




# A Copyright Protection Scheme of Visual Media in Big Data Environment

Shiqi Wang<sup>1</sup>, Jiaohua Qin<sup>1</sup>(✉), Mingfang Jiang<sup>2</sup> , and ZhiChen Gao<sup>3</sup>

<sup>1</sup> College of Computer Science and Information Technology, Central South University of Forestry and Technology, Changsha 410004, China

<sup>2</sup> Department of Information Science and Engineering, Hunan First Normal University, Changsha 410205, China

<sup>3</sup> Department of Applied Mathematics and Statistics, College of Engineering and Applied Sciences, Stony Brook University, Stony Brook, NY 11794, USA

**Abstract.** Rapid development and application of big data technology is speeding up the dissemination and utilization of visible media big data. The intensive application of visual media brings about some security issues. The building of copyright protection mechanism of visual media big data under Internet environment can provide safety guarantee for content services of visual media in a digital library, and enhance integrated serviceability of digital resources in the digital library. Firstly, sparse features are extracted by exploiting the data sparsity and perception sparsity of visual media, and then a sparse perception computing model for visual media big data is built. Then the design idea of visual media copyright encryption, copyright authentication, copyright notice, and audit trail scheme are given from the point of view of sparse feature computation of visual media. Finally, a copyright protection application scheme of visual media big data under the network environment is developed. Its application in the digital library validates the effectiveness of this copyright protection mechanism of visual media. It can safeguard the confidentiality, integrity, availability, and auditing of visual media big data in the digital library, and enhance content serviceability of visual media in the digital library under big data environment.

**Keywords:** Copyright protection · Visual media · Big data · Sparsity

## 1 Introduction

Vision is an important means for human beings to know the world, and 83% of the information received by people comes from vision. The visual media composed of image, video, digital geometry, and other media information has strong intuition and universality. Compared with other media, visual media is easier to store, communicate and transmit. With the continuous development of information technology and communication technology, the application of visual media is becoming more and more extensive, and gradually become an indispensable way of information acquisition, storage, display, and expression in people's life. In recent years, with the rapid development and

popularization of mobile Internet and wireless network, the scale of Internet users has increased dramatically. At the same time, a large amount of visual media data has been produced, which accounts for more than 60% of Internet resources. The visual media data on the Internet has a wide variety, large volume, diverse data sources, low density, and sparse value of data. Users of visual media often need to get a quick response in a short time. Visual media has the characteristics of big data and has become an important information asset in modern society [1]. The emergence of network visual media has brought new opportunities and innovation for the library service model. The content service of visual media under big data environment is becoming a key form of visual media big data application, but at the same time, the disorder, uncontrollable, content authenticity and other security issues of visual media big data are increasingly urgent [2].

Due to the increasing volume of multimedia data, it is necessary to protect this data from external threats or malicious attacks. Therefore, to protect the copyright of visual media big data in the digital library, an effective security mechanism for visual media data is much needed. Kapil et al. [3] pointed out some current issues in multimedia big data and security approaches to these issues, and also discussed multimedia big data security and privacy. It analyzed possible directions to be taken while using multimedia along with security strategies. All the time data encryption and digital watermarking technology have always been used to protect the content security and copyright ownership of digital media [4–8]. Ting et al. [9] designed a provable copyright protection scheme for digital media by employing a digital watermarking technique and unpredictable signature-seeded pseudo-random bit sequence. This scheme can resolve the ownership dispute of the digital media data even though after adversarial watermark removal attacks. Kukreja proposed a copyright protection scheme using visual cryptography which produces meaningful shares to provide better security and handles false-positive cases efficiently [10]. The meaningful ownership share is generated based on the master share, both watermarks, and cover image, and the master share is overlapped with its corresponding ownership share to reveal the watermark. Experimental results show that the new scheme has good robustness against several image processing attacks and proves the copyright of the digital images. To protect the copyright of digital images on the internet, Roy et al. [11] developed an image watermarking scheme in the spatial domain. It embeds the watermark bits by adaptive LSB replacement approach and enhances watermark transparency by using a saliency map generation algorithm. Rani and Raman designed a digital image copyright protection scheme based on chaotic encryption and visual cryptography [12]. Hossaini et al. [13] designed a blind image watermarking algorithm by combining visual cryptography with directional controllable pyramid transform to protect image copyright. The use of visual cryptography makes the watermark embedded in the original image unchanged and has good robustness. Ahuja and Bedi embed a watermark by slightly adjusting some DCT coefficients to achieve a watermarking scheme suitable for MPEG-2 video and achieve copyright protection for digital video [14]. To protect the copyright of digital art images, Kamnardsiri [15] combines discrete cosine transform and discrete wavelet transform to design a robust image watermarking algorithm. However, the irrecoverability of original art image affects people's appreciation of art and reduces the artistic value of works. Hashmi et al. further

combined visible watermarking and invisible watermarking technology to achieve real-time copyright protection of images and videos and designed a digital watermarking prototype system based on Android [16]. However, these copyright protection schemes do not take full advantage of the big data characteristics of the visual media in the network environment. They cannot provide effective copyright protection for visual media big data. While copyright protection of visual media big data is an unavoidable key technical problem in the application of visual media big data. The research results of copyright protection of visual media big data will greatly promote the innovation of library digital resource service model and achieve a healthy and sustainable visual media industry. This will certainly form new technological innovation and economic growth point. This paper aims to deeply analyze the characteristics of visual media big data and to fully exploit the value sparseness and visual perception sparseness of visual media big data, and then design new copyright protection strategies and methods of network visual media big data by exploiting sparse representation of visual media big data. Finally, we'll build a new application model of copyright protection of visual media.

## 2 Sparsity in Visual Media Data

In the network environment, the data volume of visual media is very large, data types are various, data sources are diversified, the data redundancy is very high, and the data processing speed is fast. To realize efficient real-time processing and copyright protection of visual media data in big data environment, it is necessary to fully exploit the inherent characteristics of visual media big data, especially the value sparsity and visual perception sparseness of visual media big data.

### 2.1 Value Sparsity

Low-value density is a typical feature of big data. In big data environment, visual media usually has multiple identical or similar copies. Although the volume of visual media is large, its value density is low. Visual media big data is massive and heterogeneous, and its sources are diversified, which often coexist with local density and global sparsity, large volume and low value, and availability and sparsity. Since not all the data in big data are valuable to users, some junk information even is harmful to the use of data. Effective information acquisition is like 'sourcing the sand in the waves'. How to effectively filter big data, remove the coarse and store the essence, remove the false and retain the true, and analyze and identify the sparse and useful information is the key to reflect the true value of big data.

### 2.2 Perceptual Sparsity

The sparsity of data is common in natural signals. Neurobiology studies have shown that the information processing mechanism of the human visual system is a highly complex nonlinear process, which has the characteristics of receptive field hierarchy, feedback mechanism, attention selection mechanism, feature selectivity, and so on. In the process of information processing, the human visual system does not treat information equally

but shows the characteristics of selection. On the one hand, due to the limited capacity of the brain, it is difficult to process all the information in real-time. On the other hand, because the external information is not all of the important value, the brain only needs to respond to some important information. The high selectivity of the visual system to visual stimulus features is mainly reflected in orientation/direction selectivity, spatial frequency selectivity, speed selectivity, binocular disparity selectivity, color selectivity, and so on [17]. The feature selectivity of the human visual system and the perceptual sensitivity of color, intensity, texture, and temporal-spatial correlation in natural images and videos have shown that natural images, digital video, and other visual media are sparse signals, which can be expressed linearly with a small number of non-zero sparse coefficients under a set of over-complete bases, and the sparse representation of signals can obtain a good approximation of original signal.

Visual media data accounts for the overwhelming majority of big data on the internet. Data redundancy and value sparseness bring great challenges to network bandwidth and storage space. Besides, how to quickly complete data cleaning and data purification through efficient algorithms, and acquiring valuable information is an urgent problem to be solved in the application of big data. Developing the sparse representation model of visual media big data has important theoretical value and application significance for visual media content service and big data application.

### **3 Copyright Protection Scheme of Visual Media in Big Data Environment**

Because the existing digital media copyright protection schemes do not make full use of the characteristics of visual media big data, it is difficult to provide real-time and effective copyright protection for visual media communication in big data environment. By fully exploiting the sparsity of big data of network visual media, this paper builds the application model of copyright protection of visual media in big data environment and protects the copyright of visual media big data by copyright encryption, copyright authentication, copyright notice, and violation tracking. It can provide theoretical and methodological support for the content service of visual media big data in the network environment. The visual media big data content service system is an organic system engineering that integrates the storage, analysis, utilization, and display of visual media big data. The design of the big data storage system model [18] and the OSI system of ISO (International Organization for Standardization) can provide a guide for the design of the copyright protection model integrated into the content service system of visual media big data. The ISO OSI model is divided into seven levels: the physical layer, data link layer, network layer, transport layer, session layer, presentation layer, and application layer. Therefore, according to the basic principle of the OSI reference model and the basic principle of ‘data sinking, unified processing, and service improvement’, the visual media copyright protection model in big data environment can be divided into five modules: resource layer, data analysis layer, function layer, interface layer, and presentation layer. Each module is interconnected with each other to form an organic system, as shown in Fig. 1.

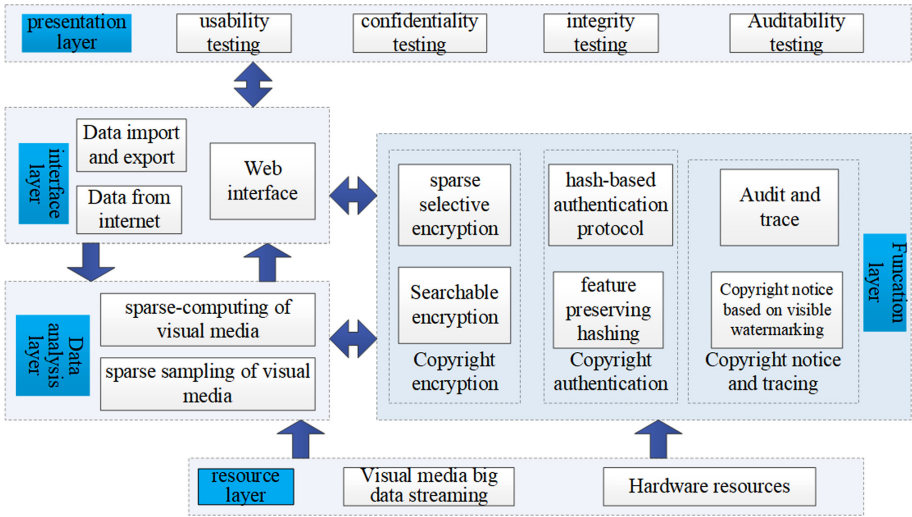


Fig. 1. Copyright protection model of visual media big data.

The basic idea of copyright protection model design of visual media big data is: starting from the sparsity of visual media big data, making full use of the value sparsity and visual sparsity of visual media big data, using sparse coding and statistical analysis to establish the sparse perception calculation model of visual media big data, take the sparse representation of visual media big data, extract the sparse features of visual media, and complete the redundancy removal Storage and data cleaning provide key technical support for real-time processing and content service of video media big data in the network environment. Through the design of visual media, big data selective encryption technology based on sparse characteristics and visual media big data searchable encryption scheme based on perceptual hash, the confidentiality, and availability of visual media are guaranteed. After that, we develop a visual media big data copyright authentication protocol based on Perceptual Hashing to maintain the content integrity of visual media big data. Through the combination of visible digital watermarking technology and robust perceptual hashing, the scheme of visual media big data copyright notice and piracy tracking is designed to ensure the audit ability of visual media content service, to realize the complete copyright protection model in the whole life cycle of visual media. The core technologies of visual media copyright protection model design in big data environment include the establishment of visual media big data perception computing model, visual media copyright encryption technology, visual media copyright authentication protocol, visual media big data copyright notice, and tracking scheme.

### 3.1 Visual Sparse Computing Model for Visual Media Big Data

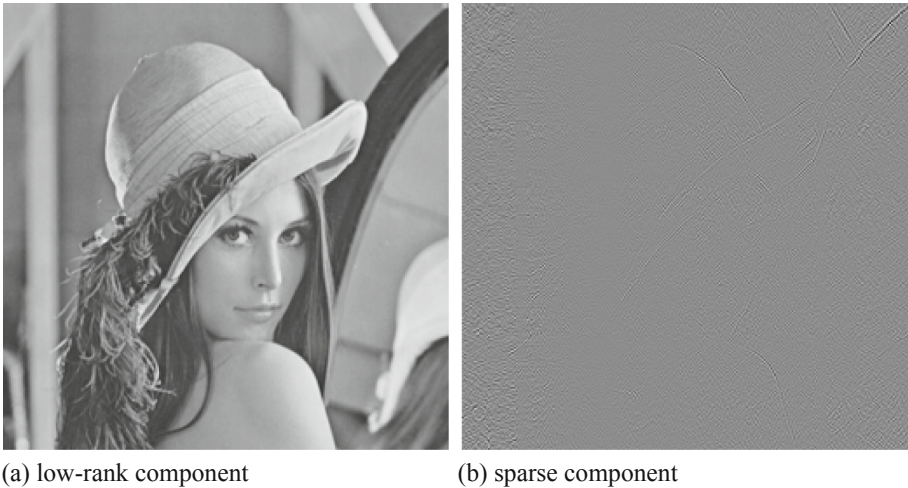
In the network environment, visual media big data has the value sparsity and visual perception sparseness. Value sparseness refers to the large data scale and high data redundancy of the visual media in big data environment. To reduce the bandwidth and storage requirements and adapt to the real-time processing environment of big data

streams, it is necessary to fully exploit the value sparsity of visual media big data to realize the sampling of large data of visual media. Taking digital image as an example, the image big data stream can be divided into fixed-size time slices, so the image big data can be expressed as a matrix, in which the image is an  $m$ -dimensional column vector, and  $n$  is the number of images in a certain time. In this way, low-rank optimization can be used to decompose the matrix  $M$  (expressed by Eq. 1), and reduce the dimension of image big data [19].

$$\begin{aligned} \min \quad & \|L\|_* + \lambda \|S\|_1 \\ \text{s.t.} \quad & L + S = M \end{aligned} \quad (1)$$

Where  $\|\cdot\|_*$  and  $\|\cdot\|_1$  represent kernel normal form and 1 normal form, respectively, which  $\lambda$  are non-negative regularization parameters.  $L$  is the low-rank component and  $S$  is the sparse component. Then the information entropy of the image can be calculated by the low-rank component  $L$ , and the sampled image (centroid media) can be determined according to the information entropy, and complete the sparse sampling of visual media

Figure 2 shows an example of low-rank decomposition. Taking the gray image ‘Lena’ as an example, the low-rank approximation and sparse component of the image matrix are illustrated in Fig. 2(a) and Fig. 2(b), respectively.



**Fig. 2.** Low-rank decomposition of Lena image.

Because of the visual sparsity of visual media, the sparse perception of centroid media is further analyzed according to the linear and nonlinear statistical characteristics of visual media, statistical characteristics in spatial and transform domain and the correlation of low dimensional and high-dimensional features. This will provide a theoretical basis for sparse sensing computing in real-time processing and copyright protection of visual media.

### 3.2 Copyright Encryption Technology for Visual Media Big Data

Encryption is an important method to protect the confidentiality of data, but for the massive heterogeneous, high redundancy visual media big data stream, the usual encryption algorithm cannot meet the real-time processing requirement in big data environment. One feasible solution to this issue is selective encryption technology where the sparsity of visual media big data will be fully exploited. The main steps of selective encryption are shown as follows.

Step1: Users send visual media streaming to remote servers.

Step2: Apply adaptive streaming sampling on visual media streaming by the use of the sparse sampling

Step3: The centroid media is selected according to the sparsity of visual media value

Step4: The low-rank component of the centroid visual media is selected to encrypt.

This selective encryption strategy for visual media big data can meet the real-time processing requirements of visual media big data.

The other scenario is privacy protection in the cloud computing environment. To maintain the security of user secret data, the visual media data must be first encrypted before uploading on the cloud server. But at the same time, people often need to retrieve the qualified visual media from the encrypted media data. To protect the privacy of the visual media data in the cloud, a privacy-preserving retrieval scheme is designed.

Step1: Apply low-rank decomposition to visual media data.

Step2: obtain the sparse representation of visual media and build a sparse computing model for visual media data.

Step3: Produce a perceptual hash of visual media.

Step4: Lossless data hiding is used to encrypt the visual media perceptual hash.

Step5: Public-key encryption is used to encrypt the keywords associated with perceptual hashes to generate keyword trapdoors.

Step6: During the user retrieval process, the server performs the retrieval according to the keyword trapdoor input

Step7: The cloud server returns the visual media ciphertext file containing the keyword corresponding to the trapdoor.

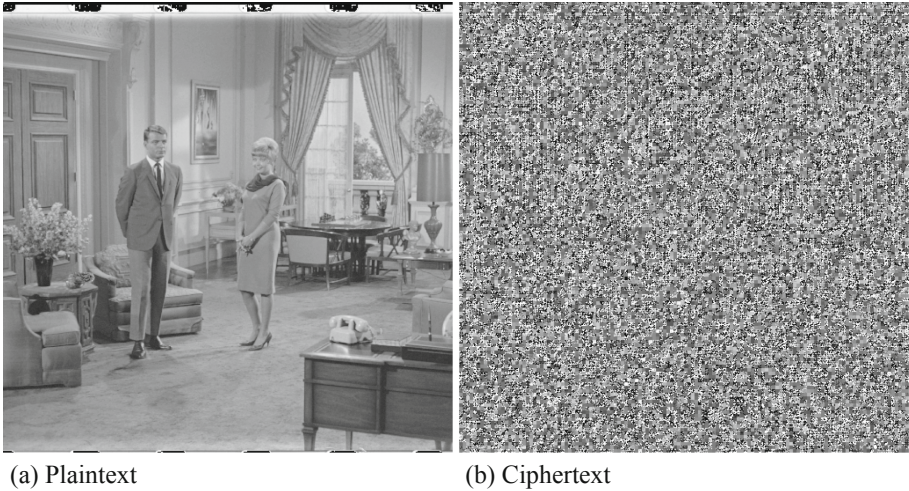
Step8: Finally, the user obtains the query results by decrypting the ciphertext of the visual media returned by the server with the user key.

An example of 'Couple' image encryption is illustrated in Fig. 3. Figure 3(a) and (b) show the plaintext and corresponding encrypted image, respectively. From Fig. 3(b), it can be found that one can hardly recognize meaningful information from the ciphertext generated by the proposed selective encryption method.

### 3.3 Copyright Authentication Protocol of Visual Media Big Data

In the network environment, the integrity authentication of visual media is very important, and the usual copyright authentication scheme based on digital watermark requires





**Fig. 3.** Selective encryption of 'Couple' image

the user end to have the function of watermark embedding and detection. However, this is not realistic in the real-time processing environment. Therefore, we design a copyright authentication protocol for visual media big data based on the perceptual hash. The detailed procedure is as follows.

Step1: Read visual media data from the cloud server.

Step2: The visual sparse computing model is used to generate perceptual hash information.

Step3: To ensure the robustness and distinction of perceptual hash sequence, the value sparseness of visual media will be fully exploited to remove redundant information. High-level semantic features of visual media can be obtained by using visual sparsity,

Step4: User sends retrieval query to the remote server.

Step5: The server extracts the visual media perceptual hash and matching it with the registered hash code in the cloud authentication center.

### 3.4 Copyright Notice and Tracking Scheme of Visual Media Big Data

Compared with encryption and digital watermarking technology, visible watermarking technology can declare copyright without watermark detection. This is a more portable and fast copyright method and is more suitable for the application of visual media content services in big data environment. To protect copyright and realize audit trail, a copyright notice and tracking scheme is designed by using adaptive visible watermarking and robust hash. The algorithm is described below

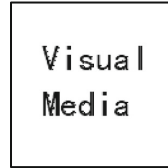
Step1: Input a binary image as the visible watermark image.

Step2: Read a gray image as the original image need to be protected.





(a) Original image (Camera)



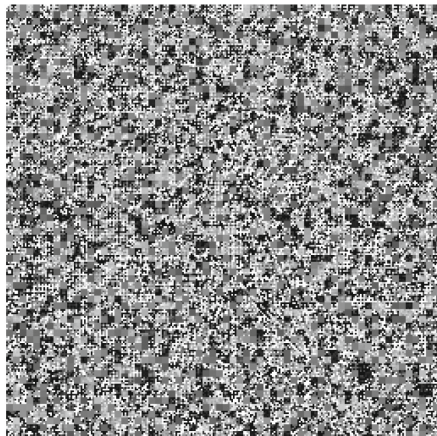
(b) Visible watermark



(c) Watermarked image



(d) Watermark removal with correct key



(e) Watermark removal with wrong key

**Fig. 4.** Visible watermark insertion and removal

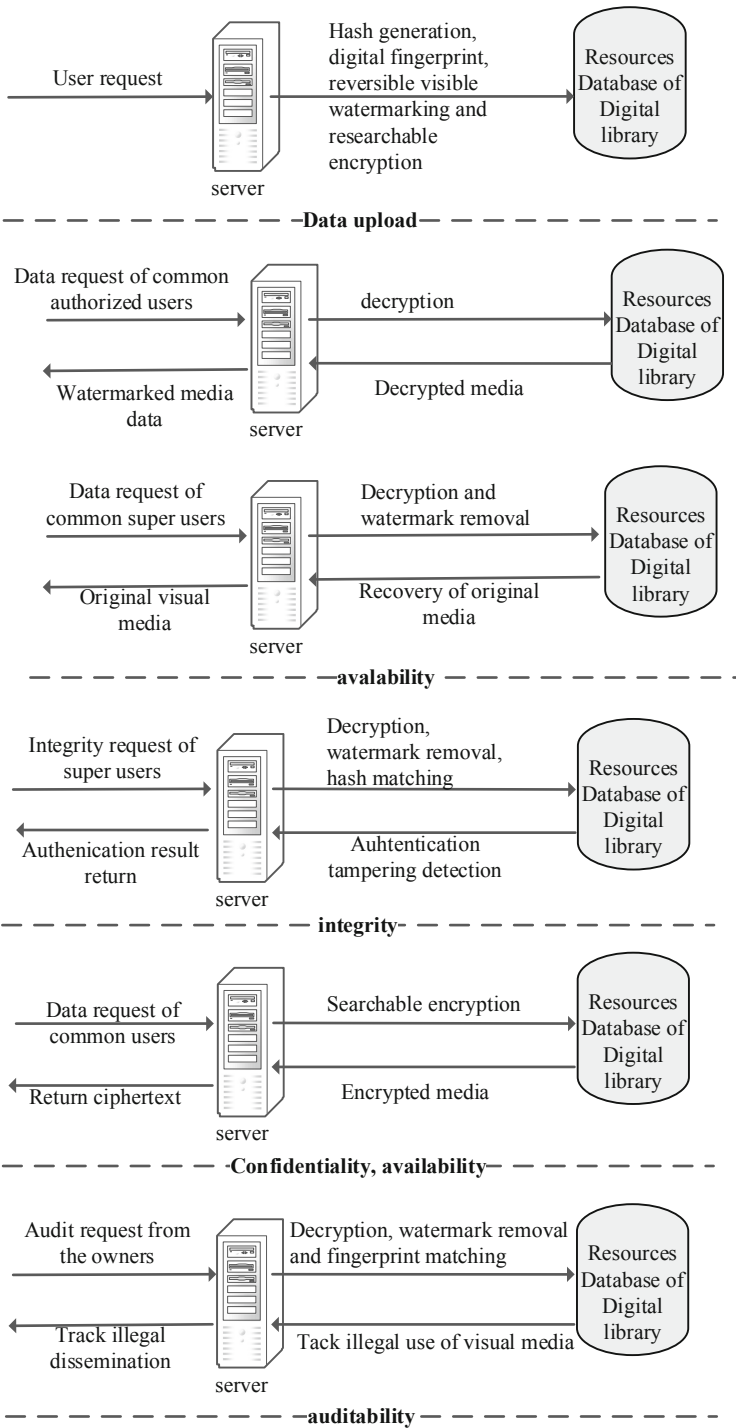


Fig. 5. An application scenario of copyright protection model for visual media in digital library

Step3: To achieve adaptive embedding of the visible watermark, the visual sparse computing model is employed to calculate the adaptive embedding factor and scale factor according to the visible watermark.

Step4: Given a user key, the server adaptively inserts the watermark signal into the original image in a visible way, and this visible embedding way can provide explicit copyright notice for the visual media without watermark detection.

Step5: Generate a robust perceptual hash of the original media data.

Step6: Catenate the perceptual and encrypted watermark signal to produce the fingerprint of the original image.

Step7: Embed the fingerprint into the original image by lossless data hiding technology.

The presented copyright notice scheme can provide high-definition visual media content services to authorized users since only users with the right key can remove the visible watermark. Moreover, the illegal propagation of authorized users will be tracked by similarity judgment of digital fingerprints. Figure 4 illustrates an example of copyright notice. One can observe that unauthorized users without the correct key cannot delete the visible watermark imposed on the watermarked image.

## 4 Application in Digital Library

Visual media is the main form of digital resources in the application of digital library, so the copyright protection of visual media content is an important part of the application of digital library, and a key step to promote the healthy development of digital library content service. This paper discusses the application of copyright protection model for visual media in digital library, as shown in Fig. 5. According to Fig. 5, it can be concluded that the proposed scheme is effective in terms of data confidentiality, integrity, availability and auditability.

## 5 Conclusion

Visual media is an important form of digital resources in the digital library. Copyright protection of big data of network visual media is an important basis for the application of visual media big data, and it is also the bottleneck of the application and promotion of content service model of the digital library. Starting from the inherent characteristics of visual media big data, and fully mining its value sparsity and visual perception sparseness, this paper designs a visual media big data copyright protection model based on sparsity, and puts forward practical ideas of visual media copyright encryption, copyright authentication, copyright notice and audit trail scheme in big data environment. Through the application practice of digital library of visual media, it is verified that the copyright protection model of visual media can effectively maintain the confidentiality, integrity, availability, and audit ability of visual media big data in the network environment. The copyright protection model can provide a security guarantee for the content service of visual media in the network environment, and promote the innovation of the content service model of the digital library.

**Acknowledgements.** This work was supported in component by the National Natural Science Foundation of China under Grant No. 61872408, the Natural Science Foundation of Hunan Province (2020JJ4238), the Social Science Fund of Hunan Province under Grant No. 16YBA102, and the Research Fund of Hunan Provincial Key Laboratory of informationization technology for basic education under Grant No. 2015TP1017.

## References

1. Singh, A., Mahapatra, S.: Network-based applications of multimedia big data computing in IoT environment. In: Tanwar, S., Tyagi, S., Kumar, N. (eds.) *Multimedia Big Data Computing for IoT Applications: Concepts, Paradigms and Solutions*, vol. 163, pp. 435–452. Springer Singapore, Singapore (2020). [https://doi.org/10.1007/978-981-13-8759-3\\_17](https://doi.org/10.1007/978-981-13-8759-3_17)
2. Ruoyu, R., Shulin, Y., Qi, Z.: Research on copyright protection of digital publishing in the era of big data. In: *Proceedings of the 2019 2nd International Conference on Information Hiding and Image Processing*, pp. 39–43. Association for Computing Machinery, London (2019)
3. Kapil, G., Ishrat, Z., Kumar, R., Agrawal, A., Khan, R.A.: Managing multimedia big data: security and privacy perspective. In: Tuba, M., Akashe, S., Joshi, A. (eds.) *ICT Systems and Sustainability*, vol. 1077, pp. 1–12. Springer Nature, Singapore (2020). [https://doi.org/10.1007/978-981-15-0936-0\\_1](https://doi.org/10.1007/978-981-15-0936-0_1)
4. Liu, Y., Peng, H., Wang, J.: Verifiable diversity ranking search over encrypted outsourced data. *Comput. Mater. Continua* **55**, 037–057 (2018)
5. Wang, B., Kong, W., Li, W., Xiong, N.N.: A dual-chaining watermark scheme for data integrity protection in internet of things. *Comput. Mater. Continua* **58**, 679–695 (2019)
6. Yang, H., Yin, J., Yang, Y.: Robust image hashing scheme based on low-rank decomposition and path integral LBP. *IEEE Access* **7**, 51656–51664 (2019)
7. Xiang, L.Y., Yang, S.H., Liu, Y.H., Li, Q., Zhu, C.Z.: Novel linguistic steganography based on character-level text generation. *Mathematics* **8**, 1558 (2020)
8. Yang, Z., Zhang, S., Hu, Y., Hu, Z., Huang, Y.: VAE-Stega: Linguistic steganography based on variational auto-encoder. *IEEE Trans. Inf. Forensics* **16**, 880–895 (2021)
9. Ting, P., Huang, S., Wu, T., Lin, H.: A provable watermark-based copyright protection scheme. In: *2015 10th Asia Joint Conference on Information Security*, pp. 124–129. IEEE, Kaohsiung (2015)
10. Kukreja, S., Kasana, G., Kasana, S.S.: Curvelet transform based robust copyright protection scheme for color images using extended visual cryptography. *Multimed. Tools Appl.* **79**, 26155–26179 (2020). <https://doi.org/10.1007/s11042-020-09130-y>
11. Sinha Roy, S., Basu, A., Chattopadhyay, A.: On the implementation of a copyright protection scheme using digital image watermarking. *Multimed. Tools Appl.* **79**, 13125–13138 (2020). <https://doi.org/10.1007/s11042-020-08652-9>
12. Rani, A., Raman, B.: An image copyright protection scheme by encrypting secret data with the host image. *Multimed. Tools Appl.* **75**(2), 1027–1042 (2014). <https://doi.org/10.1007/s11042-014-2344-0>
13. El Hossaini, A.E.A., Aroussi, M., Jamali, K., Mbarki, S., Wahbi, M.: A new robust blind copyright protection scheme based on visual cryptography and steerable pyramid. *Int. J. Netw. Secur.* **18**, 250–262 (2016)
14. Ahuja, R., Bedi, S.S.: Copyright protection using blind video watermarking algorithm based on MPEG-2 structure. In: *International Conference on Computing, Communication & Automation*, pp. 1048–1053. IEEE, Greater Noida (2015)

15. Kamnardsiri, T.: Digital art image copyright protection using combined DWT-DCT based watermarking technique. In: 1st International Conference on Digital Arts, Media and Technology (ICDAMT 2016), pp. 83–94. IEEE, Chiang Rai (2016)
16. Hashmi, M.F., Shukla, R.J., Keskar, A.G.: Real time copyright protection and implementation of image and video processing on android and embedded platforms. *Proc. Comput. Sci.* **46**, 1626–1634 (2015)
17. Mairal, J., Elad, M., Sapiro, G.: Sparse representation for color image restoration. *IEEE Trans. Image Process.* **17**, 53–69 (2007)
18. Chen, X., Wang, S., Dong, Y., Wang, X.: Big data storage architecture design in cloud computing. In: Chen, W., Yin, G., Zhao, G., Han, Q., Jing, W., Sun, G., Lu, Z. (eds.) BDTA 2015. CCIS, vol. 590, pp. 7–14. Springer, Singapore (2016). [https://doi.org/10.1007/978-981-10-0457-5\\_2](https://doi.org/10.1007/978-981-10-0457-5_2)
19. Zhou, X., Yang, C., Zhao, H., Yu, W.: Low-rank modeling and its applications in image analysis. *ACM Comput. Surv.* **47**, 1–33 (2014)