Secret Medical Image Sharing and EPR Data Embedding Scheme over Cloud Computing Environment

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

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

F.E.Z. Abou-Chadi
Faculty of Engineering
Mansoura University,
Mansoura, Egypt

ABSTRACT
The fast development in the term of telecommunication helps on the appearance of variety of modern applications such as the telemedicine where the patients' digital data can transfer over insecure mediums between the doctors for farther diagnosis and dealing with these transmitted data. Therefore, the protection of the exchanged medical data is essential especially when working on the cloud computing environment, where the security is considered a major issue. In addition to the security, the high visibility of the medical images must also be achieved. This paper presents a novel approach that guarantees the 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 (EPR) string data between those parities while preserving the shared medical image from the distortion. The experimental results show the efficiency of the proposed scheme and also the robustness against various types of attacks.

Keywords
Cloud computing, EPR, Cloud drops, encryption, spatial synchronization, authentication

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

Cloud computing offers resources encapsulation on the Internet in the form of dynamical, 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 the benefits introduced by this computing paradigm like transmission, storage, and further processing needs on the user data. Despite all the advantages associated with the cloud computing, it has a number of disadvantages such as the data security which considered as 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.

Previous work reported deploying of standard cryptography techniques [5, 6]. Every user has his secret key to encrypt and decrypt data. The key will be revoked if the user leaves the cloud using proxy re-encryption schemes. A generic scheme was proposed in [7] to enable fine-grained data sharing over the cloud by making use of attribute-based predicate encryption and proxy re-encryption. Unfortunately, the processing overhead required verifying the signatures of the transferred keys and files to ensure complete security from alteration doesn't meet the speed requirements of cloud environments. In [8] a new mechanism of ensuring trust and security in Software as a Service (SaaS) was introduces. Trust Ticket, with the supporting protocols, helps a data owner in establishing a link between a cloud service provider and a registered user. This trust is established through a data owner's control over data and a registered user; because a registered user is linked with a cloud service provider by a data owner through Trust Ticket. Although third party authentication scheme reduces the processing overhead carried by cloud service provider and data owner, it can become complicated by the fact that users may frequently enter or leave the cloud. A trust management model based on fuzzy set theory was introduced in [9]. Trust similarity has been addressed to prevent the behavior of associated cheat of middle nodes. This model is geared toward the cloud users who are making their decision on whether to use services of some cloud computing providers by giving them trust evaluation sets about providers and then building reasonable trust relationship between them.

In recent years, 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 [10, 11] to deal the exchanging, storing and sharing on medical images in the way that verifying data integrity, availability, and confidently.

A watermark-aware trusted running environment to protect the software running in the cloud was introduced in [12]. Experimental results within a real private software cloud were introduced to demonstrate that the approach can provide a large-scale protection with a small overhead. In [13] a cloud watermarking technique based on data coloring was introduced. Each user is specified with a special color, which is able to protect copyright and should not affect the normal use of data. Although data coloring technique meets the main goal of cloud computing, it is considered a vulnerable

technique, since the detector can proceed in the manner prescribed to detect the watermark.

This paper introduces a newly developed method for medical data limited sharing over cloud environment. The new method provides three levels of authentication. The first level is between data owner and cloud service provider, the second one is between the destination and data owner. Finally the third one is between the owner and destination of the data to confirm the identity of the sender. Two of these levels depend on a private authentication keys. While the last level is based on the cloud model that was introduced as an authentication data sharing technique. The proposed method takes into account the essential features of digital watermarking techniques [14]. Invisibility, robustness, and detection ability are considered. The three levels help to improve of the security and to reduce unauthorized usage attempts on the transferred data.

In addition to the limited sharing, the proposed scheme also provides a secure hiding 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 [15]. Therefore, according to the importance and the sensitivity of this sort of data, the transmission of the EPR needs to ensure the privacy and the protection until it finally arrives to the required destination and this what the proposed scheme can also guarantee.

The remainder of this paper is arranged as follows: Section 2 describes the proposed method. Section 3 presents the experimental results obtained from the proposed method. Finally, section 4 presents the conclusion and the future work.

2. THE PROPOSED SCHEME

The proposed scheme consists of three main stages as shown in Figure 1. The first stage is to dynamically embed the EPR data into the original medical image. Secondly, 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.

2.1 The 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 [16]. 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 addition to the dynamic embedding algorithm, symmetric secret key (K_1) was applied to perform a spatial synchronization embedding/extraction processes by 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 [17] 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 [18].

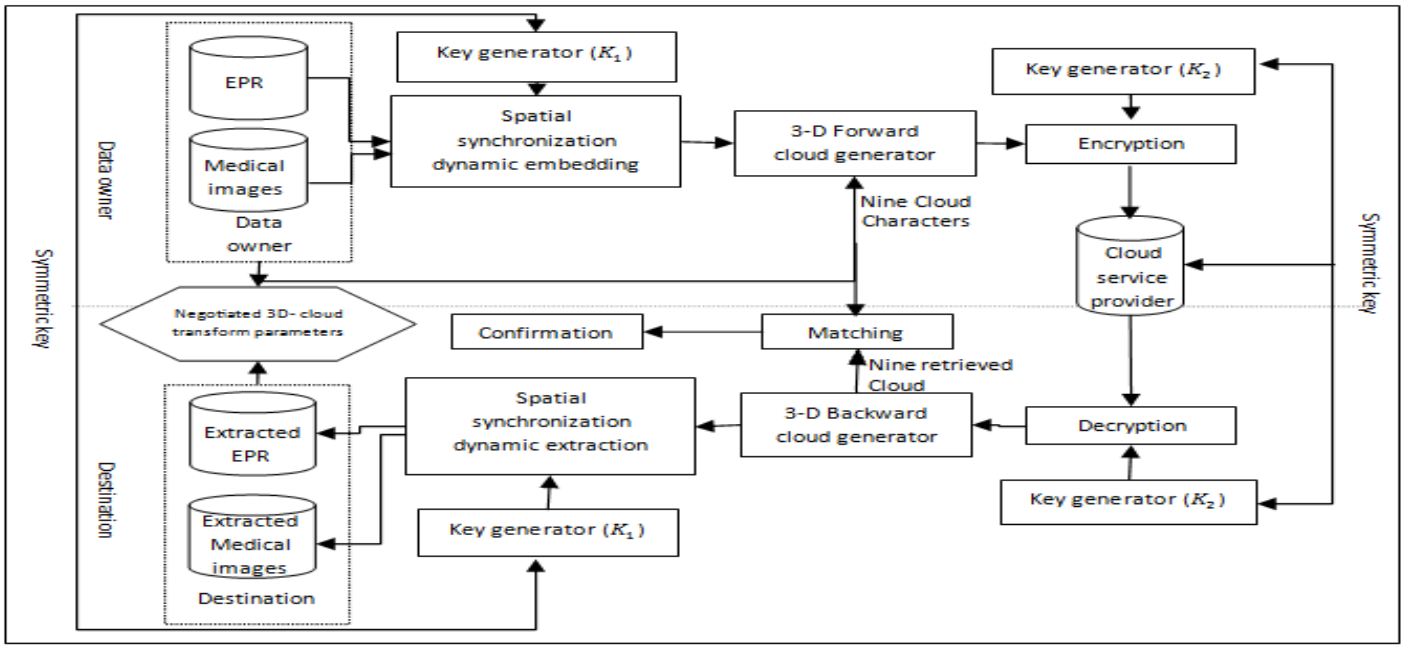

Fig 1: The proposed scheme framework

2.1.1 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. Figure 2 illustrates the steps of this phase and how the dynamic idea is applied for the required embedding process.

Algorithm1: Spatial synchronization dynamic embedding algorithm

Input: the cover medical image (CMI) and D_i.

Output: The watermarked medical image WMI

Steps:

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_is' according to Ub_i until finally construct the WMI.

Fig 2: Spatial synchronization dynamic embedding algorithm [16]

2.1.2 Spatial synchronization dynamic extraction phase

Figure 3 shows the required steps for the extraction phase by illustrating how the EPR data can be extracted in a dynamic manner using the same key used in the embedding phase.

Algorithm 2: Spatial synchronization dynamic extraction algorithm

Input: The watermarked medical image WMI, l.

Output: EPR data

Steps:

Step 1) Calculate BS, Nb and Ub_ivalues respectively through Figure 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 [16]

2.2 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 its 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 [19] 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 Generator" is applied to the previously generated cloud drops.

To clarify the cloud model idea, Figure 4 shows the cloud drops resulted from the forward cloud generator using E_x*=1* and different E_n and H_e values. The results indicate that as E_n*≤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 Figure 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'.

Therefore, by expanding the one-dimensional cloud model into a three-dimensional model, whereE_x, E_y and E_z refers to the components of the RGB color 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 Figures 5 and 6.

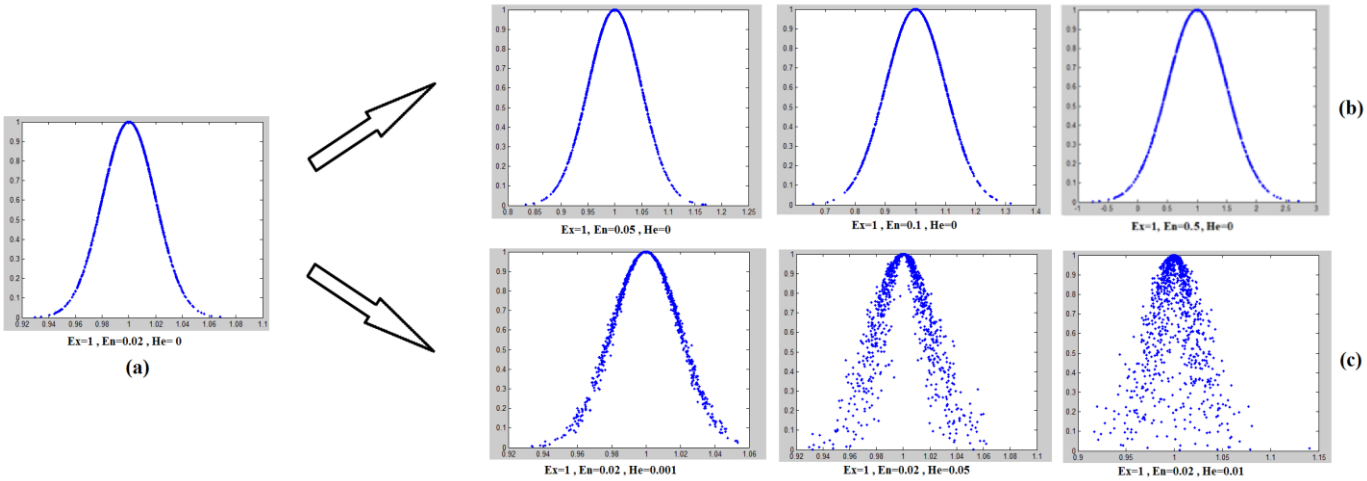

Fig 4: The resulting cloud drops using (a) E_x =1, E_n=0.02 and H_e=0, (b) E_x =1, E_n=0.05 and H_e=0, E_x =1, E_n=0.1 and H_e=0, E_x =1, E_n=0. 5 and H_e=0 (c): E_x =1, E_n=0.02 and H_e=0.001, E_x =1, E_n=0.02 and H_e=0.05, E_x =1, E_n=0.02 and H_e=0.01

Algorithm 3: Three dimension 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)

Steps:

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:

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

$$y_i = NORM\ (E_y, {E_{ny}}'^2_i)$$

$$z_i = NORM\ (E_z, {E_{nz}}'^2_i)$$

Step 3) x_i, y_i and z_i are cloud drops in each of the images' dimensions.

Step 4) Repeat Steps 1 to 3, in the entire WMI pixels to generate the required approximated shared image (ASI).

Fig 5: Three dimension Forward Cloud Generator

Algorithm 4: Three dimension Backward Cloud Generator

Input: Approximated Shared Image (ASI)

Output: $(E_x', E_y', E_z', E_{nx}', E_{ny}', E_{nz}', H_{ex}', H_{ey}', H_{ez}')$.

Steps:

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 ${S_z}^2$:

$${S_x}^2 = \frac{1}{n-1}\sum_{i=1}^{n}(x_i - \bar{X})^2, \text{ then } H_{ex}' = \sqrt{{S_x}^2 - {E_{nx}}'^2}$$

$${S_y}^2 = \frac{1}{n-1}\sum_{i=1}^{n}(y_i - \bar{Y})^2, \text{ then } H_{ey}' = \sqrt{{S_y}^2 - {E_{ny}}'^2}$$

$${S_z}^2 = \frac{1}{n-1}\sum_{i=1}^{n}(z_i - \bar{Z})^2, \text{ then } H_{ez}' = \sqrt{{S_z}^2 - {E_{nz}}'^2}$$

Fig 6: Three dimension Backward cloud Generator

2.3 Encryption/Decryption Technique

In this step, cryptographic algorithm [20] 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 [21].

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 2.1, 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 it desynchronizes the encrypted image at the destination. In other words, it helps the owner to be ensured that he is the recipient of the data and in turn 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.

3. EXPERIMENTAL RESULTS

The performance of the proposed scheme was investigated using digital simulation techniques. It was carried out using MATLAB and a set of 350×350×3 MR images collected from standard web portal for MRI images [22]. Moreover, MRI images from standard web portal [23] were used for further investigation of the proposed scheme efficiency. The quality of the retrieved data was evaluated using standard quality metrics. The quality metrics used for performance evaluation are; (i) The peak signal to noise ratio (PSNR), that measure the image quality since the high PSNR values provides higher image quality and the small values of it indicates high numerical differences between the images[24] without considering the characteristics of the human visual quality (HVS)[25]. (ii) The structural similarity (SSIM) index address, which is an important medical image quality metric used to measure the local rather than the global images similarities [25]. (iii) The number of changing pixel rate (NPCP), (iv) 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 [26] and (v) Bit Error Rate (BER) to evaluate the similarity between the original and the retrieved data [25]. Eq. (1-7) mathematically expresses these quality metrics.

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

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

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 [25]

$$\begin{aligned} \mathrm{SSIM}(\mathrm{OMI},\mathrm{RMI}) = {} & \mathrm{LC}(\mathrm{OMI},\mathrm{RMI})^{\alpha} \\ & \times \mathrm{CC}(\mathrm{OMI},\mathrm{RMI})^{\beta} \\ & \times \mathrm{SC}(\mathrm{OMI},\mathrm{RMI})^{\lambda} \end{aligned} \qquad (3)$$

Where: $\mathrm{OMI}, \mathrm{RMI}$ 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. [25]

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

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

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

Where F denotes the largest supported pixel value of the image format and T represents the size of the OMI and RMI [26].

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

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 [27].

Furthermore, the processing time, overhead computations complexities and the robustness of the algorithm against different types of attacks of the proposed scheme were investigated.

Starting with the medical images shown in Figure 7 (a), and using the related EPR data shown in Figure 8(a), the resulted images from the embedding process using secret key K_1 are shown in Figure 7(b). The 3D-CT approximations are shown in Figure 7 (c). (E_x, E_y and E_z equals to colour channels pixels of the medical image, 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 version is shown in Figure 7 (d). This version resides at the CSP, since the first level of authentication occurs between the users and CSP. At the destination side, the users are authenticated to the CSP using the encryption symmetric key (K_2), and then get the approximated versions of the shared data. Then, the destination accomplish the second level of authentication through 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}') for the confirmation of the data owner identity. By using the secret K_1 between the data owner and the destination, spatially and dynamically embedded EPR data can be retrieved as finally shown in Figure 8 (b).

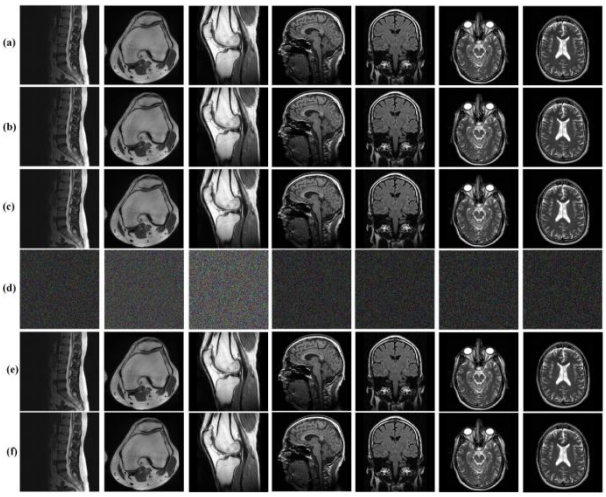

Fig 7: (a) The original medical images, (b) The images after embedding process, (c) The approximated images (d) The encrypted images, (e) The decrypted images, (f) The reconstructed lossless medical images

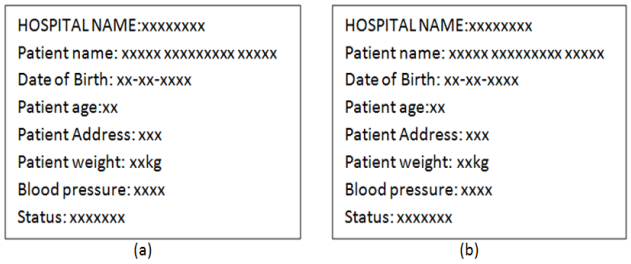

Fig 8: Example of EPR string data, (a) Original EPR data, (b) Retrieved EPR data

For the scheme performance, Table 1 depicts the processing time and the total number of computations for each step in the scheme using 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).

Table 1. Performance evaluation of the proposed scheme

	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

The *PSNR*, *SSIM*, *NPCP* and *UACI* metrics were also calculated and are illustrated in Table 2. The results show that the images have been retrieved without any distortion. This is due to the usage of the dynamic embedding algorithm that exploits the overall capacity of the host image for the embedding process. Also the usage of the cloud model with *Enx*, *Eny*, *Enz* values less than or equal to 0.1 and *Hex*, *Hey*, *Hez* values equal to zero helps to generate an approximated image which have a most representative of the shared image.

Table 2. Quality evaluation of the proposed scheme

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

The results reported in [28] show that although the encryption scheme presented preserves the results from the pixel expansions, it provides only one level of authentication, which used to confirm the identity of the destination of the data. However, the proposed scheme, in addition to preserve the shared medical image from the pixel expansion, three levels of authentication are also presented to confirm the identity of the data owner, the service provider and the destination of the data which in turn increases the security level and as a result decreases the unauthorized access attempts to these sensitive data. Moreover, the presented scheme offers an embedding capability of the EPR string data that helps to facilitate the communication between the owner and the destination of the data.

When exposed to attacking attempts, the proposed scheme shows robustness and allows the attacked encrypted image and its embedded EPR data to be retrieved. At the same time the cloud characters extracted from the received image would not be retrieved correctly. This helps to detect at the receiving side that the transmitted data faced some type of attack that modifies the nature of the transmitted data.

It is argued to evaluate the robustness of the presented scheme against a number of attacking attempts, such as the salt and pepper and the speckle noise. The MSE and PSNR were respectively calculated and the results are tabulated in Table 3. It can be seen that the proposed scheme shows higher robustness compared to those reported in [29, 30, 31 and 32]. This indicates that despite of the attempts to destroy or to attack the transmitted data, the data can be preserved and retrieved in the destination side with an acceptable degree of visibility.

Table 3. PSNR values under different attacks

Attack type	MSE	PSNR (db)
Non attacked image	0	Infinite
Salt and pepper noise (0.003)	0.5257	50.9231
Salt and pepper noise (0.01)	115.8620	27.4914
Salt and pepper noise (0.05)	578.5766	20.5072
Salt and pepper noise (0.1)	1183.3	17.3999
Speckle noise (0.01)	19.9383	35.1339
Speckle noise (0.1)	180.5496	25.5648
Average Filter 3×3	53.9534	30.8106
Motion (10,45)	53.5876	30.8402

Then, by calculating the bit error rate (BER) using Eq (7) Table 4 shows the results that are acceptable in most attacks types with respect to [25]. The table shows that the proposed scheme provides more robustness under the salt and pepper noise since this type of noise affects random pixels so the whole image would not be affected and so not the whole embedded EPR data would be destroyed which mean retrieving the attacked EPR with a minimum degree of distortion and acceptable degree of meaningful. For the Speckle noise, average and motion filters because these types of attacks affects the whole images' pixels which in turn affects the pixels' bits, the retrieved EPR data would suffer from a high degree of attacks which affects its meaningful.

Table 4. BER results for the EPR data under different attacks

Attack type	BER
Non attacked image	0
Salt and pepper noise (0.003)	0.1404
Salt and pepper noise (0.01)	0.2809
Salt and pepper noise (0.05)	2.6685
Salt and pepper noise (0.1)	5.1966
Speckle noise (0.01)	53.3708
Speckle noise (0.1)	51.6854
Average Filter 3×3	48.4551
Motion (10,45)	53.6517

4. CONCLUSION

In this paper a novel scheme of secure medical image sharing system suited for cloud computing environment is presented to protect data owners against malicious cloud service provider and/or unauthorized data users. This was done based on three authentication levels; the first is between data owner and cloud service provider based on symmetric cryptography, the second level which is between authorized user and data owner is done based on 3D cloud generator parameter and for the third authentication level, which allows data owner to be sure that the data accessed only through the authorized user, another secret key known only by those two parities is used. In addition, the proposed scheme uses effective embedding scheme, which is the dynamic embedding algorithm, to hide the electronic patient records (EPR) within the transmitted shared medical image in an efficient way that helps to protect it from being attacked. Using 3D cloud generation provides essential features of invisibility, robustness and detection ability which made it more suited to the insecure cloud computing environment. The experimental results shows the efficiency of the presented scheme in the term of quality and how it enhance the security level as compared with one of the recently presented schemes. Also the experiments illustrate the robustness of the proposed scheme against different types of attacks that can expose the transmitted secure data. In the future, the proposed scheme will be tested in other medical applications, such as audio and video medical data to provide a wide security space for the transmission of the medical data with different types of it. Also, the performance of the presented scheme will be examined under the usage of asymmetric keys.

5. 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), 2012, pp. 297–308.

[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] M. Sudha, Dr.Bandaru Rama Krishna Rao, M. Monica "A Comprehensive Approach to Ensure Secure Data Communication in Cloud Environment" International Journal of Computer Applications, Volume 12– No.8, December 2010 pp.19-23.

[6] Tran, D.H.; Hai-Long Nguyen; Wei Zha; Wee Keong Ng. "Towards security in sharing data on cloud-based social networks ". 8th International Conference on Information, Communications and Signal Processing.DOI: 10.1109/ICICS.2011.6173582, 2011, Page(s): 1 – 5.

[7] Yanjiang Yang, Youcheng Zhang. "A Generic Scheme for Secure Data Sharing in Cloud". 40th International Conference on Parallel Processing Workshops (ICPPW 2011) , DOI: 10.1109/ICPPW.2011.51, Page(s): 145 – 153.

[8] M. Ahmed, Yang Xiang. "Trust Ticket Deployment: A Notion of a Data Owner's Trust in Cloud Computing" .2011 IEEE 10th International Conference on Trust, Security and Privacy in Computing and Communications. DOI: 10.1109/TrustCom.2011.17. Page(s): 111 – 117.

[9] Xiaodong Sun, Guiran Chang , Fengyun Li. "A Trust Management Model to Enhance Security of Cloud Computing Environments".2011 Second International Conference on Networking and Distributed Computing (ICNDC), 21-24 Sept. Page(s): 244 – 248.

[10] 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

[11] 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.

[12] Junning Fu, Chaokun Wang ; Zhiwei Yu ; Jianmin Wang ; Jia-Guang Sun . "A Watermark-Aware Trusted Running Environment for Software Clouds". IEEE Fifth Annual China Grid Conference, 16-18 July 2010, Page(s): 144 – 151.

[13] Yu-Chao Liu, Yu-Tao Ma, Hai-Su Zhang, De-Yi Li and Gui-Sheng Chen," A method for trust management in cloud computing: data coloring by cloud watermarking" , International journal of automation and computing, 2011.

[14] Ingemar J. Cox, Digital Watermarking and Steganography, Morgan Kaufmann, Burlington, MA, USA, 2008.

[15] 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.

[16] Z. Eslami and J. Zarepour Ahmadabadi, "Secret image sharing with authentication-chaining and dynamic embedding", the journal of systems and software 84, 2011.

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

[18] 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.

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

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

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

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

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

[24] Alain Horé and Djemel Ziou, " Image quality metrics: PSNR vs. SSIM", 2010 International Conference on Pattern Recognition, 2010 IEEE.

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

[26] 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.

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

[28] 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).

[29] 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).

[30] 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.

[31] 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.

[32] 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.