Journal of Computers Vol. 30 No. 6, 2019, pp. 286-296
doi:10.3966/199115992019123006024

A Blockchain-Based Scheme for Secure Sharing of X-Ray Medical Images

Bing-qi Liu[1], Ming-zhe Liu[1*], Xin Jiang[1], Fei-xiang Zhao[1], Rui-li Wang[2]

[1] State Key Laboratory of Geohazard Prevention and Geoenvironment Protection, Chengdu University of Technology, Sichuan, China
liumz@cdut.edu.cn

[2] Institute of Natural and Mathematical Sciences, Massey University, Auckland, New Zealand

Received 10 May 2019; Revised 10 June 2019; Accepted 2 July 2019

Abstract. This paper proposes a secure sharing and trading scheme of X-Ray medical image data based on block chain, as it can be used for further scientific research processing. The specific representation includes the following steps: i. The original X-Ray data of medical instruments are transmitted to the cloud platform through the MQTT protocol; ii. The patient information (name, medical card number, etc.) of the image data is encrypted by hashing algorithm to protect privacy; iii. Applying a watermark to the image data; iv. Generating blocks through the consensus mechanism of block chain. The scheme proposed in this paper overcomes the security challenges faced by the traditional cloud-based image data management solution: user privacy disclosure, illegal tampering, and the risk of data being stolen and sold, and realizes a secure transaction system connecting users with data needs, which makes the huge image data on clinical medicine have higher scientific research value.

Keywords: blockchain, cloud platform, public ledger, X-Ray medical image

1 Introduction

X-Ray medical images are used for radiotherapy, as well as have high scientific research and market value. How to obtain these valuable data has become a bottleneck in the development of artificial intelligence in the medical field. The current centralized, cloud-based image data management solution cannot be expanded, nor can it solve the security challenges faced by large hospitals.

Although large hospitals already have relevant big data platforms in the field, most artificial intelligence products have too little training data and require a large amount of manpower and material resources to label training data. The hospital's big data platform is dedicated to off-line data analysis inside hospitals and basically does not have a real data sharing system and related products for enterprises outside hospitals, especially the development and development of a safe data sharing platform that can guarantee patients' privacy, prevent data tampering and illegal circulation. In view of the huge demand for safe data sharing platforms in the intelligent medical industry and other artificial intelligence research and markets, and the fact that the research and product development in actual depth study have to rely heavily on labeled data, it is of great research significance to successfully develop a safe image data platform.

2 Related Works

2.1 Blockchain Technology

Up to now, block chain technology has been used in electronic medical record cases in the medical field, and future applications in the medical field may also include image data, health insurance, biomedical

* Corresponding Author

research, drug supply and procurement processes and medical education [1]. Zhou et al. [2] propose a threshold based on block chain, this system has gained some special advantages, such as dispersion, tamper resistance and recording nodes to help users verify verifiable public information. Patel [3] uses block chain as a distributed data storage to establish a ledger of radiology research and patient-defined access rights, eliminates third-party access to protected health information, meets many standards of interoperable health systems, and is easily extended to areas other than medical imaging, but the complexity and security of the framework's privacy and security model are difficult to be guaranteed.

To overcome security problem, the solution proposed by the document [4] outlines the framework of the cloud platform, internal work and protocols for processing heterogeneous medical data. Dagher et al. [5] proposed a high-level decentralized block chain system named Ancile, while acknowledging that some nodes should have higher permissions. This study shows that it is not possible to completely hide all information and maintain an accessible and interoperable system, but by using smart contracts to separate information, Ancile still provides significant privacy protection and data Integrity. Li et al. [6] proposed DPS, the user can permanently save important data, the original data can be Verified. The literature [7] uses the MEDREC of the shared chain to record genomic sequencing data, allowing individuals to sell access to their entire genome. The solution proposed by the document [8] based on the block chain of geographical space uses a cryptographic spatial coordinate system to add an immutable spatial context so that these geographical spatial chains can record a specific time of an entry, also require verification by both parties.

The document [9] creates a sensor system that uses the licensing mechanism of block chains to collect intelligent contracts for evaluating patient information, which trigger alarms to apply to patients and medical service providers. The document [10] designs a block chain network called "MedBlock" for electronic medical records, which combines customized access control protocol and symmetric cipher technology to show high information security. The document [11] proposes a practical group optimization algorithm using bionic methods to improve the security of medical data management, and examines the characteristics of access control with a machine learning prediction method to enhance detection of unknown root.

As above of all, the security problem of block chain technology had been paid attention to by academic circles. There are some research methods of block chain in electronic medical record storage and application examples of distributed database. However, the access control protocol is mainly used in security of block chain for medical images, and useful image data information has not been used for security reporting.

2.2 Digital Watermarking

The remote transmission of digital medical images is an important part of telemedicine. During the network transmission, medical images may encounter some unexpected situations such as illegal tampering and illegal copying. In order to prevent and detect this situation in time, some researchers proposed to introduce digital watermarking technology into the remote transmission of digital medical images.

Generally speaking, the digital medical image watermarking algorithm is divided into three parts: watermark generation, watermark embedding and watermark extraction [12-13, 18]. These algorithms are divided into two categories, the first category is mainly to process images in pixel domain and the second category is to process images in various transform domains. In the field of digital watermarking of medical images, quite a number of algorithms have been produced in recent years [15]. The digital watermarking algorithm in pixel domain usually uses LSB substitution and various chaotic sequences [14, 16-17, 19]. The digital watermarking algorithms in the transform domain generally use wavelet transform, discrete cosine transform and Fourier transform [20-23].

Medical images are different from ordinary natural images in that the former has a strong regional value, that is, only a part of the medical images are valuable, and the rest are often meaningless. Meaningful regions are called regions of interest (ROI) and meaningless regions are called regions of non-interest (RONI). In general, the watermark should be added completely away from the region of interest in order to keep information beneficial to diagnosis as much as possible. Guo and Zhuang [24] proposes a medical image watermarking scheme that requires a diagnostic doctor to specify ROI region.

Duan et al. [25] proposed an energy conduction model ECM (Energy Conduction Model) for accurate

segmentation of ROI and RONI of medical images, but the algorithm is inefficient. In addition, some medical image watermarking algorithms [26-28] which partition ROI and Roni have achieved good results, but these algorithms often lack protection for the most important parts of medical images and cannot restore the original medical images. Therefore, some researchers have proposed some digital watermarking schemes [29-32] that can completely restore the original medical image, but these methods often need to transmit some information about watermark extraction and original medical image restoration to the receiver on another completely secure channel.

All of the above watermarking algorithms will change the original medical image to a certain extent, so some researchers put forward the concept of 'zero watermarking', that is, to generate a watermark from the image without modifying the original medical image and upload it to the database, only a unique watermark can be generated from the same medical image, and copyright protection can be achieved by this method [33-35]. However, this approach requires the construction of a complex and completely fair authentication system [36].

3 Blockchain-based System Design

In this paper, we realize the guidance of all historical data, helps the hospital to construct the image data and realize the full-position analysis and response of the image data, which can be used not only in the scientific research of tumor treatment, but also in the clinical response of tumor treatment, and can also guide the improvement and upgrading of tumor treatment drugs.

3.1 System Structure

The main functions include digital watermarking of image data, privacy protection of image data, platform authentication access, Internet of things access and block chain sharing scheme (see Fig. 1).

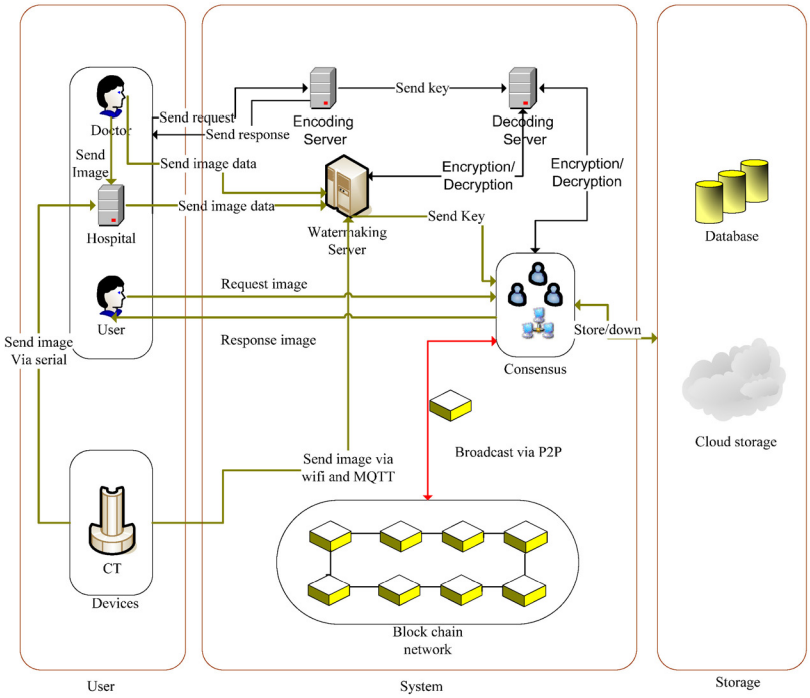

Fig. 1. System module

X-Ray image encryption module. Based on packet key management, the data transmission network with strong anti-interference ability, high transmission speed and self-adaptive matching of keys is controlled through the authenticator, key server and authentication server.

Data transmission module. Using the algorithm of digital signature, the abstract of the image data to be signed is generated by using hash function, and the ciphertext obtained by encrypting the abstract with public key is the digital signature.

Digital watermarking module. The watermark application function of different image data is realized, and the security of image data is guaranteed and will not be tampered with.
Block chain privacy protection module. Using block chain isolation verification technology can not only ensure the legitimate use of the data demander, but also protect the user's privacy to the maximum extent. For example, the patient's name, medical card number and other information are encrypted by hash algorithm, and the authenticity of the data is guaranteed by isolation verification.
Block chain consensus module. Using the open source Fabric smart contract, data traceability can confirm data ownership and circulation channels. If data is illegally re-disseminated by users, it can provide proof materials for infringement complaint stage and provide a more credible big data trading environment.

3.1 X-Ray Image Encryption

For the sparse representation of an X-Ray image to be useful within the current trend of medical technology developments it should be suitable to be encapsulated in a small file. Accordingly, the coefficients of the atomic decompositions need to be converted into integer numbers. This operation is known as quantization. We adopt a simple and commonly used uniform quantization technique. For $q = 1,...,Q$ the absolute value coefficients $C_{\mathrm{q}}|(n)|, n = 1,...,k_q$ are converted to integers as follows:

$$c_q^{\Delta}(n) = \begin{cases} \left\lceil \dfrac{c_q(n) - \theta}{\Delta} \right\rceil, if \left| c_q(n) \right| \geq \theta \\ 0 \quad \text{otherwise,} \end{cases} \tag{1}$$

where $\lceil X \rceil$ indicates the smallest integer number greater than or equal to x, Δ is the quantization parameter, and θ the threshold to disregard coefficients of small magnitude. The signs of the coefficient are encoded separately, as a vector s_q using a binary alphabet.

In order to store the information about the particular atoms presented in the approximation of each block, we proceed as follows: firstly each pair of indices $\left(\ell_n^{x,q}, \ell_n^{y,q}\right)$ corresponding to the atoms in the decompositions of the block I_q is mapped into a single index $o_q(n)$. Then the set $o_q(1),...,o_q(k_q)$ is sorted in ascending order $o_q(n) \to \tilde{o}_q(n), n = 1,..,k_q$. This guarantees that, for each q-value, $\tilde{o}_q(i) < \tilde{o}_q(i+1), i = 1,...,k_q - 1$. The order of the indices induces an order in the unsigned coefficients, $c_q^{\Delta} \to \tilde{c}_q^{\Delta}$ and in the corresponding signs $s_q \to \tilde{s}_q$. The advantage introduced by the ascending order of the indices is that they can be stored as smaller positive numbers, by taking differences between two consecutive values. Certainly by defining $\delta_q(n) = \tilde{o}_q(n) - \tilde{o}_q(n-1), n = 2,...,k_q$ the string $\tilde{o}_q(1), \delta_q(2),...,\delta_q(k_q)$ stores the indices for the block q with unique recovery. The number 0 is then used to separate the strings corresponding to different blocks.

$$st_{ind} = \begin{bmatrix} \tilde{o}_1(1), \delta_1(2),...,\delta_1(k_1), 0, \tilde{o}_2(1), \delta_2(2),...,\delta_2(k_2), \\ 0,...,\tilde{o}_{K_Q}(1), \tilde{o}_{K_Q}(2),...,\delta_{K_Q}(k_{K_Q}) \end{bmatrix} \tag{2}$$

The quantized magnitude of the re-ordered coefficients is concatenated in the strings st_{cf} as follows:

$$st_{cf} = \left[\tilde{c}_1^{\Delta}(1),...,\tilde{c}_1^{\Delta}(k_1), \tilde{c}_2^{\Delta}(1),...,\tilde{c}_2^{\Delta}(k_2),...,\tilde{c}_{K_Q}^{\Delta}(k_{K_Q}) \right] \tag{3}$$

Using 0 if the sign is positive and 1 if it is negative, the signs of the coefficients are placed in the string, st_{sg} as

$$st_{ind} = \left[\tilde{s}_1(1),...,\tilde{s}_1(k_1), \tilde{s}_2(1),...,\tilde{s}_2(k_2),...,\tilde{s}_{k_Q}(1),...,\tilde{s}_{k_Q}(k_Q) \right] \tag{4}$$

The next encoding/decoding scheme summarizes the above described procedure.

Encoding Given an image partition $I_q \in R^{N_b \times N_b}, q = 1,...,Q$, approximate each element of the partition by the atomic decomposition:

$$I_q^{k_q} = \sum_{n=1}^{k_q} c_q(n) d_{\ell_n^{x,q}}^x \left(d_{\ell_n^{y,q}}^y\right)^T \tag{5}$$

The approximation is carried out on each block, independently of the others, until the stopping criterion is reached.

For each q quantize as in Eq.(1) the magnitude of the coefficients in the decomposition Eq.(5) to obtain $c_q^{\Delta}(n), n = 1,...,k_q$. Store the signs of the nonzero coefficient as components of a vector s_q. For each q map the pair of indices $\left(\ell_n^{x,q}, \ell_n^{y,q}\right), n = 1,...,k_q$ in Eq.(5) into a single index $o_q(n), n = 1,...,k_q$ and sort these numbers in ascending order to have the re-ordered sets:

$\tilde{o}_q(1)...,\tilde{o}_q(k_q); \tilde{c}_q^{\Delta}(1)...,\tilde{c}_q^{\Delta}(k_q)$ and $\tilde{s}_q(1)...,\tilde{s}_q(k_q)$ to create the strings: st_{ind}, as in Eq.(2), and st_{cf}, and st_{sg} as in Eq.(3) and Eq.(4) respectively. Let's recall the content of the file encoded by the above steps:

st_{ind} contains the difference of indices corresponding to the atoms in the approximation of each of the blocks in the image partition.

st_{cf} contains the magnitude of the corresponding coefficients (quantized to integer numbers).

st_{sg} contains the signs of the coefficients in binary format. The quantization parameter Δ also needs to be stored in the file. We fix $\theta = 1.3\Delta$ or all the images.

Decoding Recover the indices from their difference. This operation also gives the information about the number of coefficients in each block. Read the quantized unsigned coefficients from the string st_{cf} and transform them into real numbers as $\left|\tilde{c}_q^r(n)\right| = \Delta \tilde{c}_q^{\Delta}(n) + (\theta - \Delta/2)$. Read the corresponding signs from the string st_{sg}. Recover the approximated partition, for each block, through the liner combination

$$I^{r,k_q} = \sum_{n=1}^{k_q} \tilde{s}_q(n) \left|\tilde{c}_q^r(n)\right| d_{\ell_n^{x,q}}^x \left(d_{\ell_n^{y,q}}^y\right)^T \tag{6}$$

Assemble the recovered image as

$$I^{r,k} = \hat{J}_{q=1}^{Q} I_q^{r,k_q}, \tag{7}$$

where the $\hat{J}$ indicates the operation for joining the blocks to restore the image.

3.3 Digital Watermarking for Multimodality Image

Due to the defect of the implementation principle of position encryption, although the watermark image after position encryption has already been scrambled in visual effect, it cannot change the histogram of the original image. It is easy to leak the statistical information of the watermark image. Therefore, in order to enhance security, this paper intends to encrypt the watermark image by combining position encryption with gray value encryption (two-factor encryption). This encryption method (see Fig. 2) can reduce the probability that the watermark will be decoded when the watermark image is extracted and ensure the security and confidentiality of the watermark. From the point of view of watermark encryption, the two-factor encryption mechanism generates two chaotic matrices when encrypting digital watermarks. The marked spatial coordinate information and volume size information are used for position encryption, and the information such as terminal number, geographical location and shooting time are used for gray-scale encryption. By combining the two, chaotic sequences are unpredictable. Therefore, even if the watermark sequences are known, they cannot be cracked without the chaotic encryption key matrix. In order to meet the requirements of watermark security, it has played a better role in protecting copyright.

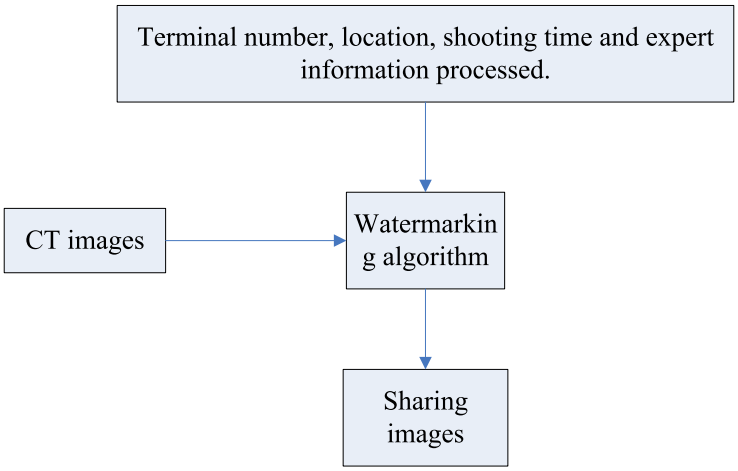

Fig. 2. Digital watermark

3.4 Blockchain Implementation

The block chain network of the data sharing platform provides a variety of block link ports. Its transaction interface is first for message queue data transmission, and this submission is real-time submission. The core block chain module receives the authentication request and notifies the consensus node through TCP for verification. After verification is completed, the consensus node will send out TCP asynchronous messages, and the block chain module will receive the verification result message. If a consensus is reached, the transaction will first be written into the local MySQL account book, and then the block information of the block chain will be broadcast to the block chain network through P2P. The result is a phased notification to each node. As shown in the Fig. 3, MySQL technology is used to store the public ledger information of the block chain locally.

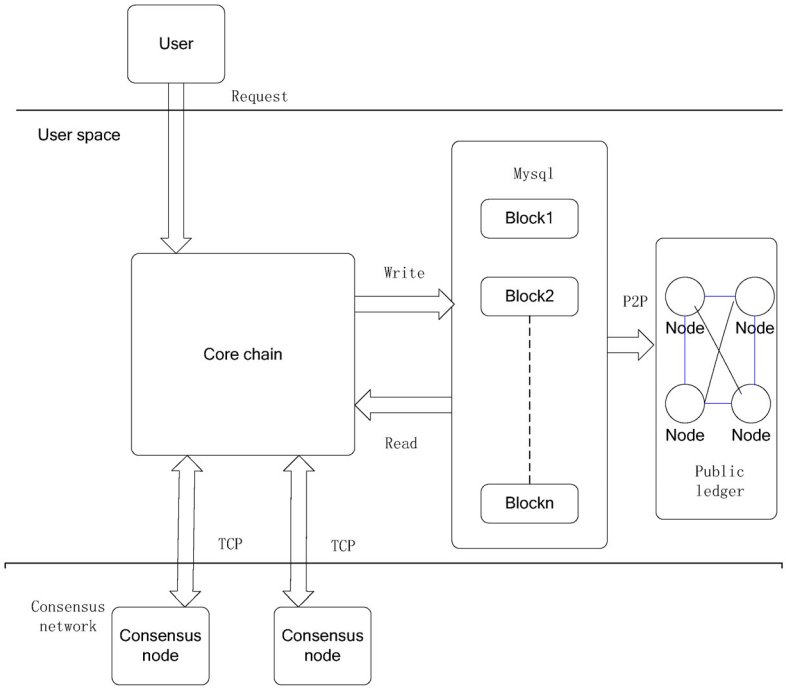

Fig. 3. Internal structure of block chain

4 Experiments and Evaluation

4.1 Experiments

We illustrate the effectiveness of the proposed sharing scheme by storing the outputs of high quality sparse approximation of two data sets: the Lung Nodule Analysis 2016 dataset (abbreviated as LUNA) and the training set of Data Science Bowl 2017 (abbreviated as DSB). The LUNA dataset includes 1186 nodule labels in 888 patients annotated by radiologists, while the DSB dataset only includes the per-subject binary labels indicating whether this subject was diagnosed with lung cancer in the year after the scanning. The DSB dataset includes 1397, 198, 506 persons (cases) in its training, validation, and test set respectively.

The quality of the approximation (the classical Peak Signal-to-Noise Ratio) is calculated as:

$$PSNR = 10Log_{10}(\frac{(2^8-1)^2}{MSE}) \tag{8}$$

MSE indicates as:

$$MSN = \frac{\| I - I^{r,K} \|_F^2}{N_x N_y} \tag{9}$$

This quality guarantees that the approximation is indistinguishable from the image, in the original size. For the comparison with standard formats all the PSNRs are fixed as values for which JPEG and JPEG2 produce the required MSSIM. For producing a requested PSNR with the sparse representation approach we proceed as follows: the approximation routine is set to yield a slightly larger value of PSNR and the required one is then obtained by tuning the quantization parameter $\triangle$.

As a measure of sparsity we use the Sparsity Ratio, which is defined as:

$$SR = \frac{Number\ of\ \ pixels\ in\ the\ image}{Number\ of\ \ coefficients\ in\ the\ representation} \tag{10}$$

Accordingly, the sparsity of a representation is manifested as a high value of SR.

In addition to the SR, which is a global measure of sparsity, a meaningful description of the variation of the image content throughout the partition is rendered by the local sparsity ratio, which is given as

$$sr(q) = \frac{N_b^2}{K_q}, q = 1,...,Q, \tag{11}$$

Where K_q is the number of coefficients in the decomposition of the q-block and N_b^2 is the number of pixels in the block.

4.2 Evaluation

The approximation of all the images in DSB are performed in both the pixel intensity and the wavelet domain. The size of the blocks in the image partition is fixed taking into account previously reported results, which indicate that 16 is a good trade-off between the resulting sparsity and the processing time. The information about the sizes of the corresponding files is given in bits per pixel (bpp) in the third and forth columns of Table 1. The results for JPEG and JPEG2 are placed in the fifth and sixth columns, respectively. The last two rows of the table are the mean value of standard deviation (std) of the corresponding columns. As shown in Table 1, all the files corresponding to approximations in the wavelet domain (S_{pd}) are smaller than those corresponding to approximations in the pixel intensity domain (S_{pd}), and also smaller than the JPEG ones. On average the files with the sparse representation in the wavelet domain are 22% smaller than those with the representation in the pixel domain, and 27% smaller than the JPEG files. In the present form JPEG2 produces the smallest files (on average 9% smaller than the files with the representation in the wavelet domain). However, both JPEG and JPEG2

formats involve an entropy coding step, which is not included in our scheme. Instead, the outputs of our algorithm are stored in HDF5 format.

Table 1. Comparison of size rate (in bpp) for the DSB, listed in the first column. The third column shows the bpp values corresponding to the sparse representation in the pixel domain (*Spd*). The forth column shows the corresponding results in the wavelet domain (*Swd*). The fifth and sixth columns are the bpp values for the formats JPEG and JPEG2, respectively

Image	dB	*Spd*	*Swd*	JPEG	JPEG2
1	48.1	0.443	0.286	0.436	0.234
2	48.6	0.462	0.306	0.449	0.247
3	47.4	0.441	0.320	0.419	0.244
4	48.0	0.488	0.316	0.485	0.286
5	48.1	0.624	0.391	0.566	0.335
6	47.1	0.676	0.416	0.575	0.334
7	48.8	0.612	0.424	0.586	0.371
8	46.4	0.599	0.452	0.546	0.346
9	49.1	0.612	0.419	0.573	0.364
10	45.8	0.697	0.453	0.594	0.358
11	44.3	0.519	0.465	0.605	0.393
12	44.3	0.691	0.629	0.832	0.521
13	44.1	0.827	0.686	0.874	0.629
14	43.4	0.816	0.693	0.924	0.619
15	48.9	1.000	0.867	1.152	0.759
16	49.2	1.384	1.240	1.584	1.056
17	44.3	1.596	1.418	1.828	1.248
18	44.4	1.606	1.435	1.827	1.310
19	47.0	2.131	1.922	2.463	1.630
20	47.4	2.395	2.298	2.764	1.902
Mean value	46.7	0.938	0.727	1.004	0.659
Std	1.9	0.573	0.521	0.707	0.500

A very interesting feature of the numerical results is that the quantization process, intrinsic to the economic store of the coefficients in the image approximation does not reduce the sparsity. For the sake of comparison in addition to calculating the SR_S obtained with the dictionary approach in both domains, before and after quantization, we have also calculated the corresponding SR_S produced by nonlinear thresholding of the wavelet coefficients. The results are shown in Fig. 4. As already discussed, since the quantization of coefficients degrades quality, to achieve the required PSNR the approximation of the image has to be carry out up to a higher PSNR value. Nevertheless, because the quantization process maps some coefficients to zero, for the corpus of 20 images in this study, quantization does not affect sparsity. On the contrary, as can be observed in Fig. 4, for the sparsest images (first 5 images in Table 1) sparsity actually benefits from quantization. It is also clear that for the images in the upper part of the table the SR in the wavelet domain is significantly larger than in the pixel intensity domain. However, the level of sparsity achieved by the dictionary approach is, in both domains, significantly higher than that achieved by nonlinear thresholding of the wavelet coefficients. If the dictionary approach operates in the wavelet domain, then after quantization the mean value gain in SR with respect to thresholding of the wavelet coefficients is 163%, with standard deviation of 17%. In the pixel intensity domain the corresponding gain is 113%, with standard deviation of 30%.

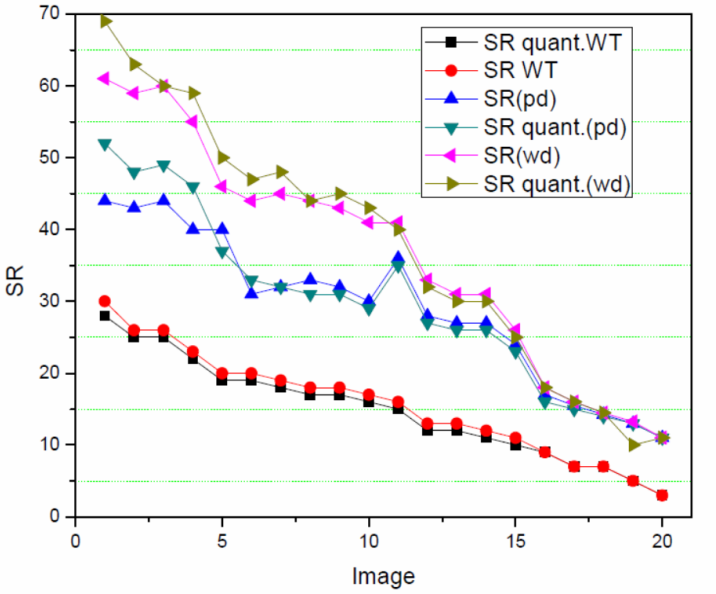

Fig. 4. Comparison of the SRs, before and after quantization, corresponding to the dictionary approaching both the pixel intensity and the wavelet domain and to the wavelet approximation by nonlinear thresholding

5 Conclusion

In this paper, we proposed a blockchain-based mechanism to mediate secure problem between users and a pool of shared (sensitive) data. Compared to the traditional cloud-based image data management network, we constructed a scalable (redesigned to allow speedy transactions) and lightweight blockchain to demonstrate the efficiency of data. In the proposed system, communication, authentication protocols and consensus algorithms between entities were not fully investigated. It would be interesting to extend this work by fully exploring these in future studies. We state that the architecture descried in this paper is a top layer of the blockchain-based sharing control system that is under implementation and testing. In our future work, an experimental study will be conducted to improve the systems efficiency and to obtain empirical data for further studies.

References

[1] I. Radanović, R. Likić, Opportunities for use of blockchain technology in medicine, Applied Health Economics & Health Policy 16(5)(2018) 583-590.

[2] L. Zhou, L. Wang, Y. Sun, MIStore: a blockchain-based medical insurance storage system, Journal of Medical Systems 42(8)(2018) 149.

[3] V. Patel, A framework for secure and decentralized sharing of medical imaging data via blockchain consensus, Health Informatics Journal 25(4)(2019) 1398-1411.

[4] H. Kaur, M.A. Alam, R. Jameel, A.K. Mourya, V. Chang, A proposed solution and future direction for blockchain-based heterogeneous Medicare data in cloud environment, Journal of Medical Systems 42(8)(2018) 156.

[5] G.G. Dagher, J. Mohler, M. Milojkovic, P.B. Marella, Ancile: privacy-preserving framework for access control and interoperability of electronic health records using blockchain technology, Sustainable Cities & Society 39(2018) 283-297.

[6] H. Li, L. Zhu, M. Shen, F. Gao, X. Tao, S. Liu, Blockchain-based data preservation system for medical data, Journal of Medical Systems 42(8)(2018) 141.

[7] K. Gammon, Experimenting with blockchain: can one technology boost both data integrity and patients' pocketbooks?, Nature Medicine 24(4)(2018) 378-381.

[8] M.N.K. Boulos, J.T. Wilson, K.A. Clauson, Geospatial blockchain: promises, challenges, and scenarios in health and healthcare, International Journal of Health Geographics 17(1)(2018) 25.

[9] K.N. Griggs, O. Ossipova, C.P. Kohlios, A.N. Baccarini, E.A. Howson, T. Hayajneh, Healthcare blockchain system using smart contracts for secure automated remote patient monitoring, Journal of Medical Systems 42(7)(2018) 130.

[10] K. Fan, S. Wang, Y. Ren, H. Li, Y. Yang, Medblock: efficient and secure medical data sharing via blockchain, Journal of Medical Systems 42(8)(2018) 136.

[11] A. Firdaus, N.B. Anuar, M.F.A. Razak, I.A.T. Hashem, S. Bachok, A.K. Sangaiah, Root exploit detection and features optimization: mobile device and blockchain based medical data management, Journal of Medical Systems 42(6)(2018) 112.

[12] F. Hartung, M. Kutter, Multimedia watermarking techniques, Proceedings of the IEEE 87(7)(1999) 1079-1107.

[13] H. Nyeem, W. Boles, C. Boyd, A review of medical image watermarking requirements for teleradiology, Journal of Digital Imaging 26(2)(2013) 326-343.

[14] N.L. Ping, K.B. Ee, G.C. Wei, A study of digital watermarking on medical image, in: Proc. World Congress on Medical Physics and Biomedical Engineering, 2006.

[15] K.A. Navas, M. Sasikumar, Survey of medical image watermarking algorithms, in: Proc. 4th International Conference: Sciences of Electronic, Technologies of Information and Telecommunications, 2007.

[16] S. Boucherkha, M. Benmohamed, A lossless watermarking based authentication system for medical images, in: Proc. International Conference on Computational Intelligence, ICCI 2004, 2004.

[17] N. Memon, Watermarking of medical images for content authentication and copyright protection, [dissertation] Pakistan: Faculty of Computer Science and Engineering, GIK Institute of Engineering Sciences and Technology, 2010.

[18] D. Bouslimi, G. Coatrieux, M. Cozic, C. Roux, A joint encryption/watermarking system for verifying the reliability of medical images, IEEE Transactions on Information Technology in Biomedicine 16(5)(2012) 891-899.

[19] M.M. Abd-Eldayem, A proposed security technique based on watermarking and encryption for digital imaging and communications in medicine, Egyptian Informatics Journal 14(1)(2013) 1-13.

[20] N.A. Memon, S.A.M. Gilani, Adaptive data hiding scheme for medical images using integer wavelet transform, in: Proc. International Conference on Emerging Technologies, 2009.

[21] F. Ahmed, I.S. Moskowitz, A semi-reversible watermark for medical image authentication, in: Proc. Transdisciplinary Conference on Distributed Diagnosis and Home Healthcare, 2006.

[22] A. Mehto, N. Mehra, Adaptive lossless medical image watermarking algorithm based on DCT & DWT, Procedia Computer Science 78(2016) 88-94.

[23] R. Thanki, S. Borra, V. Dwivedi, K. Borisagar, An efficient medical image watermarking scheme based on FDCuT-DCT, Engineering Science & Technology An International Journal 20(4)(2017) 1366-1379.

[24] X. Guo, T.G. Zhuang, A region-based lossless watermarking scheme for enhancing security of medical data, Journal of Digital Imaging 22(1)(2009) 53-64.

[25] C.J. Duan, J.F. Ma, Y.B. Zhang, K. Hou, S.L. Bao, Energy conduction model and its application in medical image segmentation, Journal of Software 20(5)(2009) 1106-1115.

[26] F. Rahimi, H. Rabbani, A dual adaptive watermarking scheme in contourlet domain for DICOM images, Biomedical Engineering Online 10(1)(2011) 53.

[27] O.M. Al-Qershi, B.E. Khoo, Authentication and data hiding using a hybrid ROI-based watermarking scheme for DICOM images, Journal of Digital Imaging 24(1)(2011) 114-125.

[28] C.K. Tan, J.C. Ng, X. Xu, C.L. Poh, Y.L. Guan, K. Sheah, Security protection of dicom medical images using dual-layer reversible watermarking with tamper detection capability, Journal of Digital Imaging 24(3)(2011) 528-540.

[29] W. Pan, G. Coatrieux, J. Montagner, N. Cuppens, F. Cuppens, C. Roux, Comparison of some reversible watermarking methods in application to medical images, in: Proc. International Conference of the IEEE Engineering in Medicine & Biology Society, 2009.

[30] H.H. Tsai, H.-C. Tseng, Y.S. Lai, Robust lossless image watermarking based on alpha-trimmed mean algorithm and support vector machine, Journal of Systems & Software 83(6)(2010) 1015-1028.

[31] H. Rahmani, R. Mortezaei, M.E. Moghaddam, A new lossless watermarking scheme based on DCT coefficients, in: Proc. International Conference on Digital Content, Multimedia Technology and ITS Applications, 2010.

[32] I.F. Kallel, M.S. Bouhlel, J.C. Lapayre, Improved Tian's method for medical image reversible watermarking, Gvip Journal 7(2)(2007) 1-5.

[33] R.D. Fu, W. Jin, A wavelet-based method of zero-watermark utilizing visual cryptography, in: Proc. International Conference on Multimedia Technology, 2010.

[34] W. Jin, J.X. Li, C.Q. Yin, An image zero-watermarking scheme based on visual cryptography utilizing contour-wavelet, Journal of Optoelectronics Laser 20(5)(2009) 653-656.

[35] C. Qu, X. Yang, D. Yuan, Zero-watermarking visual cryptography algorithm in the wavelet domain, Journal of Image & Graphics 19(3)(2014) 365-372.

[36] A. Roček, K. Slavíček, O. Dostál, M. Javorník, A new approach to fully-reversible watermarking in medical imaging with breakthrough visibility parameters, Biomedical Signal Processing & Control 29(2016) 44-52.