Data Hiding in Image Using Steganography Technique

Abhinav Singh[1], Ravi Yadav[2], Ashish Chopra[3]
[1, 2, 3] NIT Kurukshetra, India.

Abstract- *Steganography is the art of hiding the fact that communication is taking place, by hiding information in other information. Many different carrier file formats can be used, but digital images are the most popular because of their frequency on the Internet. For hiding secret information in images, there exists a large variety of steganographic techniques some are more complex than others and all of them have respective strong and weak points. Different applications have different requirements of the steganography technique used. For example, some applications may require absolute invisibility of the secret information, while others require a larger secret message to be hidden. This paper intends to give an overview of image steganography, its uses and techniques. It also attempts to identify the requirements of a good steganographic algorithm and briefly reflects on which steganographic techniques are more suitable for which applications.*

Keywords- encoding, decoding, encryption, decryption, RGB

I. INTRODUCTION

Since the rise of the Internet one of the most important factors of information technology and communicationhas been the security of information. Cryptography was created as a technique for securing the secrecy of communication and many different methods have been developed to encrypt and decrypt data in order to keep the message secret. Unfortunately it is sometimes not enough to keep the contents of a message secret, it may also be necessary to keep the existence of the message secret. The technique used to implement this, is called steganography. Steganography is the art and science of invisible communication. This is accomplished through hiding information in other information, thus hiding the existence of the communicated information. The word steganography is derived from the Greek words "*stegos*" meaning "cover" and "*grafia*" meaning "writing"defining it as "covered writing". In image steganography the information is hidden exclusively in images.Steganography differs from cryptography in the sense that where cryptography focuses on keeping the contents of a message secret, steganography focuses on keeping the existence of a message secret . Steganography and cryptography are both ways to protect information from unwanted parties but neither technology alone is perfect and can be compromised. Once the presence of hidden information is revealed or even suspected, the purpose of steganography is partly defeated. The strength of steganography can thus be amplified by combining it with cryptography.

II. STEGANOGRAPHY CONCEPTS

Although steganography is an ancient subject, the modern formulation of it is often given in terms of the *prisoner's problem* proposed by Simmons , where two inmates wish to communicate in secret to hatch an escape plan. All of their communication passes through a warden who will throw them in solitary confinement should she suspect any covert communication .The warden, who is free to examine all communication exchanged between the inmates, can either be passive or active. A *passive* warden simply examines the communication to try and determine if it potentially contains secret information. If she suspects a communication to contain hidden information, a passive warden takes note of the detected covert communication, reports this to some outside party and lets the message through without blocking it. An *active* warden, on the other hand, will try to alter the communication with the suspected hidden information deliberately, in order to remove the information.

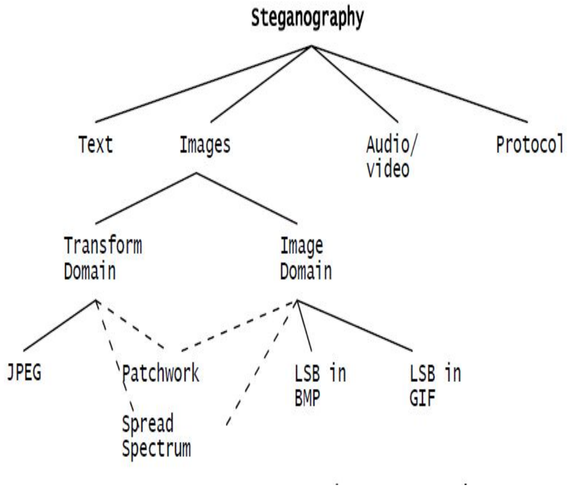
III. IMAGE DEFINITION

To a computer, an image is a collection of numbers that constitute different light intensities in different areas ofthe image. This numeric representation forms a grid and the individual points are referred to as pixels. Most images on the Internet consists of a rectangular map of the image's pixels (represented as bits) where each pixel is located and its colour. These pixels are displayed horizontally row by row. The number of bits in a colour scheme, called the bit depth, refers to the number of bits used for each pixel .The smallest bit depth in current colour schemes is 8, meaning that there are 8 bits used to describe the colour of each pixel . Monochrome and greyscale images use 8 bits for each pixel and are able to display 256 different colours or shades of grey. Digital colour images are typically stored in 24-bit files and use the RGB colour model, also known as true colour. All colour variations for the pixels of a 24-bit image are derived from three primary colours: red, green and blue, and each primary colour is represented by 8 bits . Thus in one given pixel, there can be 256 different quantities of red, green and blue, adding up to more than 16-million combinations, resulting in more than 16-

million colours. Not surprisingly the larger amount of colours that can be displayed, the larger the file size .

IV. IMAGE AND TRANSFORM DOMAIN

Image steganography techniques can be divided into two groups: those in the Image Domain and those in the Transform Domain . Image – also known as spatial – domain techniques embed messages in the intensity of the pixels directly, while for transform – also known as frequency – domain, images are first transformed and then the message is embedded in the image .Image domain techniques encompass bit-wise methods that apply bit insertion and noise manipulation and are sometimes characterised as “simple systems” . The image formats that are most suitable for image domain steganography are lossless and the techniques are typically dependent on the image format .Steganography in the transform domain involves the manipulation of algorithms and image transforms .These methods hide messages in more significant areas of the cover image, making it more robust. Many transform domain methods are independent of the image format and the embedded message may survive conversion between lossy and lossless compression .In the next sections steganographic algorithms will be explained in categories according to image file formatsand the domain in which they are performed.



V. LEAST SIGNIFICANT BIT

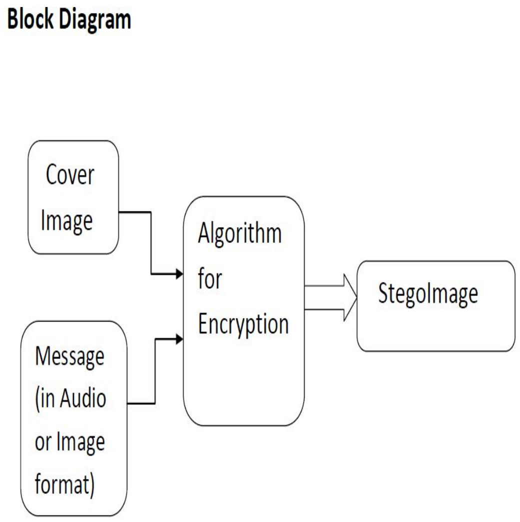
Least significant bit (LSB) insertion is a common, simple approach to embedding information in a cover image. The least significant bit (in other words, the 8th bit) of some or all of the bytes inside an image is changed to a bit of the secret message. When using a 24-bit image, a bit of each of the red, green and blue colour components can be used, since they are each represented by a byte. In other words, one can store 3 bits in each pixel. An 800 × 600 pixel image, can thus store a total amount of 1,440,000 bits or 180,000 bytes of embedded data . For example a grid for 3 pixels of a 24-bit image can be as follows:

(00101101 00011100 11011100)
(10100110 11000100 00001100)
(11010010 10101101 01100011)

When the number 200, which binary representation is 11001000, is embedded into the least significant bits of this part of the image, the resulting grid is as follows:

(0010110**1** 0001110**1**1101110**0**)
(1010011**0** 1100010**1**0000110**0**)
(1101001**0** 1010110**0** 01100011)

Although the number was embedded into the first 8 bytes of the grid, only the 3 underlined bits needed to be changed according to the embedded message. On average, only half of the bits in an image will need to be modified to hide a secret message using the maximum cover size . Since there are 256 possible intensities of each primary colour, changing the LSB of a pixel results in small changes in the intensity of the colours. These changes cannot be perceived by the human eye - thus the message is successfully hidden. With a well-chosen image, one can even hide the message in the least as well as second to least significant bit and still not see the difference.



VI. CONCLUSION

In the present world, the data transfers using internet is rapidly growing because it is so easier as well as faster to transfer the data to destination. So, many individuals and business people use to transfer business documents, important information using internet. Security is an important issue while transferring the data using internet because any unauthorized individual can hack the data and make it useless or obtain information un- intended to user. If a message is encrypted and hidden with a steganographic method it provides an additional layer of protection and reduces the chance of the hidden message being detected. Steganography is still a fairly new concept to the general public although this is likely not true in the world of secrecy and espionage.

REFERENCES

[1] Amirthanjan,R. Akila,R&Deepikachowdavarapu, P., 2010. A Comparative Analysis of Image Steganography, International Journal of Computer Application.

[2] Bandyopadhyay, S.K., 2010. An Alternative Approach of Steganography Using Reference Image. International Journal of Advancements in Technology.

[3] Cox, I. Miller, M. Bloom, J. Fridrich, J &Kalker, T. 2008. Digital watermarking and Steganography.2ndEd. Elsevier.

[4] Obaida Mohammad Awad Al-Hazaimeh Hiding Data in Images Using New Random Technique Department of Information Technology, AL-BALQA Applied University/Al-Huson University College, Irbid, Al-Huson, 50, Jordan.

[5] An Overview of Steganography by Shawn D. Dickman Computer Forensics TermPaper, James Madison University.

[6] A Tutorial Review on Steganography by Samir K Bandyopadhyay, Debnath Bhattacharyya, DebashisGanguly, SwarnenduMukherjeet and Poulami Das University of Calcutta.

[7] Exploring Steganography: Seeing the Unseen by Neil F. Johnson SushilJajodia George Mason University.