo-randomly chosen pixels. If the stego-image is different from the cover image at the given message pixel, the message bit is a 1. Otherwise, the message bit is a 0. The encoder can modify the 1 value pixels in such a manner that the statistical properties of the image are not affected. If an attacker interferes with the stego-image by cropping, scaling or rotating, the receiver can easily detect it.

III. RESULTS

The proposed method is simulated using MATLAB. For experiments, different amount of sensitive data is embedded in different standard color images. The standard color images used for experimental purposes include baboon.jpeg. The proposed method is evaluated experimentally from three different viewpoints.

Objective analysis using PSNR and MSE is performed on the proposed method to evaluate its performance. PSNR is a statistical image quality assessment standard used for measuring the obvious distortion between stego and cover image. The PSNR is measured in decibels (dB)[3]. PSNR values below 30dB show low quality of stego images and hence it brings noticeable changes in stego images which can be seen by naked eyes[4, 5]. To achieve good quality of stego images, PSNR value must be 40dB or above than 40bB[6]. MSE is used to calculate the error between the original and stego image[7].

In this paper we compare the bit inversion LSB stegnographic technique and improved bit inversion LSB stegnographic technique.

Figure 2 to figure 7 shows the results of Improved bit inversion LSB stegnographic technique.

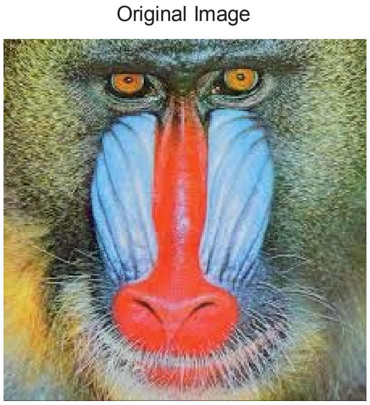


Figure 2. Original image

Figure 2 shows the original image.

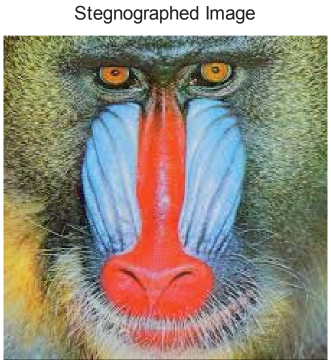
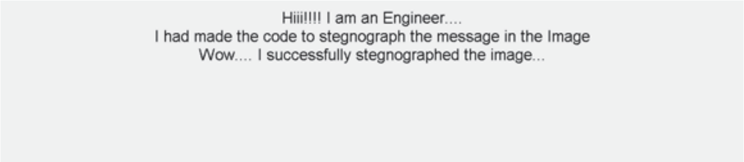


Figure 3. Stegnographed image

Figure 3 shows the stegnographed image.



Hiii!!!! I am an Engineer....
I had made the code to stegnograph the message in the Image
Wow.... I successfully stegnographed the image...

Figure 4. Secret Message

Figure 4 shows the secret message.

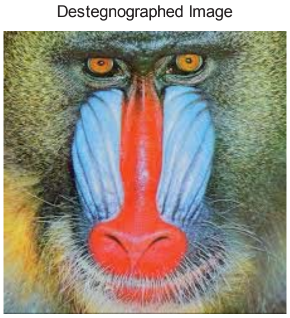
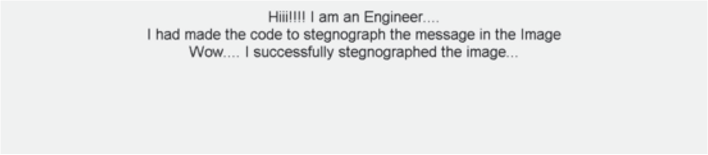


Figure 5. Destegnographed image

Figure 5 shows the destegnographed image.



Hiii!!!! I am an Engineer....
I had made the code to stegnograph the message in the Image
Wow.... I successfully stegnographed the image...

Figure 6. Secret Message extracted from the cover image

Figure 6 shows the secret message which is extracted from the cover image.

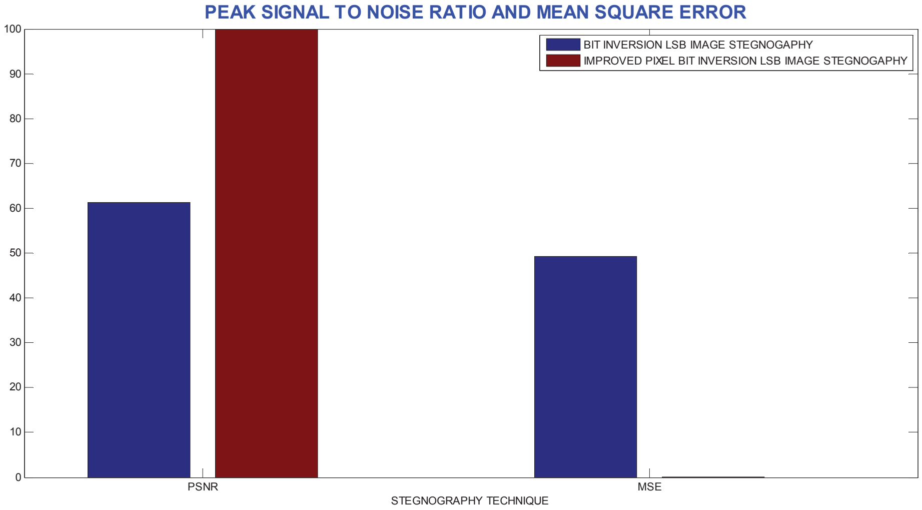


Figure 7. Comparison bar graph of bit inversion LSB stegnographic technique and improved bit inversion LSB stegnographic technique

Figure 7 shows the comparison bar graph of bit inversion LSB stegnographic technique and improved bit inversion LSB stegnographic technique. This results shows that PSNR of improved bit inversion LSB stegnography is higher than PSNR of bit inversion LSB stegnography and MSE of improved bit inversion LSB stegnography is less than MSE of bit inversion LSB stegnography Our results indicate that the improved bit inversion LSB stegnography is better than simple bit inversion LSB stegnography.

IV.CONCLUSION

Our results indicate that the improved bit inversion LSB stegnography is better than simple bit inversion LSB stegnography.The image resolution doesn't change much and is negligible when we embed the message into the image and the image is protected. So, it is not possible to damage the data by unauthorized personnel.

Now a days, image steganography is broadly used in steganography field. So there is lot to do as per research is concerned. We can use EXOR and improved LSB algorithm with other cryptographic algorithms and steganographic algorithms which can reduce the space and time complexity and increase the level of security.

REFERENCES

[1] Piyush Goel and Jayanta Mukherjee(2008), “Data Hiding in Digital Images : A Steganographic Paradigm”.

[2] Kshetrimayum Jenita Devi and Sanjay Kumar Jena(2013), “A Sesure Image Steganography Using LSB Technique and Pseudo Random Encoding Technique”.

[3] M. Sajjad, I. Mehmood, N. Abbas, and S. W. Baik, "Basis pursuit denoising-based image superresolution using a redundant set of atoms," Signal, Image and Video Processing, pp. 1-8, 2014.

[4] M. Sajjad, I. Mehmood, and S. W. Baik, "Image super-resolution using sparse coding over redundant dictionary based on effective image representations," Journal of Visual Communication and Image Representation, vol. 26, pp. 50-65, 2015.

[5] R. J. Mstafa and K. M. Elleithy, "A highly secure video steganography using Hamming code (7, 4)," in Systems, Applications and Technology Conference (LISAT), 2014 IEEE Long Island, 2014, pp. 1-6.

[6] M. Sajjad, I. Mehmood, and S. W. Baik, "Sparse representations-based super-resolution of key-frames extracted from frames-sequences generated by a visual sensor network," Sensors, vol. 14, pp. 3652-3674, 2014.

[7] M. Sajjad, N. Ejaz, I. Mehmood, and S. W. Baik, "Digital image super-resolution using adaptive interpolation based on Gaussian function," Multimedia Tools and Applications, pp. 1-17, 2013.