Secure Medical Images Sharing over Cloud Computing environment

Fatma E.-Z. A. Elgamal
Information Technology dept.
Faculty of Computers and Information Sciences, Mansoura University
Mansoura, Egypt

Noha A. Hikal
Information Technology dept.
Faculty of Computers and Information Sciences, Mansoura University
Mansoura, Egypt

F.E.Z. Abou-Chadi
Electronics and Communications Engineering dept.
Faculty of Engineering, Mansoura University,
Mansoura, Egypt

***Abstract*—Nowadays, many applications have been appeared due to the rapid development in the term of telecommunication. One of these applications is the telemedicine where the patients' digital data can transfer between the doctors for farther diagnosis. Therefore, the protection of the exchanged medical data is essential especially when transferring these data in an insecure medium such as the cloud computing environment, where the security is considered a major issue. In this paper, two security approaches were presented to guarantee a secure sharing of medical images over the cloud computing environment by providing the mean of trust management between the authorized parities of these data and also allows the privacy sharing of the Electronic Patients' Records string data between those parities while preserving the shared medical image from the distortion. The first approach apply spatial watermarking technique while the second approach implements a hybrid spatial and transform techniques in order to achieve the needed goal. The experimental results show the efficiency of the proposed approaches and the robustness against various types of attacks.**

Keywords—Cloud computing; Electronic Patients' Records; Cloud drops; encryption; spatial synchronization; authentication; Hybrid image watermarking; spatial watermarking; Discrete cosine Transform

I. INTRODUCTION

In recent years and as a result of the fast development in the technology and telecommunications, a lot of digital applications such as the telemedicine start to emerge. This application facilitates the transmission and sharing of the patient's medical data by the healthcare professionals for further diagnosis works [1].

Cloud computing, the environment that offers resources encapsulation on the Internet in the form of dynamic, scalable, and virtualized services [2], presents a variety of on demand services to the public such as the telemedicine services. Over this environment, the user can enjoy a lot of benefits offered by this computing paradigm like transmission, storage, and further processing needs on the user data. In spite of the cloud computing advantages, it has a number of disadvantages such as the data security which considered a major problem that face the users of this technology since they outsource their data to distributed storage systems and not a local ones [3]. Therefore, when transferring user's data over the cloud environment, especially the medical data, this kind of data which contains crucial information about the patients, a high level of protection of the integrity and confidentiality [4] of these data have to be guaranteed to overcome any attacking attempts that may face these transmitted data.

One of the solutions to achieve the required trust management between the cloud computing parities is to use 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 [5]. 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 when dealing with medical images [6]. On the other hand, the transform domain methods can guarantee more robustness against attacks but needs more processing powers and computation times [7].

In recent years and in order to overcome this problem, medical image exchanging over cloud environments has gained a great interest. The medical images present in the cloud can provide the necessary details to the doctors and the patient can seek the treatment in different branch hospital, reduce the information and computational resource maintenance in the hospital. Furthermore, existing medical equipments can be rebuilt to be more efficient and low-cost as medical terminal units. Different proposals were introduced in [8, 9] to deal the exchanging, storing and sharing on medical images in the way that verifying data integrity, availability, and confidently.

This paper introduces two approaches aims to provide the mean of trust management between data parties over the cloud computing environment. The two methods achieve the required goal through providing three levels of authentication, from data owner to the destinations, from the data owner to the cloud service provider and finally from the destination to data owner. For the first approach, the idea of the spatial watermarking techniques has been exploited. While in the second approach, a hybrid model based on the idea of the spatial and the transform techniques were implemented.

In addition to offering the trust management, the proposed approaches allow secure sharing of the Electronic Patients' Record (EPR), which is string data helps to speed up the clinical communication, reduce the diagnostic errors by providing more accurate and timely clinical information and also the EPR assist doctors in diagnosis and treatment [10]. So and since it is considered a sensitive data, the proposed approaches guarantee the protection of them while they are transferred.

The reminder of this paper is organized as follows; Section 2 describes the spatial embedding based approach. Section 3 combine the first approach with discrete cosine Transform to provide hybrid spatial and transform embedding approach. Section 4 presents the experimental results while section 5 shows the paper conclusion.

II. Spatial Synchronization And Dynamic Embedding Approach

The three main stages of this approach are shown in Fig. 1. The first stage dynamically embeds the EPR data into the original medical image. Then, the cloud model is applied to the medical image to extract the approximated version. Finally, the encryption process is done using a symmetric negotiated private key between the authorized parities of the data.

A. *Spatial domain dynamic embedding/extraction algorithm*

The purpose here is to hide the EPR data into the original shared medical image in an effective way that does not affect the visual quality of the medical image using Dynamic Embedding algorithm [6]. The main task is to exploit the overall capacity of the cover image in order to guarantee a high visibility which is a necessity especially when dealing with medical images. Moreover, this method provides a flexibility of cover images' size rather than restricting its size to be more than or equal the fourfold size of the embedded data as in static embedding techniques.

In other words, this step gets the benefits of the shorter execution time associated with spatial watermarking algorithms. But in the same time and due to the usage of the dynamic embedding algorithm, it can overcome the drawback of inserting the hiding data in the LSB of the cover image block pixels that decrease the visibility of the resulting image.

In addition to the dynamic embedding algorithm, symmetric secret key (K_1) was applied to perform a spatial synchronization embedding/extraction processes through using this key as a seed in a pseudo random number generator (PRNG) in order to generate random arrangement of the used pixels for the embedding/extraction processes within the medical image. To accomplish this, the Mersenne Twister algorithm [11] 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_1 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 [12].

Spatial synchronization dynamic embedding phase: The cover medical image (CMI) and the EPR string data (D_i) are the inputs of this step where their sizes, |CMI| and l respectively, are used to dynamically determine the size of each block of which the cover image is divided in and for the LBS used for the embedding process. In addition, to the added security, changing the known static embedding ways and using secret key (K_1) for rearranging the pixels used in the embedding process. Dynamic embedding process also improves the visibility by regulating the embedding steps according to the used inputs. This is required especially for the medical images where high quality is a major aspect that has to be guaranteed. Fig. 2 illustrates the steps of this phase and how the dynamic idea is applied for the required embedding process.

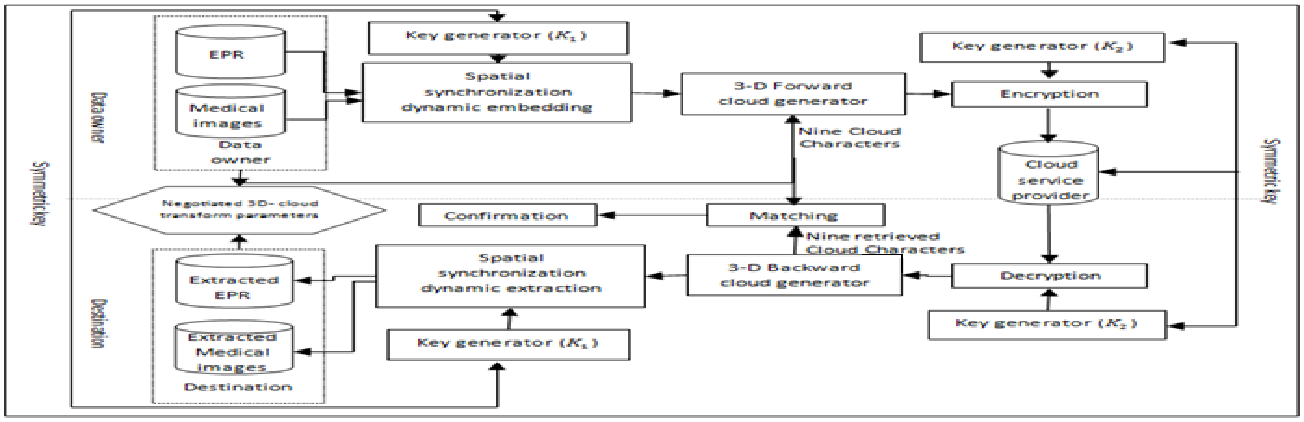


Fig. 1. The proposed scheme framework

1) Spatial synchronization dynamic extraction phase: Fig. 3 show the required steps for the extraction phase. It illustrates how the EPR data can be extracted in a dynamic manner using the same key used in the embedding phase.

B. The 3D cloud generation

The aim of this step is to generate approximated shared medical image after embedding the EPR data to form both the required image to be shared and at the same time represents one level of authentication that is used by the destination of the data in order to confirm the identity of data owner. To accomplish this, three dimension cloud model is applied, with six cloud characters E_x, E_y, E_z, E_{nx}, E_{ny}, E_{nz}, H_{ex}, H_{ey}, H_{ez} used for the required confirmation step. This is an expansion form of one dimension cloud model [13] where the expected value (E_x) is the point that is most representative of the qualitative concept, the entropy (E_n) is The uncertainty measurement of the qualitative concept which is determined by both the randomness and the fuzziness of the concept to represent the measurement of randomness and the value region in which the drop is acceptable by the concept, and the hyper-entropy (H_e) is the second-order entropy of the entropy.

These values are the general concepts that are applicable in one-dimensional and can be extended to higher dimensional situations. According to these cloud characteristics, the next step is to perform a "forward cloud generator" that aims to generate cloud drops to express the concept quantitatively. Then, to extract the cloud characteristics, the "Backward cloud generators" is applied to the previously generated cloud drops.

Therefore, by expanding the one-dimensional cloud model into a three-dimensional model, whereE_x, E_y and E_z are refers here to the components of the RGB colour format of the original image. Algorithm 3 and algorithm 4 represent the forward and backward cloud generators in the three-dimensional model as shown in Fig. 4 and Fig. 5.

```
Algorithm 1: Spatial synchronization dynamic embedding algorithm
Input: the cover medical image (CMI) and $D_i$.
Output: The watermarked medical image WMI
 Step 1) Divide CMI into blocks (B) with sizes (BS) changes
         according to the size of the CMI and l. So, BS will be:
         $BS=\left\lfloor\frac{|CMI|}{l}\right\rfloor$
Where: |CMI| is the size of the CMI.
 Step 2) Determine the number of LSB where the hidden data
         will be replaced in each block pixel ($B_i$), 1=<i<=BS
         through:
         $Nb = \frac{|D_i|}{BS}$
 Step 3) Since Nb may not be integer, the number of used bits
         in each pixel $B_i$ of B is obtained as:
         $Ub_i = \begin{cases} \lfloor Nb \rfloor, & if\ i = 1, \dots, BS * \lceil Nb \rceil - |Di| \\ \lceil Nb \rceil, & otherwise \end{cases}$
 Step 4) Use a pseudorandom generator with $K_1$ to embed the
         $D_i$ bits into the corresponding rearranged pixels bits inside
         $B_i$s' according to $Ub_i$ until finally construct the WMI.
```

Fig. 2. Spatial synchronization dynamic embedding algorithm [6]

```
Algorithm 2: Spatial synchronization dynamic extraction algorithm
Input: The watermarked medical image WMI, l.
Output: EPR data
 Step 1) Calculate BS, Nb and $Ub_i$values respectively through
         Fig. 2.
 Step 2) Apply $Ub_i$ in each block pixel determined by $K_1$,
         which generates spatial schedule of the right sequence of
         the embedded pixels, to retrieve the embedded EPRs' bits.
 Step 3) Use the retrieved bits to finally reconstruct the
         required EPR data.
```

Fig. 3. Spatial synchronization dynamic extraction algorithm [6]

```
Algorithm 3: Three dimensional Forward Cloud Generator
Input: ($E_x$, $E_y$, $E_z$, $E_{nx}$, $E_{ny}$, $E_{nz}$, $H_{ex}$, $H_{ey}$, $H_{ez}$ ), WMI
Output: the Approximated Shared Image (ASI)
Step 1) Generates three-dimensional normally distributed
        random vector (${E_{nx}}'_i, {E_{ny}}'_i, {E_{nz}}'_i$) where:
$E_{nx}{}'_i = NORM\ (E_{nx}, {H_{ex}}^2)$
$E_{ny}{}'_i = NORM\ (E_{ny}, {H_{ey}}^2)$
$E_{nz}{}'_i = NORM\ (E_{nz}, {H_{ez}}^2)$
Step 2) Generates three-dimensional normally distributed
        random vector ($x_i, y_i, z_i$) where $x_i$, $y_i$ and $z_i$ are cloud
        drops in each of the images' dimensions.:
$x_i\ = NORM\ (E_x, {E_{nx}}'^2_i)$
$y_i\ = NORM\ (E_y, {E_{ny}}'^2_i)$
$z_i\ = NORM\ (E_z, {E_{nz}}'^2_i)$
Step 3) Repeat Steps 1 to 3, in the entire WMI pixels to
        generate the required approximated shared image (ASI).
```

Fig. 4. Three dimensional Forward Cloud Generators

```
Algorithm 4: Three dimensional Backward Cloud Generator
Input: Approximated Shared Image (ASI)
Output: (${E_x}'$, ${E_y}'$, ${E_z}'$, ${E_{nx}}'$, ${E_{ny}}'$, ${E_{nz}}'$, ${H_{ex}}'$, ${H_{ey}}'$, ${H_{ez}}'$).
 Step 1) Calculate Ex', Ey' and Ez':
         ${E_x}' = \bar{X} = \frac{1}{n}\sum_{i=1}^{n} x_i$ ,
         ${E_y}' = \bar{Y} = \frac{1}{n}\sum_{i=1}^{n} y_i$ ,
         ${E_z}' = \bar{Z} = \frac{1}{n}\sum_{i=1}^{n} z_i$
 Step 2) Calculate ${E_{nx}}'$, ${E_{ny}}'$ and ${E_{nz}}'$:
         ${E_{nx}}'=\sqrt{\frac{\pi}{2}}\left(\frac{1}{n}\sum_{i=1}^{n}|x_i - {E_x}'|\right)$,
         ${E_{ny}}'=\sqrt{\frac{\pi}{2}}\left(\frac{1}{n}\sum_{i=1}^{n}|y_i - {E_y}'|\right)$,
         ${E_{nz}}'=\sqrt{\frac{\pi}{2}}\left(\frac{1}{n}\sum_{i=1}^{n}|z_i - {E_z}'|\right)$
 Step 3) Calculate ${H_{ex}}'$, ${H_{ey}}'$ and ${H_{ez}}'$ using the variances ${S_x}^2$,
         ${S_y}^2$ and ${S_z}^2$:
         ${S_x}^2 = \frac{1}{n-1}\sum_{i=1}^{n}(x_i - \bar{X})^2$, then ${H_{ex}}'= \sqrt{{S_x}^2 - {E_{nx}}'^2}$
         ${S_y}^2 = \frac{1}{n-1}\sum_{i=1}^{n}(y_i - \bar{Y})^2$, then ${H_{ey}}'= \sqrt{{S_y}^2 - {E_{ny}}'^2}$
         ${S_z}^2 = \frac{1}{n-1}\sum_{i=1}^{n}(z_i - \bar{Z})^2$, then ${H_{ez}}'= \sqrt{{S_z}^2 - {E_{nz}}'^2}$
```

Fig. 5. Three dimensional Backward cloud Generator

C. Encryption/Decryption Technique

In this step, cryptographic algorithm [14] with pseudorandom number generator was applied for the encryption/decryption. The idea is that, the owner of the data uses a private key K_2 to generate a spatial schedule, which is used to encrypt the required approximated shared image. The goal of the detector is to use K_2 for the decryption process. For simplicity, symmetric technique is assumed, where the encrypting and corresponding detection key is identical [15].

K_2 is used as a seed to a pseudo random number generator (PRNG) using the Mersenne Twister algorithm, for the reasons illustrated in subsection II.A, to provide random arrangement of the pixels for the encryption/decryption processes on the shared image.

The resulting schedule rearranges the image pixels randomly, in spatial domain, to encrypt the approximated watermarked image. The used key is substantial to desynchronize the encrypted image at the destination. In other words, it helps the owner to be ensured about the identity of the data recipient. In other words the usage key provides a mean of authentication between the data owner and the service provider and also between the data owner and the destination of the shared data since they are the legal recipients of the data.

III. Spatial Synchronization, Dynamic And Transform Embedding Approach

In this approach, the same stages of Fig. 1 are performed but rather than using the dynamic embedding algorithm only to perform the embedding process, the second approach uses both dynamic embedding along with the Discrete Cosine Transform DCT algorithm and Inverse Discrete Cosine Transform IDCT that are widely used transform algorithms [16] to perform the embedding process.

The purpose of the extra step here is to get the benefit of the DCT algorithm that provides more robustness against attacks than the spatial embedding algorithms so it can help to preserve the hidden data much better than the first approach. While the first approach guarantee more fast computations than this approach.

The inserted steps were in the embedding/extraction stages. Therefore the new algorithms are as shown in Fig. 6 and Fig. 7.

```
Algorithm 5: Spatial synchronization dynamic and transform embedding algorithm
Input: the cover medical image (CMI) and $D_i$.
Output: The watermarked medical image WMI
  Step 5)  Divide CMI into blocks (B) with sizes (BS) changes according to the size of the CMI and l. So, BS will be:
           $BS=\left\lfloor \frac{|CMI|}{l} \right\rfloor$
Where: |CMI| is the size of the CMI.
  Step 6)  Determine the number of LSB where the hidden data will be replaced in each block pixel ($B_i$), 1=<i<=BS through:
           $Nb = \frac{|D_i|}{BS}$
  Step 7)  Since Nb may not be integer, the number of used bits in each pixel $B_i$ of B is obtained as:
           $Ub_i = \begin{cases} \lfloor Nb \rfloor, & if\ i = 1, \dots, BS * \lceil Nb \rceil - |Di| \\ \lceil Nb \rceil, & otherwise \end{cases}$
  Step 8)  Use a pseudorandom generator with $K_1$ to rearranged pixels bits inside $B_i$s'.
  Step 9)  Transform the rearranged pixels using DCT.
  Step 10) Embed the $D_i$ bits into the rearranged transformed pixels according to $Ub_i$.
  Step 11) Retransform the resulted pixels after the embedding process using IDCT.
```

Fig. 6. Spatial synchronization dynamic and transform embedding algorithm

```
Algorithm 6: Spatial synchronization dynamic extraction algorithm
Input: The watermarked medical image WMI, l.
Output: EPR data
Steps:
  Step 4)  Calculate BS, Nb and $Ub_i$ values respectively through Fig. 2.
  Step 5)  Apply $Ub_i$ in each block pixel determined by $K_1$, which generates spatial schedule of the right sequence of the embedded pixels.
  Step 6)  Transform the rearranged pixels using DCT.
  Step 7)  Retrieve the embedded EPRs' bits from the transformed pixels values.
  Step 8)  Use the retrieved bits to finally reconstruct the required EPR data.
```

Fig. 7. Spatial synchronization dynamic and transform extraction algorithm

IV. Experimental Results

The results of the proposed schemes have been carried out inside MATLAB environment with a set of 350×350×3 MR images obtained from standard web portal for MRI images [17]. Moreover, MRI images from standard web portal [18] were used for further investigation of the proposed scheme efficiency. Then, in order to test the quality of the both schemes, numbers of quality metrics were applied. These metrics include Mean square Error (MSE) and peak signal to noise ratio that were calculated using (1) and (2) respectively. Structural similarity (SSIM) index address was also applied to measure the local images similarities and it was measured through (3). The number of changing pixel rate (NPCP) and the unified averaged changed intensity (UACI) metrics to test the number of changed pixels and the number of averaged changed intensity respectively between encrypted/decrypted images [19] were also calculated using (4), (5) and (6) respectively. Finally, to measure the rate of the bits error (BER), (7) was used in order to check the performance of the proposed schemes in the presence of the attacking attempts.

$$MSE = \frac{1}{MP} \sum_{i=0}^{M-1} \sum_{j=0}^{P-1} [OMI(i,j) - RMI(i,j)]^2 \qquad (1)$$

$$PSNR = 10\, log_{10} \left(\frac{R^2}{MSE} \right) \qquad (2)$$

Where R is the maximum fluctuation in the input image data type, M, P are the sizes of the original medical image (OMI) and the retrieved medical images (RMI) respectively [20]

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

Where: OMI, RMI are the original and the reconstructed medical images respectively? LC is the luminance, CC is the contrast and SC is the structure of OMI and RMI. α,β and λ are ≥ 1 and are used to weight the importance of each of the three components. [20]

$$D(i,j) = \begin{cases} 0, if\ OMI(i,j) = RMI(i,j) \\ 1, if\ OMI(i,j) = RMI(i,j) \end{cases} \quad (4)$$

$$NPCR: N(OMI, RMI) = \sum_{i,j} \frac{D(i,j)}{T} \times 100\% \quad (5)$$

$$UACI: U(OMI, RMI) = \sum_{i,j} \frac{|OMI(i,j) - RMI(i,j)|}{F.T} \times 100\% \quad (6)$$

Where F denotes the largest supported pixel value of the image format and T represents the size of the OMI and RMI [19].

$$BER = \frac{100}{l} \sum_{i=1}^{l} \begin{cases} 1, D_i' = Di \\ 0, D_i' \neq Di \end{cases} \quad (7)$$

Where D_i and D_i' are the i^{th} bit of the embedded and the recovered EPR data respectively and l is the length of the EPR data [21].

Before going through these measurements, the processing time of the both approaches were illustrated in Tables 1 and 2. These results were computed on a personal computer worked with Intel (R) Core (TM) i3 CPU, 2.53 GHz and installed memory (RAM) of 2.00GB (1.86 GB usable).

The results in the tables shows that the first approach that apply only the dynamic embedding algorithm has less processing time since it performs the embedding/extraction processes in the spatial domain and dealing with the pixels bits directly. While in the second and because of converting the pixels to their DCT coefficients this consume some additional time to perform the embedding/extraction processes.

TABLE I. PERFORMANCE EVALUATION OF THE FIRST APPROACH

	Processing time (sec)	Addition / subtraction	Multiplication / Division	Special functions
EPR spatial synchronization dynamic embedding step:	0.23	4631	6	2298
3D Forward Cloud Generator:	2.37	735000	735001	735000
Encryption step:	0.84	367500	1	2
Decryption step:	0.66	367500	1	2
3D Backward Cloud Generator:	1.35	10637	6	54
EPR spatial synchronization dynamic extraction step:	0.19	1249	6	2296

TABLE II. PERFORMANCE EVALUATION OF THE SECOND APPROACH

	Processing time (sec)	Addition / subtraction	Multiplication / Division	Special functions
EPR Spatial synchronization, dynamic and transform embedding step:	0.4	4631	6	5146
3D Forward Cloud Generator:	2.28	735000	735001	735000
Encryption step:	0.87	367500	1	2
Decryption step:	0.66	367500	1	2
3D Backward Cloud Generator:	2.26	10637	6	54
EPR Spatial synchronization, dynamic and transform extraction step:	0.28	1249	6	3720

Now, to evaluate the images quality, Table 3 and 4 were constructed. Tables 3 show that the first approach guarantees lossless reconstruction of the transferred medical images in the absence of the attacks. Table 4 shows some degree of distortion in the second approach due to the quantization operations performed during the embedding stage. But it still provides acceptable quality results as shown especially for the *SSIM* that considered as an ideal metric for testing similarities in medical images due to focusing on the local rather than global image similarity and placing more emphasis on the Human Visual System (*HVS*) than *PSNR* [20]. In general, the high results of the both approaches have been achieved due to the usage of the dynamic embedding algorithm that exploits the overall capacity of the cover image for the embedding process. In addition to that, applying *Enx*, *Eny*, *Enz* values less than or equal to 0.1 and *Hex*, *Hey*, *Hez* values equal to zero helps to generate an approximated images that most represents the original images.

Fig. 8 and Fig. 9 shows the resulting images after each step of the both approaches respectively. Start with Fig. 8 (a) that represents the original images, then after adding the EPR data shown in Fig. 10(a) through using the dynamic embedding algorithm the results will be as shown in Fig. 8 (b). The 3D-CT approximation images are shown in Fig. 8 (c) whereE_x, E_y and E_z equals to colour channels pixels of the medical images, E_{nx}, E_{ny} and E_{nz} values equal to 0.1, 0.01 and 0.02, H_{ex}, H_{ey} and H_{ez} equals to zero. The encrypted versions are then shown in Fig. 8 (d). These images can reside in the cloud service provider CSP where the first level of authentication can takes place between the data owner and the CSP throughK_2. Then, after the arrival of these encrypted images to the destination, the destination uses K_2 to decrypt the images which in turn provide the second level of authentication and obtain the results shown in Fig. 8 (e). Then the destination performs 3D backward cloud generator to retrieve the cloud characters (E_x', E_y', E_z', E_{nx}', E_{ny}', E_{nz}', H_{ex}', H_{ey}' *and* H_{ez}') to accomplish the confirmation of the data owner identity that provides the third level of authentication. Finally the destination applies K_1 to finally get the hidden EPR data as shown in Fig. 10(b) and Fig. 10(c) from the two approaches respectively.

In Fig. 9 that refers to the second approach results, the same procedures were applied except for the embedding step which accomplished in the second approach through using dynamic embedding algorithm along with the DCT technique to provide more robustness against attacks.

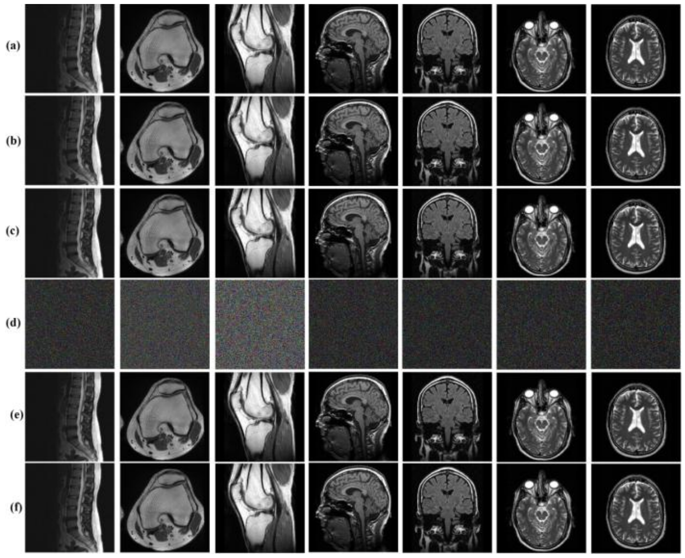


Fig. 8. The results of the first approach (a) The original medical images, (b) The images after embedding process, (c) The approximated images (d) The encrypted images, (e) The decrypted images, (f) The reconstructed lossless medical images

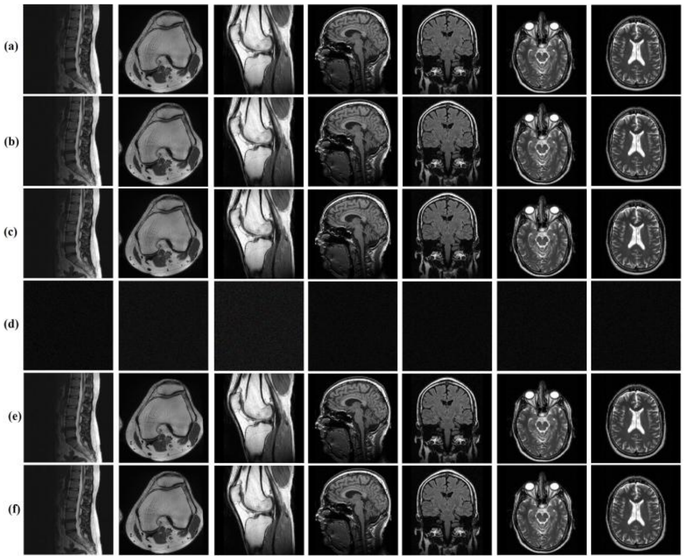
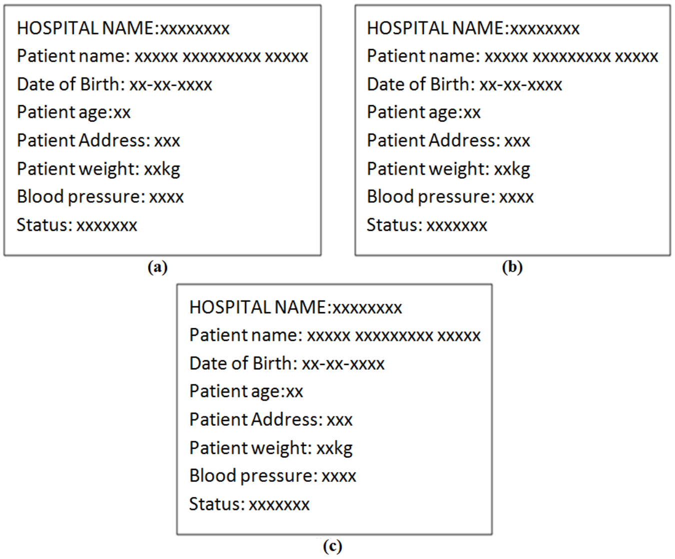


Fig. 9. The results obtained from the second approach (a) The original medical images, (b) The images after embedding process, (c) The approximated images (d) The encrypted images, (e) The decrypted images, (f) The reconstructed medical images



HOSPITAL NAME:xxxxxxxx
Patient name: xxxxx xxxxxxxxx xxxxx
Date of Birth: xx-xx-xxxx
Patient age:xx
Patient Address: xxx
Patient weight: xxkg
Blood pressure: xxxx
Status: xxxxxxx

(a)

HOSPITAL NAME:xxxxxxxx
Patient name: xxxxx xxxxxxxxx xxxxx
Date of Birth: xx-xx-xxxx
Patient age:xx
Patient Address: xxx
Patient weight: xxkg
Blood pressure: xxxx
Status: xxxxxxx

(b)

HOSPITAL NAME:xxxxxxxx
Patient name: xxxxx xxxxxxxxx xxxxx
Date of Birth: xx-xx-xxxx
Patient age:xx
Patient Address: xxx
Patient weight: xxkg
Blood pressure: xxxx
Status: xxxxxxx

(c)

Fig. 10. The used EPR data, (a) Original EPR data, (b) Retrieved EPR data using first approach, (c) Retrieved EPR data using second approach

The scheme presented in [22] also provides a lossless retrieval of the shared image while preserving the resulting images from pixels expansion. But it offers only one level of authentication. The presented approaches here preserve the images from pixels expansion; guarantee high level of visibility of the retrieved images and at the same time offers three levels of authentication between the all authorized parties of the shared data, the owner of the data, the cloud service provider and finally the destination of the shared data which consists of the shared image and the EPR data.

Finally, the robustness of the proposed approaches has been evaluated through calculating the MSE and the PSNR for the attacked images as presenting in Tables 5 and 6 and calculating the BER for the hidden EPR data as shown in Tables 7 and 8.

Tables 5 and 6 shows that the proposed schemes provide higher degree of robustness with respect to [23, 24, 25, 26]. This means that the both approaches help to deliver the shared data to the other side of the communication with an acceptable level of quality.

For the BER results, the illustrated results in Tables 7 and 8 shows that the proposed schemes provide higher degrees of robustness under salt and pepper noise than the other attacks types. This is because salt and pepper noise affects random pixels and so not the whole embedded data were be altered. For the other attacks that affect the entire image pixels, the effect on the embedded data would be larger and hence higher BER values. The tables also shows that the second approach provides higher robustness results than first approach in most types of attacks and this is due to applying discrete cosine transform in the embedding step that helps to achieve higher robustness results against attacks as compared with performing the embedding process using dynamic embedding that is a spatial embedding algorithm.

For the salt and pepper noise, the second approach shows less robustness results than the first approach since the salt and pepper noise in the first approach affects the pixels themselves and do not propagate the distortion leading to minimum BER values. While in the second approach the distortion propagates and causes modifications in the coefficients values that increase the effects on the BER results as compared with the first approach. Moreover, the second approach, that is a hybrid between the spatial and the transform embedding processes, shows acceptable results with respect to [27].

TABLE III. QUALITY EVALUATION OF THE FIRST APPROACH

Image	MSE	PSNR (db)	SSIM	NPCR	UACI
Image 1	0	Infinity	1.000	0	0
Image 2	0	Infinity	1.000	0	0
Image 3	0	Infinity	1.000	0	0
Image 4	0	Infinity	1.000	0	0
Image 5	0	Infinity	1.000	0	0
Image 6	0	Infinity	1.000	0	0
Image 7	0	Infinity	1.000	0	0

TABLE IV. QUALITY EVALUATION OF THE SECOND APPROACH

Image	MSE	PSNR (db)	SSIM	NPCR	UACI
Image 1	0.0940	58.3988	0.9997	0.3461	0.0031
Image 2	0.0239	64.3420	1.000	0.3306	0.0014
Image 3	0.4962	51.1744	0.9987	0.6604	0.0140
Image 4	0.1408	56.6460	0.9999	0.3412	0.0036
Image 5	0.1337	56.8688	0.9999	0.3861	0.0035
Image 6	0.1017	58.0587	0.9997	0.2612	0.0029
Image 7	0.1350	56.8263	0.9998	0.2718	0.0034

TABLE V. PSNR VALUES UNDER DIFFERENT ATTACKS IN THE FIRST APPROACH

Attack type	MSE	PSNR (db)
Non attacked image	0	Infinite
Salt and pepper noise (0.001)	11.2154	37.6326
Salt and pepper noise (0.01)	115.8620	27.4914
Salt and pepper noise (0.1)	1183.3	17.3999
Speckle noise (0.001)	2.1763	44.7536
Speckle noise (0.01)	19.9383	35.1339
Speckle noise (0.1)	180.5496	25.5648
Average Filter 3×3	2166.9	14.7725
Motion (10,45)	2223.5	14.6603
Rotation (25°)	3777.7	12.3585
Rotation (45°)	3776	12.3605
Bluring	2518.6	14.1192

TABLE VI. PSNR VALUES UNDER DIFFERENT ATTACKS IN THE SECOND APPROACH

Attack type	MSE	PSNR (db)
Non attacked image	0.0940	58.3988
Salt and pepper noise (0.001)	11.3072	37.5973
Salt and pepper noise (0.01)	114.0611	27.5594
Salt and pepper noise (0.1)	1183.4	17.3994
Speckle noise (0.001)	2.2749	44.5612
Speckle noise (0.01)	20.1879	35.0799
Speckle noise (0.1)	180.7737	25.5595
Average Filter 3×3	2167	14.7722
Motion (10,45)	2223.7	14.6601
Rotation (25°)	3777.1	12.3593
Rotation (45°)	3775.3	12.3613
Bluring	2518.7	14.1191

TABLE VII. BER RESULTS FOR THE EPR DATA UNDER DIFFERENT ATTACKS IN THE FIRST APPROACH

Attack type	BER
Non attacked image	0
Salt and pepper noise (0.001)	0
Salt and pepper noise (0.01)	0.2809
Salt and pepper noise (0.1)	5.1966
Speckle noise (0.001)	53.6517
Speckle noise (0.01)	53.3708
Speckle noise (0.1)	51.6854
Average Filter 3×3	48.4551
Motion (10,45)	53.6517
Rotation (25°)	50.5618
Rotation (45°)	49.6489
Bluring	49.7893

TABLE VIII. BER RESULTS FOR THE EPR DATA UNDER DIFFERENT ATTACKS IN THE SECOND APPROACH

Attack type	BER
Non attacked image	0
Salt and pepper noise (0.001)	0
Salt and pepper noise (0.01)	1.3343
Salt and pepper noise (0.1)	8.3567
Speckle noise (0.001)	45.1545
Speckle noise (0.01)	48.5253
Speckle noise (0.1)	48.8764
Average Filter 3×3	48.7360
Motion (10,45)	47.5421
Rotation (25°)	48.8062
Rotation (45°)	49.4382
Bluring	48.7360

CONCLUSION

The presented paper introduces two approaches with aim of providing the mean of the trust management between the parties of the cloud computing environment that considered as unsecure environment to deal with. Both approaches provide three levels of authentication that are from the owner to the destination of the data. The second one is between the owner of the data and the cloud service provider. The third level is from the destination of the data to its owner. The first approach exploits the advantage of the spatial embedding techniques that considered fast and require less processing time. This approach uses dynamic embedding algorithm to increase the visibility of the shared images. The second approaches implements discrete cosine transform along with the dynamic embedding algorithm to get the advantage of the DCT in providing more robustness against attacks while preserving the fastness and the highest visibility results obtained from dealing with dynamic embedding algorithm. The future work has an aim of implementing the hybrid model using other transform domain embedding techniques and evaluates the results in order to maximize the robustness against the attacking attempts. Also it has an aim of applying the proposed approaches in other sorts of medical data and test the consequent performance.

REFERENCES

[1] Sonika C. Rathi, Vandana 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) , pp. 297–308 , 2012.

[2] Borko Furht, Armondo Escalante, HandBook of Cloud computing, Springer Science + business Media, LLC 2010.

[3] Danwei Chen and Yanjun He, "A Study on Secure Data Storage Strategy in Cloud Computing", Journal of Convergence Information Technology, Volume 5, Number 7, September 2010.

[4] Mustafa Ulutas, Güzin Ulutas, Vasif V. Nabiyev." Medical image security and EPR hiding using Shamir’s secret sharing scheme". The Journal of Systems and Software 84 (2011), 341–353.

[5] Jasni Mohamad Zain and Malcolm 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.

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

[7] Siau-Chuin Liew, Siau-Way Liew and Jasni Mohd 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.

[8] Chao-Tung Yang; Lung-Teng Chen; Wei-Li Chou; Kuan-Chieh Wang, "Implementation of a Medical Image File Accessing System on Cloud Computing". 2010 IEEE 13th International Conference on Computational Science and Engineering (CSE), DOI:10.1109/CSE.2010.48, pp.:321-326

[9] G.Kanagaraj,A.C.Sumathi. "Proposal of an open-source Cloud computing system for exchanging medical images of a Hospital Information System". 2011 3rd International Conference on Trendz in Information Sciences and Computing (TISC), DOI:10.1109/TISC.2011.6169102 .Page(s): 144 – 149.

[10] House of Commons, Health Committee. The Electronic Patient Record. Sixth Report of Session 2006–07, Volume I, Ordered by The House of Commons to be printed 25 July 2007.

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

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

[13] Deyi Li, Yi Du, Artificial Intelligence with Uncertainty, Chapman and Hall/CRC, pp. 107–151, September 27, 2007.

[14] A.Menezes, P.van Oorschot, and S.Vanstone, Handbook of Applied Cryptography, CRC Press, 1996.

[15] Teddy Furon, Watermarking for alternative requirements, INRIA, Université de Rennes 1, 2005.

[16] Mr.Navnath S. Narawade and Dr.Rajendra D.Kanphade," DCT Based Robust Reversible Watermarking For Geometric Attack". International Journal of Emerging Trends & Technology in Computer Science (IJETTCS), Volume 1, Issue 2, July – August 2012.

[17] RadLink centre (2000) RadLink Diagnostic Imaging, http://radlink.com.sg/ [Accessed 17/1/2013].

[18] SoftWays' Medical Imaging Group (2003) Magnetic Resonance - Technology Information Portal, http://www.mr-tip.com/ [Accessed 17/1/2013].

[19] Yue Wu, Joseph P. Noonan, Sos Agaian, "NPCR and UACI Randomness Tests for Image Encryption", Journal of Selected Areas in Telecommunications (JSAT), April Edition, 2011.

[20] Farhad Rahimi and Hossein Rabbani, "A dual adaptive watermarking scheme in contourlet domain for DICOM images", BioMedical Engineering OnLine, 2011.

[21] Chun-Shien Lu, Multimedia security: steganography and digital watermarking techniques for protection of intellectual property. Idea Group Inc (IGI), 2005, pp. 100.

[22] Hao-Kuan Tso and Der-Chyuan Lou, "Medical image protection using secret sharing scheme". In Proceedings of the 6th International Conference on Ubiquitous Information Management and Communication (ICUIMC '12). ACM, New York, NY, USA, Article 93, 4 pages, (2012).

[23] Surya Pratap Singh, Paresh Rawat and Sudhir Agrawal, "A Robust Watermarking Approach using DCT-DWT". International Journal of Emerging Technology and Advanced Engineering (ISSN 2250-2459, Volume 2, Issue 8, August 2012).

[24] U. M. Gokhale and Y. V. Joshi, "A New Watermarking Algorithm Based on Image Scrambling and SVD in the Wavelet Domain". ACEEE Int. J. on Network Security, Vol. 02, No. 03, July 2011.

[25] Khaled Loukhaoukha, Jean-Yves Chouinard, and Abdellah Berdai, "A Secure Image Encryption Algorithm Based on Rubik’s Cube Principle". Hindawi Publishing Corporation Journal of Electrical and Computer Engineering Volume 2012, Article ID 173931, 13 pages.

[26] Patil Ramana Reddy, Munaga.V.N.K.Prasad and D.Srinivasa Rao, "Digital Image Watermarking Using SPIHT". International Journal of Recent Trends in Engineering, Vol 2, No. 3, November 2009.

[27] Ghazali Bin Sulong, Harith Hasan, Ali Selamat, Mohammed Ibrahim and Saparudin, " A New Color Image Watermarking Technique Using Hybrid Domain". IJCSI International Journal of Computer Science Issues, Vol. 9, Issue 6, No 1, November 2012.