A New Image Steganography Based On Mathematical Methods

M.Sarika
M.Tech
Vidya Vikas Institute of Technology
Chevella, India

Abstract: Stenography is art of hiding information in ways that prevent the detection of hidden messages. Stenography derived from Greek, literally means "Covered Writing". This paper introduces a novel method to detect the typical LSB (Least Significant Bit) embedding and the LSB matching steganography methods applied to grayscale images. The proposed method determines the changes made to some selected features extracted from the gray level run length matrix. It is shown that the run length characteristics can significantly be affected by the embedded message bits so can be employed as a measure that is quite sensitive to the arrangements of the image pixel values. The extracted features are examined by a nonlinear SVM (support vector machine) classifier with quadratic kernel that can distinguish between stego and clean images. Experimental results are given to demonstrate the competitively higher performance of the proposed method, as compared to other well-known steganalysis methods, at different embedding rates.
Keywords: Stenography, SVM

I INTRODUCTION

The hide a message, open a bitmap file, then enter a password or select a key file. The key file can be any file or another bitmap. This password or key will be treated as a stream of bytes specifying the space between two changed pixels. I don't recommend text files, because they may result in a quite regular noise pattern. The longer your key files or password is the less regular the noise will appear. Next step, enter the secret message or choose a file, and click the Hide button. The application writes the length of the message in bytes into the first pixel. After that it reads a byte from the message, reads another byte from the key, and calculates the coordinates of the pixel to use for the message-byte. It increments or resets the color component index, to switch between the R, G and B component. Then it replaces the R, G or B component of the pixel (according to the color component index) with the message-byte, and repeats the procedure with the next byte of the message. At last, the new bitmap is displayed. Save the bitmap by clicking the Save button. If the grayscale flag is set, all components of the color are changed. Grayscale noise is less visible in most images. 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 secret key present. Steganography includes a vast array of techniques for hiding messages in a variety of media. Among these methods are invisible inks, microdots, digital signatures, covert channels and spread-spectrum communications. Today, thanks to modern technology, steganography is used on text, images, sound, signals, and more. To extract a hidden message from a bitmap, open the bitmap file and specify the password or key you used when hiding the message. Then choose a file to store the extracted message in (or leave the field blank, if you only want to view hidden Unicode text), and click the Extract button. The application step through the pattern specified by the key and extracts the bytes from the pixels. At last, it stores the extracted stream in the file and tries to display the message. Don't bother about the character chaos, if your message is not a Unicode text. The data in the file will be all right. This works with every kind of data, you can even hide a small bitmap inside a larger bitmap. If you are really paranoid, you can encrypt your files with PGP or GnuPG before hiding them in bitmaps. Now a days, various modes of communication like LAN, WAN and INTERNET are idle used for communicating information from one place to another around the lobe. Such communication networks are open which any one can access easily. They are regularly monitored and an intercepted. Steganography, from the Greek, means covered or secret writing, and is a long-practiced form of hiding information. Although related to cryptography, they are not the same. Steganography's intent is to hide the existence of the message, while cryptography scrambles a message so that it cannot be understood. More precisely, "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 secret message present."

II STEGANOGRAPHY

Steganography is an ancient art of hiding information. Digital technology gives us new ways to apply steganographic techniques, including one of the most intriguing—that of hiding information in digital images. It includes vast arrays of secret communications methods that conceal the message's very existence. These methods are including invisible inks, microdots, character arrangement, digital signature, covert channels and spread spectrum communications. Stenography and Cryptography are cousins in the spy craft family. Cryptography scrambles a message so it cannot be understood. Stenography hides the message so it cannot be seen. A message in cipher text, for instance, might arouse suspicion on the part of the recipient while an "invisible" message created with stenographic regions. Figure 1.1. Generic form of Image Steganography includes a vast array of techniques for hiding messages in a variety of media. Among these methods are invisible inks, microdots, digital signatures, covert channels and spread-spectrum communications. A message is embedded in a cover media in an invisible manner so that one could not suspect about its existence. In this paper we present a substitution based information protection method where we combine cryptographic, steganographic and signal processing concepts together for achieving security. The method is known as Steganography Based Information Protection method. In this method we substitute the information bit in randomly selected pixels at random places within LSB region.

The LSB matching, a counterpart of LSB replacement, retains the favorable characteristics of LSB replacement, it is more difficult to detect from statistical perspective. In LSB matching, if the bit must change, the operation of ±1 is applied to the pixel value. The use of + or - is chosen randomly and has no effect on the hidden message. The detectors for both LSB replacement and ±1 embedding work the same way: the LSB for each selected pixel is the hidden bit. Since LSB techniques are fairly easy to implement and have a potentially large payload capacity, there is a large selection of Steganography software available for purchase and via shareware (e.g., www.stegoarchive.com). This seemingly innocent modification of the LSB embedding is significantly harder to detect, because the pixel values are no longer paired. Theoretical analysis and practical experiments show that steganalysis of LSB matching is more difficult than that of LSB replacing (Ker, 2005a). As a result, none of the existing attack methods on LSB replacement can be adapted to attack LSB matching.

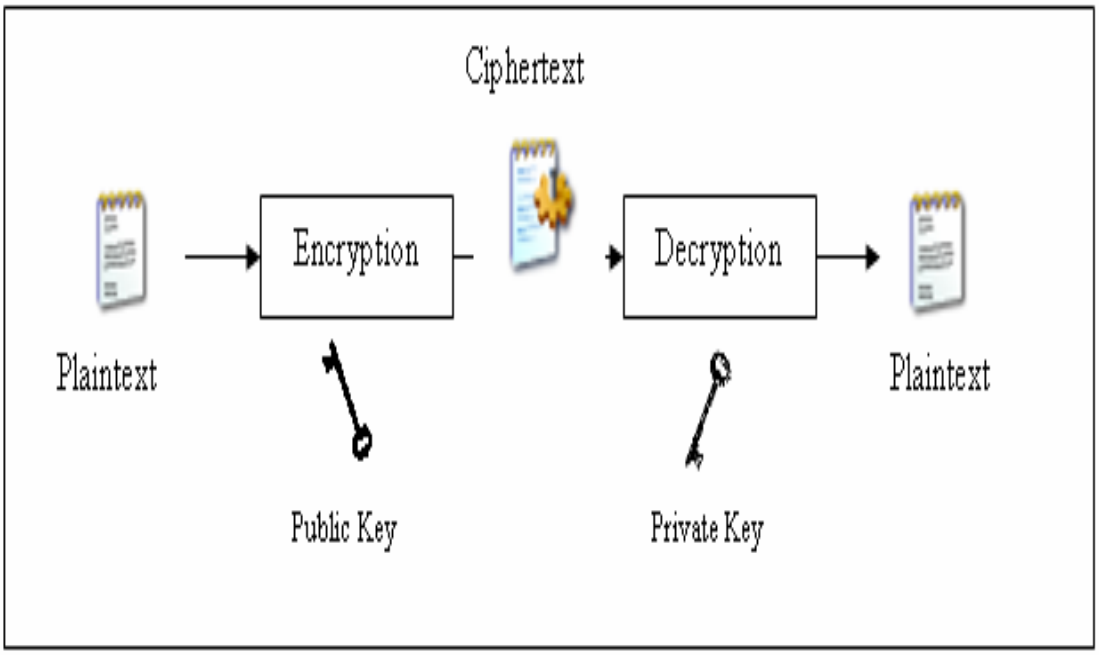

Figure 2.1: Public-key scheme

III STUDY OF THE SYSTEM

A. feasibility study

The feasibility of the project is analyzed in this phase and business proposal is put forth with a very general plan for the project and some cost estimates. During system analysis the feasibility study of the proposed system is to be carried out. This is to ensure that the proposed system is not a burden to the company. For feasibility analysis, some understanding of the major requirements for the system is essential.

Three key considerations involved in the feasibility analysis are

- ECONOMICAL FEASIBILITY
- TECHNICAL FEASIBILITY
- SOCIAL FEASIBILITY
-

B. economical feasibility

T

This study is carried out to check the economic impact that the system will have on the organization. The amount of fund that the company can pour into the research and development of the system is limited. The expenditures must be justified. Thus the developed system as well within the budget and this was achieved because most of the technologies used are freely available. Only the customized products had to be purchased.

III EXISTING SYSTEM

The present system is presently is an undeveloped system. Before developing the Hiding messages in the noise of a picture is not possible to hide the message.

A. Problems in existing system

Our focus is hiding the message of a related picture based on the certain key. The present system is an undeveloped system. Before developing the Hiding messages in the noise of a picture is not possible to hide the message for related picture. The existing system is manual and the manual system works in the following way: In Existing System, today's dynamic and information rich environment, information systems have become vital for any organization to survive. With the increase in the dependence of the organization on the information system, there exists an opportunity for the competitive organizations and disruptive forces to gain access to other organizations information system. This hostile environment makes information systems security issues critical to an organization. Current information security literature either focuses on anecdotal information by describing the information security attacks taking place in the world or it comprises of the technical literature describing the types of security threats and the possible security systems.

IV PROPOSED SYSTEM

The present system is used to provide hide the message to the selected bitmap picture based on the key. The key is in the format of text or a file. Using this key convert the message in the form of stream of bytes .Then using Extract button extract a hidden message from a bitmap file based on the same key or file used for hiding the message. The algorithm present in the existing system was somewhat complicated. In Cryptography, the meaning of data has been changed. So, it makes intention to the hacker to hack or destroy the data. In our proposed system, we implement a new technology called Stenography for Network security. It not only changes the meaning of data but also hides the presence of data from the hackers. In order to secure the transmission of data, Cryptography has to be implemented. Cryptography is the science of devising methods that allow information to be sent in a secure form in such a way that the only person able to retrieve this information is intended recipient.

V CONCLUSION

In this paper, a new image steganography scheme which is a kind of spatial domain technique. In order to hide secret data in cover-image, the first component alteration technique is used. Techniques used so far focuses only on the two or four bits of a pixel in a image ,(at most five bits at the edge of an image.) which results less peak to signal noise ratio and high root mean square error i.e. less than 45 PSNR value. Proposed work is concentrated on 8 bits of a pixel (8 bits of blue component of a randomly selected pixel in a 24 bit image), resulting better image quality. Proposed technique has also used contrast sensitivity function (CSF) and just noticeable difference (JND) Model. Proposed scheme can embed more data than previous schemes [7, 5, 10], and shows better

imperceptibility. To prove this scheme, several experiments are performed, and the experimental results are compared with the related previous works. Consequently, the experimental results proved that the proposed scheme is superior to the related previous works. The future work is to extend proposed technique for videos and to modify given scheme to improve image quality by increasing PSNR value and lowering MSE value.

VI RESULTS

Lena image	LSB3	PVD	Lie Chang's	Jae Gil Yu	First Component alteration technique
PSNR	37.92	41.48	37.53	38.98	46.11

Fig5.0 Vessel Image

Fig 5.1 Stego image

REFERENCES

1. D. Kahn, The Codebreakers, Macmillan,New York, 1967.
2. B. Norman, Secret Warfare, Acropolis Books, Washington, D.C., 1973.
3. H.S. Zim, Codes and Secret Writing,William Morrow, New York, 1948.
4. J. Brassilet et al., "Document Marking and Identification using Both Line and Word Shifting," Proc. Infocom95, IEEE CS Press, Los Alamitos, Calif., 1995.
5. P. Wayner, Disappearing Cryptography,AP Professional, Chestnut Hill, Mass.,