International Journal of Information and Computation Technology.
ISSN 0974-2239 Volume 4, Number 5 (2014), pp. 453-458

http://www. irphouse.com /ijict.htm

Data Encryption by Image Steganography

Sneha Bansod and Gunjan Bhure

Computer Applications Department, Kavikulguru Institute Of Technology & Science, Ramtek, Rashtrasant Tukadoji Maharaj Nagpur University, Nagpur.

Abstract

In modern era data is heavily gaining importance as information is dependent on the raw facts i.e data. The exchange of information is required to share resources among the distributed users which may be separated by locations. While transferring the data among the users the confidentiality and privacy should be maintained. The digitally shared data between the users should be converted to some unreadable format which will not be tampered by the intruders. To meet these requirements the technique Steganography can be used. In this technique we use different mediums to hide the data that are text, images, audio, video etc. this paper is focusing on encrypting of data by using image steganography.

Keywords: Cover media, cipher text, stego-function,data hiding, secret value.

1. Introduction

Steganography is a technique use to hide a secret information in such a way that someone unable to find the presence of the information. The term “Steganography” is a combination of two greek words “Steganos + Graphy”. The meaning of steganos is covered or secrete and the graphy means writing or drawing. Hence the covered writing is also called as steganography. It is more secured than the method called Cryptography because with cryptography only the scrambling of message is possible, whereas in steganography we use some media to encrypt the data. The main goal of steganography is to hide the information using some covered media. In case of cryptography the user can able to see the contents of message but can’t comprehend the information. On the other hand, in steganography the existence of information will not be noticed by viewer because it is embedded inside some medium. This medium is also called as carrier or cover object. It may be an image, video, texts, sound or any music file.

2. History of Steganography

In earlier, days there is also a secret communication carried out with different steganography techniques. The Greek historian Hirodotus recorded two stories for steganography techniques used at that time. The first was suppose any first party wants to send any secret message to the second party, then first party use to shave the head of one of the trusted person and write message on the scalp of that person. When the person's hairs grew back, he was sent to the second party, the second party again shave the head of that person to read the secret message.

The next story is to use the Wax-covered tablet. The secret message was written on wood after removing the wax from the tablet, and then it will be again recovered with the wax and sent to the destination. Some different technique is used by Romans for secret communication. They used invisible inks to write the message. This invisible ink can be made by some natural substances like milk and fruit juices. We can see the contents written by this invisible ink by heating it.

Write a secret message Recover the message

Fig. 1: Message hiding using Invisible ink.

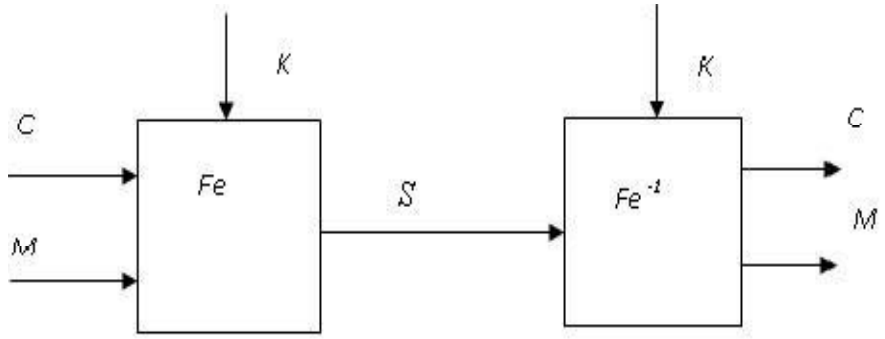
Later on Germans developed microdot technology which FBI Director J. Edgar Hoover referred to as "the enemy's masterpiece of espionage. Microdots are photographs the size of a printed period, having the clarity of standard-sized typewritten pages. The first microdots were discovered masquerading as a period on a typed envelope carried by a German agent in 1941. The message was not hidden, nor encrypted. It was just so small as to not draw attention to itself. Besides being so small, microdots permitted the transmission of large amounts of data including drawings and photographs [5].

3. Information Hiding Using Steganography

To hide the secret information we require following elements.

- The secret message (M), which is going to be hidden, it may be a plain text or cipher text or any type of data.
- The Cover media (C) , which hold the message
- The Stego-Function (Fe) and its inverse (Fe-1)
- The Stego-Key (K) or Password use to hide or unhide the data.

The secret message is embedded in the covered media on which stego-function is applied along with stego-key or password to form a stego-object. The schematic representation of this procedure is shown in following fig 2.



Data Embedding at sender side Data Extracting at receiver side

Fig. 2: The Schematic Representation of Steganography.

Where, C-> cover media, M->secret message, K-> secret key, Fe And Fe-1stego function.

The basic formula of the steganographic procedure can be given by:

Cover media + secret message + stego key = stego-object $C+M+K=S$

In above Fig. at the sender side user embed the message in cover medium using stego-function along with stego-key. On the other side of receiver, the extraction of secret message is taken place. To recover the secret message from stego medium we require the cover medium and the decoding stego-key. The above process is also called as encoding and decoding of message in steganography. The decoding is an exact reverse process of an encoding.

4. Types of Steganography

The steganography is having following types as shown in fig.3

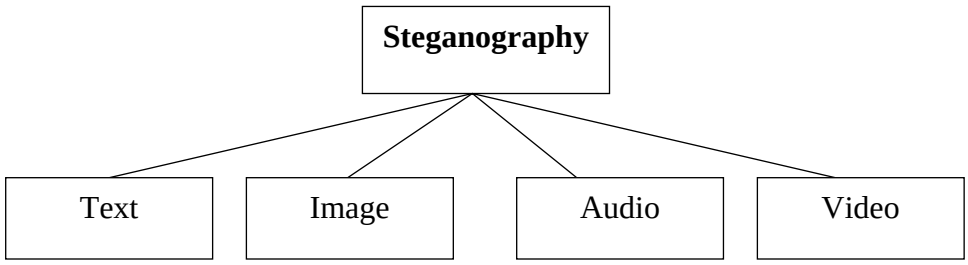


Fig. 3: Types of Steganography.

In the first type of Steganography, the cover media will be the “text cover”. The basic advantage of preferring text steganography is that, it requires less memory and

simple communication. The message is embedded in cover text file by using some embeding algorithm, so that the "stego text"or "cipher text" is formed. This stego text is then sent to the receiver side through transmission channel. This stego text is processed by the extraction algorithm by using "secret key" or "stego key".

Among four types of steganography, image steganography is the most popular technique. We take the detail look on this in the next section. The next technique is hiding the secret message by using Audio file as cover media. In the video steganography, we use the video file as cover media to embed the secret message.

5. Image Steganography

Images are one of the preferred media to hide the information due to their high capacity and low impact on the visibility. We can use the common image format of images like GIF (Graphics Interchange Format), BMP (Windows Bitmap), JPEG (Joint Photographic Expert Group) etc.[2] There are many approaches to hide the messages in the images..

Some common approaches are:

- Least significant bit substitution.
- Transform techniques
- Masking and filtering

LSB (Least Significant Bit) Substitution is the process of modifying the least significant bit of the pixels of the cover media [4]. LSB Substitution lends itself to become a very powerful Steganography method with few limitations.The approach is Transform technique also known as Transform Domain Embedding. Transform techniques embed the message by modulating coefficients in a transform domain, such as the Discrete Cosine Transform (DCT) used in JPEG compression.

Masking and filtering techniques, usually restricted to 24 bits and gray scale images, hide information by marking an image, in a manner similar to paper watermarks. The techniques performs analysis of the image, thus embed the information in significant areas so that the hidden message is more integral to the cover image than just hiding it in the noise level[3].In this paper we have focused on LSB substitution technique.

5.1 Least significant bit (LSB) substitution

This substitution technique will modify the last significant bit of the cover image. To form the stego- image we require two files, first cover image file and second message file. Before embedding process, the system must know the size of the cover image file. The standard size of this image is 800*600 pixels, which can embed up to 60kb size of message. This substitution technique will modify the last significant bit of the cover image. To form the stego- image we require two files, first cover image file and second message file. Before embedding process, the system must know the size of the cover image file. The standard size of this image is 800*600 pixels, which can embed up to 60kb size of message.

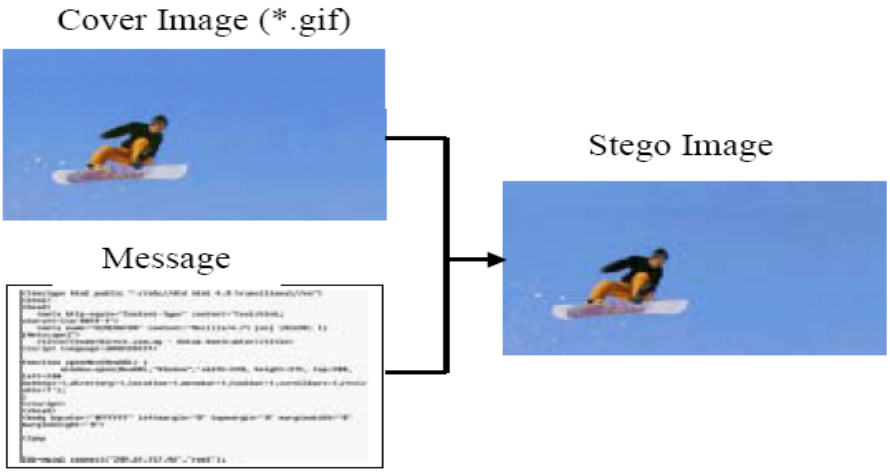


Fig. 4: Process of forming Stego-image.

The cover image will be combined with message to produce the stego-image as shown in fig.4, In the LSB technique, the LSB of the pixels is replaced by the message to be sent. The message bits are permuted before embedding, this has the effect of distributing the bits evenly, thus on average only half of the LSB's will be modified. Popular steganographic tools based on LSB embedding[6,7,8], vary in their approach for hiding information. Some algorithms change LSB of pixels visited in a random walk, others modify pixels in certain areas of images, or instead of just changing the last bit they increment or decrement the pixel value [8].

5.2 Advantages and Disadvantages

The advantages of LSB are its simplicity to embed the bits of the message directly into the LSB plane of cover-image and many techniques use these methods [10]. Modulating the LSB does not result in a human-perceptible difference because the amplitude of the change is small. Therefore, to the human eye, the resulting stego-image will look identical to the cover-image. This allows high perceptual transparency of LSB.

However, there are few weaknesses of using LSB. It is very sensitive to any kind of filtering or manipulation of the stego-image. Scaling, rotation, cropping, addition of noise, or lossy compression to the stego-image will destroy the message. On the other hand, for the hiding capacity, the size of information to be hidden relatively depends to the size of the cover-image. The message size must be smaller than the image. A large capacity allows the use of the smaller cover-image for the message of fixed size, and thus decreases the bandwidth required to transmit the stego-image [9].

Another weakness is an attacker can easily destruct the message by removing or zeroing the entire LSB plane with very little change in the perceptual quality of the modified stego-image. Therefore, if this method causes someone to suspect something hidden in the stego-image, then the method is not success [11].

6. Conclusions

Due to heavy requirement of information it is necessary to keep the data safe for future references, the data and the usage can be done but at other side there can be certain issues like intruders, man-in-middle attack which makes the digital transmission to be careful, the approach with respect the image stegnography is useful if the user wants the data to be hidden but in certain way making it confidentiality property is followed.

The approach can be very useful for the person who can be known to the system and works around the things which might require the confidentiality to be followed, the approach is one of the alternatives so as the data is hidden using some JPEG or BMP images which may be useful in hiding the data very easily.

7. Acknowledgements

The work herewith represented is not possible without infrastructure, literature & motivation. I am very thankful to the Dr. Bhaskar Patel, Principal KITS, Ramtek & the management for providing such a great environment & providing various infrastructural facilities without which this task could not be achieved. My sincere thanks to the Mr. Sanjay Borikar for constantly encouraging for such activities. I am very thankful to my family & friends.

References

[1] Souvik Bhattacharyya , Indradip Banerjee and Gautam Sanyal, A Novel Approach of Secure Text Based Steganography Model using Word Mapping Method(WMM)

[2] KK Ravi Ayappa, STEGANOGRAPHY -INFORMATION HIDING FOR SECURE COMMUNICATION

[3] MUHALIM MOHAMED AMIN , SUBARIAH IBRAHIM ,MAZLEENA SALLEH ,MOHD ROZI KATMIN INFORMATION HIDING USING STEGANOGRAPHY

[4] Nick Nabavian, Data Structures:Image Steganography, CPSC 350 , Nov. 28, 2007

[5] Arvind Kumar Km. Pooja, Steganography- A Data Hiding Technique, International Journal of Computer Applications (0975 – 8887) Volume 9– No.7, November 2010

[6] F. Collin, Encryptpic, http://www.winsite.com/bin/Info?500000033023.

[7] G. Pulcini, Stegotif,http://www.geocities.com/SiliconValley/9210/gfree.html.

[8] T. Sharp, Hide 2.1, 2001, http://www.sharpthoughts.org.

[9] G. Simmons, The prisoners problem and the subliminal channel," CRYPTO, pp. 51-67, 1983

[10] E. P. Simoncelli, Modeling the joint statistics of images in the wavelet domain," Proceedings of the 44th Annual Meeting, 1999.

[11] Mehdi Kharrazi, Husrev T. Sencar, and Nasir Memon, Image Steganography: Concepts and Practice.