Random Image Steganography in Spatial Domain

Dr. Diwedi Samidha[1], Dipesh Agrawal[2]
[1,2]NRIIST,
[1,2]Bhopal, [1,2]India
[2]agrawal.dipesh@gmail.com

Abstract— **Steganography is an art of hiding information in some media. This paper describes various image steganography techniques, based on spatial domain and by considering pixel values in binary format. Spatial domain is based on physical location of pixels in an image. Generally 8 bit gray level or colour images can be used as a cover to hide data. Again binary representations of these pixels are considered to hide secret information. Random bits from these bytes are used to replace the bits of secret. In this paper, many steganography techniques can be used like Least Significant Bit (LSB), layout management schemes, replacing only 1's or only zero's from lower nibble from the byte are considered for hiding secret message in an image. Along with these techniques, some more methods are proposed, based on selection of random pixels from an image and again secret data is hidden in random bits of these randomly selected pixels. For this purpose, many parameters of an image are considered like physical location of pixels, intensity value of pixel, etc.**

Keywords— **Steganography, LSB, Raster Scan, Random scan, Layout Management**

I.INTRODUCTION

Steganography is a technique of hiding secret information in any of media like – image, text, audio and video. Message to be hidden is concealed in another file called cover media. Combination of secret message and cover file is called as ―stego‖. This stego is transmitted over a network to specified destination. Data can be hidden in pixels of an image.

A pixel has some integer value, based on the intensity of colour that is displayed by a pixel. This integer value can be converted into binary format, i.e. in the form of bytes of 1's and 0's. Individual bits from these bytes can be used to hide secret information. These bits can be selected randomly from a byte and replaced with a secret data. Pixels in which data is to be hidden are also selected randomly, from an image.

Thus, pixels used for data hiding can be selected using various algorithms and techniques, described in this paper are – Layout management schemes [2]. Also, bits from each selected pixel can chosen randomly using some algorithms, like LSB [1].

This paper proposes new methods for selection of pixels from an image, randomly for hiding secret data. Also some techniques are proposed to select bits randomly from the bytes which represent pixels of an image.

II. RELATED WORK

Steganography is one more information security tool like Cryptography and Watermarking. Cryptography There are so many image steganography techniques based on spatial domain. Spatial domain means actual physical location of a pixel in an image. While hiding data in a pixel, the physical location of a pixel is considered and then the binary format of that pixel value is used to hide the data.

A. Least Significant Bit:

One of the simplest and very popular technique of steganography is Least Significant Bit (LSB). In this technique, least significant bit or bits of a pixel are replaced by the bits of data to be hidden [1].

LSB can be extended up to 4 least significant positions from a byte, i.e. we can replace four bits of hidden data with the original value of a pixel, whose binary value is of 8 bits. So, out of 8 bits, at max 4 bits can be used to hide data. We can replace last two bits also. Replacing four bits, may cause distortion in an image due to noticeable change in colour and intensity of an image.

B. Replacing only 1's or Zero's:

Another technique is, to consider binary values of a pixel and replace all 1's only from last four least significant bits, with the bits of data to be hidden [4].

Same way we can do for 0's only. This will dynamically hide number of bits or bytes, in the cover medium. Detection of hidden data will be very difficult for any intruder.

C. Layout Management Schemes:

Another approach can be, to consider layout of pixels from an image in various ways, and according to the logical sequence of pixels, data can be hidden in the LSBs, up to four positions at max [2].

Pixels can be considered in any sequence like, starting from centre position and coming outside in a rectangular way. Similarly, starting from outer pixel, going towards the centre in a rectangular way. This approach is shown in figure given below.

Another approach is, consider pixels in snake movement, diagonal movement, starting from top left or top right or bottom left or bottom right.

978-1-4673-5301-4/13/$31.00 ©2013 IEEE

Hence we can use any arrangement of pixels and can make logical sequence of these pixels to hide secret data.

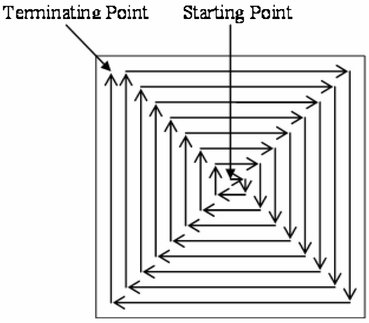

Fig. 1 Logical sequence of pixels from centre to outer side

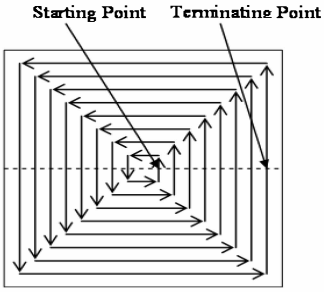

Fig. 2 Logical sequence of pixels towards centre from outer side

III. PROPOSED WORK

In our work, we proposed following methods of hiding data based on random bits of random pixel positions of an image.

A. Replacing Intermediate Bit

Using this technique, any bit or any intermediate bit from a given byte (of a pixel value) can be replaced by the bit of a data to be hidden.

For ex. Original data is –

TABLE I
COVER DATA

10101110	00011101	11001101	11110001
01010100	11101111	10110001	10101000

Message to hide is – 11001101

Bits are replaced according to any random sequence from LSB to MSB position

TABLE II
COVER DATA + SECRET DATA = STEGO

10111110	00011111	11001101	11100001
5th Bit	2nd Bit	6th Bit	4th Bit
01011100	11101111	10100001	10101010
4th Bit	3rd Bit	5th Bit	2nd Bit

Underlined bits shows the bits of secret message are replaced with the bits of original data at that position.

B. Raster Scan Principle

This method is similar to Raster Scan principle of displaying an image on CRT display. In this, pixels from alternate horizontal lines are used for replacing the secret information. A simple LSB scheme can be used for pixels of first horizontal line. Then second line is skipped. Again third line is used to hide secret information and so on. We can also use 2:1 interlacing, 4:1 interlacing and so on.

Consider original data –

TABLE III
COVER DATA

10101110	00011101	11001101	11110001
11100010	01011011	00111001	11000111
10101010	11100010	00101010	01011100
00000000	00011100	11000010	11111110

Message to hide is - 11001101

Message will be hidden using following technique.

TABLE IV
COVER DATA + SECRET DATA = STEGO

10101111	**00011101**	**11001100**	**11110000**
11100010	01011011	00111001	11000111
10101011	**11100011**	**00101010**	**01011101**
00000000	00011100	11000010	11111110

In above table, individual bits of secret message are replaced with bits of original pixels. Pixels are selected according to the raster scan method.

C. Random Scan Principle

This method is similar to Random Scan principle of displaying an image on CRT display. In this, the sequence, in which pixels are drawn, they are used to hide secret information. Again any simple data hiding algorithm like LSB, can be used to hide secret information. By this method, data can be hidden in random pixels in an image.

TABLE V
COVER DATA

10101110	00011101	11001101	11110001
11100010	01011011	00111001	11000111
10101010	11100010	00101010	01011100
00000000	00011100	11000010	11111110

Message to hide is - 11001101

Message will be hidden using following technique.

TABLE VI
COVER DATA + SECRET DATA = STEGO

10101111	00011101	**11001101**	**11110000**
11100010	**01011010**	00111001	11000111
10101011	11100011	**00101011**	01011101
00000000	**00011100**	11000010	**11111111**

In this table, individual bits of secret message are replaced with individual bits of original pixels. Where pixels are selected randomly.

D. Colour based data hiding

In this scheme one fixed colour is used to hide secret data. Intensity values of this fixed colour are converted into binary format and the secret information is hidden in this binary data.

For ex. consider a gray scale 8 bit image, having intensity values ranging from 0 to 255.

Suppose we have fixed a colour, whose intensity value is 155. Binary value of this is - 10011011.

We will find total number of pixels from an image, having the same intensity value.

Suppose there are 50 pixels found. Then we can hide secret information in these 50 pixels, using any data hiding technique like – LSB etc.

We can extend this technique by taking more than one fixed colour of pixels, from an image.

E. Shape based data hiding

In this scheme, any shape can be taken to hide the data in an image. For ex. consider a triangular shape. As shown in figure below.

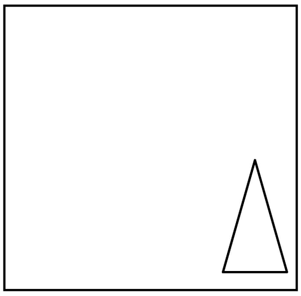

Fig. 3 Shape based data hiding

According to figure, secret information can be hidden only in the pixels which are available in triangular shape, instead of hiding secret information in whole image. We can use any shape having any dimensions.

We can extend this technique, by using any shape of any dimension at any place in an image.

IV.CONCLUSION

In this paper, along with existing techniques of image steganography, some new methods for hiding data in images are discussed. Data can be hidden in pixels. Physical location of these pixels can be decided using the techniques which are described in this paper. After selecting random pixels, the secret data can be hidden in random bits, which are represented in the bytes of binary digits. While selecting these pixels, many parameters from an image are considered for ex. Colour of pixels, physical location of pixels etc. Based on these parameters and by considering some more parameters from an image, we can derive some more techniques of image steganography, based on spatial domain steganography and random bit steganography.

REFERENCES

[1] Ali K. Hmood, B. B. Zaindan, –an overview on hiding information techniques in images‖ journal of applied sciences 10 (18): 2094-2100, 2010 ISSN 1812-5654. 2010 Asian network for scientific information.

[2] Sanjeev Manchanda, Mayank Dave, S. B. Singh, –Customized and secure image steganography through random numbers logic.‖ Signal Processing: an International Journal, Volume 1: issue (1).

[3] Mohammad Tanvir Parvez, Adnan Abdul-Aziz Gutub, –RGB intensity based variable bits image steganography‖ 2008 IEEE Asia-Pacific Services Computing Conference.

[4] Rengarajan Amirtharajan, Jiaohua Qin, John Bosco Balaguru Rayappan. Information Technology Journal 11(5): 566-576, 2012, ISSN 1812-5638, 2012 Asian Network for Scientific Information.

Dr. Samidha Dwivedi Sharma is currently working as a Head of the Department of Information Technology, NRI Group of Institutions, Bhopal, M.P., INDIA. She has of more than 15 Years teaching experience in different esteemed university. She Worked as a Chairperson (HOD) of Information System with King Abdulaziz University (Female Section), Rabigh, Saudi Arabia from 2010 to 2011. *She has* been *teaching* for *15 years*.She completed her bachelor’s degree in Science (B.Sc.) with Mathematics subject in 1992 from Dr. H. S. Gour Central University (formerly, Sagar University) Sagar, M P, India. She received her Master degree in Computer Application in the year 1997 from Barkatullah University, Bhopal, India. She has obtained Ph. D. Degree in Computer Science and Application from Dr. H. S. Gour Central University (formerly, Sagar University) Sagar, M P, India. Her fields of interests are Database Management Systems, Mobile database, Data Structure and mobile computing. She has published 5 national and international research papers. She is a life member of ISTE.

Dipesh Agrawal was born on January 6, 1983 in Nasik, Maharashtra, India. He has received the B.E degree in Computer Engineering from Amrutvahini College of Engineering, Pune University, Pune, Maharashtra, India, in Sept 2007. He is currently pursuing his M.Tech. degree in Information Technology from NRI Institute of Science and Technology, RGTU University, Bhopal, Madhya Pradesh, India. His areas of interest include Image Processing, Steganography and Information Security.