AN EFFECTIVE STEGANOGRAPHY TECHNIQUE APPLIED IN MEDICAL IMAGES

[1]R.Kanmani, [2]Dr.S.Mary Praveena
[1]Assistant Professor(Senior Grade) Department of ECE,Sri Ramakrishna Institute of Technology,Tamilnadu,India.
[2]Associate Professor Department of ECE, Department of ECE,Sri Ramakrishna Institute of Technology,Tamilnadu,India.

ABSTRACT

Advances in Information and Communication technologies, force us to keep most of the information confidentially. Consequently, the security of information has become a fundamental issue. Besides cryptography, steganography can be employed to make information more robust and secure.

In this paper, a effective steganography technique has been proposed in which Spatial Domain has been employed for embedding patient data into the medical images and to analyze the stego image by various statistical parameters. It is easy to come up with sophisticated variants of this present method that use a stego-key is also proposed i.e., If the key is, say, 1011, then data bits are hidden in the least significant bits of bytes 1, 3, and 4 but not of byte 2, then in bytes 5, 7, and 8, but not in byte 6, and so on and are therefore more difficult to break and the same has been successfully implemented using MATLAB Coding. Comparison results shows that for high payload, prior scheme supersede the later and for security related issues the later wins.

Keywords *Steganography , Spatial Domain, Stego-Key, hidden in LSB of bytes, Security*

I. INTRODUCTION

The growing possibilities of modern communications need the special means of security especially on computer network. The network security is becoming more important as the quantum of data being exchanged on the internet increases. Therefore, the confidentiality and data integrity are required to be protected against unauthorized access. This has resulted in an explosive growth of the filed of information hiding. In addition, the rapid growth of publishing and broadcasting technology also requires an alternative solution for hiding information. The copyright of digital media such as audio, video and other media available in digital form a may lead to large-scale unauthorized copying. This is because of the digital formats making it possible to provide high image quality even under multi copying. The problem of an unauthorized copying is of great concern especially to the music, film, book and software publishing industries. To overcome this problem, encrypted information can be hidden in the digital media in such a way that it could not be easily extracted without a specialized technique.

Information hiding is an emerging research area, which encompasses applications such as copyright protection for digital media, Watermarking, fingerprinting and steganography [2]. In watermarking applications, the message contains information such owner identification and a digital time stamp, which is usually applied for copyright protection. With fingerprint, the owner of the data set embeds a serial number that uniquely identifies him as the owner. This adds to copyright information and makes it possible to trace any unauthorized copying. Steganography hides the secret message within the host image and its presence is imperceptible.

In these applications, information is hidden within a host image to be reliably communicated to a receiver. The host image is purposely corrupted, but in a covert way, and designed to be invisible to an informal analysis. However, this paper mainly deals with information hiding using steganography approach.

Among the various hiding information techniques, transform techniques embed the message by modulating coefficients in a transform domain, such as the Discrete Cosine Transform (DCT) used in JPEG compression, Discrete Fourier Transform, or Wavelet Transform. These methods hide messages in significant areas of the cover-image, which make them more robust to attack. By considering these facts, the authors employ wavelet transform to split the cover image into various spectral regions in which the high frequency component is selected to embed the data to be hidden. Since Matlab supports variety of wavelets along with the image processing tools, it has been used to implement the hiding.

II OVERVIEW ON STEGANOGRAPHY

The word steganography comes from the Greek Steganos, which means covered or secret and graphy means writing. Steganography is the art and science of hiding information such that its presence could not be detected[3]. Secret information is encoded in a manner such that the very existence of the information is visible.

The main goal of steganography is to communicate securely in a completely undetectable manner and to avoid drawing suspicion to the transmission of a hidden data [5]. It is a not to keep others from knowing the hidden information, but it is to keep others from thinking that the information even exists. If a steganography method causes someone to suspect there is secret information in a carrier medium, then the methods has failed [6].

Until recently, information hiding techniques received very much less attention from the research community and from industry than cryptography. This situation is however, changing rapidly and the first academic conference on this topic was organized in 1996. since then, there has been a rapid growth of interest in steganography . This is due to following reasons [7].

1. The publishing and broadcasting industries, have became interested in techniques for hiding encrypted copyright marks and serial numbers in digital films, audio recordings, books and multimedia products.

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 basic model of steganography consists of carrier, message and password. Carrier is also known cover-object, which embeds the message and serve hide its presence. Basically, the model for steganography is show fig 1 message is the data that the sender wisher remains it confidential. It may be plain text, cipher,other image, or anything that can be embedded in a stream such as a copyright mark, a communication, or a serial number. Password is as a stego-key, which ensures that only the recipient cover-object with the secretly embedded message then called the stego-object.

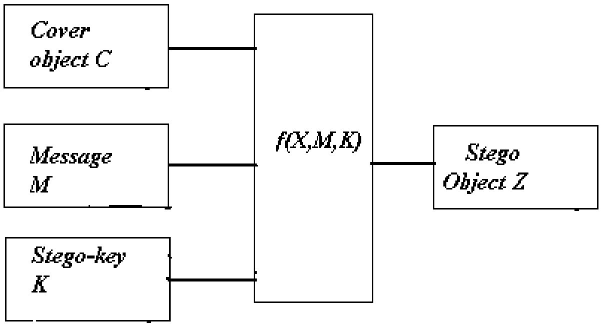


Fig 1. Basic Steganography Model

To recover the message from a stego-object requires the cover object itself and a corresponding decoding which is used during the encoding process. The original image may or may not be required in most application to extract, the message. The components that make up the basic framework of what it takes to communicate using steganography. Take a look at each piece individually: cover object, sego-key, and stego-object. The cover object is what is actually going to be seen out in the open the picture, sound, or movie that will be used to carry the message right under everyone’s noses. The stego-key is the code that the person sending the secret message is going to use to embed the message into the cover object; the recipient to extract the secret message will use this same stego-key. Stego-keys can come in many forms; they can be a password or an agreed-upon place to look for the hidden message. Abbreviations and Acronyms

The stego-object is the combination of the cover object, the stego-key, and the secret message. These three combine to create the condition where a cover object is carrying a secret message to be defined.

There are several suitable carriers that can be used as cover-object as listed below [8]:

1. Network protocols such as TCP, IP, and UDP.
2. Audio that use digital audio formats such as avi, mpeg, mpi, and coc.
3. File and disk that can hide and append files by using the slack space.
4. Text files such as html and java.
5. Image files such as bmp, gif, and jpg, where they can be both color and gray-scale.

In general, the information hiding process extract message from the redundant bits from cover-objects. The process consists of two steps [9,10]as follows:

The first is identification of redundant bits in a cover object. Redundant bits are those that can be modified without corrupting the quality or destroying the integrity of the cover-object.

Secondly the embedding process which, selects the subset of the redundant bits to be replaced with data from a secret message. The stego-object is created by replacing the selected redundant bits with message bits.

III Error Metrics

The effectiveness of the stego process proposed has been studied by estimating MSE, PSNR.

1. Mean Square Error
2. Peak Signal to Noise Ratio

Mean Square Error

The cumulative squared error between the Stego cover and the original cover image is calculated by using the equation given below:

$$MSE = \frac{1}{MN}\sum_{i=1}^{M}\ \sum_{j=1}^{N}\left(X_{i,j} - Y_{i,j}\right)^2$$

where M and N denote the total number of pixels in the horizontal and the vertical dimensions of the image Xi,j represents the pixels in the original cover image and Yi,j, represents the pixels of the stego-image.

Peak Signal To Noise Ratio (PSNR)

The PSNR is calculated using the equation,

$$PSNR = 10\log_{10}\left(\frac{I_{\max}^{2}}{MSE}\right)dB$$

where I_{max} is the intensity value of each pixel which is equal to 255 for 8 bit gray scale images.

The higher PSNR value indicates a better image quality. It is well known that an image with a PSNR value greater than 30 dB is acceptable to human perception. In addition, the visual quality and a comparison of the embedding capacity.

Typical PSNR values range between 20 and 40. They are usually reported to two decimal points (e.g., 25.47). The actual value is not meaningful, but the comparison between two values for different reconstructed images gives one measure of quality.

Higher the PSNR lower the error

The peak signal to noise ratio (PSNR) is used to estimate the visual quality of the compression images.

IV Data Embedding and Extraction using k-bit pixel embedding scheme

Embedding:

Step 1: Read the Medical cover image and the secret

Data to be embedded.

Step 2: Convert the secret data into binary row matrix.

Step 3: Read k value.

Step 4: Simple LSB embedding.

Step5: Stego cover is formed.

Extraction:

Step 1: Read the stego image.

Step 2: Get the K value from the user.

Step 3: Stego extraction

Step 4: Now convert each 8 bits into a character.

Step 5: Secret message is recovered.

Data Embedding and Extraction using symmetric key

Embedding:

Reading an image and converting it into binary data

Converting color image to gray image

Embed the text with the image

Use the stego key say 1011 to embed the text

Calculate MSE and PSNR Values.

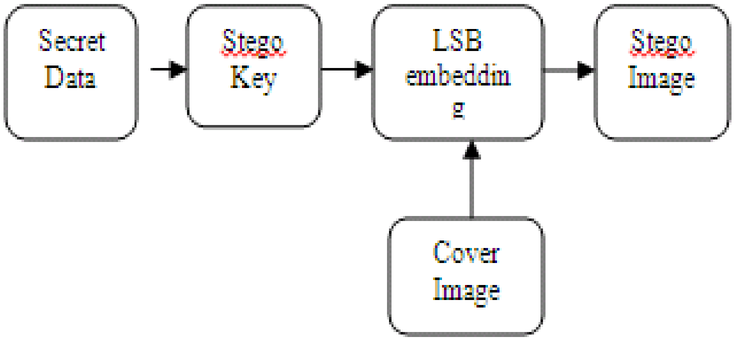


Fig 2.Diagram for embedding data using symmetric key

Extraction**:**

Reading an embedded image and converting it into binary data

Extract the text using the same stego key

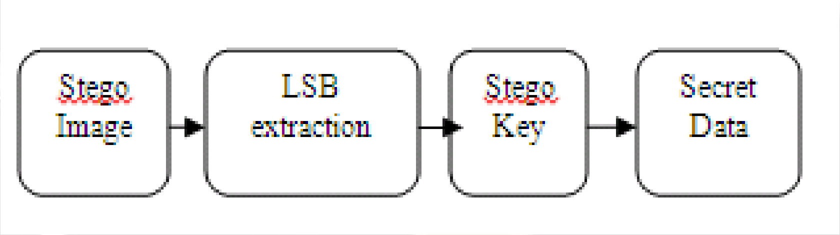


Fig 3. Diagram for extraction using Symmetric key

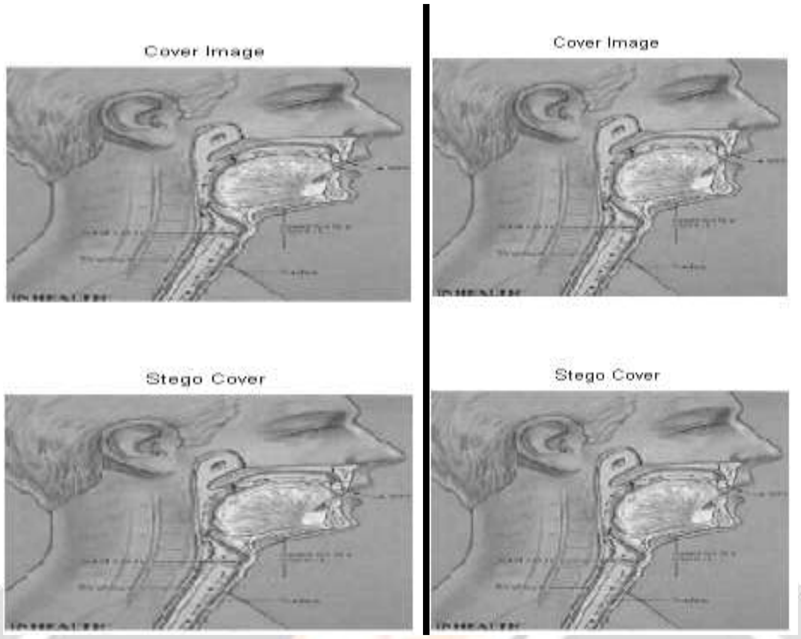
Results for Different Images

Tabulation for k bit embedding

Image Name	No of Pixels	K bit embed	100% Secret data bits	MSE	PSNR	Time Taken S
Throat Cancer	256× 256	4	262144	60.9919	30.2477	1.0790
		3	196608	14.1006	36.7293	1.0970
		2	131072	03.4509	43.3237	1.1130
		1	65536	00.5004	51.1378	1.1120

Table 1. Tabulation for K bit embedding for Throat Cancer image

For k=1 and k=2 , while considering the throat cancer image as cover as follows


Cover Image

Cover Image

Stego Cover

Stego Cover

Fig 4. Cover & Stego of Throat Cancer image

For cover image as HEART 170 × 170 pixels with k = 1, 2, 3 and 4 . With stego key 1101 have been plotted considering the full embedding capacity.

	KEY	K	MSE	PSNR	Time Taken (S)
HEART	1101	4	30.684	33.2617	3.204
	1101	3	5.7256	40.5526	3.147
	1101	2	1.9468	45.2376	3.637
	1101	1	0.3752	52.3883	10.49

Table 2.Tabulation for K-bit embedding using symmetric key for heart image

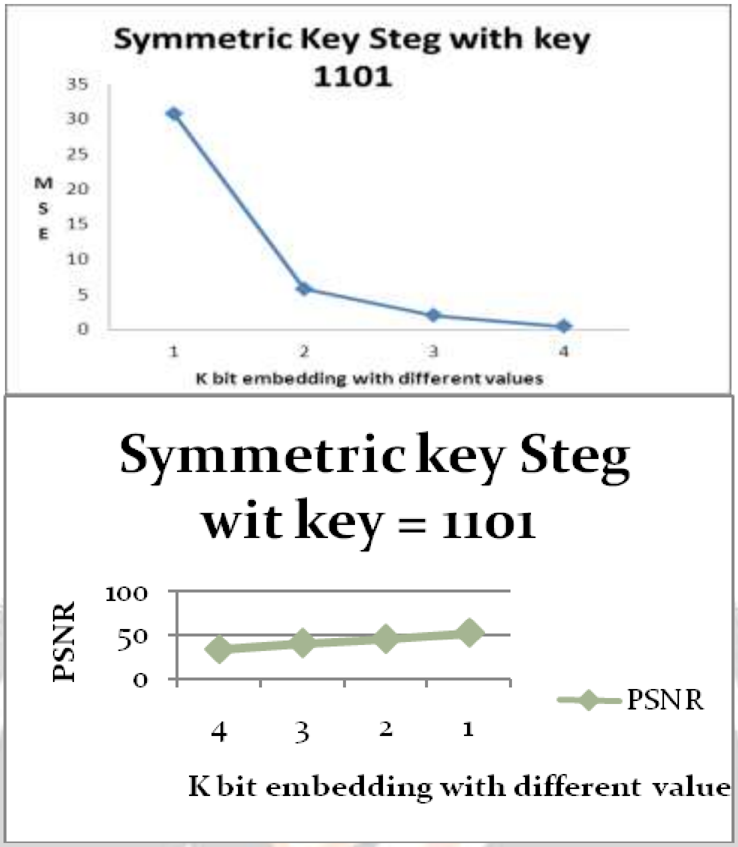


Fig 6.K bit Embedding with different values versus MSE & PSNR values

The corresponding stego cover and the cover image is as follows For k = 1, 2 with symmetric key 1101

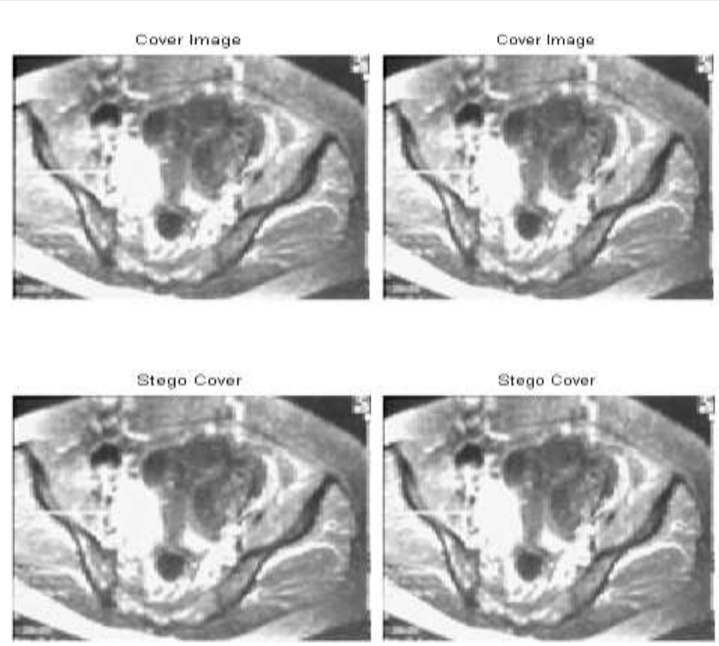


Fig 7 Stego Cover and cover image using stego key

V. CONCLUSION

In this paper, an effective steganography technique has been employed for embedding patient data into the different medical images and the stego image were analyzed by MSE & PSNR.

In the first implementation, Simple K bit LSB embedding has been employed and the results are analyzed for three different medical images with maximum payload. To further increase the security, symmetric key stego system has been implemented and the results are analyzed for the same medical images with varying key length. Stego key say, 1011, are used to hide data bits in the least significant bits of pixel 1, 3, and 4 but not of pixel 2, then in pixel 5, 7, and 8, but not in pixel 6, and so on are presented in this project. If the stego key is 5 then it will double the brute force attack than 4 and so forth. The key length decides the security level of the present implementation. Its suggested that a length of 16, 32, 64, 128 key length or 256 key length with 50% 0 and 50% 1 on it will be the optimum length and more suited for practical usage. This paper has been implemented successfully using MATLAB 7.1

VI REFERENCES

[1] Rajendra Acharya U, P. Subbanna Bhat, Sathish Kumar, Lim Choo Min ,**“**Transmission and storage of medical images with patient information**”** Computers in Biology and Medicine 33 (2003) 303–310 ELSEVIER.

[2] P.Moulin & J.A.O’ Sullivan, “Information Theoretic Analysis of Information Hiding “, IEEE International Symposium on Information Theory, Boston,MA,October,1999.

[3] C.Cachin, “An Information – Theoretic Model For Steganography”, in Proceedind 2nd Information Hiding Workshop,Vol.1525.pp.306-318, 1998.

[4]R.Chandramouli, N.Menon, “Analysis of LSB Based Image Steganography Techniques”, IEEE pp.1019-1022,2001.

[5] Chin-Chen Chang , Chia-Chen Lin ,Chun-Sen Tseng ,Wei-Liang Tai “Reversible hiding in DCT-based compressed images” Department of Computer Science and Information sciences 177 (2007) 2768–2786.

[6] Ching-Nung Yang ,Tse-Shih Chen, Kun Hsuan Yu,Chung-Chun Wang “Improvements of image sharing with Steganography and authentication” ,The Journal of Systems and Software 80 (2007) 1070–1076 ELSEVIER

[7] KokSheik Wong, Xiaojun Qi, Kiyoshi Tanaka “A DCT-based Mod4 steganographic method”,Signal Processing 87 (2007) 1251–1263 ELSEVIER.

[8] Chin-Chen Chang ,Chih-Yang Lin ,Yu-Zheng Wang “New image steganographic methods using run-length approach”, Information Sciences 176 (2006) 3393–3408 ELSEVIER.

[9] Chang-Chou Lin, Wen-Hsiang Tsai “Secret image sharing with steganography and authentication”, The Journal of Systems and Software 73 (2004) 405–414 ELSEVIER.

[10] Gopalakrishna Reddy Tadiparthi , Toshiyuki Sueyoshi **“**A novel steganographic algorithm using animations as cover**”** Decision Support Systems -11483 (2008) No.of pages 12 ELSEVIER.

[11]Rajendra Acharya U, U.C. Niranjan, S.S. Iyengar, N. Kannathala, Lim Choo Min “Simultaneous storage of patient information with medical images in the frequency domain**”** Computer Methods and Programs in Biomedicine (2004) **76**, 13—19 ELSEVIER.

[12] Yuan-Hui Yu , Chin-Chen Chang , Iuon-Chang Lin “A new steganographic method for color and grayscale image hiding**”** Computer Vision and Image Understanding 107 (2007) 183–194 ELSEVIER.