Volume 2, No. 1, January 2011

Journal of Global Research in Computer Science

ISSN-2229-371X

RESEARCH PAPER

Available Online at www.jgrcs.info

A NEW STEGANOGRAPHY METHOD BASED ON HIOP (HIGHER INTENSITY OF PIXEL) ALGORITHM AND STRASSEN'S MATRIX MULTIPLICATION

Khosravi Sara [1] , Abbasi Dezfoli Mashallah [2] , Yektaie Mohammad Hossein [3]

[1]Department of Computer Engineering, Science and Research Branch, Islamic Azad University, Khouzestan-Iran
sara_khosravi_1362@yahool.com
[2]Department of Computer Engineering, Science and Research Branch, Islamic Azad University, Khouzestan-Iran

m.abbasi@khouzestan.srbau.ac.ir
[3]Faculty Member Of Islamic Azad University Of Abadan, Abadan, Iran
Mh.yektaie@gmail.com

Abstract: As the communication increases day by day the value for security over network also increases. There are many ways to hide information or transmission of information secretly . In this sense steganography is the best part of sending information secretly. Steganography in the last few years has gained a wider audience. 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 exist a large variety of steganography techniques some are more complex than others and all of them have respective strong and weak points. The out come of this paper is to generate a cross platform that can effectively hide a message inside a digital image file. 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 astrassen multiplication in each block . 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 as far as possible does not change the image size.

Key words: Steganography, LSB, digital image, pixel, HIOP, color intensity, image quality, image size

.

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].

There has been a rapid growth of interest in this subject over the last ten years and for two main reasons[3].

1. The publishing and broadcasting industries have become interested in techniques for hiding encrypted, copyright marks and serial numbers in digital films audio recordings, books and multimedia products; an appreciation of new market opportunities created by digital distribution is coupled with a fear that digital works could be too easy to copy.
2. Moves by various governments to restrict the availability of encryption services have motivated people to study methods by which private messages can be embedded in seemingly innocuous cover messages. The ease with which this can be done may be an argument against imposing restrictions.

Capacity, security and robustness, are the three main aspects affecting steganography and its usefulness [4].

- Capacity refers to the amount of data bits that can be hidden in the cover medium.
- Security relates to the ability of an eavesdropper to figure the hidden information easily.
- Robustness is concerned about the resist possibility of modifying or destroying the unseen data.

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.

Stegananalysis 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],[6].

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 [4]. Otherwise, they must extract features for every specific insertion algorithm separately [5].

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.

HISTORICAL INSTANCES OF STEGANOGRAPHY

1- In 440 BC, Herodotus mentions two examples of Steganography in The Histories of Herodotus. Demeratus sent a warning about a forthcoming attack to Greece by writing it on a wooden panel and covering it in wax. And other of Histiaeus, who shaved the head of his most trusted slave and tattooed a message on it. After his hair had grown the message was hidden [7].

2- During World War II, invisible inks were used to conceal information in seemingly standard, innocuous memos or letters. Common sources for invisible inks are milk, vinegar, fruit juices and urine. Each one of these substances darkens when heated and was especially effective during this time due to the fact that the sources were always readily available [8]

3- In the Second World War the Microdot technique was developed by the Germans. Information, especially photographs, was reduced in size, extremely difficult to detect [9].

4- Although steganography is an ancient subject, the modern formulation of it is often given in terms of the prisoner's problem proposed by Simmons [10], where two inmates wish to communicate in secret to hatch an escape plan. All of their communication passes through a warden who will throw them in solitary confinement should she suspect any covert communication [11].

The warden, who is free to examine all communication exchanged between the inmates, can either be passive or active. A passive warden simply examines the communication to try and determine if it potentially contains secret information. If she suspects a communication to contain hidden information, a passive warden takes note of the detected covert communication, reports this to some outside party and lets the message through without blocking it. An active warden, on the other hand, will try to alter the communication with the suspected hidden information deliberately, in order to remove the information [13].

DIFFERENT KINDS OF STEGANOGRAPHY

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

The.Figure 1 shows the four main categories of file formats that can be used for steganography.

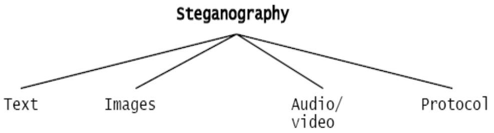

Figure 1:category of steganography

Hiding information in text is historically the most important method of steganography. An obvious method was to hide a secret message in every nth letter of every word of a text message. It is only since the beginning of the Internet and all the different digital file formats that is has decreased in importance [12].

Given the proliferation of digital images, especially on the Internet, and given the large amount of redundant bits present in the digital representation of an image, images are the most popular cover objects for steganography.

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

To hide information in audio files similar techniques are used as for image files. One different technique unique to audio steganography is masking, which exploits the properties of the human ear to hide information unnoticeably. A faint, but audible, sound becomes inaudible in the presence of another louder audible sound [12]. This property creates a channel in which to hide information. Although nearly equal to images in steganographic potential, the larger size of meaningful audio files makes them less popular to use than images [1].

The term protocol steganography refers to the technique of embedding information within messages and network control protocols used in network transmission [13]. In the layers of the OSI network model there exist covert channels where steganography can be used [14]. An example of where information can be hidden is in the header of a TCP/IP packet in some fields that are either optional or are never used. A paper by Ahsan and Kundur provides more information on this [15]

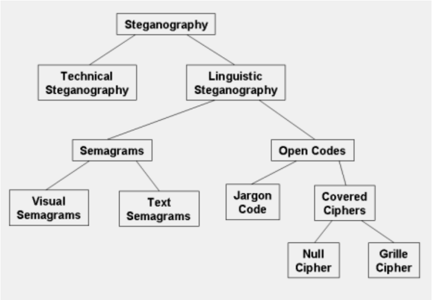

Figure 2. Classification of steganography techniques

Figure 2 shows a common taxonomy of steganographic techniques:

• Technical steganography uses scientific methods to hide a message, such as the use of invisible ink or microdots and other size reduction methods.

• Linguistic steganography hides the message within the carrier in some non-obvious ways and is further categorized as semagrams or open codes.

• Semagrams hide information by the use symbols or signs. A visual semagram uses innocent-looking or everyday physical objects to convey a message, such as doodles or the positioning of items on a desk (or Web site)

. A text semagram hides a message by modifying the appearance of the carrier text, such as subtle changes in font size or type, adding extra spaces, or different flourishes in letters or handwritten text.

• Open codes hide a message within a legitimate carrier message in ways that are not obvious to an unsuspecting observer. The carrier message is sometimes called the overt communication while the hidden message is the covert communication. This category is subdivided into jargon codes and covered ciphers.

• Jargon code, as the name suggests, uses language that is understood by a group of people

but is meaningless to others. Jargon codes include warchalking (symbols used to indicate the presence and type of wireless network signal underground terminology, or an innocent conversation that conveys special meaning because of facts known only to the speakers. A subset of jargon codes are cue codes, where certain pre-arranged phrases convey meaning.

• Covered, or concealment, ciphers hide a message openly in the carrier medium so that it can be recovered by anyone who knows the secret for how it was concealed. A grillecipher employs a template that is used to cover the carrier message; the words that appear in the openings of the template are the hidden message. A null cipher hides the message according to some prearranged set of rules, such as "read every fifth word" or "look at the third character in every word."

DIFFERENCE OF STEGANOGRAPHY WITH OTHER TECHNOLOGIES

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 [16]. 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 [12]

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].

CURRENT WORK

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 [18].

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 [19].

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 [19].

Not surprisingly the larger amount of colors that can be displayed, the larger the file size [20]. in image steganography it works by changing a few pixel color value.

CONVERT TEXT TO BYTE

Data 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.

MESSAGE EMBEDDING IN DIGITAL IMAGE

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.

Algorithm to find the pixel

We suggeste new algoritm in this paper. This algorithm measures the intensity of the pixel and then hide data in 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 figure 3.

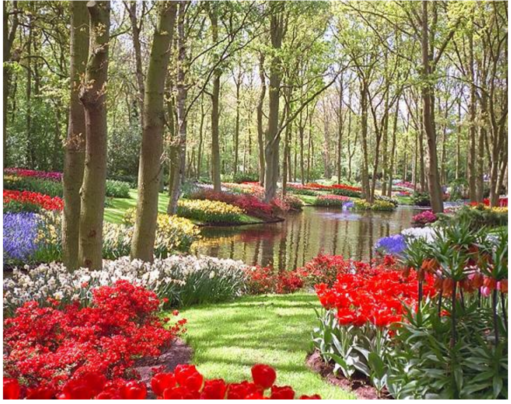

Figure 3

In figure 4, pixels whit higher intensity are greater average_ number are marked with black color.

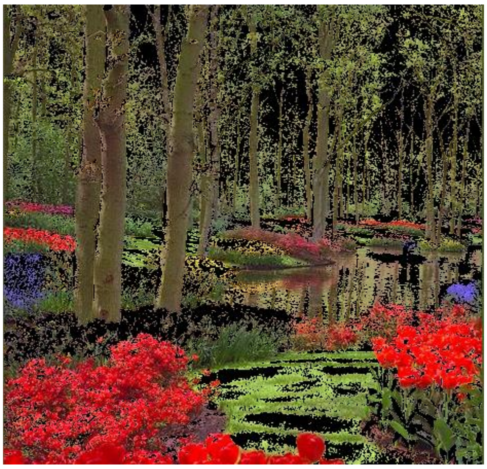

Figure 4

The total number of pixels in figure 5 is 215232. That number of pixels marked is 58468. To determine pixel whit more Intensity, we con add factor k to average number, whatever K is more the selected pixeld are less.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 bolck n*n. pixels with Higher intensity are compared than thier 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 To implement a security level, we want to creat more scattere in selected pixels. Untill understaning the implemented algorithm would be more difficult and the discovering of information may not be possible without the algorithm. Therefore, we use matrix multiplication.acording to Figure 5 data elements in each block are read in form of row and column and put them in two matrices.

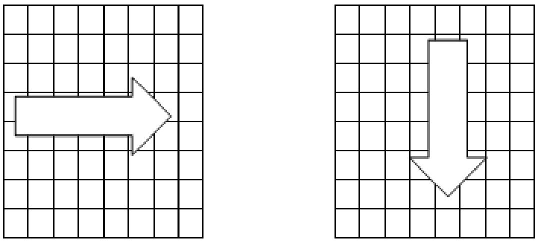

Figure 5

Then these two matrices are multiplied togetherFor this task we use astrassen multiply algorithm with complexity $O(n^{2.81})$.

We examine this method to store the text " save the text in the image" in figure 6. If 8 = N,we check the information which are stored in the first block whit this method. If the Astrassen beat is implement in this block And we compute the average color and obtained average by strasen multiplying , 10 pixels are selected toata store the data. We doing this algorithm for green and blue color in block. 11 percent of colors in block are changed.

Figure 6

Changes in red pixels number selected is shown in Figure 7.

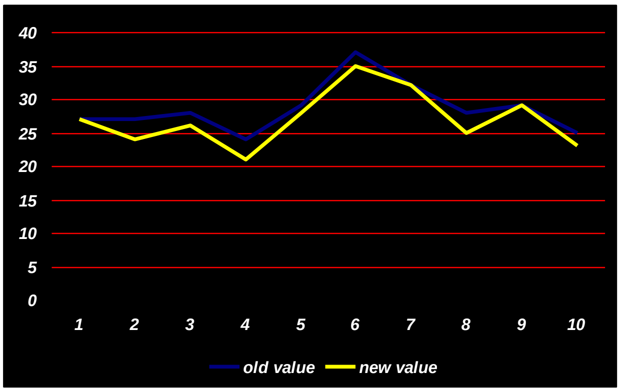

Figure 7

Changes in the amount of green pixels selected is shown in Figure 8.

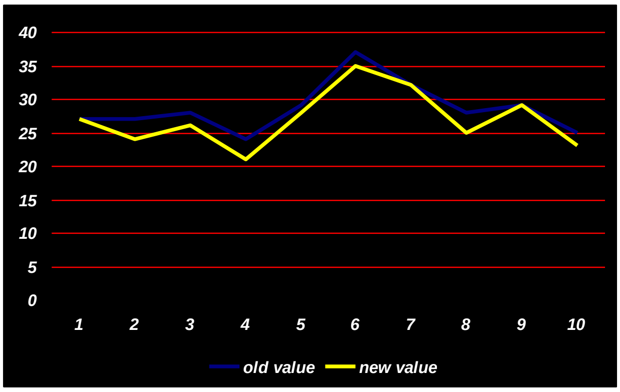

Figure 8

Changes in the amount of blue pixels selectedis shown in Figure 9.

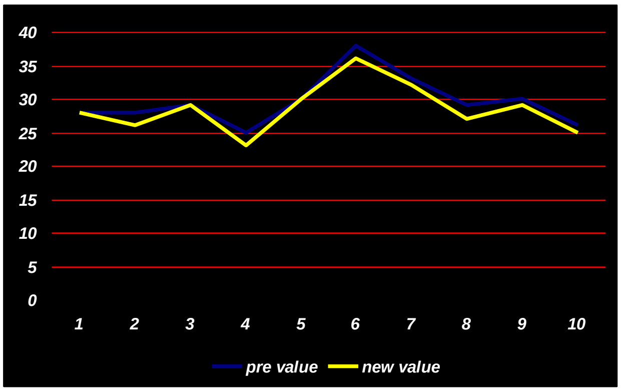

Figure 9

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) data elements in each block are read in form of row and column and put them in two matrices. two matrix multiply whit astrassen Multiplying and determinde the average matrix. elements are greater average, are selected.
6) Common elements in Paragraph 4 and 5 are selected.
7) we estimate the least significant bits in marked pixels.
8) embed the text into the LSB.

MESSAGE EXTRACTION

In this section we will discuss the retrieving the message from the image independent of the file format. 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 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 leas SB.
3)we combine 8 bit and convert them into one character.

DECREASING RATE OF CHANGE

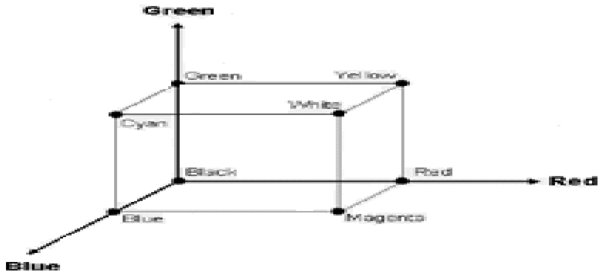

Figure10: 3D cube structure of a pixel

Let's think about a color pixel of a 24 bit BMP image represented in figure10 Each axis of the cube contain a color schema which represented in binary is like 10101000,11010101,01010110 where first 8 bit represent R (Red) second 8 bit represent G (Green) and third 8 bit represent B (Blue).

Images are the most popular cover objects for steganography.As it involves the conversion of message into the digital image. In order to hide the message, it is first converted into byte format and then stored in byte array. Then the message is encrypted and then embeds each bit into the LSB position of each pixel position. Proposed approach involves change in LSB of each pixel byte i.e. RGB instead of only in green byte. Hence reduces the distortion rate that is look of original image First the informationi stored in byte of green color If needed, other colors to be used later. So selected pixels are scattered and security image is higher.

Techniques LSB use in bmp image So that the use of a bit LSB in each color to hide information Reduce the amount of change and Noise, but Amount of data stored in the image is less.

CONCLUSION

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 highlevel or topsecret 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 crossplatform self evaluating tool. A also describe the benefits from the approach like the security of message increases and distortion rate has reduced.

REFERENCES

[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] Mehdi Kharrazi, Husrev T. Sencar, Nasir Memon," Performance study of common image steganography and steganalysis techniques". Journal of Electronic Imaging 15(4), 041104(Oct–Dec 2006)

[5] Harmsen, J.J., Pearlman, W.A; "Steganalysis of additive noise modelable information hiding".Rensselaer Polytechnic Institute, Troy, New York, May 2003.

[6] Mehmet U.Celik, Gaurav Sharma, A.Murat Tekalp,"Universal Image Steganalysis Using Rate-Distortion Curves", Proc.SPIE: Security, Steganography, and watermarking of Multimedia Contents VI,vol.5306,Sane Jose, 19-22,Jan 2004.

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

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

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

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

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

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

[13] Artz, D., “Digital Steganography: Hiding Data within Data”, IEEE Internet Computing Journal, June 2001

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

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

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

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

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

[19] Owens, M., “A discussion of covert channels and steganography”, SANS Institute, 2002

[20] “Reference guide: Graphics Technical Options and Decisions”,