International Journal of Information, Control and Computer Sciences
ISSN: 2517-9942
Vol:1, No:6, 2007

Labeling Method in Steganography

H. Motameni, M. Norouzi, M. Jahandar, and A. Hatami

***Abstract*—**In this paper a way of hiding text message (Steganography) in the gray image has been presented. In this method tried to find binary value of each character of text message and then in the next stage, tried to find dark places of gray image (black) by converting the original image to binary image for labeling each object of image by considering on 8 connectivity. Then these images have been converted to RGB image in order to find dark places. Because in this way each sequence of gray color turns into RGB color and dark level of grey image is found by this way if the Gary image is very light the histogram must be changed manually to find just dark places. In the final stage each 8 pixels of dark places has been considered as a byte and binary value of each character has been put in low bit of each byte that was created manually by dark places pixels for increasing security of the main way of steganography (LSB).

***Keywords*—**Binary image, labeling, low bit, neighborhood, RGB image, steganography, threshold.

I. Introduction

AT the glance to establishing the hiding text, image or etc, Æneas the Tactician can be referred, and other classical writers, concentrated on methods for hiding messages rather than for enciphering them [1]; and although modern cryptographic techniques started to develop during the Renaissance, in 1641 that John Wilkins still preferred hiding over ciphering [2] because it arouses less suspicion.

In hiding process the following concept may be observed:

Cover-object: refers to the object used as the carrier to embed messages into. Many different objects have been employed to embed messages into for example images, audio, and video as well as file structures, and html pages to name a few.

Stego-object: refers to the object, which is carrying a hidden message. So given a cover object, and a message the goal of the steganographer is to produce a stego object which would carry the message.

The studying of communications security includes not just encryption but also traffic security, whose essence lies in hiding information. This discipline includes such technologies as spread spectrum radio, which is widely used in tactical military systems to prevent transmitters being located; temporary mobile subscriber identifiers, used in digital phones to provide users with some measure of location privacy; and anonymous remailers, which conceal the identity of the sender of an email message [3].

Two techniques are available to those wishing to transmit secrets using unprotected communications media. One is cryptography, where the secret is scrambled and can be reconstituted only by the holder of a key. When cryptography is used, the fact that the secret was transmitted is observable by anyone. The second method is steganography[1]. Here the secret is encoded in another message in a manner such that, to the casual observer, it is unseen. Thus, the fact that the secret is being transmitted is also a secret. An important sub discipline of information hiding is steganography.

Whereas cryptography is about protecting the content of messages, steganography is about concealing their very existence. It comes from Greek roots, literally means, "covered writing" [4], and is usually interpreted to mean hiding information in other information.

There are a number of other applications driving interest in the subject of information hiding (Fig. 1).

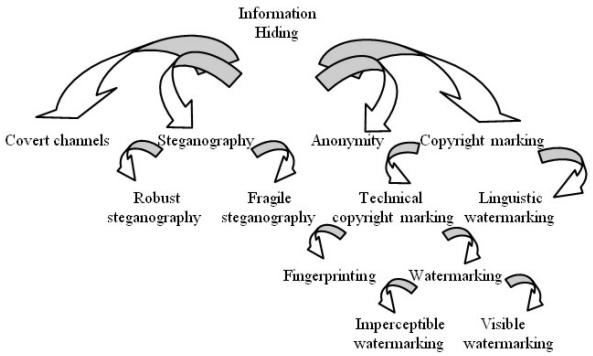


Fig. 1 A classification of information hiding techniques based on [5]

- Military and intelligence agencies require unobtrusive communications. Even if the content is encrypted, the detection of a signal on a modern battlefield may lead rapidly to an attack on the signaler. For this reason, military communications use techniques such as spread spectrum modulation or meteor scatter transmission to make signals hard

Manuscript received March 2007.

H. Motameni is with the Department of Computer Islamic Azad university, sari Branch, Iran (corresponding author to provide phone: +98-911-114-0554; e-mail: motameni@iausari.ac.ir).

M. Norouzi is now in the university of Olom fonon, babol, mazandaran, Iran (e-mail: marzy_a27@yahoo.com).

M. Jahandar is now finished his studing in the university of Olom fonon, babol, mazandaran, Iran (e-mail: tunder_daryakenar@yahoo.com).

A. Hatami is with the Department of Computer, University of Olom fonon, babol, mazandaran, Iran (e-mail: bird_artus@yahoo.com).

[1] The term steganography derives from a method of hidden writing discussed by Trimetheus in his three-volume Steganographia [6].

for the enemy to detect or jam.

- Criminals also place great value on unobtrusive communications. Their preferred technologies include prepaid mobile phones, mobile phones that have been modified to change their identity frequently, and hacked corporate switchboards through which calls can be rerouted.
- Law enforcement and counter intelligence agencies are interested in understanding these technologies and their weaknesses, so as to detect and trace hidden messages.
- Recent attempts by some governments to limit online free speech and the civilian use of cryptography have spurred people concerned about liberties to develop techniques for anonymous communications on the net, including anonymous remailers and Web proxies.
- Schemes for digital elections and digital cash make use of anonymous communication techniques.
- Marketers use email forgery techniques to send out huge numbers of unsolicited messages while avoiding responses from angry users.

II. What is Steganography?

Steganography techniques can be used to hide data within digital images with little or no visible change in the perceived appearance of the image. An important step in developing a theory of steganography is to clarify the definitions. Intuitively, the purpose of steganography is to set up a secret communication path between two parties such that any person in the middle cannot detect its existence; the attacker should not gain any information about the embedded data by simply looking at cover-text or stego-text. Simmons first formalized this in 1983 as the prisoner's problem [7]. Alice and Bob are in jail and wish to prepare an escape plan. The problem is that the warden Willie arbitrates all their communications. If Willie sees any Cipher text in their messages, he will frustrate them by putting them into solitary confinement. So Alice and Bob must find a way to exchange hidden messages. Simmons showed that such a channel exists in certain digital signature schemes: the random message key used in these schemes can be manipulated to contain short messages. This exploitation of existing randomness means that the message cannot even in principle be detected and so Simmons called the technique the 'subliminal channel'. The history of the subliminal channel is described in [8], whereas further results may be found in [9], [10].

In the general case of steganography, where Willie is allowed to modify the information flow between Alice and Bob, he is called an active warden; but if he can only observe it he is called a passive warden. Further studies showed that public key steganography is possible (in this model, Alice and Bob did not exchange secrets before going to jail, but have public keys known to each other) -although the presence of an active warden makes public key steganography more difficult [11].

This difficulty led to the introduction, in [12], of the supraliminal channel, which is a very low bandwidth channel that Willie cannot afford to modify as it uses the most perceptually significant components of the cover object as a means of transmission. For example, a prisoner might write a short story in which the message is encoded in the succession of towns or other locations at which the action takes place. Details of these locations can be very thoroughly woven into the plot, so it becomes in practice impossible for Willie to alter the message -he must either allow the message through or censor it. The effect of this technique is to turn an active warden into a passive one. The same effect may be obtained if the communicating parties are allowed to use a digital signature scheme.

III. Related Work

As follows image steganography algorithm classified into four different parts:

A. LSB

A simple way of steganography is based on modifying the least significant bit layer of images, known as the *LSB technique*. In the LSB technique, the least significant bits of the pixels is replaced by the message which bits are permuted before embedding. In some cases (Fridrich et al. [13]) LSB of pixels visited in random or in certain areas of image and sometimes increment or decrement the pixel value.

B. DCT

DCT (discrete cosines transform) is used in JPEG compression. Embedding in DCT domain is simply done by altering the DCT coefficients, for example by changing the least significant bit of each coefficient [14].One of the limitation in DCT domain happened when 64 coefficients are equal to zero. Values will have an effect on the compression rate. So the number of bit one could embed in DCT domain is less that the number of bits one could embed by the LSB method. Also embedding capacity becomes dependent on the image type used in the case of DCT embedding. . There are different methods for altering the DCT coefficients that reviews of jsteg please refer to [15].

C. Frequency Domain

Another transform domain for embedding is frequency domain. They first decor relate the image by scrambling the pixels randomly, which in effect whitens the frequency domain of the image and increases the number of transform coefficients in the frequency domain thus increasing the embedding capacity [14]. Note the result is a salt and pepper image.

D. Parallel Extract and Parallel Deposit

Many important applications, however, can realize substantial performance benefits from bit-oriented instructions. Propose the parallel extract (pex) and parallel deposit (pdep) instructions to accelerate compressing and

expanding selections of bits. The fast inverse butterfly and butterfly network circuits can implement these instructions. Latency and area costs of alternative functional units have been evaluated for implementing subsets of advanced bit manipulation instructions. [16] By MATLAB's bwpack function [17] benefits from pex. Binary images in MATLAB are typically represented and processed as byte arrays – a byte represents a pixel and has permissible values 0x00 and 0x01. However, certain optimized algorithms are implemented for a bitmap representation, in which a single bit represents a pixel. To produce one 64-bit output word requires 64 extr and 63 dep instructions [16].

In this paper the first method is considered but concentrating on sequence of color by labeling the image have been analyzed and the message on certain color of image is embedded, so it is thought that by this technique the security of LSB method increased.

IV. Labeling Algorithm

Pixel Connectivity

A morphological processing starts at the peaks in the marker image and spreads throughout the rest of the image based on the connectivity of the pixels. Connectivity defines which pixels are connected to other pixels. A group of pixels that connected based on Connectivity types called an Object.

More about Connectivity in an Image

The following chart (Table I) lists all the standard two-dimensional connectivities.

Selecting a Connectivity

The type of neighborhood that may choose affects the number of objects found in an image. For example (Fig. 2), if you specify a 4-connected neighborhood, this binary image contains three objects; if you specify an 8-connected neighborhood, the image has one object.

TABLE I
SUPPORTED CONNECTIVITY

Two−Dimensional Connectivities		
4-connected	Pixels are connected if their edges touch. This means that a pair of adjoining pixels are part of the same object only if they are both on and are connected along the horizontal or vertical direction.	
8-connected	Pixels are connected if their edges or corners touch. This means that if two adjoining pixels are on, they are part of the same object, regardless of whether they are connected along the horizontal, vertical, or diagonal direction. Three-Dimensional Connectivities	

0	0	0	0	0	0	0
0	1	1	1	1	0	0
0	1	1	0	0	0	0
1	0	0	1	1	0	0
0	0	0	1	1	0	0
0	0	0	0	0	0	0

Fig. 2 A binary image

What was mentioned before is the introduction of connectivity for labeling object of an image. The graythresh function uses Otsu's method, which chooses the threshold to minimize the intraclass variance of the black and white pixels.

1) At first threshold of image has been computed in order to uses thresholding to convert this grayscale image to binary. An output as a binary image is needed that has values of 1 (white) for all pixels in the input image with luminance greater than variance and 0 (black) for all other pixels. [18]

2) Now every thing is ready to label the binary Image that is result of previous level. Type of Connectivity has been mentioned before can be used in this stage to label our Image, that here 8-Connectivety has been used .for this purpose the general procedure outlined in reference is used [19]:

a) Run-length encodes the input image.

b) Scan the runs, assigning preliminary labels and recording label equivalences in a local equivalence table.

c) Resolve the equivalence classes.

d) Relabel the runs based on the resolved equivalence classes.

3) Then labeled image has been converted to RGB in order to coloring each Object by different color. It has not been forgotten that the zero label (that is sign of black color) shown by white color in result of this part (Fig. 3(b)).

4) Start at the peaks in the image pixel and spreads throughout the rest of the image. Each pixel of RGB has 3 layer of color (RED-GREEN-BLUE), to distinguish WHITE color of RGB's image that refer to BLACK pixel of the original image the value of each color layer must be equal to 255.

5) Each pixel has eight bits and each eight pixel has been considered as a byte; each block of byte works as bit so low bit of each pixel is chosen for this purpose. In this stage, the characters of text have been converted into binary then break

it to eight bits and each bit has been put in low bit of each eight pixel.

Corresponding to mention method has high security in operability of changes but it has low security in decoding Image and finding secret message, so security have been increased as have been expressed below.

6) In developing security process of decoding, advantage of RGB - labeling of gray Image has been used and it has been matured with stage 5 but just the low bit of labeled pixel has been changed that are dark (Example Fig. 3). It means that a sample mask of our picture has been created and exchanging low bit of that pixel has been started on the source picture and only in the limitation of mask.

7) Reversion algorithms is exactly such as CODING method that has been referred in above steps, with this difference that first low bit of pixel has been read in the limitation after creating mask of the picture.

Note that in some cases if the sequence color is light gray a variance must be chosen manually to finding darker part of image to put data in those points because if this problem has not been considered the effect of putting data in image is observable (Fig. 4).

V. Case Study

In this stage, above steps have been deployed By MATLAB applications because the Toolbox of the image processing of Matlab provides most of function that was needed. With adding this text into source image, no changes have been seen:

This is test, HELLO WORLD!!!
This is test, HELLO WORLD!!!
This is test, HELLO WORLD!!!
…

The result of running of project is shown on cameraman picture. (Fig. 3)

As in Fig. 3 (d) to more apprehending of source Image and export Image, a part of cameraman picture has been provided (Fig. 3(a) and (b)) in the chart with integer value that refers the color of those image.

Refer to Fig. 3(b) the column that must be changed has been highlighted by new value, for example in this picture the number of character can be see, how change the main value of picture. Here the first number of character has been converted to binary format.

"This is test, HELLO WORLD!!!"
T: 84 (ASCII code): 1010100 (Binary)
h: 104 (ASCII code): 1101000 (Binary)
i: 105 (ASCII code): 1101001 (Binary)
…

Refer to this paper it is observed that each bit of byte (show one character) settled in last bit of each pixel sequentially. So values of all pixels haven't been changed yet and the text is stored in the picture with high security.

VI. Conclusion

In this paper a technique of information hiding in steganography in particular has been presented and present a way for labeling different color to identify dark area of image and then hide the text in those places but the data is not put directly in those pixels but they have been put in low bits of each eight pixel.

Our future work's are using the advantage of palette and composition of the gif image that is implemented before and also defining precedence of label object that recognizing as follow:

1) Ordinal (it means that precedence of each sequence of color is chosen manually)
2) Randomize

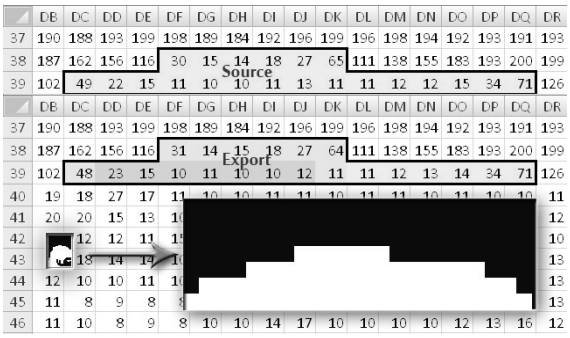
Both ways that has been mentioned are the techniques that used separately in steganography from many years ago but here the way of hiding text have been employed by using of this palette and labeling to become complicated and have wonderful security.

Appendix

(a)

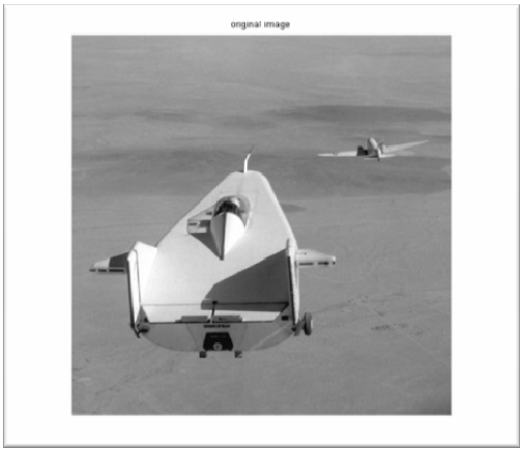
(b)

(c)



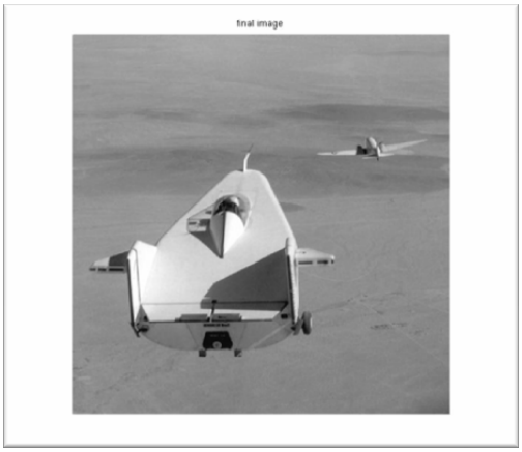
(d)

Fig. 3 (Cameraman) an image with normal histogram (a) original gray image (b) labeled binary image and manipulate histogram and convert to RGB (c) final image with embedded message (d) chart show a part of source picture that change after embedded message



(a)

(b)



(c)

Fig. 4 (Liftingbody) an image with manual histogram (a) original gray image (b) labeled binary image and manipulate histogram and convert to RGB (c) final image with embedded message

REFERENCES

[1] A. Tacticus, How to survive under siege / Aineias the Tactician, pp. 84-90, 183-193. Clarendon ancient history series,Oxford, England: Clarendon Press, 1990, ISBN 0-19-814744-9,translated with introduction and commentary by David Whitehead.

[2] J. Wilkins, Mercury: or the secret and swift messenger: showing, how a man may with privacy and speed communicate his thoughts to a friend at any distance. London: printed for Rich Baldwin, near the Oxford-Arms in Warnick-lane, 2nd edn.,1994, copy of Sir Geofirey Keynes, courtesy of the Rare Book Section, Cambridge University Library, (IX pp. 67).

[3] D. Chaum, 'Untraceable electronic mail, return addresses and digital pseudonyms." Communications of the A.C.M., vol. 24, no. 2, pp. 84-88, Feb. 1981.

[4] The Oxford English dictionary: being a corrected re-issue." Clarendon Press, Oxford, 2005.

[5] B. Pfitzmann, 'Information hiding terminology." In Anderson, pp. 347-350, ISBN 3-540-61996-8, results of an informal plenary meeting and additional proposals.

[6] Kahn, D., The Codebreakers, MacMillan Company, 1967.

[7] G. J. Simmons, 'The prisoners' problem and the subliminal channel." In Chaum [20], pp. 51-67.
[8] 'The history of subliminal channels." IEEE Journal of Selected Areas in Communications, vol. 16, no. 4, pp. 452-462,May 1998, ISSN 0733-8716, special issue on copyright & privacy protection.
[9] G. J. Simmons, ed., Contemporary Cryptology – The Science of Information Integrity. New York, New York, U.S.A.: IEEE Press, 1992.
[10] "Results concerning the bandwidth of subliminal channels."IEEE Journal of Selected Areas in Communications, vol. 16, no. 4, pp. 463-473, May 1998, ISSN 0733-8716, special issue on copyright & privacy protection.
[11] R. J. Anderson and F. A. P. Petitcolas, "On the limits of steganography."IEEE Journal of Selected Areas in Communications, vol. 16, no. 4, pp. 474-481, May 1998, ISSN 0733-8716, special issue on copyright & privacy protection.
[12] S. Craver, On public-key steganography in the presence of an active warden." Tech. Rep. RC20931, I.B.M. Research Division,T.J. Watson Research Center, Yorktown Heights, New York,U.S.A., Jul. 1997.
[13] J. Fridrich and M. Goljan, "Digital image steganography using stochastic modulation", SPIE Symposium on Electronic Imaging, San Jose, CA, 2003.
[14] M.Kharrazi, Husrev T. Sencar, and N.Memon, "Image Steganography", Concepts and Practice. April 2004
[15] A. Westfeld,"F5a steganographic algorithm: High capacity despite better steganalysis," 4th International Workshop on Information Hiding. 2001.
[16] Yedidya Hilewitz and Ruby B. Lee, Fast Bit Compression and Expansion with Parallel Extract and Parallel Deposit Instructions, Proceedings of the IEEE 17th International Conference on Application-Specific Systems, Architectures and Processors (ASAP), pp. 65-72, September 11-13,2006
[17] The Mathworks, Inc., Image Processing Toolbox User's Guide: http://www.mathworks.com/access/helpdesk/help/toolbox/images/images.html.
[18] Otsu, N., "A Threshold Selection Method from Gray-Level Histograms," IEEE Transactions on Systems, Man, and Cybernetics, Vol. 9, No. 1, 1979, pp. 62-66.
[19] Haralick, Robert M., and Linda G. Shapiro, Computer and Robot Vision, Volume I, Addison-Wesley, 1992, pp.28-48.
[20] D. Chaum, ed., Workshop on Communications Security (CRYPTO'83),Santa Barbara, California, U.S.A., 1984, IEEE, Plenum Press.