International Journal of Information, Control and Computer Sciences
ISSN: 2517-9942
Vol:4, No:7, 2010

A Dynamic RGB Intensity Based Steganography Scheme

Mandep Kaur, Surbhi Gupta, Parvinder S. Sandhu, Jagdeep Kaur

***Abstract*—**Steganography meaning covered writing. Steganography includes the concealment of information within computer files [1]. In other words, it is the Secret communication by hiding the existence of message. In this paper, we will refer to cover image, to indicate the images that do not yet contain a secret message, while we will refer to stego images, to indicate an image with an embedded secret message. Moreover, we will refer to the secret message as stego-message or hidden message. In this paper, we proposed a technique called RGB intensity based steganography model as RGB model is the technique used in this field to hide the data. The methods used here are based on the manipulation of the least significant bits of pixel values [3][4] or the rearrangement of colors to create least significant bit or parity bit patterns, which correspond to the message being hidden. The proposed technique attempts to overcome the problem of the sequential fashion and the use of stego-key to select the pixels.

***Keywords*—**Steganography, Stego Image, RGB Image, Cryptography, LSB.

I. Introduction

IT is the process of hiding a message in a medium, such as a digital picture or audio file, so as to resist detection. It is the secret transmission of a message. It is different from encryption, because the goal of encryption is to make a message difficult to read while the goal of steganography is to make a message altogether invisible. A steganographic [8] message may also be an encrypted as an extra barrier to interception, but need not be. Used as an alternate to encryption, it takes advantage of unused bits within the file structure or bits that are mostly undetectable if modified. A steganographic message rides secretly to its destination, unlike encrypted messages, which although undecipherable without the decryption key, can be identified as encrypted. It includes a vast array of secret communication methods that conceal the message's very existence. These methods include invisible inks, microdots, character arrangement, digital signatures, covered channels, and spread spectrum communications.

Embedding data, which is to be hidden into an image, requires two files. The first is the image that will hold the hidden information, called the cover image. The second file is the message- the information to be hidden. When combined the cover image and the embedded message make a stego-image or stego-file as shown in figure 1.

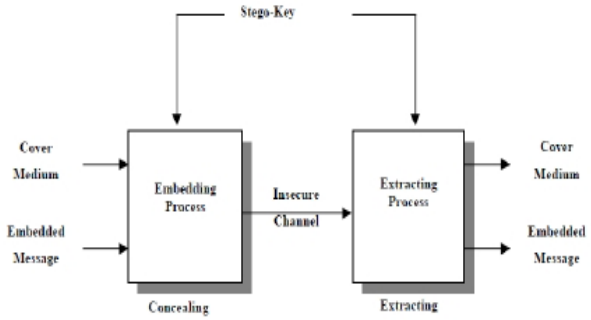

Fig. 1. Steganographic Process

A. Applications of Steganography

Like many security tools, steganography can be used for a variety of reasons:

i) Confidential communication and secret data storing: Steganography can be used to maintain the confidentiality of valuable information, to protect the data from possible sabotage, theft, or unauthorized viewing [5]. It provides us with:

- Potential capability to hide the existence of confidential data
- Hardness of detecting the hidden data
- Strengthening of the secrecy of the encrypted data

ii) Access control system for digital content distribution: A prototype of an "Access Control System" [21] for digital content distribution through Internet has been developed. The following steps explain the scheme:

- A content owner classify his/her digital contents in a folder-by-folder manner, and embed the whole folders in some large vessel according to a steganographic method using folder access keys, and upload the embedded vessel (stego data) on his/her own Webpage.
- On that Webpage the owner explains the contents in depth and publicize worldwide. The contact information to the owner (post mail address, e-mail address, phone number, etc.) will be posted there.
- The owner may receive an access-request from a customer who watched that

Surbhi Gupta is associated with Deptt. of CSE & IT, Rayat Instiiute of Engg. & Information Technology, Rail Majra, Punjab, India.
Jagdeep Kaur is associated with CEC, Landran, Punjab India
Mandeep Kaur and Parvinder S. Sandhu are associated with Feptt. Of CSE & IT, Rayat & Bahra Institute of Engineering & Bio-Technology, Sahauran, Distt. Mohali (Punjab)-140104 INDIA.

Webpage. In that case, the owner may (or may not) creates an access key and provide it to the customer (free or charged).

iii) Digital watermarks

Steganography can also be used in digital watermarks that include things like watermarking images such as copyright protection which are intended to prevent or deter unauthorized copying of digital media. Digital watermarks[15][17], sometimes known as fingerprinting, are similar to steganography in that they are overlaid in files, which appear to be part of the original file and are thus not easily detectable by the average person.

iv) Modern printers

Steganography is used by some modern printers, including HP and Xerox brand color laser printers. Tiny yellow dots are added to each page. The dots are barely visible and contain encoded printer serial numbers, as well as date and time stamps [8].

v) Moreover, it can also be used to tag notes to online images.

vi) Illegitimate purposes

And, as was pointed out in the concern for terrorist purposes, it can be used as a means of covert communication.

When hiding information inside images the LSB (Least Significant Byte) method[19] is usually used. To a computer an image file is simply a file that shows different colors and intensities of light on different areas of an image. The best type of image file to hide information inside of is a 24 Bit BMP (Bitmap) image. The reason being is this is the largest type of file and it normally is of the highest quality. When an image is of high quality and resolution it is a lot easier to hide and mask information inside of. Although 24 Bit images are best for hiding information inside of due to their size some people may choose to use 8 Bit BMP's or possibly another image format such as GIF, the reason being is that posting of large images on the internet may arouse suspicion. It is important to remember that if you hide information inside of an image file and that file is converted to another image format, it is most likely the hidden information inside will be lost.

B. RGB Model

In this paper, we proposed a technique called RGB intensity based steganography model. To a computer an image is an array of numbers that represent light intensities at various points (pixels) these pixels makeup the image's raster data. Digital images are typically stored in either 24-bit (RGB) or 8-bit (Grayscale) files. A 24-bit image provides the most space for hiding information; however it can be quite large (with the exception of JPEG images). All color variations for the pixels are derived from three primary colors: red, green, and blue. Each primary color is represented by one byte.

The RGB color model is an additive color model in which red, green, and blue light are added together in various ways to reproduce a broad array of colors. The main purpose of the RGB color model is for the sensing, representation, and display of images in electronic systems, such as televisions and computers, though it has also been used in conventional photography.

In this technique, variable numbers of bits are stored in each channel of pixel. The sequence of the channel is based on random order. Here, one channel is used as a pixel indicator, that decides the state whether data is present or not in other two respective channels. Suppose if R channel acts as an indicator then G and B channels will be used to hide the data.

B. Advantages

The proposed RGB intensity based steganography technique consists of following advantages:

- RGB is the most common and simplest model.
- The technique is more secure; third party cannot easily detect the presence of hidden data.
- One of the main advantages is its capacity, because it embeds large amount of data as compared to previous techniques.

II. Related Work

Data hiding technique [1] is a new kind of secret communication technology. It has been a hot research topic in recent years, and it is mainly used to convey messages secretly by concealing the presence of communication. There have been proposed many techniques about data hiding. A large number of popular data hiding tools, such as S-Tools 4, HideBSeek, Steganos and StegoDos[13] etc, that are based on LSB replacement. By using information hiding techniques, it is possible to fuse the digital content within the image signal regardless of the file format and the status of the image.

Curran[2] explained that Steganography was a process that involves hiding a message in an appropriate carrier for example an image or an audio file. The carrier can then be sent to a receiver without anyone else knowing that it contains a hidden message. This was a process, which can be used for example by civil rights organizations in repressive states to communicate their message to the outside world without their own government being aware of it. Less virtuously it can be used by terrorists to communicate with one another without anyone else's knowledge. In both cases the objective was not to make it difficult to read the message as cryptography does, it was to hide the existence of the message in the first place possibly to protect the courier.

Provos and Honeyman discussed existing steganographic systems and presented recent research in detecting them via statistical steganalysis[19]. Other surveys focused on the general usage of information hiding and watermarking or else provide an overview of detection algorithms. In this paper, three different aspects in information-hiding systems contend with each other: capacity, security, and robustness. Capacity refers to the amount of information that can be hidden in the cover medium, security to an eavesdropper's inability to detect hidden information, and robustness to the amount of modification the stego medium can withstand before an adversary can destroy hidden information.

Sutaone and Khandare explained in their paper a steganography system was designed for encoding and decoding a secret file embedded into an image file using random LSB insertion method in which the secret data were spread out among the image data in a seemingly random manner. This could be achieved using a secret key. The key used to generate pseudorandom numbers, which will identify where, and in what order the hidden message was laid out. The advantage of this method was that it incorporates some cryptography in that diffusion is applied to the secret message.

Parvez and Gutub introduced a new algorithm for RGB image based steganography. This concept referred to a technique of storing variable number of bits in each channel (R, G or B) of pixel based on the actual color values of that pixel: lower color component stores higher number of bits[3]. The sequence of channels was selected randomly based on a shared key. This technique ensured a minimum capacity and can accommodate to store large amount of data. Experimental results show that our algorithm performs much better compared to the existing algorithms. This algorithm[4] can also be used to store fixed no of bits per channel, but can still offer very high capacity for cover media.

This algorithm also offered very high capacity for cover media compared to other existing algorithms. In this paper, there were some experimental results showing the superiority of the algorithm and also some comparative results with other similar algorithms in image based steganography.

Javed et.al, focused on the analysis and enhancement of steganographic strategies for multimedia data hiding authentication. Based on an authentication game between an image and its authorized receiver, and an opponent, security of authentication watermarking was measured by the opponent's inability to launch a successful attack. In this work, they considered two stages of data hiding mechanism: Hiding the data in an image along with conditional security and detecting the hidden data. They proposed a novel security enhancement strategy [8] that resulted in efficient and secure LSB-based embedding and verification phenomenon. They showed that using their approach, protection is achieved without significant increase in image size and color distortion, and without sacrificing the image or video quality.

III. Methodology

Our technique is based on RGB images. The least significant bit insertion method is probably the most well known image steganography technique. It is a simple method in which information can be embedded in a graphical image files. When applying LSB techniques to each bytes of an 8-bit image, one bit can be encoded to each pixel. Any changes in the pixel bits will be indiscernible to the human eye. The main advantage of LSB insertion[3] is that data can be hidden in the least and second to least bits and still the human eye would be unable to notice it. Care needs to be taken in the selection of the cover image, so that changes to the data will not be visible in the stego-image. The four least significant bits of one of the channel will be used as an indication to the existence of hidden data in other two channels as follow:

TABLE I MEANING OF INDICATOR VALUES WHEN REFERRING TO FOUR LEAST SIGNIFICANT BITS

Pixel indicator	Pixel(1)	Pixel(2)	Pixel(3)	Pixel(4)
0000	No hidden data	No hidden data	0-bits of data	0-bits of data
0100	No hidden data	Contains hidden data	0-bits of data	2-bits of data
0101	No hidden data	Contains hidden data	0-bits of data	4-bits of data
1000	Hidden data in 1st channel	No hidden data	0-bits of data	2-bits of data
1010	Hidden data	No hidden data	4-bits of data	No hidden data
1111	Hidden data	Hidden data	4-bits of data	4-bits of data

The least two significant bits [4] of one of the channel, that can be used as an indicator will be selected in a random fashion. The proposed technique attempts to overcome the problem of the sequential fashion and the use of stego-key to select the pixels.

Therefore, we propose the following dynamic algorithm:

- Four LSB's of one of the three channels will be used as pixel indicator. The order of the indicator can be selected randomly.
- Data will be stored in other two channels, instead of pixel indicator. The channel, whose color value is lowest among the two channels other than the indicator, will store the data in its least significant bits.
- The selection of the indicator is based on the specified range that is, if, the color value of the channel is between 0-85, then we can afford 4 bit changes, if the value lies between 85-170, then there will be 2 bits of changes and no data will be hidden in channels having value between 170-255. The lower the value, the higher the data-bits to be stored.
- The very first value 4 will be selected as pixel indicator and other channels will be used to store the data bits.

The flowchart of the proposed algorithm is shown in figure 2 and meaning of indicator values when referring to four least significant bits is tabulated in table 1.

IV. Conclusion

In this paper, we conclude that our proposed system provides a good and efficient way to conceal data and reached the destination in a safe manner. We have addressed the problem of steganography of RGB images. Steganography using LSB with more than one bit used for the hidden data gives us more space to store data. We used image color values to decide whether to hide the data bits or not. We explained the dynamic approach which is more secure and at the same time, it has shown great results in terms of capacity. . In this

approach, we have enhanced the previous work which uses only 2 LSB's of channels but in our approach, not only we are using 2 LSB's but also making use of 4 LSB's.

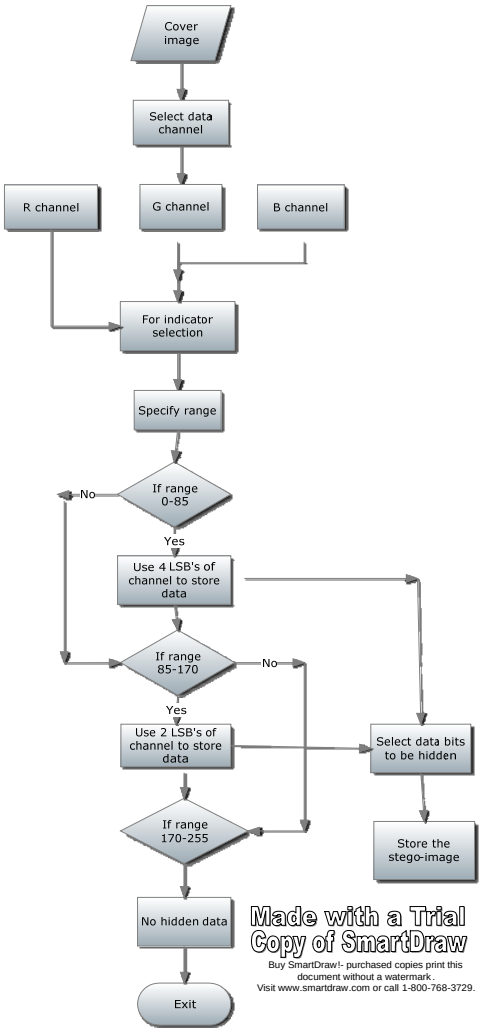

Fig. 2. Flowchart of the Proposed Algorithm

REFERENCES

[1] Provos, N., Honeyman, P, Hide and seek: An introduction to steganography, IEEE Security & Privacy Magazine 1 (2003) pp. 32-44.

[2] Karen Bailey, Kevin Curran, An evaluation of image based steganography methods using visual inspection and automated detection techniques, Multimedia Tools and Applications, Vol 30 , Issue 1 (2006) pp. 55-88.

[3] Adnan Gutub, Mahmoud Ankeer, Muhammad Abu- Ghalioun, Abdulrahman Shaheen, and Aleem Alvi, Pixel indicator high capacity technique for RGB image based Steganography, WoSPA 2008 – 5th IEEE International Workshop on Signal Processing and its Applications, University of Sharjah, Sharjah, U.A.E. 18 – 20 March 2008.

[4] S. Venkatraman, A. Abraham, M. Paprzycki, "Significance of Steganography on Data Security", International Conference on Information Technology: Coding and Computing (ITCC'04), Las Vegas, 5-7 April 2004.

[5] N.F. Johnson, S. Jajodia, "Exploring Steganography: Seeing the Unseen", IEEE computer, Vol. 31, No. 2, pages 26-34, February 1998.

[6] K. Bailey, K. Curran, "An Evaluation of Image Based Steganography Methods", Multimedia Tools & Applications, Vol. 30, No. 1, pages 55-88, July 2006.

[7] Artz, "Digital Steganography: Hiding Data within Data", Los Alamos NationalLaboratory, http://www.cc.gatech.edu/classes/AY2003/cs6262_fall/digital_steganography.pdf, May 2001.

[8] Silman, J., Steganography and Steganalysis: An Overview, SANS Institute 2001.

[9] [Zollner98] Zollner J., H. Federrath, H. Klimant, A. Pfitzmann, R. Piotraschke, A. Westfeld, G. Wicke, G. Wolf, Modelling the Security of Steganographic Systems, Information Hiding, 2nd International Workshop, IH'98 Portland, Oregon, USA, Computer Science 1525. pp. 344-354, April 1998.

[10] S. Lyu and H. Farid, steganalysis using higher-order image statistics, IEEE Transactions on Information Forensics and Security, 1(1)(2006) 111-119.

[11] D. Kahn, The Codebreakers: The comprehensive history of secret communication from ancient times to the Internet, Scribner, December 5, 1996. C. Hosmer, Discovering hidden evidence, Journal of Digital Forensic Practice, (1)(2006)47-56.

[12] J.C. Hernandez-Castro, I. Blasco-Lopez and J.M. Estevez-Tapiador, Steganography in games: A general methodology and its application to the game of Go, Computers and Security, Elsevier Science, 25(2006) 64-71.

[13] P. Hayati, V. Potdar, E. Chang, A survey of steganographic and steganalytic tools for the digital forensic investigator,available from: http://debii.curtin.edu.au/~pedram/images/docs/survey_of_steganography_and_steganalytic_tools.pdf

[14] W. Bender, W. Butera, D. Gruhl, R. Hwang, F.J. Paiz and S. Pogreb, Applications for data hiding, IBM Systems Journal, 39 (3&4)(2000) 547-568.

[15] F.A.P. Petitcolas, "Introduction to information hiding", in: S. Katzenbeisser and F.A.P. Petitcolas, (ed.) (2000) Information hiding techniques for steganography and digital watermarking, Norwood: Artech House, INC.

[16] N. F. Johnson and S. Katzenbeisser, "A survey of steganographic techniques," in Proc. Information Hiding, Norwood, MA, 2000, pp. 43–78.

[17] J.-L. Dugelay and S. Roche, "A survey of current watermarking techniques," in Information Hiding Techniques for Steganography and Digital Watermarking, S. Katzenbeisser and F. A. P. Petitcolas, Eds. Norwood, MA: Artech House, 1999, ch. 6

[18] A.Westfeld and A. Pfitzmann, "Attacks on steganographic systems," in Proc. 3rd Information Hiding Workshop, Dresden, Germany, 1999, pp. 61–76.

[19] N. Provos and P. Honeyman, Detecting steganographic content on the Internet, Center for Information Technology Integration, University of Michigan, technical report, August 31, 2001.

[20] M. Kharrazi, H.T. Sencar and N. Memon, Performance study of common image steganography and steganalysis techniques, Journal of Electrical Imaging, 15(4)(2006)1-16.

[21] J. Fridrich, Application of data hiding in digital images, Tutorial for the ISSPA'99, Brisbane, Australia, August 22-25 1999.

[22] S.C. Katzenbeisser, Principles of steganography, in: S. Katzenbeisser and F.A.P Petitcolas, (ed.), Information hiding techniques for steganography and digital watermarking, Norwood: Artech House, INC,2000.

[23] P. Kruus, C. Scace, M. Heyman and M. Mundy, A survey of steganographic techniques for image files, Advanced Security Research Journal, V (I) (2003)41-51.