Journal of Engineering and Computer Sciences
Qassim University, Vol. 9, No. 1, pp. 39-57 (January 2016/Rabi' I 1437H)

Medical Image Security Using a Novel Steganography Technique

Mohamed Tahar Ben Othman

Computer Science Department, College of Computer, Qassim University

Kingdom of Saudi Arabia

Emails: maathaman@qu.edu.sa; mtothman@gmail.com

(Received 9/3/2016, accepted 4/5/2016)

ABSTRACT. The exchange of the medical patient's information through the Internet, known as Telemedicine, has become imperative. Indeed, for practical purposes, patient files have to be shared to several medical locations (with different specializations, for example) and insurance companies. On the other hand, the privacy and security of a patient's health information has to be safeguarded. Through the Internet, the patient's health information can be disclosed or tampered, either accidentally or maliciously. To address this issue, intensive research has been conducted in the last decade to ensure the secure and safe transmission of such information through medical image steganography. This issue is of supreme importance when conducting remote surgeries, also known as Tele-surgery, wherein a doctor is performing surgery on a patient who does not physically share the same location. In this case, real-time security is absolutely needed. As this domain still requires much research, we propose a new steganography technique based on image clustering of the Region of Non-Interest (RONI) of the image. This new technique demonstrates that while the Region of Interest (ROI) in medical image is not used in this process, the robustness against some attacks, such as rotation and cropping, is still highly effective. Results show that this robustness is related to the size of duplication of the embedded stego-information and the dispersal rate of this duplication.

Keywords: Medical image steganography, Telemedicine, ROI, RONI, Dispersal rate

1. Introduction

In the last decade, several types of research were conducted to ensure medical information confidentiality and authentication while transmitting patient files using an open access network. On the other hand, separating the Electronic Patient Record (EPR) and the images may lead to the detachment of EPR from the cover holding it, which can lead to faulty and dangerous medical decisions. To avoid this detachment, different techniques of steganography/watermarking were proposed to embed the needed data into the image. The integrity of the medical data must be protected, as high risks of inappropriate use of medical information can be the result of data tampering. Several techniques were used to overcome the increasing difficulties of maintaining the security of patient information. Medical images are generally embedded by medical information. Data hiding techniques are used for concealing patient information with medical images [1]. As this information is sensitive and the medical image has zero tolerance for noise, neither the information nor the image should be destroyed by either watermarking data or tampering. These techniques present a wide number of security aspects, such as data privacy, image integrity, authenticity, detection of tampered elements and image correction, confidentiality, and authentication. Although the Digital Imaging and Communications in Medicine (DICOM) is used to store, transmit and print medical image information, security means are still necessary [2]. Steganography is the process of hiding information in a carrier, such as a text, a voice medium, an image, or a video. The frequency of digital images on the Internet and their impressive ability in hiding data without quality degradation make them the most used carrier as steganography covers [3]. Although steganography is a high-security technique for data transmission, its robustness depends on the level of resistance against attacks.

A good image steganography technique aims at three aspects [3]: 1) the capacity, the maximum data that can be stored in a cover image; 2) the imperceptibility, the visual quality of a stego-image after data hiding; and 3) the robustness against attacks.

The rest of this paper is presented as follows: the general structure of the steganography scheme is given in Section 2. Section 3 provides an introduction on the medical image's sensitivity. Section 4 presents the related works mainly focusing on methods based on the Least Significant Bit (LSB). The proposed solution is explained in Section 5. Section 6 reveals the experimental results, and lastly, the conclusion is detailed in Section 7.

2. Image steganography

Image steganography is a technique of hiding a message in a cover image, in such a way that its presence cannot be discerned. Image steganography can be done in spatial [4, 5, 6, 7, 8] or transformational [9, 10, 11, 12] domains. The spatial domain is simpler and faster in execution, but vulnerable to compression and geometric

distortions, such as rotation, scaling and cropping, for instance. The transformational domain, while robust against many geometric distortions and filtering, requires a higher computational time and complexity [13]. Figure 1 presents the general steganography schema.

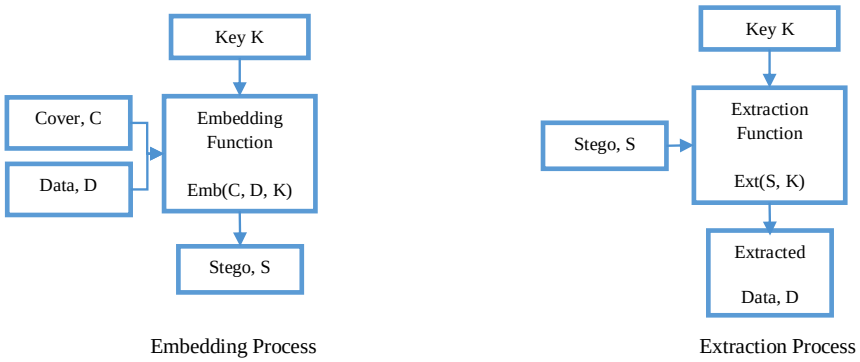


Fig. (1). General Steganography schema

3. Medical Image's Sensitivity

The images distributed in an easily accessible open network are susceptible to accidental or intentional attacks, leading to the introduction of artifacts, consequently causing the loss of the patient's identity. Although there are risks of inappropriate use of medical information, given the ease with which digital data can be manipulated, the exchange of the medical history of the patient among medical experts, which includes clinical images, prescriptions, initial diagnosis, is a necessity. On the other hand, health policies have stipulated stringent rules regarding the disclosure of patients' information, which are classified as highly sensitive data. Medical images have zero tolerance for noise, a particularity that contrasts that of most images, pushing researchers to improve the security of these types of digital images. The main security characteristics of medical information are: confidentiality, reliability, and availability [13]:

1.Confidentiality: ensures that only the entitled users have access to the information.

2.Reliability has two sides: a) integrity — the information has not been modified by non-authorized people; and b) authenticity — a proof that the information belongs to the correct patient and issued from the right source.

3.Availability: warrants an information system to be used in the normal scheduled conditions of access.

Medical image steganography techniques may be classified into three categories: a) authentication schemes, which include tamper detection and recovery; b) data-hiding schemes to hide Electronic Patient Records; and c) schemes that combine authentication and data hiding [5].

4. Related Work

Medical images are extremely sensitive as they contain patient information, which requires uncompromising security during both storage and transmission. Several steganography LSB based techniques have been proposed. A study of the recent works was conducted with most concluding that the advantages of steganography based on LSB are that it is easy to implement, it has a high embedding capacity when using more than one bit per pixel, all while assuring that the difference between the resulting stego-image and the original image cannot be visually identified. Also, the different researches agree on the fact that the main shortcoming of this technique is that it is not resistant to attacks like JPEG compression and LSB attacks. Moreover, in case the LSB based technique has high imperceptibility, several research proposals limit attention to only one bit per pixel for data hiding, which results in low capacity.

Akhtar N. *et al.* [3] proposed an improvement to the plain LSB based image steganography. They used the bit inversion technique to improve the stego-image quality. They implemented two schemes of the bit inversion techniques. One technique assumes that the cover image is already transferred to its destination contrarily to the other technique. In both techniques, LSBs of some pixels of the cover image are inverted if they map a pattern of some bits of the pixels. Using this technique they reduce the number of modified bits, which improves the quality of the stego image.

Mei-Ching Chen *et al.* proposed in [14] an LSB steganography method based on Huffman Encoding. Their algorithm has three main parts for the embedding process, starting with the Huffman encoded bit stream of the secret image, followed by the size of the encoded bit stream and ending with the Huffman table corresponding to the secret image. The main objective is to better secure the embedded data without compromising the quality of the stego-image.

Weiqi L. *et al.* proposed in [15] an edge adaptive scheme, which selects the embedding regions according to the size of the secret message and the difference between two consecutive pixels in the cover image, by considering the difference between the pixel and its neighbors. For lower embedding rates, only sharper edge regions are used, while keeping the other smoother regions as they are. They experimented with seven different steganalysis algorithms — the results of hiding data in 6000 natural images. They found that their proposed scheme could enhance the security significantly compared to the typical LSB-based approaches.

Malay Kumar K. *et al.* proposed in [16] a fragile, blind, high payload capacity, medical image watermarking (type of steganography) technique that preserves the Region Of Interest (ROI). The watermark is embedded in the spatial domain. Through experiments, they found that their scheme can maintain Electronic Patient Report (EPR)/DICOM data privacy and medical image integrity. This effectiveness is proven through various image quality measures, such as PSNR, MSE, and MSSIM.

Dharwadkar N.V. *et al.* present in [17] a reversible, fragile, spatial domain watermarking scheme for medical images. They store the key (fingerprint) in unaltered components of the medical image. The key is used to recover the extracted watermark. The extracted watermark is used for copyright justifications.

N. Kumar *et al.* proposed in [18] a new steganography method in spatial domain, which embeds patient information in the cover medical image using a dynamically generated key. The main aim of the proposed method is to generate a key for steganography techniques to maintain the reversibility of the original cover image. Putting aside their analysis of the Peak Signal to Noise Ratio (PSNR) and the Mean Square Error (MSE) that give an idea about the stego-image's quality, the authors did not take into account any type of attacks that may impact their proposed method.

All these techniques focus on the quality of the stego-image and disregard the process's robustness against attacks. Our proposed solution to secure data hiding, to assure the good quality of the stego-image, all while presenting a robust steganography technique.

5. Proposed Technique

5.1 Image clustering with content addressable method

In [19, 20] we proposed a new clustering technique called Content Addressable Method (CAM) that consists of choosing a configurable number of bits for each pixel of the cover image. These bits are used as an address regrouping all entries sharing the same feature. Unlike geometric clustering, in our proposed clustering technique, the pixels that belong to the same cluster may be distinct from each other in geometric points of view, which helps in reducing the effect of attacks. On the other hand, clustering is regrouping the pixels with the same predefined features, used to store a portion of the EPR data, which helps retrieval and adds robustness to the hiding process. The more the distribution of pixels over clusters is uniform, the more the watermark is robust against attacks.

5.2 Cluster dispersal rate

As condense area is liable to attacks, we defined in [19] the dispersal rate (DR) of a set of pixels in the image as the closest area containing these pixels over the total area. We believe that if the cluster dispersal rate is high, the stego-image will be more robust against attacks. For sake of simplicity, we considered only the smallest rectangle holding the set of pixels. We defined two levels of the dispersal rate:

1- The Cluster Dispersal Rate (CDR): This defines the area on the image occupied by a cluster. This normally depends on the image itself and the clustering function. Our proposal in medical images is to consider pushing to a higher CDR by cluster implant. Cluster Dispersal Rate is calculated according to the Equation 1.

$$\mathrm{CDR}_c = \frac{\left(x_{max_c} - x_{min_c}\right) * \left(y_{max_c} - y_{min_c}\right) * 100}{\mathrm{MxN}}, \qquad (1)$$

where, M and N represent the images′sizes and $x_{max}, x_{min}, y_{max}$, and y_{min} are the coordinates of the smallest rectangle containing the cluster c

2- The In-cluster Dispersal Rate (ICDR): It was called in [19] Sub-cluster Dispersal Rate (SDR). The ICDR defines the sub-cluster pixels dispersal within the cluster, which depends on the cluster construction. As we introduce a new technique to implant the cluster, this rate is taken into consideration while implanting. Equation 2 presents the average ICDR of sub-clusters in a given cluster.

$$\mathrm{avg}(\mathrm{ICDR}_c) = \frac{\sum_{sc}\left(x_{max_{sc}} - x_{min_{sc}}\right) * \left(y_{maxs_c} - y_{min_{sc}}\right) * 100}{nsc_c * \left(x_{max_c} - x_{min_c}\right) * \left(y_{max_c} - y_{min_c}\right)}, \qquad (4)$$

Where nsc_c is the number of subclusters in cluster c

5.3 Cluster implant

The crown implant is the base that holds the artificial teeth while hiding its artificial character. In the same way, the cluster implant is the way to insert clusters in the RONI so it can handle the embedding data without visually damaging the image. Table 2 presents two different clustering algorithms. The first algorithm has four steps, starting from step 1 which represents the Content base Addressing Method and, depending on the level of uniformity, the algorithm goes through the remaining steps. As soon as a certain level of uniform distribution is attained the algorithm stops to keep the PSNR acceptable (PSNR is considered not acceptable when it drops below 30 DB and ensures good quality when it is over 35 DB [6]). The second algorithm implants the clusters, taking into account, firstly, the dispersal rate and the distribution uniformity.

Table (1). Clustering algorithm

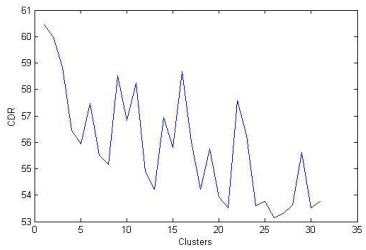
	Algorithm 1	Algorithm 2

Step 1	For each pixel (i, j) of the RONI
	c ← 5 LSBs of R (in RGB) // *c: cluster*
	sc ← 5 LSBs of G (in RGB) // *sc: sub-cluster*
	add the pixel (i j) to the sub-cluster(c, sc)
		c=1
		sc=1
		For each pixel (i, j) of the RONI
		RONI(i,j,1) ← c
		RONI(i.j,2) ← sc
		c = (c+1) mod maxClusters
		subClusters(c)= (subClusters(c)+1) mod maxSubCluster;
		sc=subClusters(c);

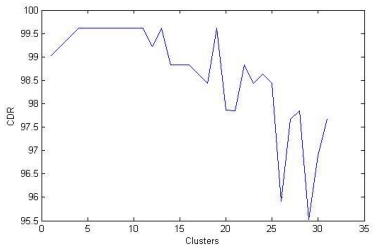
Step 2	For each cluster if subcluster_size > maxduplication Add pixels to a subcluster (subcluster_size < minduplication) within the same cluster by changing only 1 bit of the current subcluster ID. *maxduplication is a parameter that gives the maximum stego-information duplication, any sub-cluster with a size greater than this parameter may be used to implant some sub-clusters, with a size less than minduplication, in its neighborhood.*	
Step 3	For each cluster if subcluster_size > maxduplication Add pixels to a subcluster (subcluster_size < minduplication) in a different cluster by changing only 1 bit of the current cluster ID.	
Step 4	For each cluster if subcluster_size > maxduplication Add pixels to a subcluster (subcluster_size < minduplication) in the same or a different cluster by gradually changing the number of bits of the current subcluster ID or cluster ID.	

The Cluster Dispersal Rate (CDR) is calculated for each cluster. Figure 2 presents the CDR plot for each image. As it can be seen from Figure 2, in Brain 1, using Algorithm 1, clusters occupy between 53% and 60% of the area of the image, whereas, in the remaining images, clusters are dispersed on more than 90% of the area.

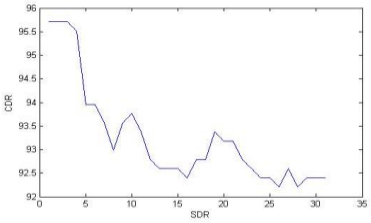
Figure 3 presents the Average In-Cluster Dispersal Rate of sub-clusters using Algorithm 1. It averaged more than 55% of all sub-clusters in *Imaging_Xray* image and is low in all other images that may not resist to cropping attacks.



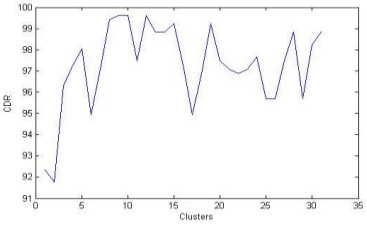
Brain 1



Brain 2

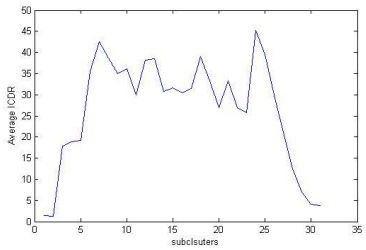


Imaging Xray

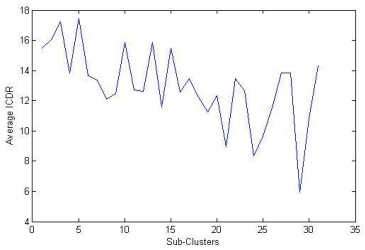


Pic. content Xray

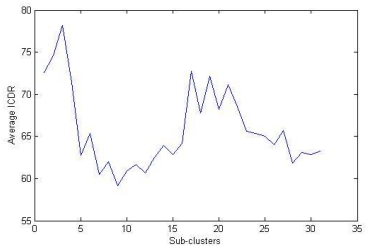
Fig. (2). Algorithm 1 - Clusters Dispersal Rate



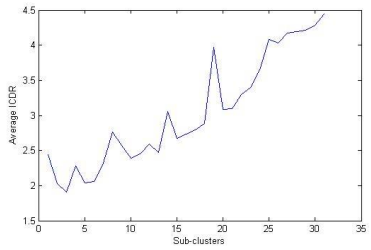
Brain 1



Brain 2

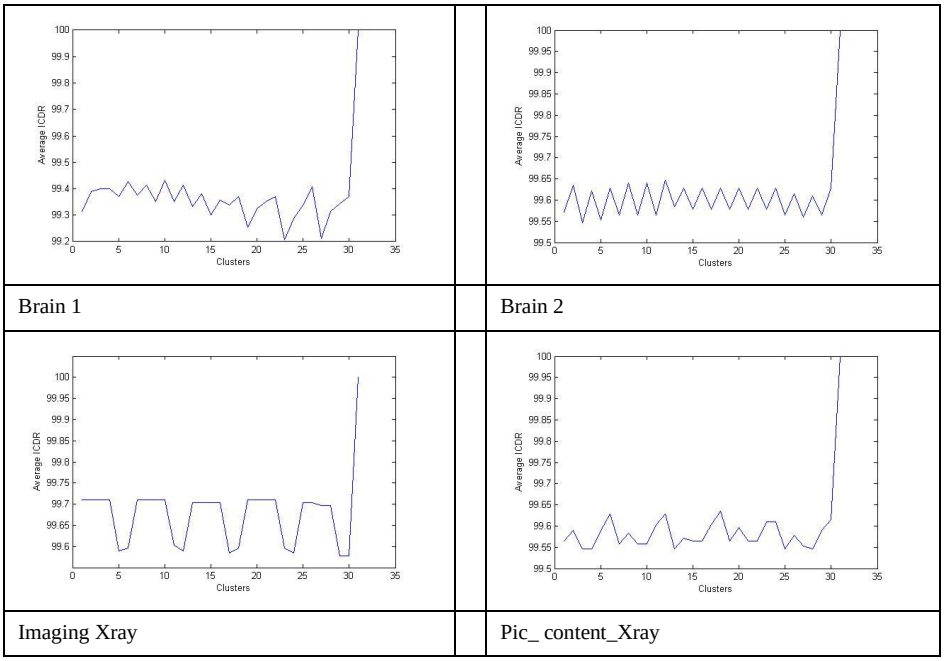


Imaging Xray



Pic. content Xray

Fig. (3). Algorithm 1 - In-Cluster Average Dispersal Rate



Brain 1		Brain 2
Imaging Xray		Pic_ content_Xray

Fig. (4). Algorithm 2 - In-Cluster Average Dispersal Rate

Although algorithm 2 produces a completely uniform distribution, and Figure 4 shows that the ICDR is considerably improved using Algorithm 2, the PSNR (Equation 3) presented in Table 2 severely dropped. For this reason, in the remainder of the paper, we consider the first algorithm.

$$\mathrm{PSNR} = 10\log\left(\frac{\max\left(\mathrm{i}^2(\mathrm{x},\mathrm{y})\right)}{\frac{1}{\mathrm{MxN}}\sum_{\mathrm{y}=1}^{\mathrm{M}}\sum_{\mathrm{x}=1}^{\mathrm{N}}\left(\mathrm{i}(\mathrm{x},\mathrm{y})-\mathrm{w}(\mathrm{x},\mathrm{y})\right)^2}\right) \quad (3)$$

Where; *i(x,y)* and *w(x,y)* is the value of the pixel (x,y), respectively, in the original and stego-image.

Table (2). PSNR Algorithm 1 vs. Algorithm 2

	PSNR Algorithm 1	PSNR Algorithm 2
Brain1	37.45	26.56
Brain2	36.88	27.22
Imaging Xray	41.68	28.33
Pic. content_xray	36.77	27.97

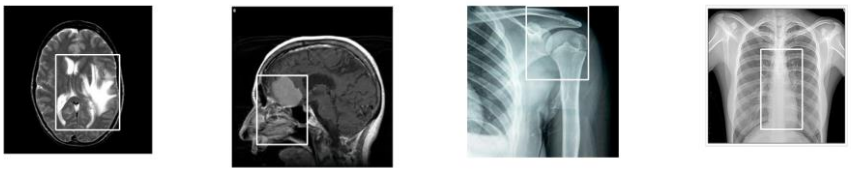
The embedded data is formed by two parts: the Electronic Patient Record and the ROI signature. Figure 5 demonstrates a proposed format of the Electronic Patient Record (EPR). The EPR is the information of the patient that may contain the patient's ID (PID) and the description of the status given by the specialist to which the ROI coordinates, the Upper-Left-pixel-Coordinates (ULPC) and the Lower-Right-Pixel-Coordinates (LRPC) and the Scale of the ROI signature are added, as shown in Figure 1.

PID	**ULPC**	**LRPC**	**Scale**	**Description**
4 bytes	18 bits	18 bits	12 bits	60 bytes

Fig. (5). Electronic Patient Record (EPR)

5.4 Information embedding:

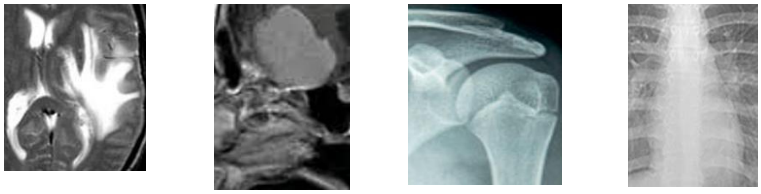
Figure 9 summarizes the embedding process. To secure the ROI part, a ROI signature is formed and inserted with the EPR in the RONI. The ROI signature is a resized binary image of the ROI. The Scale field in the EPR record is providing the size to which the ROI is resized to. The signature can be compared after extraction only visually as to give an idea of whether the ROI has been tampered. Figure 6 shows the original used images where the ROI is indicated. ROI is generally delimited by the specialists.



Brain 1 Brain 2 Imaging_Xray Pic_content_xray

Fig. (6). Original images with delimited ROI

Figure 7 shows the extracted ROI. The binary and resized binary (signature) of each ROI are given in Figure 8.



Brain 1 Brain 2 Imaging_Xray Pic_content_xray

Fig. (7). ROI

Brain 1 Brain 2 Imaging_Xray Pic_content_xray

Fig. (8). ROI (and resized) signature

The flowchart of the embedding process is given in Figure 9.

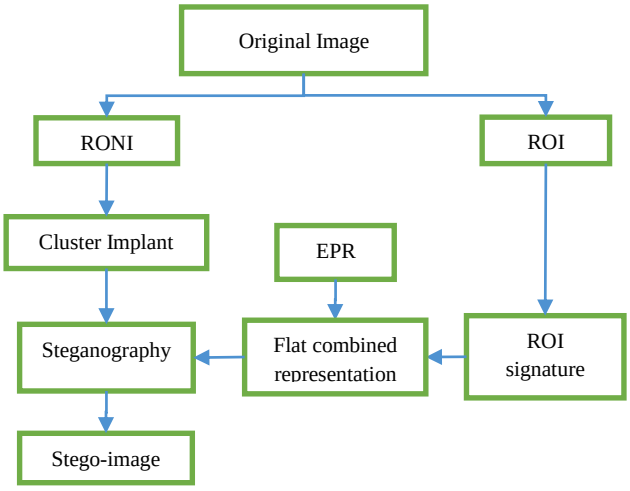


Figure (9). Embedding process

5.5 Information Extraction:

Figure 10 shows the extraction process. The first step of the extraction process is to go through the extraction of the clusters. Each cluster contains sub-clusters that contain the same hidden information. To reduce the tamper effect on the Content Address and the embedded information we use the Decision Building Table we defined in [20]. The sub-cluster value indexes the row of the table, and the value of the embedded information indexes the column. We believe that, if the dispersal rate is high, the probability of changing the same information to the same value is low. In conclusion, the higher counter indicates the appropriate information.

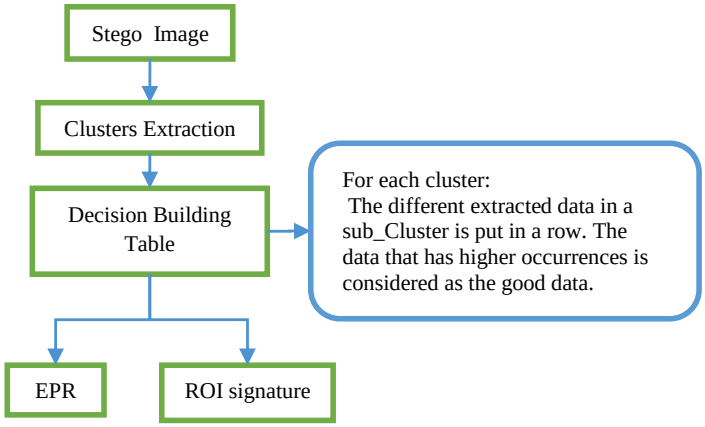
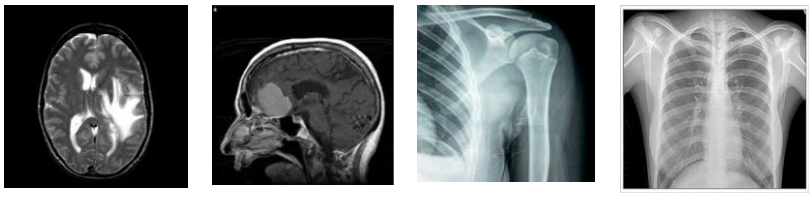


Fig. (10). Extraction process

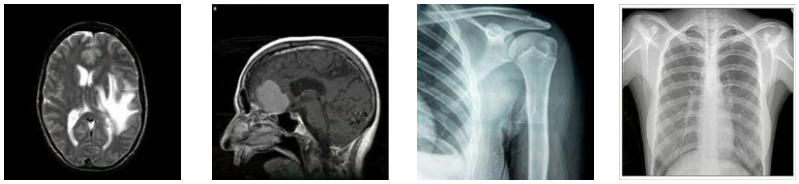
6. Experimental Results

Figures 11, 12, and 13 show the original images, the images after clusters implant, and the stego-images.



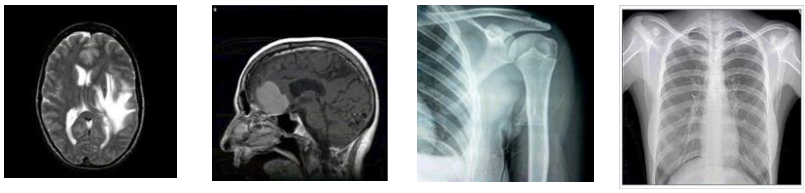
Brain 1 Brain 2 Imaging_Xray Pic_content_xray

Fig. (11). Original images



Brain 1 Brain 2 Imaging_Xray Pic_content_xray

Fig. (12). After clusters implant



Brain 1 Brain 2 Imaging_Xray Pic_content_xray

Fig. (13). Stego images

Table (3). PSNR after clustering and after embedding

	PSNR after clustering implant	PSNR after Embedding
Brain1	37.45	35.91
Brain2	36.88	32.84
Imaging_Xray	41.68	35.07
Pic_content_xray	36.77	32.33

As it can be seen in Table 3, the PSNR is considerably high (greater than 30) in all images after both clusters implant and stego-embedding.

Figure 14 presents the different exerted attacks: rotation 5º, rotation 15º, rotation 125º and cropping.

An example of the extracted signature for each image is shown in Figure 15. The bit error rate (Equation 4) and Normalized Cross Correlation (Equation 5) are used to measure the quality of the extracted EPR and ROI signature:

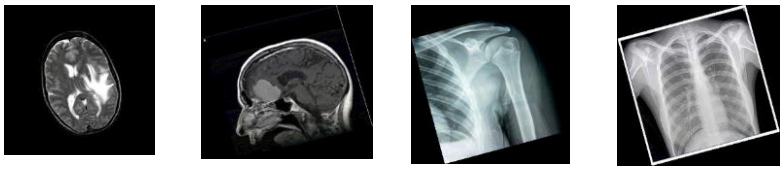
$$BER = \frac{number\ of\ error\ bits * 100}{total\ number\ of\ bits} \quad (4)$$

$$NCC = \frac{\sum_x \sum_y i(x,y)w(x,y)}{\sum_x \sum_y i^2(x,y)} \quad (5)$$

Where; *i(x,y)* and *w(x,y)* is the value of the pixel (x,y), respectively, in the original and stego-image.

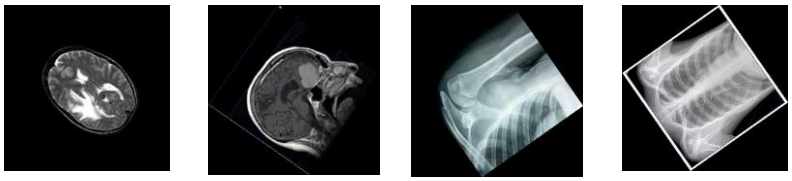
Brain 1 Brain 2 Imaging_Xray Pic_content_xray

Rotation 5°



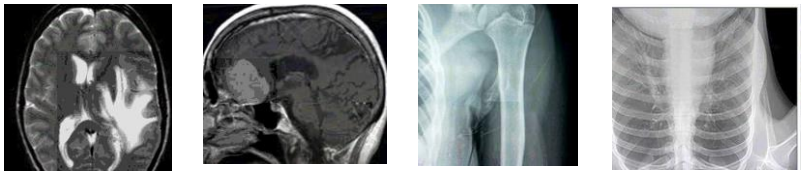
Brain 1 Brain 2 Imaging_Xray Pic_content_xray

Rotation 15°



Brain 1 Brain 2 Imaging_Xray Pic_content_xray

Rotation 125°



Brain 1 Brain 2 Imaging_Xray Pic_content_xray

Cropping

Fig. (14). Attacked stego images

Brain 1 Brain 2 Imaging_Xray Pic_content_xray

Fig. (15). Extracted signatures

Table (4). Brain 1 results

attack	EPR Bit Error Rate	ROI Sig. Bit Error Rate	EPR Cross correlation	ROI Sig. Cross correlation
None	2.13	0.07	0.96	0.79
Rotation 5º	2.13	0.07	0.96	0.79
Rotation 15º	2.13	0.07	0.96	0.79
Rotation 125º	2.13	0.07	0.96	0.79
Cropping 1	2.13	0.07	0.96	0.79
Cropping 2	2.74	0.08	0.95	0.79

Table (5). Brain 2 results

attack	EPR Bit Error Rate	ROI Sig. Bit Error Rate	EPR Cross correlation	ROI Sig. Cross correlation
None	0	0	1	1
Rotation 5º	0	0	1	1
Rotation 15º	0	0	1	1
Rotation 125º	0	0	1	1
Cropping 1	0.61	0.08	0.99	0.94
Cropping 2	1.82	0.17	0.97	0.93

Table (6). Imaging_Xray results

attack	EPR Bit Error Rate	ROI Sig. Bit Error Rate	EPR Cross correlation	ROI Sig. Cross correlation
None	1.22	0.02	0.99	0.98
Rotation 5º	1.22	0.02	0.99	0.98
Rotation 15º	1.22	0.02	0.99	0.98
Rotation 125º	1.22	0.02	0.99	0.98
Cropping 1	1.22	0.02	0.99	0.98
Cropping 2	1.22	0.02	0.99	0.98

Table (7). Pic_content_xray results

attack	EPR Bit Error Rate	ROI Sig. Bit Error Rate	EPR Cross correlation	ROI Sig. Cross correlation
None	0	0	1	1
Rotation 5º	0	0	1	1
Rotation 15º	0	0	1	1
Rotation 125º	0	0	1	1
Cropping 1	1.21	1.50	0.91	0.89
Cropping 2	1.97	1.73	0.92	0.87

Tables 4-7 separately provide the quality of the extracted EPR and signature, after a variety of attacks. We can see that most of the results are promising. The signature NCC is low in Table 4 for all attacks because of the low CDR for the *brain 1* image. Also, the NCC is decreasing in the cropping in Table 7, as a result of the low ICDR of the image *Pic. content. xray*.

7. Conclusions

Using the Internet to transfer medical images has become inevitable, despite the fact that patients' health information can be disclosed or tampered with, either accidentally or intentionally. The aim of this paper is to provide a way to help secure the image's quality and the information it contains. We chose to focus on two types of attacks, namely rotation and cropping. The steganography is made on RONI part of the image, where the Electronic Patient Record and a ROI signature is embedded. The embedding is made on the spatial domain due to its simplicity and capacity. RONI part is divided into clusters. Each cluster is divided into sub-clusters and each sub-cluster holds the same information. Medical and normal images differ in the sense that the ROI part is not used and may not be recognized in the destination, which may impact the extraction. Results show that our technique is robust against rotation attacks. Also, the cropping attacks' effects depend on the CDR and ICDR. Other ways to implant clusters will be looked upon in the future, with a more meaningful way to calculate the dispersal. A study of the combination of the Algorithm 1 and Algorithm 2 of clustering will be a priority.

8. Acknowledgment

The Author gratefully acknowledges financial support for the present work (project ID 2701) from the Deanship of Scientific Research at Qassim University.

9. References

[1] Al-Qershi O. M., Khoo B. E., "ROI–based Tamper Detection and Recovery for Medical Images Using Reversible Watermarking Technique", IEEE International Conference on Information Theory and Information Security (ICITIS), (2010), Beijing, pp. 151 – 155.

[2] Rafael A. S., Marcel P. J., "Assessment of Steganographic Methods in Medical Imaging", XXVI Conference on Graphics, Patterns and Images, SIBGRAPI (2013), Arequipa-Peru.

[3] Akhtar N., Khan S., Johri P., "An Improved Inverted LSB Image Steganography", International Conference on Issues and Challenges in Intelligent Computing Techniques (ICICT), (2014), pp. 749 - 755.

[4] Akhtar N., Johri P., Khan S., "Enhancing the Security and Quality of LSB Based Image Steganography", 5th International Conference on Computational Intelligence and Communication Networks (CICN), (2013), pp. 385 – 390.

[5] Yung-Yi L., Ran-Zan W., "Improved Invertible Secret Image Sharing with Steganography", Seventh International Conference on Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP), (2011), pp. 93 – 96.

[6] Anbarasi L.J., Kannan S., "Secured secret color image sharing with steganography", International Conference on Recent Trends in Information Technology (ICRTIT), (2012), pp. 44 – 48.

[7] Das R., Tuithung T., "A novel steganography method for image based on Huffman Encoding", 3rd National Conference on Emerging Trends and Applications in Computer Science (NCETACS), (2012), pp. 14 – 18.

[8] Sarreshtedari S., and Akhaee M.A., "One-third probability embedding: a new ±1 histogram compensating image least significant bit steganography scheme", *Image Processing, IET*, Vol. (8), No. 2, (2014), pp. 78 – 89.

[9] Prabakaran, G., Bhavani, R., and Rajeswari, P.S., "Multi secure and robustness for medical image based steganography scheme", International Conference on Circuits, Power and Computing Technologies (ICCPCT), (2013), pp. 1188 – 1193.

[10] Keshari S. and Modani S.G., "Weighted fractional Fourier Transform based image Steganography", International Conference on Recent Trends in Information Systems (ReTIS), (2011), pp. 214 – 217.

[11] Zhiyuan Z., Ce Z., and Yao Z., "Two-Description Image Coding With Steganography", *IEEE Signal Processing Letters*, Vol. (15), (2008), pp. 887 – 890.

[12] Thanikaiselvan V. and Arulmozhivarman P., "High Security Image Steganography Using IWT and Graph Theory", IEEE International Conference on Signal and Image Processing Applications (ICSIPA), (2013), pp. 337-342.

[13] Nyeem H., Boles W., and Boyd C., "A review of medical image watermarking requirements for tele-radiology", *Journal of Digital Imaging*, Vol. (26), No. 2, pp. 326-343.

[14] Chen, Mei-Ching, Agaian S.S., and Chen C.L.P., "Generalized collage steganography on images", IEEE International Conference on Systems, Man and Cybernetics, (2008), pp. 1043 – 1047.

[15] Weiqi L., Fangjun H., and Jiwu H., "Edge Adaptive Image Steganography Based on LSB Matching Revisited", IEEE Transactions on Information Forensics and Security, Vol.(5), No. 2, (2010), pp. 201 – 214.

[16] Kundu M.K. and Das S., "Lossless ROI Medical Image Watermarking Technique with Enhanced Security and High Payload Embedding", International Conference on Pattern Recognition, (2010), pp. 1457 – 1460.

[17] Dharwadkar N.V., Amberker B. B., and Supriya & Prateeksha B. P. , "Reversible Fragile Medical Image Watermarking with Zero Distortion", International Conference on Computer and Communication Technology (ICCCT), (2010), pp. 248 – 254.

[18] Kumar N. and Kalpana V., “A Novel Reversible Steganography Method using Dynamic Key Generation for Medical Images”, *Indian Journal of Science and Technology*, Vol. (8), No. 16, (2015).

[19] Mohamed T.B.O, "Novel image clustering based on image features for robust reversible data hiding", *International Journal of Fuzzy Systems and Advanced Applications*, (2015), pp. 1-8.

[20] Mohamed T.B.O, "New Image Watermarking Scheme based on Image Content Addressing Method", The 13th WSEAS International Conference on Applied Computer and Applied Computational Science, (2014).

أمن الصور الطبية باستخدام تقنيات جديدة للإخفاء

محمد طاهر بن عثمان

قسم علوم الكمبيوتر – كلية الحاسب – جامعة القصيم – ص.ب. (٦٦٨٨) – القصيم ٥١٤٥٢

المملكة العربية السعودية

(قدم للنشر ٢٠١٦/٣/٩، قبل للنشر ٢٠١٦/٥/٤)

ملخص البحث.أصبح تبادل المعلومات الطبية للمريض من خلال شبكة الإنترنت، والمعروفة باسم التطبيب عن بعد، حتمي. في الواقع، لأغراض عملية، ملفات المرضى يجب أن تكون مشتركة لعدة مواقع طبية (مع التخصصات المختلفة، على سبيل المثال)، وشركات التأمين. من ناحية أخرى، فإن خصوصية وأمن المعلومات الصحية للمريض يجب أن تصان. ولكن من خلال شبكة الإنترنت، المعلومات الصحية للمريض يمكن الكشف عنها أو العبث بهاإما عن قصد أو غير قصد. ولمعالجة هذه المسألة، أجريت بحوث مكثفة في العقد الماضي لضمان انتقال آمن لهذه المعلومات من خلال إخفاءها داخل الصورالطبية. تزيد أهمية هذه المسألة عند إجراء العمليات الجراحية عن بعد، حيث أن الطبيب المنفذ للعملية الجراحية والمريض لا يتشاركان فعليا نفس المكان. في هذه الحالة، هناك حاجة ماسة لأمن المعلومات في الوقت الحقيقي (Real Time). ولأن هذا مجال لا يزال يتطلب الكثير من البحث، فإننا نقترح تقنية إخفاء المعلومات جديدة على أساس تقسيم المنطقة غير ذات الاهتمام(RONI)من الصورة إلى تكتلات (Clusters) بتقنية جديدة. توضح هذه التقنية الجديدة أنه في حين لم يتم استخدام المنطقة ذات الاهتمام (ROI) من الصورة الطبية، فإن المعلومات المخفية تصمد ضد بعض الهجمات، مثل الدوران والاقتصاص. وتشير النتائج إلى أن درجة الصمود مرتبط بحجم تكرار المعلومة ومعدل انتشارها دخل الصورة.