Interactive Sharing Method of Digital Media Image Information Based on Differential Privacy Protection

Wei Li(✉) and Jieling Jiang

Guangzhou Academy of Fine Arts, Guangzhou 510006, China
iccu007@163.com

Abstract. Because digital media image information is vulnerable to external attacks during interactive sharing, resulting in poor interactive sharing effect, a digital media image information interactive sharing method based on differential privacy protection is proposed. According to the sensitivity of digital media images, calculate the amount of digital media image information to be protected, and build a defense model of differential privacy protection mechanism. With LAN as the main communication medium, the C/S structure is used to realize the interactive management of digital media image information, calculate the information flow injected by a node to the interaction center, and ensure the smooth interaction process. The analysis of information set is in danger of being violated, revealing that the information set has the diversified characteristics of entropy to resist external attacks. Calculate the energy and distance of non-uniform clustering nodes, obtain the template mapping radius, and determine the weighted minimum value according to the residual energy of cluster heads and the spacing between clusters. Combined with multi-source information fusion method, the information sharing process of single node and multiple nodes is designed. The experimental results show that this method can realize information interaction, and the information is saved completely. The maximum amount of shared information is 900 bits, which has a good sharing effect.

Keywords: Differential Privacy Protection · Digital Media Image · Information Interaction · Information Sharing

1 Introduction

In the process of the continuous development of modern digital technology and the Internet, digital media technology has improved the richness of information resources, especially in the process of the continuous application of digital media technology, computer technology and network communication technology, digital media has penetrated into all aspects of life, making human beings enter the digital era. The digital media environment has created a diverse and rich ocean of open information for people. In the interactive sharing of digital media image information, participants may need to share

L. Yun et al. (Eds.): ADHIP 2023, LNICST 549, pp. 3–19, 2024.
https://doi.org/10.1007/978-3-031-50549-2_1

personal image data, such as photos or videos. However, these data may contain sensitive personal information, such as facial features, geographic location, etc. In order to protect these personal privacy, researchers have begun to explore how to address security issues during the data sharing process.

Literature [1] proposed a sharing scheme based on blockchain, designed a digital media image information security sharing model in combination with the blockchain distributed architecture, accessed the information in the model to the information collector, encrypted the information using an improved EIGamal encryption algorithm, and exchanged information using points instead of tokens in the traditional negotiation mechanism. After all nodes reached an agreement, The information package is stored in the information database to realize information sharing in the form of query and submission; Literature [2] proposes a sharing method based on the whole network power supply topology model. This method achieves the standardization of digital media image graphics information by establishing a graphics information sharing architecture and interaction model, and decoupling and exchanging different types of information based on CIM. However, in the above methods, most of the information is stored in relational databases, making it difficult to effectively share unstructured information. The amount of shared information is relatively small, and there may be situations of information loss.

In order to solve the shortcomings of the above methods, a digital media image information interactive sharing method based on Differential privacy protection is proposed.

2 Design of Real-Time Interaction Scheme of Digital Media Image Information

2.1 Construction of Interactive Defense Model Based on Differential Privacy Protection

Because digital media images are vulnerable to external attacks in the process of information exchange, a differential privacy protection mechanism is proposed. Based on this, the built interactive defense model is shown in Fig. 1.

It can be seen from Fig. 1 that digital media images may have multiple attack modes in the information exchange process, so when the real system is attacked, the digital media image data in the Physical system is synchronized to the virtual system through virtual to real mapping [3]. When the virtual system is attacked, the digital media image data in the virtual system is synchronized to the Physical system through virtual to real mapping; By providing feedback on the system synchronization process through virtual dual redundancy information, an interactive defense mode is formed to resist external attacks on digital media images during information exchange, prevent network vulnerabilities from being invaded, and provide a secure environment for information exchange security identification [4].

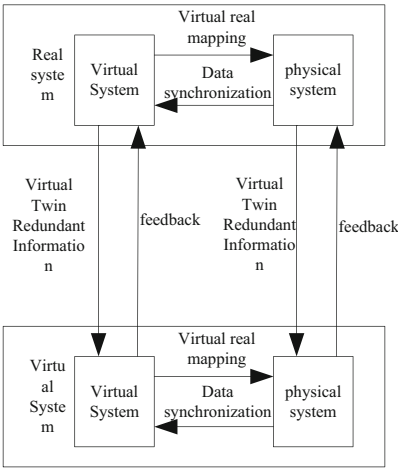


Fig. 1. Interactive Defense Model

In the defense link of differential privacy protection mechanism, the amount of digital media image information to be protected is calculated according to the sensitivity of digital media image, and the calculation formula is:

$$M = \left(M_x - \varepsilon \cdot \frac{|D_2 - D_1|^2}{\lambda} \right) \cdot t \tag{1}$$

In formula (1), M_x indicates the amount of input information; ε indicates the quantitative difference of sensitive information defense; λ indicates the level of information to be protected; D_1, D_2 indicates the attack intensity of any two messages; t indicates the defense duration.

In the process of malicious autonomous defense, due to the existence of the link layer, information at all levels is exchanged at will, resulting in tampering and collision of the link layer [5]. Therefore, in order to enhance the attack detection of the link layer, the defense capability of the link layer should be strengthened. Based on this, the defense model of differential privacy protection mechanism is constructed as follows:

$$W = \frac{\sqrt{\eta \cdot M}}{D_0 \times N^2} \tag{2}$$

In formula (2), η indicates information access rights; D_0 indicates the signal strength under attack; N Indicates that the information layer has been tampered with attack nodes. Differential privacy protection mechanism is the ability to provide a higher level of information security for the privacy of digital media images and better protect information from hacker intrusion by using differential private key technology on the premise that the attacker has mastered massive information [6]. By constructing this model, real-time detection and protection of digital media image information interaction can be realized.

2.2 Real Time Information Interaction

In order to realize the automatic collection, deep mining and feedback of digital media image information, the C/S structure is adopted to realize the interactive management of digital media image information with the whole process as the center, the computer as the core, and the LAN as the main communication medium. Its structure is shown in Fig. 2.

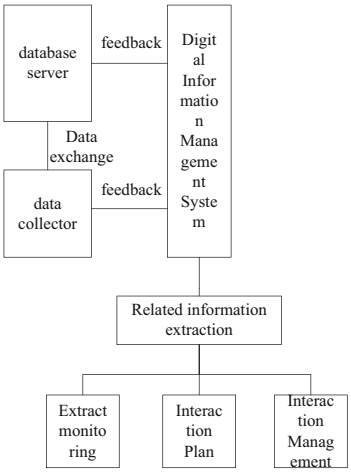


Fig. 2. Information interaction module

It can be seen from Fig. 2 that the information interaction module is mainly composed of the following three parts: the information acquisition part, which is responsible for providing the signal from the sensor to the computer for signal identification after effective processing; Information database service part, which stores the information of the information collection part in the information database, and can provide information support for information mining through information interaction with different information; In the application part of digital system, the digital information management system can deeply mine the information hidden in the production process and show it to the managers, making the managers' analysis of decision-making more intuitive and effective [7, 8].

The designed digital media image information interaction process is as follows:

On the information database server, establish an information directory for security detection of the interactive environment. In the information database server, the real-time information interaction mechanism is introduced to establish a group address composed of multiple users. In this way, each network element can establish a new information identification node [9] on a coordinator node. If the internal coordination node conflicts with the external coordination node during transmission, a real-time interaction technology is introduced according to the communication protocol between communication nodes.

Each interaction node acquires node information intelligently and autonomously through the Internet of Things access node. One node injects the calculation formula of information flow into the interaction center, which can be expressed as follows:

$$S=l_k^c \cdot \left\{s_k^c\right\} + l_k^d \cdot \left\{s_k^d\right\} \tag{3}$$

In formula (3): k indicates the number of packets; $\left\{s_k^c\right\}$ indicates the packet error correction retransmission information set, $\left\{s_k^d\right\}$ represents the packet control signaling set, l_k^c, l_k^d it respectively represents the length of error correction retransmission packet and the length of packet control signaling.

Each information is evenly distributed into the interaction defense model based on differential privacy protection to ensure smooth interaction process, so as to detect the non-zero kurtosis of each information. The spatial distribution vector based on differential privacy protection can be expressed as:

$$E_M=\frac{r_N^2}{T} \tag{4}$$

In formula (4), r_N represents the dangerous defense radius; T indicates the time-frequency distribution range of information. If the two kinds of interactive information are within the spatial distribution range of the above differential privacy protection, it indicates the information interaction security.

3 Design of Digital Media Image Information Security Sharing Scheme

3.1 Sharing Attack Resistance Based on Anonymous Differential Privacy Protection

The protection of differential privacy does not necessarily guarantee the security of digital media image information in the sharing process. In some special cases, the information set will still be in danger of being violated because it cannot completely avoid the attacker's prior knowledge and homogeneous attacks. The probability calculation formula is:

$$P = \beta(t) \cdot \frac{1}{\iota(\iota+1)} \tag{5}$$

In formula (5), $\beta(t)$ stay t the proportion of hazard information in the total information within the time; ι indicates the degree of adjacent information connection [10].

In order to overcome the shortcomings of anonymity and prevent different types of attacks, it is necessary to have different sensitivities in all information sets, and the following conditions must be met: if the anonymous tags in the disclosed information set conform to the above expression, the disclosed information set has the characteristics of entropy diversification:

$$\zeta = \sum_{a \in M} P(a, b) \cdot \log(P(a, b)) \tag{6}$$

In formula (6), $P(a, b)$ indicates that the sensitive information value is a the information of is on the label b probability in. The public information set meets the recursive diversity feature, if and only if any anonymous group label of the public information set meets the formula:

$$M_{\zeta} < \log(\zeta) \cdot (m_{x1} + m_{x2} + \ldots + m_{xn}) \tag{7}$$

In formula (7), $m_{x1}, m_{x2}, \ldots, m_{xn}$ an information set that represents the amount of input information. Recursive diversity can adjust the constant value to reduce the skew rate of the frequency of constant values given by different information sets of each anonymous group.

3.2 Information Sharing Process Design

In the process of information sharing, affected by the shared platform server, the location of information sharing nodes cannot be accurately determined, resulting in poor information sharing effect. To this end, the sharing process of non-uniform clustering information fusion is designed, which integrates decentralized information with non-uniform clustering information fusion technology. The interaction process designed is as follows:

Step 1: abstract the topology of the network and give the topology relationship;

Step 2: Obtain the topology in the network;

Step 3: Although the interactive platform server is the source of information, the accessed object can be used as the source server during configuration.

Step 4: Establish the fusion cluster based on this principle. In order to achieve non-uniform clustering, it is necessary to introduce different competition radii at the cluster head node to reduce the number of "hot zone" problems. It is necessary to calculate the energy and distance of non-uniform clustering nodes. The formula is:

$$Q = i \cdot \frac{Q_i}{Q_0} \tag{8}$$

$$L = \frac{L' - L_{\min}}{L_{\max} - L_{\min}} \tag{9}$$

In the above formula, i indicates the number of uneven clustering wheels; Q_i, Q_0 represent the initial and current energy of the node respectively; L' represents the distance between any two nodes; $L_{\min}$, $L_{\max}$ it respectively represents the nearest and farthest distance of any two nodes in all nodes.

To facilitate the rational use of information, the template mapping radius is designed in the information database mode, and the calculation formula is:

$$r' = 1 - Q \cdot L \tag{10}$$

In formula (10), the candidate node uses the existing information to construct a new node and uses it as the initial cluster head. After the initial cluster head is determined, broadcast the cluster head message. The unselected cluster head will no longer be in the

sleep state, and select the cluster head with the lowest communication cost to complete the cluster creation.

Step 5: In the process of intra cluster and inter cluster information fusion, it can be divided into two stages: intra cluster communication and inter cluster communication. In the process of inter cluster communication, the intra cluster and cluster head direct communication is realized through the single hop technology. Between two adjacent secondary clusters, the weighted minimum value is determined according to the residual energy of the cluster head and the spacing between clusters. The formula is:

$$\omega_j = \min\left(\mu \cdot \frac{L_j}{Q_j}\right) \tag{11}$$

In formula (11), μ respectively represent the j adjustment coefficient of nodes. According to the results of the above calculation, when two information centers cannot support each other, they cannot be merged. In order to distinguish between trusted and untrusted information, multi-source information fusion method is adopted. The formula is:

$$A_{x_1x_2} = \begin{cases} 0 \\ 1 - \dfrac{\sum\limits_{x_1 \cap x_2 \in M} m(x_1)m(x_2) \cdot \omega_j}{\sum\limits_{x_1 \cap x_2 \notin M} m(x_1)m(x_2) \cdot \omega_j} \end{cases} \tag{12}$$

In formula (10), $m(x_1)$, $m(x_2)$ respectively x_1, x_2 The amount of trusted and untrusted information. Using the regularization method, the relative importance of the fusion order is determined, the untrusted information is eliminated, and the effective information fusion is completed.

Step 6: Considering the special requirements of the information demand side, share the information of a single node, as shown in Fig. 3.

Each cluster head node broadcasts information with the competition radius as the transmission radius. After the cluster head receives the broadcast information from the cluster head node, a single node requests information sharing. The digital media image dispatching center uses its private key and the public key provided by the information demander to generate a proxy re encryption key, and provides a proxy re encryption key and an information request to multiple signature notaries. The notary will input the information into the information management contract, input the information into the corresponding file, download the corresponding password information from the file, and use the trap gate to verify whether the digital media image information required by the information demander is consistent with the provider. Homomorphic encryption mechanism is adopted to integrate the downloaded heterogeneous information ciphertext according to the required information requirements. The proxy key is used to re encrypt the encrypted ciphertext, and the ciphertext information is transmitted to the information requester through the off chain channel. Information demander uses private key to decrypt heterogeneous information and realize information sharing of single node.

Step 7: Based on the single node sharing mode, combine it with secure multi-party computing technology to form a multi node sharing mode, as shown in Fig. 4.

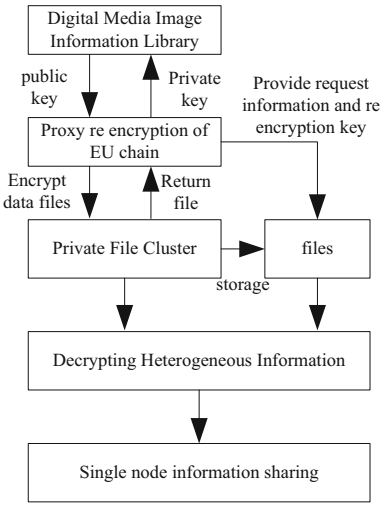


Fig. 3. Single node information sharing process

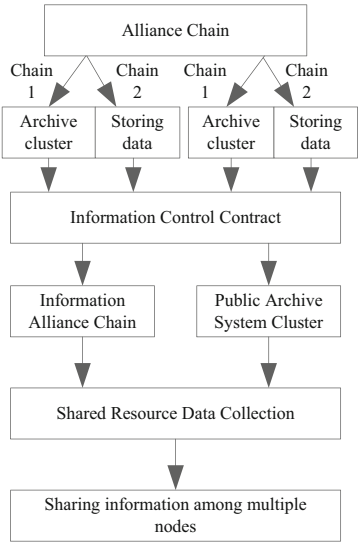


Fig. 4. Information sharing process of multiple nodes

As shown in Fig. 4, when the information demander generates a success rate information sharing request, the notary will query the file cluster according to the information demander's requirements, introduce the information control contract, and perform ciphertext operations on the information sets required by different nodes. The encrypted information and its information are divided into several blocks, and the proxy re encryption method is used to divide and re encrypt them, and they are transmitted on the link. The information demander reconstructs the encrypted text and generates the encrypted

text according to the specific reconstruction algorithm. The obtained information collection ciphertext is uploaded to a common file cluster and information alliance chain. Each node will download the required information from the research information alliance chain and the public archive system cluster, thus realizing the information sharing of multiple nodes.

4 Experiment

In order to verify the effectiveness of the interactive sharing method for digital media image information based on differential privacy protection, the blockchain based sharing method proposed in reference [1] and the sharing method based on the full network power topology model proposed in reference [2] were used as comparative methods to jointly test the effectiveness of comparative experiments.

4.1 Experimental Scenario Setting

Network based virtual world refers to multiple users in different physical environment locations, or multiple virtual worlds connected with each other through the network, or multiple users participating in a virtual reality world at the same time, using the interaction between computers and other users. The experiment scenario based on virtual reality system is shown in Fig. 5.

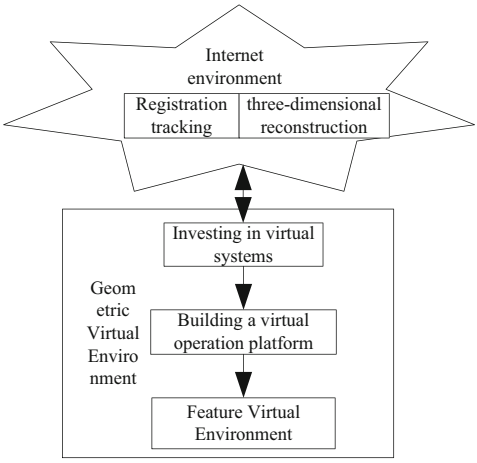


Fig. 5. Experimental scenario based on virtual reality system

In the application process, using the virtual environment of the Internet, you can digitize the information and then conduct interactive operations without any restrictions, and conduct a complete simulation process operation in a virtual environment, and record the whole process.

4.2 Simulation of Experiment Process

In the experimental scenario based on virtual reality system, establish a life cycle of digital media image information, and its model is shown in Fig. 6.

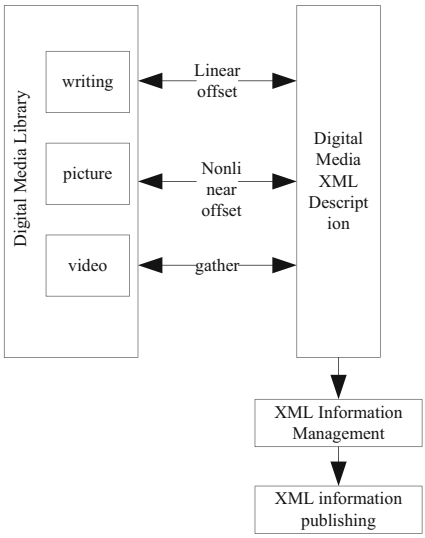


Fig. 6. Life cycle of digital media image information

Because XML is a structure oriented and content oriented description language, its inherent advantages make it easy to handle the access of various applications to resources as an exchange language, so XML schema is introduced into this model, and this technology is used to standardize the various stages of the digital life cycle.

(1) Generation phase

In this model, XML description is introduced in the generation phase, that is, the corresponding metadata description is generated at the same time as the material of digital media is generated, focusing on recording the relevant information during the generation of digital media, such as the author/owner of the media, creation time, keywords and instructions for use, and recording in the form of XML documents.

(2) Management phase

Different from traditional media, digital results enable digital media to be stored, managed and reused. In the current application requirements, the management of digital media mainly includes storage management, retrieval support (such as content-based query), copyright management, security management, etc. Taking content-based retrieval as an example, there are two main technical means at present: identification technology and MetaData retrieval technology. The recognition technology uses some special algorithms to search and match the original digital media files, such as matching the hue of the image; The database retrieval method is to store the MetaData information of each

digital media in a readable language in the database, and then use the retrieval mechanism provided by the database to retrieve information. Although the technical principles used in various applications are similar, the structure of management information may be completely different in different applications, which causes difficulties in information sharing.

(3) Release phase

The main task of the publishing phase is to send the information to the place where users can reach, and the publishing phase will also generate an XML document for outward delivery, which contains various information of digital media required by users.

This process needs to use the local weighted fitting method to correct the image. First, take the control point as the center, control the control point in the circle, and perform local surface fitting on the control point, because the selected polynomial is quadratic. After the control points are locally fitted, the control points correspond to a fitting result.

If the local control points in the image are sparse, several auxiliary control points need to be added to ensure that the control circle contains enough control points. The specific operation steps are as follows:

Step 1: Select an inscribed square in the control circle, and use the points on each side of the square as new control points. Since the square can be selected under control, the new points can be controlled within the image range.

Step 2: In the standard space, there will be several control points near the newly added control points. Triangle these points to obtain several triangles and determine the triangle nearest the newly added control points.

Step 3: Use the control points formed by each vertex of the nearest triangle to build a correction model, and the collinear position of the new control points in the distorted image can be calculated through this model.

Step 4: After all control points complete the above local surface fitting, any point will correspond to a fitting result. The mapping relationship of each distortion point in the image can be obtained from nearby calculated points, so as to achieve distortion point correction.

4.3 Experimental Results and Analysis

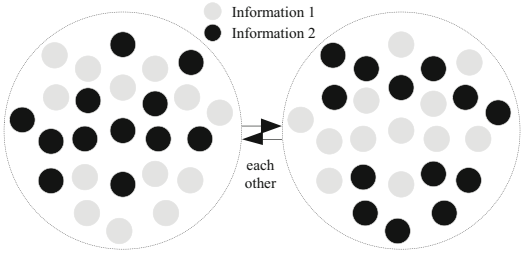
Two scenarios are set, one is that there is a large amount of untrusted information in Scenario 1, and the other is that there are information leakage points in multi-channel in Scenario 2. In these two cases, the sharing scheme based on blockchain, the sharing method based on the whole network power supply topology model and the sharing method based on differential privacy protection are respectively used to compare and analyze the effect of information interaction and sharing.

4.3.1 Analysis of Information Interaction Results

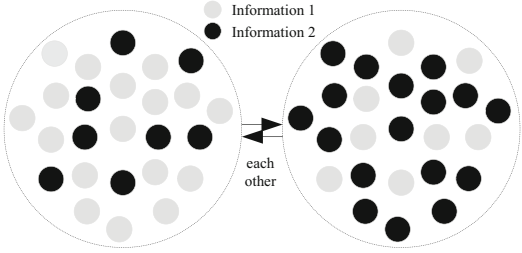
For information interaction analysis, compare the information interaction results of the three methods.

(1) Situation 1

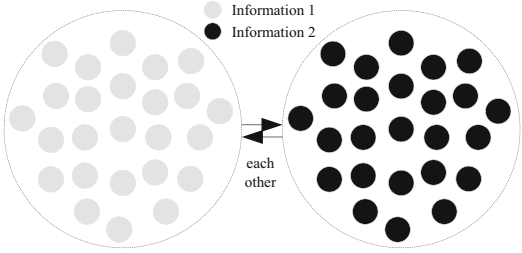
In this case, compare the information interaction of the three methods, as shown in Fig. 7.



(a) Blockchain based sharing scheme



(b) Sharing method based on whole network power supply topology model



(c) Sharing method based on differential privacy protection

Fig. 7. Information interaction of three methods in case 1

It can be seen from Fig. 7(a) and Fig. 7(b) that in an environment with a large amount of untrusted information, the two comparison methods mix the two kinds of information

together in the process of information interaction. After the interaction is completed, the two kinds of different information are not completely distinguished, and more information is lost, which cannot guarantee the integrity of the interaction information. From Fig. 7(c), it can be seen that the method proposed in this article fully distinguishes the two types of information after interacting with each other. Both types of information fully participate in the interaction process without any information loss, indicating that the information exchange effect is good and the security is high. This is because this method uses a trap gate to verify whether the digital media image information required by the information demander is consistent with the provider, and uses the Homomorphic encryption mechanism to integrate the downloaded heterogeneous information ciphertext according to the required information requirements, ensuring the integrity of the interactive information.

(2) Situation 2

In this case, compare the information interaction of the three methods, as shown in Fig. 8.

It can be seen from Fig. 8 that using the sharing scheme based on blockchain and the sharing method based on the whole network power supply topology model can not only fail to realize all information interaction, but also cause information loss; However, using the sharing method based on differential privacy protection, although individual information cannot interact, it does not affect the overall interaction effect, and the information is saved completely.

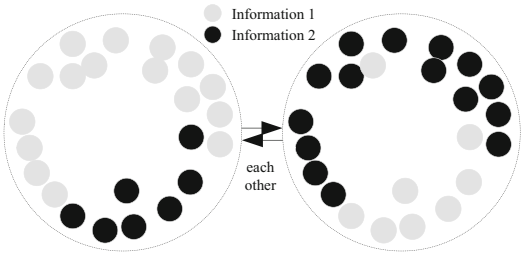
4.3.2 Analysis of Information Sharing Results

For information sharing analysis, compare the information sharing results of three methods.In the process of information sharing, if there is a large amount of untrusted information, it will cause some interference to the sharing process. In this case, compare the amount of information shared by the three methods, and the comparison results are shown in Fig. 9.

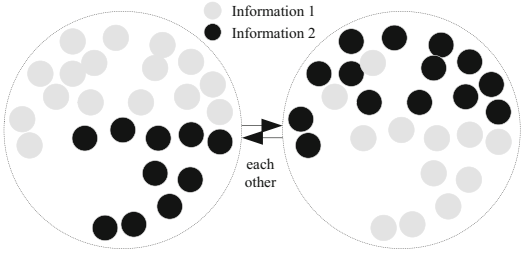
It can be seen from Fig. 9 that the maximum amount of shared information is 630 bit in case 1 and 505 bit in case 2 when using the blockchain based sharing scheme; Using the sharing method based on the whole network power supply topology model, the maximum amount of shared information in case 1 is 800 bits, and the maximum amount of shared information in case 2 is 500 bits; Using the sharing method based on differential privacy protection, the maximum amount of shared information in case 1 is 900 bits, and the maximum amount of shared information in case 2 is 780 bits. This is because the method in this article divides the encrypted information and its information into several blocks, uses proxy re encryption method to divide and re encrypt, and transmits it on the link, achieving maximum information sharing.

4.3.3 Analysis of Real-Time Results of Information Interaction and Sharing

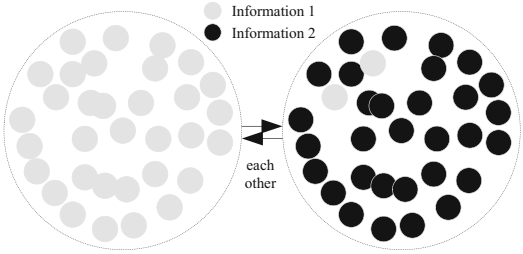
In order to verify the real-time performance of the method proposed in this article in the process of information exchange and sharing, 5000 bit digital media image information was randomly selected as sample data, and three different methods were used for



(a) Blockchain based sharing scheme



(b) Sharing method based on whole network power supply topology model

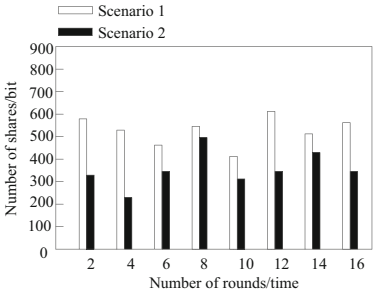


(c) Sharing method based on differential privacy protection

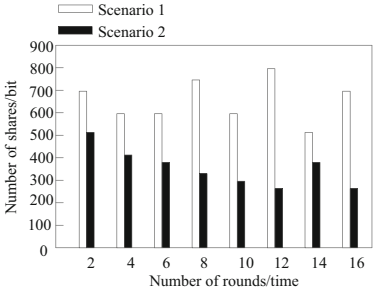
Fig. 8. Information interaction of three methods in case 2

interaction and sharing. The time spent completing interaction and sharing by different methods was counted. The less time it takes, the better the real-time performance of information exchange and sharing. The results are shown in Table 1.

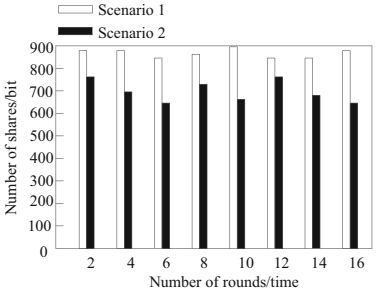
According to Table 1, it can be seen that using a blockchain based sharing scheme to complete interactive sharing between 1000 bit and 5000 bit takes 1.45 ms to 5.21 ms; The sharing method based on the entire network power supply topology model takes 1.67 ms to 5.37 ms to complete the interactive sharing of 1000 bit to 5000 bit; Using the sharing method based on Differential privacy protection to complete 1000 bit–5000 bit interactive sharing takes 0.78 ms–4.25 ms; The relatively short time consumption indicates that the information exchange and sharing method proposed in this article has good real-time performance. This is because the proposed method in this article takes computers as the



(a) Blockchain based sharing scheme



(b) Sharing method based on whole network power supply topology model



(c) Sharing method based on differential privacy protection

Fig. 9. Information sharing of three methods

core and local area networks as the main communication medium, and adopts a C/S structure to achieve interactive management of digital media image information. Each interactive node intelligently and independently obtains node information through the Internet of Things access node, and each cluster head node broadcasts information with a competitive radius as the transmission radius, saving time for information exchange and sharing.

From the above analysis results, it can be seen that the interaction effect of the research method is good, the amount of shared information is large, and it has good real-time performance.

Table 1. Time consumption/ms for interaction and sharing between different methods

Amount of information/bit	Blockchain based sharing scheme	Sharing method based on whole network power supply topology model	Sharing method based on differential privacy protection
1000	1.45	1.67	0.78
2000	2.66	2.98	1.88
3000	3.34	3.56	2.65
4000	4.08	4.32	3.48
5000	5.21	5.37	4.25

5 Conclusion

Based on the existing interactive sharing technology, an information interactive sharing method based on differential privacy protection is designed. This method combines the differential privacy protection mechanism to reduce the loss rate of information. At the same time, this method effectively prevents external attacks and ensures the security of information interaction and sharing by introducing the differential privacy protection mechanism into the process of information anonymization. The experimental results show that the proposed protection method can effectively ensure the availability of information while improving the security of information. However, due to time constraints, this article did not test the effectiveness of information interaction and sharing in the presence of noise interference. In the following research, we will focus on the impact of information noise on the sharing effect, continuously improve the design method, and provide technical support for the secure interaction and sharing of digital media image information.

References

1. Lihua, Z., Cao, Y., Ganzhe, Z., et al.: Blockchain-based secure data sharing scheme for microgrid. Comput. Eng. **48**(01), 43–50 (2022)
2. Guangyu, T., Xinkun, J.: Research and application of graphic model data sharing technology based on power supply topology model of the whole network. Electric. Measure. Instrument. **59**(06), 105–112 (2022)
3. Zhang, F., Gong, Z.: Supply chain inventory collaborative management and information sharing mechanism based on cloud computing and 5G Internet of Things. Math. Probl. Eng. **2021**, 1–12 (2021). https://doi.org/10.1155/2021/6670718
4. Kang, Y., Li, Q.: Design and implementation of data sharing traceability system based on blockchain smart contract. Sci. Program. **2021**, 1–14 (2021). https://doi.org/10.1155/2021/1455814
5. Yang, Y., Wang, B.: Information-sharing mechanism of synergistic incentive among EPC subjects of energy efficiency retrofitting of existing buildings against COVID-19. Int. J. Low-Carbon Technol. **3**, 3 (2021)
6. Gill, A.Q.: A theory of information trilogy: digital ecosystem information exchange architecture. Information (Switzerland) **12**(7), 283 (2021)

7. Cheng, T.: Information hiding mechanism based on QR code and information sharing algorithm. Int. J. Embedded Syst. **14**(1) (2021)
8. Zhu, L., Li, F.: Agricultural data sharing and sustainable development of ecosystem based on block chain. J. Clean. Product. **315**(Sep.15), 127869.1–127869.9 (2021)
9. Defranco, J.F., Ferraiolo, D.F., Kuhn, D.R., et al.: A trusted federated system to share granular data among disparate database resources. Computer **54**(3), 55–62 (2021)
10. Cheng, X., Niu, T., Wang, Y.: Information hiding mechanism based on QR code and information sharing algorithm. Int. J. Embedded Syst. **14**(1), 1–8 (2021)