Raju Int. Journal of Engineering Research and Applications www.ijera.com
ISSN : 2248-9622, Vol. 4, Issue 10(Part - 2), October 2014, pp.36-38

RESEARCH ARTICLE OPEN ACCESS

Improved LSB Steganograhy Technique for grayscale and RGB images

Raju*, Mohit Dhanda**
*(Department of Eletronics & Communication, GNI Mullana, Mullana.)
** (Department of Eletronics & Communication, GNI Mullana, Mullana)

ABSTRACT
A number of techniques are there to converse securely. Encryption and cryptography are enabling us to have a secure conversation. To protect privacy and communicate in an undetectable way it is required to use some steganography technique. This is to hide messages in some other media generally called cover object. In todays digital world where images are a common means of information sharing, most of the steganography techniques use digital images as a carrier for hiding message. In this paper a LSB based technique is proposed for steganograpgy. This technique is different from standard LSB technique that along with message hidden in LSB bits a part of message also resides at other selective bits using a key. The method is developed to increase the payload capacity and make detection impossible.
Keywords – LSB, peak signal-to-noise ratio, (PSNR), Steganography, Steganalysis, stegokey.

I. INTRODUCTION

Hiding sensitive information within usual communications is an art termed 'Steganography'. It is one of the fundamental ways in which information can be kept confidential. For instance, by hiding covert messages within other, messages, the chance of the communication being detected is reduced. The original message is usually encrypted and then hidden within a carrier text, image or other file, producing the stego-text or hidden data. It should be noted that the main goal of steganography is to communicate securely in a completely undetectable manner [1]. Steganography also plays a major role in the associated technology of digital image watermarking. Images are the most widespread carrier medium [2]. Here, a stego tool modifies data in such a way that the image is still visible through an applied watermark, but there is no way to remove this watermark without destroying the image. When the message is hidden in the carrier a stego-carrier is formed for example a stego-image. Hopefully it will be perceived to be as close as possible to the original carrier or cover image by the human senses. The sender (or embedder) embeds the secret message to be sent into a graphic file (the cover image or the carrier). This results in the production of what is called a stego-image. Additional secret data may be needed in the hiding process e.g., a stegokey[4,5]. Cryptography and steganography can be used together. As cryptography only transforms the data into gibberish form and transmits it, it tends to attract the intruders attention. On the other hand steganography made the task of the intruder even more difficult by hiding the very existence of the secret data. However, steganography could be a failure even if the presence of secret data is detected. Thus to enhance the security of communications over covert channels, it is proposed to first encrypt the secret data using a suitable encryption algorithm, compress it and then embed it into a cover using an appropriate steganographic method[6]. If compressed the message will take up far less space in the carrier and will minimize the information to be sent. The random looking message which would result from encryption and compression would also be easier to hide than a message with a high degree of regularity. Therefore encryption and compression are recommended in conjunction with steganography [7]. One of the earliest methods to discuss digital steganography is credited to Kurak and Mc Hugh [8], who proposed a method which resembles embedding into the 4 LSB,s (least significant bits). Miaou et al. [9] present an LSB embedding technique for electronic patient records. Nirinjan and Anand [10] and Li et al. [11] also discuss patient data concealment in digital images. This paper proposes an improved LSB(least Significant bit) based Steganography technique for images imparting better information security. It presents an embedding algorithm for hiding encrypted messages in pixel locations in LSB and some selected bit positions determined by a key. The encryption and compression are eliminated in this scheme. The

proposed approach is to achieve a better payload capacity and PSNR value.

II. METHODOLOGY

Steganography involves hiding data in an covert message and doing it in such a way that it is difficult for an opponent to detect and difficult to remove. Least Significant Bit (LSB) embedding is a simple strategy to implement steganography.

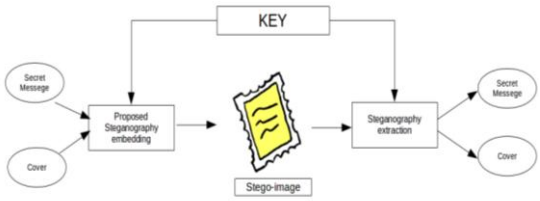

Figure :-1 image steganography process

Like all steganographic methods shown in figure-1 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. This schemes works for grayscale as well as RGB images. For example, embedding into the least significant bit changes the color value by one. Using higher order bits for embedding message distorts the image to a greater extent thus loosing the purpose. In case embedding is performed on the least significant pixel,it will increase the the likelihood of detection. In a LSB embedding, some information is always lost from the cover image. This is an effect of embedding directly into a pixel. LSB algorithms have a choice about how they embed that data to hide. They can embed losslessly, preserving all information about the data, or the data may be generalized so that it takes up less space. Digital images are represented as arrays of pixel values. A pixel is a point of an image. For a grayscale image there exists only one matrix containing grayscale level values for each pixel of image. When dealing with the RGB images there are three matrics each for red(R), green(G) and blue(B) colors. Capacity of RGB image is therefore high as a large number of LSB positions are present for embedding data. The numeric value of each pixel is stored in bytes and represents a digital color. Each of the bytes defines the amount of light intensity in each of the primary colors: red, green, and blue (RGB) and can hold values from 0 to 255 (values which can be stored in 8 bits 2^8). For example, 255 for the red value and 0 for the blue and green will render the color red. Other values close to 255 for the red component and 0s for the blue and green will also render a shade of red which may appear to be the same color to the human eye.

The proposed algorithm uses the LSB locations in the image along with some predefined bit positions in image. The predefined bit locations are decided by a digital key. This key is only known to the sender and the receiver. The key embeds the information at specific locations. To retrieve the message at receiver end this key is again required. In standard LSB staganography where the key is used only for extracting the message in our algorithm this key performs two operations i.e. retrieving the message in LSB bits along with the data hidden in specific locations other than LSB positions.

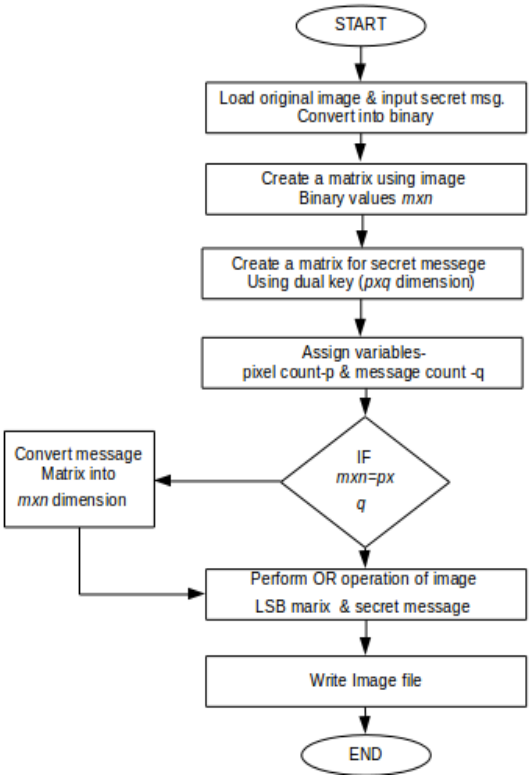

Figure:-2 flowchart for the proposed protocol.

The key is actually a combination of two keys one part belongs to LSB data extraction and the other required to extract data from specific bit locations.

III. RESULT & CONCLUSION

In LSB based steganography LSB positions can be used for hiding information. It is easy for any eavesdropper to corrupt the data by just manipulating the LSB in pixels values. In this proposed method as selective bit postions definded by key and LSB are used for hiding data. The key is selected in a way to optimize the PSNR value. It becomes much difficult to detect and extact data. Along with this the payload capacity is also increased.

REFERENCES

Journal Papers:

[1.] Ismail Avcibas, Nasir Memon, and Bulent Sankur, February 2003, " Steganalysis Using Image Quality Metrics",*IEEE Transaction on Image Processing , 12(2).*

[2.] Westfield Andreas, Pfitzmann Andreas (1999 October) Attacks on steganographic systems. *Third International Workshop,* IH_99 Dresden Germany, Proceedings, Computer Science 1768, pp 61–76.

[3.] Johnson Neil F, Zoran Duric, Sushil Jajodia (2001) *information hiding, and watermarking attacks & countermeasures.* Kluwer.

[4.] Pfitzmann Birgit (1996, May–June) *Information hiding terminology.* First International Workshop, Cambridge, UK, Proceedings, Computer Science 1174, pp 347–350.

[5.] Zollner J, Federrath H, Klimant H, Pfitzmann A, Piotraschke R, Westfeld A, Wicke G, Wolf G (1998, April) *Modelling the security of steganographic systems, Information Hiding, 2nd International Workshop*, IH_98 Portland, Oregon, Computer Science 1525, pp 344–354.

[6.] Aisha Fernandes and W. Jeberson, "Covert communication techniques in the digital world" Proc. Of the International conference

[7.] Fridrich Jiri (1999), *A new steganographic method for palette-based images. Center for Intelligent Systems,* SUNY Binghamton, Binghamton, New York. IS&T_s PICS Conference, pp 285–289.

[8.] C. Kurak, J. McHugh, *A cautionary note on image downgrading, in: Proceedings of the IEEE 8th Annual Computer Security Applications Conference*, 30 November–4 December, 1992, pp. 153–159.

[9.] S. Miaou, C. Hsu, Y. Tsai, H. Chao, A secure data hiding technique with heterogeneous data-combining capability for electronic patient records, in: *Proceedings of the IEEE 22nd Annual EMBS International Conference*, Chicago, USA, July 23–28, 2000, pp. 280–283.

[10.] U.C. Nirinjan, D. Anand, Watermarking medical images with patient information, in: *Proceedings of the 20th Annual International Conference of the IEEE Engineering in Medicine and Biolog Society*, Hong Kong, China, 29 October–1 November 1998, pp. 703–706