Construction of Digital Media Copyright System Based on CAD Technology Under the Background of Internet of Things+

Shi Zhang[1], Rong Zeng[2], Qing Zhou[3] and Feng Chen[4,*]

[1]School of Media and Animation, LuXun Academy of Fine Arts, Liaoning 116650, China, zhangshichenfeng@163.com
[2]School of Media and Animation, LuXun Academy of Fine Arts, Liaoning 116650, China, zengrong@lumei.edu.cn
[3]School of Environmental Art, Shanghai Vocational College of Arts and Crafts, Shanghai 201800, China, 6163110014.edu@bkkthon.ac.th
[4]School of Media and Animation, LuXun Academy of Fine Arts, Liaoning 116650, China, chenfeng@lumei.edu.cn

Corresponding author: Feng Chen, chenfeng@lumei.edu.cn

Abstract. Digital media has become a media technology with wide communication capability in the Internet. In the process of copyright protection, the traditional digital media copyright protection system. This paper analyzes the architecture, system function modules and system performance of the data encryption system with different encryption mechanisms, encryption algorithms and encryption granularity, and makes system logic structure analysis, process analysis and database logic analysis and implementation. Based on the above analysis, a concrete scheme design is made. With the rapid improvement of computer processing power, this method of increasing the key length to improve the system security becomes more and more unsafe. Secondly, once the encryption method is decrypted, the information becomes plain text completely, which has poor protection ability for digital media transmission, and often causes abnormal media content after transmission. Based on this, this paper designs a digital media copyright protection system under the background of Internet. According to the hardware structure, the key data watermark encryption module and the key data transmission protection module are designed, and the copyright security of digital media is improved by watermark programming. Through experimental analysis, under the same attack, the simulation results show that the watermark embedded in the low-frequency coefficient is slightly better than that embedded in the high-frequency coefficient, which indicates that this algorithm has certain anti-attack, stability and applicability.

Keywords: Internet, Digital Media Copyright System, Watermark, Information Hiding, Multimedia Image.
DOI: https://doi.org/10.14733/cadaps.2023.22-33

1 INTRODUCTION

In recent years, with the common development of digital technology and network technology, video, audio, image and other digital media have been rapidly popularized. In view of the current Internet environment, Athanere and Thakur [1] have tested and set up a watermark encryption module to encrypt key data in digital media. In order to ensure that the encryption effect meets the requirements of Internet transmission, the encryption process is completed in the form of layered encryption. With the promotion of network and communication technology, multimedia transaction provides many convenient conditions for the exchange and use of digital products, and further promotes the promotion and publicity of digital products. Digital products also have some shortcomings, such as being easily copied, disseminated and tampered, which bring great challenges to the publishing protection of digital products. A series of issues such as copyright protection and legal authentication of digital products have increasingly attracted people's attention. Many legitimate copyright owners dare not easily publish or publish their own works. Moreno et al. [2] believe that this has hindered the dissemination and promotion of digital products to a great extent. Assuming that the amount of encrypted image information is too large, the encryption is more difficult and the operation is more complicated. Traditional cryptography can't guarantee the absolute safety of products in terms of product security protection, thus restricting the process of informatization. Therefore, cryptography can't meet the needs of modern products. In terms of the security of digital multimedia information today, we must find a new way to solve the potential infringement problem and make up for the deficiency of cryptography.

As an important research direction of information hiding and copyright protection, digital watermarking has attracted much attention from experts and scholars. In recent years, the research on digital watermarking has gone deeper and deeper, and more and more papers have been published. However, the problems still exist. There is no uniform standard to evaluate the performance of digital watermarking algorithm reasonably and fairly, but different related standards can be used to evaluate its advantages and disadvantages to the greatest extent. The application of relevant theoretical basis needs to be further explored. It is a direct method to construct digital signature by using one-way trapdoor function. The trap information is used as the signer's private key. The signer's ownership of the private key indicates the authenticity of the signature. The visible watermark of the image can be displayed on the monitor screen. It can be an electronic stamp image or a line of explanatory text. Hwangbo and Kim [3] make visible changes to the image, which can be seen by the observer and used to announce the copyright of the image. Early picture creators often put watermarks on the edge of pictures, which made it easy for picture thieves to cut out copyright information through image editing software. In order to solve the problem of information security and copyright protection, people first think of encryption. Cryptography is one of the main traditional technologies in the field of information security, and it is also the core technology in the field of information security. The security of watermarking refers to its ability to resist malicious attacks. Because cracking the key requires some professional knowledge, for legitimate users, the purpose is not to attack the watermark maliciously. Generally speaking, in order to enhance the security of the watermarking algorithm when designing the watermarking algorithm, Garba et al. [4] make the key have enough key space to at least resist malicious exhaustive attacks. All kinds of media are transformed from traditional ways to digital ways in transmission and expression, which makes most of the cultural industries have more powerful vitality and advantages. The development of digital copyright management technology in China is basically synchronized with the international development, but this is only in the aspects of copyright protection of e-books and the construction and development of electronic libraries. Traditional anti-counterfeiting packaging of electronic audio-visual products relies on various anti-counterfeiting labels for anti-counterfeiting and anti-theft. However, this kind of protection has been completely ineffective for infringement such as copying, illegal downloading and spreading. To solve this problem, in recent years, digital media copyright protection system has been widely used to protect the content of digital media works. With the continuous upgrading of Internet technology, the copyright protection ability of this system in data transmission is gradually declining. Therefore, a digital media copyright protection system under the background of Internet is designed in this study. In this paper, understanding the essence of digital watermarking from the basic point of view is more conducive to the further research of digital watermarking. Then, digital watermarking is classified, and its common characteristics are discussed according to its different characteristics and application fields. Then, the analysis and selection of embedding domain of digital watermarking algorithm is one of the keys of digital watermarking research. According to the needs, the appropriate embedding domain can be selected, which can show the advantages and disadvantages of different embedding domains more clearly. Digital watermark works will inevitably be attacked intentionally or unintentionally in the process of transmission, copying and printing, and these attacks will affect the quality of watermark extraction. Generally, the quality of watermark algorithm is verified and judged according to the quality of extracted watermark after attack.

2 RELATEDWORK

As people's lives become digital information, digital watermarking technology has become a powerful means to maintain digital multimedia works. Digital watermarking technology can be traced back to the ancient traditional watermarking technology. Watermarking in the primitive era is a kind of information used for marking. The original watermark is used to prove the legitimacy of banknotes, stocks, stamps, certificates, documents, etc. The purpose of watermarking is that it does not affect the use of the original content, but also plays an anti-counterfeiting role. Digital watermarking technology has been attached great importance by Chen et al. [5] since it was proposed. Jain et al. [6] proposed a watermarking scheme combining micro-genetic algorithm with singular value decomposition, and used micro-genetic algorithm to optimize the watermark strength, so as to improve the robustness of the watermark and the visual quality of the watermarked image. Yu et al. [7] proposed a blind multi-functional image watermarking algorithm by combining sub block segmentation and self-embedding technology. The algorithm can effectively resist noise, filtering, clipping, compression and joint attacks, but the combination of joint attacks. Fkirin et al. [8] think that the owners of digital works embed different watermark information in each copy before the works are published, which can be used as the serial number of the works. When the work is pirated or there is a copyright dispute, the watermark signal extracted from it can be used as the basis of ownership, thus protecting the legitimate rights and interests of the owner. Alkanhel and Abdallah [9] think that digital audio watermarking technology is a kind of information hiding technology. Its basic idea is to embed secret information in digital audio through certain algorithms, so as to protect the copyright of products, prove the authenticity and reliability of products, track piracy or provide additional information of products. Keivani et al. [10] regard the watermark system as a communication channel, and the watermark data and various signal processing are compared as noise during transmission. Add the restriction of global energy at the embedded end to restrict its insensitivity. At present, there are many research results on the theoretical model of watermarking, which can be summarized into two categories: one is that from the communication point of view, watermarking is regarded as a communication mode, and the system performance can be analyzed by information theory, signal processing technology or game theory. Agarwal and Singh [11] pointed out that many universities and companies are making efforts to realize watermarking technology, and at the same time, the research on the basic theory of watermarking has been developed, and some of them have been put into use. In the design, it is necessary to consider satisfying the constraints, including fidelity, economy and robustness. Copyright protection is the earliest application of watermark, and the application also includes operation tracking, ownership verification and so on. The method of embedding information is also often used in broadcast monitoring companies. Therefore, the application scope of watermarking will also expand with the gradual development of watermarking technology. According to the related literature, the single digital watermark copyright authentication can no longer meet people's needs, so it is very urgent to establish an online digital watermark copyright protection system. Aiming at the current situation and the defects of existing products, combined with the rapid development of Internet technology, this paper proposes an online authentication system for digital media copyright. The owner of multimedia works generates a watermark with a key and embeds it in multimedia data. Then his watermark version of multimedia works can be publicly released.

3 DESIGN OF DIGITAL MEDIA COPYRIGHT SYSTEM

3.1 Hardware Design of Digital Media Copyright Protection System under the Background of Internet

Frequency sensitivity is a characteristic that we often consider when embedding watermarks. It reveals the sensitivity of human eyes to sine wave stimulation with different frequencies, which indicates that human eyes are much more sensitive to the changes in low frequency region than those in high frequency region. We can apply this feature to our image watermarking system, because the first problem to be solved before embedding the watermark is to determine the embedding area. After knowing the frequency sensitivity of human beings, we will know which frequency band to embed the watermark in. For example, human beings are sensitive to the change of low frequency band, but insensitive to the change of high frequency band. If invisibility and robustness are considered comprehensively, embedding the watermark into the middle frequency band of the image will get a better effect. In the audio feature value extraction part, feature value information is extracted to reflect. In order to improve the effectiveness and attack resistance of the scheme. In this design, in order to improve the adaptability of the digital media copyright protection system to the Internet, the hardware part of the system is optimized, and the optimized hardware frame structure is shown in Figure 1.

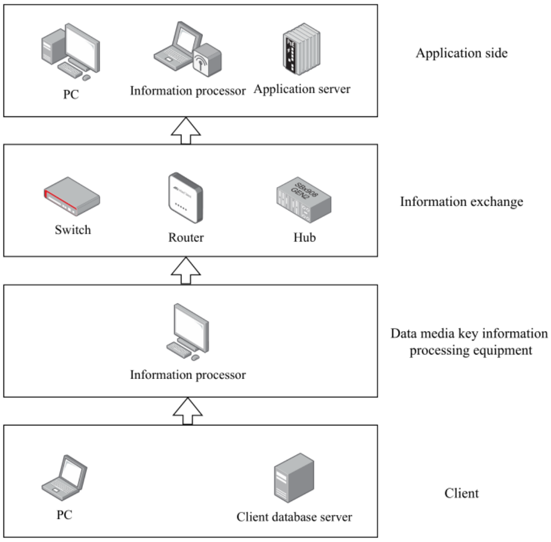

Figure 1: Design framework of digital media copyright protection system.

According to the above framework, the system hardware is selected and detailed. In this design, the core processor and key data collector of the system are reset. The core processor is the core part of the whole system. It is not only the general control end of the Internet, but also responsible for capturing the key information of digital media and realizing data transmission. Therefore, many aspects need to be considered in the selection of the core processor. To ensure the feasibility of this chip in system operation, the reset circuit is designed. In the design of this circuit, a delay capacitor is added, and a resistor of no less than 2000 ohms is connected in series in the circuit to improve the reliability of the circuit and reduce the interference of voltage on the circuit. In view of the current Internet environment, this design system tests and sets a watermark encryption module to encrypt key data in digital media. In order to ensure that the encryption effect meets the requirements of Internet transmission, the encryption process is completed in the form of layered encryption, and the expression of watermark strength factor can be obtained by derivation as shown in (1).

$$F=\sqrt[3.5]{\sum_{i,k}\left(\frac{S_2(i,k)-S_1(i,k)}{W(i,k)}\right)} \tag{1}$$

The encryption function is substituted into the watermark strength factor expression and encrypted, as shown in formula (2).

$$F=\alpha W_{wat}(S_2,S_1) \tag{2}$$

The watermark encryption process of digital media key data is shown in formula (3).

$$A_{i,j}^{CAD}A(m,n)\cdot(1+\alpha)(1+NVF(i,j)) \tag{3}$$

Assuming that the Cartesian coordinate system is the origin coordinate, transform any point in the Cartesian coordinate system into the polar coordinate system to obtain the polar coordinate. The change formulas are shown in (4) and (5).

$$r=\sqrt{(x-x_0)^2+(y-y_0)^2} \tag{4}$$

$$\theta=\tan\frac{x-x_0}{y-y_0} \tag{5}$$

To characterize the properties of wavelet packet coefficients, we must first define the cost function of a sequence, and then find the basis that minimizes the cost function among all wavelet packet bases in the wavelet library. For a given vector, the minimum cost is the most effective representation, and this basis is called the optimal basis. Commonly used cost functions are shown in (6) and (7).

$$M(u)=\sum_{k\in Z}|u_k|^2\log|u_k| \tag{6}$$

$$M(c)=\sum_{k\in Z}\log|s_k|^2 \tag{7}$$

With the above cost function, the wavelet packet sequence that minimizes the information cost function can be obtained, and the optimal basis can be obtained. Wave transform can not only analyze frequency, but also deal with abrupt signals and non-stationary signals, which Fourier analysis can't do. The basic idea of wavelet transform comes from classical harmonic analysis, and its appearance has brought revolutionary influence to the research of digital media copyright. Digital media images are decomposed by wavelet, and the first-order decomposition can get 10 frequency bands, which are low frequency, vertical, horizontal and diagonal. The second-order decomposition decomposes the low frequency into frequency bands, as shown in Figure 2.

After layer wavelet transform, most of the energy of digital media is gathered. Other parts reflect the details and texture information of the digital media. The watermark embedded in these parts is easily attacked and loses its function, so it is often embedded in. Only when embedding the watermark in this part, the watermark capacity should be considered, otherwise it will affect the quality of the original digital media. Discarding some values with small amplitude in the transformation coefficient matrix can reduce the calculation dimension and improve the operation speed.

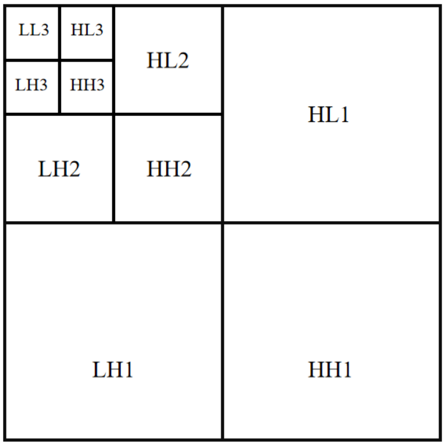

Figure 2: Schematic diagram of three-level wavelet decomposition.

Watermark embedding in spatial domain is often poor in robustness and easy to lose, while in transform domain, the watermark is embedded in transform domain first, and then transformed inversely, so that the watermark can be distributed to all pixels and has better robustness. In the above digital media feature selection process, this paper selects 32, 16,15,10,4 as the dimensions to be selected for feature analysis, and calculates the proportion of unchanged symbols in their respective coefficient matrices, as shown in Figure 3.

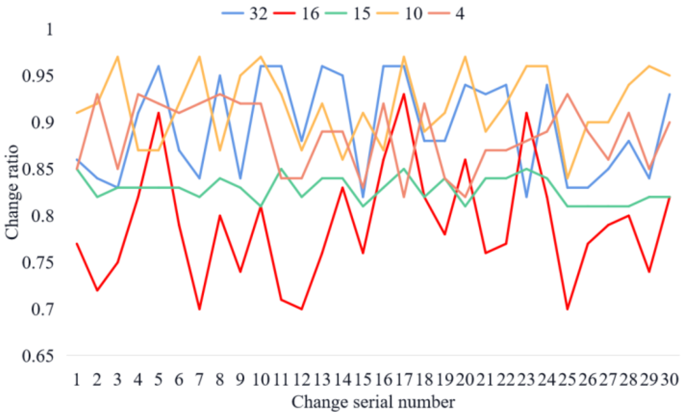

Figure 3: Conforms to the change ratio.

It can be seen from the Fig that different dimensions selected will have a certain impact on the results, but the impact is not significant, and the symbols of each group of dimension matrix values basically remain unchanged. The evaluation of watermarking system or scheme is multifaceted, which requires not only the evaluation of robustness, but also the subjective or quantitative evaluation of distortion caused by watermarking. Generally speaking, there is a contradiction between robustness and visual invisibility. Robustness is related to the amount of embedded data, watermark embedding strength and other factors. The more information to be embedded, the higher the robustness of the watermark, which in turn increases the perceptibility of the watermark. The evaluation of watermarking algorithms can't only be based on whether people can distinguish it with naked eyes, but also a variety of objective evaluation criteria should be adopted to make a unified comparison of watermarking algorithms. In this case, the measurement of quantization distortion is more effective, and the comparison between different methods tends to be reasonable, because the results do not depend on subjective evaluation.

3.2 Digital Watermarking and Embedding

The system mainly consists of two parts: watermark production and embedding and watermark extraction or detection, which constitute the core of digital watermarking system. Pseudo-random number generators are usually used to generate watermarks. They are usually based on the spread spectrum principle in communication, that is, digital watermarking products are defined as channels, digital watermarking is defined as signals transmitted in channels, and various attacks on watermarks are defined as noise in channels. There are two ways to judge watermarks, namely, detection and extraction. Meaningless watermarks are generally detected and meaningful watermarks are generally extracted. At present, most embedded watermarks.

Information is a meaningful watermark. The main factors affecting robustness are as follows. Watermark information embedded in digital media, watermark embedding strength, size and characteristics of digital media, embedding position, etc. The embedded information is an important parameter, which directly affects the robustness of digital media. The more embedded information, the worse the robustness of digital media watermarking. Secondly, to increase the robustness, it is necessary to increase the intensity of watermark embedding, which will correspondingly increase the invisibility of watermark. The size of digital media has a direct impact on the robustness of digital media embedded with watermark. Considering these factors, in order to get proper benchmark and performance evaluation, watermark embedding methods must be tested on different data sets. In addition, in order to obtain statistically valid results, many different keys and various watermarks must be used to evaluate these methods. The amount of embedded information is usually certain and depends on the specific application. If we want to compare the watermark embedding methods, we must ensure that all the methods to be investigated have the same amount of embedded information.

Usually, in order to have better robustness of the watermark image, a larger quantization step should be selected. However, a larger quantization step will lead to the degradation of the visual quality of the image. Therefore, the selection of quantization step size needs to weigh the invisibility and robustness of watermark. The quantization step size is 25 for the watermarking algorithm in Krawtchouk transform domain and 40 for the watermarking algorithm in FrKT domain, respectively, to test the embedding change of the watermark, as shown in Figure 4.

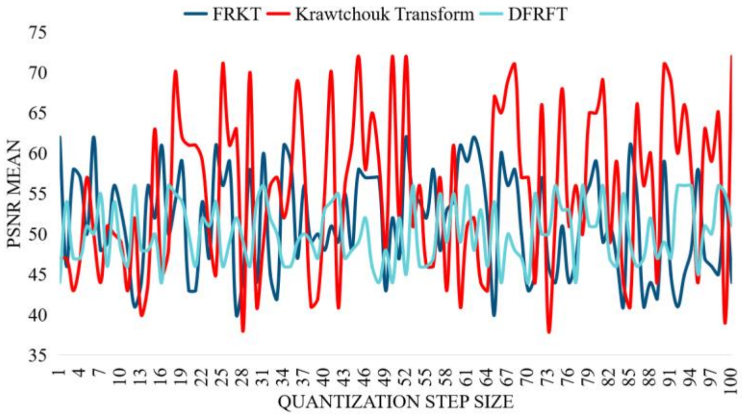

Figure 4: Changes of average value with quantization step size.

In this experiment, each binary image was combined with 15 original color images to generate zero watermark, and a total of 105 experimental combinations were generated. The transparency, security and robustness of the watermarking system are tested, and the normalized correlation coefficient, signal-to-noise ratio, mean square deviation and peak signal-to-noise ratio are used to objectively and quantitatively evaluate the performance of the watermarking system. The experimental results show that this watermarking system is robust to various attacks. Common image processing attacks are carried out on each combined protected image, and watermarks are extracted to analyze the robustness of the algorithm. The results are shown in Table 1.

Type of attack	Chang method	Rawat method	Crown method
Median filter 3*3	0.0482	0.0515	0.0029
Median filter 5*5	0.0211	0.0153	0.0221
Median filter 7*7	0.0249	0.0228	0.0293
Mean filter 3*3	0.0239	0.0174	0.0154
Mean filter 5*5	0.0346	0.0248	0.0331
Mean filter 7*7	0.0071	0.0038	0.0421

Table 1: Comparison of BER values under different attack types.

Although the required independent observation signals can be obtained by segmentation, after the image is segmented, the similarity between each block and the image itself is lost, and the extracted features can't reflect the overall properties of a specific image well. In order to solve this problem, four sub-images of the original image can be obtained by extraction, and these sub-images can be treated as observation signals for independent component analysis. Then the extracted images are all similar to the original images, so that the obtained features can better reflect the overall properties of the images.

Through the experiment, we can easily find that the original image can be obtained after a certain number of image transformations, and the transformation periods of various orders are shown in Table 2.

Order	2	7	9	11	31	41	49	61	101
Cycle	4	13	7	31	61	31	13	61	151

Table 2: Period of 2D Arnold transformation.

In the process of practical research and experiment, it can be concluded that after the images are scrambled for different times, the image rendering process is completely different. With the increase of scrambling times, the image becomes more and more messy at first, and then becomes clearer and clearer. When the scrambling period is reached, the original image will be found, which is an advantage of scrambling transformation, showing periodicity. This feature is applied to our image watermarking system, because the first problem to be solved before embedding the watermark is to determine the embedding area. After knowing the frequency sensitivity of human beings, we will know which frequency band to embed the watermark in. Combining with the feature point detection method, the local watermark of the image is designed to solve the problem of robustness of the watermarked image against translation attack, and a limited number of fractional orders are selected for comparison. It is difficult to give the optimal fractional order by manually selecting the fractional order. The experimental results are shown in Figure 5 and Figure 6.

Component-based design simplifies the maintenance of application programs. As components can be updated and replaced independently, new functions can be easily added by updating specific components in the application. In this method, the information representing different authors is mixed by linear mixing to generate the watermark signal to be embedded. The embedding process of watermark is completed by using linear mixed model in wavelet domain. In the process of extracting watermark signal, blind extraction of watermark signal is realized by means of blind source separation technology. Compared with other multi-watermarking methods, this method is simpler and requires less computation. According to the anti-attack ability, it can be divided into two types: robust watermark and fragile watermark. Robust watermark has strong resistance to common image processing operations, and even if the image has been damaged to a certain extent, it can extract watermark information, which is mainly used to identify copyright information in digital works. It requires that the embedded watermark can withstand various common attacks. Fragile watermarks can be damaged by image processing or other attacks. Fragile watermarks are sensitive to signal processing. According to the state of fragile watermarks, it can be judged whether the data has been tampered with. According to the division of watermark embedding domain, image watermarking can be divided into spatial domain and frequency domain. Watermarking in spatial domain is realized by modifying the intensity value or gray value of image pixels. This method does not need to transform the original image, and directly superimposes the watermark information on the signal space, which is simple in calculation and high in efficiency. However, due to the compromise between invisibility and robustness of the watermark, the range of selectable attributes is small, and the generated watermark has local characteristics, so it is difficult to resist the attack of common image processing and the influence of noise interference, and its robustness is poor.

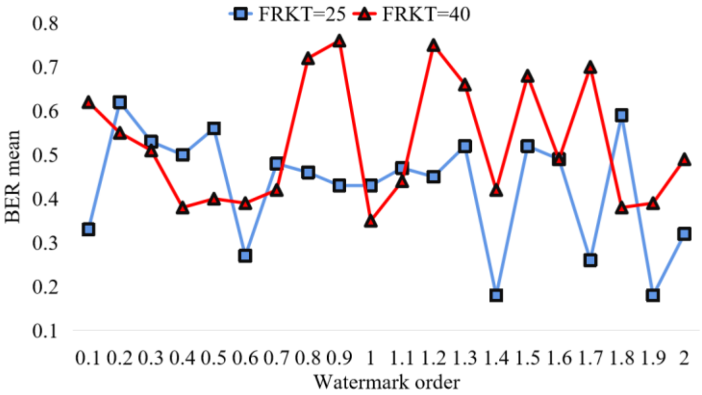

Figure 5: Different FRKT orders in watermark.

In the process of watermark embedding, because the watermark signal is embedded into the host signal after linear mixing of wavelet coefficients, after a lot of experiments, local tampering in time domain has almost no influence on the watermark information implied in the secret signal. The time domain waveforms of the host signal and the secret signal are shown in Figure 7.

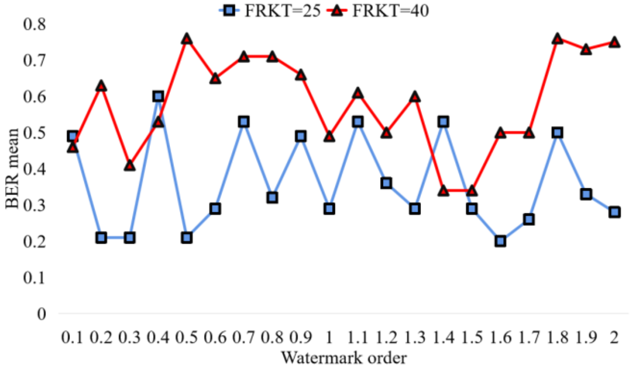

Figure 6: Different FRKT orders in the same watermark.

As can be seen from the Fig, even if there is a slight error in the key, the watermark signal cannot be detected correctly, so the security of this method can be guaranteed by the key information. The algorithm in this paper has good invisibility. After embedding the watermark, there is no audio-visual difference between the watermarked audio and the original audio. The algorithm is also robust, and most of the attacks used in simulation are strong. However, the similarity between the extracted watermark and the original watermark is high. At the same time, the watermark is embedded in the high frequency coefficients of wavelet transform by a similar method. Under the same attack, the simulation results show that the watermark embedded in the low frequency coefficient is slightly better than that embedded in the high frequency coefficient, which indicates that this algorithm has certain anti-attack, stability and applicability.

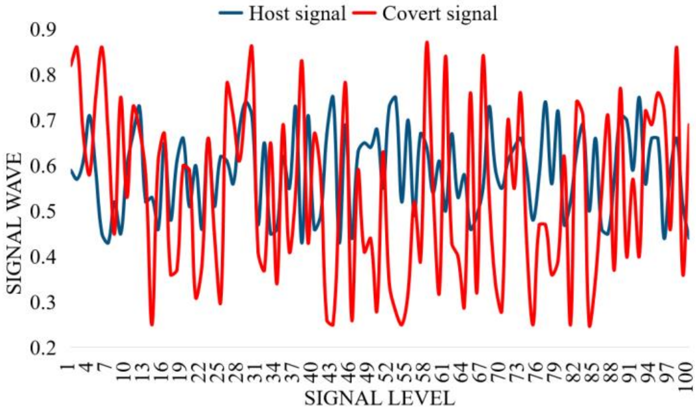

Figure 7: Waveform diagram of digital media copyright signal.

4 CONCLUSIONS

With the advent of the information age, the rapid development of computer network technology, multimedia information technology and related disciplines, and the rapid spread of digital products, digital information is becoming more and more important in modern life. However, with the spread of digital products, the resulting infringement problem has become increasingly serious. How to effectively protect the legitimate rights and interests of the copyright owners of digital products has become an urgent problem of digital information security. When faced with such a situation, digital watermarking technology appears immediately, and becomes a research hotspot to solve the problem of multimedia copyright protection.

In this paper, a group of robust features of color digital media are constructed. Because the low-frequency coefficients of digital media wavelet transform are robust to digital media noise and compression, we choose the low-frequency coefficients of color digital media after wavelet transform as the construction basis. After dividing the wavelet coefficients into blocks, each color digital media block is transformed into a two-dimensional matrix. Next, the two-dimensional matrix generated by each block is decomposed by singular value, and its first singular value is selected as the robust feature of digital media and binarized. Then, combined with the visual encryption algorithm, the binarized features of digital media are used as a share of the watermark, and then the second share is generated by combining the watermark, which can be stored in an authentication institution for digital media authentication. Finally, compared with the existing zero-watermark algorithm, the proposed algorithm has higher robustness. Independent modules greatly increase the possibility of generalization of system modules, further promote the reuse of modules, reduce redundant codes, make the system clean and agile, and facilitate future expansion. Design an independent business process through detailed analysis of requirements and functional modules. The business process of this system is carried out strictly according to the actual process, and the logic relationship in the process is judged, so it is practical.

Shi Zhang, https://orcid.org/0000-0002-8608-3956
Rong Zeng, https://orcid.org/0000-0002-0123-4066
Qing Zhou, https://orcid.org/0000-0001-6354-5153
Feng Chen, https://orcid.org/0000-0001-9412-2604

References

[1] Athanere, S.; Thakur, R.: Blockchain based hierarchical semi-decentralized approach using IPFS for secure and efficient data sharing, Journal of King Saud University-Computer and Information Sciences, 34(4), 2022, 1523-1534. https://doi.org/10.1016/j.jksuci.2022.01.019

[2] Moreno, X.-C.; Al-Kadhimi, S.; Alvelid, J.; Bodén, A.; Testa, I.: Imswitch: generalizing microscope control in python, Journal of Open Source Software, 6(64), 2021, 3394. https://doi.org/10. 21105 / joss. 03394

[3] Hwangbo, H.; Kim, J.-K.: Development of Security Anomaly Detection Algorithms using Machine Learning, The Journal of Society for e-Business Studies, 27(1), 2022, 1-13. https://doi.org/10.7838/jsebs.2022.27.1.001

[4] Garba, A.; Dwivedi, A.-D.; Kamal, M.; Srivastava, G.; Tariq, M.; Hasan, M.-A.; Chen, Z.: A digital rights management system based on a scalable blockchai, Peer-to-Peer Networking and Applications, 14(5), 2021, 2665-2680. https://doi.org/10.1007/s12083-021-01098-2

[5] Chen, S.; Su, Q.; Wang, H.; Wang, G.: A high-efficiency blind watermarking algorithm for double color image using Walsh Hadamard transform, The Visual Computer, 38(6), 2022, 2189-2205. https://doi.org/10.1007/s00371-021-02277-1

[6] Jain, J.; Jain, A.; Srivastava, S.-K.; Verma, C.; Raboaca, M.-S.; Illés, Z.: Improved Security of E-Healthcare Images Using Hybridized Robust Zero-Watermarking and Hyper-Chaotic System along with RSA, Mathematics, 10(7), 2022, 1071. https://doi.org/10.3390/math10071071

[7] Yu, X.; Wang, C.; Zhou, X.: Review on Semi-Fragile Watermarking Algorithms for Content Authentication of Digital Images, Future Internet, 9(4), 2017, 56-56. https://doi.org/info:doi/10.3390/fi9040056

[8] Fkirin, A.; Attiya, G.; El-Sayed, A.; Shouman, M.-A.: Copyright protection of deep neural network models using digital watermarking: a comparative study, Multimedia Tools and Applications, 81(11), 2022, 15961-15975. https://doi.org/10.1007/s11042-022-12566-z

[9] Alkanhel, R.; Abdallah, H.-A.: Securing Color Video When Transmitting through Communication Channels Using DT-CWT-Based Watermarking, Electronics, 11(12), 2022, 1849. https://doi.org/10.3390/electronics11121849

[10] Keivani, M.: Sazdar, A.-M.: Mazloum, J.: Application of Empirical Wavelet Transform in Digital Image Watermarking, Traitement du Signal, 37(5), 2020, 839-845. https://doi.org/10.18280/ts.370517

[11] Agarwal, N.: Singh, P.-K.: Discrete cosine transforms and genetic algorithm based watermarking method for robustness and imperceptibility of color images for intelligent multimedia applications, Multimedia Tools and Applications, 81(14), 2022, 19751-19777. https://doi.org/10.1007/s11042-021-11337-6