Copyright Protection and Violation Detection Using Blockchain

MDL18CS027 11 Ardra Mohan
MDL18CS068 31 Malavika Rajesh Vikraman
MDL18CS104 51 Sandra Jacob
MDL18CS106 52 Sanjana S
Govt. Model Engineering College
Thrikkakkara

November 28, 2021

Overview

Introduction

- World is seeing a constant increase in the amount of data being produced.
- Difficulty in data management.
- This results in an added advantage to many knowingly or unknowingly, resulting in copyright infringement.

Copyright

It is a form of intellectual property law, protects original works of authorship including literary, dramatic, musical, and artistic works, such as poetry, novels, movies, songs, computer software, and architecture.

Area of the Proposed Project

- Digitalisation has made it considerably easy to copy, replicate and sell the works of a copyright owner without his permission and detection of such infringement becomes difficult
- The issues of copyright law in the digital environment we are trying to solve:
  - Lack of transparency about the legal status of copyrighted works
  - Author's difficulty to get compensated fairly
  - Piracy
  - Copyright violations

Problem statement

- The Internet/digital environment is creating new and newer avenues for rights and consumer privacy violations, and an increasing number of cyber frauds are taken to courts year by year. In practice it is rather difficult to impose copyright law on internet users.
- The project aims to address the serious problem of copyright violations of images and provide a means for owners to protect their work.

Abstract

- We aim to design a web application to upload images, which will be linked to a blockchain network and encrypted according to an algorithm.
- Blockchain is a distributed database that provides a secure, yet transparent way to protect any type of records.
- It provides a proof-of-property solution which will provide a unique ID for claiming the copyright of the image on the system. If any other user tries to upload an image which is already stored in the system, the information of the user will be obtained.

Existing System

Digital Rights Management System

- A set of access control technologies for restricting the use of proprietary hardware and copyrighted works.

Digital Fingerprinting

- It is a steganographic technique which is used to prevent illegal copying and protect the content owner's copyright by embedding identifiers in media such as videos and photos

Digital Watermarking

- Digital watermarking is the process of embedding a digital code (watermark) into a digital content like image, audio, or video.

Disadvantages

- Due to the online availability of content, anyone can download content and make copies.
- There is no way to track the leakage or copyright for the spread of digital material.
- Information about copyright owners is scattered in various databases of publishers, record companies, collecting societies, and other entities, which do not have incentives to share it.
- Watermarking doesn't prevent image copying but we can track down and detect ownership of copied images. Watermarks vanish if someone manipulates the image.

Proposed System

- Image copyright protection system using Blockchain technology along with digital fingerprint
- Image uploading is done using a web portal that sends images to the system's backend
- Backend consists of a Blockchain network, handled by a Blockchain manager
- Blockchain manager is a virtual entity that contains methods for validating the uploaded image with already existing images

Proposed System

- System consists of 3 subsystems
- **Image uploading:** By a web portal, user can either claim the copyright or check the image for copyright issues
- **Generating digital fingerprint:**
  - Pixel by pixel comparison takes a lot of time.
  - Perceptual hash algorithms can be used for comparison of images
  - Common perceptual hash algorithms are aHash, pHash, dHash
  - dHash algorithm tracks gradients
  - Bits are set when left pixel is brighter than right pixel

Proposed system

- **Copyright violation detector:**
  - Hamming distance of digital fingerprints are calculated
  - If hamming distance <=10, then images are quite similar and this instance is most likely to be a copyright violation
  - Information of user is passed to owner
  - Else, not similar images

Papers

- Digital steganography and Watermarking for Digital Images : A review of Current Research Directions
- Photograph Ownership and Authorization using Blockchain
- Encryption-then-Compression-Based Copyright- and Privacy-Protected Image Trading System
- Classification of Watermarking Methods Based on Watermarking Approaches
- Decentralised Image Sharing and Copyright Protection using Blockchain and Perceptual Hashes
- An Overview of Smart Contract: Architecture, Applications, and Future Trends

Oleg Evsutin , Anna Melman and Roman Meshcheryakov, “Digital steganography and Watermarking for Digital Images : A review of Current Research Directions” in IEEE Access, published on September 8, 2020, doi: 10.1109/ACCESS.2020.3022779

Abstract:
In this paper, an overview of promising research in the area of copyright protection for digital objects is provided. First of all, we provide basic information about this field of research and consider the main applications of its methods. Next, we review works demonstrating current trends in the development of methods and algorithms for data hiding in digital images.This review is not exhaustive; it focuses on contemporary works illustrating current research directions in the field of information embedding in digital images. This is the main feature of review, which distinguishes it from previously published reviews. The paper concludes with an analysis of identified problems in the field of digital steganography and digital watermarking.

Advantages:

- Watermarking and steganography is used for protecting digital data and is relevant for various multimedia data, such as images, audio recordings, video files.
- 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.
- Digital watermarks are often used to protect the authorship of multimedia files, to control the integrity of data, and to authenticate the sources of this data. The classic digital watermark application is connected with multimedia protection
- Robust digital watermarks can withstand the most common attacks on the digital watermarks such as rotation, scaling – reducing or increasing the size of the image, compression, noise overlay.

Disadvantages:

- Steganographic techniques make use of open communication channel, which makes it more vulnerable towards steganalysis and makes it less secure.

Kaushal Poudel,Arpan Pokhrel,Arun Babu Aryal, “Photograph Ownership and Authorization using Blockchain”, in 2019 Artificial Intelligence for Transforming Business and Society (AITB), added to IEEE Xplore on 02 January 2020, doi: 10.1109/AITB48515.2019.8947438

Abstract:
This paper describes the integration of blockchain, distributed storage, and peer-to-peer communication in order to solve the current problem of handling photograph ownership and authorization. Ethereum blockchain is implemented to achieve secure transaction and handling functionality regarding authorization with the help of smart contracts that runs on the blockchain. As the storage layer, the paper discusses the InterPlanetary File System (IPFS) as a distributed database with which the photographs can be stored such that decentralization can be achieved. Only after the verifying the similar image does not exist on the system the image is stored in IPFS. The existence of a duplicate image is done with the implementation of dHash algorithm and hamming distance. Whisper protocol allows the owner of the photograph and user on the Ethereum blockchain to leverage peer-to-peer communication to reach a consensus.

Advantages:

- Blockchain is used to keep the decentralized record of ownership
- Storing photographs on the decentralized platform(IPFS) can make it more secure
- Designing a smart contract in which the user and owner can agree on the use of the owner's property can address the problem of unauthorized use.
- Whisper Protocol protects user privacy

Disadvantages:

- Due to the absence of watermarking, copyright identification is not easy to carry out
- No tracing and detection of copyright violators

Wannida Sae-Tang, Masaaki Fujiyoshi, and Hitoshi Kiya. 2017. Encryption-then-Compression-Based Copyright- and Privacy-Protected Image Trading System. In Proceedings of the International Conference on Advances in Image Processing (ICAIP 2017). Association for Computing Machinery, New York, NY, USA, 66–71. DOI:https://doi.org/10.1145/3133264.3133281

Abstract:
This paper proposes an encryption-then-compression (ETC)-based copyright- and privacy-protected image trading system. It focuses on image copyright protection, consumer's privacy protection, and compression-friendliness with accepting any fingerprinting techniques. In the system, the 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. With the same system features, the proposed system gives better performances in terms of visual protection, image quality, compression compatibility, and fingerprinting than those of conventional systems.

Advantages:

- It achieves better performances than those of the conventional systems in terms of visual protection, image quality, compression compatibility, and fingerprinting
- The consumer's information should be protected against a content provider (CP). Therefore, a trusted third party (TTP) was introduced to the system to handle the copyright protection task instead of the CP

Disadvantages:

- Only works for JPEG
- Copyright violation identification, tracing and detection is not implemented

M. Boreiry and M. Keyvanpour, "Classification of watermarking methods based on watermarking approaches," 2017 Artificial Intelligence and Robotics (IRANOPEN), 2017, pp. 73-76, doi: 10.1109/RIOS.2017.7956446.

Abstract:
Watermarking is extremely important when it comes to protecting digital data. One of the main important issues in watermarking operation is the watermarking robustness. The basic requirement in watermarking is resisting in front of distortion and initial attacks, which is commonly examined based on the data processing standards. Many methods have been proposed in the field of video watermarking that are resistant to certain attacks, therefore some attacks can break the watermark. So, the correct identification of methods and knowing the strength and weakness of each method lead to propose appropriate solution in order to reduce the effects of attacks with presenting secure algorithm in video watermarking.

Advantages and disadvantages:

TABLE 1: INVESTIGATION OF VIDEO WATERMARKING METHODS IN SPATIAL DOMAIN

Method	*Main idea*	*advantages*	*Disadvantages*
LSB	This method change pixel value for embedding watermarking.	Resistance to geometric attacks such as removal of inner distance, scaling, rotation, simplicity and lack of computational complexity and conceptual clarity	Fail in facing with cropping attacks, compression, low-pass filter. Robustness restriction, capacity limitation in data storage and low resistance
Spread Spectrum	Each bit of watermark aj is spread over several chips and modulated by a binary pseudo-noise sequence. The watermark is embedded in a vector form. Data recovery is done by the means of high-pass filter.	In this method, by using energetic signal propagation a high resistance can be achieved.	The blind watermarking technique in order to embed the watermark don't use the host signals. Do not specifically protect the value of DC blocks.
A 2D spread spectrum	A watermark pattern S × S is created in the beginning while this pattern is embedded alternatively. Around some points will be chosen to be fixed. After generating the watermark frames using the host masks the spatial mask will be applied on them.	A little calculation will be used in detection algorithm.	This technique in blind watermarking technique that embeds a watermark signal without using host signals will fail. Don't specifically protect from the value of DC blocks.
CDMA	In CDMA technique one of the four least significant bit-planes will be replaced by watermark planes. The random periodic quaternary sequence is used to select the bit-planes that should be replaced.	This method has more data capacity for watermark.	Fail in facing with statistical attacks (average frames)

Figure: Watermarking approaches

Advantages and disadvantages:

method	*Main idea*	*advantages*	*disadvantages*
DCT	First, the host video transforms by using frequency domain methods, then the transformation coefficients domain change for embedding watermark data. Finally, the inverse transformation is used to obtain the image of watermarked video.	Showing more resistance against attacks in compare with spatial domain.	Complicated calculations. High-frequency components tend to remove in compression level.

TABLE 5: COMPARISION BETWEEN METHODS BASED ON CONFIGURATIONS

approach	*method*	*resistance*	*reliability*	*invisibility*	*applicability*	*Time complexity*
Pixel domain approach	SS	acceptable	acceptable	good	good	good
	JAWS	acceptable	acceptable	good	good	good
	CR	good	good	good	poor	poor
	CDMA	acceptable	acceptable	good	acceptable	acceptable
	RBEM	acceptable	acceptable	good	acceptable	acceptable
Compression domain approach	VLC	poor	poor	good	good	good
	H.264	good	good	good	acceptable	acceptable
Transformation domain approach	TDC	good	good	good	acceptable	acceptable
	PW	acceptable	acceptable	good	acceptable	good
	DCT	good	good	good	good	acceptable

R. Mehta, N. Kapoor, S. Sourav and R. Shorey, "Decentralised Image Sharing and Copyright Protection using Blockchain and Perceptual Hashes," 2019 11th International Conference on Communication Systems Networks (COMSNETS), 2019, pp. 1-6, doi: 10.1109/COMSNETS.2019.8711440.

Abstract:
To counter copyright problems, we propose a decentralised peer-to-peer photo sharing marketplace built on top of Ethereum test chain and demonstrate how it is fair, trustworthy and practical. Our decentralised application leverages perceptual hashes and robust smart contracts of Ethereum to automatically detect and reject tampered images that are perceptually similar to images already present on the marketplace. Due to inherent properties of Blockchain, our marketplace has no central authority controlling it, no third party interference, no single point of failure, zero-censorship and preserves online user privacy. To the best of our knowledge, this is the first work that provides a practical solution for automatically detecting and rejecting perceptually similar images on a decentralised image sharing platform, thus protecting the copyrights of genuine image authors.

Advantages:

- Due to the absence of central authority, the marketplace is free from censorship and interference
- The Blockchain transactions only contain IPFS hashes for retrieving images.Thereby reducing the cost of storage in blockchain
- Perceptual hashes are able to detect tampering in the events where modifications made to images are not too extreme and there's still good level of structural similarity between original image and its tampered version

Disadvantages:

- There are some cases for which hashing algorithms fails to identify fraudulent images, like 90 degrees rotated images

S. Wang, Y. Yuan, X. Wang, J. Li, R. Qin and F. Wang, "An Overview of Smart Contract: Architecture, Applications, and Future Trends," 2018 IEEE Intelligent Vehicles Symposium (IV), 2018, pp. 108-113, doi: 10.1109/IVS.2018.8500488.

Abstract:
With the rapid development of cryptocurrency and its underlying blockchain technologies, platforms such as Ethereum and Hyperledger began to support various types of smart contracts. Smart contracts are computer protocols intended to digitally facilitate, verify, or enforce the negotiation or performance of a contract. Smart contracts have broad range of applications, such as financial services, prediction markets and Internet of Things (IoT), etc. However, there are still many challenges such as security issues and privacy disclosure that await future research. In this paper, we present a comprehensive overview on blockchain powered smart contracts. First, we give a systematic introduction for smart contracts, including the basic framework, operating mechanisms, platforms and programming languages. Second, application scenarios and existing challenges are discussed. Finally, we describe the recent advances of smart contract and present its future development trends, e.g., parallel blockchain. This paper is aimed at providing helpful guidance and reference for future research efforts.

Advantages:

Smart contracts have three characteristics, namely, autonomy, self-sufficiency, and decentralization.Autonomy means that after they are launched and executed, the contracts and the initiating agents need not be in further contactSecond, smart contract can be self-sufficient in their ability to marshal resources — that is, raising funds by providing services, and spending them when needed, e.g., gain processing power or storageThird, smart contracts are decentralized as they do not subsist on a single centralized server, they are distributed and self-executed across network nodes

Disadvantages:

- Reentrancy vulnerability: This problem occurs when an attacker utilizes a recursive call function to conduct multiple repetitive withdrawals, while their balances are only deduced once .This may result in unexpected behaviors, even eventually consuming all the gas.
- Due to the immutable nature of blockchain, contracts cannot be modified once they are deployed, so hackers can exploit this vulnerability to attack.

Table

Paper	Methodology	Advantages	Disadvantages
Digital Steganography and Watermarking for Digital Images : A review of Current Research Directions	Watermarking and Steganography	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 channel, which makes it more vulnerable towards steganalysis and makes it less secure
Photograph Ownership and Authorization using Blockchain	Blockchain and IPFS	Designing a smart contract can address the problem of unauthorized use. Whisper Protocol protects user privacy	Watermarking isn't present so copyright identification isn't easy to carry out. No tracing and detection of copyright violators.

Paper	Methodology	Advantages	Disadvantages
Encryption-then-Compression-Based Copyright- and Privacy-Protected Image Trading System	ECT Techniques and Fingeprinting	Better performances than those of the conventional systems in terms of visual protection, image quality, compression compatibility, and fingerprinting	Copyright violation identification, tracing and detection is not done. Only works for JPEG
Classification of Watermarking Methods Based on Watermarking Approaches	Watermarking techniques	Robust watermarking schemes, like DCT and DWT based watermarking techniques are generally more resistant to attacks.	Application of just digital watermarks to images do not guarantee proper copyright protection.

Paper	Methodology	Advantages	Disadvantages
Decentralised Image Sharing and Copyright Protection using Blockchain and Perceptual Hashes	Blockchain and Perceptual Hash	The Blockchain transactions only contain IPFS hashes for retrieving images. Thereby reducing the cost of storage in blockchain. Perceptual hashes are able to detect tampering.	There are some cases for which hashing algorithms fails to identify fraudulent images, like 90 degrees rotated images
An Overview of Smart Contract: Architecture, Applications, and Future Trends	Smart Contracts in Blockchain	Autonomy, self-sufficiency, and decentralization.	Due to the immutable nature of blockchain, hackers can exploit this vulnerability to attack contracts. Reentrancy vulnerability may result in unexpected behaviors, even eventually consuming all the gas.

Problem statement

- With the rise of the Internet, 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 drastic change in output value.
- Inorder to better accomplish the task of copyright protection and violation detection, we analyzed papers and proposed a new system with added features and better efficiency.

Methodology

The aim is to create a system for protecting copyrights and also for detecting violations of copyrights, using Blockchain technology.

- Copyright violation detection, making use of traceability property of Blockchain.
- Similarity of images will be computed using perceptual hashing and Hamming distance which will ensure a much better performance
- Digital fingerprint is generated and digital watermarking is added to it in order to better protect the copyrights
- IPFS is used for decentralized storage, thereby making the system cost effective.
- Smart Contracts are used to automate trusted transactions between owner and user
- Users only need to know how to operate a webpage to use the system.

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] K. Poudel, Arun Babu Aryal, Arpan Pokhrel, Dr. Pranita Upadhyaya, *Photograph Ownership and Authorization using Blockchain*,IEEE Xplore, January 2020

[3] W Sae-Tang ,M. Fujiyoshi ,H. Kiya, *Encryption-then-Compression-Based Copyright- and Privacy-Protected Image Trading System*, ACM Digital Library,August 2017

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

[5] Rishabh Mehta,Naman Kapoor, Soumya Sourav,Rajeev Shorey, *Decentralised Image Sharing and Copyright Protection using Blockchain and Perceptual Hashes* 11th International Conference on Communication Systems Networks (COMSNETS), 2019

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

Thank You!