Model Engineering College Ernakulam
Department of Computer Engineering
B. Tech. Computer Science & Engineering
CS 451 Project Preliminary
Literature Survey Report
Copyright Protection and Violation Detection Using Blockchain

11 MDL18CS027 Ardra Mohan
31 MDL18CS068 Malavika Rajesh Vikraman
51 MDL18CS104 Sandra Jacob
52 MDL18CS106 Sanjana S

December 7, 2021

Keywords: Blockchain, IPFS, Smart Contracts, Watermarking, Perceptual Hashing Algorithm

Abstract

Copyright refers to the legal right of the owner of intellectual property. Copyright ownership gives authors exclusive right to use their work and share it with those who they deem fit. Copyright protects the right of the authors, that is, the owners of the intellectual properties. With the development of technology and growth of the internet, services and contents are being distributed online via delivery channels and sharing systems. Because these platforms are widely used, tracing violations of copyright and ensuring secure distribution of content has become a problem for content owners. Copyright infringement is the use or production of copyright protected material without the permission of the copyright holder. It is a big challenge in today's world. The aim is to design a system involving a Blockchain network to which images can be uploaded and checked for copyright protection and violation detection.

1 Introduction

With the development of digital technology, multimedia, digital works in the form of image, audio, video and others have been published on the Internet. Over time, copyright protection and violation detection have become an urgent issue that needs to be addressed, especially since digital content such as images can be copied, processed and shared easily. Pirates exploit these characteristics of digital content to undermine the legitimate rights of copyright owners. For traditional copyright protection, copyright owners need to provide digital works and some personal information as copyright information to the copyright registration agency. This agency will manually review the submitted information and store it. This not only results in inefficiencies and increase in cost, but also has the risk of information being tampered with and leaked. In the past, traditional digital copyright protection system based on digital watermarking mainly focused on implementation of watermarking text or image while ignoring the generation and storage of watermark information. Thus, it is high time we develop a global system that addresses this need.

2 Literature Survey

We have done this literature survey in an order from watermarks and steganography which was used in the past, to the recent Blockchain watermark to understand the flaws in the current systems. This literature survey presents:

1. O. Evsutin, A. Melman and R. Meshcheryakov [1] present an overview of promising research in the area of copyright protection for digital objects. They also provide basic information about this field of research and discusses its main applications. Steganographic methods make embedded information invisible to an attacker. A digital watermark is a label that allows, for example, to identify the author of a digital object, or to confirm the authenticity and integrity of this object. Steganographic techniques make use of open communication channels, which makes it more vulnerable towards steganalysis and makes it less secure. Watermarks are generally vulnerable towards distortion and most common attacks such as rotation, scaling – reducing or increasing the size of the image, compression, noise overlay.

2. M.Boreiry and Mohammad-Reza Keyvanpour [2] focus on classifying watermarking methods based on the different watermarking approaches. The basic requirement in watermarking is resisting distortion and initial attacks, which is commonly examined based on the data processing standards. Many methods have been proposed in the field of video and image watermarking that are resistant to certain attacks, therefore some attacks can break the watermark. Robust watermarking schemes, like DCT and DWT based watermarking techniques are generally more resistant to attacks. These have good resistance, reliability, invisibility and applicability. However, application of just digital watermarks to images do not guarantee proper copyright protection.

3. Keta Raval and Sameena Zafar [3] focus on proposing a system using a different type of watermarking technique. Most watermarking algorithms transform the host image and embedding of the watermark information in a robust way. Uncompressed digital images need a lot of storage capacity and bandwidth so efficient image transmission needs image compression. Here, Digital Watermarking by Transform Algorithm based on DCT-DWT watermarking is proposed, which helps to do secure image transmission. Though, the downside is that it increases the potential for unauthorized distribution of such information and significantly increases the problems associated with copyright protection.

4. Wannida Sae-Tang, Masaaki Fujiyoshi and Hitoshi Kiya [4] focus on image copyright protection, consumer's privacy protection, and compression-friendliness with accepting any fingerprinting techniques. In the system they have proposed, ETC is applied to images for visual protection of consumer's privacy, whereas the conventional purpose of ETC techniques does not assume that a trusted third party decompresses an image for digital fingerprinting. This system achieves better performances than those of the conventional systems in terms of visual protection, image quality, compression compatibility, and fingerprinting. However, it works only for JPEG and copyright violation identification, tracing of violators and copyright detection is not carried out.

5. Hashmi et al. [5] propose a Real-time Copyright Protection Algorithm using both visible as well as invisible watermarking schemes. The invisible watermarking scheme uses DCT analysis, whereas the visible watermarking scheme is implemented using image processing properties of Android. In this system, pre-specified copyright information is embedded directly on pictures when they are taken. Here the efficiency of watermarking is high and the visible text watermark is also resilient to be removed by common image processing algorithms. The embedding process is automatic too. The increase in computational complexity is compensated by the speed of implementation. However, only copyright protection is done, so there is no way to detect if any violation occurs.

6. A. Nayak and K. Dutta [6] provide a well-defined study with a collection of all relevant research areas and technologies on Blockchain. Blockchain is a distributed ledger technology which maintains a list of records that goes on increasing continuously known as blocks. These blocks are secured from tampering and revision. It is a technology for decentralizing transactions and managing data. The growing interest among researchers and technologists is the central attribute of Blockchain, that it provides a high level of security, anonymity and data integrity without any intervention from a third party. Blockchain technology offers a lot of disruptive power that has potential. With Blockchain becoming the future of transactions in the financial sector, it also comes with its own burden of risks. But it is used widely since it has the potential to revolutionize the existing technology.

7. Shuai Wang et al. [7] present a comprehensive overview on Blockchain powered Smart Contracts. First, they give a systematic introduction for Smart Contracts, including the

basic framework, operating mechanisms, platforms and programming languages. Second, they discuss application scenarios and existing challenges. Finally, they describe the recent advances of Smart Contracts and presents its future development trends. Their paper is aimed at providing helpful guidance and reference for future research efforts. Smart Contracts can be implemented in Blockchain networks for carrying out trusted transactions and agreements and are automatically executed when the agreed upon conditions are met, without involvement of any intermediary.

8. Benet and Juan [8] give an insight about the need for constructing a global distributed file system. First, they explain about HTTP and Git, the two earliest versions of a global distributed system. They also discuss about how HTTP do not take advantage of recent technological advancements and how a global distributed file system is needed for handling large multimedia content as well as large datasets and for file sharing. Then, they talk about IPFS and its different components and how it helps in ensuring distributed file sharing. Identities of nodes, networking between nodes, data distribution and how IPFS utilizes Merkle DAG has also been discussed in great detail. IPFS also has a lot of different use cases, of which, the most prominent ones are that it can be as an encrypted file or data sharing system as well as database.

9. Sarohi, Harsh Kumar, and Farhat Ullah Khan [9] mainly focus on retrieving image from content. They have proposed a new perceptual hashing based approach for Image Retrieval. Content Based Image Retrieval (CBIR) is considered most efficient to search large image collections. The proposed method uses perceptual hash function which calculates similar hash value for similar images. Finally, using an adequate distance or similarity function to compare two perceptual hash values, it can be decided whether two images are perceptually different or not. This is a low cost system that focuses on efficient retrieval of images based on its color by constructing hashes. However this method does not provide a safe storage facility.

10. M. Li et al. [10] propose a Blockchain-watermarking scheme to protect the privacy, integrity and availability of compressed sensed images, it combines multimedia watermarking, compressed sensing, Interplanetary File System (IPFS) and Blockchain technologies. Based on the reliable authentication of watermarking, the confidentiality protection of compressed sensing, the secure storage of IPFS, and the decentralization and non-tamperability of Blockchain, the all-round security protection of the image of big data based on compressive sensing can be realized. Experiments show that the proposed scheme is effective and feasible. The system generates hash values the will be saved in the IPFS that provides a low cost storage. However the system does not detect copyright violations.

3 Proposed System

3.1 Problem Statement

With the evolution of ICT (Information Communication Technology), content is stored and distributed digitally. This leads to a situation where digital content, especially images are used in such a way that some non-authors get credit for other contributor's images, which violates copyright laws and this affects the rightful image owner mentally and financially. While some websites do check whether the new image being uploaded is already present on the marketplace by usage of cryptographic hashes, which are prone to avalanche effect, a phenomenon where a small change in input value leads to a drastic change in output value.

To develop a global system for Copyright Protection and Violation Detection using Blockchain technology along with IPFS and utilizing DCT Watermarking technique and Perceptual Hashing Algorithms.

3.2 Objectives

The main objectives are :

1. Copyright violation detection, making use of traceability property of Blockchain.
2. Similarity of images will be computed using perceptual hashing and hamming distance which will ensure a much better performance.

3. Digital fingerprint is generated and digital watermarking is added to it in order to better protect the copyrights.
4. IPFS is used for decentralized storage, thereby making the system cost effective.
5. Smart Contracts are used to automate trusted transactions between owner and user.

References

[1] O. Evsutin, A. Melman and R. Meshcheryakov, *Digital Steganography and Watermarking for Digital Images: A Review of Current Research Directions*, IEEE Access, September 2020.

[2] M. Boreiry, Mohammad-Reza Keyvanpour, *Classification of Watermarking Methods Based on Watermarking Approaches*, Artificial Intelligence and Robotics (IRANOPEN) Conference, IEEE Xplore, April 2017.

[3] Keta Raval, and Sameena Zafar, *Digital Watermarking with Copyright Authentication for Image Communication*, International Conference on Intelligent Systems and Signal Processing (ISSP), March 2013.

[4] Wannida Sae-Tang, Masaaki Fujiyoshi, and Hitoshi Kiya, *Encryption-then-Compression-Based Copyright and Privacy Protected Image Trading System*, Proceedings of the International Conference on Advances in Image Processing, August 2017.

[5] Hashmi, Mohammad Farukh, Shukla, Ronak, Keskar and Avinash, *Real Time Copyright Protection and Implementation of Image and Video Processing on Android and Embedded Platform*, International Conference on Information and Communication Technologies(ICICT), December 2015.

[6] A. Nayak and K. Dutta, *Blockchain: The perfect data protection tool*, IEEE Xplore, March 2018.

[7] Shuai Wang, Yong Yuan, Xiao Wang, Juanjuan Li, Rui Qin and Fei-Yue Wang, *An Overview of Smart Contract: Architecture, Applications, and Future Trends*, IEEE Xplore, October 2018.

[8] Benet and Juan, *IPFS - Content Addressed, Versioned, P2P File System.* , Research Gate , July 2014.

[9] Sarohi, Harsh Kumar and Farhat Ullah Khan, *Image retrieval using Perceptual Hashing,* IOSR Journal of Computer Engineering, 2013.

[10] M. Li, L. Zeng, L. Zhao, R. Yang, D. An and H. Fan, *Blockchain-Watermarking for Compressive Sensed Images*, IEEE Access, April 2021.

Internal Guide:

Mrs. Sony P
Asst. Professor
Department of Computer Engineering
Model Engineering College