Comparative Analysis of Steganographic Algorithms intacting the information in the Medical images regarding their efficiency

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

Rajwinder singh
HEAD, 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 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- Steganography, Low Bit Encodig algorithm, Spread-spectrum, Echo-hiding.

I. INTRODUCTION

The main goal of steganography is to hide a message in the cover file which may be an image , image or a video file, thereby obtain a new data ***d'***, practically indistinguishable from the original file. The eavesdropper cannot detect the presence of m in d']. Thus Steganography attempts to hide all evidence regarding the existence of communication. When digital image is used, it is found that the visual lobe of human is resistant to the low scale image alterations and is unable to detect the change in the phase. While in image, if we scan the watermarked file and the original one, there will be a cleye difference seen in the stretching of the pixels, which is undesirable for covert communication point of view. This gives an advantage to image file over image as a cover media. Usually, human eyes perceive higher pictures better than the lower ones, and it is thus easier to hide data among low pictures without the human eye noticing the alteration. This very property of human perception system is exploited and the base cover for information hiding is created. Cleverly embedding the information in the significant parts (higher significant bits) of the cover file will result in a loss of quality since some of the information will be lost. Using various algorithms, we can employ the virtue of information hiding in image communication for transmitting hidden text along with the image or music. The proposed approach is quite crucial in military-warfare conditions, as well in the protection of intellectual possessions. The covert nature is the desirable feature which denies an unauthorized user from mining sensitive information or claiming the ownership of music in case of water-mark embedding. A simple technique which involves the embedding of information in the least significant bits of the cover-image file is known as Low-bit Encoding Technique. The most important advantage prevailing in it is the minimization of the distortion.

II. INFORMATION HIDING

Low Bit Encoding technique is the simplest way to entrench information in a digital image file. The Binary message that has to be hidden, substitutes the least significant bit of each sampling point.

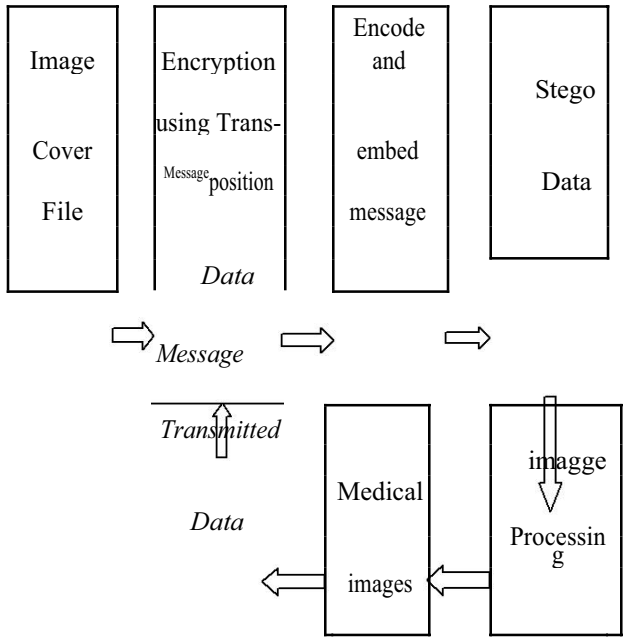


Fig. 1. Basic transmitter block diagram employing medical image

Firstly, the cover image is taken and the message is embedded in it. The message is required to be encrypted so that no other person than the desired destination can get the sent information. Here transposition cipher method is used for the same. After encoding and embedding it in the image file, it is processed using Digital Signal

or image with the hidden text in it. Using UMTS back-bone of image communication it is not possible to crack the information, when an image or media is sent to the intended recipient.

III. TECHNIQUES FOR DATA HIDING

3.1 Basic Low Bit Encoding Technique

Low Bit Encoding refers to the data hiding in the Least Significant Bit of the cover (image) sample in the time domain. Normally, the total number of samples in the image file is greater than the length of the secret message to be encoded. One must then decide the selection of the subset of samples that will contain the secret message and convey that decision to the receiver. [3] By substituting the least significant bit of each sampling point with a binary message, LSB coding allows for a large amount of data to be encoded. The algorithm given below is run for Low Bit Encryption technique.

3.2 Algorithm:

- Take an image file.
- Quantize it with 2^n levels ($n \leq 256$), for an 8-bit code-word. Say a(i,8)
- Take the text message to be hidden inside image file.
- Consider a key that is used to encrypt the text using Transposition cipher Method.
- L_H__LI_WKH_NH_LV_PDGH_RI_µP_DOSKDEHWV_When the
    - letters of the message are arranged in to form
    - µP_QXPEHU_RI_FROXPQV_

  Convert it to binary and reshape the matrix.
- Position the encrypted message in one column. Say b(i,1)
- Replace the last bit of the 8-bit code word of the image with the encrypted message.
  i.e. a (i,8) = b (i,1)
- De-quantize it to obtain the original image with the text inserted in it.

3.3 Limitations:

Mainly two types of attack take place on the method employed and hence two types of robustness exist. First type of attack aims to reveal the concealed message while the second one tries to destroy the hidden message. Substitution techniques are susceptible against both types of attacks. The challenger who tries to reveal the hidden message requires understanding about the significant bits which are modified. Since substitution techniques usually modify the bits of lower layers in the samples, it becomes easy to reveal the hidden message if the low intelligibility causes suspicions and hence it can be fragile.

These attacks can also be characterized in another way as the deliberate attacks and the non-deliberate attacks. Even non-deliberate attacks like transition deformation could wreck the

hidden message if is embedded in the bits of lower layers in the samples. To combat this problem, embedding the message bits should take place in the deeper layers and other bits (the bits proceeding and succeeding the embedded ones) can be altered to decrease the amount of the error, but this leads to a sort of complexity. So a sort of compromise is required between complexity and robustness.

3.4 *Modified Least Significant Bit Method*

With the usage of the standard LSB coding method the original host image bit in the i^{th} layer (i=1,..., 16) with the bit from the watermark (message) bit stream is replaced. In the case when the original and message bit are different and i^{th} LSB layer is used for embedding the error caused by watermarking is 2^i-1 quantization steps (QS) with the amplitude range is [-32768 to 32767]. The embedding error is positive if the original bit was 0 and watermark bit is 1 and vice versa.

[2] If only one of 16 bits in a sample is fixed and equal to the message bit, the other bits can be flipped in order to minimize the embedding error. The detail algorithm is as follows:

if host sample a>=0
1 0 0 1 1 0 1 1
if bit 0 is to be embedded
1 0 0 1 1 0 0 1
if a(i ±1) =0 then A(i ± 1) A(i ± ___ __$____ ___ _
if a(i ±1) =1 then A(i ± 1) A(i ± ___ __$____ ___ __DQG
1 0 0 1 1 0 0 0
if a(i+1)=0 then A(i+1) = 1
1 0 0 1 1 1 0 0
else if a(i+2)=0 then A(i+2)=1

else if a(15) =0 then A(15) = 1

1 0 0 1 1 0 1 1
else if bit 1 is to be embedded
1 0 0 1 1 0 1 1
if a(i ±1) =1 then A(i ± 1) A(i ± ___ __$__ ___ _
1 0 0 1 1 0 1 0
if a(i ±1) =0 then A(i ± 1) A(i ± ___ __$__ ___ __DQG
if a(i+1)=1 then A(i+1) = 0
1 0 0 1 0 0 1 0
else if a(i+2)=1 then A(i+2)=0

else if a(15) =1 then A(15) = 0

3.5 Similar is the case for host-sample < 0. 3.3 Alternate Bit Encoding

In this method, the alternative layers of the data fragments are selected and accordingly the message data is hidden. E.g. If (LSB-8^{th} layer) is selected, then 1^{st} message data goes to the 8^{th} layer, 2^{nd} data to the 7^{th} layer, 3^{rd} data goes again to the 8^{th} layer, 4^{th} data go into 7^{th} layer and the process continues. And

reverse process is being carried out at the receiver end to get the actual message data.
This method is better than the Low Bit Encoding method because it has more robustness and higher SNR value.

Consider digitized image sequence as: 0 1 1 0 1 0 1 0 1 0 0 1 1 1 0 1 0 1 1 1 0 1 1 1 1 0 1 0 1
1 1 0 1 1 0 0 1 0 1 0

Let the data to be embedded (hidden) be: **01100**

The encoded sequence as a result of this algorithm will be: 0 1 1 0 1 0 1 **0** 1 0 0 1 1 1 **1** 1 0 1 1 1 0 1 1 **1** 1 0 1 0
1 1 **0** 0 1 1 0 0 1 1 0 **0**

3.6 *Spread Spectrum Method*

The basic spread spectrum method attempts to spread secret information across the image signal. This is analogous to a system using an implementation of the LSB coding that randomly spreads the message bits over the entire picture file. [11] However, unlike LSB coding, the Spread Spectrum method spreads the secret message over the picture file's frequency spectrum, using a code that is independent of the actual signal. As a result, the final signal occupies a bandwidth in excess of what is actually required for transmission. The algorithm is given below:

Call the Image file.
Take its Quantization. (Supose **256** Quantization level).
Convert this into binary. Let¶V say a(i).
Take the text message and message key.
Encrypt the message and put it on a given layer.
Take any random pulse.
Ex-or it with stego file.

3.7 Echo Hiding Method

In this method the secret message is embedded into cover image signal is known as an echo. It allows for a high data transmission rate and provides superior robustness when compared to the noise inducing methods. Here three parameters are considered to hide the data successfully, viz. amplitude, decay rate, and offset (delay time) from the original signal as shown in fig.2. They are set below the human hearing threshold as a result the echo is not easily resolved. Echoes when done well can often improve the aural quality of the picture rather than distort it.

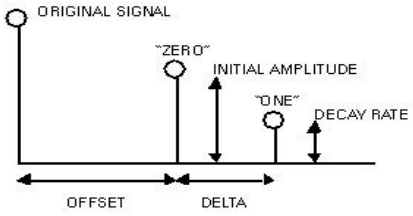


Fig.2 Parameters of echo

Offset (delay) is also varied to represent the encoded binary message. [11] One of the offset values represents a binary one, and other represents zero. If only one echo was produced from the original signal, only one bit of information could be encoded. Therefore, the original signal is broken down into blocks before the encoding process begins. Once the encoding process is completed, the blocks are concatenated back together to create the final signal. The following algorithm is used to encode each block:

- Let x=original signal
- Length(e.g. 50,000)
- offset_zero=50
- offset_one=80
- let Message=1 0 0 0 1 1 0 1 1 1 0
- Message_length=100
- Window_block=signal_length / message_length=500

The final signal is retrieved by recombining the blocks. Fig. 3 shows the implementation of the Echo-hiding process. The "one" echo signal is multiplied by the "one" mixer signal and the "zero" echo signal is multiplied by the "zero" mixer signal. The two results so obtained are added together to get the final signal. The final signal is less abrupt than the one obtained using the first echo hiding implementation. This is because the two mixer echoes are complements of each other and that ramp transitions are used within each signal. These two characteristics of the mixer signals produce smoother transitions between echoes.

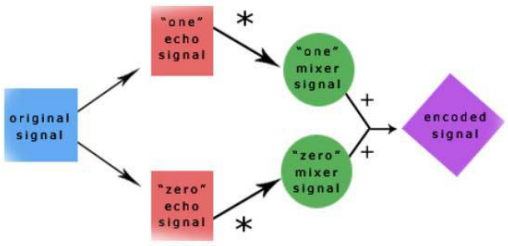


Fig. 3 *Implementation of the Echo-hiding process*

IV. APPLICATIONS

It is truely said that if you can¶t avoid a problem then join it. The 9/11 attack was made possible with the use of Steganography tools. To carve a diamond, another diamond is required, so to combat the attacks, the constructive Steganography is required. The stego data obtained from MATLAB script can be processed to imply upon the time Considerations. Then using a compatible editor, it can be downloaded to a smart image phone. In this case the hidden message could be any ones contact details or any other message that can be transmitted from the sender to the recipient through blue-tooth or through UMTS network. If the stego file is transmitted through the UMTS network then there is no doubt about the authenticity and robustness as it is hardly possible to break the encryption

of UMTS network. The recipient on the other end can retrieve the message from the stego file and can get the information. Another important feature is that, only recipient has the key to decode the image file, so the interceptor may get only the cover image file and not the hidden text inside.

Another application of Steganography/Water-marking lies in military/electronic war-fare situations. Secret water-mark can be embedded inside the image file or image file showing the map of enemy or any such sensitive information. Only the intended recipient can decode the file and can have the access.

V. EXPERIMENTAL RESULTS:

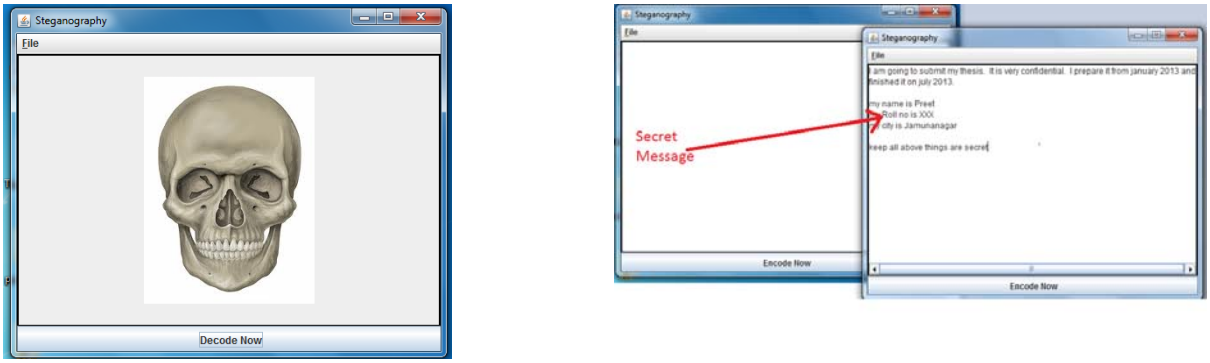
This section compares the image quality of medical images that were embedded with a variety of messages. First, the three test images are presented. This is followed by a discussion on the watermarks that have been hidden in the images. The quantitative image quality results of each experiment are shown next. Finally, the appropriateness of each watermarking system for medical image data is dis-cussed.

The medical images were used in the watermarking experiment. The image is from a Magnetic Resonance Imaging (MRI) modality and from a Com-puted Tomography (CT) modality. Note that the images vary in size: 470 × 579 for the MRI image and 1022 × 689 for the CT and CXR images.

Four different watermarks were embedded in the med-ical images: text files with 108 and 1080 characters each, and JPEG images of size 4kb and 40kb. The text files were hidden in the images to test the image quality difference be-tween embedding a text file, and another that is ten times larger, in an image. The same type of experiment was repli-cated with the image watermarks

Fig results of embedding the four wa-termarks in each of the medical images. Before analysing the results, some notes must be made about the outcomes. Firstly, JPHide was not able to produce results for the MRI data. Secondly, program informs the user if a watermark is too large to embed in an image (in the sense that the watermark will cause significant visible distortio ns in the image). This was the case when embedding the 40kb logo in the CT and CXR images, and hence the results are shown in parentheses. The results are included for com-pleteness, and to compare JPHide with the other two sys-tems. Note also that in many cases, both MSE and MAE provide the same quantitative values. This is due to the bi-nary nature of the images. Both sets of results are shown to emphasise the weakness of JPHide when embedding the logo within the medical images.

Some general observations can be made about the out-comes. Firstly, image quality degrades as more data is embedded in an image. Secondly, increased water-mark robustness is related to a decrease in image quality, as expected. Some specific results are now presented, by considering each quality metric separately.



(a) (b)

Figure 2. Test data: (a)Original image (b) Message LSB

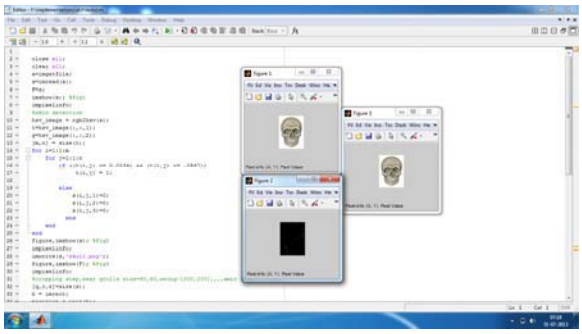


Figure3 .dct

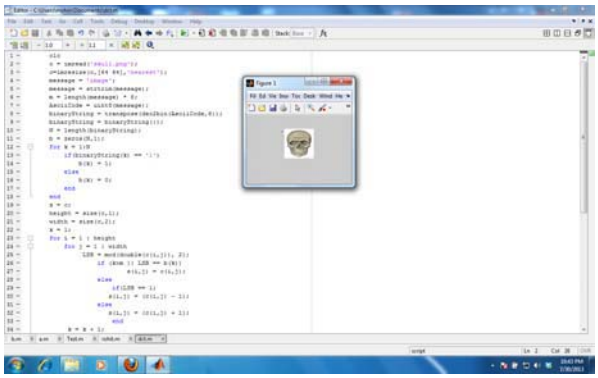


Figure 4. Spread Spectrum

JPHide pro-duced much higher values than other systems for the CT and CXR images, due to the 'heaviness' of the embedding, which greatly increased the amount of information in the stego images.

An interesting anomaly occurred in the *PSNR* results for watermarked MRI image. The PSNR values were very low, although all four other metrics indicated that S-Tools embedding provided minimal image degradation. The reason for the result is unknown.

From the discussions above, some general conclusions have been reached about medical image watermarking, using these approaches. Firstly, LSB encoding generally provides less image degradation than DCT. Sec- ondly, more research is required before systems such Spread Spectrum method, which provide minimal image degradation, are used to embed watermarks in the images. This is because even high quality stego images may have small changes in image pixel values, which can change the interpretation of the im-age. Note that image interpretation is used by radiologists for diagnosis and in imaging applications such as automatic image segmentation.

An example where the same watermark will produce different effects on two different image types is using LSB embedding for (1) X-ray and (2) Ultrasound images. Image enhancement, a common operation on the X-ray images.

VI. CONCLUSION

This preliminary study has shown that medical image watermarking is still an open field of research. This is primarily due to the special nature of the images, which should not be perceptually altered. The study compared three wa-termarking systems, applying their techniques to hide data in medical images. As expected, watermark robustness is related to a decrease in image quality. Also, even stego images from the most fragile system.

From the discussions above, some general conclusions have been reached about medical image watermarking, using these approaches. Firstly, LSB encoding generally provides less image degradation than DCT. Sec- ondly, more research is required before systems such Spread Spectrum method, which provide minimal image degradation, are used to embed watermarks in the images.

REFERENCES

[1] B. Macq and F. Dewey. Trusted headers for medical images. In DFG VIII-D II Watermarking Workshop, Erlangen, Germany, Oct. 2010.

[2] A. Maeder and M. Eckert. Medical image compression: Quality and performance issues. SPIE: New Approaches in Medical Image Analysis, 3747:93–101, 2012.

[3] M. Nishio, Y. Kawashima, S. Nakamuar, and N. Tsukamoto. Development of a digital watermark method suitable for medical images with error correction. RSN Archive Site: http://archive.rsna.org/index.cfm,. accessed 18 January 2010.

[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): 488-497.2010

[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] N.F. Johnson, S. Jajodia, Exploring steganography: seeing the unseen, IEEE Computer 31 (2) (1998) 26–34.

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

[8] P. Moulin, R. Koetter, Data-hiding codes, Proceedings of the IEEE 93 (12) (2005) 2083–2126.

[9] D. Kahn, The codebreakers: the comprehensive history of secret communication from ancient times to the Internet, Scribner, December 5, 1996.

[10] J.P. Delahaye, Information noy_ee, information cach, Pour la Science 229 (1996) 142–146 /www.apprendre-en-ligne.net/crypto/stega no/229_142_146.pdfS (in French).

[11] Bruce Schneier. Applied Cryptography. JohnWiley & Sons, New York, 1995. ISBN 0-47111-709-9.

[12] Neil F. Johnson and Sushil Jajodia. Exploring steganography: Seeing the unseen. IEEE Computer, 31:26–34, Feb 1998.

[13] Rafael C. Gonzalez and Richard E. Woods. *Digital Image Processing*. Prentice-Hall, Boston, MA, USA, second edition, 2002. ISBN 0-20118-075-8.

[14] Peter Wayner. Disappearing cryptography. Morgan Kaufmann Publishers, San Francisco, CA, USA, second edition, 2002. ISBN 1-55860-769-2.

[15] Sara V. Hart, John Ashcroft, and Deborah J. Daniels. Forensic examination of digital evidence: a guide for law enforcement. Technical Report NCJ 199408, U.S. Department of Justice – Office of Justice Programs, Apr 2004.

[16] Sheridan Morris. The future of netcrime now (1) – threats and challenges. Technical Report 62/04, Home Office Crime and Policing Group, 2004.

[17] Anderson Rocha and Siome Goldenstein. Progressive Randomization for Steganalysis. In 8th IEEE Intl. Conf. on Multimedia and Signal Processing, 2006.