Le Danh Tai
Ta Minh Thanh

A PROPOSAL OF DIGITAL CONTENTS COPYRIGHT PROTECTION BY USING BLOCKMARKING TECHNIQUE

Abstract *Recently, Blockmarking technique [15] is proposed for a new hybrid model based on the combination of blockchain and watermarking method. In this model, it not only achieves the goal of image copyright protection but also stores the image into the blockchain network such as IPFS system. In this paper, we propose a new DRM system by inheriting the idea of Blockmarking. The copyright contents can be distributed via IPFS blockchain, then be restored by using the reconstruction license for each legal user. Also, in our method, based on the reconstruction licenses, the distributed contents can be reconstructed from IPFS with various watermarking patterns. It helps us can manage the legal users and trace the traitor if a dispute occurs. The experimental results show that our method successfully achieved the purpose of digital copyright protection.*

Keywords InterPlanetary File System (IPFS), copyrights protection, Distributed Watermarking Method, Digital Rights Management (DRM)

Citation Computer Science 25(4) 2024: 621–636

1. Introduction

1.1. Overview

The raging of piracy has brought immeasurable losses to content creators, especially prominent in areas such as news, design, photography and e-commerce. However, because the digital content itself is difficult to identify with embezzlement and the legal process takes a long time, victims often choose the actual fee of the violation, which also makes to the increase copyright infringement.

In recent years, with increasing awareness of copyright protection at national, social and individual levels, the protection of copyright such as videos, music and literature has taken a big step forward. Additionally, the content creators also create the non-fungible tokens (NFT) by minting their digital contents via blockchain marketplace. In order to create an NFT art, a creator needs to upload their digital content to a marketplace that supports NFTs, such as OpenSea[1]. The platform will then mint the content into an NFT and assign it a unique identifier and metadata. The creator can then set the price and terms of sale for their NFT, such as a fixed price, an auction, or a royalty fee. The platform will also charge a fee for the creation and listing of the NFT. To buy an NFT, a buyer needs to have a digital wallet that supports NFTs, such as MetaMask[2]. Such NFTs are very valuable. However, due to some characteristics of the digital contents itself, the process of copyright protection has progressed slowly. The content of the digital contents is indispensable, the value of the digital contents is increasingly enhanced, and the copyright protection of the digital contents becomes indispensable.

To address such digital content infringement on the market today, the researchers hope to solve the dilemma of rights protection through technology, to be able to trace the original author by how to label and engrave their own work imprints. Blind watermark is a type of digital watermarking technology, which can hide digital information in an digital contents. The processed image appears to be unchanged, but in fact the image already has a unique identifier. Regardless of whether it is cut, pasted, rotated, zoomed or added text or filters, the content of the watermark will be affected to some extent. This allows copyright protection and tracking without damaging the original work and going unnoticed.

The most robust watermarking techniques focused on copyright protection are frequency domain based watermarking methods. The frequency domain can be applied on the watermarking techniques by single frequency domain or hybrid frequency domain. Such combination of frequency domain can define the robustness of watermarking methods [5,11,13]. The disadvantage of this watermarking algorithm is that it is not possible to embed one bit of watermark in all blocks, resulting in low capacity. To improve payload capacity, all blocks are used for embedding purposes in [10]. The

[1] https://opensea.io/

[2] https://metamask.io/

robustness of the proposed scheme was tested against various single and combined attacks, and a good quality watermark was extracted even after multiple simultaneous attacks on the system.

In order to get the balance of imperceptibility and the robustness for frequency domain watermarking methods, Thanh *et al.* had proposed the q-logarithm frequency domain (q-LFD) for image watermarking. They have applied the q-LFD for single frequency domain in order to create a new frequency domain such as q-DCT [23], q-DWT [20], and q-SVD [21]. It is clear that depends on the values of q parameter, they could provide a new frequency domain for robustness and high quality of image watermarking methods. However, to find out the optimal values of q parameter, it's algorithm is quite complicated for analysis.

Nowadays, the non-fungible tokens (NFT) marketplaces cannot handle the challenges related to NFT ownership claims[3], illegal redistribution, and data ownership traceability[4]. The creation of NFTs has specifically led to a lucrative market for verifying ownership of unique digital assets, including digital art products. However, this NFT trading market also raises risks such as fraud, stolen works, authenticity and copyright issues. Illegal traders exploit the market by trading unauthorized copies of digital objects as NFTs.

To overcome these problems, the watermarking methods [18] can combine with blockchain technique [19] to make the efficient NFT marketplace. Saeed *et al.* [12] proposed a marketplace based on watermarking and NFT technologies. In their system, the ownership data is stored as an NFT, then the copyright information is embedded into the content of the NFT. The watermarked information can be extracted from the watermarked NFT to identify the owner and the buyer of the traded data. Dalla *et al.* [4] also proposed the digital watermarking as a means to establish the authenticity of NFTs and showed the potential of NFTs ownership protection technique. Sarad Venugopalan and Heiko Aydt [25] proposed a solution that puts control back in the hands of information owners by storing encrypted content on a data warehouse and providing additional security against hacks and zero day exploits. Content on their data warehouse is never decrypted or returned to its owner for decryption during rekeying. Their solution seems to be good for proving the ownership of NFT, however, such system requires the complicated infrastructure.

With another appraorches, Tai *et al.* [15] had proposed the Blockmarking technique to embed the various watermarks information into many distributed patches of NFT stored in IPFS. They proposed the idea to extend the model of DRM system by using the distributed feature of blockchain network. Tai *et al.* [16] also extend such model on distributing NFT image system combined with watermarking technique. They could prove that their hybrid model based on watermarking algorithm with blockchain technology can work with the copyright protection of NFT image.

[3] https://fromlight2art.com/how-to-protect-your-nfts-for-artists/

[4] https://www.imatag.com/blog/digital-art-and-nft-how-to-solve-the-trust-issue

To build a transparent digital product copyright protection system, Digital Rights Management (DRM) solution for NFT marketplace is proposed to effectively manage the processing flow of digital products from manufacturers to users. The DRM solution allows producers to control what users can do with digital content such as photos, videos, logos, audio files and so on. DRM is the management of legal access to digital content. It also can restrict the use of proprietary hardware and copyrighted works. DRM technologies govern the use, modification and distribution of copyrighted digital contents. Therefore, such DRM technologies include licensing agreements and encryption.

1.2. Classification of DRM system

Based on technical solutions to classify DRM solutions, we can divide DRM into several solutions as follows:

- **Provider-based DRM system (PDRM):** focuses on the protecting of contents provider's copyright [1, 8, 24]. It is also called provider-centric DRM solutions. That means PDRM proves the copyrights of producers when he/she claims a right to his digital contents. Therefore, even if the digital contents are sold for end users, the copyright of producers/authors is still remained.
- **User-based DRM system (UDRM):** is the users-centric DRM solution. It protects the copyrights of end users after he/she bought the digital contents. UDRM is used to implement the system for embeding the copright information of legal users into the digital contents [6, 7, 17, 18]. Therefore, UDRM requires the user's information when he/she registers to buy the digital contents. The watermarked contents from UDRM may be processed under various attacks such as blur, noise addition, soften, sharpen, JPEG conversion, Rotation, Scaling, and Translation (RST) and so on. Also, the extracted watermark is required to be clear in order to judge the rights of users.
- **Hybrid model DRM system (HDRM):** is used to protect both copyrights of providers and legal users [15, 26]. In this case, HDRM requires the watermark W from the provider P and the watermark W_u from the user U. This solution is potential for DRM because of adaptation with new technology likes AI and blockchain techniques.

Three models of DRM above can be applied on real applications. However, each has several problems. Although HDRM can improve the problems of PDRM and UDRM, it is still dependent to authority judgement with saving of copyrights information in their central database. Also, only authority judgement can judge the traitors or copyright of providers/users. If such DRM systems apply on blockchain for protecting the NFT assets, the NFT marketplace can be efficiently managed. New method of the design for embedding the watermark into digital contents before minting its NFT is required. Therefore, we need to improve such problem by employing the advantages of blockchain technology combined with watermarking method.

1.3. Our contributions

Previous DRM solutions have been effectively applied in copyright management system. DRM system consists of three components such as watermarking processing, license management, and legitimate user tracking. However, that DRM system belongs to a third party, so the above three components can be controlled by the third party. Especially, recent DRM systems are hard to apply on NFT marketplace for NFT copyright protection.

In order to solve such issue, we propose a new DRM system based on redundant digital contents distributed through a blockchain network by using many patches from digital contents. We also propose a systematic information restructuring method for content distribution and verify legitimate users. Our method can manage multiple digital patches of digital images from the blockchain network. The digital content is firstly split to get multiple patches. Then, they are saved to the InterPlanetary File System (IPFS). We also prepare some watermark patterns to embed in each digital patch before saving them on IPFS.

We emphasize the following contributions in our paper:

1. *Distributed digital contents management instead of central management*
   Our system proposes a new method for digital contents management. The copyrighted digital content is divided into many patches, called NFT assets. Such patches can be overlapped or non-overlapped. Afterwards, all patches are uploaded on IPFS system. IPFS is a modular suite of protocols purpose built for the organization and movement of content-addressed data. Therefore, the saving of digital contents does not depend on the database of third party. In order to access the distributed patches (NFTs), we can manage the content identifier, or CIDs, is a label used to point to each digital patch in IPFS. Therefore, by using the distributed NFT stored via IPFS, we can manage the copyright of NFTs more conveniently.

2. *Propose watermarking method for the distributed patches before minting NFTs*
   Our system provides new watermarking method to embed the copyright information into the distributed image patches before minting NFTs on blockchain. Therefore, in our system, before becoming NFTs, the copyright information is also embedded into the digital contents. That makes our system different from other proposals.

3. *Propose new method for managing legal users by using licensing system*
   In order to manage the legal users, we propose the licensing system to control the watermark patterns for reconstructing the watermarked digital contents by using the downloaded NFTs from IPFS. Such watermark patterns are used to identify the legal users. Also, when dispute about the right to use digital products happens, we can trace the traitor and judge the copyrights of digital content.

4. *Legal users identification using new watermark patterns*
   Instead of using only one watermark logo for identifying the copyright of digital contents, we propose new approach that employs multiple watermark logos for proving the right legal users and also tracing the traitors. This is the novel idea to improve the conditional DRM system for managing legal users.

1.4. Roadmap

The remain of our paper is organized as follows. The explaination of preliminaries is described in Section II. In Section III, the components of proposed DRM method based on digital watermarking combined blockchain network are introduced, including watermark embedding and extracting processes. Our simulation results are described in Section IV. The conclusion is shown in Section V.

2. Preliminaries

To solve the problem of Digital Rights Management abusing detection to protect multimedia content, we have proposed a new watermarking scheme based on the DCT transform domain. We employ the IPFS blockchain for distributed storage of digital contents, the watermarking technique for embedding the copyright information, and distributed patches reconstruction.

2.1. Blockchain network

Blockchain is an potential technique that encompasses many technologies,e.g. cryptography, mathematics, consensus algorithms and economic models [9]. It also enhances customer service, drives end-to-end value, and increases operational efficiency. It is a secure, shared and immutable distributed ledger (database). Such a database records all of the network's transaction data into blocks. It uses a peer-to-peer (P2P) network and a consensus mechanism to solve the problem of distributed data synchronization. Therefore, it is not necessary to have a centralized trusted authority [14].

In the blockchain, block data is defined as a back-linked record in the order of blocks of transactions. Such blockchain data can be saved in a database (as a large file). Each block in the chain can be specified using the cryptographic hash algorithm SHA256[5] on the block header. The block consists of two parts, the main structure data and the header information. The main structure data records a list of transaction information across the network, while the header information includes the hash of the previous and current block, Merkle Root, timestamp, nonce, and other information.

Since all list of transactions is permanently stored in a block, if we apply blockchain technology to manage copyright, we can track all the transactions that belong to a certain digital asset. That makes it our advantage over other DRM systems because everyone can claim the copyright of digital content through the blockchain network.

[5] https://emn178.github.io/online-tools/sha256.html

2.2. Decentralized storage: IPFS

IPFS is a P2P distribution hypermedia protocol that aims to act as a universal file system for all computing devices [3]. IPFS can be considered similar to the WWW. It is like a single BitTorrent pool that exchanges digital objects in a single Github repository. IPFS combines a decentralized hash table, data exchange and a self-certifying namespace, also forming a generic Merkle architecture.

In particular, in the IPFS system, there is no single point of failure and the nodes do not need to trust each other. Based on that, distributed digital content delivery can save network bandwidth consumption [2].

IPFS is a technology especially suitable for distributing digital content over a blockchain network. We can manage the CIDs inside the DRM system to achieve certain digital content. We will show how to integrate IPFS technology with DRM system in our proposed method. Such a combination of techniques may replace third-party functionality.

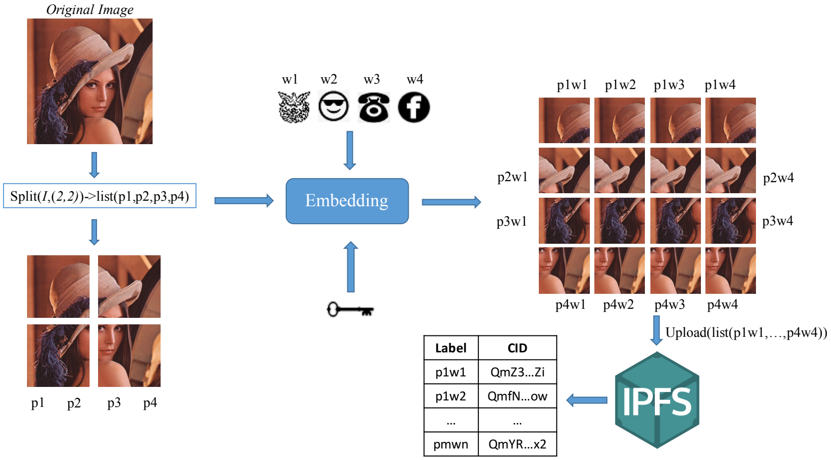
3. Proposal of Blockmarking based DRM system

3.1. Overview of our system

Store blockchain-based IPFS decentralized content on the web by dividing large digital files into patches and distributing those patches across the network. Thus, if IPFS replaces the functionality of authority judgement in a DRM system, the copyrighted contents (copyrighted NFTs) can be distributed over the blockchain network. Based on that, the storage of copyrighted content does not depend on the authority judgement. Also, when someone wants to check the copyright of any content, they can obtain the content via IPFS and extract the watermark. There are two main processes that comprise our recommended approach: embedding and distribute embedded patches in IPFS storage, copyrighted contents delivery and copyright confirmation via IPFS.

3.2. Embedding and distributing embedded patches in IPFS storage

Our idea changes the normal way to store the digital contents for sale by moving the digital contents to NFTs marketplace. We do not save the copyrighted contents into the centric database of content providers. In order to take advantage of IPFS, we consider to split the original content I into many patches. Then, we embed multiple watermarks into those patches. Afterwards, the embedded patches are distributed via IPFS by minting them to NFTs via blockchain. The workflow of this stage is shown in Figure 1.



Label	CID
p1w1	QmZ3...Zi
p1w2	QmfN...ow
...	...
pmwn	QmYR...x2

Figure 1. The process of Embedding and Distributing embedded patches in IPFS storage

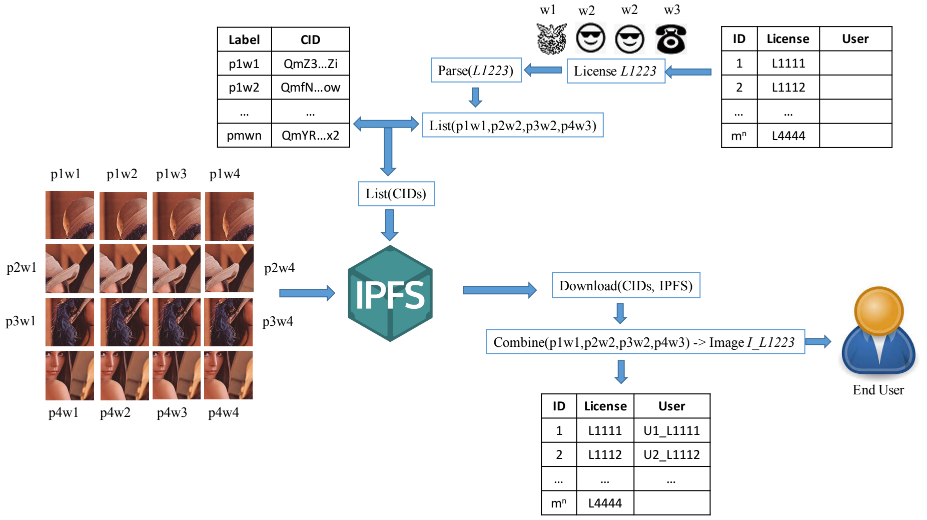
The algorithm is explained as follows:

1. The original content I is split into m patches of image. Such patches denotes as $\{p1, p2, p3, \ldots, pm\}$.
2. n patterns of watermarks, *e.g.* $\{w1, w2, w3, \ldots, wn\}$ are used to embed into m patches of image. After that, we can obtain $m \times n$ watermarked patches. That means we have $\sum_{i=m}^{j=n} p_i w_j$ watermarked patches. Such watermarked patches are minted via IPFS network. After uploaded, CIDs are generated for referencing content in distributed information systems.
3. All CIDs are collected, then they are saved into key-value as {Label, CID} system.

3.3. Licensing management

After uploaded the watermarked patches (NFTs) via IPFS, we can manage all CIDs by using key-value table <Label, CID>. By using this table, we can randomly generate the license table L beforehand, then assign the license number for according legal users when he/she bought the digital contents. The detail of licensing process management is shown in Figure 2. This algorithm is introduced as follows:

1. The license table L is randomly generated based on the CIDs table. Since licenses are based on n (the number of watermark), the license number can denote as $\{L1111, L1112, L1113, \ldots, Lnnnn\}$.
2. When users want to buy the digital contents, he/she requests to provide a license number. The provider send him/her a license number from the license table L. According to such license number, n patterns of CIDs are decided. Afterwards, n patterns of image patches (NFTs) are downloaded from IPFS to combine into the watermarked contents I' for end user U.
3. After sent the license number for end user, the information of user and license number are stored into license table. Based on table L, the producer can manage the license and that of legal user.



Label	CID
p1w1	QmZ3...Zi
p1w2	QmfN...ow
...	...
pmwn	QmYR...x2

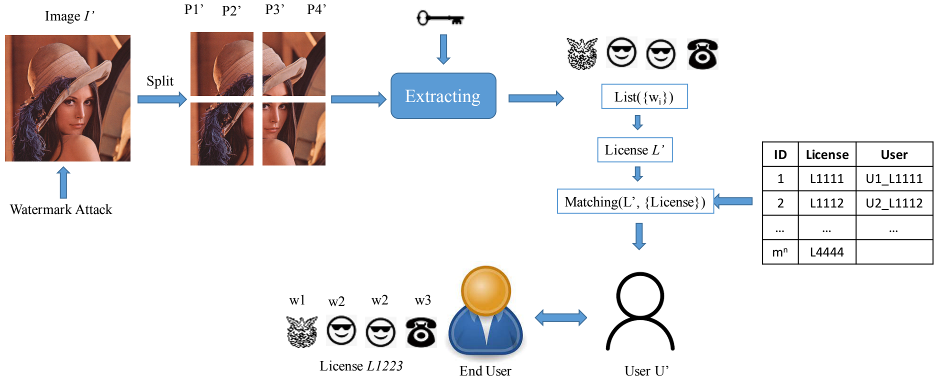
ID	License	User
1	L1111	
2	L1112	
...	...	
m^n	L4444	

ID	License	User
1	L1111	U1_L1111
2	L1112	U2_L1112
...	...	...
m^n	L4444	

Figure 2. Licensing process management

3.4. Copyrights identification

When the copyright dispute happens or an illegal distribution of copyrighted products is discovered, it is essential to confirm the copyright and identify the legal owner. In our method, suppose there is a copyright dispute of the copyrighted content I', we need to extract the watermark patterns from I', then match the patterns via license table. According that, the information of legal users can be detected. This algorithm is shown in Figure 3.



ID	License	User
1	L1111	U1_L1111
2	L1112	U2_L1112
...	...	...
m^n	L4444	

Figure 3. Copyrights identification process

1. The digital content I' is split into m patches of image. Such patches denotes as $\{p'1,'p2, p'3, \ldots, p'm\}$.
2. n patterns of watermarks, *e.g.* $\{w'1, w'2, w'3, \ldots, w'n\}$ are extracted from m patches of image. After that, we can obtain the watermark patterns. Based on the watermark patterns, we can detect the license number $Lxxx$, then we can trace the legal user of digital content.
3. After detected the legal user by using the license number $Lxxx$, we can judge the rights of watermarked contents.

According to analysis above, we emphasize that our proposed system can replace the conventional DRM system by employing the blockchain technology. We can distribute digital contents through IPFS, then anyone can check the copyright of the content transparently.

3.5. The benefit of our proposed system

In our system, the original image I is divided into m patches. Afterwards, each patch is watermarked separately with n patterns of watermark logos or ID information. In order to sell to many end users, therefore, we can obtain n^m different combinations of watermarked images employing $n \times m$ different watermarked patches. Then, $n \times m$ different watermarked patches are minted as NFTs and are saved to the IPFS network, and each patch gets unique address (CID)[6] which can be used to download the patch. The end user when buying an image obtains m CIDs that can be used to download m patches and then reconstruct the whole image with different watermark patterns.

According to above explanation of our algorithm, the main benefit of our proposed system is that it saves the disk space, computing power, and Internet network bandwidth (as some patches may be locally cached) as normally for L end users (buyers) we need to upload L different copies of watermarked (whole) images to the IPFS network. In the proposed system, the maximum number of legal users is n^m. In most cases $n = 2$ or 3 (for $m = 16$), therefore the required disk space is only doubled/tripled for managing L users with L licenses. The watermarking system might be also more immune to watermarking attacks.

4. Performance analysis and discussion

4.1. Experimental environment

In order to perform the efficiency of the proposed algorithm, we employ six color images from image database[7] with size $M \times N = 512 \times 512$ pixels. For embedding watermark patterns, we use four logomarks in our experiments, and they are the binary image with size 64×64 as shown in Figure 4.

[6] https://docs.ipfs.tech/concepts/content-addressing/#how-cids-are-created

[7] www.vision.kuee.kyoto-u.ac.jp/IUE/IMAGEDATABASE/STDIMAGES/

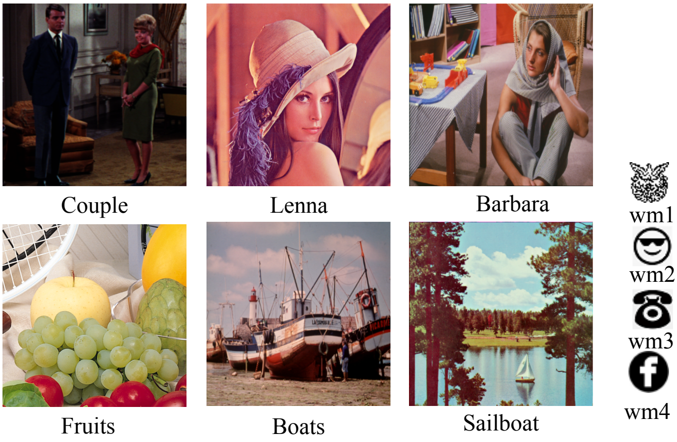


Figure 4. Experimental images

In general, to measure the efficiency of image watermarking schemes, their invisibility, robustness, and computing time are calculated and are compared each others. To evaluate the invisibility capability, we use the peak signal-to-noise ratio ($PSNR$) to measure the similarity between the original color image I and the watermarked image I' with size of $M \times N$.

The value of $PSNR$ is employed as a measure for evaluating the quality of the watermarked image comparing with that of the original image. $PSNR$ is described by the following equation:

$$PSNR = 10 \log_{10} \frac{255^2}{MSE}, \tag{1}$$

where MSE is mean square error between the original and watermarked image. MSE is defined as:

$$MSE = \frac{1}{MN} \sum_{i=0}^{M-1} \sum_{j=0}^{N-1} (I(i,j) - I'(i,j))^2 \tag{2}$$

In order to measure the robustness of our method, we also used the normalization correlation (NC) value [22] and calculated it over all extracted logomarks.

4.2. Experimental results

In order to evaluate our proposed system, we split the original image I into $n = 4$ non-overlap blocks image. We called them as Patch1, Patch2, Patch3, Patch4. Then, four logomarks patterns are embedded into each patch image for generating the embedded patches images. After that, the embedded block images are minted to NFTs to IPFS network. The testing for confirmation of image quality and the robustness of watermark extraction are performed, then the results are shown in Table 1.

Table 1
Experimental values of PSNR/NC for all images

Image	Patch1	Patch2	Patch3	Patch4	PSNR	PSNR
	PSNR/NC	PSNR/NC	PSNWNC	PSNR/NC	Average/NC	Combine/NC
Lenna	47.21/1.0	47.63/0.9931	46.16/0.9980	48.67/0.9940	47.41/0.9963	47.24/0.9961
Couple	50.23/0.7805	50.27/0.9795	51.70/0.6543	52.25/0.8377	51.11/0.813	50.94/0.8047
Barbara	45.90/0.9958	47.79/1.0	47.04/0.9940	48.66/1.0	47.34/0.9975	47.11/0.9975
Fruits	44.96/0.9876	48.25/0.9977	47.78/0.9940	46.80/0.9940	46.95/0.9933	46.55/0.9926
Sailboat	43.98/1.0	43.62/0.9977	46.05/1.0	45.54/1.0	44.80/0.9994	44.57/0.9995
Boats	50.60/0.9979	48.84/0.9954	46.38/0.9980	46.32/0.9311	48.03/0.9806	47.41/0.9800

We tried to generate the random license, then restored the watermarked contents by retrieving the watermarked NFTs from IPFS. Afterwards, we evaluated the robustness of the embedding method by using some attacks such as Gaussian noise, salt&pepper noise, JPEG compression, erasing, change histogram, and change color. The testing of above attacks on Lena image is shown in Table 2. According Table 2, we can see that the copyright logo can be clearly recognized. The values of PSNR and NC are suitable for copyright protection. In general, the value of PSNR is over 40dB, and the value of NC is over 0.9.

Table 2
Experimental values of PSNR/NC for Lena after attacks

Attack	Patch1	Patch2	Patch3	Patch4	NC Average	NC Combine
Gaussian noise	0.7712	0.7706	0.7382	0.7194	0.7499	0.7566
Salt&Pepper noise	0.7509	0.6971	0.7618	0.7318	0.7354	0.8538
Jpeg compression	0.4015	0.4134	0.3758	0.4311	0.4055	0.4111
Erasing	0.7587	0.7293	0.7078	0.7699	0.7414	0.7276
Histogram	0.8656	0.8220	0.8223	0.8180	0.8319	0.8679
Color change	1.0	0.9931	0.9960	0.9841	0.9993	0.9950

The visualization of the attacked Lena can be seen in Figure 5. It is clear that, based on the watermarked patterns, we can match the license number and detect the legal users based on our license management system. We also retrieved the similar results based on experimental results of another images.

We also compared the proposed method with several previous methods for NFT copyright protection. Such comparison is show in Table 3. Our method and Saeed *et al.* [12] use the watermark information to prove the copyright of NFT contents. Meanwhile, Dalla *et al.* [4] only used watermark for authentication information. In case of illegal NFT redistribution, our method can track the legal users by using the license number *Lxxx* to extract the watermark pattern. However, other methods cannot track the redistributed users when a dispute occurs.

According to above analysis, we can understand that our method can be applied for NFTs marketplace efficiently.

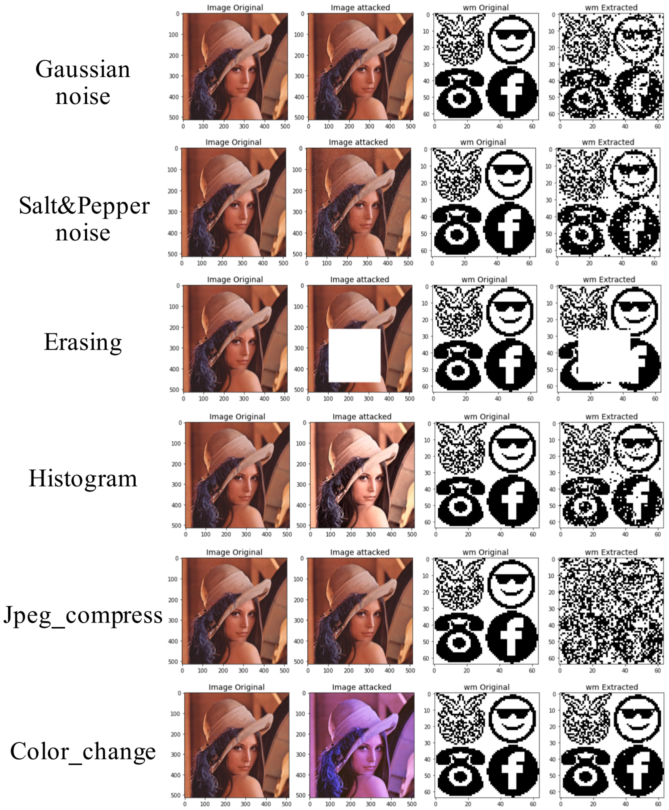


Figure 5. Logo patterns extraction under several attacks (for Lena)

Table 3
Comparison with some previous methods

Criteria	Our method	Saeed [12]	Dalla [4]
Watermarking for NFT	✓	✓	×
Legal users tracking	✓	×	×
Combination NFT patches	✓	×	×

4.3. Discussion

The limitation of the proposed method is that if the end user buys 2 or more copies of the same image with different watermarking, it is possible to construct an image with different watermarking IDs. In this case the image can be redistributed and the end users who redistribute the image may not be properly identified. That means the extracted watermarking pattern does not belong to the licenses that are generated beforehand. Therefore, the image is redistributed and the end users who redistribute the image may not be properly identified, however, the users use such image with wrong watermark pattern that does not belong to the license database L, such users are judges as illegal users.

The solution to the above problem might be that one patch has as many watermarks as the number of users or the n is much larger than required and additional algorithm is used to track the users who redistributed the image. This solution will be solved in the future works.

5. Conclusions

We have presented a new distributed image by using IPFS combined watermarking method for copyright protection and users authentication system without third parties. The original digital images are split into many blocks image, then are embedded with various watermark patterns, and uploaded on the online storage via IPFS. The license number is used to generate the watermark patterns for achieving the embedded blocks image from IPFS. Those also can be used for specify the legal users. According to the experimental results, the watermark patterns could be successfully extracted and distinguished each others.

References

[1] Asikuzzaman M., Pickering M.R.: An Overview of Digital Video Watermarking, *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 28(9), pp. 2131–2153, 2018. doi: 10.1109/TCSVT.2017.2712162.

[2] Badr B., Horrocks R., Wu X.: *Blockchain by Example: A Developer's Guide to Creating Decentralized Applications Using Bitcoin, Ethereum, and Hyperledger*, Packt Publishing, 2018.

[3] Benet J.: IPFS – Content Addressed, Versioned, P2P File System, 2014. doi: 10.48550/ARXIV.1407.3561.

[4] Dalla Preda M., Masaia F.: Exploring NFT Validation through Digital Watermarking. In: *The 18th International Conference on Availability, Reliability and Security (ARES 2023), August 29 September 01, 2023, Benevento, Italy*, Association for Computing Machinery, New York, NY, USA, 2023. doi: 10.1145/3600160.3605063.

[5] Gaid S.K., Jabbar K.K.: Frequency Domain for Color Image Authentication Proofing, *Journal of Physics: Conference Series*, vol. 1963(1), 012094, 2021. doi: 10.1088/1742-6596/1963/1/012094.

[6] Iwakiri M., Thanh T.M.: Fundamental Incomplete Cryptography Method to Digital Rights Management Based on JPEG Lossy Compression. In: *2012 IEEE 26th International Conference on Advanced Information Networking and Applications*, pp. 755–762, 2012. doi: 10.1109/AINA.2012.111.

[7] Iwakiri M., Thanh T.M.: Incomplete Cryptography Method Using Invariant Huffman Code Length to Digital Rights Management. In: *2012 IEEE 26th International Conference on Advanced Information Networking and Applications*, pp. 763–770, 2012. doi: 10.1109/AINA.2012.112.

[8] Mary S.J.J., Joe S.S.A., Siddique M.: IRDM watermarking with EMRC6 encryption for DRM system. In: *2018 Majan International Conference (MIC)*, pp. 1–5, 2018. doi: 10.1109/MINTC.2018.8363157.

[9] Nakamoto S.: Bitcoin: A Peer-to-Peer Electronic Cash System. pp. 1–9, 2008. Available at https://bitcoin.org/bitcoin.pdf.

[10] Parah S.A., Sheikh J.A., Loan N.A., Bhat G.M.: Robust and blind watermarking technique in DCT domain using inter-block coefficient differencing, *Digital Signal Processing*, vol. 53, pp. 11–24, 2016. doi: 10.1016/j.dsp.2016.02.005.

[11] Pardhu T., Perli B.R.: Digital image watermarking in frequency domain. In: *2016 International Conference on Communication and Signal Processing (ICCSP)*, pp. 0208–0211, 2016. doi: 10.1109/ICCSP.2016.7754123.

[12] Ranjbar Alvar S., Akbari M., Yue D.M.X., Zhang Y.: NFT-Based Data Marketplace with Digital Watermarking. In: *KDD '23: Proceedings of the 29th ACM SIGKDD Conference on Knowledge Discovery and Data Mining*, pp. 4756–4767, Association for Computing Machinery, New York, NY, USA, 2023. doi: 10.1145/3580305.3599876.

[13] Srivastava R., Tomar R., Gupta M., Yadav A.K., Park J.: Image Watermarking Approach Using a Hybrid Domain Based on Performance Parameter Analysis, *Information*, vol. 12(8), 2021. doi: 10.3390/info12080310.

[14] Sultan K., Ruhi U., Lakhani R.: Conceptualizing Blockchains: Characteristics & Applications, *ArXiv*, vol. abs/1806.03693, 2018.

[15] Tai L.D., Thanh N.V., Thanh T.M.: Blockmarking: Hybrid Model of Blockchain and Watermarking Technique for Copyright Protection. In: *SoIC '22: Proceedings of the 11th International Symposium on Information and Communication Technology*, pp. 398–404, Association for Computing Machinery, New York, NY, USA, 2022. doi: 10.1145/3568562.3568575.

[16] Tai L.D., Thanh T.M.: Digital Image Watermarking Algorithm Using Blockmarking Technique for Copyright Protection. In: *2023 15th International Conference on Knowledge and Systems Engineering (KSE)*, pp. 1–4, 2023. doi: 10.1109/KSE59128.2023.10299411.

[17] Thanh T.M., Iwakiri M.: A Proposal of Digital Rights Management Based on Incomplete Cryptography Using Invariant Huffman Code Length Feature, *Multimedia Systems*, vol. 20(2), pp. 127–142, 2014. doi: 10.1007/s00530-013-0327-z.

[18] Thanh T.M., Iwakiri M.: Fragile Watermarking with Permutation Code for Content-Leakage in Digital Rights Management System, *Multimedia Systems*, vol. 22, pp. 603–615, 2016. doi: 10.1007/s00530-015-0472-7.

[19] Thanh T.M., Quyet D.T.: A study on gas cost of ethereum smart contracts and performance of blockchain on simulation tool. In: *Peer-to-Peer Networking and Applications*, pp. 200–212, Special Issue on 2 – Track on Security and Privacy, 2024. doi: 10.1007/s12083-023-01598-3.

[20] Thanh T.M., Tanaka K.: A proposal of novel q-DWT for blind and robust image watermarking. In: *2014 IEEE 25th Annual International Symposium on Personal, Indoor, and Mobile Radio Communication (PIMRC)*, pp. 2061–2065, 2014. doi: 10.1109/PIMRC.2014.7136511.

[21] Thanh T.M., Tanaka K.: Blind Watermarking using QIM and the Quantized SVD Domain based on the q-Logarithm Function. In: J. Braz, S. Battiato, F.H. Imai (eds.), *VISAPP 2015 – Proceedings of the 10th International Conference on Computer Vision Theory and Applications, Volume 3, Berlin, Germany, 11–14 March, 2015*, pp. 14–25, SciTePress, 2015. doi: 10.5220/0005291900140025.

[22] Thanh T.M., Tanaka K.: The novel and robust watermarking method based on q-logarithm frequency domain, *Multimedia Tools and Applications*, vol. 75, pp. 11097–11125, 2016. doi: 10.1007/s11042-015-2836-6.

[23] Thanh T.M., Thanh N.T.: Extended DCT Domain for Improving the Quality of Watermarked Image. In: *2015 Seventh International Conference on Knowledge and Systems Engineering (KSE)*, pp. 336–339, 2015. doi: 10.1109/KSE.2015.70.

[24] Thomas T., Emmanuel S., Subramanyam A.V., Kankanhalli M.S.: Joint Watermarking Scheme for Multiparty Multilevel DRM Architecture, *IEEE Transactions on Information Forensics and Security*, vol. 4(4), pp. 758–767, 2009. doi: 10.1109/TIFS.2009.2033229.

[25] Venugopalan S., Aydt H.: Improving Confidentiality for NFT Referenced Data Stores, 2023.

[26] Zhaofeng M., Weihua H., Hongmin G.: A new blockchain-based trusted DRM scheme for built-in content protection, *EURASIP Journal on Image and Video Processing*, 91, 2018. doi: 10.1186/s13640-018-0327-1.

Affiliations

Le Danh Tai
Le Quy Don Technical University, 239 Hoang Quoc Viet, Bac Tu Liem, Ha Noi,
ledanhtai@lqdtu.edu.vn

Ta Minh Thanh
Corresponding author. Le Quy Don Technical University, 239 Hoang Quoc Viet, Bac Tu Liem, Ha Noi, thanhtm@lqdtu.edu.vn

Received: 24.04.2023
Revised: 24.02.2024
Accepted: 9.06.2024