IJISET - International Journal of Innovative Science, Engineering & Technology, Vol. 1 Issue 4, June 2014.
www.ijiset.com
ISSN 2348 – 7968

A Novel Approach for Stegranography Method using Filter based Hierarchical Technique

M. Radhika Mani[1], K. Chandra Sekhar[2] and G. Suryakala Eswari[3]

[1] Associate Professor, Dept. of CSE, Pragati Engineering College
Surampalem, E.G.dist., A.P., India- 533437

[2] Assistant Professor, Dept. of CSE, Pragati Engineering College
Surampalem, E.G.dist., A.P., India- 533437

[3] Assistant Professor, Dept. of CSE, Pragati Engineering College
Surampalem, E.G.dist., A.P., India- 533437

Abstract

The present paper proposes various image steganography methods which are applied for storing the secret information. The methods include block based steganography for hiding the message. To test the integrity and robustness, the proposed methods are applied on various images like human faces, textures and medical images. For the comparison of the quality of the stego images, delectability and the stealthiness of the embedded information, various measures of image quality such as MSE, MAE, PSNR, SNR, and RSNR are evaluated for the techniques.

Keywords: *Cover Image, Stego Image, Window and performance measure.*

1. Introduction

There is a strong need for an alternative or complement to cryptography [1,2]: a technology that can protect content even after it is decrypted. Watermarking [3] has the potential to fulfill this need because it places information within the content where it is never removed during normal usage. Decryption [5], re encryption, compression, digital-to-analog conversion, and file format changes—a watermark can be designed to survive all of these processes[13][16]. A watermark is a recognizable image or pattern that appears as various shades of lightness/darkness when viewed by transmitted light (or when viewed by reflected light, atop a dark background), caused by thickness variations in the paper[4][7].Data hiding becomes an important field as the use of public networks such as internet[1][8][9] becomes popular. Hiding in digital media is a young field and is growing in an exponential rate[10]. Steganography is used to hide information inside other. As derived from Greek, the word steganography[11] literally means “Covered Writing”.

Steganography is the art and science of communicating in a way which hides the existence of communication[13][1], or it is the art of hiding information in ways that prevent the detection of hidden messages, or it is the art of passing information in a manner that the very existence of the message in unknown, or it is hiding a secret message within a larger one in such a way that others cannot discern the presence or contents of the hidden message. The main objectives of the security or steganographic algorithms should be such as to provide confidentiality [5][4], data integrity and authentication. Applications for such a data-hiding scheme include in-band captioning, covert communication, image tamper proofing, authentication, embedded control, and revision tracking[3][7].The steganography techniques can be classified as follows: (i) Spatial domain based steganography (ii)Transform domain based steganography (iii)Document based steganography (iv) File structure based steganography and (v) Other categories, e.g. video compress encoding and spread spectrum technique based.

2. Methodology

Steganographic applications only require the flexibility to alter Cover Object (C) in order to be able to embed the hidden information. For these constraints to be effectively achieved, the present paper proposes a novel technique of steganography based on partitioning the cover image in to blocks.In the proposed filter based hierarchical technique, the text to be hidden in the 3 cover images is divided into 15 unequal parts, then each part is converted into their binary form, and the 3 cover images are divided into 16 blocks each. A block is selected randomly from the 16 blocks in each of 3 stego images. The randomly selected block number is converted into equivalent binary form and stored in an array. The blocks with same numbers are selected from 3 stego images. Now, a 5×5 window is considered in each of the 3 blocks selected and the mean value is calculated for those three 5×5 window. The block with minimum value of mean of the 5×5 window is selected. The LSB’s of the pixels other than the pixels that are in the 5X5 sub image are replaced with the first part of the hidden text sequentially. This procedure is repeated for all parts of the hidden text. For the successful retrieval of

ISSN 2348 – 7968

the hidden text, the sequence of selected block numbers is pre-appended with its length and embedded in the LSB's of the pixels in the 16th block of the 1ststego image. The process of the embedding text adapting block based three images technique is depicted in the figure 1.

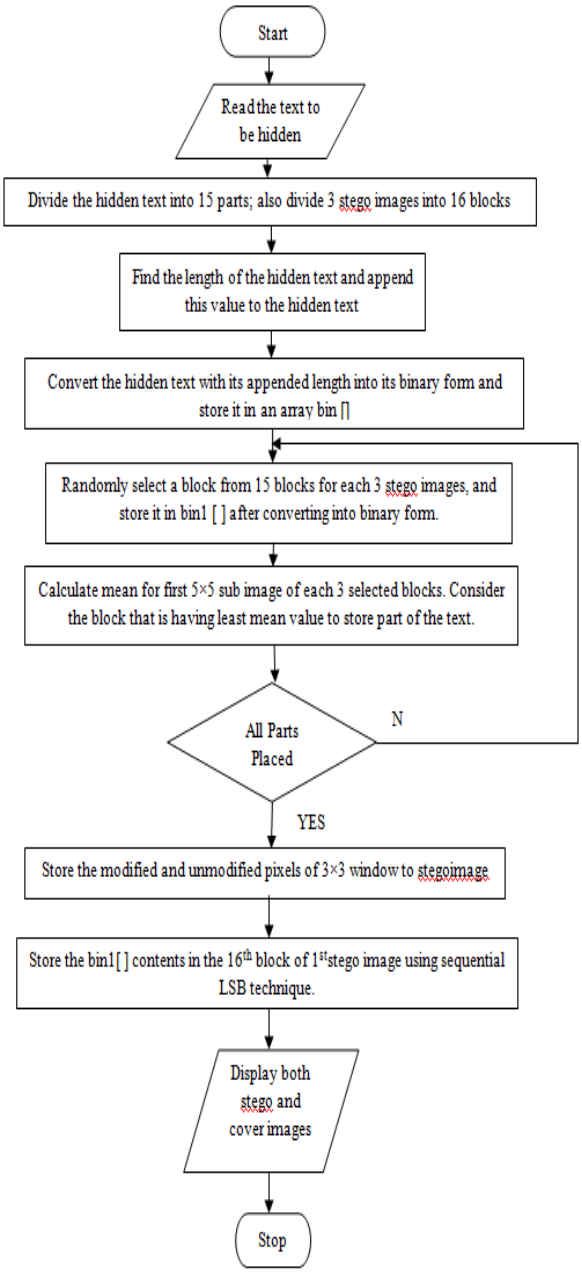

Fig.1. Flow chart for data hiding adapting filter based hierarchical technique.

In retrieval process to obtain the hidden text all the 3 stego images must be considered. Even if one stego image is not considered, hidden text cannot be revealed. Initially, the 3 stego images are divided into 16 blocks. The 16th block of the 1ststego image is considered to retrieve the sequence of blocks to retrieve the text sequentially. The LSB's of the first 8 pixels in 16th block gives the length of the sequence of blocks and the 9th pixel on wards the blocks order is obtained. Now, a 5×5 window is considered in each 3 blocks and the mean value is calculated. A block in which the 5×5 window with least mean value is present, is selected, to get the first part of the hidden text. The LSB's of the pixels other than the pixels that are in the 5×5 window are retrieved and grouped into 8 bits each. When the grouped bits are converted into ASCII form first 8 bits give the length of the text in that block and then onwards the 8 bits gives a character. Thus we will retrieve the first part from that block. This procedure is repeated until entire hidden text from the 3 stego images is retrieved.

The entire purpose of steganography is defeated if the steganography is detectable. For some algorithms, more data can be inserted before the personnel visually take notice. However, by definition, the security of the steganography algorithm is based on the statistics, but not on perception, as most of the steganalysis take place by identifying statistically anomalous patters in the image pixels. Various measures are given by the Equations (1) to (6).

$$MSE = \sum_{i=1}^{M}\sum_{j=1}^{N}\frac{(I_c - I_s)^2}{M \times N} \quad (1)$$

$$MAE = \sum_{i=1}^{M}\sum_{j=1}^{N}\frac{|I_c - I_s|^2}{M \times N} \quad (2)$$

$$RMSE = \sqrt{\frac{\sum_{i=1}^{M}\sum_{j=1}^{N}(I_c - I_s)^2}{M \times N}} \quad (3)$$

$$PSNR = 10 \times \log_{10}\left(\frac{255}{MSE}\right)^2 \quad (4)$$

$$SNR = \frac{\sum_{i=1}^{M}\sum_{j=1}^{N} I_s}{\sum_{i=1}^{M}\sum_{j=1}^{N}(I_c - I_s)} \quad (5)$$

$$RSNR = \frac{\sum_{i=1}^{M}\sum_{j=1}^{N} I_s}{\sum_{i=1}^{M}\sum_{j=1}^{N}(I_c - I_s)^2} \quad (6)$$

ISSN 2348 – 7968

Where, I_c is intensity of cover image, Isis intensity of stego image, M×N is the image size and L is the peak signal value of the cover image.

3. Results and Discussions

The proposed filter based method of steganography is applied on the original images of figures of 2(a) to 2(i). The hidden message "password_mission_qn8" is embedded in the images and the stego images are shown in the figures 3 (a) to3 (i). The stego images clearly indicate the robustness and integrity of the proposed methods as the method proposes to embed the information by imposing a hierarchical structure on a partitioned cover image blocks. The quality parameters specified in Equations (1) to(6) are evaluated and tabulated in the Table 1.

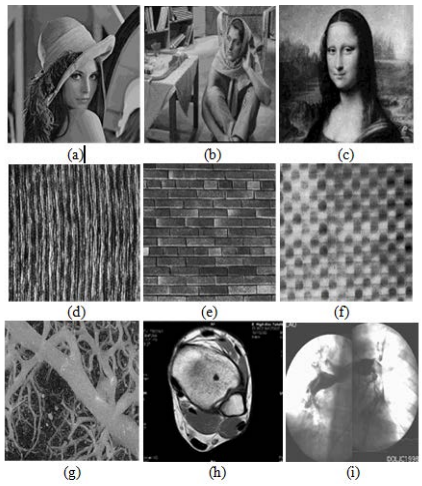

Figure 1 Original Cover Images (a) Lena(b) Barbara(c) Monalisa (d) D76 (e) D94(f) D8 (g) CT scan (h) MRI scan (i) 11-Ray.

Table 1 Measures of image quality for proposed method.

	Image name	MSE	MAE	RMSE	SNR	RSNR	PSNR
Human	Lena	41.65260	5.793800	6.453883	1.000000	1.000000	15.737961
	Barbara	49.464050	6.425000	7.033068	1.000000	1.000000	14.245010
	Monalisa	53.761575	5.994525	7.332229	1.000000	1.000000	13.521364
Textures	D76	40.706100	5.440350	6.380133	1.000000	1.000000	15.937614
	D94	31.890100	5.223550	5.647132	1.000000	1.000000	18.057686
	D8	69.738275	7.928275	8.350945	1.000000	1.000000	11.261380
Medical images	CT scan	0.001675	0.001675	0.040927	30116.164	173.54009	103.65050
	MRI scan	37.273275	3.628825	6.105184	1.000000	1.000000	16.702853
	X-ray	78.921275	7.436125	8.883765	1.000000	1.000000	10.186922

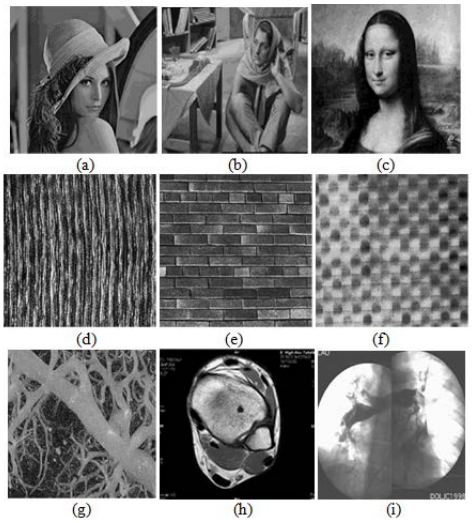

Figure 2 Original Cover Images (a) Lena(b) Barbara(c) Monalisa (d) D76 (e) D94(f) D8 (g) CT scan (h) MRI scan (i) 11-Ray.

4. Conclusions

In the present paper, a protocol is described, implemented, and tested for improving the robustness of information hiding schemes. It utilizes a quad tree structured hierarchical view of the cover object and dynamically determines regions where changes to the object for embedding message data. The proposed methods maintain high perceptional quality of the stego images and thus improve the stealthiness of the embedded message.

References

[1] R.J. Anderson and F.A.P. Petitcolas, "On the Limits of Steganography," J. Selected Areas in Comm., vol. 16, no. 4, 1998, pp. 474–481.

[2] M. Chapman, G Davida, and M. Rennhard. "A Practical and Effective Approach to Large-Scale Automated Linguistic Steganography" found online at http://www.nicetext.com/doc/isc01.pdf

[3] Curran, K. and Bailey, K. "An evaluation of image-based steganography methods". International Journal of Digital Evidence, Fall 2003.

[4] K. Ahsan, and D. Kundur, "Practical Internet Steganography: Data Hiding in IP" found online at <http://www.ece.tamu.edu/~deepa/pdf/txsecwrksh03.pdf>.

[5] J. Fidrich, M. Golijan, and R. Du, "Reliable Detection of LSB Steganography in Color and Grayscale Images".

[6] T. Handel and M.Sandford, "Hiding data in the OSI network model," Cambridge, U.K., May-June 1996, First International Workshop on Information Hiding.

[7] Herodotus, "The Histories", Penguin Classics; Reprint edition, September 1, 1996.

[8] Jackson, J. T., Gregg, H., Gunsch, G. H., Claypoole, R. L.,and Lamont, G. B. "Blind Steganography detection using acomputational immune system: A work in

ISSN 2348 – 7968

progress".International Journal of Digital Evidence, December 2003.
[9] N. Johnson, "Digital Image Steganography and Digital Watermarking Tool Table", found online at http://www.jjtc.com/Steganography/toolmatrix.htm.
[10]N.F. Johnson and S. Jajodia, "Steganalysis: The Investigation of Hidden Information," found online at <http://www.jjtc.com/pub/it98jjgmu.ps>.
[[11] R. Krenn, "Steganography: Implementation & Detection", found online at <http://www.krenn.nl/univ/cry/steg/presentation/2004-01-21-presentation-steganography.pdf>.
[[12] A. B. Pfitzmann, "Information Hiding Terminology," Proc. First Int'l Workshop Information Hiding, Lecture Notes in Computer Science No. 1,174, Springer-Verlag, Berlin, 1996, pp. 347-356.
[13] T. Aura, "Invisible Communication," EET 1995, technical report, Helsinki Univ. of Technology, Finland, Nov. 1995; http://deadlock.hut.fi/ste/ste_html.html.
[14] W. Bender et al., "Techniques for Data Hiding," IBM Systems J., Vol. 35, Nos. 3 and 4, 1996, pp. 313-336.
[15] E. Koch, J. Rindfrey, and J. Zhao, "Copyright Protection for Multimedia Data," Proc. Int'l Conf. Digital Media and Electronic Publishing, Leeds, UK, 1994.
[[16] W. Brown and B.J. Shepherd, Graphics File Formats: Reference and Guide, Manning Publications, Greenwich Conn., 1995.