Recent Advances in Technology and Engineering (RATE-2017)
6th National Conference by TJIT, Bangalore

International Journal of Science, Engineering and Technology
An Open Access Journal

Image Encryption Using Enhanced LSB Technique

[1]K Chetan Sastry, [2]Manjunath Kulkarni, [3]Varun Kumar

Abstract

Steganography is defined as the study of invisible communication that usually deals with the ways of hiding the existence of the communicated message. Generally data embedding is achieved in communication, image, text, voice or multimedia content for copyright, military communication, authentication and many other purposes. In image Steganography, secret communication is achieved to embed a message into cover image and generate a stego image. The goal of steganography is to hide the existence of the message from unauthorized party. The modern secure image steganography presents a task of transferring the embedded information to the destination without being detected by the attacker. Many different carrier file formats can be used, but digital images are the most popular because of their frequency on the Internet. Image steganography is taking the cover object as image. Generally, in this technique pixel intensities are used to hide the information. The concept of steganography known as 'Enhanced LSB Algorithm' is employed to hide an image in an another image, which has negligent distortion as compared to the Least Significant Bit Algorithm.

Keywords—cover image; secret image; stego image; LSB algorithm; bit replacement; enhanced lsb algorithm; randomization.

Introduction

The word 'Steganography ' is originated from the Greek word Steganos (Covered), and Graptos (Writing) which literally means "cover writing". Steganography is a science of invisible or secret communication. The 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 application.

Image steganography is method of hiding information into cover-image; generating a stego image an then transmitting information to the other party by known medium, where the third party does not know that this stego-image has hidden message. After receiving stego-image, the hidden message can be extracted with or without using stego-key .

Terminologies used in Image steganography are as follows:-

A. Cover image: Original image which is used as a carrier for hidden information.

B. Message: Actual information which is used to hide into images. Message could be a plain text or some other image.

C. Stego image: After embedding message into cover image is known as stego-image.

D. Stego-Key: A key is used for embedding or extracting the messages from cover-images and stego-images.

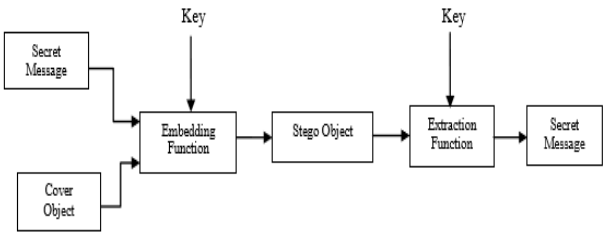

Fig.1. Basic block diagram of image steganography

The secret image to be sent is embedded into the cover image by means of a stego key using any of the embedding algorithm. The embedding algorithm generates a stego image, which is transmitted to the

destination. At the receiving end, using the same stego key and extracting algorithm the secret image can be uncovered.

The randomization method improves the security of normal LSB based steganography. And also improve the information carrying capacity of cover image compared to plain LSB[1]. Classical examples include a Roman general that shaved the head of a slave tattooing a message on his scalp. When the slave's hair grew back, the General dispatched the slave to deliver the hidden message to its intended recipient. Ancient Greeks covered tablets with wax and used them to write on. The tablets were composed of wooden slabs. A layer of melted wax was poured over the wood and allowed to harden as it dried. Hidden messages could be carved into the wood prior to covering the slab. When the melted wax was poured over the slab, the now concealed message was later revealed by the recipient when they re-melted the wax and poured it from the tablet [2]. Steganography can be used within digital images by LSB Substitution method[3].The LSB Algorithm has more amount of distortion, so "Enhanced LSB" is proposed. It improves the performance of the LSB method and minimizes the distortion level which is negligent to human eye[4]. LSB based techniques pose a difficult challenge to a stego-analyst as it is difficult to differentiate final image and the cover image which is given as input. The differences between them will be very slight. Major advantage of this method is, it is quick and easy. This method works well with gray scale images. It is mainly used for image integrity[6]. The computational complexity is reduced. The LSB algorithm is used for both 8 bit and 24 bit image of the same size of cover and secret image, so it is easy to be implementing in both grayscale and color image. Benefited from the effective optimization, a good balance between the security and the image quality is achieved[7][10]. A novel method for embedding a grey data is proposed. This method not only provides a way for embedding valued secret image into a cover but also the preserves the quality of cover images and secret image with no loss. The method produces the stego-image but also offers an easy way to accomplish image cryptography with random key generator and pseudorandom number generator[8].

Image steganographic techniques.

A. Spatial domain method: Spatial domain techniques are broadly classified into

1. Least significant bit (LSB)

2. Pixel value differencing (PVD)

3. Edges based data embedding method (EBE)

4. Random pixel embedding method (RPE)

5. Mapping pixel to hidden data method

6. Labeling or connectivity method

7. Pixel intensity based method

8. Texture based method

9. Histogram shifting methods.

B. Transform Domain Technique: The process of embedding data in the frequency domain of a signal is much stronger than embedding principles that operate in the time domain.

Most of the strong steganographic systems today operate within the transform domain, which have an advantage over spatial domain techniques as they hide information in areas of the image that are less exposed to compression, cropping, and image processing[5].

Transform domain techniques are broadly classified into:

1. Discrete Fourier transformation technique (DFT).

2. Discrete cosine transformation technique (DCT).
3. Discrete Wavelet transformation technique (DWT).
4. Lossless or reversible method (DCT)

5. Embedding in coefficient bits

C. Distortion Techniques: 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.

The encoder adds a sequence of changes to the cover image. So, information is described as being stored by signal distortion.

D. Masking and Filtering: These techniques hide information by masking an image, in the same way as to paper watermarks. These techniques embed the information in the more significant areas than just hiding it into the noise level. The hidden message is more integral to the cover image[5].

Types of Steganography

A. Image Steganography: Taking the cover object as image in steganography is known as image

steganography. In this technique pixel intensities are varied.

B. Video Steganography: Video Steganography is a technique to hide any kind of files or information into digital video format. Video (combination of pictures) is used as carrier for hidden information. Generally discrete cosine transform (DCT) alter values (e.g., 8.667 to 9) which is used to hide the information in each of the images in the video, which is not noticeable by the human eye.

*C. Network Steganography***:** When Taking Cover Object As Network Protocol, The Protocol Is Used As Carrier, Is Known As Network Protocol Steganography

D. Audio Steganography **:** The method of taking audio as a carrier for hiding information is called audio steganography. It has become very significant medium due to voice over ip (voip) popularity. Audio steganography uses digital audio formats such as wave, midi, avi mpeg or etc for steganography.

*E.Text Steganography: I*n text steganography, the number of tabs, white spaces, capital letters, like morse code is used to achieve steganography.

IV. least significant bit technique

Least Significant Bit (LSB) insertion method is a common and simple approach for image steganography. This technique allows hiding information within an image by replacing only the least significant bit of each pixel of the cover image. i.e. only a single bit is replaced in each pixel. Replacement of LSB does not make changes on the cover image and hence intended user will not get the idea of secret information. The cover image should be eight times larger than the secret image.

A. Least significant bit algorithm

1. Select a cover image of size m*n as an input.

2. The image to be hidden is embedded in rgb component only of an image.

3. Use a pixel selection filter to obtain the best areas to hide the bits of the pixels of the secret image in the bits of the pixels of the cover image.

4. After that Message is hidden using Bit Replacement method.

enhanced least significant bit technique

The enhanced method incorporates *randomization algorithm* in which the bits of the secret image are embedded in the random pixels of the cover image and these random pixels are generated by RC4 algorithm. This technique implements steganography for images, with an improvement in both security and image quality.

The RC4 algorithm generates the pixels of cover image in a random order and the secret image bits are embedded into these pixels in the respective order. This stego-key can be made available at the receiver by embedding within the transmitting image.

A. Enhanced least significant bit algorithm

1. Select a cover image of size m*n as an input.

2. The image to be hidden is embedded in the blue component of an image.

3. Use a pixel selection filter to obtain the best areas to hide the bits of the pixels of the secret image in the bits of the random pixels of the cover image.

4. Generate pixels of cover and secret images.

5. Generate array of cover image locations for selected stego-key using rc4 algorithm.

6. Replace the lsbs of cover image pixels in the sequence generated in step 5, with secret image bits.

B. Flowchart

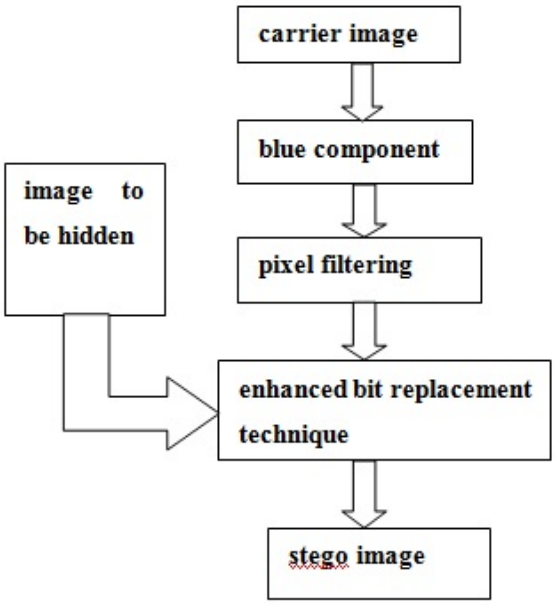

Fig.2. Flowchart of Enhanced LSB

Advantages of Enhanced Lsb Technique

A. The system enhances the security of the lsb technique by randomly dispersing the bits of secret image in the cover image.

B. The image quality is preserved by the system since all the secret image bits are embedded in the cover image.

C. Improvement in both security and image quality.

D. Enhanced lsb algorithm has negligent distortion as compared to the least significant bit algorithm.

Simulated Results

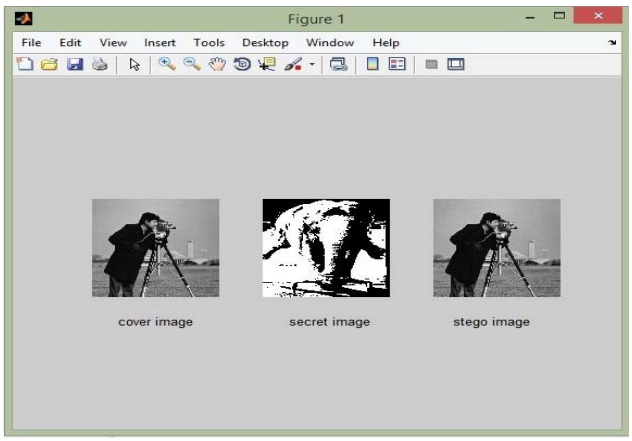

Fig.3. Simulated output 1

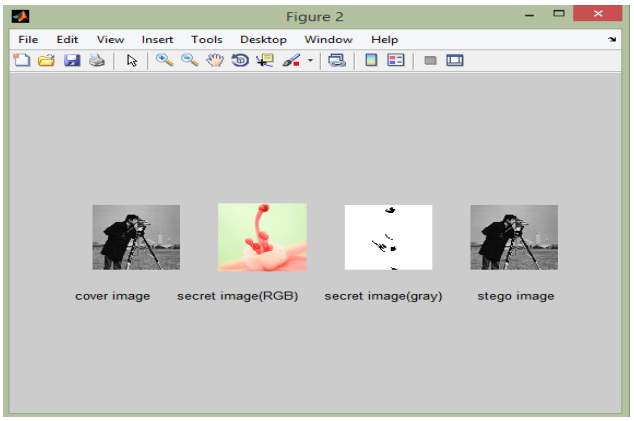

Fig.4. Simulated Output 2

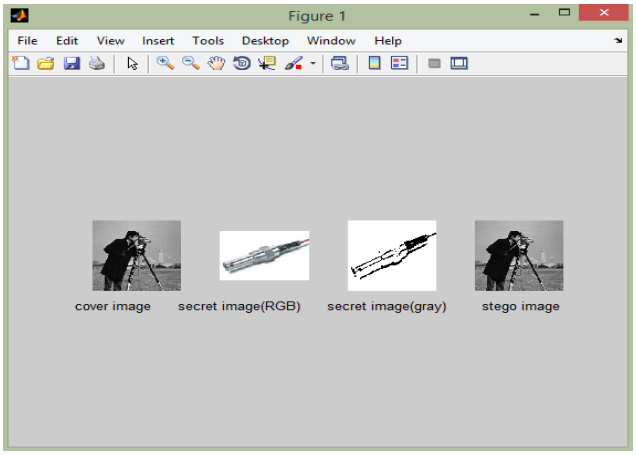

Fig.5. Simulated Output 3

In Fig.3 the secret image is of type JPEG , in Fig.4 the secret image is of type PNG , in Fig.5 the secret image is of type BITMAP, which are embedded into the cover image of type TIFF. The stego and cover images look identical to each other as only one LSB is replaced.

Conclusion

The Least Significant Bit Algorithm is most commonly used technique for steganography but LSB offers more amount of distortion and is less secure due to sequential mapping. In contrast , Enhanced Least Significant Bit (ELSB) technique offers better performance and high security as the information is hidden in only one of the three colors that is BLUE color of the carrier image. This minimizes the distortion level which is negligent to human eye and the secret image pixels are hidden in the random pixels of the cover image.

The secret image and cover image can be of same format or different format[9].

Future Work

The decryption of the secret image using enhanced LSB algorithm can be done . Image steganography hybrid methods can also be incorporated in order to improve the performance and security of the system.

References

[1] Mekha Jose,"Hiding Image in Image Using LSB Insertion Method with Improved Security and Quality".

[2] Shawn Dickman,"An Overview of Steganography",Computer Forensics Term Paper, James Madison University

[3] Nick Nabavian,"Image Steganography".

[4] Shilpa Gupta,Geetha Gujaral and Neha Agarwal," Enhanced LSB algorithm for image stegnography",IJCEM International Journal of Computational Engineering & Management, Vol. 15 Issue 4, July 2012.

[5] Mehdi Hussain and Mureed hussain,"A Survey of Image Steganography Techniques", International Journal of Advanced Science and Technology Vol. 54, May, 2013[6] R. Rathna Krupa," An Overview of Image Hiding Techniques in Image Processing", The SIJ Transactions on Computer Science Engineering & its Applications (CSEA), Vol. 2, No. 2, March-April 2014.

[7] Vijaykumar Sharma & Vishal Shrivastava ," A Steganography algorithm for hiding image in image by improved lsb substitution by minimize detection", Journal

of Theoretical and Applied Information Technology 15th February 2012. Vol. 36 No.1.

[8] Kaveh Ahmadi, Maral Mohamadi Zanjani," A New Method for Image Security and Data Hiding in Image'', 2011 2nd International Conference on Business, Economics and Tourism Management IPEDR vol.24 (2011) © (2011)IACSIT Press, Singapore.

[9] Tushina, Mukesh Kumar," An Enhanced and Secure Image Steganographic Technique Using RGB-Box Mapping'', Computer Science & Engineering Department, the Technological Institute of Textile & Sciences, Bhiwani, India.

[10] Kshetrimayum Jenita Devi, " A Secure Image Steganography Using LSB Technique and Pseudo Random Encoding Technique", Department of Computer Science and Engineering National Institute of Technology Rourkela.

[11] Bedwal, An Enhanced and Secure Image Steganographic Technique Using RGB-Box Mapping'', Computer Science & Engineering Department, the Technological Institute of Textile & Sciences, Bhiwani, India.

[12] Vishal Shrivastava," A Steganography algorithm for hiding image in image by improved lsb substitution by minimize detection",Journal of Theoretical and Applied Information Technology 15th February 2012. Vol. 36 No.1.

[13] Maral Mohamadi Zanjani," A New Method for Image Security and Data Hiding in Image'', 2011 2nd International Conference on Business, Economics and Tourism Management IPEDR vol.24 (2011) © (2011)IACSIT Press, Singapore.

[14] Mukesh Kumar," An Enhanced and Secure Image Steganographic Technique Using RGB-Box Mapping'', Computer Science & Engineering Department, the Technological Institute of Textile & Sciences, Bhiwani, India.

Author's details

Student, sixth semester, department of electronics and communication engineering, Rao Bahadur Y Mahabaleshwarappa Engineering College, Ballari, Karnataka, India, Email: kchetansastry19395@gmail.com