Review of Different Steganographic techniques on Medical images regarding their efficiency

Preet Kamal
DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING
CHANDIGARH ENGINEERING COLLEGE
LANDRAN, MOHALI (PUNJAB), INDIA

Gagandeep Jindal
DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING
CHANDIGARH ENGINEERING COLLEGE
LANDRAN, MOHALI (PUNJAB), INDIA

Abstract-Digital steganography is propose to increase medical image security, confidentiality and integrity. Medical image steganography is a special subcategory of image steganography in the sense that the images have special requirements. Particularly, steganographed medical images should not differ perceptually from their original counterparts, because the clinical reading of the images (e.g. for diagnosis) must not be affected. This paper presents a preliminary study on the degradation of medical images when embedded with different steganographic algorithm, using a variety of popular systems. Image quality is measured with a number of widely used metrics, which is applied elsewhere in image processing. The general conclusion that arises from the results is that typical data embedding can cause numerical and perceptual errors in an image. The greater the robustness of a data hiding, the greater the errors are likely to be. Consequently medical image steganography remains an open area for research, and it appears that a selection of different watermarks for different medical image types is the most appropriate solution to the generic problem.

Keywords – Annotation, Steganography, Image steganography, medical image steganography.

I. INTRODUCTION

Steganography is the art and science of invisible communication. This is accomplished through hiding information in other information, thus hiding the existence of the communicated information. The word steganography is derived from the Greek words “stegos” meaning “cover” and “grafia” meaning “writing” defining it as “covered writing”. In image steganography the information is hidden exclusively in images. Three different aspects in information-hiding systems contend with each other: capacity, security, and robustness. Capacity refers to the amount of information that can be hidden in the cover medium, security to an eavesdropper’s inability to detect hidden information, and robustness to the amount of modification the stego medium can withstand before an adversary can destroy hidden information. Adaptive steganography with a high embedding capacity and a low distortion is an attractive topic in the area of information hiding (Yang et al., 2008). In digital images, parts with high contrast and noise-like textures have been found to be appropriate locations to hide pseudo-random encrypted messages, due to the statistical similarities between the covert and the selected cover signals (Dulce et al., 2007).
Various steganalysis attacks have been proposed in the literature to distinguish between original and stego objects. A successful attack is supposed to detect the changes in the cover objects caused by the message embedding process. Recently, a set of steganographic algorithms have been developed which employ some adaptation techniques to minimize the changes made to the cover object characteristics (Franz et al., 2004). Early proposals are steganographic method which uses the difference value between two neighbor pixels to determine the number of secret bits to be embedded (Wu et al., 2003) dithering to get image information that can be used by adaptive steganographic algorithms, the “pixel-value differencing” (PVD) and LSB replacement method (Wu et al., 2005), the defining of texture in order to detect regions with textures not homogeneous and also an adaptive LSB steganographic method with larger embedding capacity using PVD (Franz et al., 2004). In this work we propose an algorithm which selects 2×2 blocks of high contrast image parts. Message bits are embedded into these selected blocks with Mod-4 (Qi et al., 2005) embedding method in order to decrease the effects of modifications caused by the embedding process. The embedding capacity denotes the number of bits that can be embedded into the given cover image. Our method can embed a large number of secret data and maintain original quality of the stego images.

II. RELATED WORK

With the boost of computer power, the internet and with the development of Digital Signal Processing (DSP), Information Theory and Coding Theory, Steganography went "Digital". In the realm of this digital world Steganography has created an atmosphere of corporate vigilance that has spawned various interesting applications of the science. Contemporary information hiding was first discussed in the article "The prisoners' Problem and the Subliminal Channel". More recently Kurak and McHugh carried out work which resembled embedding into the 4LSBs (Least Significant Bits). They discussed image downgrading and contamination which is now known as Steganography. Cyber-terrorism, as coined recently, is believed to benefit from this digital revolution. Cyber-planning or the "digital menace" as Lieutenant Colonel Timothy L. Thomas defined it is difficult to control. Provos and Honeyman scrutinized 3 million images from popular websites looking for any trace of Steganography. They have not found a single hidden message. Despite the fact that they gave several assumptions to their failure they forget that Steganography does not exist merely in still images. Embedding hidden messages in videos and audios is also possible and even in a simpler form such as in Hyper Text Mark up Language (HTML), executable files (.EXE) and Extensible Markup Language (XML). Steganography is employed in various useful applications e.g., Copyright control of materials, enhancing robustness of image search engines and Smart IDs where individuals' details are embedded in their photographs. Other applications are Video-audio synchronization, companies' safe circulation of secret data, TV broadcasting, Transmission Control Protocol and Internet Protocol packets (TCP/IP) - for instance a unique ID can be embedded into an image to analyze the network traffic of particular users, embedding Checksum etc. In a very interesting way Petitcolas demonstrated some contemporary applications; one of which was in Medical Imaging Systems where a separation is considered necessary for confidentiality between patients' image data or DNA sequences and their captions e.g., Physician, Patient's name, address and other particulars. A link however, must be maintained between the two. Thus, embedding the patient's information in the image could be a useful safety measure and helps in solving such problems.

2.1 Steganalysis

Steganalysis is the science of attacking Steganography in a battle that never ends. It mimics the already established science of Cryptanalysis. Note that a Steganographer can create a Steganalysis merely to test the strength of her algorithm. Steganalysis is achieved through applying different image processing techniques e.g., image filtering, rotating, cropping, translating, etc, or more deliberately by coding a program that examines the stego-image structure and measures its statistical properties e.g., first order statistics (histograms), second order statistics (correlations between pixels, distance, direction). Apart from many other advantages higher order statistics, if taken into account before embedding, can improve the signal-to-noise ratio when dealing with Gaussian additive noise. In a less legitimate manner, virus creators can exploit Steganography for their ill intention of spreading Trojan Horses. If that were to happen, anti-virus companies should go beyond checking simply viruses' fingerprints as they need to trace any threats embedded in image, audio or video files using Steganalysis. Passive Steganalysis is meant to attempt to destroy any trace of secret communication whether it exists or not by using the above mentioned image processing techniques, changing the image format, flipping all LSBs or by lossy compression e.g., JPEG. Active Steganalysis however, is any specialized algorithm that detects the existence of stego-images. There are some basic notes that should be observed by a Steganographer: 1- In order to eliminate the attack of comparing the original image file with the stego image where a very simple kind of Steganalysis is essential, we can newly create an image and destroy it after generating the stego image. Embedding into images available on the World Wide Web is not advisable as a Steganalysis devotee might notice them and opportunistically utilize them to decode the stego.

III. STEGANOGRAPHY METHODS

3.1 Steganography Exploiting Image Format

Steganography can be accomplished by simply feeding into a Microsoft XP command window the following half line of code:

C:\> Copy Cover.jpg /b + Message.txt /b Stego.jpg

This code appends the secret message found in the text file 'Message.txt' into the JPEG image file 'Cover.jpg' and produces the stego-image 'Stego.jpg'. The idea behind this is to abuse the recognition of EOF (End of file). In other words, the message is packed and inserted after the EOF tag.

3.2 Steganography in the Spatial Domain

In spatial domain methods a Steganographer modifies the secret data and the cover medium in the spatial domain, which is the encoding at the level of the LSBs. This method has the largest impact compared to the simplicity.

3.3 Steganography in the Frequency Domain

New algorithms keep emerging prompted by the performance of their ancestors (Spatial domain methods), by the rapid development of information technology and by the need for an enhanced security system. The discovery of the LSB embedding mechanism is actually a big achievement. Although it is perfect in not deceiving the HVS, its weak resistance to attacks left researchers wondering where to apply it next until they successfully applied it within the frequency domain. DCT is used extensively in Video and image (i.e., JPEG) lossy compression. Most of the techniques here use a JPEG image as a vehicle to embed their data. JPEG compression uses DCT to transform successive sub-image blocks (8x8 pixels) into 64 DCT coefficients.

3.4 Performance Measures

As a performance measurement for image distortion, the well known Peak-Signal-to-Noise Ratio (PSNR) which is classified under the difference distortion metrics can be applied on the stego images. It is defined as:

$$PSNR = 10\log 10\left(\frac{C_{max}^2}{MSE}\right)$$

Where MSE denotes the Mean Square Error which is given as:

$$MSE = \frac{1}{MN}\sum_{x=1}^{M}\sum_{y=1}^{N}(S_{xy} - C_{xy})^2$$

and holds the maximum value in the image, for example:

$$C_{max}^2 \leq \begin{cases} 1, & \text{double-precision} \\ 255, & \text{uint8 bit} \end{cases}$$

x and y are the image coordinates, M and N are the dimensions of the image, Sxy is the generated stego image and Cxy is the cover image.

3.5 Adaptive Steganography

Adaptive Steganography is a special case of the two former methods. It is also known as “Statistics-aware embedding” and “Masking”. This method takes statistical global features of the image before attempting to interact with its DCT coefficients. The statistics will dictate where to make the changes. This method is characterized by a random adaptive selection of pixels depending on the cover image and the selection of pixels in a block with large local STD Standard Deviation .The latter is meant to avoid areas of uniform color e.g., smooth areas. This behaviour makes adaptive Steganography seek images with existing or deliberately added noise and images that demonstrate colour complexity. Wayner, dedicated a complete chapter in a book to what he called ‘life in noise’, pointing to the usefulness of data embedding in noise. It is proven to be robust with respect to compression, cropping and image processing. Whilst simple, edge embedding is robust to many attacks (given its nature in preserving the abrupt change in image intensities) and it follows that this adaptive method is also an excellent means of hiding data while maintaining a good quality carrier.

IV. PROPOSED APPROACH

Digital Steganography in medical images is a fascinating scientific area which falls under the umbrella of security systems. We have presented in this work some background discussions on algorithms of Steganography deployed in digital imaging. The emerging techniques such as DCT, DWT and Adaptive Steganography are not an easy target for attacks, especially when the hidden message is small.

4.1 Proposed Data Hiding Model

Figure 1 below shows the block diagram of the proposed image steganographic model. The input messages can be in any digital form, and are often treated as a bit stream. The input message is first converted into encrypted form through proposed encryption method. This encrypted message generates the secret key which may be used as a password before starting of the embedding or extracting operation for increasing another level of security. Second the image is re -shaped to the 2×2 blocks of non-overlapping spatially adjacent pixels. Then the valid blocks are selected from these blocks. Block Q is valid if the average difference between the gray level values of the pixels of that and it's mean (C) exceeds a threshold (minimum contrast), as described in (1). By definition, a valid block is associated with part of noisy region in the image.

$$\text{valid blocks(Q)} : \mathrm{C} = \left(\frac{1}{4} \sum_{x \varepsilon Q} |\, x - m_Q \,|\right) > T \qquad (1)$$

where mQ is the mean gray level value of the pixels in the block and T is the minimum contrast defined by the user. Taken T = 10, in this work. Before describing the embedding phase, some of the variables are defined. Given a block Q,

$$\sigma_Q = \sum_{x \varepsilon Q} x$$
$$\delta(\sigma_Q, 4) = (\sigma_Q \bmod 4)_2$$
$$A = \{x \mid x \varepsilon Q, x \geq m_Q\}$$
$$B = \{x \mid x \varepsilon Q, x < m_Q\}$$

The subscript 2 in the definition of $\delta(\sigma_Q, 4)$ indicates to convert the resulting value into the binary representation. It is obvious that the range of $\delta(\sigma_Q, 4)$ is { 00; 01; 10; 11}.

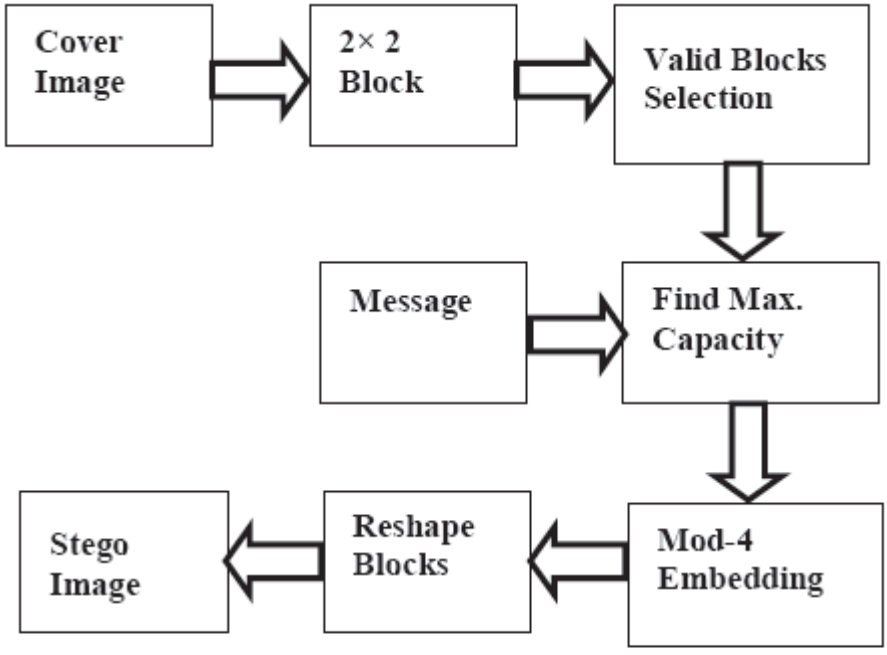

Figure 1. Block diagram for the proposed system.

REFERENCES

[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. "Adaptive Data Hiding in Edge Areas of Images With Spatial LSB Domain Systems," IEEE Transactions on Information Forensics and Security, 3(3): 488-497, 2008

[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.

[6] C.C chang, T.chen, L.Z.chung, A stegnographic method based upon JPEG and quantization table modification ,information sciences 141(1-2)(2002)123-138.

[7] L.YU, Y.Zhao,R.Ni, Zhu, PM1 stegnography in JPEG images, using genetic alogrith,soft computing 13 (4) (2009) 393-400.

[8] N.Provos, P.Honeyman, Hide and seek: an introduction to stegnography,IEEE Security and Privacy 1 (3) (2003) 32-44.

[9] W. Bender, W. Butera, D. Gruhl, R. Hwang, F.J. Paiz, S.Pogreb, Applications for data hiding,IBM Systems Journal 39 (3&4) (2000) 547-568.

[10] R. Bohme, A. Westfield, Exploiting preserved statics for stegnalsis, Lecture Notes in computer science, vol. 3200/2005, Springer, Berlin, 2005,pp.82-96