International Journal of Computational and Applied Mathematics. ISSN 1819-4966 Volume 12, Number 1 (2017)

PERFORMANCE OF STEGANOGRAPHIC METHODS IN MEDICAL IMAGING

V.Mahalakshmi[1] S.Satheeshkumar[2] Dr.S.Sivakumar[3]

[1]*Assistant professor, Department of Computer Science & IT, C. P. A College, Bodinayakanur, mahamsc91@gmail.com*

[2]*Research Scholar, Department of Computer Science, C.P.A. College, Bodinayakanur, satheeshvasan007@gmail.com*

[3]*Associate Professor and Head, Department of Computer Science, C. P. A College, Bodinayakanur. sivaku2002@yahoo.com*

ABSTRACT

The rapid development of data transfer through internet has made it easier to send the data accurate and faster to the destination. Unauthorized users modify and misuse the valuable information through hacking. So, in order to transfer the data securely to the destination without any modifications, there are many approaches like Cryptography, Steganography, etc. In the information era, information sharing and transfer has increased exponentially. The information vulnerable to unauthorized access and interception, while in storage or transmission. Steganography is the major technique for secret communication. In research work, image steganography and its different security methods to secure a medical image, particularly Magnetic Resonance Imaging (MRI). In steganography, the contents of the secret message is embedded into the cover medium. Three different steganographic algorithms is used, Least Significant Bit (LSB) algorithm, Division into block and Mean change modified method. The measurements are SSD (Sum of Squares of Differences), SAD (Sum of Absolute Differences), MAD (Maximum Absolute Differences) and Peak Signal to Noise Ratio (PSNR) are used to comparing them in terms of speed and accuracy.

Keywords: Steganography, Cryptography, MRI, LSB, Division into blocks.

1. INTRODUCTION

Computers are as secure as real world systems, and people believe it. Security that guarantees to stop bad things from happening, and the main reason is that people don't buy it. Information Security concerns, critically discuss the properties, which help to transmit the data or information over a network without any modifications. The characteristics of information are availability, accuracy and authenticity.

Security is splitted to cryptography one part and the other part is Information hiding. Information hiding techniques have recently become important in a number of application areas. Digital audio, video, and pictures are increasingly furnished with distinguishing but imperceptible marks, which may contain a hidden copyright notice or serial number or even help to prevent unauthorized copying directly[1].

There are various applications in Information hiding trechnique. They are Steganography, Cryptography and Watermarking. Steganography differs from cryptography in the sense that where cryptography focuses on keeping the contents of a message secret, steganography focuses on keeping the existence of a message secret. Once the presence of hidden information is

revealed or even suspected, the purpose of steganography is partly defeated. The strength of steganography can thus be amplified by combining it with cryptography.

The word steganography is of Greek origin and means "covered, or hidden writing". "Steganography is the art and science of communicating in a way which hides the existence of the communication. In contrast to Cryptography, where the enemy is allowed to detect, intercept and modify messages without being able to violate certain security premises guaranteed by a cryptosystem, the goal of Steganography is to hide messages inside other harmless messages in a way that does not allow any enemy to even detect that there is a second message present"[2].

The information-hiding process in a steganographic system starts by identifying a cover medium's redundant bits (those that can be modified without destroying that medium's integrity). The embedding process creates a stego medium by replacing these redundant bits with data from the hidden message. Essentially, steganographic communication senders and receivers agree on a steganographic system and a shared secret key that determines how a message is encoded in the cover medium[3]. The scope of Steganography is to reliably send hidden information secretly, not merely to obscure its presence[4].

2. MATERIALS AND METHODS

There are various applications to secure an image[5]. Here medical applications is used, particularly in an application of MRI (Magnetic Resonance Imaging) scanning. MRI images of the brain image is taken as an input image. Fig. 2 shows MRI brain image collected. It is of 24-bit of 251×244 dimension.

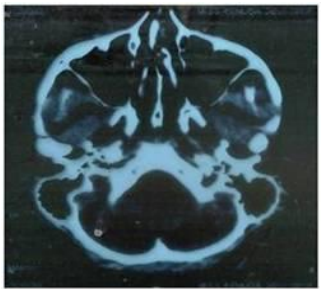


Figure 1: MRI Image: Brain

Steganography in computer era is considered a sub-discipline of data communication security domain. Modern techniques of steganography exploit the characteristics of digital media by utilizing them as carriers (covers) to hold hidden information. Covers can be of different types including image, audio, video, text. The sender embeds data of any type in a digital cover file using a key to produce a stego-file, in such a way that an observer cannot detect the existence of the hidden message[5]. At the other end, the receiver processes the received stego- file to extract the hidden message. The basic steps involved in Steganography is shown in Figure.

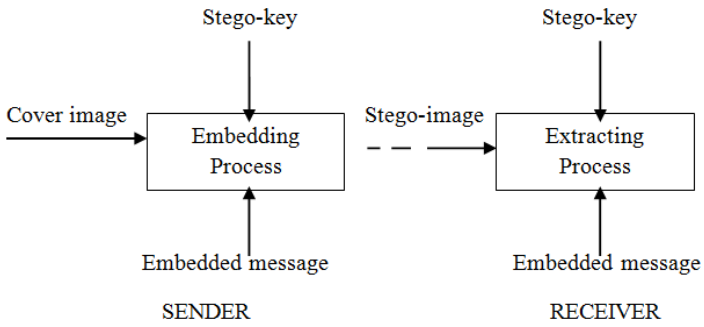


Figure 2: Conceptual diagram of steganography

The cover-Image is an original image which is used as a carrier for hidden information. Stego-image is used to embed the message into cover image. Stego-key is used to hide the information. Embedded image is refers to the amount of data that can be inserted into the cover-media without deteriorating its integrity.

Three steganographic methods are described and later assessed for usability in medical imaging.

1. The Least Significant bit Insertion
2. Division into Blocks and Mean Modification
3. Mean Change Modified method

3. THE LEAST SIGNIFICANT BIT INSERTION

The LSB assumes that information in a 24-bit digital image is represented by an array of triplets, and these triplets correspond to intensities of red, green and blue (RGB model). Each pixel of the image can be described by a triple of values associated to each color. In the case of 8-bit images, the image is represented by an array of grayscale values. The least significant bit insertion method is the most obvious and also the most well-known for hiding information in images. The change of the least significant bit should cause an image alterarion that is barely noticeable.

Step 1 : Consider the binary representation of information S to be hidden.
Step 2 : The least significant bit of each pixel in the image is overwritten by $S_i \varepsilon X =$ *{0,…….,*$2^{nc} - 1$*}, for* $1 \leq i \leq |S|$ *and* n_c *is the number of bits in graphical palette. So*

$$S_i = \sum_{k=1}^{nc} b[i,k].\,2^{nc-k}$$

Step 3: (b[i,1] b[i,n_c]) is the binary representation of S_i and b[i,n_c] is least significant bit

4. DIVISION INTO BLOCKS AND MEAN MODIFICATION

We can divide the image manually in the paint and taking equal part at a time, but method is too tedious and is neither too accurate. So, the simpler way out is to use MATLAB to do the job for us. So here we will be dividing the image into multiple parts (nXm) and then uploading all the images, so that when we insert them in the chat we get a Jumbo Image in the chat box comprising of various small images that we had uploaded earlier.

Step 1 : Let B a block of size mxn, the mean value of this block will be changed to represent the k-th bit of S.

Step 2 : Calculate the mean value M_i of block B, calculate $M_{Si}(j)$, which corresponds to the j-th mean center of the spectrum with the symbol S_i; calculate the new mean

$$M_d(i) = \arg\min |M_{Si\,(j)} - M_i|$$

Step 3 : Let $\Delta M(i) = M_d(i) - M(i)$ corresponds to the change to be produced in each pixel of B, aiming the lowest possible degradation in the image and also pointing to the bit that stores information S_i.

Step 4 : Otherwise, each bit 0 is obtained from the equation K/2 + 2Kt and each bit 1 is obtained from 3K/2 + 2Kt, where K is the width of the spectrum.

Step 5: Finally, the elements $B_{ij} \leftarrow B_{ij} + [\Delta M(i)]$

5. MEAN CHANGE MODIFIED METHOD

Seeking an improvement to the algorithm proposed in the previous subsection, Mortazavian et al. devised a technique that shuffles the image pixels prior to steganography. This minimizes the block effect, and adds security. The generator of pseudo-random numbers shuffles the pixels according to a certain seed. This seed can be seen as a key shared between Alice and Bob. In addition, the algorithm must reduce (or increase) the grayscale intensities of pixels being modified until expected mean is reached.

However, this algorithm must avoid substantial changes to a particular region. For that, a switch mode that will be constrained by a certain threshold is used, so the algorithm will not reduce the grayscale palette by a large amount to achieve expected mean if that degrades the image, but it will increase intensities of each pixel so that total change required is reached.

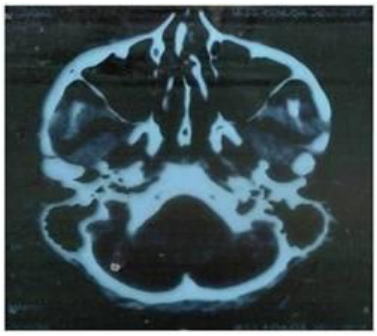
Step 1 : N1: number of pixels whose values are above $\Delta M(i)$, those to be modified.

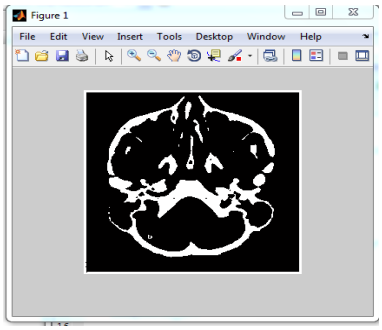
Step 2 : ΔG_T : amount of alteration required to mean of block be closer to $M_d(i)$, given by $\Delta G_T = |\Delta M(i)|.N$, where N is total number of pixels.

Step 3 : $M_{d2}(i)$, $\Delta M_2(i)$, N2 and ΔGT_2 are defined equivalently by $M_d(i)$, $\Delta M(i)$, N1 and ΔG_T in switch mode

6. RESULTS AND DISCUSSION

Using the method of Least Significant Bit Insertion, the results are not satisfactory for medical imaging applications. In this embedding scheme, only the LSB plane of the cover image is overwritten with the secret bit stream. As a result, and thus it is very easy to detect the existence of hidden message even at a low embedding rate using some reported steganalytic algorithms.

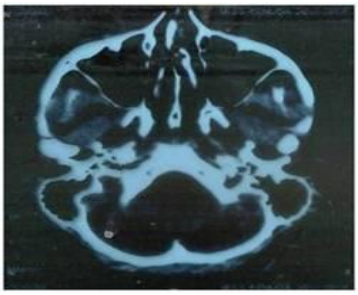


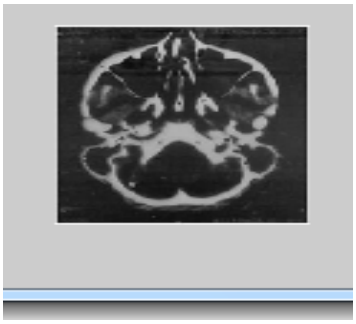


(a) Original Image of brain image (b) Stego image of LSB

Figure 3: Original image and Stego image

The division into block method is addressed by shuffling the image prior to embedding the data. This method decreases the grey-level value of modifiable pixels successively until the total necessary alteration is met, but in the same time it prevents the maximum alteration of each pixel.

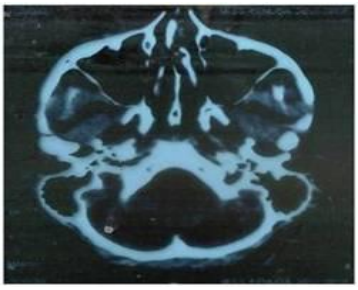


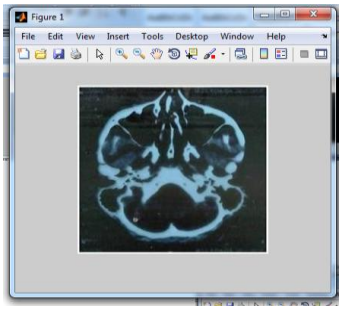


(a) original Image of brain image (b) Stego image of Division into Block

Figure 4: Original image and Stego image

The pixel value increased, so the mean modification method increases the grey level values of the pixels which are modifiable in the pixels with grey-level values less than one by one until the total amount of modification reaches, which means that the mean of the block has reached.





(a) Original Image of brain image (b) Stego image of Mean Modification

Figure 5: Original image and Stego image

Image analysis is the extraction of meaningful information from images. Image Analysis can involve the calculation of an image transformation achieved by optimization of some measure computed directly from intensity values of the images. Accurate definition of similarity measure is a key component in image analysis. Most commonly used intensity-based similarity measures, including Sum of Squares of Differences (SSD), Sum of Absolute Differences (SAD), Correlation Coefficient (CC), Maximum Absolute Differences (MAD), Correlation Ratio (CR), Mean Square Error (MSE), Peak Signal to Noise Ratio (PSNR) and Mutual Information (MI), rely on the assumption of independence and stationarity of the intensities from pixel to pixel

Four criteria were considered to compare the resultant images with the input.

Sum of Squares of Differences (SSD)

$$SSD = 1/N \sum_{i,j} |A_{ij} - B_{ij}|^2$$

where matrix A correspond to the original image and matrix B corresponds to the after image steganography.

Sum of Absolute Differences (SAD)

$$SAD = 1/N \sum_{i,j} |A_{ij} - B_{ij}|$$

where matrix A correspond to the original image and matrix B corresponds to the after image steganography.

Maximum Absolute Difference (MAD)

$$MAD = 1/N \max |A_{ij} - B_{ij}|$$

where matrix A correspond to the original image and matrix B corresponds to the after image steganography.

Peak signal to Noise Ratio (PSNR)

$$PSNR = 10.\log\left[\frac{255^2}{MSE}\right] \quad \text{where}$$

$$MSE = \frac{1}{MN}\sum_{i=1}^{M}\sum_{j=1}^{N}[I(i,j) - K(i,j)]^2$$

Where max=255 is the maximum possible pixel value of the image and *M* and *N* are the number of rows and columns in the input images

The evaluation of performance of the three steganography methods by measuring the quality stego images firstly by using four criteria, SSD, SAD, MAD, PSNR. These methods are used to evaluate the quality of stego images and measured values are tabulated in Tab. 1. It measures the efficiency of a particular stego method over another in terms of imperceptibility or stego image quality. This measure has been tested and validated to be used with many image processing applications.

Image Analysis Terms	LSB Insertion	Division into Blocks	Mean Modification
SSD	1244	120	12
SAD	12	7	3
MAD	2.10×10^{-3}	10.18×10^{-3}	4.10×10^{-4}
PSNR	55.78	51.25	50.36

Table 1: Measures of LSB, Division into Blocks and Mean Modification method for MRI Brain image

7. CONCLUSION

Security is an important issue while transferring the data using internet because any unauthorized individual can hack the data and make it useless or obtain information un- intended to him. This research work proposed steganographic methods to MRI image. The application creates a stego image in which the data is embedded and is protected which is highly secured. This provides higher security and can protect the MRI image from stego attacks. In mean modification method, the image resolution doesn't change much and is negligible when we embed the image and the image is protected with the secure image. So, it is not possible to damage the data by unauthorized personnel. This provides high security and can protect the image from stego attacks with quantitative measures of the image comparison, the mean modification method produced better performance than the others. Future of Information Hiding provides an analysis of the trends that are shaping the domain of steganography and offers approaches that could help in its commercialization

REFERENCES

[1] Fabien A. P. Petitcolas, Ross J. Anderson and Markus G. Kuhn, "Information Hiding - A Survey".

[2] J.R. Krenn "Steganography and Steganalysis" January 2004,

[3] Mehdi Kharrazi, Husrev T. Sencar and Nasir Memon, "Image Steganography: Concepts and Practice".

[4] Nick Nabaviannabav "Image Steganography", 2007

[5] MariaPetrou, CostasPetrou "Fundamentals of image processing"

[6] Rohini Paul Joseph, C. Senthil Singh, M.Manikandan, "Brain Tumor Mri Image Segmentation And Detection In Image Processing".

[7] Gunjan CHUGH, Image Steganography Techniques, 2013.

[8] Alex Toumazis, "Steganography", December 3, 2009

[9] Ravinder Reddy Ch1 Roja Ramani, "The Process of Encoding and Decoding of Image Steganography using LSB Algorithm", November 2012.

[10] Shuhong Jiao, Robert Goutte, "A Secure Transfer of Identification Information in Medical Images by Steganocryptography".

[11] DG Nishimura, Principles of Magnetic Resonance Imaging, April 1996.

[12] Jessica Fridrich, Jan Kodovský, "Statistically Undetectable JPEG Steganography: Dead Ends, Challenges, and Opportunities".

[13] Sophie Engle, "Current State Of Steganography: Uses, Limits, & Implications"

[14] Akhtar, N.; Johri, P.; Khan, S., "Enhancing the Security and Quality of LSB Based Image Steganography," Computational Intelligence and Communication Networks (CICN), 2013 5th International Conference

[15] Sophie Engle,"currentstate of steganography: uses, limits, & implications" IEEE paper