International Journal of Engineering Research and General Science Volume 3, Issue 5, September-October, 2015
ISSN 2091-2730

Hiding The Results of Medical Test in Medical Digital Image

Orooba Ismaeel Ibraheem Al-Farraji

Orooba1@gmail.com

Abstract— Digital image steganography has been proposed as a method to enhance medical data security . confidentiality and integrity . Medical image steganography requires extreme care when embedding additional data within the medical images because the additional information must not affect the image quality. Many of the exploration systems used for medical diagnosis are based on the medical study images.

Keywords— medical Image, results of medical tests, steganography, text in Image steganography , Information Hiding

INTRODUCTION

Steganography is an art and science of invisible communication [10].In recent years image steganography has become an important research area in data security , confidentiality and image integrity. Medical image steganography requires extreme care when embedding additional data within the medical images because the additional information must not affect the image quality.

Medical images are stored for different purposes such as diagnosis , long time storage and research .

In the medical field the importance of the medical data security has been emphasized , especially with respect to the information referring to the patients (personal data, studies and diagnosis) [1]. On other hand the amount of digital medical images transmitted over the internet has increased rapidly , on the other hand the necessity of fast and secure diagnosis is important in the medical field ,i.e telemedicine, making steganography the answer to more secure image transmission . For applications that with images , the steganography aim is to embed invisible message in an image.

USES OF STEGANOGRAPHY

Steganography can be used anytime you want to hide data. There are many reasons to hide data but they all boil down to the desire to prevent unauthorized persons from becoming aware of existence of message. In the business world Steganography can be used to hide a secret chemical formula or plans for a new invention. Steganography can also be used for corporate espionage by sending out trade secrets without anyone at the company being any the wiser. Steganography can also be used in the non-commercial sector to hide information that someone wants to keep private. Spies have used it since the time to pass messages undetected [1].

The healthcare industry and especially medical imaging systems may benefit from information hiding techniques the use standards such as DICOM (digital imaging and communication in medicine) which separates image data from the caption, such as the name of the picture is lost, thus, embedding the name of the patient in the image could be a useful safety measure [5].

DIGITAL MEDICAL IMAGE

A digital image is a two dimensional function, f, that takes an input two spatial coordinates x and y and returns a value f(x,y). The value f(x,y) is a gray level of the image at that point. The gray level is also called the intensity.

Digital images are a discretized partition of the spatial images into small cells which are referred to as pixels - picture elements.

Medical imaging is a field where researchers develop tools and technology to acquire, manipulate and archive digital images which are used by the medical profession to provide better care to the patients.

THE NEW PROPOSED SYSTEM

The new proposed system take as input the embedded-object which in our case file of text and the cover object which is either a 256 color-image or gray scale image (size 640 x 480).

We use in our case an 8-bit image and since 8-bit image and since 8-bit values can only have a maximum of 256 colors the image must be chosen much more carefully.

BACKGROUND

Steganographic software is new and very effective. Such software enables information to be hidden in image, sound and apparently "blank" media.

In the computer, an image is an array of numbers that represent light intensities at various points in the image. A common size is 640 by 480 and 256 colors (or 8 bits per pixel). Such an image could contain about 300 kilobits of data [3].

There are usually two types of files used when embedding data into an image. The innocent looking image which will hold the hidden information a "container." A "message" is the information to be hidden. A message may be plain-text, cipher text, other images or any thing that can be embedded in the least significant bits (LSB) of an image.

For example: Suppose we have a 24-bit image 1024 x 768 (this is a common resolution for satellite images, electronic astral photography and other high resolution graphics). This may produce a file over 2 megabytes in size (1024x768x24/8 =2,359,296 bytes). All color variations are derived from three primary colors, Red, Green and Blue. Each primary color is represented by 1 byte (8 bits). 24-bit images use 3 bytes per pixel. If information is stored in the least significant bit (LSB) of each byte, 3 bits can be a stored in each pixel. The "container" image will look identical to the human eye, even if viewing the picture side by side with the original. Unfortunately, 24-bit images are uncommon (with exception of the formats mentioned earlier) and quite large. They would draw attention to themselves when being transmitted across a network. Compression would be beneficial if not necessary to transmit such a file. But file compression may interfere with the storage of information.

THE NEW PROJECT OPERATION

The embedding process of new system has many operations:

Select cover image, by taking the medical image for specific patient stored previously.

Input the results of medical tests to be hidden that can be done by open new file and entered directly or by select a previous stored file.

Open –cover (bmp file) and split the body to blocks , we split the body in order to obtain small number of position to be easy in hide.

Find the position where to hide the bytes of the text in the blocks of image (cover) and store the block numbers and the number of position in file to use later.

Substitute the character in the position get from the search program, in fact the substitution it merely locate the position that hide in it.

Hide position will hide the block numbers where the character was hidden.

Combine the blocks into a one file and then combine the header and the body file into a file to perform the stego-object (bmp file).

The new proposed system has a key which is used to extract the embedding image from stego –image. , the key is the size of text file and number of position we began hide in it the second key is transferred separately.

In figure (1) shows the flowchart of system.

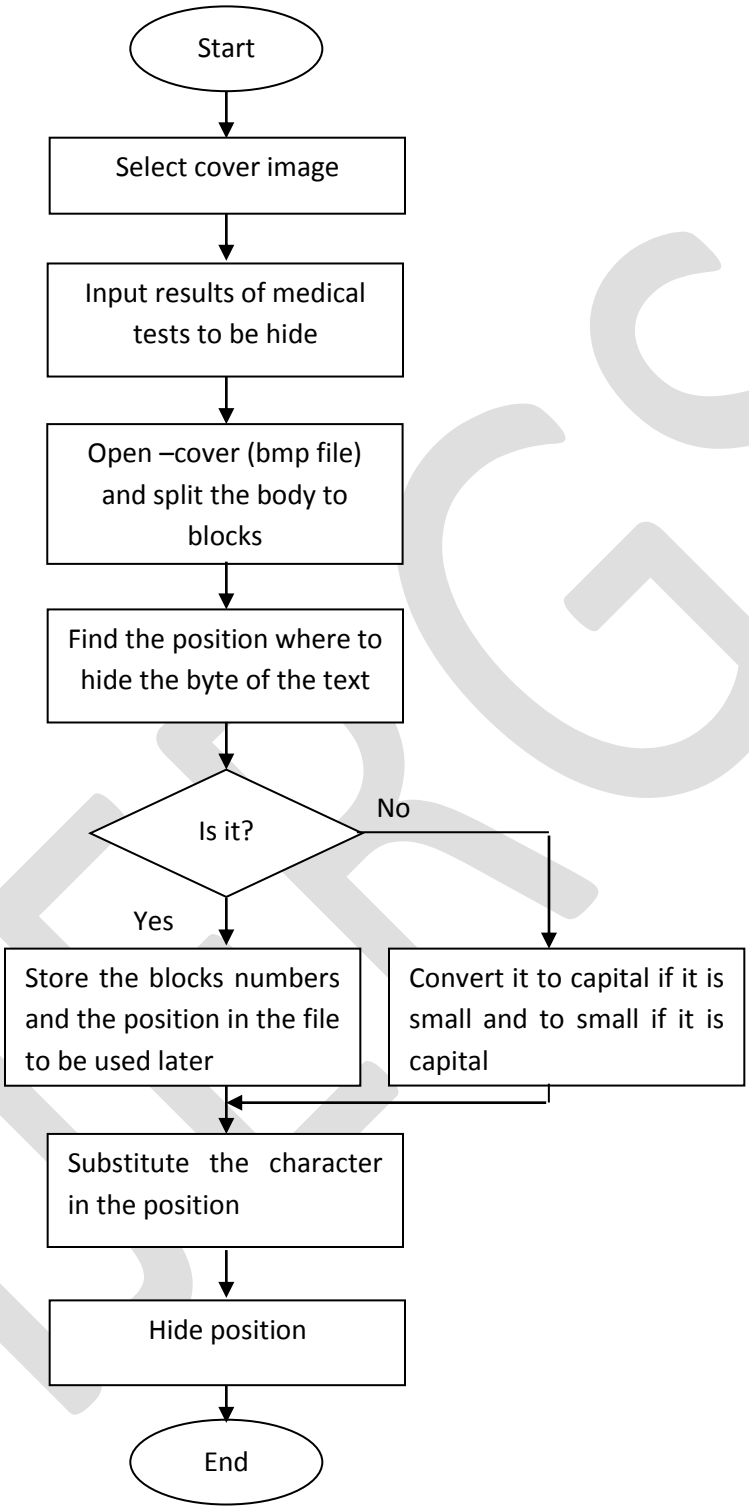

Figure (1) Flowchart of the system

The following steps describe the algorithm:

Step1- Open Cover (the bmp-file) Operation

This operation will open the bmp file and save header in a file and save the palette value of body in another file.

Step2- Split the body of the image file operation

This operation will split the body image in equal blocks to use these blocks in hide medical tests, we split the body in order to obtain small number of position to be easy in hide.

Step3- Find the position operation this operation is done by read a block from block image file and test if block is suitable to hide a byte from text file or not. The testing is done by compare the value of the palette with ASCII value of character. Then we find the position that we hide the character and save the block number and position in a file.

Step4- Substitute the character operation this operation is done by read character from text file and locate the position was to hide the character in the block. Replace the character in specific position and hide the position of the replaced character in the first row and last row of the block.

To find the coordinates (i.e., row and column number) of position we apply the following equations:

R= pos div 20 ……1

R: row

Pos: position in array

The equation for the column position is:

C= pos mod 20 ……..2

C: column

We substitute the row value that is calculated, from equation 1 into the current block that we search on it. We substitute it into first row (in LSB). While for the column value that is calculated from equation 2, we substitute it into last row of the current search block .we substitute it into LSB, in this operation the substitute of character don't change any thing in the pixel because the value of pixel in the palette equal to ASCII value of character, only change the places in the picture that we substitute the position of character in it. This change is unnoticeable because the number of position is small and substitute in LSB.

7 EXTRACTING THE EMBEDDING TEXT

Extracting the text is done by using the key stored into first block position that contains the key which is the length of the text that is hidden in the image.

Later get the row position from the first row and convert the binary value to a decimal value and in the same way we position by applying the following equation

Pos =(r+1) * 20- (20-c)

Get the character value from the specific position.

The following steps describe the algorithm:

Step1- Open the bmp file by reading the header and getting the body of the file

Step2- Split the file into blocks

Step3- by using the key get the first block that contains the first byte of the text.

Step4- Read the second byte of the key (which is the length of the text that is hidden in the image)

- For I= 1 to the length of the message do

Step5- Find the position of the embedded character from the first and the last row of the block.

Get the row position from the first row.

Convert the binary value to a decimal value.

Get the column position from the last row

Convert the binary value to a decimal value, get the position by applying the following equation:

Pos =(r+1) * 20- (20-c)

Get the character value from specific position.

Step6- From the current block find the position of the next block.

The number of the block is hidden in the first row (the second half) and the second half of the last row.

Step7- The end

EXPERIMENTAL RESULTS

The proposed system has been built using Borland C++ and can run on Pentium I computer and above, the setting of screen must be 800 X 600.

The results of the proposed system has been illustrated in the following

EXAMPLE

The medical test results size 110 character with space is:

RBC = 0-I/HPF , Pus cell= I-3/HPF , Casts=Nil ,Crystals= Amorph.ueate(+) Ca.oxalate(Few), Epi.Cell: Few, Other: Mucus(+)

And the gray scale image 640X 480 pixels so as mentioned previously shown in figure (2).

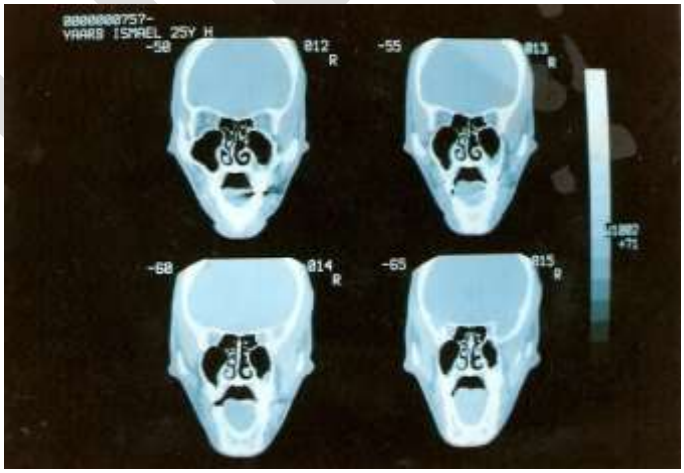

Figure (2): CT-scan Image (before Steganography)

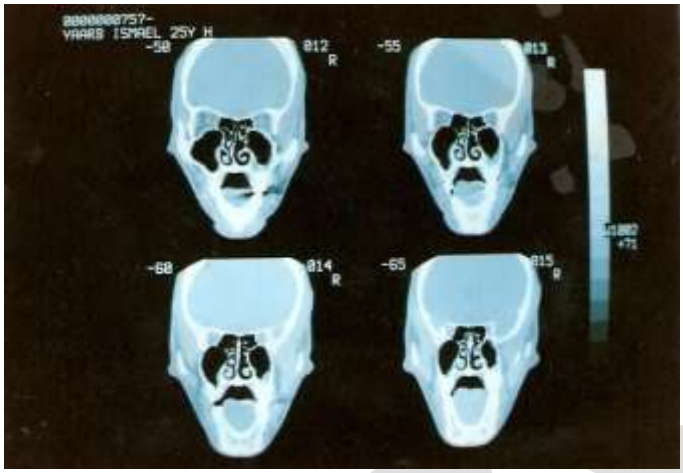

Figure (3): CT-scan Image (After Steganography)

Experimental Results And Performance Analysis

Use PSNR Function to Test the results

Signal to Noise Ratio (PSNR) is generally used to analyze quality of image, sound and video files in dB (decibels). PSNR calculation of two images, one original and an altered image, describes how far two images are equal. Figure 5 shows the famous formula.

MSE: Mean-Square error.
x: width of image.
y: height.
x*y: number of pixels (or quantities).

This function displays the PSNR (peak signal-to-noise ratio) between two images. The answer is in decibels (dB).

PSNR is very common in image processing. A sample use is in the comparison between an original image and a coded/decoded image. Typical quoted PSNR figures are in the range +25 to +35dB.

The syntax for this file is PSNR(A,B), where A and B are MATLAB Intensity Images, with matrix-elements in the interval [0,1]

$$PSNR(dB) = 10 * \log(\frac{255^2}{MSE})$$

$$MSE = \sum_{i=1}^{x}\sum_{j=1}^{y}\frac{\left(\left|A_{ij} - B_{ij}\right|\right)^2}{x * y}$$

.**PSNR formula**.

In watermarking. We asked each one of them of she/he could tell a watermarked image if they are presented with a pair of same size images printed on a piece of paper, one watermarked and the other not. None could tell the watermarked image from the non-watermarked image.

In order to observe the image quality of watermarked image objectively, the PSNR (Peak Signal to Noise Ratio) value of the image is calculated using the equation 3 and if the PSNR value is greater than 35dB, the watermarked image is within acceptable degradation levels.

PSNR =10×lg((2*n* −1)2 /*MSE*) (3)

Where *n* means the number of bits per sample value, the *MSE* represents mean square error between the host image and the watermarked image.

By using Matlab we input figure(2) and figure(3) to function PSNR the results equal 28.722 db and this value acceptable.

CONCLUSIONS

The proposed system proved to be a good system used to hide a text in medical digital image by compare value of palette with ASCII of character and if equal we hide position un another Place .

- In the proposed system transfer the medical image with The Results of Medical Test in high security

- The proposed system proved to be easy to use and efficient in terms security and hide every things about the patients.

- the proposed connect the computer science with medicine by useful a way and help in transfer medical information among the doctors in different country .

REFERENCES:

[1] G. Coatrieux et al. "Relevance of watermarking in Medical imaging " In IEEE embs Information Technology Applications in Biomedicine , Arlington, USA. 2000, pp. 250-255.

[2] Mike cry " Font color Steganography" , May ,11,2009

[3] Francesco Queirolo "steganography in Images", final communications Report, visited on : 26-2-2002, http://google.yahoo.com/bin/

[4] Johnson, Neil F., Duric, Zoron, Jajodia, "Information Hiding steganogarphy and watermarking- Attacks and Countermeasures" , Kluwer Academic Publishers., 2001

[5] Johnson, N.A., "Steganography", visited on: 2-2-2002. http://www.jjtc.com/stegdoc/indexz.html

[6] Johnson, N. F. "steganograhpy " , visited on: 18-2-2002. http://www.jjtc.com/stegdoc/sec313.html

[7] Katzenbeisser S. and petitcolas F., "Information Hiding Techniques for . steganograhpy and Digital Watermarking ",Artech House, USA 2000.

[8] Stevens, Roger T. "Graphics Programming in C",BPB Publications, 1993.

[9] Rodriguez-Colin Raul, Feregrino-Uribe Claudia, Trinidad-blas Gershom de J. "Data Hiding Scheme for Medical Images", Luis Enrique Erro No. 1 Sta . Maria Tonantzintla, Puebla, Mexico C. P. 72840 , 2008

[10] Shuliang Sun[1,2], "A New Information Hiding Method Based on Improved BPCS Steganography" , Volume 2015 , Article ID 698492, 7 pages , 2015