ISSN: 0975-8585

Research Journal of Pharmaceutical, Biological and Chemical Sciences

Information Hiding Technique for Secure Transmission of Medical Images.

Priya S*[1], Santhi B[1], Swaminathan P[1], Abhinaya M[1], Suppriya V[1], and Raja Mohan J[2].

[1]School of Computing, [2]School of Electrical and Electronics Engineering, SASTRA University, Thanjavur, Tamil Nadu, India.

ABSTRACT

Information hiding plays a major role in telemedicine to transmit the medical data in a secured manner among specialists for diagnosis and treatment. In which electronic patient information (EPI) is embedded within a medical image and transmitted to the remote specialists. Now the specialists extract the EPI and reconstruct the medical image in a secured manner. During transmission, there is a chance to attack the medical information. So, the medical information is protected from the intentional and unintentional attack. This paper proposes a data hiding method for medical images. Using radix base value**,** the EPI is embedded within a cover medical image. Performance of the proposed method is analysed using peak signal to noise ratio (PSNR) and mean absolute error (MAE). These measures prove that the proposed method yields good results than others.

Key words: Information hiding, Stegnography, medical images, radix number, PSNR, MAE.

**Corresponding author*

INTRODUCTION

Data hiding is the technique which protects the data by embedding the secret data within multimedia data such as audio, image, video, etc. One important data hiding technique is Steganography which is to conceal the contents of the message from the attacker [1]. In telemedicine medical scanned images are transmitted to the remote specialist along with patient information. These medical data must be protected during transmission in an unsafe medium. Steganography is used to protect the medical data and at the specialist side, the secret data embedded is extracted without any loss.

Image stegnography technique is used to hide the information inside the cover image and it does not show any visual difference in the image. It can be divided into two. They are spatial domain and transform domain. In spatial domain image pixel values are directly manipulated. But in transform domain, image is manipulated through various transforms like discrete cosine transform (DCT),discrete wavelet transform (DWT), etc. The image stegnography technique was rapidly developed due to the redundancy of digital image pixels [2]. In Steganographic method the performance is concluded based on its transparency, robustness, statistical delectability and capacity [3].

Based on JPEG compression with quantization error, a stegnography technique is developed by considering the JPEG compressed image through various scaling factor. One of the scaling factors is used to control the bit rate of the stego image while the other is used to guarantee the quality of the stego image [6]. The histogram-modification method was proposed. It changes all the pixels including those pixels in which secret data is not embedded. In order to solve this problem, a threshold and neighboring pixels are used to differentiate the embedded pixels with non embedded pixels. The absolute difference is higher than the pre-threshold, then the pixel cannot be embedded with the secret data remains unchanged. In other words, the pixel is changed only when the secret data are embedded [10].

A novel interpolation technology can be applied to information hiding. Moreover, a novel reversible steganography based on the extended image interpolation technique is designed. By improving the capacity, IMNP increase the image quality. Also Its computing complexity is low and performance between interpolating pixels[4] is high. A dynamic steganographic scheme based on the concept of human vision sensitivity is capable of producing a high quality stego image according to the desired demand of the embedding capacity given by users. This scheme takes the local textural characteristics of the cover image into consideration [5].

In this paper, reversible medical image stegnography technique is proposed for secret data sharing that facilities high payload capacity with minimum perceptual distortion and also resisting visual detectability. First, the embedding procedure dynamically divides the original image into a number of non-overlapping sub-blocks sized i × j, such as 3 × 3. Then the cover image is generated and the secret data can be embedded into a cover image. On the receiver side the embedded numerals are exhumed and reunited to recover back the message. The proposed method operates on a different numeral system called Varying Radix Numeral System (VRNS) and Adaptation and Radix (AIHR) whose basics are described in Section 2. Section 3 narrates the embedding and extracting procedures of the proposed algorithm. The experimental results are discussed in Section 4.

Related Work

Varying radix numeral system based adaptive image steganography (VRNS)

A digital image is a combination of signals which holds different frequency level. Basically the low frequency signal lies in the flat and plane areas and the high-frequency signal present in the edges and sharp ends. Only fewer changes are made in low frequency region, because it is more susceptible to human eye and the embedding capacity is low. So, a large amount of informations are embedded in high frequency region.

Low-frequency region pixels range is similar with its neighboring pixels range, **but high**-frequency region pixels are not similar with neighboring pixels. So, this pixel relationship is used to calculate the amount of secret information. Using variable radices, the embedded secret data is changed into various information. By the embedded adjacent pixels, these radices are determined randomly. Larger radix will be used for the complex adjacent relationship.

Adaptation and radix (AIHR)

In ARHS scheme, the secret data is embedded within the cover image and the output is obtained from a stego image. The setgo image quality is not affected with high capacity after embedding the secret data**.** Redundancy of images in some pixel **is** similar to the adjacent pixel values. In order to reduce the difference values between adjacent pixels, the results of redundancy from an effective image hiding method is used to maximize the embedding capacity to the larger and more.

Consider an original image of size HXW. Number of non-overlapping sub-blocks of size hXw is divided from an original image. For each block, diagonal pixel is selected as the unvaried pixel (or pivot pixel) such as Ir. The number of pixels in which secret information is concealed and using unchanged pixels and the other pixels, a pixel value differences is evaluated by unvarying pixels. And then, the cover image is embedded with secret information, then the stego image is obtained. By reversing the embedding process, the secret data is extracted.

METHODS

By improvising the model of the data hiding technique, this paper promotes the payload capacity with minimum perceptual distortion. In figure 1, the proposed method general procedure is shown. It shows that how the cover medical image is produced from the original medical using varying radices and then secret information (EPI) is hidden to get a stego image as output. At the receiver side, from the stego image, the EPI is extracted and original medical image is reconstructed. The better performance of the algorithm provides high payload capacity, good image quality and higher capacity. It gives the better relation between cover image and the input image. In order to achieve this goal, the proposed method provides better image hiding technique in order to improve reduce the distortion level.

The secret message to be embedded is converted into a sequence of numerals using varying radices. The most widely used radix is decimal system with radix r = 10 and is the language of mathematics. Binary system having radix r = 2 is used internally in all computers and in digital circuitry. These radices are determined by the neighborhood of pixels. The secret message is embedded into pixels at a rate of one numeral per block. Thus, the embedding capacity is improved. This paper uses the effective technique to increase the embedding capacity of the image. The embedding and extracting phases examples are described in the following sub section.

Data hiding scheme

Let I be an original medical image with size H × W and it is divided into number of blocks **with** each block size is 3X3. Then cover medical image C of size HXW is produced using varying radices. This cover image is used for hiding secret information. The cover image block C of size 3X3 can be formed from equation (3,4).

$q_0 = \mathrm{mod}\ (wk, R_0)$ (1)
$q_i = \mathrm{mod}\ ((wk - q_i - 1)/R_i - 1, R_i)$, i =1 to 3 (2)
$p(m(1,1)) = m(1,1) - \mathrm{mod}\ (m(1,1), l)$ (3)
$c_i = m_i - \mathrm{mod}\ (m_i, R_i)$ i=0 to 3, l=4 (4)

The cover image block pixel (p) in (1,1) position is used as an unchanged or pivot pixel in which no secret information is hidden, but number of radices are hidden. x_i, y_i and z_i information is described in equation**(5)**.

$x_i = c_i - R_i + q_i$
$y_i = c_i + q_i$ (5)
$z_i = c_i + R_i + q_i$, i= 0 to 3
The stego image (S) formation is described in equation-6.
$I_i - x_i \leq y_i - I_i \wedge (I_i \in [m(1,1)])$
$_{Si} = I_i - x_i > y_i - I_i \wedge (I_i \in [m(1,2)])$ (6)
$I_i - y_i \leq z_i - I_i \wedge (I_i \in [m(2,1)])$

$l_i - y_i > z_i - l_i \wedge (l_i \in [m(2,2)])$ i = 0 to 3

$q_i = \mathrm{mod}\,(S(x,y),R_i)$ i= 0 to 3, x = 0 to 3, y = 0 to 3 (7)

$wk = q_0 + q_1 \times R_0 + q_2 \times R_0 \times R_1 + q_3 \times R_0 \times R_1 \times R_2$ (8)

Pseudo code:

Embedding:

```
Input   : Original medical image (m), secret data (wk), radix value (R).
Output: Stego image.
Step 1: Divide the original image into number of blocks with each block size is 3x3.
Step 2: Generate the cover image using equation (3) and (4).
Step 3: Embed secret information within a cover image using equation (1),(2),(5) and (6).
```

Extraction:

```
Input   : Stego image (S), radix value (R).
Output: Secret data (wk), original image.
Step 1: Divide the stego image.
Step 2: Generate the stego cover image using equation (7) for each block.
Step 3: Extract the secret data using equation (8).
Step 4: Reconstruct the original image.
```

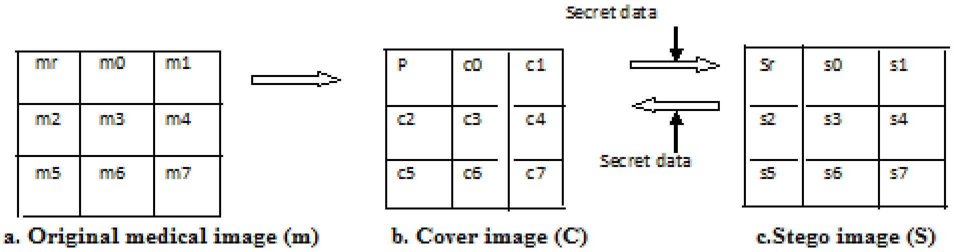

Figure.1: Proposed Method

EXPERIMENTAL RESULTS

The performance of the proposed method is analyzed using ordinary images and medical images with size 250x250. Matlab version R2013a is used for the experimental results. There are about 1338 images used from image database for the experiment, few images are randomly considered as shown in figure2. The ordinary original with its stego and extracted images are shown in figure 2,3 and 4 respectively. Original medical images with its stego and extracted images are shown in figure 5, 6 and 7 respectively. Stego and reconstructed images are shown in figure 3&6 and figure 4&7. Visually there is no different between original and stego images. To measure the performance of the proposed method PSNR and MAE measures are used.

PSNR measure is used to calculate the cover and stego images quality. If PSNR value is below 30dB, then the image quality is very low and it is not considered. In the proposed method, original gray scale image of size 250x250 is considered as an original image. To represent the difference between the observation values predicted by the statistical modelling in MSE to the actual observation helps in determining the limit to which the model fits the data and whether it is possible to simplify the model by eradicating some of the explanatory variables without affecting the model's predictive ability.

Table1 lists the PSNR and MAE values for the different ordinary images and table 2 lists the measures values for medical images. PSNR values for proposed method for ordinary and medical images are high. It shows that, the proposed method does not affect the image quality. MAE values between original and extracted images also nearly equal to zero. It means that the proposed method extract the images without loss. From these analyses, it is found that the quality of the images in the proposed scheme is high. At the remote specialist side the EPI is extracted from the stego medical image and extracted medical image is used for diagnosis purpose.

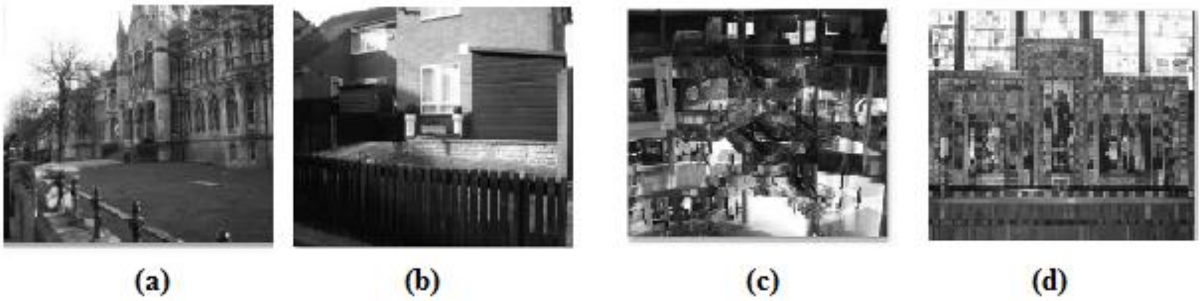

Figure 2: ordinary original images: (a) image1 (b) image2 (c) image3 (d) image4

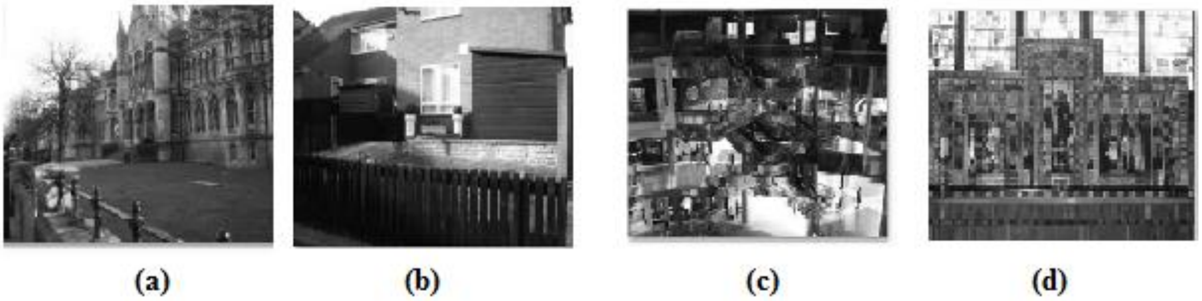

Figure 3: Stego images: (a) image1 (b) image2 (c) image3 (d) image4

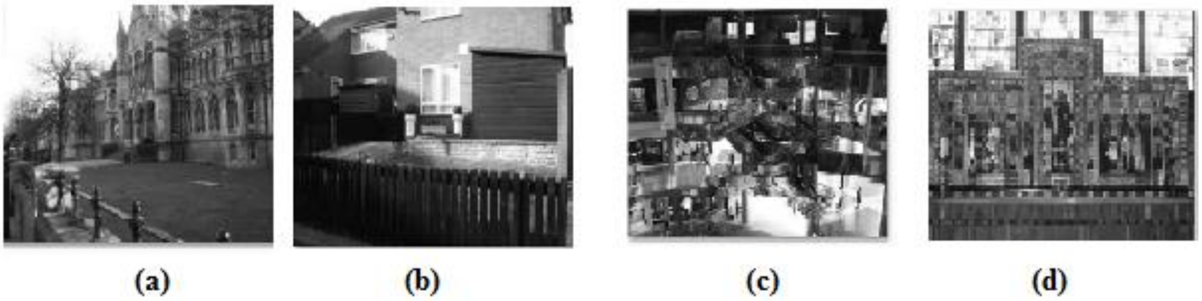

Figure 4: Extracted images: (a) image1 (b) image2 (c) image3 (d) image4

Table 1: performance measures of the proposed method for ordinary images.

Images	PSNR	MAE
image 1	67.8370	0.0052
image 2	70.1797	0.0043
image 3	70.6582	0.0048
image 4	71.5347	0.0041

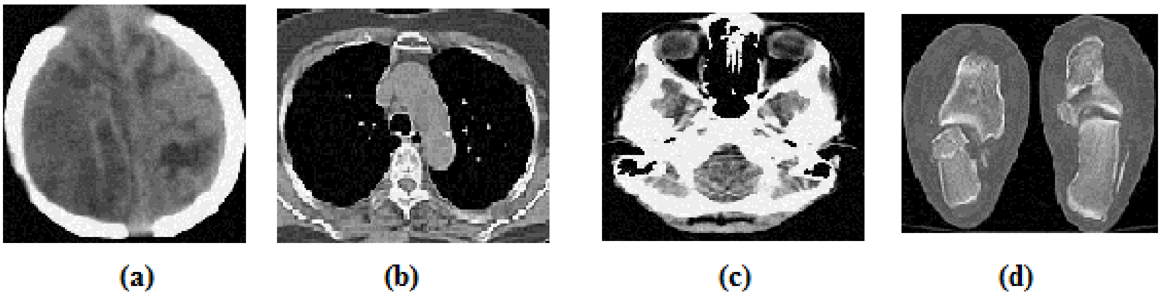

Figure 5:Original medical images: (a) brain (b) chest (c) head (d) foot

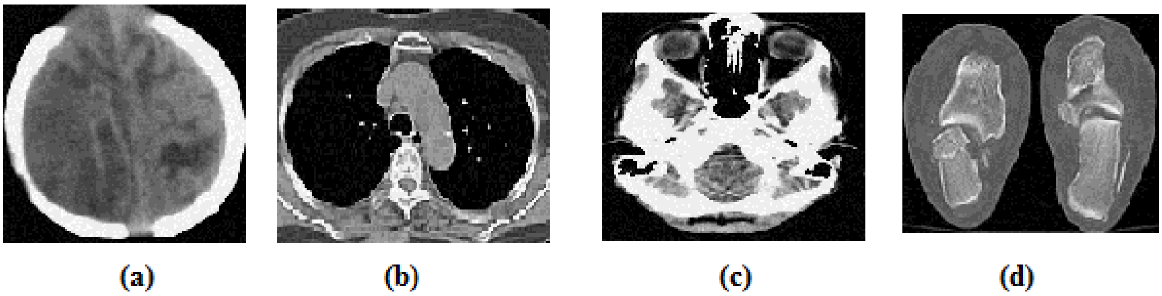

Figure 6: Stego Images. (a) brain (b) chest (c) head (d) foot

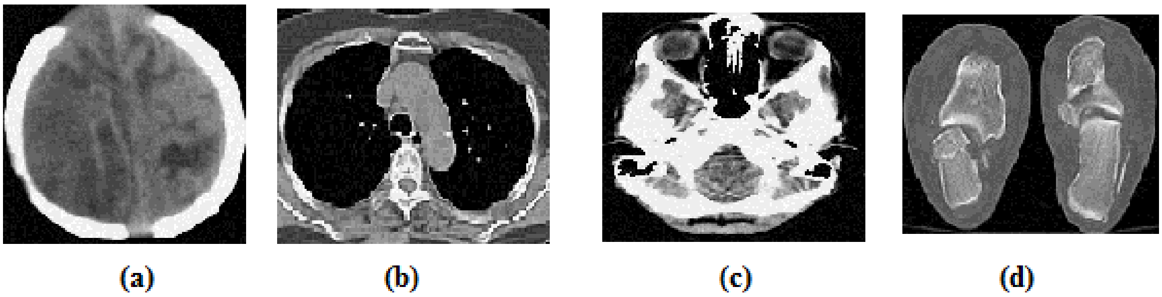

Figure 7: Reconstructed medical images (a) brain (b) chest (c) head (d) foot

Table 2: performance measures of the proposed method for medical images.

Images	PSNR	MAE
Brain	63.44	0.0074
Chest	65.67	0.0055
head	64.32	0.0064
foot	67.14	0.0051

CONCLUSION

This paper proposed a data hiding technique to protect medical images along with EPI. By using various radix number EPI is embedded within a medical images. At the receiver side the hidden EPI and medical images are extracted without any loss. PSNR and MSE is used to measures the performance of the proposed method. PSNR value is high and MAE value is equal to zero. This shows that the proposed method transmit the medical image in a secured manner.

REFERENCES

[1] Tuncer T, Avci E. Displays 2016; 41,1-8.

[2] Geetha S, Kabilan V, Chockalingam S P, Kamaraj N. 2011;111 (16),792–797.

[3] Tanga M, Zenga S, Chena X, Hub J, Du Y. Optik 2016; 127,471-477.

[4] Hu J, Tianrui Li. Computers and Electrical Engineering,2015; 46,447–455.

[5] Lou D C,Wub N I, Wang C M,Lin Z H,Tsai C S. The Journal of Systems and Software 2010;83(7),1236–1248.

[6] Johri S, Asthan A. Journal of Global Research in Computer Science 2012; 3 (3), 41-45.

[7] Zenga X,Li Z,Ping L. AEU-International Journal of Electronics and Communications 2012; 66 (7),532–539.

[8] Chang C C, Huang Y H, Tsai H, Qin C. AEU-International Journal of Electronics and Communications, 2012;66(9):758– 766.

[9] Lina C C, Tai W L, Chang C C. Pattern Recognition 2008;41 (12), 3582 – 3591.

[10] Wang C T, Hsiang-Fu Yu. Journal of Visual Communication and Image Representation 2012;23(5):798–811.