International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Impact Factor (2012): 3.358

Hiding Image in Image Using LSB Insertion Method with Improved Security and Quality

Mekha Jose

School of Computer Sciences, M G University, Kottayam Dst, Kerala, India

Abstract: ***The information hiding techniques arose to satisfy the need for covert communication. Steganography is an extremely useful method for covert information transmission. Steganography is the data hiding technique which allows hiding secret message or image within a larger image or message such that the hidden message or an image is undetectable. This paper proposes an image hiding steganographic method, of hiding an image within a cover image. This steganographic method aims to minimize the visually apparent and statistical differences between the cover image and a stego image with increase in the size of the payload. The proposed algorithm uses the binary codes which is the binary representation of pixels inside the image. This algorithm make use of least significant bit (LSB) technique, which is a popular technique in steganography ,in which least significant bits of cover are altered by secret data bits. The proposed method incorporate randomization algorithm which improve the security of LSB scheme. The bits of the secret image are embedded in random pixels of the cover image and these random pixels are generated by RC4 algorithm. The system enhances the security of the LSB technique by randomly dispersing the bits of secret image in the cover image which makes it harder for unauthorized people to extract the original image. Since all the secret image bits are embedded in the cover image the exact secret image can be regenerated from the stego-image and thereby the image quality is preserved by the system. Thus the proposed system implements steganography for images, with an improvement in both security and image quality***.

Keywords: Data hiding, Steganography, LSB encoding, Image Steganography, Randomization, RC4 Algorithm

1.Introduction

The communication security remains as a serious concern in information security. Secure data transfer is the need of every time. A number of hardware and software solutions have been proposed and implemented for information security, which restrict the unauthorized access, disclosure and malicious use of personal and classified information etc. Data hiding is a popularly used technique for secure communication. Data hiding is the technique of embedding information into digital content without causing perceptual degradation. Watermarking, cryptography and steganography are three famous techniques used in data hiding.

Watermarking is the process of hiding digital information in a carrier signal, where hidden information does not need to contain a relation to the carrier signal. Digital watermarks can be used to verify the authenticity or integrity of the carrier signal and also to show the identity of its owners. It is prominently used for tracing copyright infringements and for banknote authentication. Both steganography and digital watermarking employ steganographic techniques to embed data covertly in noisy signals but their priorities differ. Steganography provide priority to offer imperceptibility to human senses, whereas digital watermarking tries to control the robustness as top priority.

Cryptography is a popularly used technique for secure communication in the presence of third parties. Cryptography was synonymous with encryption, which involve the conversion of information from a readable form to apparent nonsense. A particular decoding technique will be required to decrypt or recover the original information from an encrypted message. The source of an encrypted message shares the decoding technique only with intended recipients; thereby avoid the unauthorized or unintended third party access to the secret information.

Steganography is considered to be the art of hiding information. In steganography the existence of the message itself is not disguised, but the content is obscure. The goal of steganography is to hide information such that the adversary is completely unaware of the communication. Steganography focuses on keeping the existence of hidden information undetectable to human eyes. Cryptography involves converting intelligent information to a meaningless form, whereas steganography hides information where the fact of information hiding is also hidden. Steganography involves any process that deals with hiding data or information within another data. The main motive of steganography technique is to prevent detection of hidden information and thereby ensure secure information transfer. In Greek steganography is defined as covering writing. Steganography technique have been employed in ancient Greek times, there exist the practice of tattooing secret message on shaved head of a messenger, and letting his hair grow before sending him through the enemy territory. However majority of the steganography techniques have been developed and computerized steganography usage have been started only by 2000. Batch steganography, permutation steganography, least significant bit(LSB), bit plane complexity segmentation(BPCS) and chaos based spread spectrum image steganography(CSSIS) are some of the steganography techniques used for data hiding.

Introduction of digital technology bring out a lot of developments in the field of steganography. Now we were able to use a number of medias as cover for hiding information like image, audio, video, text etc. Steganography techniques involve a cover object which is used to cover the secret information, a host object which is

Licensed Under Creative Commons Attribution CC BY

message or image to be transmitted, a steganography algorithm which implement the process of information hiding and a stego-key used by the algorithm. In image steganography the cover will be an image and the output of the embedding process will be an image called stego-image, which is the cover image with secret information hidden inside. The secret information can be a message or another image. This stego-image is sent to the receiver side where the receiver applies de-steganography on the received image and retrieves the hidden information from it. A good technique of image steganography focuses on three aspects. First one is the capacity, which is the maximum amount of data that can be stored inside the cover image. Second one is the imperceptibility, which refers to the quality of stego-image generated after data hiding and the last one is robustness. All steganographic methods are expected to comply with a few basic requirements which include invisibility, payload capacity, robustness against statistical attacks, robustness against image manipulation etc.

One of the common and simple approach for image steganography is the least significant bit (LSB) insertion method. This LSB based technique can be used to hide an image within another image. This involves replacement of LSB's of cover image pixels with secret image bits. Thus an image is hidden inside another image by altering only the LSB's of the cover. The change in LSB does not make much effect on the cover image and hence it will not give even an idea that some information is hidden behind the image. Several steganography techniques based on least significant bit insertion method have been proposed and implemented. When LSB insertion method is employed on a 24-bit image, three bits can be encoded into each pixel, since each pixel is represented by three bytes. Changes in these LSB bits will be imperceptible to the human eye. When LSB techniques are employed on 8-bit color images, more care need to be taken. So, when 8 bit images are used as cover the grey images are recommended for data hiding.

2.Existing System

Image is represented with various light intensities, which is represented by pixels of the image and pixels represent a number. So image is an array of pixel values having different values at different locations.

Digital images typically have either 24-bit or 8-bit representation. ie. either 24 bits or 8 bits are used to represent a pixel. 24-bit images are the true color images and they offer more space for hiding information. However, 24-bit images are generally large in size and not that common, and they would attract attention when they are transmitted across a network or the Internet. So generally 8 bits images like GIF files are used to hide information, in which each pixel is represented by a single byte. So each pixel can have values ranges from 0 to 255 and which in turn represent 256 colors.

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 the LSB's of the cover image. Replacement of LSB does not make changes on the cover image and hence intended user will not get the idea of secret information. The existing method of image steganography using plain LSB insertion method replaces only the least significant bit of each of the pixel of the cover image. i.e. only a single bit is replaced in each pixel. The LSB replacement allows hiding information behind cover image directly. And since it change only a single bit of a pixel it do not cause detectable difference in image quality.

The Four bit and Six bit data hiding methods which are based on LSB steganography can be used to improve the information carrying capacity of cover image used. In plain LSB method since a single LSB bit is modified in each pixel and each pixel is represented with 8 bits, the cover image is required to be 8 times bigger than the secret image. The 4 bit and 6 bit methods modifies more number of LSB bits and thus the size requirement of cover image in plain LSB method is reduced by these methods.

In 4 bit data hiding method the last four LSB bits of each of the cover image pixel is replaced with corresponding first four MSB bits of secret image. ie. This method embeds the 4 MSB bits of secret image into 4 LSB bits of cover image. The 6 bit method embeds 6 MSB bits of each pixel of secret image into LSB bits of two cover image pixels, 3 bits on each pixel. ie. 3 LSB bits of cover image pixels will be modified. Thus six bit data hiding method embeds first 3 MSB bits of secret image to last 3 LSB bits of a cover image pixel. Again the next 3 bits of secret image is placed in 3 LSB bits of next pixel of cover image.

3.Proposed System

The paper proposes the steganographic technique of 3 bit data hiding method which is based on LSB steganography. In the existing plain LSB approach the large size requirement of cover image remain as a disadvantage. ie. The cover image is required to be at least 8 times bigger than the message image. The 4 bit and 6 bit LSB data hiding methods overcome this size requirement. But quality of retrieved image is not offered by these methods. Another big disadvantage of these methods is the sequence-mapping problem. i.e. There is a direct mapping between cover image and secret image pixels. Due to this simplicity of these methods an attacker who suspects that some information is hidden behind the cover image, he can easily extract information by just collecting LSBs of stego image. The proposed method of 3 bit LSB steganography is a solution to these problems.

In 3 bit data hiding technique the secret image bits are taken 3 at a time. Each of the 3 bits of secret image is embedded into last 3 LSB bits of cover image pixels. So last 3 bits cover image pixels are replaced with secret image bits. Thus with each of the 8 bits the cover image pixel 3 bit will be secret information. The Figure 1 shows the 3 bit data hiding method. Since all the secret image bits are embedded in the cover image, secret image can be retrieved from cover image with exact quality by this method. This 3 bit data hiding technique avoid the sequence mapping problem and enhances the LSB technique by incorporating randomization with LSB insertion. By this the secret image bits will be randomly dispersed in the cover image pixels and thus make

Licensed Under Creative Commons Attribution CC BY

it harder for unauthorized people to extract the hidden image.

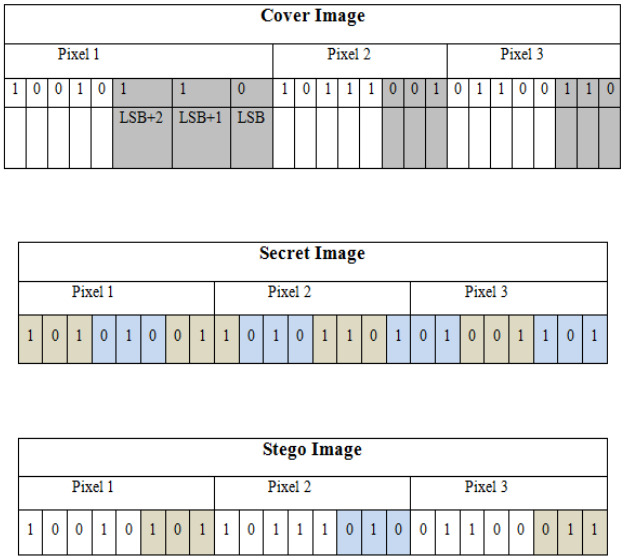


Figure 1: 3 bit data hiding method

LSB steganography with randomization

The existing LSB techniques are considered easy and direct methods to hide an image in a cover image. The information is embedded using the concept of sequence-mapping. Even though LSB technique hides the information in such way that the humans do not recognize its existence, still there exists the possibility of retrieving the secret information due to the simplicity of the technique

.

Therefore, we propose the randomization technique to improve the security of LSB scheme. This method embeds the secret image bits into random pixels of the cover image. And thus this allows overcoming the sequence mapping problem and making the system more secure. The RC4 algorithm is used for implementing this randomization. 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. Since RC4 have very simple structure and can be implemented efficiently RC4 is widely used. RC4 also offers simple key scheduling and output generation process. Since the secret information is randomly dispersed it is more difficult for an intruder to extract the hidden information. This algorithm makes use of a stego-key which is required during embedding and extracting the secret information. This stego-key can be made available at the receiver by embedding within the transmitting image or can be supplied to the receiver separately. In the absence of stego-key it is very hard to know the sequence in which cover image pixels are used for embedding the information. Thus this RC4 based randomization improves the security of the system.

Following steps describes how RC4 algorithm is used to generate random cover image pixels.
Step 1: Pixilate both the images
Step 2: Generate array of cover image locations for selected stego-key using RC4 algorithm.
Step 3: Replace the LSBs of cover image pixels in the sequence generated in step 2, with message image bits

Thus the proposed method offers improvement in information carrying capacity with improved security and quality.

4.Conclusion

Steganography is an efficient technique that can be used for secret information transfer. This technique allows hiding an image, which is a secret, into a cover image. Steganography provides an effective way of secret communication since the attacker is unable to detect the presence of hidden secret information. The least significant bit (LSB) based steganography is a common and simple approach for embedding information in images. We present a LSB based steganography method which is more secure and strong than existing LSB method.

We propose an image hiding technique which allows hiding an image within another image. The proposed method improves the security of normal LSB based steganography. And also improve the information carrying capacity of cover image compared to plain LSB. The system make use of LSB(Least Significant Bit) based image steganography and the proposed 3 bit data hiding method improve the quality of secret image retrieved at the receiver.

For security enhancement, the order of selected cover-image pixel for embedding the secret image bits depends on the random numbers generated by the RC4 using a shared key. Even if an attacker identifies the existence of hidden information in a cover, it is difficult for him to recover it because the bits are embedded in a random order. The 3 bit data hiding method hides all the secret image bits at the same time offers improvement in information carrying capacity and allows regenerating the secret image at exact quality at the receiver.

The security of the proposed system can be further improved by incorporating cryptographic encryption with the system. The secret image which is to be hidden can be encrypted before performing the proposed LSB technique. This could be considered in future.

References

[1] Reena M Patel,D J Shah , “Concealogram : Digital image in image using LSB insertion method”, International journal of electronics and communication engineering & technology(IJECET), 2013.
[2] Nadeem Akhtar, Pragati Johri, Shahbaaz Khan, “Enhancing the security and quality of LSB based image steganography”, 2013 5th International Conference on Computational Intelligence and Communication Networks.
[3] Mamta.Juneja , Parvinder S. Sandhu, “An improved LSB based Steganography with enhanced Security and Embedding/Extraction”, 3rd International Conference on Intelligent Computational Systems (ICICS'2013) January 26-27, 2013 Hong Kong (China)J.

Licensed Under Creative Commons Attribution CC BY

[4] S. M. Masud Karim, Md. Saifur Rahman, Md. Ismail Hossain, "A New Approach for LSB Based Image Steganography using Secret Key", Proceedings of 14th International Conference on Computer and Information Technology (ICCIT 201 I) 22-24 December, 201 I, Dhaka, Bangladesh.
[5] Morkel T., Eloff J. H. P., and Olivier M. S., "An Overview of Image Steganography", Information and Computer Security Architecture (ICSA) Research Group, University of Pretoria, South Africa, 2005.
[6] C. K. Chan, L. M. Cheng, "Hiding data in image by simple LSB substitution", pattern recognition, Vol. 37, No. 3, 2004, pp. 469-474.
[7] R. Chandramouli, N. Memon, "Analysis of LSB Based Image Steganography Techniques", IEEE pp. 1019-1022, 2001.
[8] Jhukkj F. Hartung and M. Kutte "Information hiding-a survey, " Proceedings of the IEEE: Special Issue on Identification and Protection of Multimedia Content, Volume: 87 Issue:7, pp. I062-I078, July. 1999.

Author Profile

Ms. Mekha Jose, presently pursuing her Masters' degree in Computer Science and Technology (specialization: Communication and Network Technology) from School of Computer Sciences, M G University, Kottayam, Kerala, India. She obtained her Bachelor's degree in Computer Science and Engineering from Amal Jyothi College of Engineering, Kanjirappally, kerala, India

Licensed Under Creative Commons Attribution CC BY