IMAGE STEGANOGRAPHY BY USING MAPPING OF LETTERS TO PIXELS AND INDICATOR CHANNELS

Jatinder Kumar M.Tech(Student)
Department of Computer Engineering
M.M. Engg. College, M.M. University, Mullana,
Ambala-133 203, Haryana, India
jkteji@yahoo.co.in

Mr. Ashish Oberoi (Faculty)
Department of Computer Engineering
M.M. Engg. College, M.M. University, Mullana,
Ambala-133 203, Haryana, India
a_oberoi01@yahoo.co.in

Abstract:By using Steganography the existence of a message can be hide so that if it commonly perfomed successfully then found no suspicion at all. Using steganography, information can be hidden in such as images, audio files, text files, videos files and other means of data transmissions. The main idea for this is to use enough number of bits from each pixel in an image to map them to 26 alphabetic English characters ('a'…'z') and some special characters that are mostly using in writing a secret message. We know that in every image, there are pixels. Each pixel contains three bytes named as Red, Green and Blue(RGB) channel. The algorithm uses mapping method for data hiding and Pixel Indicator Technique for indication that data is hidden here. The basic concept is to convert secret message into ASCII (American Standered Code of Information Interchange code. As ASCII code is a 7 bit code, so for matching bits every byte only 7 MSBs of each channel will be used and the LSB of all three channels are free to work as an indicator. The main goal of this method, is to hide a text of a secret message in the pixels of the image in such a way that the human eyes are not able to differentiate between the original and the Stego-image, but it can be easily performed by a specialized reader machine.

Keywords— ***Steganography, LSB, encryption, cryptography.***

1.1 INTRODUCTION

Steganography is an ancient art of transmission messages in such a secret way that only the receiver knows the existence of message. So, a fundamental requirement for a stenographic method is silence; this means that the embedded messages should not be visible to the human visual system. There are two other requirements, one is to maximize the embedding capacity, and the other is security. The least-significant bit (LSB) insertion method is the most common, simple and easiest method for embedding messages in an image. However, how to decide on the maximal embedding capacity for each pixel steganography, we study techniques to achieve secret communication between two parties that are interested in hiding not only the content of a secret message but also the act of communicating it. To this aim, steganography algorithms ("stego algorithms") embed the secret information into different types of "natural" cover data like sound, images, or video. The resulting altered data is referred to as stego-data and it must be perceptually indistinguishable from its natural cover. On the other hand, stego-analysis seeks to analyze (possibly altered) cover data to decide whether a message has been embedded in it or not. Information embedding and steganography are concerned with hiding of information in a host or cover medium such as an audio, image, or video. Applications of information hiding range from secure secret communication of battlefield data to banking transactions and healthcare information via an innocuous medium transmitted through open channels. While cryptography conceals the information contents being transmitted, steganography conceals the existence of secret information in the cover medium, be it an audio, image, or video. In encryption, the message audio signal, for instance, is itself altered in such a way that it renders the resulting data unintelligible. Although persons without the encryption key cannot decipher the signal, transmitting encrypted information, in general, arouses suspicion about the presence of information. For battlefield communication, in particular, hiding the existence of information is therefore crucial. Using a host medium as a wrapper or carrier in steganography, the secret information can be kept intact as opposed to modifying it in cryptography [4].

1.2 MATERIALS AND METHODS

An English message text is written by using the alphabetic characters of the English language (which are 26 letters ('a'…'z')). Some other special characters are useful to use in writing messages which are giving the reader a good understanding of the message. Some of these characters that are adopted in this study: ('space character', '.', ',', '(' , ')' , '''). Therefore, the total numbers of characters that are used to write a message become 32-characters. This means that we need at least 5-bits to represent these 23-characters in any digital system. Now, a gray scale image is using 256 gray scales or each pixel in it. This means that we need (1- byte º 8-bits) per pixel to produce (2(8-bits) º 256) gray scales. The main operation of the algorithm in this [1, 2] proposed research is to map each 4-cases from (27 = 128) of the 7 Most Significant Bits (MSBs) in a pixel to one of the 32-cases of the (above mentioned) characters in the message. The algorithm's goal for using 4-cases instead of one case is to increase the probability of finding the matched pixels in the image.

2. LITERATURE SURVEY

The information communicated comes in numerous forms and is used in many applications. In a large number of these applications, it is desired that the communication to be done in secrete. Such secrete communication ranges from the obvious cases of bank transfers, corporate communications and credit card purchases, on down to a large percentage of everyday email. Steganography is the ancient art of embedding a secret message into a seemingly harmless message. Most of the newer applications use steganography like a watermark, to protect a copy right on information. The forms of steganography vary, but unsurprisingly, innocuous spam messages are turning up more often containing embedded text Steganography or Stego as it is often referred to in the IT community, literally means, "Covered writing" which is derived from the Greek language. Steganography is defined in [1] as follows, "Steganography is the art and science of communicating in a way which hides the existence of the communication. In contrast to Cryptography, where the enemy is allowed to detect, intercept and modify messages without being able to violate certain security premises guaranteed by a cryptosystem, the goal of Steganography is to hide messages inside other harmless messages in a way that does not allow any enemy to even detect that there is a second message present". Information may be covered by coding as in cryptography or by hiding as in watermarking (steganography). Many techniques can be used for hiding the digital data, from an application point of view. Many common digital hiding techniques employ graphical images or audio files as the carrier medium. There are many ways in which messages can be hidden in digital media. Digital forensics examiners are very familiar with data that remains in file slack or unallocated space as the remnants of previous files and, of course, one can write programs that can access slack and unallocated space directly. Small amounts of data can also be hidden in the unused portion of file headers. Another digital carrier can be the network protocols themselves. Secret TCP by Craig Rowland, for example, forms secret communications channels using the Identification field in Internet Protocol (IP) packets or the Sequence Number field in Transmission Control Protocol (TCP) segments. Steganography is different than cryptography and watermarking although they all have overlapping usages in the information hiding processes . Steganography security hides the knowledge that there is information in the cover medium, where cryptography revels this knowledge but encodes the data as cipher-text and disputes decoding it without permission; i.e., cryptography concentrate the challenge on the decoding process while steganography adds the search of detecting if there is hidden information or not. Watermarking is different from steganography in its main goal. Watermarking aim is to protect the cover medium from any modification with no real emphasis on secrecy. It can be observed as steganography that is concentrating on high robustness and very low or almost no security Steganography may have different applications.

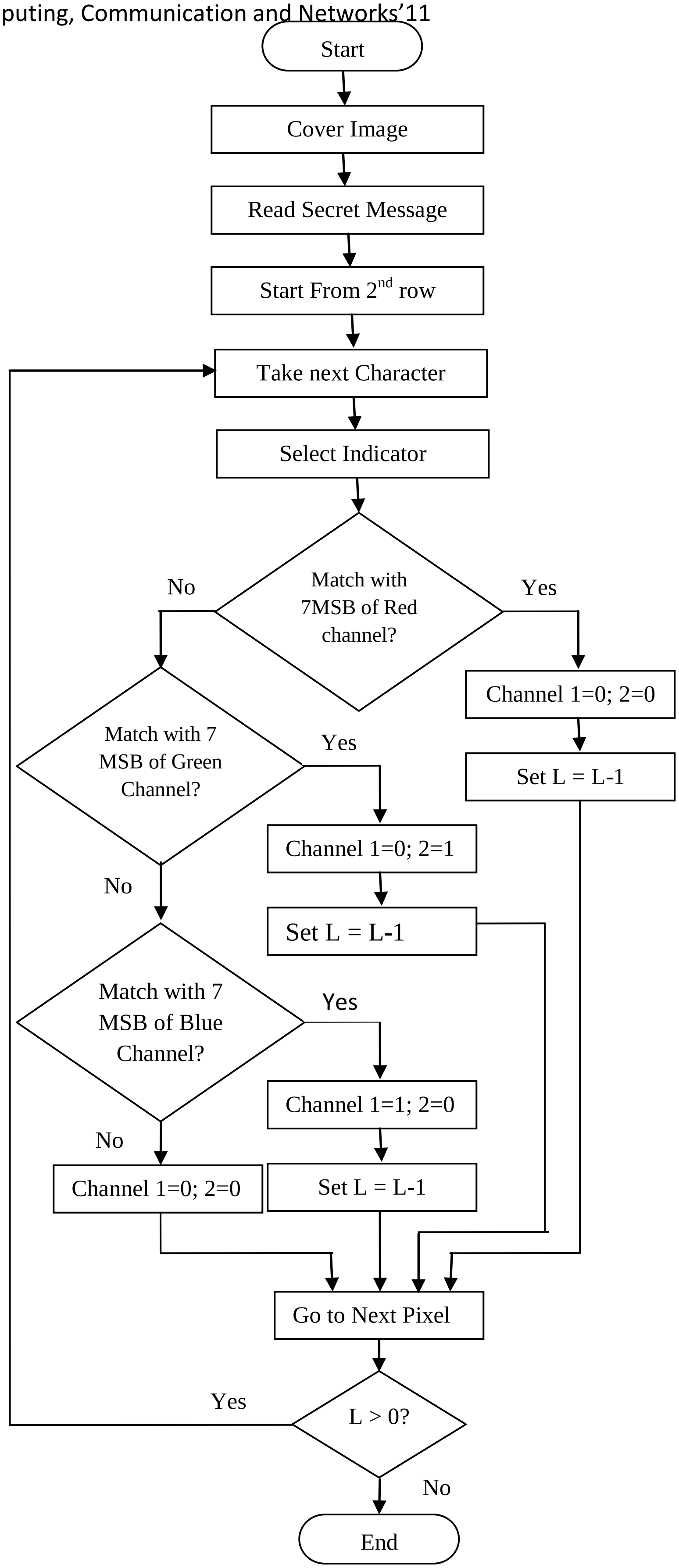

Figure 1: Flow chart for Decoding

For example, it can be used by medical doctors to combine explanatory information within X-ray images. It can be useful in communications for codes self-error correcting. It can embed corrective audio or image data in case corruption occurs due to poor connection or transmission. Steganography may be practical to form a secure channel for private communication, however, it does not cover the fact that the communication happened or the data is hidden. This makes steganography as a special technique of encryption or cryptography

3. PROPOSED ARCHITECTURE

Steganography is an ancient art of conveying messages in a secret way that only the receiver knows the existence of message [2]. So, a fundamental requirement for a stenographic method is imperceptibility; this means that the embedded messages should not be discernible to the human eye. There are two other requirements, one is to maximize the embedding capacity, and the other is security. The least-significant bit (LSB) insertion method is the most common and easiest method for embedding messages in an image. However, how to decide on the maximal embedding capacity for each pixel is still an open issue. An image stenographic model is proposed that is based on variable-sized LSB insertion to maximize the embedding capacity while maintaining the image fidelity. The proposed methodology uses the same principle of least significant bit insertion (LSB) along with a modified version of the Pixel Indicator method. Each pixel value of a color image is represented by three bytes i.e. to define the intensity of the channels RED, GREEN, BLUE.

3.1 Selecting pair of indicator channels:

We proposed model (Figure 1) we are indicator channels related to different channels also be location. It should be clear that indicator channels will be selected for every pixel. Every time we move to next pixel, the indicator channel pair will be selected depending upon the value of pseudo random number. Pseudo random number will be generated by using any function that can generate random numbers. Basically for every pixel generate a new number. Convert that into binary bit sequence. Count number of 1s present in the bit sequence and number of zeros present in the bit sequence. Also calculate the parity of the pseudo random number.

References

[1] Adnan Abdul-Aziz Gutub "Pixel Indicator Technique for RGB Image Steganography" Journal of Emerging Technologies in Web Inteligence VOL. 2, NO. 1, FEBRUARY 2010

[2] Mohammed A.F. Al-Husain "Image Steganography by Mapping Pixels to Letters" Journal of Computer Science 5 (1): 33-38, 2009

[3] Chandramouli, R. & N. Mammon "Analysis of LSB based image steganography techniques". Proceedings of the International Conference on Image Processing, Oct. 7-10, IEEE Computer Society, Washington DC., USA., pp: 1019-1022. DOI: 10.1109/ICIP.2001.958299 Dugelay, 2003

[4] Doërr, G. & J.L.." A guide tour of video watermarking. Signal Processing: Image" Comm., 18: 263-282.DOI: 10.1016/S0923-5965(02)00144-3 , 2001.