A Novel Approach for Lossless Data Hiding for Medical Images

Bharti
Bhai Gurdas Institute of Engineering & Technology, Sangrur (Punjab), India
bharti.tech15@gmail.com

Gaurav Mittal
Bhai Gurdas Institute of Engineering & Technology, Sangrur (Punjab), India
mitsgaurav@gmail.com

Abstract - With the growth of information technology, new challenges in healthcare management have come forward. Image steganography is an emerging field of research for secure medical data hiding and retrieving over internet. In our approach, a novel approach of steganography for Gray Scale Images has been proposed. In the proposed scheme, we will first detect noise in the image using Scanning Matrix. Then we will generate a key matrix to encode the text into noise of the image. By doing this, we are not changing the quality of the image and original image can be recovered with almost negligible distortion. The scheme has been proposed for images of different sizes. The experimental results show a significant improvement in terms of PSNR and MSE.

Keywords: Steganography, Gray Scale Image, Lossless Image.

1. Introduction

The security of medical records is an important issue related to privacy and safety during storage and communication [1]. Data embedding with medical images will have applications such as compact storage, efficient transmission and confidentiality of patient records [2] [3]. The aim of steganography refrain others from thinking that a secret message even exists within encrypted images. Digital images can easily be used as cover files without any doubt everywhere on the internet.

Steganography and cryptography are cousins in the spycraft family. Cryptography scrambles a message so it cannot be understood. Steganography hides the message so it cannot be seen [4].

It is assumed here that the inputs of the steganographic system are grayscale images. The cover signal is typified by an H-row, W-column (HxW) matrix whose elements are integer numbers between 0 and 255 for an 8-bit digital image [5]. Grayscale images are presented in a variety of formats but never compressed raw images have been of much interest in steganography [6]. Our proposed technique used lossless compressed medical image. Then image is converted into grayscale.

At the very first step we have to read an image in MATLAB. Our algorithm will first detect the noise present in the image using scanning method and store those coordinates in key matrix. Further we use these coordinates to store our text data in ASCII format. By doing so, we are not changing the quality of the image anymore rather we are just using the noisy pixels to store data. If there are very less noisy pixels in the image then our algorithm will search for the areas where probability of finding data is least. Further, since the imperceptibility of the stego-image is high and unintended observer will not be aware of the presence of hidden data.

2. Methodology

The proposed method is executed in MATLAB on Windows platform. A user friendly GUI is used here for psychological acceptability. The proposed work consists of two stages of encryptions which are following:

2.1. Encoding

The patient ID is assumed to be alphanumeric. It begins with a 2 character long hospital identifier, followed by 6 digits of unique patient number and ending with a 2 character department identifier [1]. The user enters the patient ID of maximum character length of 10. The encoding technique used is to convert the patient ID in ASCII format. For the
embedding of data in the cover image, noisy portions are exploited.

A flow chart is given for the illustration of processes involved for encoding and decoding in fig. 1. First of all to detect noisy portions, we count the number of neighborhood pixels of each center pixel using 3x3 scanning matrix. One pixel will have at most 8 neighbors. Then analyze the difference of that particular pixel value with its neighboring pixel values. Now count the neighbor pixels with large difference in value than threshold. If that count exceeds 3 then that pixel is labeled as noise. The scanning matrix cannot be able to detect noise from corners of the cover image. Further, we store these noisy coordinates in the key matrix. We exploit these noisy portions to encode our data. Data is arranged in ascending order and will replace the noisy pixel value of similar ones of the cover image. Therefore the patient information has been encrypted in the medical image (refer fig 3).

2.2. Decoding

After receiving the encrypted host image, the decryption process will carry out. The receiver uses key matrix, which has all the locations of encrypted text data. On the basis of above information, the receiver will then extract the original patient ID.

The test image (512*512) with and without patient data is shown in Fig 2 & 3:

Fig. 2: Host medical image without patient data.

Fig. 3: Host medical image embedded with patient data.

3. Performance Evaluation

The performance of our algorithm was evaluated using three metrics given below:

A. Peak Signal-to-Noise Ratio is given as

\[
\text{PSNR} = 10 \log_{10} \frac{255^2}{\text{MSE}} \text{ dB}
\]

where MSE is Mean Square Error.
B. Mean Square Error is given as

\[ \text{MSE} = \frac{1}{HW} \sum_{x=1}^{H} \sum_{y=1}^{W} (S_{xy} - C_{xy})^2 \]

where H & W are height and width of the image respectively. S & C are the values of pixel located in (x,y) coordinates of the stego image and cover image respectively.

C. Correlation Factor

It describes the degree of closeness of the images. Its value is unity when the cover & stego images are completely correlated and it is zero when both are completely uncorrelated. The PSNR, MSE and Correlation values for different sizes of image are shown in table 1.

<table>
<thead>
<tr>
<th>Size of the host image</th>
<th>PSNR</th>
<th>MSE</th>
<th>Correlation Factor</th>
</tr>
</thead>
<tbody>
<tr>
<td>128*128</td>
<td>68.3438</td>
<td>9.5*10^{-3}</td>
<td>0.9999</td>
</tr>
<tr>
<td>256*256</td>
<td>80.8549</td>
<td>5.4*10^{-3}</td>
<td>0.9999</td>
</tr>
<tr>
<td>512*512</td>
<td>82.7258</td>
<td>3.4*10^{-3}</td>
<td>0.9999</td>
</tr>
</tbody>
</table>

Fig 4. Graphs showing the variation of PSNR, MSE and Correlation factor with image size.

4. Conclusion and Future Improvement

Here, we have presented an algorithm with lossless data hiding scheme. Our algorithm has shown a significant improvement on lossless scheme \[1\] and outperforms in terms of parameters which were considered for evaluation. Our algorithm currently was not being used to hide data that is too large. If large amount of data need to be exchanged, the algorithm could be extended to hide different set of data in different images. Further, the scope is to extend this algorithm for the colored images also.
References


