Chapter 17

Data Hiding Using Least Significant Bit Steganography in Digital Images

B.Chitradevi, N.Thinaharan and M.Vasanthi

Abstract
Data hiding is the art of hiding data for various purposes such as to maintain private data, secure confidential data and so on. The network provides a method of communication to distribute information to the masses. With the growth of data communication over computer network, the security of information has become a major issue. There are lots of techniques used for data hiding and the well known technique is the Steganography. Steganography is art and science of invisible communication. Steganography is the method through which existence of the message can be kept secret. This is accomplished in the course of hiding information in another information, therefore hiding the existence of the communicated information. This paper presents a brief idea about the image steganography that make use of Least Significant Bit (LSB) algorithm for hiding the data into an image.

Keywords: Steganography, Least Significant Bit, Data hiding, digital images.

Introduction

Information security is the way of assuring that the private information is still secure not lost or stolen. Information is not only theft but it can be damaged by system malfunction or any other way where data has a chance of being lost. Many government institutions, military departments, hospitals, educational institutes save most of their confidential data about their employees, customers, products on computers. That information is transmitted through network to different computers, where there is a chance of loss of information due to the presence of hackers. So information assurance is important factor to be considered while working on any information security project. Information security is further separated into three dimensions as follows,

---

Department of Computer Science, Thanthai Hans Roever College (Autonomous), Perambalur, Tamilnadu, India.

S. Vignesh and A. Philip Arokiadoss (ed.), *Statistical Approaches on Multidisciplinary Research,* Volume I

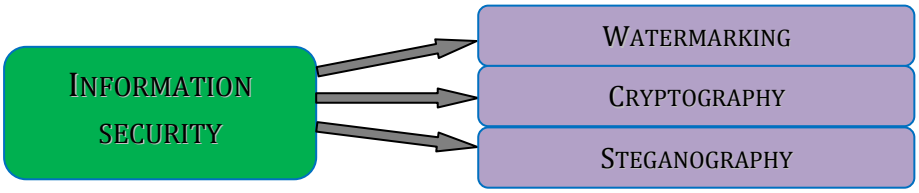


Fig17.1 Types of Information security

Watermarking

Watermarking is a recognizable image pattern that may be darker or lighter in tone, indicates the copy rights of particular documents. Usually watermarking has been used in government documents, currency notes, and stamp papers for legal purpose, passports for security features.

Cryptography: Cryptography comes from a Greek word meaning hidden or secret writing for secure communication in the presence of third parties or Un-authorized persons. Cryptography actually hides the information from illegal sources. Earlier forms of secret writing are classic cryptography, cipher texts. Cipher machine was also introduced by French but with the development of latest computers much more complex ciphers were developed and they encrypt data of any kind, whether it's a binary format, plaintext or hexadecimal data.

Steganography

The word "Steganography" comes from the Greek steganos (covered or secret) and graphy (writing or drawing) and thus means, literally, covered writing. It is a data hiding techniques, which aims at transmitting a message on a channel where some other kind of information is already being transmitted. The goal of steganography is to hide messages inside the images in such a way that does not allow any "enemy" to even detect that there is a secret message present in the image. Steganography attempts to hide the existence of communication (1). Steganography can be applied to many types of data, including audio, video, and images and can hide any kind of digital information.

Steganography

Steganography relies on hiding message in unsuspected multimedia data and is generally used in secret communication between acknowledged parties (3). The technique replaces unused or insignificant bits of the digital media with the secret data. The concept is to embed the hidden object into a significantly larger object so that the change is undetectable by the human eye. All digital file formats can be used for steganography, but the formats those are with a high degree of redundancy are more suitable (4).

Table17.1 Keys in Steganography

1	**Pure Key steganography**	It requires no prior exchange of information between the two parties communicating and relies on secret through obscurity. This means that the algorithms not publicly known, and therefore the level of testing is also unknown, making the tool unproven. One has to go on faith alone in those involved in the tool's creation to be assured covert communication. Numerous instances of the false sense of security through obscurity can be cited(6).
2	**Secret key steganography**	It uses a publicly known algorithm, and relies on a secret key chosen beforehand by the two parties communicating. This key is needed to both embed and extract the hidden information, and if the proper key is not used, it cannot be known if data is actually hidden in a given cover object (7).
3	**Public key steganography**	It entails the sender using the recipient's public key to embed the information, which can only be detected using the recipient's private key. This is analogous to how the public key infrastructure works in cryptography. The interesting characteristic with public key steganography is that even the sender should not be able to detect the secret message in the resulting stego object (8).

Table17.1 Keys in Steganography

The redundant bits of an object are those bits that can be altered without the alteration being detected easily. The most popular cover objects used for steganography are digital images. Digital images often have a large amount of redundant data, and this is what steganography uses to hide the message. There are three types of keys in steganography: *pure steganography, secret key steganography, and public key steganography* (5). The above table shows the keys in steganography,

Types of Steganography

There are many types of steganography methods. In this paper, we are going to take a short look at different steganography methods. Fig. 2 below shows the different categories of file formats that can be used for steganography techniques (6),

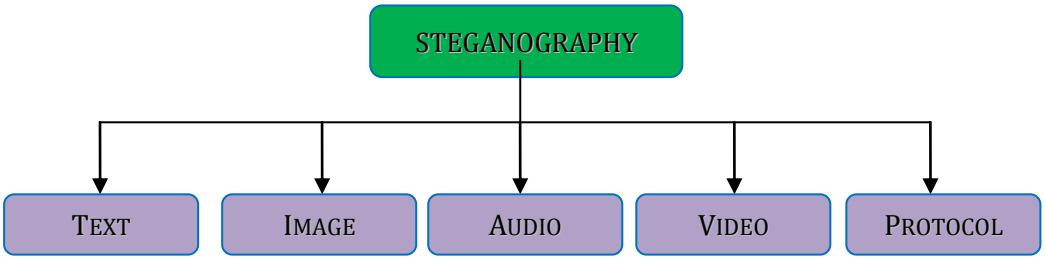


Fig 17.2Types of Steganography

The following table gives the details of steganography methods,
Table 17.2 Types of Steganography

1	**Text Steganography**	In text steganography formatting or by changing certain characteristics of textual elements can be changed. It consists of line-shift coding, word-shift coding and feature coding.
2	**Image Steganography**	Image is commonly used cover file. There are different file formats are available for digital images and for these file formats different algorithms are exist such as least significant bit insertion, Masking and filtering, Redundant Pattern Encoding, Encrypt and Scatter, Algorithms and transformations.
3	**Audio Steganography**	Secret message is embedded into digitized audio signal which result slender shifting of binary sequence of the equivalent audio file. There are a number of methods like LSB coding, Phase coding, spread spectrum, Echo hiding which are used for audio steganography.
4	**Video Steganography**	Video files consist of assortment of images and sounds, so most of the presented techniques on images and audio can be applied to video files too. An advantage of using video steganography is that large amount of data that can be hidden inside the cover file and it is the fact that it is flow of images and sounds.
5	**Protocol Steganography**	Protocol steganography embeds the information using network control protocol like http, ftp, tcp, Ssh, udp etc. Secret information is embedded in voice-over IP. Protocol steganography is an advance dimension of steganography and more secure than other dimensions.

Steganography proves to be an incredibly effective way of hiding the act of communication. The ease and effectiveness of Least Significant Bit (LSB) embedding make it an attractive method to transmit messages without detection.

Least Significant Bit (LSB)

In Steganography, The most well known techniques to data hiding in images are least significant bit (LSB) substitution, and masking & filtering techniques. LSB is a simple approach to embedding information in an image. But image manipulation can destroy the hidden information in this image. Applying LSB technique to each byte of a 24-bit image, three bits can be encoded into each pixel, as each pixel is represented by three bytes. Applying LSB technique to each byte of an 8-bit image, only one bit can be encoded into each pixel, as each pixel is represented by one byte (11).

Least Significant Bit (LSB) embedding is a simple strategy to implement steganography. Like all steganography methods, it embeds the data into the cover so that it cannot be detected by a casual observer. The technique works by replacing

some of the information in a given pixel with information from the data in the image. While it is possible to embed data into an image on any bit-plane, LSB embedding is performed on the least significant bit(s). This minimizes the variation in colors that the embedding creates (12). The following steps illustrate how this method is used to hide the secret data "A" in cover image "Mansoura.bmp" (12).

Step1: Convert the data from decimal to binary.

[Message] —Dec2Bin→ [1000001]

Step2: Read Cover Image "Mansoura.bmp" as shown in Fig3,

144	142	146	152	156	147	151	157
160	155	159	162	133	123	133	145
144	141	141	138	61	55	65	79
120	123	131	144	50	61	74	92
170	167	167	166	61	59	56	59
120	125	131	132	61	59	59	59
124	133	139	131	88	76	77	76
138	153	167	154	139	.....	.....	.....

Fig 17.3 The cover image “Mansoura.bmp"

Step3: Convert the Cover Image from decimal to binary.

10010000	10011010	10011100	10010010	10010110	10011101	10101111	10100101
10100000	10011011	10011111	10100010	10000101	01111011	10000101	10010001
10010000	10001101	10001101	10001010	00111101	00110111	01000001	01001111
01111000	01111011	10000011	10010000	00110010	00111101	01001010	01011100
10101010	10100111	10100111	10100110	00111101	00111011	00111000	00111011
01111000	01111101	10000011	10000100	00111101	00111011	00111011	00111011
01111100	10000101	10000111	10000011	01011000	01001100	01001101	01001100
10001010	10011001	10100111	10011010	10001011	.....	.....	.....

Step4: Break the byte to be hidden into bits.

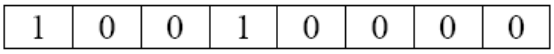
Thus [10000001] —is divided into 8 bits→ [1 0 0 0 0 0 0 1].

Step5: Take first 8 byte of original data from the Cover Image.

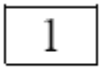
10010000	10011010	10011100	10010010	10010110	10011101	10101111	10100101

Step6: Replace the least significant bit by one bit of the data to be hidden as follows,

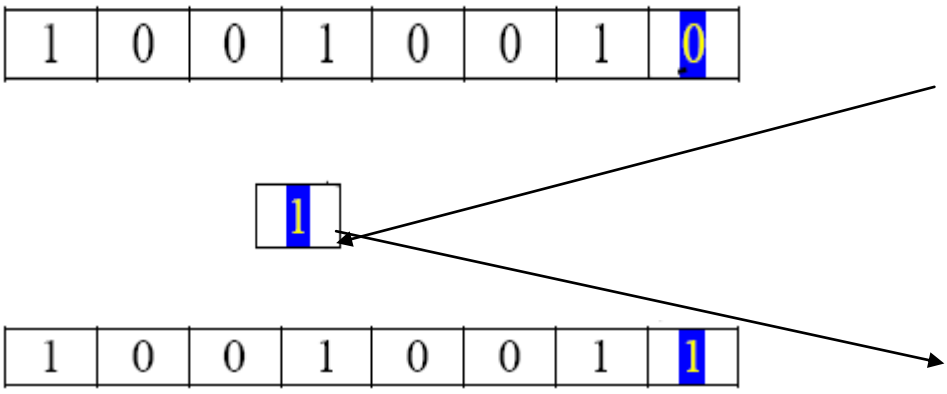
- First byte of original data from the Cover Image



- First bit of the data to be hidden



- Replace the least significant bit



- Repeat the replace for all bytes of Cover Image.

- Finally the cover image before and after steganography is shown in following figure,

Fig 17.4Cover Image before steganography

Fig 17.5 Cover Image after steganography

The reversible perturbation of values used in steganography enables the embedding of data into a cover medium. Choosing to modify values that have a small affect on the cover medium limits the ability to detect the embedding. Embedding strategies may be easily derived and implemented to complicate detection and inhibit the retrieval of the message by a third party, while still allowing easy retrieval by the intended recipient. LSB Embeddings may be detected simply through visual inspection of an image and its bit-planes, or more reliably through methods which use statistical metrics to identify the likelihood an image contains hidden data. While an embedding may be detected, it may not be easily decoded, nor may a stego object be discovered due to the sheer number of images available (12).

Conclusion

Steganography proves to be a significant technique for evading detection when communicating. The detection issues with steganography create challenges for security systems in attempting to prevent the transmission of steganographic content. As the need to communicate in secret will always exist, steganography will likely continue to play an important role enabling covert communication. LSB technique described in this paper helps to successfully hide the secret data into the cover file with minimum distortion made to the cover file. The most commonly used technique. The least significant bit technique causes higher distortion to the cover file in many cases.

References

A. E.Mustafa,A.M.F.ElGamal,M.E.ElAlmi,M.E.ElAlmi "A Proposed Algorithm For Steganography In Digital Image Based on Least Significant Bit" Research Journal Specific Education, Issue No. 21, April. 2011

Alain, C. Brainos (), A Study Of Steganography And The Art Of Hiding Information, East Carolina University.

Chi-Kwong,C., Cheng, L.(2004): Hiding data in images by simple LSB substitution, Journal of Pattern Recognition, Vol (37).

Gerad, G.(2006) : An Investigation of Scalable Vector Graphics as Cover Medium for Steganography, Ms.C, faculty of college of arts and science, American University.

http://www.slideshare.net/beautifulneha/steganography-10710623.

K.B.Raja, C.R.Chowdary, Venugopal K R, and L.M.Patnaik," A Secure Image Steganography using LSB, DCT and Compression Techniques on Raw Images" Department of Computer Science Engineering, Bangalore 2005 IEEE.

Kaushal M. Solanki, 2005, Multimedia Data Hiding: From Fundamental Issues to Practical Techniques, Ph.D, Electrical and Computer Engineering, university of california, Santa Barbara.

Laskar, S.A. and Hemachandran, K. (2012), "An Analysis of Steganography and Steganalysis Techniques", Assam University Journal of Science and Technology, Vol.9, No.II, pp.83-103, ISSN: 0975-2773.

Lee, L.(2004) : LSB Steganography :Information Within Information, Journal of Computer Science, Vol (265), No (5).

Rabah, K. (2004), "Steganography – The Art of Hiding Data", Information Technology Journal, Vol.3, no.3, pp. 245-269.

Samer, A.(2006):A New Algorithm for Hiding Gray Images using Blocks, Information, Security Journal, The Hashemite University, Jordan, Volume (15), Issue (6).

Samer, A.(2006):A New Algorithm for Hiding Gray Images using Blocks, Information, Security Journal, The Hashemite University, Jordan, Volume (15), Issue (6).

Tables :

Figures :