



MEASUREMENT OF THE IMAGE QUALITY :STEGANOGRAPHY

ARCHANA GUPTA¹, Dr. ANUJ SHARMA²

¹Research Scholar in Singhania University, Pachari Bari, Jhunjhunu (Rajasthan)

²Dean Academic Affairs, Om Institute of Technology and Management
Hisar - Chandigarh Road



ARCHANA GUPTA

ABSTRACT

This Paper focused on the qualitative and quantitative improvement in medical imaging with advancement in watermarking. The significance of watermarking applications in medical imaging to attain privacy and security .It was shown that the watermarking assures the authenticity and integrity of a medical images.

Key Words: Steganography, LSB , PSNR ,MSE.

©KY Publications

I. INTRODUCTION

Steganography is the art and science of invisible communication..It is play an important role in information security. It deals with embedding information in a given media without making any visible changes to it. It is a technology that hides a message within a object. For this security purpose we proposed watermarking technique for authentication of medical image. Medical image watermarking means embedding the patient information in the medical image. Watermarking increase the storage compatibility and avoid storing of multiple information etc..In image steganography the information is hidden exclusively in images. Three different aspects in information hiding system contend with each other: Capacity, Security and Robustness.

The basic model of steganography uses a cover object (any object that can be used to hold secret information inside), the secret message (the secret information that is to be sent) and a

steganography algorithm/technique (the procedure to hide secret message inside the cover object).

The outcome of the process is the stego object which is the object that has the secret message hidden inside. This stego object is sent to the receiver where receiver will get the secret data out from the stego image by applying decoding algorithm. Generally message appears something else to third part: images, articles shopping lists etc. The hidden message may be in invisible ink between the visible lines of a private letter. It is high security technique for long data transmission.

It is a method of hiding message such that only receiver is able to read the message .It is the art and science of writing hidden messages in such a way that no one, except sender and receiver are able to detect the message.

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.

The basic model of steganography consists of carrier, message and password. Carrier is also known as cover -object, which the message is embedded and serves to hide the presence of the message.

Message is the data that the sender wishes to remain it confidential. It can be plain text, cipher text, other image or anything that can be embedded in a bit stream such as a copyright mark, a covert communication or a serial number. Password is known as stego-key, which ensures the message from a cover-object. The cover-object with the secretly embedded message is then called the stego-object.

It is necessary to achieve high embedding capacity and visual quality. The important factors that needs to be considered while designing a steganographic system are embedding capacity means number of secret bits that can be embedded per pixel. Visual quality of stego image (i.e. image distortion) security and amount of data (compression) shared. So , compression , redundant bit and bit depth make digital image format more stronger than other format .And these factor help in achieving high embedding capacity and visual quality. The basic model of steganography uses a cover object, the secret message and a steganography algorithm/technique. The out-come of the process is the stego object which is the object that has the secret message hidden inside. This stego object is sent to the receiver where receiver will get the secret data out from the stego image by applying decoding algorithm.

To easily access of medical information. To the maintenance of electronic health record.To avoid the distribution of famous persons reports to tabloids.To the maintenance of high fidelity.To avoid the misinterpreted tele-diagnosis results.

We will try to achieve high level flexibility that support all type of image format with security. Adaptive techniques are not an easy target for attacks because image statistics distortion is kept to a minimum.

Result and Performance analysis:

The factors to be considered while designing a steganography system are:

1. Number of bits to be embedded.
2. Visual quality of the image.
3. Less distortion in the embedded cover image compared to original image.

The performance is evaluated based on PSNR (Peak Signal to Noise Ratio) which defines the quality of the image. The PSNR is defined as follows.

$$PSNR = 10\text{Log}_{10} (255^2/MSE) \text{ db}$$

Where MSE is Mean Square Error between the original image and the stego image. Larger the PSNR value better the quality which means stego image will be almost similar to original image.

Experimental Results and Discussion

Experiments are carried out on certain categories of medical images varying in size and bits per pixels. Standard results are taken using various medical images .To evaluate the data hiding capacity and medical image quality, the performance evaluation is measured by PSNR,MSE,SSIM,SNR,BER ,RMSE etc. We have presented an algorithm with lossless data hiding scheme. Our algorithm has shown a significant improvement on lossless scheme and output performs in terms of parameters which considered for evaluation.

Result and Performance analysis:

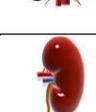
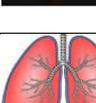
Measurement of the image quality using various parameters.....

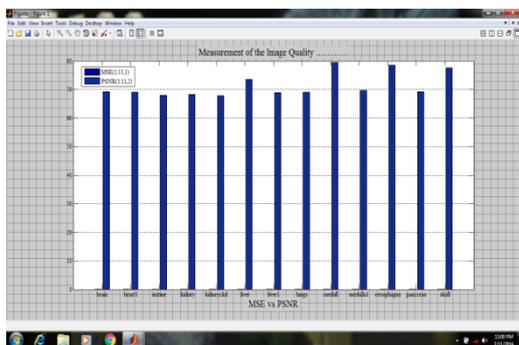
Table 1: MSE and PSNR values of different images.

S.N	Images	Images Name	MSE	PSNR
1		brain.png	0.007753 67	69.269 7
2		heart1.png	0.008035 06	69.114 9
3		Instine.png	0.010404 2	67.992 7
4		kidney.png	0.009587 51	68.347 7
5		kidneyckd.png	0.010982 6	67.757 8

6		liver.png	0.002842 93	73.627 1
7		liver1.png	0.008472 85	68.884 5
8		lungs.png	0.007989 64	69.139 5
9		medull.png	0.000737 3	79.488 4
10		medulla1.png	0.007131 12	69.633 2
11		oesophagus.png	0.000911 22	78.568 5
12		pancreas.png	0.007708 41	69.295 1
13		skull.png	0.001149 07	77.561 3

Table 2: BER and PSNR values of different images.

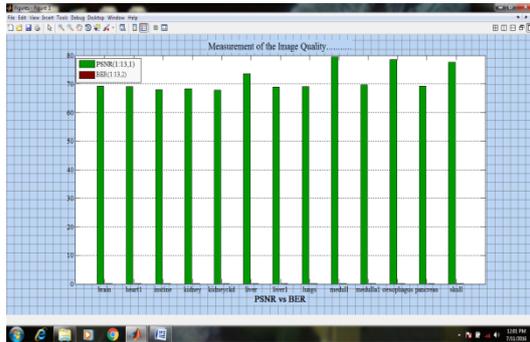
S.No	Images	Images Name	BER	PSNR
1		brain.png	0.01443 63	69.26 97
2		heart1.png	0.01446 87	69.11 49
3		Intstine.png	0.01470 75	67.99 27
4		kidney.png	0.01463 11	68.34 77
5		kidneyckd.png	0.01475 85	67.75 78
6		liver.png	0.01358 19	73.62 71
7		liver1.png	0.01451 71	68.88 45
8		lungs.png	0.01446 35	69.13 95
9		medull.png	0.01258 05	79.48 84
10		medulla1.png	0.01436 1	69.63 32
11		oesophagus.png	0.01272 77	78.56 85
12		pancreas.png	0.01443 1	69.29 51
13		skull.png	0.01289 3	77.56 13



Graph showing the MSE vs PSNR variation.

PSNR measures in decibels. The quality of the stego image compared with the cover image; higher the PSNR better the quality. It is used to measure the similarity between before and after compression of the image.

Measurement of the image quality using various parameters.....



Graph showing the PSNR vs BER variation.

BER (Bit Error Rate) = 1/PSNR

If BER is low then higher will be the reliability of image.

Conclusion

The greatest advantage of this method is that it makes only negligible alteration to the cover image; therefore the method is applicable for medical images without reducing their authenticity. Compressing medical image offers a method of reducing the cost of storage and increasing the speed of transmission.

Future scope

The coverage of this research provides strength to this reference resource for both secure multimedia distribution researchers and also decision makers in obtaining a greater understanding of the concepts ,issues, problems ,trends, challenges and opportunities related to this field of study .It is our sincere hope that this research and its great amount of information and research will provide a scientifically and scholarly sound treatment of state-of-art techniques to students, researchers , academics, personnel of law enforcement and IT/multimedia practitioners who are interested or involved in the study ,research, use, design and development of techniques related to secure multimedia distribution.

REFERECES

[1]. B. Macq and F. Dewey. Trusted headers for medical images. In DFG VIII-D II Watermarking Workshop, Erlangen, Germany, Oct. 1999.
 [2]. A. Maeder and M. Eckert. Medical image compression: Quality and performance

issues. SPIE: New Approaches in Medical Image Analysis, 3747:93–101, 1999.
 [3]. M. Nishio, Y. Kawashima, S. Nakamuar, and N. Tsukamoto. Development of a digital watermark method suitable for medical images with error correction. RSNA 2002 Archive Site: <http://archive.rsna.org/index.cfm>, 2002. accessed 18 January 2005.
 [4]. Yang, C. H., Weng, C. Y, and S. J. Wang et al., 2008. "Adaptive Data Hiding in Edge Areas of Images With Spatial LSB Domain Systems," IEEE Transactions on Information Forensics and Security, 3(3): 488-497.
 [5]. Ramezani M., and S. Ghaemmaghami, 2010. Towards Genetic Feature Selection in Image Steganalysis," in 6th IEEE International Workshop on Digital Rights Management, Las Vegas, USA.