International Journal of Computing and Digital Systems
ISSN (2210-142X)
Int. J. Com. Dig. Sys. 10, No.1 (May-2021)

http://dx.doi.org/10.12785/ijcds/100159

Design Scheme For Copyright Management System Using Blockchain and IPFS

Ali Muwafaq Alchaqmaqchee[1] and Saad Najim Alsaad[2]

[1,2]Department of Computer Science, Mustansiriyah University, Baghdad, Iraq

Received 28 May.2020, Revised 17 Jul. 2020, Accepted 29 Jul. 2020, Published 02 May. 2021

Abstract: The existing technologies allow to distribute digital images quickly and easily through the internet. The misuse of digital images, intentionally or unintentionally, increases dramatically especially with copyright protection that facing a major challenge. There are many unsolved problems in the centralized copyright office registration such as high cost services, long time processing, store copyright information in the centralized server and susceptibility to tampering registration records. In this paper, a schema of copyright digital management system is designed based on blockchain, Inter Planetary File System (IPFS) and Perceptual hash image. Blockchain technology evolvement has very changed the network that makes numerous applications become distributed and decentralized without loss of security. Moreover, our solution exploits the benefits of IPFS to store image and text file of copyright owner's information on a decentralized file system. Perceptual image hashing is used for authentication based on the understanding of the image content. The scheme uses Point to Point (P2P) network to improve the copyright image management, make the distribution of copyrighted work without third part and finally protect the copyright owner.

Keywords: Image Copyright, Blockchain, IPFS , Perceptual Hash Image

1. INTRODUCTION

The rapid evolution of the multimedia technologies makes the distribution and the proliferation of multimedia content so easy [1]. The popularity of social media and smart phones also effectively participate in making sharing and creation of images and video simple for most of people [2]. In Facebook, about 350 million of images are downloaded and 250 billion of images are uploaded everyday [3]. The evolution in technology presents many advantages privileged to user. But the availability of many image processing tools also simplifies to use this data by unauthorized users. Attackers and unauthorized user enable to copy, distribution, delete, and change digital information easily [1,4]. Hackers take advantage of these digital work features to make use of the legal rights of copyright owners to obtain personal benefit illegally [5]. Therefore, the protected is needed for numerous of the inventive work of people for their distributed and possession in cyber space through the internet [6].

There are many problems unsolved in the traditional digital right management (DRM). For instance, in the traditional copyright office, copyright owner's need to provide the office several personal information as copyright information. The centralized office checks and submits information manually to be saved in the centralized server. The centralized copyright office registration has shortcomings of high cost, guarantee quality of media works is hard, difficulty traceability, complex procedures and ease to manipulate registration records make the users dissatisfied because it is required to demonstrate that the information is indeed original, not modified [2,7,8].

Researches on copyright digital images using watermarking is not a new thing. There are many researches on watermarking images has published. Many researchers keep going to innovate to find best watermark techniques. Most of watermark technique is aiming to be imperceptibility and robustness, whereas generation and storage of the watermarked image information is ignored [5].

The Dropbox as one of internet-based cloud services example is considered as one of crucial for multimedia delivery that satisfying low cost, high performance and high availability .However, the privacy breach problem cannot be solved by having user control alone over data because as once the user allow to the third party to access then the third party can do whatever he wants and that affects negatively to the data integrity [9,10].

This paper is structured as follows: section two presents related work. Section three gives the background about system, section four describes scheme methodology, section five discusses the simulation of the scheme and finally the conclusion.

E-mail: alimuwafaq92@gmail.com, dr.alsaadcs@uomustansiriyah.edu.iq

2. RELATED WORK

Zhaoxiong et al. [5] used blockchain to store watermark information and achieved time-stamp authentication in order to protect the legitimate rights of each copyright owner. As a result, a new option for protection digital copyright business in the rapid growing internet era is provided.

Herbert and Litchfield [11] used blockchain for decentralized software license verification to minimize software piracy and supply record of all licenses owned by user to protect software copyright. The authors utilized methods for software license validity. The features of software license are hard to copy, easily validated and cannot be regenerated.

McConaghy and Holtzman [12] employed the blockchain to register a cryptographic hash of the work information. At once the work is registered, a particular number of editions is added. The works can be transfered or shared to provide perfect source of work that transfer through the service. Lastly, the web crawl technology finds online similar images, even if the original image was modified.

Vishwa and Hussain [10] presented a decentralized framework of information management that guarantee the privacy of user data controlled by protocol that uses blockchain technology. Smart Contracts used to describe how to ensure user data on blockchain.

Zheng et al [13] presented a model storage for blockchain based on IPFS. The result has a certain degree of improvement in storage space, security and new node synchronization speed.

Kishigami et al. [14] proposed decentralized blockchain based on digital content distribution. It contents three modules: First, Licensor: has two main functions (license control of all owned contents, upload the contents file). Second, Licensee has two major applications (license control application and content player). Third, Mining server, it is the main module of the system. It can produce the new block that contain the rights data. The proposed system examined nearly by 100 people, they suggested a lot of ideas to improve the system and the most exciting and attractive point is the decentralization mechanism.

Palai et al. [15] presented a method for block summarization to reduce blockchain storage overhead for system that include transferable transactions. The result is reducing the blockchain volume and make computational activities suitable for nodes with minimum memory capacity or processing power and make it less rely on peers.

Zyskind et al. [16] proposed a decentralized personal information management system in order to guarantee user own and control information. AS a result, the user data privacy is protected.

Rahulamathavan et al. [17] proposed a secure blockchain architecture for internet of Thing (IoT) application using attribute-based encryption (ABE) technique. The result referred that IoT supported by the blockchain can get advantage related to privacy.

Malik et al [18] used blockchain as a tool for allowing the official individuals documents to be shared by government organization and educational institutions. Document verification process and issue process efficiency is very high improved with blockchain model, with advantages of transparency, security and reliability.
Es-Samaali et al. [19] proposes access control framework using bockchain to enhance the platform of big data. The authors claimed of achieving three objectives: no central authority, high transparency and Light weightiness.

3. BACKGROUND

In this section, we discuss concepts and tools that used in the system.

A. Blockchain

Blockchain is an essential technology of Bitcoin that consider the decentralize as noteworthy characteristic of it [20]. It is a constantly increasing list of records that provide a dependable time stamping based on cryptographic hash and distributed consensus that registers all of events that happened in the system [21]. A blockchain is a public and open source P2P networkwith same right of nodes. It is digital ledger that distributed among the network peers. The digital ledger is immutable (it can't be changed after registered). It is recorded in sequential chain of blocks that are connected over a cryptographic hash [22]. All blocks in the blockchain hold its own digital signature and its own information of transaction data and state [23]. The modern researches explicit that the blockchain is efficient solution to handle issues such as unsecure data storage, high cost and low efficiency [20].

Blockchains supply new model for storage information In a safety way based on the principle of decentralization. Generally, the main features of blockchain may be summarized as: [24]:

• Transparency: The information on blockchain is a public and can't be manipulated.
• Redundance: All nodes of the blockchain retain a copy of the information. It can't be easily taken by a malicious action (attacker).
• Immutability: Blockchain is designed to store data to be immutable and tamperproof. Basically, the data of blockchain is verified by unique cryptographic hash. The resulting blocks are linked to the previous blocks by reference to the previous block hash. If any modification is made to the content of the block, the next block will still contain the previous block hash. So, the hacker must modify all blocks to cover up a single block change.

• Disintermediation: removal of mediator like bank from transaction, leads to reduction transaction cost and risk related with existence of this intermediary.

Hence, the blockchain proved it is trusted when regarding to the effective and safe storage of the transaction [10].

B. IPFS

The InterPlanetaryFileSystem is a decentralize file system which is linked over computers that shared a file system. It works like to BitTorent network [22]. It is P2P distributed file system, aims to substitute HTTPs [25] and relies on a distribute hash table (DHT) to restore file location and node connection data [26]. IPFS is content address, assigning a unique hash to store file in the network. It contains deduplication technique, without use centralize server restriction. The data that requested with higher frequency, IPFS organize duplicate data over the that request to be read directly in the next request. Generally, IPFS is high throughput, secure, content address storage model, high capability storage and synchronous access [13].

The main characteristics of IPFS can summarizes as [27]:

• Availability: No single point of failure.

• Reliability: Trust to the content without need confidence to the peer which serve it.

• Bandwidth optimizations

• Security: Content address and content signing prevent distributed denial-of-service (DDoS) attack that HTTP is exposed to.

C. Perceptual hash

Perceptual hash is a finger print of a multimedia files derived from different features of it is content. Perceptual hash defines two files similar if both hold similar characteristic, that is linked to numerous applications like content authentication, images forgery, detect similarity of images, and image retrieval. This method different with cryptographic hash function which depend on the breakdown effect of small alteration in the input leading to large changes in the output [28,29].

Perceptual image hashing should maintain four major features so that guarantee the efficient and secure at the same time [30]:

- Robustness: meaning when use the same key, perceptually similar two image will produce similar hash.
- Discriminability: meaning when use the same key, perceptually different two image will produce different hash.
- Unpredictability: guarantee the attacker won't obtain the same hash for the original image by tampering or modify image data bit.
- Compactness: comparison between the size of the hash and the size of image is much smaller.

4. SCHEME METHODOLOGY

In this paper, a decentralized storage system is proposed based on the Blockchain technology and IPFS to store copyright information securely and to provide timestamp authentication. Figure1 depicts the schematic diagram of the proposed system. Perceptual hashing is performed to the input image in order to solve image content authentication problem. Once the hash of IPFS is written into blockchain, it will be difficult to modify or delete, also it is fundamental for an online copyright management to ensure that each work gets uploaded only once not more.

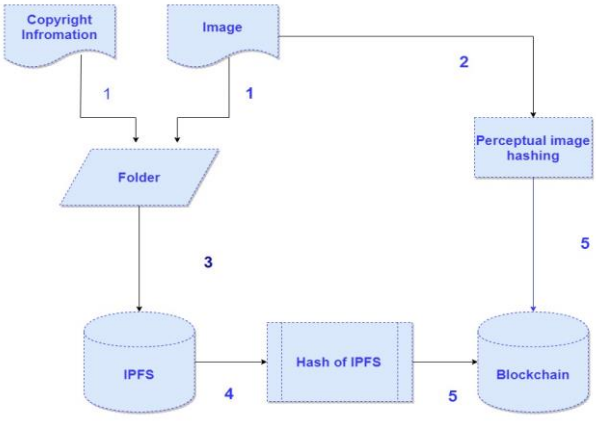

Figure 1. Schematic diagram scheme

The particular processes of the scheme above is presented in details in Algorithm 1.

Algorithm 1: Steps of figure1 implementation
Input: Folder of image and its copyright information
Output: Hash image and link of IPFS saved in blockchain
Step1: Join Node : Join node(computer or any device) to the public network by running the ipfs daemon in terminal using go-ipfs software .
Step2:Submit Upload Folder : Usage ipfs (add -r /Path) to add a folder to distributed system(IPFS).

Step3: Generate ID for the Image: Compute image ID using perceptual hashing image to emphasize content authentication.
Step4: Save Hashes in the Blockchain: Save the hash of IPFS and perceptual image hash to the blockchain.

5. SIMULATION OF THE SCHEME

This section is dedicated to the proposed system simulation. Barbara image is chosen (Figure 2).

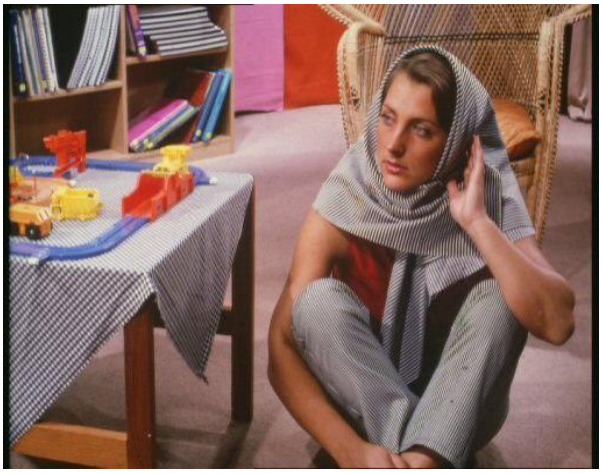

Figure 2. Barbara.jpg

*1) IPFS Entrance :*go-ipfs software is the main implementation of IPFS provided by website https://dist.ipfs.io/#go-ipfsit used to generate the IPFS as shown in figure 3. The computer that run the software became node in an IPFS distributed web.

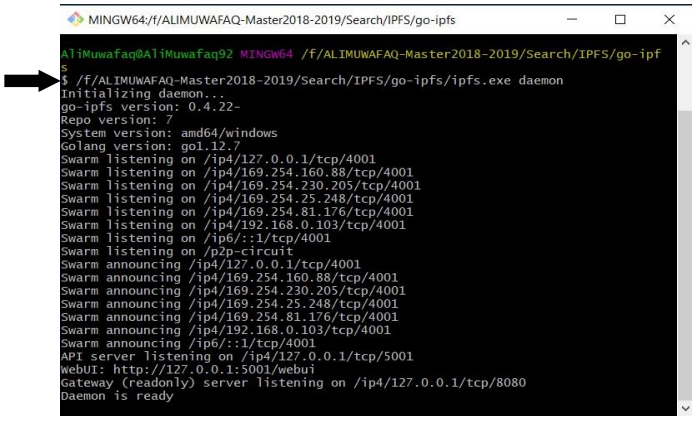

Figure3. Running of go-ipfs

2) Generate Perceptual Hash: Different versions of a perceptual image hash are available in Python image hash library like Average hash, Perception hash (Phash), Difference hash (Dhash) and Wavelet hash (Whash). PHASH is selected for simulation since it gives the best in the test. The perceptual hash (id) value of barbara.jpg is (**c9c91a74f0e74987)** .

3) Generate hash from IPFS: Open another terminal and load the folder containing image barbara.jpeg and text file barbara_CopyrightInfo.text as folder (Figure 4). The folder has been uploaded to IPFS and obtained the hash value: (QmWUPyM513fZwHm2odKsPWeNZQDN7de5Jzgj34 dL2ywP79) as the ID of the folder .The hash value of folder is the name in the IPFS distributed web.

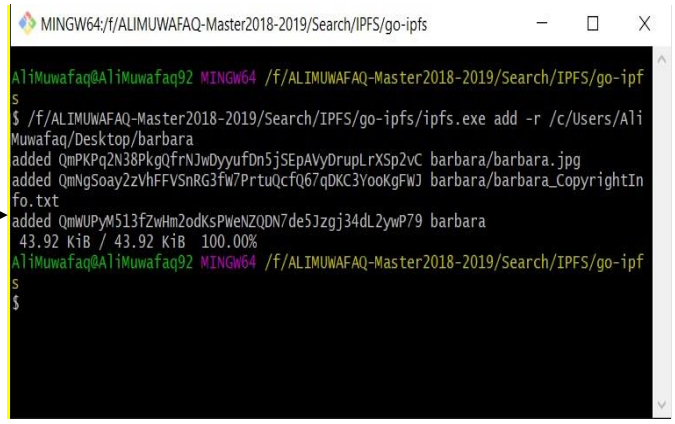

Figure 4. Upload of folder Barbara

4) Generate a new block: Save the hash of IPFS and perceptual image hash in the blockchain as show in the figure5. The benefit of IPFShash is to confirm that original owner's is rightfully and credited for their works. The perceptual image hashis to detect the tampered images automatically that have similar perceptual image hash to reject it.

Figure 5. generate a new block to save hash of IPFS

5) Browsing in the IPFS network: After saving the hash of IPFS and perceptual hash in blockchain we can confirm from image owner genuine by browsing in any web browser using IPFS Link to reach the folder as shown in figure 6. It contains image and its information as shown in the figure 7 and 8respectively.

Figure 6. Display of folder Barbara

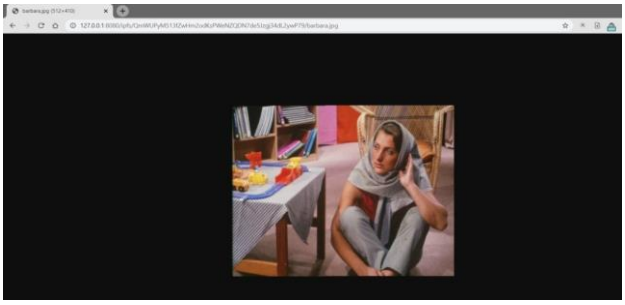

Figure 7. Display of image barbara.jpg

Figure 8. Display of text Barbara CopyrightInfo.txt

6. CONCLUSION

We proposed a decentralized scheme for digital copyright protection. The scheme uses blockchain, IPFS and perceptual image hashing to supply a new method for digital copyright protection in the rapid increasing Internet era. The traditional copyright registration requires:

a. high cost due it requires large-scale server storage devices.

b. long time, since the centralized agency review the submitted information manually.

c. susceptibility to tampering recording registers. In centralized systems, documents can be manipulated or deleted. Furthermore, the developers or users associated with the system has the control to change entries stored on the central server. On other hand, the decentralize technology is characterized by its security and credibility. The perceptual hashes are effective tools to image content authentication. We used it due to it has distinct features and it has less susceptible than traditional cryptographic hash algorithm like SHA256 and MD5, rotation, resizing and compression operations.

It is worthy to mention to the work in reference five. The authors did not save the hash of IPFS in distributed ledger (blockchain), but instead, hash of image is saved. This hash can't return the image. In our paper the hash of IPFS is saved in the blockchain, this hash contains image and its information that can be used to confirm the original owner's is rightfully and credited for their works. As a future work, copyright management system for audio and video can be developed. We predict that our proposed digital copyright management system would contributes to the evolution for copyright image protection.

REFERENCES

[1] Singh, Durgesh, and Sanjay K. Singh. "DWT-SVD and DCT based robust and blind watermarking scheme for copyright protection." Multimedia Tools and Applications 76.11 (2017): 13001-13024.

[2] Qi, Y., and X. Liu. "Digital copyright protection based on blockchain technology." (2018): 61-70.

[3] Sharon, M. Blessy, and S. J. Saritha. "Edge based robust image watermarking scheme for copyright protection of images." 2017 International Conference on Energy, Communication, Data Analytics and Soft Computing (ICECDS). IEEE, 2017.

[4] Arora, Shaifali M. "A DWT-SVD based robust digital watermarking for digital images." Procedia computer science 132 (2018): 1441-1448.

[5]Meng, Zhaoxiong, et al. "Design scheme of copyright management system based on digital watermarking and blockchain." 2018 IEEE 42nd Annual Computer Software and Applications Conference (COMPSAC). Vol. 2. IEEE, 2018.

[6] Arrasyid, AdliAzhar, et al. "Image Watermarking using Triple Transform (DCT-DWT-SVD) to Improve Copyright Protection Performance." 2018 International Seminar on Research of Information Technology and Intelligent Systems (ISRITI). IEEE, 2018.

[7] Zhang, Xuewang, and Yijun Yin. "Research on Digital Copyright Management System Based on Blockchain Technology." 2019 IEEE 3rd Information Technology, Networking, Electronic and Automation Control Conference (ITNEC). IEEE, 2019.

[8] Nizamuddin, N., et al. "Decentralized document version control using ethereum blockchain and IPFS." Computers & Electrical Engineering 76 (2019): 183-197.

[9] Bhowmik, Deepayan, and Tian Feng. "The multimedia blockchain: A distributed and tamper-proof media transaction framework." 2017 22nd International Conference on Digital Signal Processing (DSP). IEEE, 2017.

[10] Vishwa, Alka, and FarookhKhadeer Hussain. "A Blockchain based approach for multimedia privacy protection and provenance." 2018 IEEE Symposium Series on Computational Intelligence (SSCI). IEEE, 2018.

[11] Herbert, Jeff, and Alan Litchfield. "A novel method for decentralised peer-to-peer software license validation using cryptocurrency blockchain technology." Proceedings of the 38th Australasian computer science conference (ACSC 2015). Vol. 27. 2015.

[12] McConaghy, Masha, et al. "Visibility and digital art: Blockchain as an ownership layer on the Internet." Strategic Change 26.5 (2017): 461-470.

[13] Zheng, Qiuhong, et al. "An innovative IPFS-based storage model for blockchain." 2018 IEEE/WIC/ACM International Conference on Web Intelligence (WI). IEEE, 2018.

[14] Kishigami, Junichi, et al. "The blockchain-based digital content distribution system." 2015 IEEE fifth international conference on big data and cloud computing. IEEE, 2015.

[15] Palai, Asutosh, Meet Vora, and Aashaka Shah. "Empowering light nodes in blockchains with block summarization." 2018 9th IFIP International Conference on New Technologies, Mobility and Security (NTMS). IEEE, 2018.

[16] Zyskind, Guy, and Oz Nathan. "Decentralizing privacy: Using blockchain to protect personal data." 2015 IEEE Security and Privacy Workshops. IEEE, 2015.

[17] Rahulamathavan, Yogachandran, et al. "Privacy-preserving blockchain based IoT ecosystem using attribute-based encryption." 2017 IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS). IEEE, 2017.

[18] Malik, Gunit, et al. "Blockchain Based Identity Verification Model." 2019 International Conference on Vision Towards Emerging Trends in Communication and Networking (ViTECoN). IEEE, 2019.

[19] Es-Samaali, Hamza, AissamOutchakoucht, and Jean Philippe Leroy. "A blockchain-based access control for big data." International Journal of Computer Networks and Communications Security 5.7 (2017): 137.

[20] Xu, Ruzhi, et al. "Design of network media's digital rights management scheme based on blockchain technology." 2017 IEEE 13th International Symposium on Autonomous Decentralized System (ISADS). IEEE, 2017.

[21] Zeng, Jing, et al. "A Solution to Digital Image Copyright Registration Based on Consortium Blockchain." Chinese Conference on Image and Graphics Technologies. Springer, Singapore, 2018.

[22] Salah, K., A. Alfalasi, and M. Alfalasi. "A Blockchain-based System for Online Consumer Reviews." IEEE INFOCOM 2019-IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS). IEEE, 2019.

[23] Xu, Quanqing, et al. "Building an Ethereum and IPFS-Based Decentralized Social Network System." 2018 IEEE 24th International Conference on Parallel and Distributed Systems (ICPADS). IEEE, 2018.

[24] Savelyev, Alexander. "Copyright in the blockchain era: Promises and challenges." Computer law & security review 34.3 (2018): 550-561.

[25] Chen, Yongle, et al. "An improved P2P file system scheme based on IPFS and Blockchain." 2017 IEEE International Conference on Big Data (Big Data). IEEE, 2017.

[26] Steichen, Mathis, et al. "Blockchain-based, decentralized access control for IPFS." 2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData). IEEE, 2018.

[27] Sarıtekin, Recep Ahmet, et al. "Blockchain based secure communication application proposal: Cryptouch." 2018 6th International Symposium on Digital Forensic and Security (ISDFS). IEEE, 2018.

[28] Putro, Prasetyo Adi Wibowo. "Physical document validation with perceptual hash." 2017 3rd International Conference on Science in Information Technology (ICSITech). IEEE, 2017.

[29]Wang, Xiaofeng, et al. "Image alignment based perceptual image hash for content authentication." Signal Processing: Image Communication 80 (2020): 115642.

[30] Viies, Vladimir. "POSSIBLE APPLICATION OF PERCEPTUAL IMAGE HASHING." TALLINN UNIVERSITY OF TECHNOLOGY Faculty of Information Technology Department of Computer Engineering, Master thesis (2015).

Ali Muwafaq is Master student in the Department of Computer Science, College of Science, Al-Mustansiriya University. He is interested in information security.

Dr. Saad Najim Alsaad is Professor in Computer Science at College of Science/Mustansiriyah University / Baghdad / Iraq. He is interested in information security and object-oriented software engineering.
dr.alsaadcs@uomustansiriyah.edu.iq