International Journal of Trend in Scientific Research and Development (IJTSRD)
Volume: 3 | Issue: 4 | May-Jun 2019 Available Online: www.ijtsrd.com e-ISSN: 2456 - 6470

LSB Based Stegnography to Enhance the Security of an Image

Naveen Verma[1], Preeti Sondhi[2], Gargi Kalia[2]

[1]M.Tech Student, [2]Faculty

[1,2]Computer Science and Engineering, Universal Institute of Engineering and Technology, Lalru, Punjab, India

How to cite this paper: Naveen Verma | Preeti Sondhi | Gargi Kalia "LSB Based Stegnography to Enhance the Security of an Image" Published in International Journal of Trend in Scientific Research and Development (ijtsrd), ISSN: 2456-6470, Volume-3 | Issue-4, June 2019, pp.1480-1484, URL: https://www.ijtsrd.com/papers/ijtsrd25163.pdf

IJTSRD25163

ABSTRACT

Steganography is the technique of hiding a secret message or information in a cover message like an image, text or sound in such a way that only the desired or intended recipient knows about the existence of the secret data. It can be defined as the study of invisible communication which usually deals with the technique of hiding the existence of the secret message. The hidden message may be in the form of text, image, audio and video etc. An image after inserting the secret message into it by using a stego-key is known as a stego-image. Nowadays steganography is important due to an exponential growth in secret communication by potential computer users over the internet. In this paper we have analyzed the various steganography techniques and propose to enhance the security of the secret message by random selection of the keys to extract the secret message and working towards increasing the PSNR (Peak Signal to Noise Ratio) and decreasing the MSE (Mean Square Error).

Keywords: *steganography; data hiding; stego image; stego-image; LSB; encryption*

1. Introduction

In recent trends in the world, the communication is an indispensable need of every growing area. Everyone wants the confidentiality and safety of their communicating data. The network security is becoming indispensable as the volume of data being exchanged over the Internet is escalating day by day.

The two important techniques for providing security to information or data being shared are cryptography and steganography. Both are well known and widely used methods in information security.

In a large number of applications, it is desirable that the secracy of the communicated data or information is maintained. Such secret communication ranges from the apparent cases of bank transfers, corporate communications, and credit card purchases, on down to a large percentage of everyday email. Steganography is an ancient art of embedding a secret message (data embedding) [4] into a seemingly benign message. Most of the newer applications use steganography, for instance, a watermark to protect a copy right on information. The forms of steganography vary, but unsurprisingly, benign spam messages are turning up more often containing embedded text. Steganography [1,11] word originated from Greek words Steganos (Covered) and Graptos (Writing) which literally means cover writing. Generally, steganography is known as secret communication. Steganography means to hide message's existence in another medium (audio, video, image, communication). Today's steganography systems use multimedia objects like image, audio, video etc as cover media because people often transmit digital images over email or share them through other internet communication mediums. It is different from protecting the actual content of a message in a way which hides a message into another message.

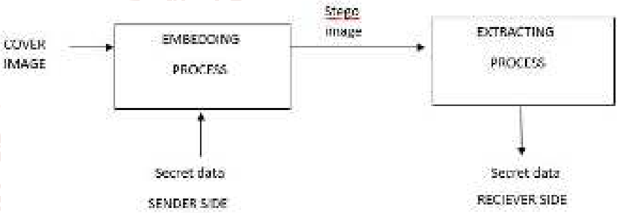


Fig. 1. A Generalized steganographic framework

2. Types and applications of Steganography

Image Steganography is the technique of steganography in which an image is taken as cover object. This steganography is known as image steganography. Generally, in this technique the LSB (Least Significant Bit) [8,9] of the image pixel value is manipulated to hide the message.

Video Steganography is a technique to hide a secret message or secret information into digital video format. Video which is a combination of picture frames is used as a carrier for secret information. Generally Discrete Cosine Transform (DCT) which alters the values, for instance, 8.667 to 9 is used to hide the secret information in each of the images in the video, which cannot be detected by the human eye. Video steganography uses formats such as H.264, MP4 (Motion Picture 4), MPEG (Moving Picture Experts Group), AVI (Audio Video Interleave) or other video formats.

Audio Steganography is a type of steganography in which the audio message is taken as a carrier for transmitting the secret information over a communication channel. It has emerged a remarkable medium due to the popularity of VOIP (Voice Over Internet Protocol). Audio steganography uses digital audio formats such as WAVE (Waveform Audio file), MIDI (Musical Instrument Digital Interface), AVI and MPEG etc for steganography.

Text Steganography is the technique of steganography in which the information is hidden in a text message, for instance, if the information text is hidden in HTML (Hyper Text Markup Language) coding of a web pages, it makes the detection of secret information almost impractical because the web pages are the basic building blocks of the websites on the internet.

There are various applications of Steganography like confidential communication and secret data storing, protection of data alteration, access control system for digital content distribution and media Database systems.

3. Techniques used in Steganography

Depending on the type of the cover object there are many suitable steganographic techniques which are followed in order to obtain security.

The terminologies used in Steganography are mentioned in the following paragraph.

Cover Message is the carrier of the message such as image, video, audio, text or some other digital media. Cover message is also called the Cover image or Cover work.

Secret Message is the information which is needed to be hidden in the cover message.

Secret Key is used to embed the secret message depending on the hiding algorithm. Secret key is also called as Stego key or encryption/decryption key.

Stego Message is the message after embedding the secret message into the cover message. Stego message is also called the stego-image, stego-work, stego-object or steganogram.

Classical LSB Algorithm

Image is composed of pixels which is a light intensity and this light intensity is a number. So an image is an array utilizing 256 colors (common images) having different pixel values at different locations. Digital images are typically stored in either 24-bit or 8-bit per pixel. A 24-bit image is sometimes known as true color image. This is obvious that a 24-bit image provides more space for hiding information; however, 24-bit images are generally large and not that common. A 24-bit image 1024 pixels wide by 768 pixels high would have a size of about 2 megabytes. Such large files would attract attention when they would be transmitted across a network or the Internet. Generally, 8 bit images are used to hide information such as GIF files represented as a single byte for each pixel. Now, each pixel can correspond to 256 colors. It can be said that pixel value ranges from 0 to 255 and the selected pixels indicates certain colors on the screen. The technique for classical least significant bit implies the replacement of LSB's of cover images with secret message data in order to hide information by altering cover image. Since LSB is replaced there is no significant effect on cover image and hence intended user will not get the idea that some message is hidden under the image. Here given a example to show LSB replacement to hide letter 'A' behind the cover image.

Cover Image bits
00100111 11101001 11001000 00100111 11001000 11101001 11001000 00100111

Message Image: 10000001

Steganographed Image
0010011**1** 1110100**0** 1100100**0** 0010011**0** 1100100**0** 1110100**0** 1100100**0** 0010011**1**

The bold bits represent the changed bits. LSB substitution requires on an average that only half the bits in an image be changed.

The disadvantages included in the LSB approach is the size of cover image required for a particular message image that is for a certain capacity of message cover image required is 8 times thus increasing the bandwidth to send the image. Another big disadvantage is that if an eavesdropper suspects that some secret data is hidden behind the cover image, he can easily extract that secret message by just collecting LSBs of stego image.

Inverted Bit LSB Substitution

Nadeem Akhtar et. al. proposed a scheme in which PSNR [4,13] of the stego image has increased and also security is maintained by selecting pixels randomly. In this technique the message bits are embedded in the cover image pixels randomly and a count with respect to the combination of bits at 2nd and 3rd bits of the pixel is maintained. Suppose 2nd and 3rd bits of a pixel are 01. If the LSB of image matches this counter is incremented for not changed pixel else counter is incremented for changed bits, same is performed for all the combinations (00, 01, 10, and 11). Example: Four message bits 1 0 0 0 are to be hidden into four cover image pixels

10000100
00101101
11101101
11101111

After plain LSB steganography [8], stegoimage pixels are

1000010**1**
0010110**0**
1110110**0**
1110111**0**

No. of changed pixels is four. According to algorithm check the 2nd and 3rd Least significant bit of the stego- image.For example let 2nd pixel=0 and 3rd pixel=1.Now if the 2nd and 3rd bit of pixel matches the required combination than invert the LSB else it will remain the same.Thus if we applied this case to above example than the pixels in the stego image will be

10000100
00101101
11101101
11101110

No. of changed pixel is one, so by employing this technique there will be increase in the PSNR. Same process will be performed for all the bit combinations. The bit inversion is performed only if the changed bits count is greater than unchanged bits count thus leading to less distortion of the cover image and leading to increased PSNR.

4. Related work

Akhtar et al [1] Nadeem Akhtar et al have implemented steganography for images, with an improvement in both security and image quality. The quality of the stego-image is improved by using bit-inversion technique. In this technique, certain least significant bits of cover image are inverted after plain LSB steganography which co-occurs with some pattern of other bits and thus reduce the number of modified LSBs. Therefore, a lesser number of LSBs of the cover image are altered in comparison to plain LSB method, thereby, improving the PSNR of stegoimage. By storing the bit patterns for which LSBs are inverted, message image can be obtained correctly.This technique uses RC4 algorithm to improve the robustness of steganography. The purpose of RC4 algorithm is to achieve the randomization in hiding message image bits into cover image pixels instead of storing them sequentially.

Sharma and Upadhaya et al [2] The authors have given overview of different steganographic techniques, its major types and classification of steganography which have been proposed in the literature during last few years. They have critically analysed different proposed techniques which show that visual quality of the image degrades when the hidden data increases up to a threshold limit using Least Significant Bit (LSB) based methods.

Latika and Gulati et al [3] The authors have given an understanding of cryptography and steganography concepts. In addition to this they have given an review of the research and developments in the field of steganography along with the various steganography techniques. Their work also provides the suggestion regarding the future researches in the field of steganography.

Champakamala et al [4] The authors has given a technique for using the hardware or electronics in image steganography. They have demonstrated that embedding secret information inside images requires thorough and in-depth computations and therefore, designing Steganography in hardware speeds up Steganography.

Bhardwaj and Sharma et al [5] In this paper the authors have provided three layers of security. Rrather than hiding the message bits directly in cover image, pixels are generated randomly through a pseudo random number generator and after that secret data is hidden behind a cover image using inverted LSB method. Their experimental study points out that the proposed system is better than basic LSB method in terms of higher visual quality which is indicated by the high PSNR values.

Arya [6] In this paper author has proposed improved LSB substitution method for hiding secret image information file into a color image. Many different carrier file formats can be used for instance, bitmap, jpeg and PNG to prove that this technique is suitable for these formats. The authors have intended the performance evaluation of secrete image steganography techniques using LSB method for data and image security, its comparison on different size and image format (.bmp; .jpg; .png) and calculation of performance parameters like PSNR and MSE for analysing the payload capacity.

Mustafa et al [7] In this paper the authors have provided a series of enhancements and argued that the proposed method fixed the weakness of Simple LSB image steganography method. The proposed method combines six fundamental improvements, specifically: CRC-32 checksum, Gzip compression, AES encryption, header information, pseudo-random pixel selection technique based on the Fisher-Yates Shuffle algorithm and 8 bpp embedding algorithm.

Ansari [8] The author has presented the comparative study and performance analysis of different image steganography techniques using various types of cover media ((like BMP/JPEG/PNG etc.) with the discussion of their file formats.

5. Proposed Work

The aim of the dissertation is to enhance the security of the stegno image which is obtained by using the LSB substitution. The problem with simple LSB technique is that if the pixels are chosen sequentially then the attacker may extract the secret message on suspicion.

Here we present a LSB based steganography method which is more secure and robust than the plain LSB method. The security of the hidden message has been enhanced by using a random key while extracting the secret message. In other words the message can only be extracted if the random key matches the value and only the recepient knows these values. This method enhances the security of the message because in no way the attacker can have information about the random key values.

6. Result and discussion

First of all the cover image is taken in which we have to hide the message. For instance, first take pout.tif image and perform steganography and then we perform steganography on football.jpg. The values of PSNR and MSE are calculated thereafter.

1. Read cover image pout.tif

The image pout.tif is taken as a cover image for hiding the message image.

Pout.tif

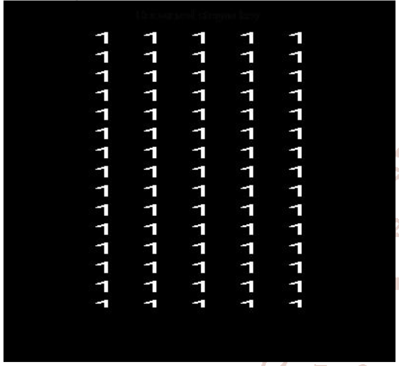
Embed message image

Message.bmp

Stegno Image

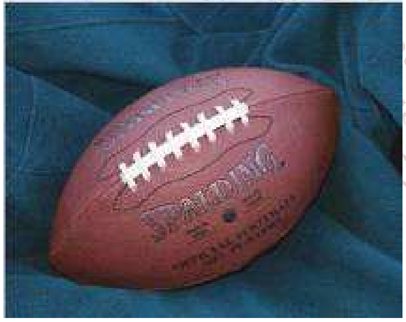
Stegano Image

Recovered message



Recovered message

2. Read Cover Image football.jpg



football.jpg

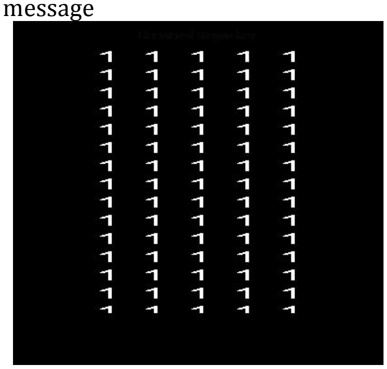
Embed Message Image

Message.bmp

Stegno Image

Stegano Image

Recovered message

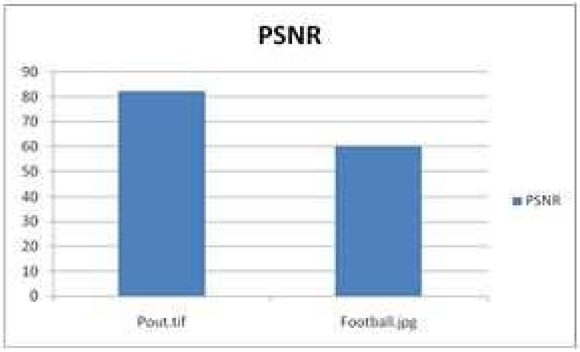


Recovered message

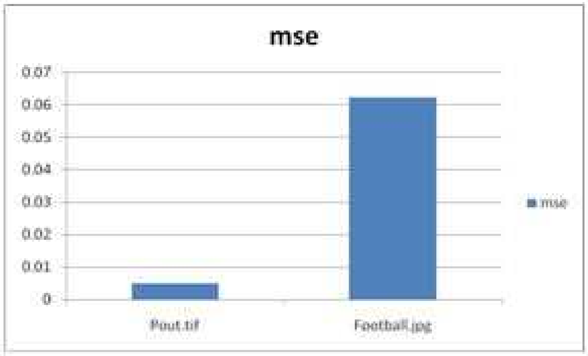
Error Metrics

Image	MSE	PSNR
Pout.tif	0.0050	82.2369
Football.jpg	0.0625	60.3412

PSNR (Peak Signal to Noise Ratio) PSNR is an engineering term for the ratio between the maximum possible power of a signal and the power of corrupting noise that affects the fidelity of its representation, because many signals have a very wide dynamic range, PSNR is usually expressed in terms of the logarithmic decibel scale. PSNR is most commonly used to measure the quality of reconstruction of lossy compression codecs. This ratio is often used as a quality measurement between the original and a compressed or reconstructed image. From the above two examples it can be inferred that obtained high PSNR indicates good quality re-construction.



MSE is the average of the squares of the error or deviations, that is, the difference between the estimator and what is estimated. The MSE assesses the quality of an estimator or predictor. MSE is a risk function, corresponding to the Expected value of the squared error loss or quadratic loss. Logically, a low value of MSE means less error which in turn results in higher PSNR. From the examples above, it can be inferred that the MSE is less than 0.1 which indicates high quality re-construction.



7. Conclusion

Steganography is an effective way to hide sensitive information. In this paper we have used the LSB Technique on images to obtain secure stego-image. Our results indicate that the combination of LSB insertion and secure key gives the accurate result and high security as compare to simple LSB insertion. This thesis focuses on the approach like increasing the security of the message along with maintaining high PSNR and reducing the distortion rate indicating high quality re-construction.

In future various filtering techniques can be applied to improve PSNR and MSE.

References

[1] S. A. Arshiya, “A Comparative Study of Recent Steganography Techniques for Multiple Image Formats“, *I. J. Computer Network and Information Security*, 2019.

[2] R. Pooja, “Analysis of Image Steganographic Techniques“, *International Journal of Computer Applications*, ISSN 0975-8887, Volume 114 Issue 1 pp. 11-17, 2015.

[3] A. Anupriya, “Performance Evaluation of Secrete Image Steganography Techniques Using Least Significant Bit (LSB) Method“, *International Journal of Computer Science Trends and Technology (IJCST)* Volume 6 Issue 2, Mar - Apr 2018.

[4] C.K. Mustafa and E. Wisam, “New LSB-based colour image steganography method to enhance the efficiency in payload capacity, security and integrity check“, *Sadhana (Indian Academy of Sciences)*, 2018.

[5] H. A. May, “An Efficient Image Cryptography using Hash-LSB Steganography with RC4 and Pixel Shuffling Encryption Algorithms“, *Annual Conference on New Trends in Information and Communication Technology Applications (NTICT),* 2017.

[6] K.T. Anand et al, “Image Steganography on Color Image using SVD and RSA with 2-1-4-LSB Technique“, *International Conference on Computation of Power,Energy, Information and Communication (ICCPEIC)*, 2017.

[7] S. V. Sylish, “Image Steganography in High Entropy Regions Using A Key and Modified LSB for Improved Security“, *Proceedings of the IEEE 2017 International Conference on Computing Methodologies and Communication (ICCMC)*, 2017.

[8] B. Rupali and S. Vaishali, “Image Steganography Based on Complemented Message and Inverted bit LSB Substitution“ *Procedia computer Science (ELSEVIER)*, 2016.

[9] K. Ashadeep and K.Rakesh et al, “Review Paper on Image Steganography“ International Journal of Advanced Research in Computer Science and Software Engineering, 2016.

[10] Latika and G. Yogita, “A Review of Steganography Research and Development“ International Journal of Advanced Research in Computer Science and Software Engineering, 2015.

[11] S. Abha et al, “A Survey of Image Steganography Techniques“, *International Journal of Computer Science and Technology (IJCST),* Volume 5, Issue 3, July - Sept 2014.

[12] Champakamala and K. Padmini *et al.,“* Least Significant Bit algorithm for image steganography“, *International Journal of Advanced Computer Technology (IJACT).*

[13] A. Nadeem, “Enhancing the Security and Quality of LSB based Image Steganography“, *5th International Conference on Computational Intelligence and Communication Networks*, 2013.

[14] K. Zaidoon and A. Al , “Overview: Main Fundamentals for Steganography“, *Journal of Computing*, Volume 2, pp. 158-165, March 2010.