International Journal of Computers and Applications

ISSN: 1206-212X (Print) 1925-7074 (Online) Journal homepage: https://www.tandfonline.com/loi/tjca20

Cloud-based Reversible Dynamic Secure Steganography Model for embedding pathological report in medical images

Sunil Kumar Patel, Chandran Saravanan & Vikash Kumar Patel

To cite this article: Sunil Kumar Patel, Chandran Saravanan & Vikash Kumar Patel (2019): Cloud-based Reversible Dynamic Secure Steganography Model for embedding pathological report in medical images, International Journal of Computers and Applications, DOI: 10.1080/1206212X.2019.1641273

To link to this article: https://doi.org/10.1080/1206212X.2019.1641273

INTERNATIONAL JOURNAL OF COMPUTERS AND APPLICATIONS
https://doi.org/10.1080/1206212X.2019.1641273

Taylor & Francis
Taylor & Francis Group

Cloud-based Reversible Dynamic Secure Steganography Model for embedding pathological report in medical images

Sunil Kumar Patel [a], Chandran Saravanan [a] and Vikash Kumar Patel [b]

[a]Department of Computer Science and Engineering, National Institute of Technology, Durgapur, India; [b]Department of Chemical Engineering, National Institute of Technology, Durgapur, India

ABSTRACT

Over past decades, several research works have been published in the direction of hiding confidential data that includes only the patients personal details in medical images. The medical images and respective pathological reports are stored separately in the storage device. Storing medical images and pathological reports separately occupy more storage compared to storing pathological reports Stego in medical images. This research identified 10.56% pixel space available in the medical image for storing other relevant secret information. In this technique, a new algorithm is proposed for generating secret keys. The secret keys are utilized to segment the medical image into five regions: (i) one Region of Interest (ROI) sub-image and (ii) four non-Region of Interest sub-images. From the four non-Region of Interest sub-images, a particular non-ROI region sub-image is randomly selected from the secret key matrix. The pathological report is embedded into the preprocessed selected non-ROI region sub-image of the medical image and generated the Stego medical image. The Stego medical image and secret key are communicated using various network communication applications to the user for deStego the original X-ray image and pathological report at the user end. The research work confirmed the quality of the medical image using MSE and PSNR values.

ARTICLE HISTORY
Received 11 March 2019
Accepted 18 June 2019

KEYWORDS
Steganography; segmentation; medical images; cloud storage

1. Introduction

Steganography is a technique that is utilized for transmitting the secret data using some medium. The medium that is utilized are digital image, audio, video, pdf file, etc. These medium mainly act as a carrier for the secret information [1]. One of the most important properties of the steganography-based system is that it should not be an easy task for malicious user to differentiate between the normal objects and the stego objects (objects that contain some secret information) [2,3]. The communication is mainly based on the method that is utilized for embedding the secret information. The detection of the secret data over the communication channel is unpredictable and challenging to extract the secret data.

Information hiding is a technique which conceals secret data in a cover medium for communicating secret data confidentially [1,4]. For designing data hiding technique, a visual requirement model is using three features called magic triangle – three requirements model [5,6] given in Figure 1. The first requirement feature is capacity, i.e. the amount of data embedded in the carrier image. Second one is robustness. By robustness, it is meant that the ability to withstand or overcome the secret data from attacked or stolen by an unintended user in adverse condition. Last one is imperceptibility. It measures the Mean-Square Error (MSE) and Peak Signal-to-Noise Ratio (PSNR). Higher PSNR value indicates better quality of Stego image. Figure 1 depicts the fundamental trade-offs between the three required features for data hiding is magic triangle – three requirements model. Robustness and embedded data capacity maintained against certain attacks, as long as its holding perceptual property at recognized degree of the Stego image. An efficient data hiding technique should be able to evade visual and statistical detection [7] against the Human Vision System (HVS) while providing an adaptable payload [8].

In the classical LSB Steganography [9,10], the secret data is converted into bit stream, which is embedded into the cover image by replacing the LSBs of the cover image with bit stream of the secret data. The Human Vision System hardly differentiates between the cover image and Stego image. For increasing the embedding capacity, two or more LSBs in each pixel are changed to embed the secret data. However, there is a trade-off between the embedding capacity and quality of Stego image. In this research article, a new algorithm is proposed for generating secret keys. The secret keys are utilized to segment the medical image into five regions. The pathological report is embedded into the preprocessed selected non-ROI region sub-image of the medical image and generated the Stego medical image. The Stego medical image and secret key are communicated using various network communication applications to the user for deStego the original X-ray image and pathological report at the user end. The proposed framework uses different clouds as storage for medical images, secret keys, pathological reports, Stego images to increase data security.

This paper is organized as follows. In Section 2, recent relevant research works are discussed. In Section 3, the CBRDSSM is explained. In subsection, a detailed description of the proposed system having segmentation, secret key generation, pixel value reduction and included Stego and deStego procedures is explained. In Section 4, experimental results and analysis performed by using the test database are discussed. Finally, Section 5 concludes the research work.

2. Related works

The growing number of e-health applications demands medical data protection and few research articles proposed to improve data

CONTACT Sunil Kumar Patel sunilpatel.bsb@gmail.com National Institute of Technology, Durgapur 713209, India

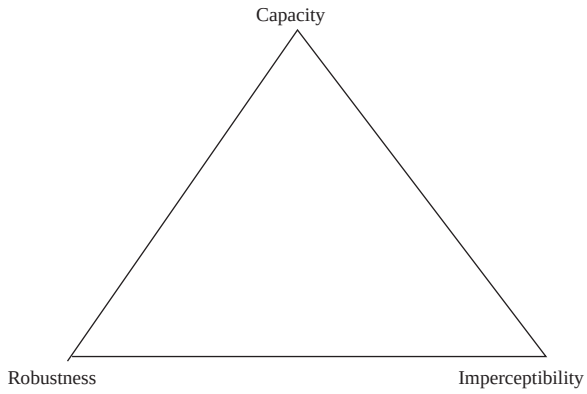

Figure 1. Magic triangle – three requirements model.

privacy, confidentiality by inserting digital patient record within medical images [11–14]. Such techniques are limited to small number of applications. Medical image watermarking is used for providing source authentication and data integrity, which uses different watermarks for different types of medical images for pathological data management and distribution [15,16].

To utilize the combined benefits of the cryptography and Steganography, crypto-watermarking algorithms had been proposed to address the security requirements of telemedicine applications [17–19]. In hybrid approaches, watermarking is used as the implementation platform. Cryptography watermarks are used for achieving integrity and authenticity of the implemented technique. The crypto-watermarking algorithms applied where robust and fragile watermarking based security applications are essential.

Dmour et al. [20] develop a high-imperceptibility digital Steganography technique that hides the Digital Patient Record (DPR) containing patient details only within the medical MRI image as cover without altering its ROI part. This utilized edge detection technique to identify the region and embed secret data in that sharp regions of the medical image. Humming code technique is used for embedding the 3 secret bits of data into 4 bits of the cover medical image, which result in enhanced quality of the carrier medical images. Then, DPR was Stego within the non-ROI region of the carrier image. It produces image without modifying the ROI, which was essential for the diagnosis. In this technique, the PSNR values were calculated considering different bits length of message, which ensure the effectiveness of Steganography technique for hiding electronic patient details. For enhancing the security different number of bits per pixel was used for embedding the DPR in medical image.

Fylakis et al. [21] introduced a technique using LSBs to hide information into the region of interest and non-ROI used for preserving the lost information as it is used for hiding data for backup. Thus the original pixels are retrieved in less distortion while the non-ROI pixels are retrieved in pseudo-random order. The technique was tested over MRI and X-ray images. The results had PSNR value over 40 dB.

Haj et al. [19] introduced a technique by combining cryptography and digital watermarking properties for providing security over the transmission of medical images. The combination of the two properties provided required authenticity and integrity. A cryptographic watermark and patient's data are hidden in the cover image before being transmitted over a vulnerable public network. It is based on dividing the image into ROI and non-ROI region and embedding three different watermarks in the non-ROI region.

The existing research works are providing confidentiality, high imperceptibility, and security by Huffman coding. In the electronic patient records [20], imperceptibility is provided by PSNR, and in the patient database [19] authenticity and integrity were provided by cryptographic watermarking. Anwar et al. [22] used digital watermark for identifying the owner of the medical images by extracting the feature of the captured ear image, after encryption used as a watermark for improving image security for transmission. The limitations of the previously published works [21,23] were limited only with patient information, electronic patient record, and patient data. In previously published research articles, the security provided only to the medical images using different steganography and watermarking technique [24,25]. In these works, security for patient information and medical images is covered separately. But, the security for patient information along with the pathological report and medical image of the same patient simultaneously is not covered.

3. Cloud-based Reversible Dynamic Secure Steganography Model (CBRDSSM)

In this section, medical secret data hiding using LSB Steganography scheme with cloud storage is proposed. In this research work, X-ray digital images of tuberculosis are used as a carrier image. The pathological report is embedded in the X-ray image, which provides privacy and reduces storage requirement for the medical data. This proposed data hiding scheme consists of various stages: segmentation, secret key generation, pixel value reduction, Stego procedure, and deStego procedure.

The underlying idea of our proposed model is depicted in Figure 2. The X-ray image and pathological report are stored in two different clouds, C1 and C2, which enhance security and management. The image and report are passed as inputs to the proposed model. Segmentation, the very first step, is performed on the X-ray image to separate the source medical image into one ROI and four non-ROIs. The secret key is generated using the four non-ROIs and stored in C3. One non-ROI is randomly selected for embedding the pathological report. Now, the selected non-ROI is preprocessed to determine the pixels which will be used for hiding the data. The secret data is the pathological report, stored in the cloud C2 is embedded in the preprocessed selected non-ROI region of the X-ray image and results the Stego X-ray image, which is stored in the cloud C4 for further communication. By using the secret key stored in cloud C3 and the Stego image in cloud C4, the deStego system extracted the original pathological report and X-ray image. The four different clouds enhance the security and management of the proposed model.

Data Dictionary. Following are the data structure for storing the information in 4 different clouds.

- **C1:** patient number, X-ray image
- **C2:** patient number, pathological report
- **C3:** patient number, key
- **C4:** patient number, Stego image.

Table 1 represents all four different clouds which are used to store the different entity with their type in the cloud database.

3.1. Segmentation

The input to the segmentation is the source carrier X-ray image. The output that is returned by the segmentation process is a binary X-ray image. Segmentation process partitions the input X-ray image into two segments (i) one ROI and (ii) four non-ROIs segment by separating foreground and background using edge detection without affecting medical data. In segmentation [26–28] process, the input

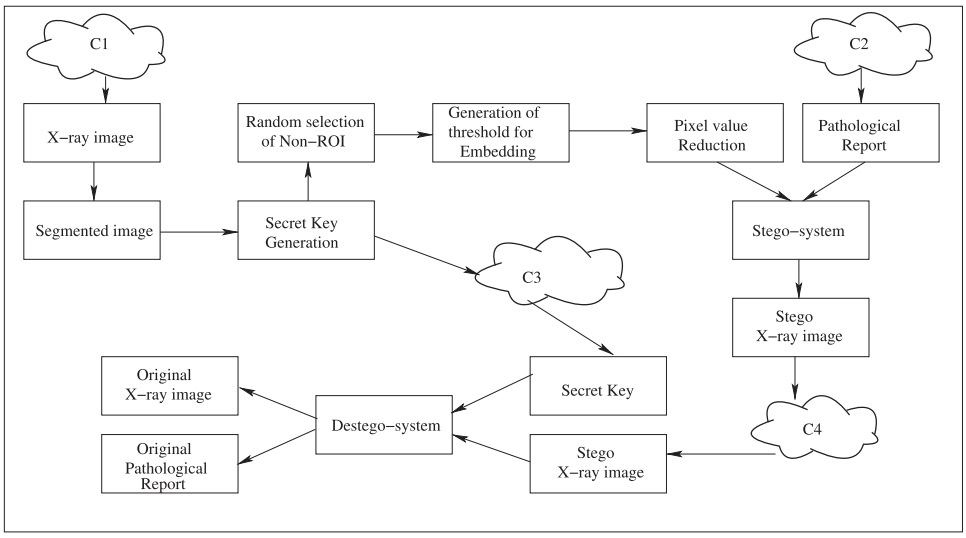

Figure 2. Data flowchart of the proposed model.

Table 1. Data dictionary.

Cloud	Entity	Type
C1	Patient number	Text
	Image	Binary
C2	Patient number	Text
	Pathological report	Binary
C3	Patient number	Text
	Key	Text
C4	Patient number	Text
	Image	Binary

image is converted into the binary image having all pixel value 0 or 255.

3.2. Secret key generation

The input to the key generation is the source carrier X-ray image. The output that is returned by the proposed algorithm (Algorithm 1) is 4×4 secret key matrix. In step 1, the dimensions height (H) and width (W) of the carrier X-ray image is calculated. The secret key matrix is initialized to null matrix M. In the next step, Gray Thresholding (GT) is performed over the source carrier X-ray image. The output is a 4×4 secret key matrix which holds the coordinates of the four non-ROIs.

The proposed algorithm considers the first non-ROI region from the top left of the medical image. However, suitable parameters are passed to the algorithm (Algorithm 1) to consider the other three non-ROIs, top right, bottom left, and bottom right. The final output secret key matrix M stored in cloud C3 contains the four coordinates of each four non-ROI regions.

3.3. Pixel value reduction

The input to the pixel value reduction is the secret key matrix returned by the above Algorithm 1. Step 1 of the proposed algorithm (Algorithm 2) determines the non-ROI by utilizing the secret key matrix. In step 2, the threshold value of pixels is calculated in the region of selected non-ROI. In step 3, the pixel values are modified in the range $(th - (2^{bit-length} + 1)\ to\ th)$. Finally, the proposed algorithm (Algorithm 2) returns the X-ray image having pixels value modified in the selected non-ROI region of the original carrier X-ray image.

Algorithm 1 Key_Generation

1: **Input:** C1: Carrier X-ray image, $key \leftarrow \phi$ // Key is a 2D-array.
2: $Arr \leftarrow \phi$, $mini \leftarrow 0$, $height \leftarrow H$, $widhth \leftarrow W$
3: **begin**
4: Convert the gray image into binary image.
5: BW is a 2D-array of pixel intensity value 0 & 1.
6: **for** $i = 1$ to height **do**
7: mini = min(Arr)
8: **for** $i = 1$ to width **do**
9: **if** $Bw(i,j) > 0$ and $i == 1$ **then**
10: Arr[i] = j-1
11: mini = Arr[i]
12: break
13: **end if**
14: thr = $mini \times 0.2$
15: **if** $BW(i,j) > 0$ and abs(j-mini) $\leq$ thr **then**
16: Arr[i] = j-1
17: break
18: **else if** $Bw(i,j) > 0$ **then**
19: i = height+1
20: break
21: **end if**
22: **end for**
23: **end for**
24: **Output:** Store the coordinates obtained in secret key matrix M.
25: **end**

3.4. Stego procedure

The inputs to the proposed algorithm (Algorithm 3) are selected processed non-ROI region of the modified X-ray image and the pathological report from the cloud C2. The output is the Stego X-ray image. In step 1 the secret data, i.e. pathological report, is embedded using the LSB technique [29,30] in the selected processed non-ROI region of the modified X-ray image. This procedure finally generates the Stego X-ray image which is stored in the cloud C4.

3.5. DeStego procedure

The input to the algorithm (Algorithm 4) is the Stego X-ray image stored in cloud C4 and the secret key matrix stored in cloud C3. The

Algorithm 2 Pixel value reduction

Input: C3: Secret key matrix, four non-ROIs
Step 1: Randomly select a non-ROI using secret key matrix
Step 2: For selected non-ROI in Step 1 calculate the threshold value given as

$$th = \frac{[min(non - ROI) + max(non - ROI)]}{2}$$

Step 3: Modifying the pixels value in the selected range:

$$(th - (2^{bit-length} + 1)\ to\ th)$$

Output: X-ray image having reduced pixel values in selected non-ROI region

Algorithm 3 Stego procedure

Input: modified X-ray image, C2: pathological report
Step 1: Using the LSB technique embed the pathological report in selected processed non-ROI region of the modified X-ray image.
Output: C4: Stego X-ray image

output is original X-ray image and pathological report. In Step 1, the non-ROI region were the data embedded is identified using secret key. In Step 2, storing the LSBs of the pixel in the non-ROI region. In Step 3, converting these bits into bytes by groping them. In Step 4, storing the bytes into the output text file in the form of ASCII values. This procedure generates the original X-ray image and pathological report separately.

Algorithm 4 DeStego procedure

Input: C4: Stego X-ray image, C3: secret key matrix
Step 1: Using secret key identify the region of data embedded
Step 2: Storing the LSB of the pixel values
Step 3: Grouping the bits into bytes
Step 4: Storing the bytes into the output text file in ASCII values
Output: Reproduced X-ray image, pathological report

4. Experimental results and analysis

The experimental results presented in this section demonstrate the performance of the proposed algorithm. To carry out our experiments, we used the Shenzhen set-Chest X-ray database [31,32] which consist of 336 cases with the manifestation of tuberculosis and 326 normal cases. The images are in PNG format; having image size varies for each X-ray images are approximately $3k \times 3k$ to $4k \times 4k$. The experiments are carried out on a personal computer, Windows 10, 64-bit operating system, x64-based processor, and MATLAB version R2016a.

The Stego image quality is verified using two metrics. First, we used the MSE and PSNR measurement to evaluate the difference between the Stego image and the original cover image. Second, we compared the quality of a cover image to that of Stego image which can be seen by HVS.

The MSE is used to measure the difference between the cover image X and Stego image Y described as [1]

$$\text{MSE} = \frac{1}{W \times H} \sum_{i=1}^{W} \sum_{j=1}^{H} (X_{ij} - Y_{ij}) \tag{1}$$

where X_{ij} is (i, j)th pixel value of cover image X and Y_{ij} is (i, j)th pixel value of Stego image Y of the size $W \times H$ pixels, W is the width and H is the height of the images.

The PSNR is used to measure the quality difference between the cover image X and Stego image Y described as [1]

$$\text{PSNR(dB)} = 10 \log_{10} \frac{x_{\max}^2}{\text{MSE}} \tag{2}$$

Figure 4. Binary image of the carrier X-ray image.

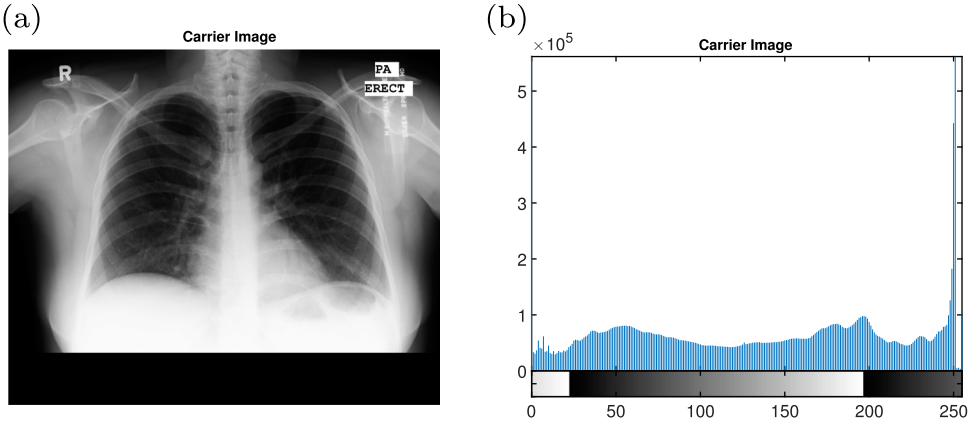

Figure 3. Carrier medical X-ray image and histogram showing the frequency of pixels value: (a) carrier X-ray image and (b) histogram of the carrier X-ray image.

where x_{max} is the maximum value for the 8-bit gray-scale image [1], $x_{max} = 255$.

Following Figure 3 showing (a) the source carrier medical X-ray image of tuberculosis having 4k×4k dimension and (b) histogram showing the frequency of pixels value throughout the X-ray image which is used as a carrier image for hiding the patient pathological report to provide the data privacy for the medical data.

Segmentation is performed to distinguish the ROI and non-ROIs over the carrier X-ray image. Following Figure 4 showing segmented X-ray image of having one ROI and four non-ROI segments in

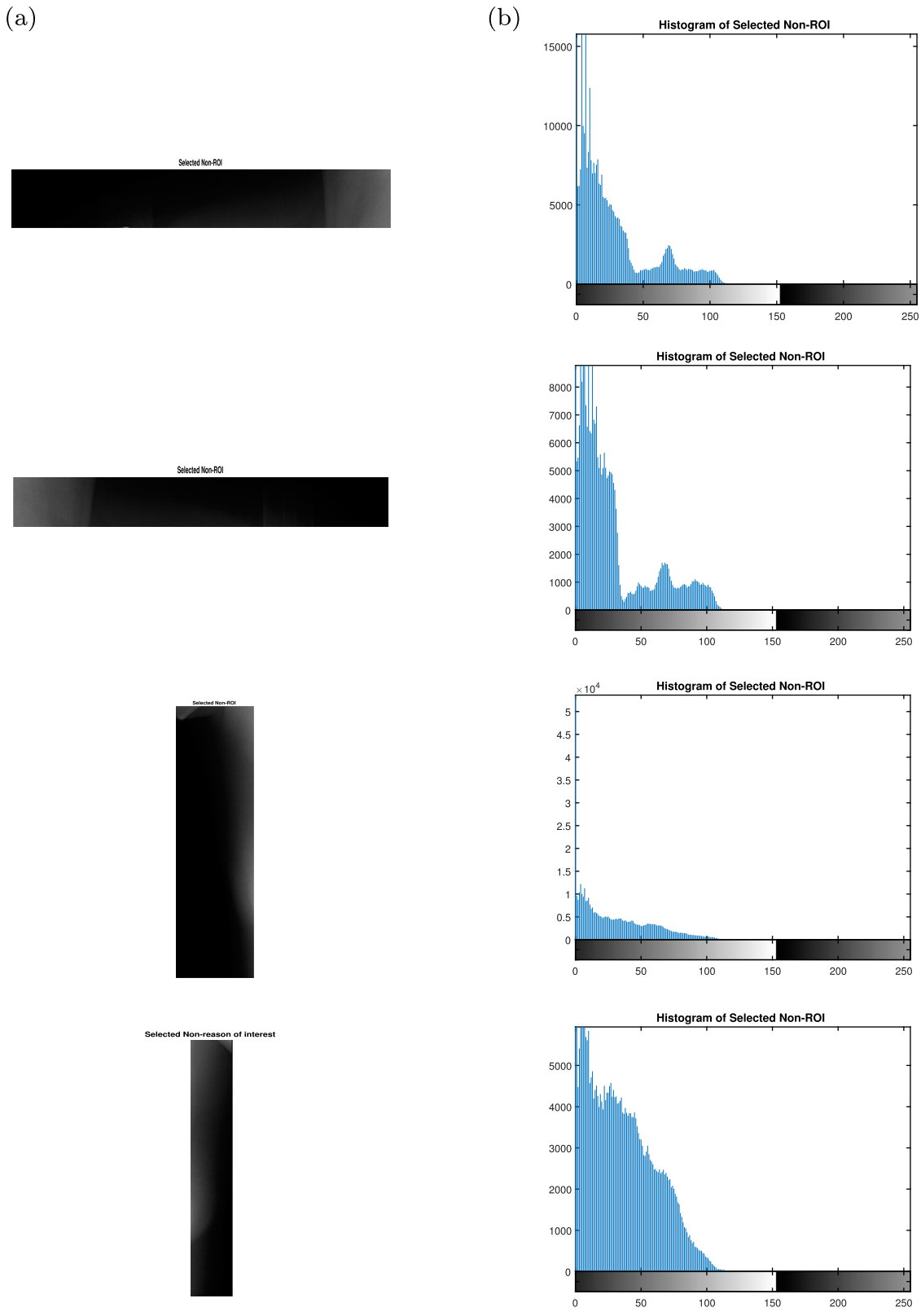

Figure 5. Selected non-ROI region of carrier X-ray image and respective histogram: (a) selected non-ROI regions and (b) histogram of selected non-ROI regions.

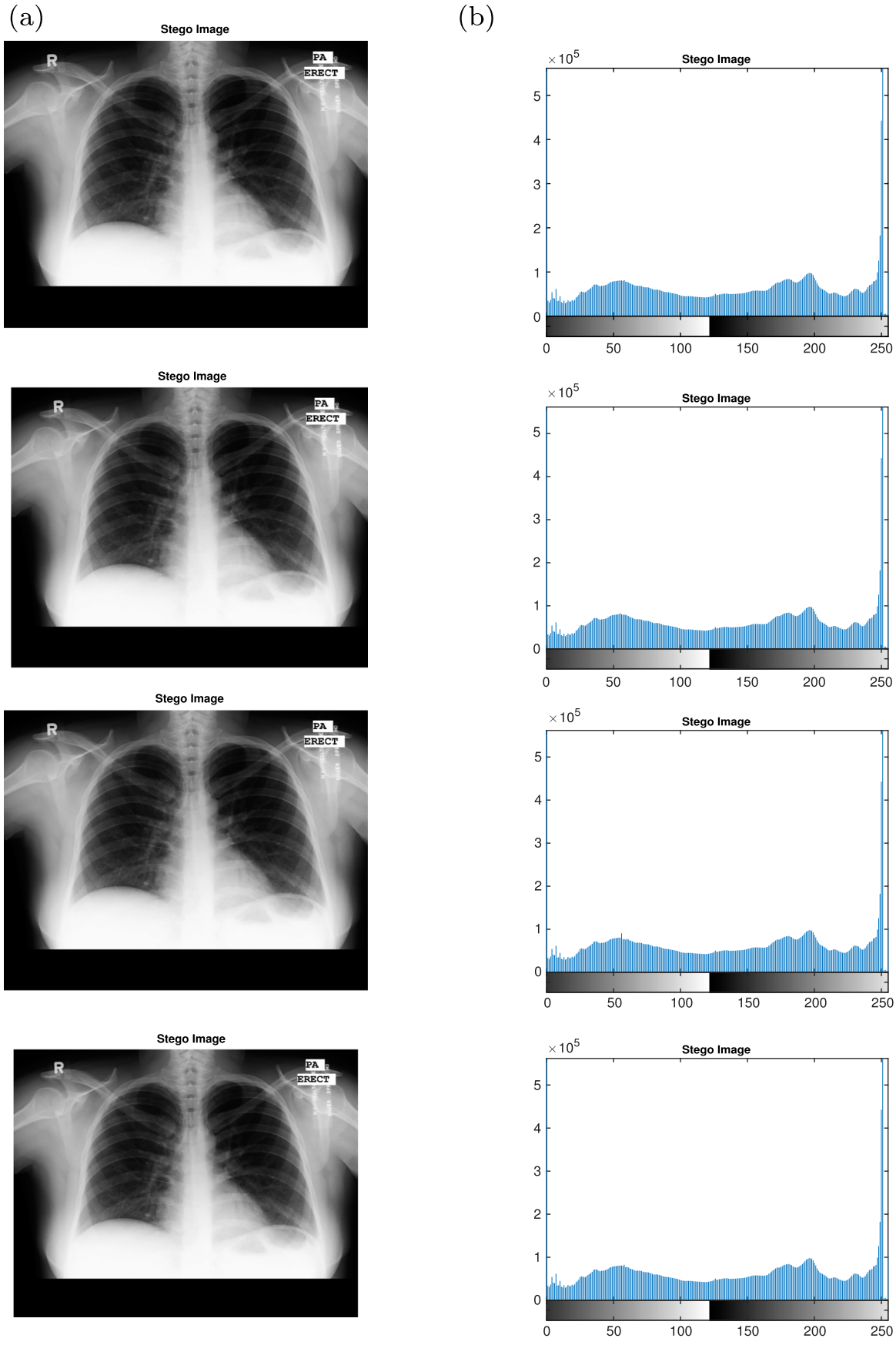

Figure 6. Stego X-ray images and respective histogram: (a) Stego X-ray images and (b) histogram of Stego X-ray images.

the carrier X-ray image. Further, randomly selecting one non-ROI segment for performing the further operation on the carrier X-ray image. The embedding of the pathological data performed only in the selected processed non-ROI region of the carrier X-ray image.

From Figure 4, we calculate the dimension of the non-ROIs and store in the form of a matrix called a secret key matrix M. From the secret key matrix M, a random selection of a row for selecting a non-ROI to carry out the Stego operation. Embedding operation is performed only in the selected non-ROI region.

Matrix M represents the secret keys, and the keys are the collection of the coordinates of the four non-ROIs from the carrier X-ray image.

$$M = \begin{bmatrix} 1 & 1 & 192 & 2162 \\ 1 & 2874 & 154 & 4892 \\ 1789 & 1 & 3440 & 442 \\ 1865 & 4687 & 3440 & 4892 \end{bmatrix}$$

A row, randomly selected from the matrix M for carrying out the embedding process. The total number of pixels lie in different non-ROI regions of the carrier X-ray image are: first non-ROI, having the coordinates (11, 1) and (192, 2162) and the total number of pixels lie in this region are 412, 751 pixels. In the second non-ROI, having the coordinates (1, 2874) and (154, 4892) and the total number of pixels lie in this region are 308, 754 pixels. In the third non-ROI, having the coordinates (1789, 1) and (3440, 442) and the total number of pixels lie in this region are 728, 091 pixels. In the fourth non-ROI, having the coordinates (1865, 4687) and (3440, 4892) and the total number of pixels lie in this region are 322, 875 pixels. The number of pixels identified for embedding process in each non-ROI regions are huge.

Following Figure 5 represents the non-ROI regions and histogram showing the frequency of the pixels value in the respective non-ROI. At a time, a single non-ROI randomly selected for performing stego operation of the pathological report.

The sample pathological report is having 990 characters including spaces and in bits 7920 by considering the ASCII value, which requires 8 bits for each character. Following Figure 6 shows (a) Stego X-ray images and (b) histogram of the Stego X-ray images. The secret data, pathological report of size 7920 bits are embedded in selected processed non-ROI region of the X-ray image. The selection of any processed-non-ROI region is random using the secret key matrix M. Comparing the two histograms from Figures 3 and 6 confirm there is no major change in the Stego image compared to the source carrier X-ray image.

In this proposed model, randomly selected non-ROI is used for Steganography. For further authentication of the proposed CBRDSSM model, the MSE and PSNR values are calculated between the preprocessed and Stego regions. These regions are the selected non-ROI region of the X-ray image, not on the entire image.

On experimentation Table 2 represents the MSE calculated using Equation (1) and PSNR calculated using Equation (2) values. The MSE and PSNR values are calculated by taking different number of LSB bits in each selected non-ROI regions in various iterations.

Tables 3 and 4 show the MSE and PSNR values taking various numbers of LSBs for performing Stego operation. Tables 3 and 4 show the MSE and PSNR values over the entire carrier X-ray image which is used for the experiment. Table 3 represents the MSE and PSNR values between the carrier X-ray and Stego X-ray images with various numbers of LSB bits. While, the Table 4 represents the MSE and PSNR values between preprocessed X-ray and Stego X-ray images with various numbers of LSB bits.

Tables 2–4 show the increasing number of LSB bits decreases the PSNR values ranging from 87.80184 dB to 55.50324 dB and increases MSE values in most of the cases ranging from 0.00010 to 0.18456. Thus the experimental results show that the proposed algorithms completed the Steganography operation on the medical image with a pathological report using various clouds. From Tables 2–4, it is clear that the proposed model confirms higher security with reduced size of data. The size of the carrier X-ray image is 2.1 MB, and the pathological report is of 12 kB. After performing embedding operation the size of Stego X-ray image is 2.1 MB, it remains equal as the carrier X-ray image. The Steganography procedure for embedding pathological report does not change the size of the original carrier X-ray image.

Table 2. MSE and PSNR values between preprocessed and Stego segment of the selected different non-ROI regions of the X-ray image.

Non-ROI region	Number of LSB bits	MSE	PSNR (dB)
First non-ROI	1 bit	0.01185	67.42583
	2 bits	0.06074	60.32943
	3 bits	0.42578	51.87284
	4 bits	3.16845	43.15632
Second non-ROI	1 bit	0.01540	66.288921
	2 bits	0.06727	59.88596
	3 bits	0.42862	51.84404
	4 bits	3.46127	42.77243
Third non-ROI	1 bit	0.00991	68.19993
	2 bits	0.07499	59.41472
	3 bits	0.69569	49.74058
	4 bits	5.91081	40.44832
Fourth non-ROI	1 bit	0.01956	65.25061
	2 bits	0.13343	56.91194
	3 bits	1.26317	47.15016
	4 bits	11.56738	37.53244

Table 3. MSE and PSNR values between the carrier image and Stego image.

Non-ROI region	Number of LSB bits	MSE	PSNR (dB)
First non-ROI	1 bit	0.00010	87.80184
	2 bits	0.00086	78.79003
	3 bits	0.00761	69.34703
	4 bits	0.06231	60.21859
Second non-ROI	1 bit	0.00013	87.01274
	2 bits	0.00074	79.43910
	3 bits	0.00609	70.31587
	4 bits	0.051142	61.05338
Third non-ROI	1 bit	0.00027	83.76834
	2 bits	0.00257	74.06033
	3 bits	0.02538	64.11875
	4 bits	0.21704	54.79934
Fourth non-ROI	1 bit	0.00022	84.58914
	2 bits	0.00198	75.19506
	3 bits	0.02048	65.05028
	4 bits	0.18456	55.50324

Table 4. MSE and PSNR values between the preprocessed image and Stego image.

Non-ROI region	Number of LSB bits	MSE	PSNR (dB)
First non-ROI	1 bit	0.00005	90.74762
	2 bits	0.00012	87.33433
	3 bits	0.00034	82.75644
	4 bits	0.00082	78.98644
Second non-ROI	1 bit	0.00009	88.45846
	2 bits	0.00022	84.63494
	3 bits	0.00076	79.31244
	4 bits	0.00166	75.96123
Third non-ROI	1 bit	0.00010	87.79981
	2 bits	0.00023	84.44986
	3 bits	0.00074	79.42196
	4 bits	0.00369	72.48747
Fourth non-ROI	1 bit	0.00010	87.96114
	2 bits	0.00022	84.73704
	3 bits	0.00064	80.09752
	4 bits	0.00431	71.81335

Table 5. Comparing the performance of proposed model with other existing approaches.

Model	MSE	PSNR
Anwar et al. [22]	0.1338	56.76
Elhoseny et al. [33]	0.1288	57.02
Proposed CBRDSSM	0.0204	65.05

4.1. Security analysis

In this proposed model, CBRDSSM comparison was carried out between preprocessed and Stego segments for the different selected non-ROI regions in Table 2, between the carrier image and Stego image in Table 3, between the preprocessed image and Stego image in Table 4. The proposed model is tested by using different sets of X-ray images from the Shenzhen set-Chest X-ray database [31,32]. The embedding procedure is carried out over different images in randomly selected non-ROIs. The security for the pathological reports in the non-ROI regions of X-ray images is analyzed by the parameters MSE given by Equation (1) and PSNR given by Equation (2). Lower the MSE values and higher the PSNR values provide better security over the steganography attacks and less distortion arises between the original carrier image and Stego image concealing the pathological report. From Tables 2–4, the MSE and PSNR values are calculated at different number of LSB bits in different selected non-ROI regions to ensure the security of the proposed CBRDSSM model.

The existing model given by Anwar et al. [22] uses 256 × 256 size of medical color images for embedding 18 bytes of data containing only the patient details. It achieved the MSE 0.0013 to 0.1338 and PSNR 76.8676 dB to 56.7648 dB for embedding only 18 bytes of data. In the model IoT-based healthcare system for secure medical data transmission given by Elhoseny et al. [33] uses DME eyes dataset [34] and DICOM dataset [35] having color and gray scale images for hiding the patient's information only. It achieved MSE values from 0.12 to 0.57 for color images and 0.14 to 0.57 for gray images and PSNR values from 57.44 dB to 56.39 dB for color images and 56.13 dB to 55.43 dB for gray images respectively. The model given by Shabir et al. [36] for providing security to clinical data uses different medical image as a carrier. In this model, the embedding of clinical data performed over the complete medical image and obtain the average PSNR value 46.3685 dB.

The performance of our work is compared with some existing work given by Anwar et al. [22] using medical color images of size 256 × 256 for the input text size of 18 bytes and Elhoseny et al. [33] by using color and gray image only for patient information. In our proposed CBRDSSM model, embedding of pathological report carried out which embedded medical data only in non-ROI regions of the carrier X-ray images. Table 5 shows the MSE and PSNR values obtained by previous model and our model. In our CBRDSSM, we achieved lesser MSE value, and higher PSNR values compare with the existing works that unveil the better performance of our CBRDSSM. In our proposed model, selection of non-ROI is random which enhances the security against steganalysis. As in this model embedding carried out only non-ROI regions which does not change the medical image data in ROI regions. This model provides security to pathological data along with preserving the authenticity of the medical X-ray images.

5. Conclusion

In this article, a reversible dynamic secure Steganography model for embedding the pathological report in medical X-ray image is proposed. At present, medical X-ray images and respective pathological reports are stored separately. This may lead to (i) more storage requirements and (ii) threat to the privacy of data. In this article, the proposed algorithms achieved security and reduced size of data by embedding the pathological report into the medical X-ray image. The experimental results confirm that the proposed algorithms retained the source medical image quality without any loss. The MSE and PSNR value at LSB 1 bit is 0.00022 and 84.58914 dB and LSB 4 bit is 0.18456 and 55.50324 dB achieved respectively. From the experimental results and analysis this model produces higher quality Stego image using HVS. Selecting the non-ROI randomly for embedding the pathological report confirms the robustness of the model against the steganalysis systems.

Acknowledgements

We would like to acknowledge Prof. Ashok Srinivasan, University of West Florida, Department of Computer Science, for his able guidance.

Disclosure statement

No potential conflict of interest was reported by the authors.

Notes on contributors

Sunil Kumar Patel is pursuing Ph.D. in the department of Computer Science and Engineering, National Institute of Technology Durgapur, India from July'2017. Received M.Tech. Degree in Information Technology from the department of CSE, NIT Durgapur, India in 2017. Received B.Tech. Degree in Information Technology from UPTU Lucknow University, India in 2012. Published an IEEE conference paper and attended workshop & seminar in Biometric security, Machine learning, and soft computing.

Chandran Saravanan has more than 23 years of teaching experience and about 16 years of research experience. Visited and participated in collaborative research at University of Texas, Arlington. One week Guest faculty at Caledonian College of Engineering, Muscat, Oman. Participated in collaborative research with CSIR-Central Electrochemical Research Institute, Tamilnadu, India. Participated in collaborative research with CSIR-Advanced Materials and Processes Research Institute, Bhopal, Madhya Pradesh, India. Member of Information Security Education and Awareness Phase I & II project and TEQIP – I and II project. Granted 1 patent, filed 1 patent, and published and accepted 98 research articles (SCI/SCOPUS/WOS/SCIE/ESCI 50 nos.) in international peer-reviewed journals, conferences, 3 books and 4 book chapters (Google citations-348, h-index-10, i10-index-10, Total Impact factor > 40.733). One of our research articles has been first in the top 20 articles, during 2013-16. Developed M.Tech. Programme on High Performance Computing and Ph.D. programme on Computer Science admitted two batches from the academic year 2014-15 in Computer Centre, NIT Durgapur. Four research scholars awarded Ph.D. degree in the year 2013, 2015, 2017, and 2018, 3 scholars submitted Ph.D. synopsis, and 2 research scholars working on Ph.D. 15 M.Tech., 11 M.C.A. 6 B.Tech., 16 B.Tech. Internship projects supervised and 2 M.Tech scholars, 7 B.Tech. Students working on projects. Organized several conferences, seminars, and workshops. Reviewer in IEEE, Springer, Elsevier, Taylor & Francis etc. Board member in several peer reviewed international journals. Nominated as a Board Member for Ph.D. viva voce and as an Indian examiner for several Ph.D. thesis in various universities.

Vikash Kumar Patel recently graduated with B.Tech degree from the department of Chemical Engineering, National Institute of Technology Durgapur, India in May'2019. He is a competitive programmer and currently working for AllinCall as a Software developer.

ORCID

Sunil Kumar Patel http://orcid.org/0000-0002-9821-0852
Chandran Saravanan http://orcid.org/0000-0002-0695-8776
Vikash Kumar Patel http://orcid.org/0000-0002-3667-6251

References

[1] Fridrich J. Steganography in digital media: principles, algorithms and applications. Cambridge: Cambridge University Press; 2009.
[2] Zielińska E, Mazurczyk W, Szczypiorski K. Trends in steganography. Commun ACM. 2014;57(3):86–95.

[3] Zielińska E, Mazurczyk W, Szczypiorski K. Development trends in steganography. Warsaw University of Technology, Institute of Telecommunications Warsaw, Poland, 00-665, Nowowiejska. 2011;15:19.
[4] Provos N, Honeyman P. Hide and seek: an introduction to steganography. IEEE Secur Priv. 2003;99(3):32–44.
[5] Johnson NF, Duric Z, Jajodia S. Information hiding: Steganography and watermarking-attacks and countermeasures. Vol. 1. Springer Science & Business Media; 2001.
[6] Patel SK, Saravanan C. Performance analysis of hybrid edge detector scheme and magic cube based scheme for steganography application. 2018 International conference on communication, computing and internet of things (IC3IoT); Chennai, India; IEEE; 2018. p. 299–303.
[7] Filler T, Judas J, Fridrich J. Minimizing embedding impact in steganography using trellis-coded quantization. In: Memon ND, Dittmann J, Alattar AM, et al., editors. Media forensics and security II. Vol. 7541. Guwahati (India): International Society for Optics and Photonics; 2010. p. 754105.
[8] Lyu S, Farid H. Steganalysis using higher-order image statistics. IEEE Trans Inf Forensics Secur. 2006;1(1):111–119.
[9] Chang W-J, Hoang Ngan Le T, Chen C-C. High payload steganography mechanism using hybrid edge detector. Expert Syst Appl. 2010;37(4): 3292–3301.
[10] Wu Q, Zhu C, Li JJ, et al. A magic cube based information hiding scheme of large payload. J Inf Secur Appl. 2016;26:1–7.
[11] Acharya R, Niranjan U, Iyengar SS, et al. Simultaneous storage of patient information with medical images in the frequency domain. Comput Methods Programs Biomed. 2004;76(1):13–19.
[12] Nayak J, Bhat PS, Kumar MS, et al. Reliable transmission and storage of medical images with patient information using error control codes. 1st IEEE proceedings of the INDICON'04 India annual conference; 2004. p. 147–150.
[13] Srinivasan Y, Nutter B, Mitra S, et al. Secure transmission of medical records using high capacity steganography. 17th IEEE symposium on computer-based medical systems. CBMS'04. Proceedings; 2004. p. 122–127.
[14] Coatrieux G, Lecornu L, Sankur B, et al. A review of image watermarking applications in healthcare. 28th annual international conference of the IEEE engineering in medicine and biology society. EMBS'06; 2006. p. 4691–4694.
[15] Planitz B, Maeder A. Medical image watermarking: a study on image degradation. Proc. Australian pattern recognition society workshop on digital image computing. WDIC'05; 2005.
[16] Giakoumaki A, Pavlopoulos S, Koutsouris D. Multiple image watermarking applied to health information management. IEEE Trans Inf Technol Biomed. 2006;10(4):722–732.
[17] Pan W, Coatrieux G, Cuppens-Boulahia N, et al. Medical image integrity control combining digital signature and lossless watermarking. In: Data privacy management and autonomous spontaneous security. Springer; 2010. p. 153–162.
[18] Coatrieux G, Huang H, Shu H. A watermarking-based medical image integrity control system and an image moment signature for tampering characterization. IEEE J Biomed Health Inform. 2013;17(6):1057–1067.
[19] Al-Haj A, Hussein N, Abandah G. Combining cryptography and digital watermarking for secured transmission of medical images. IEEE 2nd international conference on information management. ICIM'16; 2016. p. 40–46.
[20] Al-Dmour H, Al-Ani A. Quality optimized medical image steganography based on edge detection and hamming code. IEEE 12th international symposium on biomedical imaging. ISBI'15; 2015. p. 1486–1489.
[21] Fylakis A, Keskinarkaus A, Kiviniemi V, et al. Reversible blind data hiding for verifying integrity and authenticating MRI and X-ray images. IEEE 9th international symposium on medical information and communication technology. ISMICT'15; 2015. p. 185–189.
[22] Anwar AS, Ghany KKA, Mahdy HE. Improving the security of images transmission. Int J Bio-Med Inform e-Health. 2015;3(4).
[23] Usman MA, Usman MR. Using image steganography for providing enhanced medical data security. IEEE 15th annual conference consumer communications and networking conference. CCNC'18; 2018. p. 1–4.
[24] Thanki R, Borra S, Dwivedi V, et al. A steganographic approach for secure communication of medical images based on the dct-svd and the compressed sensing (cs) theory. Imaging Sci J. 2017;65(8):457–467.
[25] Tsai JM, Chen IT, Huang YF, et al. Watermarking technique for improved management of digital medical images. J Discrete Math Sci Cryptogr. 2015;18(6):785–799.
[26] Ma Z, Tavares JMR, Jorge RN, et al. A review of algorithms for medical image segmentation and their applications to the female pelvic cavity. Comput Methods Biomech Biomed Engin. 2010;13(2):235–246.
[27] Kundu MK, Das S. Lossless roi medical image watermarking technique with enhanced security and high payload embedding. IEEE 20th international conference on pattern recognition. ICPR'10; 2010. p. 1457–1460.
[28] Parker JR. Algorithms for image processing and computer vision. John Wiley & Sons; 2010.
[29] Fridrich J, Goljan M, Du R. Detecting lsb steganography in color, and gray-scale images. IEEE J Multimedia Secur. 2001;8(4):22–28.
[30] Dumitrescu S, Wu X, Wang Z. Detection of LSB steganography via sample pair analysis. International workshop on information hiding; Springer; 2002. p. 355–372.
[31] Jaeger S, Karargyris A, Candemir S, et al. Automatic tuberculosis screening using chest radiographs. IEEE Trans Med Imaging. 2014;33(2):233–245.
[32] Candemir S, Jaeger S, Palaniappan K, et al. Lung segmentation in chest radiographs using anatomical atlases with nonrigid registration. IEEE Trans Med Imaging. 2014;33(2):577–590.
[33] Elhoseny M, Ramírez-González G, Abu-Elnasr OM, et al. Secure medical data transmission model for iot-based healthcare systems. IEEE Access on Information Security Solutions for Telemedicine Applications. 2018;6:20596–20608.
[34] Rabbani H, Allingham MJ, Mettu PS, et al. Fully automatic segmentation of fluorescein leakage in subjects with diabetic macular edema. Invest. Ophthalmol. Vis. Sci.. 2015;56(3):1482–1492.
[35] McEvoy FJ, Svalastoga E. Security of patient and study data associated with dicom images when transferred using compact disc media. J Digit Imaging. 2009;22(1):65–70.
[36] Parah SA, Ahad F, Sheikh JA, et al. Hiding clinical information in medical images: a new high capacity and reversible data hiding technique. J Biomed Inform. 2017;66:214–230.

Appendix

Appendix. Sample pathological report

Patient: CINA, JOHN (M)
Referring Physician: XMRI, FIRST OPINION
MRN : JD1004 DOB: 15/08/1991
Exam Date: 27/12/2017
FAX: 998−834−2123
CLINICAL HISTORY: Cough, congestion.
COMMENTS:
PA and lateral views of chest reveal no evidence of active pleural or pulmonary parenchymal abnormality.
There are diffusely increased interstitial lung markings consistent with chronic bronchitis.
Underlying pulmonary fibrosis is not excluded.
The cardiac silhouette is enlarged.
The mediastinum and pulmonary vessels appear normal.
Aorta is tortuous.
Degenerative changes are noted in the thoracic spine.

IMPRESSION:

(1) No evidence of acute pulmonary pathology.
(2) Enlarged cardiac silhouette.
(3) Tortuous aorta.
(4) Diffusely increased interstitial lung markings consistent with chronic bronchitis.
(5) Underlying pulmonary fibrosis is not excluded.
(6) Consider follow up with Chest CT if clinically warranted.