5th SASTech
Iran |Mashhad
May 12 - 17 | 2011
5th Symposium on Advances in Science & Technology

A new steganography method based on HIOP(Higher Intensity Of Pixel) and SAOP (Save Address Of Pixel) algorithm

Sara Khosravi[1] , Mashallah abbasi Dezfoli[2] , Mohammad Hossein Yektaie[3], Moien Khosravi[4]

[1] Islamic Azad University Harsin Branch,Harsin, Iran
sara_khosravi_1362@yahool.com

[2]Department of Computer Engineering, Science and Research Branch, Islamic Azad University,Khouzestan-Iran
Abbasi_masha@yahoo.com

[3]Faculty Member Of Islamic Azad University Of Abadan, Abadan, Iran
Mh.yektaie@gmail

[4] Student Of Islamic Azad University Kermanshah Branch, Kermanshah, Iran
m_khosravi_0101@yahoo.com

Paper Reference Number: 0105-718
Name of the Presenter: Sara khosravi

Abstract

As the communication increases day by day the value for security over network also increases. There are many ways to hide and transmission information secretly. In this sense steganography is the best way of sending information secretly. Steganography is the process of hiding one file inside another.

The technology has certainly been the topic of widespread discussion among the IT community. This is the art of writing message or information in such a way that no one apart suitable recipient knows the meaning of the message or information.

For hiding secret information in images, there exists a large variety of steganographic techniques some are more complex than others and all of them have respective strong and weak points.

Steganography, like watermarking and fingerprinting is a branch of science to hide of information but, unlike watermarking and fingerprinting, whit steganogaraphy undetectable presence of a hidden text.

In this paper we are presenting the technique which works by changing a few selected pixel color value. We select pixels with the HIOP (Higher Intensity Of Pixel) algorithm. We divide the image into N blocks and determine higher intensity color of pixel in each block and use SAOP (Save Address Of Pixel) algorithm to retrieve message. We create more dispersion in a selected pixels. As a result, the security level increased in hide of data and also in discover of cipher text. It is also try not to degrade image quality and image size.

Key words: Steganography, pixel, HIOP, SAOP

1. Introduction

The rapid growth of computer networks allowed large files, such as digital images, to be easily transmitted over the internet. Data encryption is widely used to ensure security however, most of the available encryption algorithms are used for text data. Due to large data size and real time constrains, algorithms that are good for textual data may not be suitable for multimedia data .

The word steganography is derived from the Greek words "stegos" meaning "cover" and "grafia" meaning "writing" [1] defining it as "covered writing".

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 emails [2].

Steganography differs from cryptography in the sense that where cryptography focuses on keeping the contents of a message secret, steganography focuses on keeping the existence of a message secret [16]. Steganography and cryptography are both ways to protect information from unwanted parties but neither technology alone is perfect and can be compromised. Once the presence of hidden information is revealed or even suspected, the purpose of steganography is partly defeated [13]. The strength of steganography can thus be amplified by combining it with cryptography. Two other technologies that are closely related to steganography are watermarking and fingerprinting [12]. These technologies are mainly concerned with the protection of intellectual property, thus the algorithms have different requirements than steganography. These requirements of a good steganographic algorithm will be discussed below. In watermarking all of the instances of an object are "marked" in the same way. The kind of information hidden in objects when using watermarking is usually a signature to signify origin or ownership for the purpose of copyright protection [17]. With fingerprinting on the other hand, different, unique marks are embedded in distinct copies of the carrier object that are supplied to different customers. This enables the intellectual property owner to identify customers who break their licensing agreement by supplying the property to third parties [11]

In watermarking and fingerprinting the fact that information is hidden inside the files may be public knowledge –sometimes it may even be visible – while in steganography the imperceptibility of the information is crucial [16].

This paper will focus on hiding information in images in the next sections.

There are lots of techniques available that implement steganography on a variety of different electronic mediums. Images that are used for inserting and hiding secure data are called 'cover image' and the image where secret bits are inserted is called 'stego image'. There are many different Steganographic algorithms. Some of them are in spatial domain and others are in transform domain. LSB (Least Significant Bit) replacement steganography is a popular and simple technique that can hide message bits in LSB planes of image pixels. LSB based methods can be divided into tow main groups: LSB replacement, which simply replaces LSB bits of cover image with secret bits, and LSB matching where pixels are randomly incremented or decremented. In contrary; Steganalysis methods attempt to detect Stego-image and extract it. Inserting secret bits in image changes some statistics of image; this opens some roads to detect Stego-image. So the changes made by Steganographic are a key performance metric; lower change: more robust

algorithm. It is evident that the changes in cover image are related to the volume of inserted bit, so Stego-images with higher insertion rate are detected more easily.

Steganalysis methods generally are divided in two main groups: active and passive methods. In passive methods only presence or absence of hidden data is considered, while in active methods a version of inserted data is extracted, too. Furthermore, different steganalysis methods, depending on steganography algorithms they target, can be classified in two groups: Model-based (Specific) andUniversal Steganalysis .

The goal of model-based methods is attacking to Specific-Steganographic algorithm but in Universal methods attack is performed not considering any prior assumption on Steganographic algorithm and so can be used for several Steganographic algorithms [4]. Universal methods usually are preferred because of their versatility but, their performances are inferior to specific steganalysis [5],[3].

Universal methods that targets different Steganographic algorithms, usually contain two main steps: feature extraction and classification. Firstly, in extraction phase analyzer must find features that have been changed significantly as a result of hiding process and can suitably used as separating characteristics for inserted and non-inserted images. In classification phase, classifier that can be a neural network, Support Vector Machine (SVM), a similarity measure and etc, must be trained on feature vectors from both inserted and non-inserted images, which were extracted in the first step. Universal methods usually use features that are sensitive to wide variety of embedding algorithms [6]. Otherwise, they must extract features for every specific insertion algorithm separately [7][8].

The data can hide with in the image by changing the image content i.e. by changing the color of the pixels. By this technique we can hide a large volume of data inside the image. Once implemented, it is not necessarily perceptible to a human eye that the image has been changed, but to a computer simple statistical analysis can pinpoint a changed image from original one. It is so easy for a computer to notice these changes are.

2. Data and Material

The image is combination of pixels. Each pixel shows a color and specified whit a number. Thus the computer an image is a collection of numbers that constitute different light intensities in different areas of the image. This numeric representation forms a grid and the individual points are referred to as pixels [10][9].

Each pixel set of multi-bit. The number of bits in a color scheme, called the bit depth, refers to the number of bits used for each pixel. The smallest bit depth in current color schemes is 8, meaning that there are 8 bits used to describe the color of each pixel. Monochrome and grey scale images use 8 bits for each pixel and are able to display 256 different colors or shades of grey. Digital color images are typically stored in 24-bit files and use the RGB color model, also known as true color [11].

All color variations for the pixels of a 24-bit image are derived from three primary colors: red, green and blue. Three colors in each pixel create the 24 bit binary number, 8 bit of it belong to red color, 8 bit belong to blue color, 8 bit belong to green color.

Thus in one given pixel, there can be 256 different quantities of red, green and blue, adding up to more than 16-million combinations, resulting in more than 16-million colors [14]. Not surprisingly the larger amount of colors that can be displayed, the larger the file size [15]. in image steganography it works by changing a few pixel color value.

3.Research Methodology And Results

is converted into the bytes that are each character in message is converted into its ASCII equivalent.

Moreover if message is password protected, then while retrieving message, the retriever has to enter the correct password for viewing the message. For an example if we are taking the character "a" in the message then "a=" 01100001 is stored in byte array. Because ASCII value for "a" is 97 and binary equivalent is 01100001.

At 8 bit of the color number, if we change 2 least significant bit, our sighted system can detect changes in pixel. In this case, leas significant bits have 4 state, which is shown in Table 1.

Table 1

11	10	01	00

If we want to store information in 2 bit, at the worst situation, 2 bit are changed, for example if the red color number is a 10111011 pixel, and we want to store the information in 2 least significant bit, at the worst situation the red color number is change to 10111000, examinations shows that HVS can not distinguish this alteration. So we save our information into least significant bits of color.

Hiding image involves embedding the message in to the digital image. Each pixel typically has three numbers associated with it, one each for red, green, and blue intensities, and these value often range from 0-255. In order to hide the message, And data is first converted into byte format and stored in a byte array. the message is then encrypted and then embeds each bit into the LSB position of each pixel position. It uses the first pixel to hide the length of message (number of character).Suppose, we only change the last two that determine the "one place", and the "two place". We can only alter the original pixel color value by 3degre.

We use four bytes in two pixel to store 8 bits character.
The first color in first pixel : r7 r6 r5 r4 r3 r2 r1 r0
The second color in first pixel :g7 g6 g5 g4 g3 g2 g3g2
The third color in first pixel: b7 b6 b5 b4 b3 b2 b5b4
The first color in second pixel: r7 r6 r5 r4 r3 r2 r7 r6
My character have (c7 c6 c5 c4 c3 c2 c1 c0) bits. Then we can place two of these character bits in the lowest red pixel, tow more in the lowest green pixel, the two in the lowest blue pixel and the two in the lowest red other pixel as follows.

The first color in first pixel: r7 r6 r5 r4 r3 r2 c1 c0
The second color in first pixel:g7 g6 g5 g4 g3 g2 c3c2
The third color in first pixel: b7 b6 b5 b4 b3 b2 c5c4
The first color in second pixel: r7 r6 r5 r4 r3 r2 c7c6

If we take an example of pixel (255, 64, 64) with character "a", then we can obtain:

Originl pixel=(11111111,01000000,0100000)
"a" = 01100001
New pixel = (11111101, 01000000,0100000)

New pixel =(253,64,64)

Here we can notice that the new pixel of (253,64,64) is almost the same value as the old pixel of (255, 64, 64). So there will not be noticeable color difference in the image.

The suggested technique in this paper is HIOP (Higher Intensity Of Pixel) algorithm. This algorithm measures the intensity of the pixel and then hide data in **random** pixel selection with a goal to hide maximum data in each pixel without creating extra unnatural noise.

for perform this operation and find pixels whit higher intensity we obtains average color number elements in this image . The number is a boundary to determine the elements whit higher intensity, elements are greater average number are more color intensity. Thus the higher intensity of pixels in the image are selected and create scatter in selected pixels. elements selected are higher intensity pixels and have more scatter.In order to perform this algorithm the career picture Is shown "Fig. 3" and in "Fig. 4", pixels whit higher intensity are greater average number are marked with black color.

.

Fig. 4: the career picture

Fig. 5: pixels whit higher intensity

The total number of pixels in figure 5 is 215232. That number of pixels marked is 58468. To determine pixel whit more intensity, we can add factor k to average number, whatever K is more the selected pixels are less. K Can be used as key and increase security. For example in figure 5 if k=50 that number of pixels marked is 23405.For more efficient and find pixel of image that have a certain complexity, we divide image to block n*n. pixels with Higher intensity are compared than their neighboring areas and we do operations to find the pixel with higher intensity on each block. To perform this operation, and to find higher intensity pixel, we put n^2 color data element of block n *n in matrix. The average color of this block obtains. The number is a boundary to determine the elements whit higher intensity in this block . The elements that have greater average have more color intensity in this block. in "Fig. 5",selected pixels whit HIOP algorithm in total image marked with black color and in "Fig. 5",selected pixels whit HIOP algorithm in each block marked with black color.

Fig.5: HIOP in total image

Fig.5: HIOP in each block

Therefore, more scattered pixels selected and increased security.For example in figure 5, specified results whit different n in table2 is shown.

Table 2: specified results whit different n

n	Total Blocks	Total pixel selected
8	3363	45286
50	90	57573
100	25	66477

.

so, we use this algorithm for embedding the massage text.

1) First, we chose the image and massage text, that we should use them on the picture
2) We covert massage text to binary code.
3) Image divided into n blocks
4) We determine pixel with Higher intensity in each block
5) We estimate the least significant bits in pixel marked.
6) Embed the text into the LSB

Once a message has been retrieved it has to be converted in to the original message. This process can be done by reading the embedded data from the file. The read data will be in bytes format. This can be done by extract the selected pixels of output image in one array. Decoding in same manner as the reversal of encoding process i.e. first pixel value gives number of character in the message. After every pixel gives the message character's ASCII value, which then stored in byte array.

To presente the stored information in the image, we use this algorithm.

1) First, we chose the image, that the text embedded into it.
2) We retrieve the LSB.
3) We combine 8 bit and convert them into one character

Retrieve text stored in the image is done in two main stages.

- ✓ The first step to find pixel that information is stored in them
- ✓ The second phase includes putting together bits and retrieve the text is hidden

In the first step to find the pixel, we must to choose selected pixels.

As in the HIOP algorithm referred, first, we divide the image into blocks (n*n), and then the average color of each block in three dimensions (red, green, blue) obtain and we create two matrices, the elements of each block read row by row and column by column and put in each matrix and using Strassen's matrix multiplication, these two matrices have the multiply, we obtain the average matrix's elements multiplied

Now, we choose elements that is larger than average color of blocks and the average result of matrix multiplication.

We must also consider the character bits from place more value to place less value or contrast.

After considering, how to access pixels, LSB bits and how to save text characters, we start extracting LSB bits and we put them in a buffer and using the bits that are placed in buffer, hidden text obtained.

There are two methods for this

1. A buffer length of 8 bits to create, each 8-bit LSB of pixels selected to become characters and we put together the characters and get the hidden text.
2. A buffer of length count bits hidden text created, we put all bits LSB of pixels selected in buffer. Each 8-bit of buffer to become characters and we put together the characters and get the hidden text.

In general, how to obtain secret information, the processes in how to store text is used, as obtaining the mean color, consists of two matrices, beat them, taking the mean of the matrix multiplication and pixel selection is repeated and addition to these steps, bits obtained during the process are converted to text. This is causing repeated processes and is reduced speed.

One way to avoid repeating process and increasing the speed of storage, we save address of selected pixel to save. Each pixel is used for storing images is three characteristics:

1. What color of the pixels are selected for storage
2. Pixel columns
3. Pixel row

In this case, we must put address of selected pixels in specific location in the image. Usually, changes in the initial row are not cause attention, therefore, the initial row pixels to save the pixel address have selected. In each pixel we have three different colors, so to specify the type of color we need two bits. Each pixel is 24 bits, as shown in figure 3-25, two bits to determine the pixel color, 11 bits to determine column of selected pixel and 11 bits to determine row of selected pixel. How to save the address in pixel is showmen in figure 12.

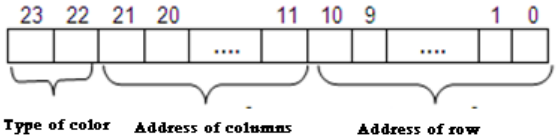

Figure 12-25:How to save the address in pixel

Since we need 4 bytes for each character, so to save the text whit length N characters, we reserve N*4 initial pixel to save address of selected pixel and we do block scheme from the last row of the data of address is located and each pixel is selected, we save its data in pixels reservation.

In this case, when you get the hide text in the image, according to the pixel address, easily, we obtain hide text in image.

5. Conclusions

As the result we can find the out come of the paper is to create across platform that can effectively hide a message inside a digital image file. As there are many application of image steganography like it allows for two parties to communicate secretly and covertly.

One of the other main uses for image steganography is for the transportation of high level or top secret documents between international governments also it allows for copyright protection on digital files using the message as a digital watermark. Image steganography has many legitimate uses as it can be used by hackers to send viruses and Trojans to compromise machines. So in conclusion, as more emphasis is placed on the areas of copyright protection, privacy protection, and surveillance, we believe that steganography will continue to grow in importance as a protection mechanism.

This paper has investigated whether taking the image as the cover into account increases the security of the message by creating cross platform self evaluating tool. Also describe the benefits from the approach like the security of message increases and distortion rate has reduced.

Acknowledgements

The authors would like to thank the guide and the Computer Science and Engineering Department of National Institute Of Technical Teachers Training And Research, Kolkata (NITTTR,Kolkata) for supporting this work.

Refrence

[1] Moerland, T., "Steganography and Steganalysis", Leiden Institute of Advanced Computing Science,www.liacs.nl/home/ tmoerl/privtech.pdf

[2] Image Steganography by Mapping Pixels to Letters, Mohammed A.F. Al-Husainy Department of Computer Science, Faculty of Sciences and IT, Al-Zaytoonah University of Jordan ,2009

[3] Wolfgang, R.B. and E.J. Delp, 1996. Watermark for digital images. Proceeding of the IEEE International Conference on Image Processing,Sep. 16-19, IEEE Computer Society, Washington DC., USA., pp: 219-222. DOI

[4]. Chen, B. and G.W. Wornell, 2001. Quantization index modulation: A class of provably good methods for digital watermarking and information embedding.IEEE Trans. Inform. Theor., 47: 1423-1443. DOI:10.1109/18.923725

[5]. -Steganography-Survey on File Systems, Uma Devi.G ,MS by Research CSE I I I T Hyderabad , 2006

//[6] Dunbar, B., "Steganographic techniques and their use in an Open-Systems environment", SANSInstitute, January 2002

//[7]Jamil, T., "Steganography: The art of hiding information is plain sight", IEEE Potentials, 18:01, 1999

//[8] Chandramouli, R., Kharrazi, M. & Memon, N., "Image steganography and steganalysis: Concepts and Practice", Proceedings of the 2nd International Workshop on Digital Watermarking, October 2003

//[9] Currie, D.L. & Irvine, C.E., "Surmounting the effects of lossy compression on Steganography", 19th National Information Systems Security Conference, 1996

//[10] Anderson, R.J. & Petitcolas, F.A.P., "On the limits of steganography", IEEE Journal of selected Areas in Communications, May 1998

[11] Artz, D., "Digital Steganography: Hiding Data within Data", IEEE Internet Computing Journal, June 2001

[12] Ahsan, K. & Kundur, D., "Practical Data hiding in TCP/IP", Proceedings of the Workshop on Multimedia Security at ACM Multimedia, 2002

//[13] Handel, T. & Sandford, M., "Hiding data in the OSI network model", Proceedings of the 1st International Workshop on Information Hiding, June 199

[14] Wang, H & Wang, S, "Cyber warfare: Steganography vs. Steganalysis", Communications of the ACM,47:10, October 2004

[15] Marvel, L.M., Boncelet Jr., C.G. & Retter, C., "Spread Spectrum Steganography", IEEE Transactions on image processing, 8:08, 1999

[16]Johnson, N.F. & Jajodia, S., "Exploring Steganography: Seeing the Unseen", Computer Journal,February 1998

[17] Owens, M., "A discussion of covert channels and steganography", SANS Institute, 2002