A Trust Management Scheme for Sharing Secure Medical Images over Cloud Computing Environment

Fatma E.-Z. A. Elgamal, Noha A. Hikal, and F. E. Z. Abou-Chadi

***Abstract*—Recently, sharing patients' history all over the world becomes a necessity to facilitate the storing, transforming and consequently the further diagnosing processes. As for medical images, there are special requirements needed such as the quality that should kept high while preserving the security and privacy arrangements especially when dealing with a public sharing environments such as the cloud computing. Therefore, performing limited sharing through the trust management will help to achieve the security needs. This paper introduce an efficient watermarking technique to guarantee the secure DICOM images sharing over the cloud computing environment using two levels of authentication through private secret key, dynamic embedding/extraction and Cloud watermarking algorithms. The experimental results are promising and showing that the proposed technique gives high PSNR for the watermarked images and their ROI respectively. It also shows robustness against the transition attacking attempts and preserves the DICOM format of the medical images.**

***Index Terms*—Cloud computing, ROI, cloud drops, dynamic embedding, spatial synchronization, watermarking.**

I. Introduction

As a result of the rapid development in the field of technology, a lot of applications began to appear in different disciplines such as teleshopping, bioinformatics, e-banking, telemedicine … etc. Telemedicine, this field that considered as critical one since it includes sending and receiving of the medical images through the healthcare professionals over the telecommunication which in turn facilitate the work of the professionals by overcoming the distance barriers [1]. However, since these critical data are transmitted over the computer networks, this makes it more likely to be attacked especially when the used network is the cloud computing which is a new technology trend that offers resources encapsulation on the Internet in the form of dynamical, scalable, and virtualized services. By exploiting these services, users outsource their data to the cloud so as to enjoy the reduced upfront maintenance and capital costs. However, adopting a cloud computing paradigm may have positive as well as negative effects on the data security of service consumers [2]. A data owner loses control over the data outsourced to a machine that can be physically located anywhere in the world. This machine is operated by a cloud service provider which is located at an unknown location to a data owner [3]. The loss of control over data is further enlarged with the lack of managing users' access to the data from practical cloud computing perspectives. Storage service providers have to guarantee the security of users' data from two main aspects. On one hand, data cannot be revised, damaged, or lost. This is the traditional problem of data security, which could be solved by a lot of existing technical means (such as data backup, recovery backup, virus killing, firewall, etc.)[4], [5]. Security service centers need to intensively provide such services for a large number of data owners. On the other hand, as the data owners care about whether the provider of data storage service will abuse their data, or reveal to the third party without authorization, a trust management between data owners and storage services providers have to exist and this is the target of this study.

One of the solutions that help for achieving the required trust management between the cloud computing parities is the use of any watermarking technique which in turn classifies into two main domains, spatial domain and transformed domain. In the spatial domain which is the most straightforward embedding method, the watermarks are embedded directly in the cover image pixels values [6]. While in the transform domain, the transform coefficients of the cover image are used to embed the watermarks in [1]. Despite the simplicity and the shorter required execution time benefits of the spatial domain, the main drawback of the implemented schemes in this domain is that they divide the cover image into fixed-size blocks of pixels so the hidden data are inserted in the LSB's of each pixel in every block and this can decrease the visibility of the resulted watermarked image which is not acceptable especially in the medical images context [7]. While the transform domain methods that guarantee more robustness against attacks need more processing powers and computation times which face one of the Cloud environment requirements, the fastness on the term of the processes execution [8].

In the present paper, a new scheme (or protocol) to enhance the trust management between the two parties who share secure data over the cloud computing environment is introduced. The proposed method exploits the advantages of the spatial domain technique which is suitable for the cloud environment and at the same time solves the problem of using a fixed-size original images blocks for the watermarking process by applying dynamic embedding process that uses the overall capacity of the cover image for the embedding process to preserve the visual quality of the watermarked medical image. Moreover, the embedding process is not be based on the dynamic embedding only, but also it is based on a secrete key which is known by the two parities only which in turn increases the required security. In addition to the dynamic embedding and secrete embedding

Manuscript received March 1, 2013; revised April 29, 2013.

Fatma E.-Z. A. Elgamal and Noha A. Hikal are with the Information Technology Department, Faculty of Computers and Information System, Mansoura University, Mansoura, Egypt (e-mail: fatma.zahraa@hotmail.com; nmhikal@yahoo.com).

F. E. Z. Abou-Chadi is with the Communication Department, Faculty of Engineering, Mansoura University, Mansoura, Egypt (e-mail: f-abochadi@ieee.org).

DOI: 10.7763/JACN.2013.V1.40

key, the transmitted watermark itself that is extracted through the correct secret key will need another step to finally produce secret authentication information that the recipient use to confirm the owner identity. This was done based on the cloud model that was introduced as an authentication data sharing technique with essential features of digital watermarking technology [9]: 1) Invisibility. Users can't feel the change of the data embedded with watermarks, i.e., the normal usability of a database should be kept. 2) Robustness. The watermark embedded should be able to resist the attack from being deleted, i.e., the watermark still exists when suffering assailant attacks. 3) Detection ability. It is easy to detect the watermark embedded in suspicious database by checking part of data.

In other words the proposed scheme achieves the security goals by providing two means of authentication, one for the sender (owner) of the data to ensure that this is the right recipient and this can be done through the secrete key known only by the owner and the receiver of the data. The other form of authentication can be done by the recipient who confirms the identity of the sender through the authentication information that is hidden in the transmitted image.

The remainder of the paper is organized as follows: Section II presents the proposed scheme in details. Section III presents the experimental results and Section IV is the conclusion and future work.

II. The Proposed Scheme

The traditional watermark synchronization is the process of identifying the correspondence between the spatial coordinates of the watermarked data and that of an embedded watermark. If the coordinates of the embedded watermark have been changed (such as when the watermarked data is rescaled, rotated, translated, shifted and cropped) the detector must identify the coordinates of the watermark prior to detection. Otherwise, if the detector can't synchronize with its input signal, an embedded watermark may not be detectable. Moreover, many of the techniques that are used to attack watermarked signals do not “remove” the watermark, as widely believed, but desynchronize the detector [10].

The proposed scheme utilizes spatial synchronization process. Establishing synchronization would involve an exhaustive search over the space of all possible geometric and spatial transformations to find the watermark. However, the proposed spatial synchronization doesn't involve such process and suites cloud computing needs by dynamically embedding the cloud watermark in a spatial redundancy manner controlled by a predefined key. This key is used to check the users' authorization. Moreover, the proposed method does not use synchronization templates that may be subject to attacks or it may affect the visibility of the watermark. Another advantage of the technique is that the watermark structure is data-dependent, which enhances security level.

The spatial and dynamic embedding/extraction of cloud watermark are done through the following steps. First, the cloud watermark is generated. Second, the framework of the spatial synchronization and dynamic embedding process is accomplished. This will be explained in the following subsections.

A. Cloud Watermark Generation

In cloud watermarking, the watermark is data dependent. Since, it is gathered from the original users' data by applying Cloud Model [11]. Before going through Cloud Model details, this scheme starts by segmenting the most important patients' data part (ROI) to compose the watermark instead of using the whole data [12]. This idea helps a lot in insulating sensitive information from abuse or tampering through sharing environments. In addition, it decreases the processing overhead and meets the requirements of the online applications. The selection for the ROI was done automatically using the algorithm developed by [12] and illustrated in Fig.1. Fig.2 shows the original image with the ROI selection result.

Algorithm 1: ROI selection algorithm
Input: The medical image (MI) of dimensions (M_r x N_c)
Output: The ROI
Steps:
Step 1) Let vectors *L* and *R* are the left and the right edges of the image, of size M_r.
Step 2) Let vectors *T* and *B* are the top and the bottom edges of the image, of size N_c.
Step 3) Select *l=min (L)*, *r=max (R)*, *t=min (T)* and *b=max (B)*.
Step 4) Define the ROI with top left coordinates of (t, l) and bottom right coordinates of (b, r).

Fig. 1. ROI automatic selection algorithm [12].

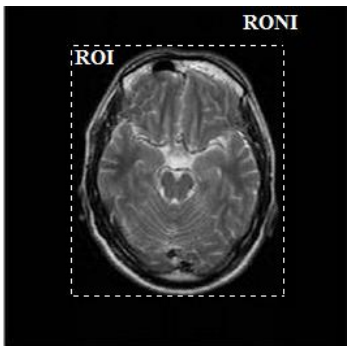

Fig. 2. ROI selection

After specifying the most sensitive part in the image, the next step is to gather the cloud drops that will play an important role in the users' identity assurance phase. To explain the cloud drops, consider *U* be a set described by a precise numbers, and *C* be the qualitative concept related to *U*, if there is a number $x \in U$ which randomly realizes the concept *C*, and the certainty degree of *x* for *C*, i.e., $\mu(x) \in [0, 1]$, is a random value with stabilization tendency:

$$\mu: U \rightarrow [0, 1] \quad ; \quad x \in U \text{ and } x \rightarrow \mu(x) \tag{1}$$

The distribution of *x* on *U* is defined as a cloud, and every *x* is defined as a cloud drop. The more cloud drops there are, the better the overall feature of this concept is represented. Also the more probable the cloud drop appears, the higher the certainty degree is, and hence the more contribution the cloud drop. The overall property of the concept can be represented by numerical values which are the overall quantitative property of the qualitative concept. These numerical values are as follows [11]:

- The expected value (E_x): The mathematical expectation of the cloud drop distributed in the universal set. In other words, it is the point that is most representative of the qualitative concept.
- The entropy (E_n): The uncertainty measurement of the qualitative concept.
- The hyper-entropy ($_{He}$): This is the uncertainty measurement of the entropy, i.e., the second-order entropy of the entropy.

Different implementations lead to different cloud model kinds. The present work considers the normal cloud model based on normal cloud drops distribution. To express the qualitative concept by a quantitative method, cloud drops are generated according to the numerical characteristic of the cloud. This is called "Forward cloud generator" or shortly forward CG. The reverse, i.e, to transfer from the quantitative expression to qualitative concept is called "backward CG", which extracts numerical characteristics from the group of cloud drops [11]. In the present work, we utilized the model developed in [11] and the algorithms of forward and backward CG are shown in Fig. 3.

Fig. 4 shows the cloud drops resulted from the forward CG using E_x=1, and different E_n and H_e values. The results indicate that as $E_n \leq 0.1$, the cloud crops range become near to E_x value which yields to more accurate E_x', E_n', and H_e' values than the other case. In Fig. 4(c), as H_e increases than 0, the cloud drops are more distributed which decrease the accuracy of E_x', E_n', and H_e', while in H_e=0, the cloud drops become a normal distribution which resulting in accurate E_x', E_n', and H_e'. In the present work, E_x, E_n, and H_e values are extracted from the selected ROI then applied to the forward CG to generate number of cloud drops which are then applied to the backward CG to retrieve E_x', E_n', and H_e' values at the receiver side.

Note that, a lot of cloud drops are formed by forward cloud generator and are used to color the user data. When the data are used, the cloud drops are extracted from the watermarked image, and E_x', E_n', and H_e' will be produced by reverse cloud generator. At the detector side, final matching will complete the confirmation.

Algorithm 2: Forward Cloud Generator Algorithm
Input: (E_x, E_n, H_e) and the number of cloud drops n.
Output: n of cloud drops x_i, $i = 1, 2 \ldots n$.
Steps:
Step 1) Generate a normally distributed random number:

$$E_n'_i = NORM\ (E_n, H_e^{\,2})$$

Step 2) Generate a normally distributed random number:

$$x_i = NORM\ (E_x, E_n'^{\,2}_i)$$

Step 3) x_i is a cloud drop in the domain.
Step 4) Repeat Steps 1 to 3, and generate the required number of drops.

Algorithm 3: Backward Cloud Generator Algorithm
Input: Samples x_i, $i = 1, 2 \ldots n$.
Output: (E_x', E_n', and H_e') representative of the qualitative concept
Steps:
Step 1) Calculate the mean and the variance of x_i:

$$\bar{X} = \frac{1}{n}\sum_{i=1}^{n} x_i\ ,$$

$$S^2 = \frac{1}{n-1}\sum_{i=1}^{n}(x_i - \bar{X})^2$$

Step 1) $E_x' = \bar{X}$

Step 2) $E_n' = \sqrt{\frac{\pi}{2}}\left(\frac{1}{n}\sum_{i=1}^{n}|x_i - E_x'|\right)$

Step 3) $H_e' = \sqrt{S^2 - E_n'^{\,2}}$

Fig. 3. Forward and backward cloud generators algorithms [11].

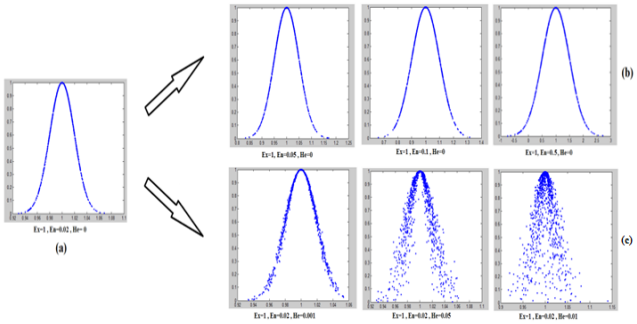

Fig. 4. The resulting cloud drops using (a) E_x =1, E_n=0.02 and H_e=0, (b) E_x =1, E_n=0.05 and H_e=0, E_x =1, E_n=0.1 and H_e=0, E_x =1, E_n=0. 5 and H_e=0 (c): E_x =1, E_n=0.02 and H_e=0.001, E_x =1, E_n=0.02 and H_e=0.05, E_x =1, E_n=0.02 and H_e=0.01

B. *Spatial Synchronization Dynamic Embedding/ Recovery*

Framework for spatial synchronization: When a watermark is embedded into an image, a parameter that defines its structure is the embedding key K_E. The owner uses K_E to generate a spatial schedule, which is used to watermark individual pixels of the image. The goal of the detector is to determine K_E to achieve spatial synchronization. If the detector cannot determine K_E, synchronization is lost. For simplicity, symmetric watermarking techniques are assumed, where the embedding and corresponding detection keys are identical [13].

Therefore, after gathering the suitable number of cloud drops, the next step is to embed theses drops in a dynamic manner controlled by the spatial synchronization key K_E. This key can be used as a seed to generate a random arrangement of the used pixels for the embedding/recovery processes within the medical image. To accomplish this, the Mersenne Twister algorithm [14] was applied which is a pseudo random number generator (PRNG) that in turn uses some kind of mathematical formulas or pre-calculated tables to generate a sequence of numbers that appear random but it is not truly random. It is completely determined by an arbitrary initial state called seed state that can be represented by K_E in this work. The reason for using Mersenne Twister algorithm is because it has a huge period length of $2^{19937} - 1$, very fast, has good equidistributional properties and passing most statistical tests [15].

The resulting schedule specifies the randomly chosen pixels, in spatial domain, to embed the cloud drops. The used key is substantial since without it the destination cannot desynchronize the embedded drops. In other words, it helps the owner to be ensured that this is the right recipient of the data. Therefore, this step represents the first level of authentication between the two parities.

Dynamic Embedding and recovery: For this step, a dynamic embedding/recovery algorithm [7] was adopted and applied. The algorithm helps to overcome the problem of the static embedding algorithms by exploiting the whole medical image's capacity in order to guarantee a high visibility. Moreover, it increases the flexibility in the term of the original medical images' size that can be of any size when it should be greater than or equal to fourfold size of the watermark when working with the static methods.

The spatial synchronization dynamic embedding/extraction steps are carried out through Fig. 5 where MI represents the original medical image, D_i

represents the 8-bit unsigned integer values of the cloud drops that resulted from the forward cloud generator and need to be embedded, where i=1, 2 … l with Dl represents the size of the watermark and WI represents the watermarked medical image. These steps show that the number of the blocks determined dynamically through the sizes of the medical image and the watermark. In addition, the used LSB in each block's pixels are also vary and not static as before. All of these reasons help to enhance the visual quality of the watermarked image.

III. Experimental Results

In this section, the results of testing the performance of the proposed algorithm are reported. Set of DICOM images were obtained from [12].It consists of 20CT and 20MR images. The testing procedure consists of three stages: firstly, a detailed study for the relation between the length of the watermark (D_i), extracted (E_x', E_n', and H_e') and the quality of the watermarked image is performed. Secondly, the cloud drops spatially and dynamically embedding/recovery performances of the proposed algorithm are examined referring to the watermarking embedding/recovery standard metrics. Finally, the robustness of the proposed technique against different types of attacks is investigated.

A. The Watermark Length, Retrieved Cloud Characters and Watermarked Image Quality

The relationships between the length of the watermark (D_i), the retrieved cloud drops characters (*Ex*', *En*', and *He*') and the *PSNR* of the watermarked image were examined. *PSNR* is calculated using (2). In this test, the values of *Ex*', *En*' and *He*' are 1, 0.1, 0 respectively.

$$PSNR = 10\,log_{10}\frac{M * P * R^2}{\sum_{M,P}[MI(m,p) - WI(m,p)]^2} \quad (2)$$

where: R is the maximum fluctuation in the input image data type, M, P are the size of the medical image (MI) and the watermarked image (WI). The calculated values are tabulated in Table I for different values of D_i. As seen from the table, the larger length of D_i resulting in more accurate cloud characters since more drops means more representative of the data. On the other hand, the usage of the dynamic embedding algorithm helps to minimize the effect of the increment in the D_i values.

TABLE I: Values of the Watermark Length, Retrieved Cloud Characters and Watermarked Image PSNR

D_i	Ex '	En '	He '	PSNR (db)	
				Watermarked image	ROI
200	1.0436	0.0824	0.0272	73.4288	73.4865
600	1.0030	0.0944	0.0250	68.4210	68.4157
1000	1.0027	0.1003	0.0177	66.2011	66.2295

B. Embedding/Recovery Performances

Regarding medical watermarking embedding/extraction performances, the most commonly standard metrics are the PSNR, especially of ROI, and the structural similarity (SSIM) index [12].

The SSIM is a very important quality measure to medical images since it places more emphasis on the human visual system (HVS) than PSNR. In other words, it considered as an ideal metric for testing the similarities in medical images because it focuses on local rather than global image similarity [12]. The SSIM is mathematically computed as [12]:

$$SSIM(RI_0, RI_0') = LC(RI_0, RI_0')^{\alpha} \times CC(RI_0, RI_0')^{\beta} \times SC(RI_0, RI_0')^{\lambda} \quad (3)$$

where: RI_0, RI_0' are the image regions for each pair of corresponding blocks. LC is the luminance, CC is the contrast and SC is the structure of RI_0 and RI_0'. α, β and λ are ≥ 1and are used to weight the importance of each of the three components.

Algorithm 4: The spatial synchronization, dynamic embedding
Input: the medical image (MI) and D_i.
Output: The watermarked medical image WI
Steps:
Step 1) Divide MI into blocks, the size of each block (BS) changes according to the size of the MI and Dl. So, the size of the blocks is calculated by:
$BS=\left\lfloor\frac{|MI|}{Dl}\right\rfloor$
Where: |MI| is the number of pixels in MI.
Step 2) Determine the number of LSB that will be replaced with the watermark in each block pixel (B_i), 1=<i<=BS through:

$$Nb = \frac{|D_i|}{BS}$$

Step 3) Since Nb may not be integer, so the number of used bits in each pixel B_i of B is obtained as follow:

$$Ub_i = \begin{cases} \lfloor Nb \rfloor, & if\ i = 1, \dots, BS * \lceil Nb \rceil - |Di| \\ \lceil Nb \rceil, & otherwise \end{cases}$$

Step 4) Use a pseudorandom generator with K_E in each block B_i to randomly arrange the embedded pixels until finally generate WI.

Algorithm 5: The spatial synchronization, dynamic recovery
Input: The watermarked medical image WI, Dl and K_E
Output: cloud characters E_x', E_n', and H_e'
Steps:
Step 1) BS, Nb and Ub_i values are calculated respectively through Steps 1 to 3 in Algorithm 4.
Step 2) K_E is used to generate the spatial schedule of the right sequence of the embedded pixels.
Step 3) By applying Ub_i in each block of the random pixels indicated through K_E, the required 8-bit unsigned integer values of the cloud drops are retrieved.
Step 4) Through using the backward cloud generator, the cloud characters Ex', En', and He' are calculated which used by the destination to confirm the identity of the owner and that provides the second level of authentication between the owner and the destination.

Fig. 5. Spatial synchronization, dynamic embedding/extraction algorithms [7].

TABLE II: PERFORMANCE OF THE PROPOSED METHOD AND [12]

Image Number	Proposed scheme PSNR (db)		PSNR (db) using [12]				Proposed scheme SSIM		SSIM using [12]			
			Wavelet Domain		Contourlet Domain				Wavelet Domain		Contourlet Domain	
	all image	ROI	all image	ROI	all image	ROI	all image	ROI	all image	ROI	all image	ROI
Image 1	68.1665	68.1414	46.4048	67.2762	45.9788	67.8702	1.0000	1.0000	0.9435	0.9989	0.9390	0.9988
Image 2	68.1018	68.0975	45.5991	66.1855	45.0714	67.3513	1.0000	1.0000	0.9395	0.9986	0.9334	0.9988
Image 3	68.1266	68.0806	46.0466	66.3350	46.2871	66.9405	1.0000	1.0000	0.9383	0.9987	0.9343	0.9981

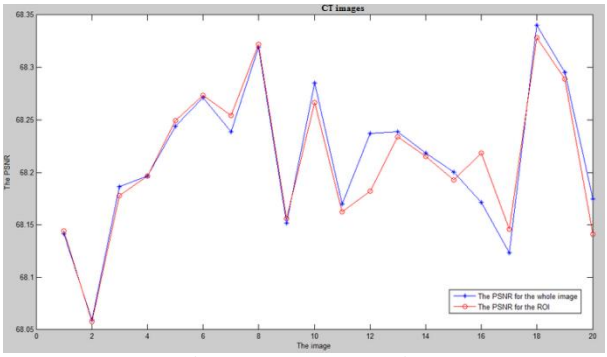

Fig. 6. Curves of PSNR values obtained for each CT image.

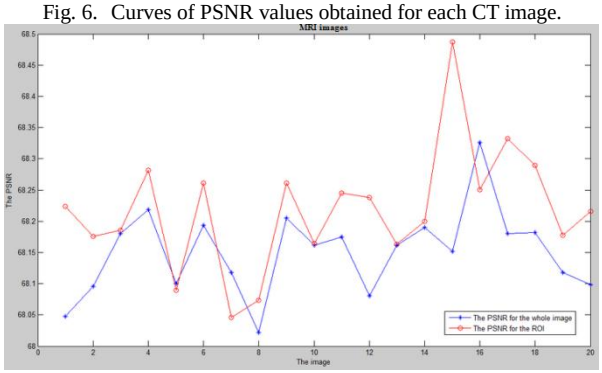

Fig. 7. Curves of PSNR values for the 20 MR images.

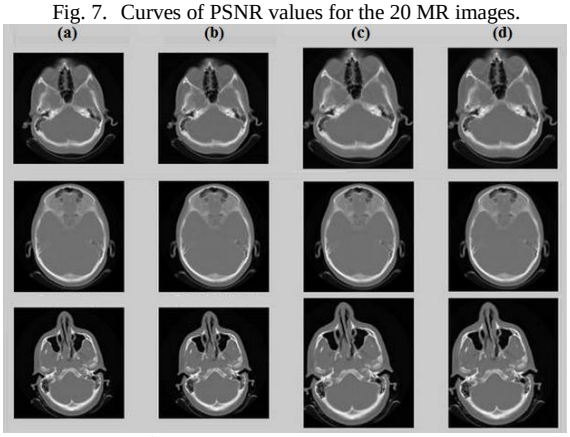

Fig. 8. Samples of CT images: (a) Original image, (b) Watermarked image, (c) Original ROI and (d) Watermarked ROI

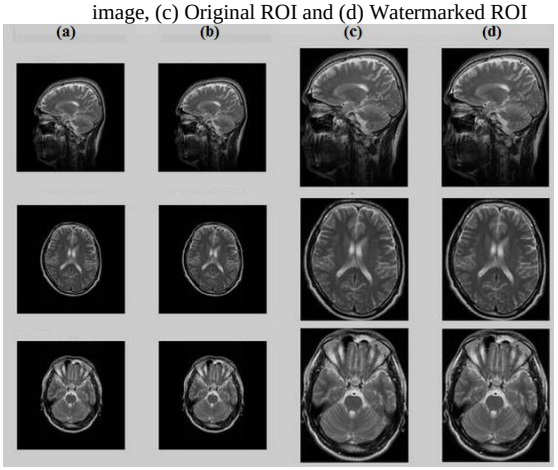

Fig. 9. Samples of MR images: (a) Original image, (b) Watermarked image, (c) Original ROI and (d) Watermarked ROI

Fig. 6 and Fig. 7 show the curves of the PSNR results obtained for the CT and MR images respectively for the full images (blue) and the selected ROI (Red). In Fig. 8 and Fig. 9, a sample of the resulting CT and MRI are illustrated, respectively. Table II tabulates the values obtained from the proposed scheme and those obtained from the algorithm described in [12] using CT images.

The results showed that the proposed scheme provides higher results because of the use of the dynamic embedding which exploits the overall capacity of the cover image to embed the watermark within, which helps to enhance the appearance of the watermarked image. Moreover, the presented scheme preserves the DICOM data format from being changed after the embedding process.

C. *Robustness Against Various Attacks*

The robustness of the proposed scheme against various types of attacks includes (average filter, median filter, salt and pepper noise, resizing and motion filter) is investigated. Table III summarizes the values of PSNR and SSIM of the watermarked image for these attacks.

TABLE III: PSNR AND SSIM VALUES OF THE WATERMARKED IMAGE FOR DIFFERENT ATTACKS

Attack type	PSNR (db)		SSIM	
	all image	ROI	all image	ROI
No attack	68.1018	68.0975	1.0000	1.0000
Average Filter3 ×3	22.8754	29.0718	0.9889	0.9930
Median Filter 3 ×3	35.6092	37.3443	0.9971	0.9970
Wiener Filter 3 ×3	26.8727	29.0718	0.9927	0.9930
Salt & pepper Noise (0.003)	28.1359	28.1237	0.3240	0.3220
Salt & pepper Noise (0.005)	25.8071	25.8114	0.1561	0.1581
Resize 25%	20.4708	12.7745	0.9568	0.7795
Resize 50%	32.6132	15.6247	0.9971	0.9117
Motion (10,45)	11.0357	11.2239	0.7218	0.7273

From the table, it can be noted that the proposed scheme is robust against the average, median, wiener filter and resizing from the values of SSIM. As for the salt and pepper noise, and motion attacks, the values are lower. This is because the watermarking process was performed in the spatial domain which affects the images pixels directly.

The robustness of the watermark against the different attacks can be measured through the bit error rate (BER) which calculated using (4) and aims to measure the ratio of the error on the watermark bits. Moreover, the normalized correlation coefficient (NC) was also calculated using (5) to measure the likeness between the original and the retrieved watermark after the attacks. Table IV shows the values of BER and NC obtained from the proposed and [12]. BER is defined as:

$$BER = \frac{\sum_{i=1}^{l} |w_i - w_i'|}{Dl} \times 100 \qquad (4)$$

where: w_i and $w_i^{'}$ are the original and retrieved watermarks bits respectively and Dl is the size of the watermark.

$$NC = \frac{\sum_{i=1}^{Dl} D_i \times D_i^{'}}{\sqrt{\sum_{i=1}^{Dl} D_i^2}\sqrt{\sum_{i=1}^{Dl} D_i^{'2}}} \quad (5)$$

where: D_i and $D_i^{'}$ are the original and retrieved watermarks respectively and Dl is the size of the watermark.

Table IV shows that the proposed scheme provides better results for the BER because of the dynamic embedding which decrease the density of the watermark inside each pixel in the image so decreasing the total distortion of the watermark bits. The algorithm of [12] gives better values for the NC coefficients. This is because when the distorted bits resulted from applying the proposed scheme used to reconstruct the watermark, the overall likeness between the attacked watermark and the original watermark become less than [12]. For the salt and pepper noise, the proposed scheme provides better results because of the minimal density of this noise which produce minimal affect on the watermark.

TABLE IV: NC AND BER VALUES OF THE ATTACKED WATERMARK

Attack Type	Proposed scheme		[12] results					
			Wavelet domain			Contourlet Domain		
				Signature	Caption		Signature	Caption
	NC	BER	NC	BER	BER	NC	BER	BER
No attack	1	0	1	0	0	1	0	0
Average Filter3 ×3	0	14.0427	0.7960	27.35	34.72	0.9983	0.25	37.08
Median Filter 3 ×3	0	14.1614	1	0	20.18	0.9966	0.50	25.15
Wiener Filter 3 ×3	0	13.8449	1	0	32.85	1	0	36.39
Salt & pepper Noise(0.003)	1	0	0.9211	11.11	10.06	0.9485	7.50	32.73
Salt & pepper Noise(0.005)	0.9689	0.0396	0.9028	13.67	13.72	0.9236	11.00	44.03
Resize 25%	0	12.4011	1	0	42.60	1	0	43.29
Resize 50%	0	15.5459	1	0	20.86	1	0	25.71
Motion (10,45)	0	11.5506	0.8856	15.66	43.97	0.9745	3.75	45.77

As shown above, although the results obtained from [12] showed that it is more robust against the attacking attempts with regards to the ability of retrieving the watermark with minimum distortion, the proposed method on the other hand provides better *PSNR, SSIM* results and higher embedding capacity which are necessary requirements when dealing with medical images. Moreover, the proposed scheme provides acceptable robustness results for the different types of attacks with regard to the attacked watermarked image.

IV. CONCLUSION

Despite all the usefulness of cloud computing, the main issue of security can face users of this new technology since they transmit their data over the cloud environment without any control especially when this data are medical images which contain the patient's critical information. In this work, a novel scheme to enhance the trust management between the two parties transmitting secure medical images over the cloud computing environment is presented. The proposed scheme utilizes the cloud watermark that helps to guarantee the essential features of the digital watermarking methods in addition to the uncertainty and irreversibility process of this model over the digital ones. Moreover, this scheme is implemented using a dynamic embedding/extraction processes to exploit all the capacity of the original image in order to increase the visibility of the resulted watermarked medical image. A private shared key is used to provide spatial synchronization embedding/extraction process in order to enhance the required security needs. The results are promising and showed that the proposed scheme preserves the watermarked medical image into its DICOM data format rather than changing it to any other data format.

ACKNOWLEDGMENT

The authors would like to thank Dr. Hossein Rabbani and Dr. Farhad Rahimi for their help by providing the required medical images used to accomplish this work.

REFERENCES

[1] S. C. Rathi and V. S. Inamdar, "Analysis of watermarking techniques for medical images preserving ROI," *Computer Science & Information Technology (CS & IT 05) - open access-Computer Science Conference Proceedings (CSCP)*, 2012, pp. 297–308.

[2] M. Miller, *Cloud Computing: Web-Based Applications That Change the Way You Work and Collaborate Online*, 2009, ch. 2.

[3] L. Wang, R. Ranjan, and J. Chen, *Cloud Computing: Methodology, Systems, and Applications*, CRC Press, 2011, ch. 1.

[4] B. Furht and A. Escalante, *HandBook of cloud computing*, Springer Science + business Media, LLC, 2010, ch. 2.

[5] B. J. S. Chee, C. Franklin Jr., and C. Franklin, Jr., *Cloud Computing: Technologies and Strategies of the Ubiquitous Data Center*, CRC Press, 2010, ch. 10.

[6] J. M. Zain and M. Clarke, "Reversible Region of Non-Interest (RONI) watermarking for authentication of DICOM Images," *IJCSNS International Journal of Computer Science and Network Security*, vol. 7, no. 9, pp. 19-28, September 2007.

[7] Z. Eslami and J. Z. Ahmadabadi, "Secret image sharing with authentication-chaining and dynamic embedding," *The Journal of Systems and Software*, vol. 84, pp. 803–809, May 2011.

[8] S.-C. Liew, S.-W. Liew and J. M. Zain, "Reversible Medical Image Watermarking For Tamper Detection and Recovery with Run Length Encoding Compression," *World Academy of Science, Engineering and Technology*, vol. 48, pp. 799-803, December 2010.

[9] Y.-C. Liu, Y.-T. Ma, H.-S. Zhang, D.-Y. Li and Gui-Sheng Chen,"A method for trust management in cloud computing: data coloring by cloud watermarking," *International journal of automation and computing*, vol. 8, no. 3, pp. 280-285, August 2011.

[10] B. Javidi, *Optical and digital techniques for information security*, Springer Science + business Media, Inc, 2005, ch. 7, pp. 135-136.

[11] D. Li and Y. Du, *Artificial intelligence with uncertainty*, Chapman and Hall/CRC, September 27, 2007, pp. 107–151.

[12] F. Rahimi and H. Rabbani. (Jun 2011). A dual adaptive watermarking scheme in contourlet domain for DICOM images. *BioMedical Engineering OnLine*. [Online]. 10:53. Available: http://www.biomedical-engineering-online.com/content/10/1/53

[13] F.-H. Wang, J.-S. Pan, and L. C. Jain, *Innovations in Digital Watermarking Techniques*, Springer-Verlag Berlin Heidelberg, 2009, ch. 2, pp. 16.

[14] *MATLAB version 7.6.0.324 (R2008a)*, 2008, computer software, The MathWorks Inc., Natick.

[15] D. P. Kroese, T. Taimre, and Z. I. Botev, *Handbook of Monte Carlo Methods*, Wiley Series in Probability and Statistics, John Wiley & Sons, New York, 2011, ch. 1, pp. 7.

Fatma E.-Z. A. Elgamal studied information technology in Faculty of Computers and Information System, Mansoura University, Mansoura, Egypt where she obtained the B.Sc in 2010. Her interest researches include cloud computing security and biomedicine.
She is now an M.Sc student in Faculty of Computers and Information System, Mansoura University, Mansoura, Egypt.

Noha A. Hikal received the Ph.D degree from Zagazig University, Egypt, in 2008. The B.Sc and M.Sc from Mansoura University, Egypt. In 1998 and 2002, respectively. All in multimedia communications. Her interest researches include network security, cloud computing security, and multeimedia applications.
She is currently a lecturer in the information technology department,faculty of computer science and information system, Mansoura university, Egypt.

Fatma E. Z. Abou-Chadi studied electrical communications engineering in Faculty of Engineering, Ain-Shams University where she obtained the BS in 1974. In 1978, she received her Master degree in Electrical Communications Engineering from Mansoura University. In 1982, she began studying Engineering applied to Medicine at Imperial College of Science and Technology, University of London, UK, where, in 1986, she received PhD degree, specializing in Biomedical Signal Processing and Informatics.

She is currently a professor Emeritus of Electrical Communications Engineering,with the Department of Electronics and Communications Engineering, Faculty of Engineering- Mansoura University. She was the dean of the Faculty of Computers & Information Sciences, Mansoura University during the period 2007-2012 and the Chairwoman of the Department of Electronics & Communications Engineering,, Faculty of Engineering- Mansoura University in 2006-2011. In 2006, she participated in establishing a new BS credit-hour program in Communications and Information Engineering andsince then she has been the Executive Manager of the program.

Dr. Abou-chadi has authored and co-authored more than 90 scientific articles and two books. Her scientific interests and current research work include Biomedical Signal Processing, Medical Imaging and Information Technology. She has exceptional knowledge in digital signal processing and time-series analysis, and has become very interested in information technology in biomedicine.

Dr. Abou-Chadi is a Senior Member at Institute of Electrical and Electronics Engineers – IEEE since 1995, and a Member of the Society of IEEE Women in Engineering since 2000.