Privacy Protection for Medical Image Management Based on Blockchain

Yifei Li[1], Yiwen Wang[1], Ji Wan[2], Youzhi Ren[1], and Yafei Li[1(✉)]

[1] School of Information Engineering, Zhengzhou University, Zhengzhou, China
[2] School of Computer Science and Technology, Beihang University, Beijing, China
wanji@buaa.edu.cn

Abstract. With the rapid development of medical research and the advance of information technology, Electronic Health Records (EHR) has attracted considerable attention in recent years due to its characteristics of easy storage, convenient access, and good shareability. The medical image is one of the most frequently used data format in the EHR data, which is closely relevant to patient personal data and involves many highly sensitive information such as patient names, ID numbers, diagnostic information and telephone numbers. A recent survey reveals that about 24.3 million medical images have been leaked from 50 countries all over the world. Moreover, these medical images can be easily modified or lost during the transmission, which seriously hinders the EHR data sharing. Blockchain is an emerging technology which integrates reliable storage, high security and non-tamperability. In this paper, we propose a privacy protection model that integrates data desensitization and multiple signatures based on blockchain to protect the patient's medical image data. We evaluate the performance of our proposed method through extensive experiments, the results show that our proposed method achieves desirable performance.

Keywords: Privacy protection · Blockchain · Medical image · Data management

1 Introduction

With the rapid development of medical research and the advance of information technology, Electronic Health Record (EHR) [12], has attracted considerable attention in recent years due to the features of easy storage, convenient access, and good shareability. The EHR data generally contains laboratory sheet, examination result, and medical image plays an essential role for cliniciansand researcher in their daily life, which are of great significance to help cliniciansmake efficient and effective diagnosis and treatment plans, and to promote the prevention of diseases by researchers.

Y. Li and Y. Wang—Equal Contribution.

C. S. Jensen et al. (Eds.): DASFAA 2021 Workshops, LNCS 12680, pp. 414–428, 2021.
https://doi.org/10.1007/978-3-030-73216-5_28

Since the EHR data is closely relevant to the patient privacy and involves many highly sensitive information, many national laws clearly stipulate that the usage of EHR data should be offered strict attention to patient privacy protection and information security. Nevertheless, the patient privacy is often leaked during the sharing process of the EHR data. A recent survey reveals that about 24.3 million medical images have been leaked from 50 countries all over the world. Moreover, these medical images can be easily modified or lost during the transmission, which seriously hinders the EHR data sharing. Hence, how to effectively balance the sharing capability and the privacy for the EHR data is the critical task to be addressed. The medical image is one of the most frequently used data format in the EHR data, and contains many privacy information such as names, ID numbers, diagnostic information, and telephone numbers. For the reason of simplification, in this paper we mainly focus on the privacy protection for the medical image data management.

Recently, a novel technology, Blockchain [11], receives strategic attention from various countries, which integrates the characteristics of reliable storage, high security and non-tampering. Notably, the feature of immutable timestamp can protect the data integrity and ensure traceability of the source and the usage for medical images. In addition, the cryptography and signature technologies can realize the data privacy protection and solve the trust certification among users. However, the usage of blockchain for the medical image sharing still has some shortcomings, e.g., the storage speed of the chain is slow and the medical images require huge storage space, resulting in poor processing performance.

In this paper, we propose an efficient privacy protection model based on the blockchain for the medical image data management, which integrates the technologies of data desensitization and multiple signature. Firstly, since the medical images typically contain the patient's personal information, thus we parse and desensitize the medical image data to separate the privacy information from the medical images. Secondly, we propose an efficient data storage strategy based on the blockchain sharding technology [17] where the patient privacy data is stored on different nodes, each single node only saves part of the encrypted patient privacy information instead of the complete medical images, addressing the problem of huge storage cost. In addition, we adopt the Inter Planetary File System (IPFS) technology to store the medical images with non-sensitive information and the hash value of the return value and text records directly on the blockchain together. Finally, we have evaluated the efficiency and effectiveness of our proposed solution through extensive experiments.

2 Related Works

In this paper, we propose an efficient solution based on blockchain to protect the security of medical image data and strengthen the patient privacy. We next introduce several relevant works in this section.

2.1 Electronic Health Record

Electronic health record (EHR) is a record about health status and health behavior of individuals throughout the life cycle and is stored and managed electronically, which can improve the efficiency of medical services and promotes the sharing capability of health information.

Zyskind [18] proposed a decentralized information management system, through MIT's OPAL platform to complete the encrypted storage of data, and the system can also use the underlying architecture of Bitcoin to achieve access control of case information. Lazarovich et al. [8] proposed a privacy storage project of the opportunity blockchain, introducing an open source third-party database to store information, and using AES (advanced Encryption Standard) symmetric encryption algorithm to enhance the security of the project. Bhuiyan et al. [2] proposed a cross-institutional security sharing model of medical files using blockchain technology, dividing multiple hospitals into two groups with different permissions. If the hospital has dishonest behavior, it will be demoted to the lower-privileged group. Xia et al. [14] proposed a medical blockchain, and the system mainly uses the PBFT technology consensus algorithm, which also uses asymmetric encryption and public key infrastructure (Public key infrastructure, PKI) and other cryptographic technologies. In addition, the system also designed storage methods for structured and unstructured data in blockchain and external databases. Cai et al. [4] proposed to use the dual chains to solve the problem of privacy leakage. The transaction chain is responsible for the transaction and settlement of commercial resources, and the user chain only saves account information and does not involve related transactions. Gay et al. [7] proposed the idea of using multiple private keys and multi-person authorization to solve the problem of user privacy protection from the two aspects of decentralization and privacy protection of electronic health records. However, the storage and sharing methods of these electronic health files often require a large amount of storage space when processing medical pictures and images, and the processing performance is reduced, which is difficult to adapt to actual application requirements.

2.2 Medical Privacy Protection

With the development of the Internet and cloud computing, more and more medical images are transmitted and stored through the Internet. However, the medical images have a lot of sensitive information, it is easy to cause the personal privacy of patients to be stolen or leaked. Many researchers have carried out Related research work on medical image privacy protection [15]. The traditional image encryption algorithms consists of the pixel scrambling [10], transform domain [13], homophobic [3], chaos-based system [5,6] approaches.

Based on pixel scrambling, the pixel original position is scrambled to destroy the correlation of the image to achieve encryption. The pixel scrambling does not change the size of original value and the statistical information of the original pixel is still retained. The biggest feature of homomorphic encryption is that the ciphertext domain can be directly operated, that is, the process of decrypting,

calculating and re-encrypting the image is no longer needed, which simplifies the image processing process.

Maniccam [10] proposed a scrambling encryption algorithm based on SCAN, which destroyed the correlation of the image according to the scrambling rules of SCAN to achieve encryption. Yang [16] uses image scrambling technology to achieve encryption, and the secret key is stored in form of image, which improves the security of image transmission. Liu [9] realizes the effect of scrambling pixels through exclusive-or and modulo calculation, thereby encrypting the image. Bhatnagar [1] uses discrete transformation to obtain sparse matrix, and then uses the sparse matrix to implement image encryption. However, these encryption methods are mainly for traditional medical images, and there are few related researches on medical images.

3 System Framework

The privacy protection integrated with data desensitization and multi-signature for medical image data includes the upload and query processing. As the processing of upload involves data desensitization, IPFS star file system and blockchain node up chain operations, multiple systems are required to cooperate with each other. For the query processing, multi-signature and access control are involved to guarantee system data accurate and secure.

3.1 Update Processing

The upload processing for medical images is the key function of the system. Initially, we execute the upload operation of the patient's medical images, the system will execute strict desensitization for these images. To reduce the huge transmit workload, we use the IPFS system to store the desensitized medical images instead of the whole images to the blockchain, and the hash values of medical images are saved in the blockchain to achieve the permanent storage. The storage steps for medical images are as follows: The digital certification authentication center has the rights of key initialization and certificate management, which allocates different keys for different patients and institutions. When a patient requests adding new medical images in the system. To prevent the image being tampered, the patient's private key is used to sign the medical images. After receiving the request to add medical image data, the system first verifies the signature according to the public key to verify the requester. If the signature verification is finished, the system generates a receipt that is sent to the IPFS server of this institution. Afterwords, once the IPFS server receives the receipt, it uses the public key of the medical institution to verify the message. If the verification is correctness, it notifies the blockchain to participate in the consensus to record the characteristic value of medical images.

3.2 Query Processing

In this system, the patient's medical image is stored in the address that corresponds to the patient's public key. This address is used as the only index in the backend to identify a certain patient. The steps for querying and modifying the medical image data are as follows: When accessing a patient's medical image, the patient's private key and the doctor's private key are used to send a signed data access request to the IPFS server. Next, the IPFS server needs to verify the signed message. If the verification is success, the IPFS server should return the desensitized medical image. After that, the IPFS server will send the signed message to the blockchain. Then, if the medical images only needs to be accessed by doctor or patient, the above two steps are enough. However, if medical image needs to be modified, multiple-signatures are required through the private keys of doctor and patient. If the verification is success, the IPFS server will modify the medical image of the patient and save the message patient ID, doctor ID, modification time, hash value of the medical image on blockchain.

4 Image Desensitization

Digital Imaging and Communications in Medicine (DICOM) not only refers to digital medical imaging and communication in medicine but also an international standard for medical images and related information. In this section, we first introduce the specification of the DICOM standard medical image, then explains the procedures of desensitizing the information carried.

4.1 Content Analysis

A standard medical image file consists of the header information and the dataset body. The header information is composed of the introduction, prefix, and file header element. The dataset body comprises multimedia information and multiple data elements (such as images and videos).

The storage information part of both the header element and the dataset element has the same data structure which mainly contains the following fourfolds: tag, type, length, value field, these four parts are described in Fig. 1.

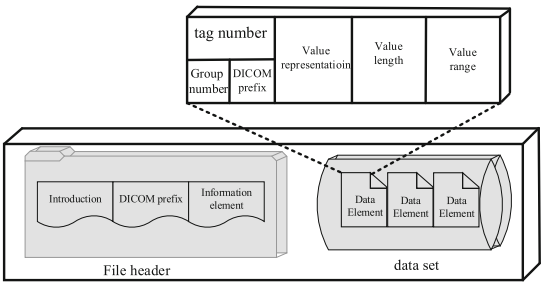

Fig. 1. The structure of DICOM file

4.2 Desensitization

In this section, we propose the method to parse the DICOM file, which consists of two steps, namely, the file resolution and file processing. The file resolution comprises three main parts: header resolution, content reading, and sensitive information. While the procedures of file processing include desensitization processing and saving file.

The file header resolution of DICOM standard medical image is bytecode data stream processing, because the first 128 bytes of the front file header does not contain valid data. Therefore the processing the byte part is skipped and the data value of 128–131 bytes is used to determine whether corresponds to the hexadecimal of the four letters "DICM" or not. If they are equal, the file is definitely DICOM standard medical image file and enter the step 2. Otherwise, the file is not a DICOM standard medical image file.

Step 1: (Data reading) The data elements in the file are stored in key-value format. The elements are read in turn and save them in the corresponding array collection. Then, go to Step 3.

Step 2: (Data filtering) Data elements are filtered out according to the DICOM standards, for example, group number '0010' is usually the patient's basic information, group number '0008' is usually the patient's condition information. The value of this part of the information is read in a group number index and the information is cached for the fourth step of desensitization.

Step 3: (Desensitization) Each byte is desensitized ac-cording to DICOM standards, such as masking sensitive labels (e.g. names), erasing hospital information and patient ID numbers, truncating dates and locations.

Step 4: (File Saving) A special tool is required while accessing standard DICOM files, which is not conducive to access to and sharing of medical images. We can choose whether to save the files as JPEG format or both DICOM and JPEG format when we work with files.

The method proposed in this section protects the patient's medical image information by using data processing and data desensitization. In the meanwhile, after the detailed analysis of medical image files, we can make the conclusion that, the anonymization of data can be better realized by two steps that are the file resolution and file processing, leading to a good share data on blockchain system.

5 Blockchain-Based Privacy Protection

The private data in the medical image needs to be protected and encrypted. This is particularly important when it refers to sensitive information, such as AIDS, hepatitis B, cancer, face-lifting, and psychosis. The research institutions should take relevant measures to make patients trust the institution fully, and build a privacy and confidentiality system with a complete data security protection mechanism. For the existing system, the personal health data of patients is managed by different hospitals or companies, and different medical institutions often

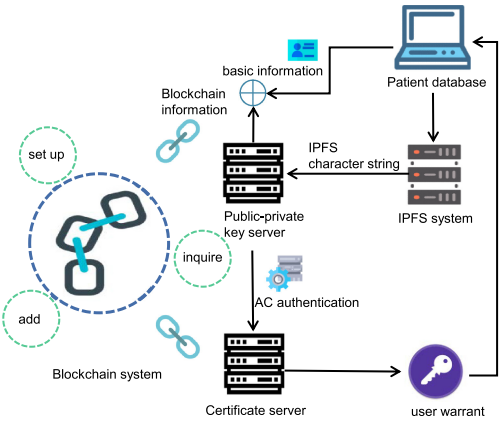

Fig. 2. The structure of DICOM file

use the information systems built by different companies, which makes it difficult to interact. Meanwhile, medical institutions are unwilling to share medical information for the sake of protecting their copyright. In this section, we propose an efficient blockchain-based solution with the features of privacy protection and reliable sharing. Putting IPFS and blockchain together improves the efficiency greatly, where IPFS stores massive amounts of data while blockchain saves IPFS addresses. At the same time, the privacy protection of the medical image data is realized through signature technology and access control mechanism (Fig. 2).

5.1 Digital Certificate Authentication

Certification Authority (CA) certification is a significant part of the system, which refers to the certification user's authority. This module is devoted to realize the function of key initialization and certificate management. It is applied to make sure the user's identity in the network. After CA authenticates the user's public key, a digital certificate will be generated, the status of which in the network is the same as that of the ID card in real life.

Table 1. Data access permissions

Type	Authority
1	Personal information
2	Medical record
3	Medical images and videos
4	Desensitized medical images
5	Feature value of medical image (hash value)

The authentication and management of user's public and private keys is the main function of CA authentication in the system, which can only be used after authentication. It includes functions such as generation and logout. The reason why the management of user's public and private keys is vital is that, the signature of user's public and private keys needed in the privacy protection and reliable sharing system of medical image data based on blockchain. Generally, each institution has its own distinct data access permission, the public and private key pairs in the CA include the following permissions which are shown in Table 1.

In order to realize the detailed division of the authority of different users, the authority control manages the authority for different users and organizations separately. Note that each patient is capable of accessing the IPFS server with the Key-1 secret key to obtain all permission of personal image data, and get the characteristic value through the blockchain consensus node server to verify whether the image data has been modified. The corresponding personal information, medical files, medical images and videos can be obtained by the research of medical institution by using Key-2. The insurance company can get the patient data through Key-3 after desensitization so as to audit the insurance claims. Due to the desensitization data without sensitive information, the risk of privacy leakage is small. By checking the hash value of image data, we can verify whether the user's data have been tampered. In case of doctor-patient disputes, the government can obtain the eigenvalue information of image data on the blockchain consensus node through Key-4, thus realizing the supervision on whether medical institutions tamper with the data of patient's image data. The research institutions can get medical images, videos, and corresponding written medical files through Key-5 to carry out scientific research. The permissions of each type of key are shown in Table 2.

Table 2. Permissions of different secret keys

Type	Authority	Owner	Key
1	1, 2, 3, 4, 5	Patients	key-1
2	1, 2, 3	Hospital	key-2
3	1, 4, 5	Government	key-3
4	5	Company	key-4
5	2, 3	Institution	key-5

5.2 Blockchain and IPFS System Storage

The IPFS is a distributed file system that includes a mapping function. It can divide files into several same size blocks with the same size, and then calculate the combination of each block to build a file retrieval table, which can realize

the purpose of storing file blocks in different server clusters. In order to achieve permanent, decentralized storage, and sharing of files, the medical image data can be identified by generating independent hash values from their content. Only one file with the same content can exist in the system, which saves storage space and strengthens the protection of user privacy.

The system used in this paper consists of three layers. The data layer includes the IPFS cloud storage cluster and the blockchain consensus node which is off-chain IPFS distributed cloud storage clusters. It is a blockchain consensus node cluster based on the alliance chain. The business layer mainly realizes the reliable access and desensitization storage functions of medical image data, and reserves smart contract interfaces, including data desensitization modules, data layer access interfaces, and smart contract modules. It can realize efficient desensitization processing of sensitive patient information, and provide access interface between user layer and data layer. The user layer consists of the medical data management system and the user mobile phone access system, which can realize the medical data query on the mobile phone, the registration of staff and patients in various medical institutions. The system architecture is as shown in Fig. 3.

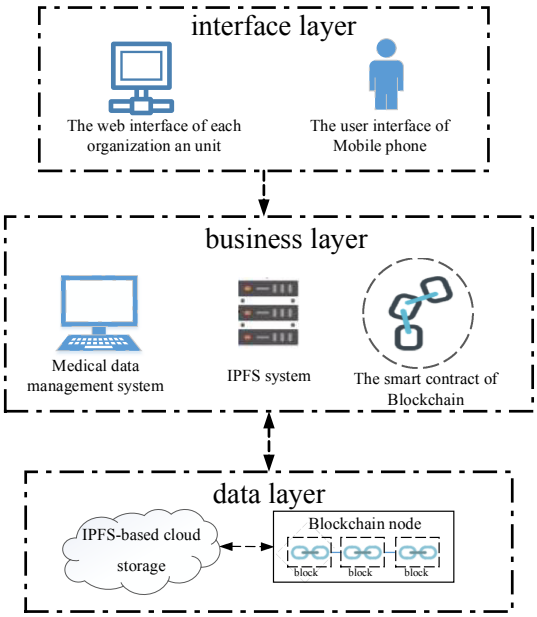

Fig. 3. System architecture based on IPFS

The steps to add medical image data are as follows:

Step 1: A patient P initiates a request to add the medical image data to the institution *Dep*.

$$R_{Add} = AddMsg||Sig_{R_{pk}}(H(AddMsg)) \tag{1}$$

$AddMsg = (ID_R, ID_P, ID_{Dep}, M_E, R_{pk}, t)$ contains the requester ID_R, patient ID_P, medical institution ID_{Dep}, medical image M_E, the public key of the requester R_{pk}, and the request time t. In order to prevent the requested content from being tampered, the private key R_{sk} of the requester will be used for signature.

Step 2: After receiving a request to add a medical image, the medical institution *Dep* first verifies the signature according to the public key R_{pk} to check the identity of the data sender. If the signature verification is successful, the receipt information is generated and sent to the IPFS server of the institution, where the receipt information is: $T = (ID_R, ID_P, ID_{Dep}, M_E, R_{pk}, Dep_{pk}, t_2)$. Next, the private key of the institution can be used to encrypt the information and send it to the IPFS server. If the signature verification fails, the request will be rejected.

Step 3: After the IPFS server receives the bill information sent by the medical institution *Dep*, it uses the public key of the medical institution Dep_{pk} to verify the message. If the verification is passed, the bill information is determined to be valid, and the IPFS server will send a notification $M = (ID_R, ID_P, ID_{Dep}, IPFS_{pk}, Hash_E, t_3)$ to the blockchain consensus node. Among them, $IPFS_{pk}$ is the public key of the IPFS server node. The blockchain node only needs to save the hash value of the file while does not need to save the complete file containing text, images, or other information.

5.3 Data Access Based on Multi-signature

The patient's medical image data is stored in a distributed manner through the IPFS system. In order to further protect the privacy of the patient and prevent the doctor from unilaterally using the patient's data information, we have designed a multi-signature algorithm (MSA), which makes it necessary to use multiple signature of doctors and patients to access the medical image data. Assuming that there are n signers and verifying that they have received at least m signatures, the signature is set to be valid, so it is especially suitable for scenarios where multiple people vote together. In the privacy protection and reliable sharing system, in order to protect the privacy of patients, at least one doctor and one patient are required to authorize at the same time to access the patient's medical image data. Therefore, the multi-signature algorithm can satisfy our application scenes well. Compared with threshold signatures, multiple signatures also have high security and are easier to design and implement. Next, we will explain the medical data access algorithm based on multiple signatures used in this paper.

Assuming that M is a message to be signed. Firstly, M is grouped into a bit string as $M = \{m_1, m_2, \cdots, m_n\}$, where m_i represents the group that needs to

be encrypted separately. The encryption system generates a key (GK) to encrypt each block. The encrypted bit group set constitutes a ciphertext signature (Sig), and finally the patient uses the private key (PK) to perform signature verification to obtain the plaintext. Generally, the MSA has three entities: key generation center (KGC), signer, and validator, which are mainly composed of the following three operations, It can be expressed as *MSA = (GK, Sig, Ver)*.

- Generate the key (GK). The CA center realizes key initialization, including the doctor's public key $PK_d = (n_d, e_d)$ and the doctor's private key $SK_d = (n_d, d_d)$ in the first layer of encryption. Then, the patient's public key $PK_p = (n_p, e_p)$ and the private key $SK_p = (n_p, d_p)$ in the second layer of encryption. Among them, n_d and e_d are the random numbers generated when the RSA algorithm generates the doctor's public key, d_d is the unique corresponding number calculated by (n_d, e_d). n_p and e_p are the random numbers generated when the RSA algorithm generates the patient's public key, d_p is the unique corresponding number calculated by (n_p, e_p).
- Generate signature (Sig). The doctor's public key $PK_d = (n_d, e_d)$ is used to encrypt and generate $Sig = M' = \{m'_1, m'_2, \cdots, m'_n\}$, where m'_i represents the first encryption of each gruop. Then, we use the patient's public key $PK_p = (n_p, e_p)$ to encrypt and generate $Sig' = M'' = \{m''_1, m''_2, \cdots, m''_n\}$, where m''_i represents the result of the second encryption of each group.
- Signature verification (Ver). After entering the patient's private key $SK_p = (n_p, d_p)$, and getting the public key of patient P from the CA center, the signature result M' is obtained. Then, the doctor's private key $SK_d = (n_d, d_d)$ is entered, the doctor's public key from the CA center can be used to verify the message M'. Finally, the final signature result M' is obtained.

The basic process of the MSA encryption algorithm in our method is as follows:

Step 1: We first find two large numbers p and q randomly and verify their primality. After the verification, we can get the random number $nd = p * q$ in the doctor's key, and the random number n_p and Euler function f_{n_p} in the patient key. Then, we divide the message M into $\{m_1, m_2, m_3, ..., m_n\}$.

Step 2: In this step, we generate the doctor's public key $PK_d = (n_d, e_d)$, where e_d is an integer randomly selected in $(1, f_{nd})$ and needs to satisfy $gcd(e_d, f_{nd}) = 1$, where *gcd* represents the greatest common divisor, the same is true for generating the patient's public key $PK_p = (n_p, e_p)$.

Step 3: In this step, we generate the doctor's private key SK_d and match the unique d_d according to the selected e_d, and then generate the patient's private key SK_p.

Step 4: We use the doctor's public key PK_d to encrypt and generate Sig = M' and use the patient's public key PK_p to encrypt and generate Sig' = M'';

Step 5: If we enter the patient's private key SK_p, we can get the public key of patient P from the CA center and get the signature result M'. If we enter the doctor's private key SK_d, we can get the public key of doctor D from the CA center and then verify the message M' to obtain the final signature result M.

6 Performance Evaluation

In this section, we have verified the performance of our proposed method that integrates data desensitization and multiple signatures. Firstly, we introduce the experimental settings including the actual simulation program and the construction of the experimental environment. Then, we test our method on real-life DICOM image dataset with size of $5k$ in terms of processing speed, access delay, and the desensitization quality.

6.1 Experimental Settings

In this paper, we build an IPFS server, a certificate authority center, and the smallest Byzantine system composed of four nodes (composed of $3F + 1$ surviving nodes, F is the number of malicious nodes). The hardware environment is as shown in Table 3.

Table 3. System settings

Items	Environment
Blockchain Node	Aliyun, Xeon E5-2682 v4, 2.5 GHz 2G DDR4
OS	Ubuntu 7.5.0-3ubuntu1 18.04
Blockchain System	Fabric 1.4
Language	python 3.8.5, nodejs v8.10.0, go1.9.5
IPFS	go-ipfs v0.4.15

6.2 Experimental Result

In this section, we report the evaluation results from the perspective of the system's image processing speed, the access delay, and the storage cost.

Effect of Processing Speed. As shown in Fig. 4, the average processing time is becoming longer as the resolution increases. For the image with a resolution of 640*480, the average processing time is about 380 ms, which means that the system has a high ability to support concurrency. When the average number of images input by the system per second is less than 50, the time for the system to process a picture is relatively stable. When the average number of images per second is greater than 100, the average time for the system to process each image increases significantly, indicating that the system can simultaneously provide image processing capabilities for approximately 100 clients.

Effect of Access Delay. Since the medical images are stored in the IPFS system, there is no need for consensus among nodes. While the text medical record information is stored on the blockchain, which needs to reach consensus

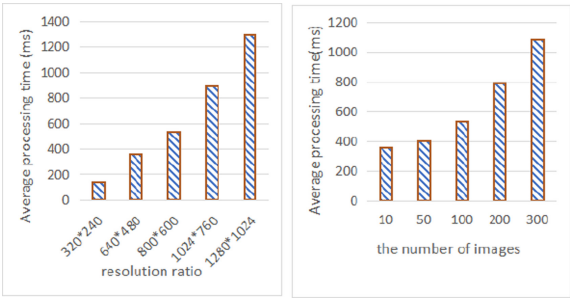

Fig. 4. Effect of image processing speed

among multiple nodes. The experimental results in Fig. 5 show that the IPFS system has high performance to obtain images, the average access delay for accessing text information and images increases with the increase of tasks. And the average access delay for medical images is significantly lower than the average access delay for obtaining text medical records.

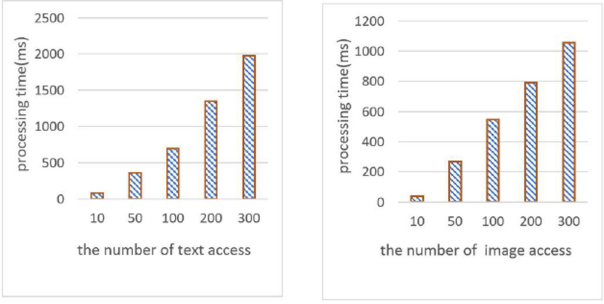

Fig. 5. Effect of access delay

Effect of Storage Cost. In Fig. 6, it can be seen that the algorithm proposed in this paper only needs to store the Hash value for the medical image data file on the blockchain. Therefore, compared with directly storing the medical image data on the blockchain, the processing time is reduced by 24.2%. When four blockchain nodes are used to store data, 77.5% of storage space is saved. The IPFS system can greatly improve storage space utilization and reduce system processing time.

Effect of Throughput. As shown in Fig. 7, with the increase in the number of transactions per second, the throughput of both increases linearly with the increase in the number of requests. However, the peak value of CA digital certification processing requests is 600 times per second, while the peak value of IPFS

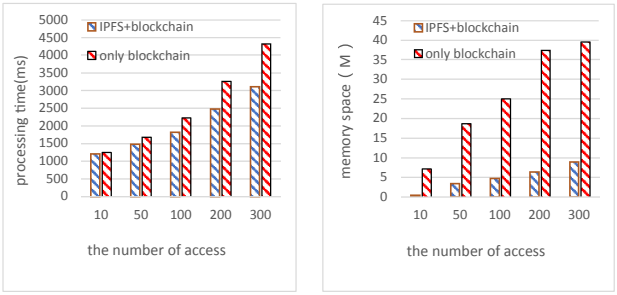

Fig. 6. Effect of storage cost

can handle about 1100 requests/second. We can also find that the concurrency of the system is mainly limited to the signature verification part. At the same time, the concurrency of image data in the blockchain system is much lower than that of the IPFS system.

Fig. 7. Effect of throughput

7 Conclusion

In this paper, we propose a privacy protection scheme for medical image data that integrates data desensitization and multi-signature. First, we designed a solution to parse the file format for the standard medical image. We also propose a data storage method based on blockchain and IPFS, the IPFS system is used for storing medical images and hash value of medical record are stored on the block chain, which improves the data storage efficiency and strengthens patient privacy protection. Finally, we tested the performance of our proposed method through extensive experiments where the results show that the proposed method in this paper achieves desirable performance.

References

1. Bhatnagar, G., Wu, Q.M.J., Raman, B.: Discrete fractional wavelet transform and its application to multiple encryption. Inf. Sci. **223**, 297–316 (2013)
2. Bhuiyan, M.Z.A., Zaman, A., Wang, T., Wang, G., Tao, H., Hassan, M.M.: Blockchain and big data to transform the healthcare. In: Proceedings of the International Conference on Data Processing and Applications, ICDPA 2018, Guangdong, China, 12–14 May 2018, pp. 62–68 (2018)
3. Brakerski, Z., Vaikuntanathan, V.: Efficient fully homomorphic encryption from (standard) LWE. SIAM J. Comput. **43**(2), 831–871 (2014)
4. Cai, G.G.: Channel selection and coordination in dual-channel supply chains. J. Retail. **86**(1), 22–36 (2010)
5. Chai, X., Fu, X., Gan, Z., Lu, Y., Chen, Y.: A color image cryptosystem based on dynamic DNA encryption and chaos. Signal Process. **155**, 44–62 (2019)
6. Chen, Q., Wu, T.T., Fang, M.: Detecting local community structures in complex networks based on local degree central nodes. Phys. A: Stat. Mech. Appl. **392**(3), 529–537 (2013)
7. Gay, J., Odessky, A.: Multi-person gestural authentication and authorization system and method of operation thereof (2017)
8. Lazarovich, A.: Invisible Ink: blockchain for data privacy. Ph.D. thesis, Massachusetts Institute of Technology (2015)
9. Liu, D., Zhang, W., Yu, H., Zhu, Z.: An image encryption scheme using self-adaptive selective permutation and inter-intra-block feedback diffusion. Signal Process. **151**, 130–143 (2018)
10. Maniccam, S.S., Bourbakis, N.G.: Lossless image compression and encryption using SCAN. Pattern Recognit. **34**(6), 1229–1245 (2001)
11. Nakamoto, S., et al.: Bitcoin: a peer-to-peer electronic cash system (2008)
12. Shahnaz, A., Qamar, U., Khalid, A.: Using blockchain for electronic health records. IEEE Access **7**, 147782–147795 (2019)
13. Sudharsanan, S.: Shared key encryption of JPEG color images. IEEE Trans. Consumer Electron. **51**(4), 1204–1211 (2005)
14. Xia, Q., Sifah, E.B., Smahi, A., Amofa, S., Zhang, X.: BBDS: blockchain-based data sharing for electronic medical records in cloud environments. Information **8**(2), 44 (2017)
15. Xie, X., Niu, J., Liu, X., Chen, Z., Tang, S.: A survey on domain knowledge powered deep learning for medical image analysis. CoRR abs/2004.12150 (2020)
16. Yang, Y.L., Cai, N., Ni, G.Q.: Digital image scrambling technology based on the symmetry of Arnold transform. J. Beijing Inst. Technol. **15**(2), 216–220 (2006)
17. Zamani, M., Movahedi, M., Raykova, M.: Rapidchain: scaling blockchain via full sharding. In: Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security, pp. 931–948 (2018)
18. Zyskind, G., Nathan, O., Pentland, A.: Decentralizing privacy: using blockchain to protect personal data. In: 2015 IEEE Symposium on Security and Privacy Workshops, SPW 2015, San Jose, CA, USA, 21–22 May 2015, pp. 180–184 (2015)