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

December 4, 2021

Overview

1. Introduction
2. Motivation
3. Problem Statement
4. Abstract
5. Existing System
6. Disadvantages
7. Proposed System
8. Literature Survey
9. Problem Statement
10. Methodology
11. References

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.

Motivation

- 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

Literature Survey

Overview

- 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.
- There are many issues that we come across:
  - Lack of transparency about the legal status of copyrighted works
  - Author's difficulty to get compensated fairly
  - Piracy
  - Copyright violations
- The project aims to address the serious problem of copyright violations of images and provide a means for owners to protect their work.
- We aim to design a web application to upload images, which will be linked to a blockchain network and encrypted according to an algorithm.
- 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.

Papers

1. Digital steganography and Watermarking for Digital Images : A review of Current Research Directions
2. Classification of Watermarking Methods Based on Watermarking Approaches
3. Digital Watermarking with Copyright Authentication for Image Communication
4. Encryption-then-Compression-Based Copyright- and Privacy-Protected Image Trading System
5. Real Time Copyright Protection and Implementation of Image
6. Blockchain: The Perfect Data Protection Tool
7. An Overview of Smart Contract: Architecture, Applications, and Future Trends
8. IPFS - Content Addressed, Versioned, P2P File System
9. Image retrieval using perceptual hashing
10. Blockchain-Watermarking for Compressive Sensed Images

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

Summary:
The development of information technology has led to a significant increase in the share of multimedia traffic in data networks. This has necessitated to solve the following information security tasks in relation to multimedia data: protection against leakage of confidential information, as well as identifying the source of the leak; ensuring the impossibility of unauthorized changes; copyright protection for digital objects. To solve such kind of problems, methods of steganography and watermarking are designed that implement embedding in digital objects hidden information sequences for various purposes.

Basic Concept

- One of the ways to ensure the security of digital data is using steganography and digital watermarking techniques
- Concealing information with the help of steganography and digital watermark embedding is a well-established and developing scientific field.
- Steganography involves the protection of some additional information that is embedded in a digital cover object.
    - The main idea of steganographic methods is to make embedded information invisible to an attacker.
    - secret information could be safely transmitted through an open communication channel
- 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.
    - The classic digital watermark application is connected with multimedia protection.

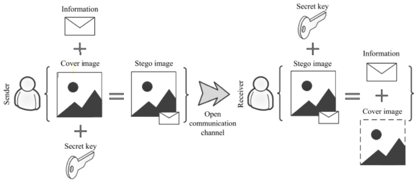
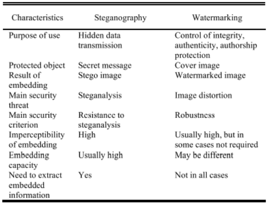


Figure: Information embedding and extracting



Characteristics	Steganography	Watermarking
Purpose of use	Hidden data transmission	Control of integrity, authenticity, authorship protection
Protected object	Secret message	Cover image
Result of embedding	Stego image	Watermarked image
Main security threat	Steganalysis	Image distortion
Main security criterion	Resistance to steganalysis	Robustness
Imperceptibility of embedding	High	Usually high, but in some cases not required
Embedding capacity	Usually high	May be different
Need to extract embedded information	Yes	Not in all cases

Figure: Stegnography vs Watermarking

Figure: Cited from ’Digital steganography and Watermarking for Digital Images : A review of Current Research Directions’

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.
- 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:

- Steganographyic techniques makes use of open communication channel, which makes it more vulnerable towards steganalysis and makes it less secure.
- Algorithms maintain confidentiality, if the algorithms are known then this technique is of no use.
- Password leakage may occur and it leads to the unauthorized access of data.
- Watermarking alone is not a complete solution for access/copy control or copyright protection
- Work in these areas is underway, but there are still a lot of problems that require new original solutions.

M. Boreiry and M. Keyvanpour, "Classification of watermarking methods based on watermarking approaches," 2017 Artificial Intelligence and Robotics (IRANOPEN), 2017

Summary:
Watermarking is extremely important when it comes to protecting digital data. The basic requirement in watermarking is resisting in front of distortion and initial attacks, which is commonly examined based on the data processing standards. Various methods have been proposed in the field of video watermarking that are resistant to certain attacks, but some attacks can break the watermark. So, understanding each method and identification of the correct method is critical. Knowing the strength and weakness of each method helps to reduce the effects of attacks with presenting secure algorithm in video watermarking and proposing an appropriate solution.

Advantages and disadvantages:

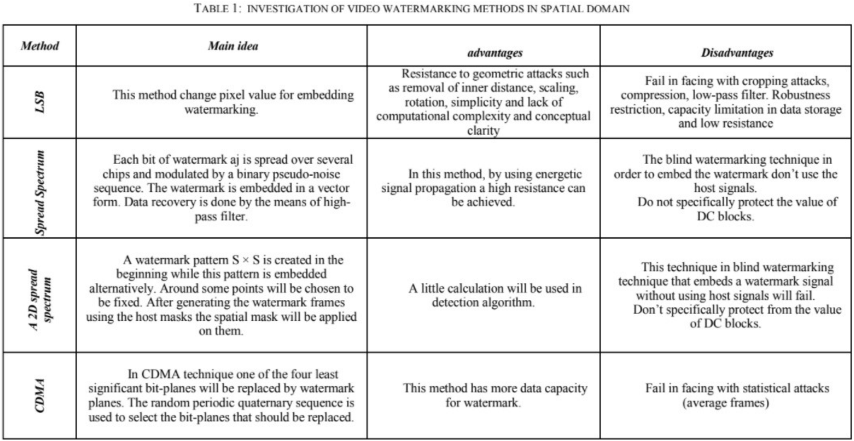
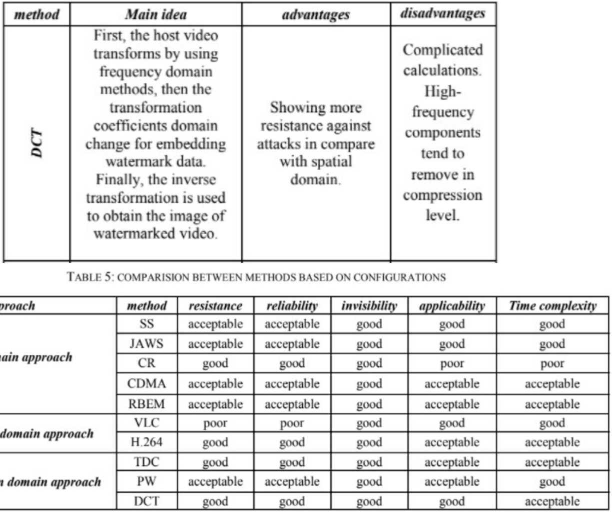


TABLE 1: INVESTIGATION OF VIDEO WATERMARKING METHODS IN SPATIAL DOMAIN

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

Figure: Cited from 'Classification of watermarking methods based on watermarking approaches'

Keta Raval, and Sameena Zafar, "Digital Watermarking with Copyright Authentication for Image Communication", 2013 International Conference on Intelligent Systems and Signal Processing (ISSP)

Summary:
In the context of multimedia communication, digital images and videos have numerous applications in the entertainment world like TV channel broadcasting. The world of digital multimedia communication faces many problems related to security and authenticity of it's digital data. Digital Watermarking algorithms used to protect the copyright of digital images and to verify multimedia data security. 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. The solution is becoming more complex with the growth of data. Here Digital Watermarking by proposed transform Algorithm based on DCT-DWT watermarking is proposed, this helps to do secure image transmission.

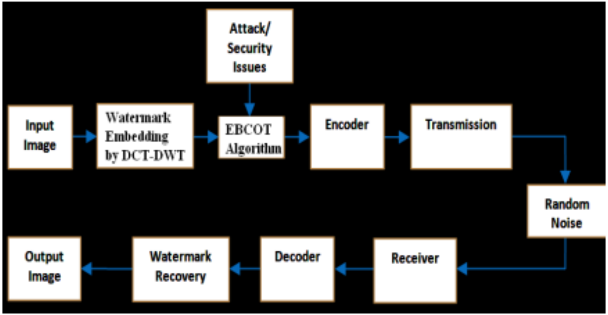


Figure: System Utilization Approach: Cited from 'Digital Watermarking with Copyright Authentication for Image Communication'

Advantages:

- Experiment results shows that recombining the DCT-DWT joint transform algorithm improved the performance of the watermarking
- Error correcting codes reduce almost all random noise that occur over a communication channel.
- Overall system designing in this approach tends to reduce noise and gives security to watermarked message image for desired application purposes.

Disadvantages:

- It increases the potential for unauthorized distribution of such information and significantly increases the problems associated with copyright protection.
- A proper encoding and decoding techniques could remove random noise occur over a communication channel. But on communication channel, watermarked may still be corrupted by noise to some extend.
- The algorithm used helps to store and transmit the watermarked image, but it's prone to attacks/security issues.

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.

Summary:
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.

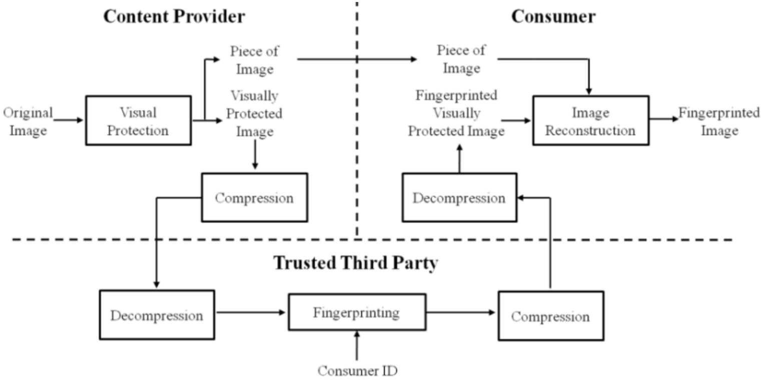


Figure 4. Proposed encryption-then-compression-based copyright- and privacy-protected image trading system.

Figure: Cited from 'Encryption-then-Compression-Based Copyright- and Privacy-Protected Image Trading System

Important requirements

- Visual protection performance
  It should be confirmed that the visual protection method/visual encryption method has good performances in terms of visual protection, security, and decrypted image quality.
- Compression compatibility
  The encryption method should be compression-friendly especially for famous compression standards.
- Fingerprinting performance
  The quality of the fingerprinted image related to the quality of the reconstructed image received by the consumer should be as high as possible, and the fingerprint should be able to be extracted correctly as much as possible.

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

Hashmi, Mohammad Farukh Shukla, Ronak Keskar, Avinash, Real Time Copyright Protection and Implementation of Image and Video Processing on Android and Embedded Platform, December 2015

Summary:
This paper proposes real time copyright protection algorithm using both visible as well as invisible watermarking schemes. The invisible watermarking schema uses DCT analysis, whereas the visible watermarking 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. However, increase in computational complexity is compensated by the speed of implementation and copyright protection is only done, so no way to detect if any violation occurs.

Invisible Watermarking

- Android app is launched, and input frame is obtained from Android Smartphone camera.
- This color frame is converted to grey scale format and then converted to frequency domain by applying DCT.
- After the transformation a small sub-matrix is extracted and binary watermark is added to this. So the size of the sub-matrix is equal to size of the watermark.
- The modified sub-matrix is then copied back to the main transformed frame and IDCT is applied.
- Thus a watermarked frame is obtained.

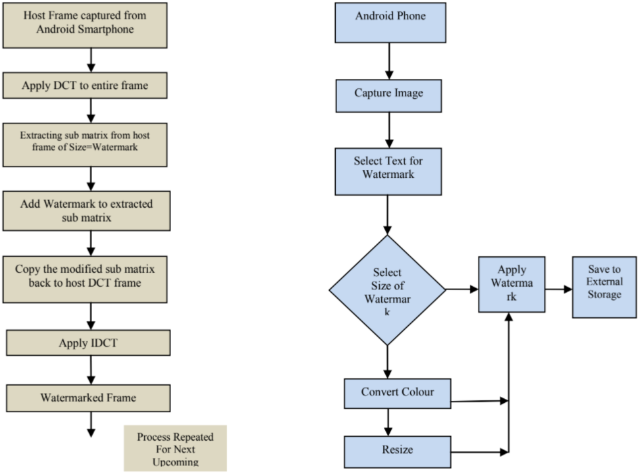

Host Frame captured from Android Smartphone
Apply DCT to entire frame
Extracting sub matrix from host frame of Size=Watermark
Add Watermark to extracted sub matrix
Copy the modified sub matrix back to host DCT frame
Apply IDCT
Watermarked Frame
Process Repeated For Next Upcoming
Android Phone
Capture Image
Select Text for Watermark
Select Size of Watermar k
Apply Waterma rk
Save to External Storage
Convert Colour
Resize

Fig. 1. (a) Block diagram of invisible watermarking

Fig. 1. (b) Block diagram of visible watermarking

Figure: Cited from: "Real Time Copyright Protection and Implementation of Image and Video Processing on Android and Embedded Platform"

Advantages:

- The invisible watermarking process is operated using DCT and so the efficiency of watermarking is high.
- The visible text watermark is also resilient to be removed by common image processing algorithms
- The watermark embedding process is automatic, with the watermark being embedded on each frame of the captured video as soon as we launch the application

Disadvantages:

- The increase in computational complexity is compensated by the speed of implementation.

A. Nayak and K. Dutta, "Blockchain: The perfect data protection tool," 2017 International Conference on Intelligent Computing and Control (I2C2), 2017

Summary:
Blockchain is a distributed ledger technology which maintains a list of records that goes on increasing continuously known as blocks that 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 provides a high level of security, anonymity and data integrity without any intervention from a third party who is in control of the transactions. In this study they have carried out a well-defined study with an aim of collecting all relevant research areas and technologies on Blockchain Technology. 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 since it has the potential to revolutionize the existing technology, it feels right.

Fundamental Elements of Blockchain

- Decentralization – Distributing control among all peers in the transaction chain instead of having one central authority controlling everything within an ecosystem. Thus the technology works on the principle of a shared infrastructure
- Digital Signature - An exchange of transactional value using unique digital signatures that rely on public and private keys to create an authentic proof of ownership
- Mining - Verification of transactions before they are added into Blockchain and after mining, digital signatures are stored in blocks using strict cryptographic patterns.
- Data Integrity - To prevent tampering of transaction data as agreed upon, the use of complex algorithm and consensus helps in ensuring data safety

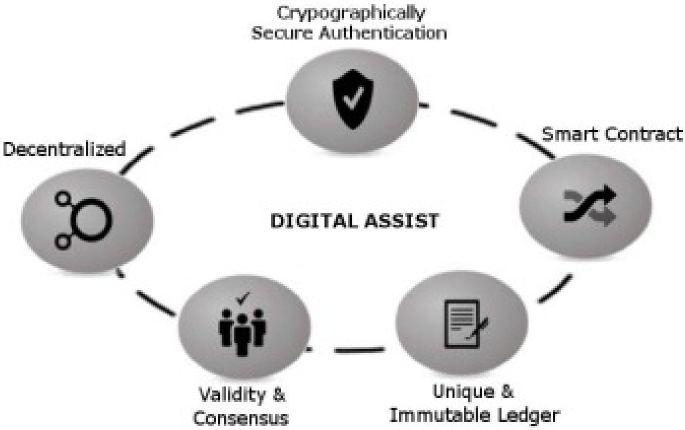


Figure: Cited from: "Blockchain: The Perfect Data Protection Tool"

Advantages:

- The significant advantage of blockchain is the method of transactions which are verified and trackable.
- Use of blockchain can aid in preservation of records, evidence and institutional memory because data that has been recorded on the blockchain is difficult to alter and not under the control of one party
- Blockchain has the potential to reduce workload of multiple stakeholders where transactions and contracts can be kept on a shared ledger and it also has the ability to provide a consistent contract execution environment automatically
- Transactions records can be placed in the Blockchain network within a very short period of time, thus reducing delivery times and document collection.

Disadvantages:

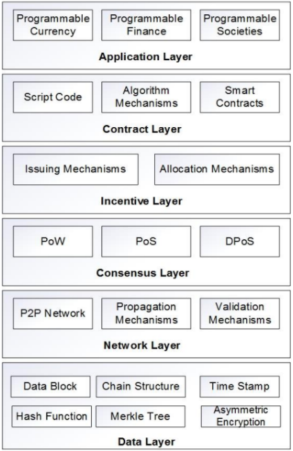
- Privacy is a concern. Question arises on who should have access to the data.
- Market disruption may result as one of the cons of blockchain. It could replace all of the current procedures where participants trade directly.

S. Wang, Y. Yuan, X. Wang, J. Li, R. Qin and F. Wang, "An Overview of Smart Contract: Architecture, Applications, and Future Trends", IEEE Intelligent Vehicles Symposium (IV), 2018

Summary:
This paper presents a comprehensive overview on Blockchain powered Smart Contracts. First, it gives a systematic introduction for smart contracts, including the basic framework, operating mechanisms, platforms and programming languages. Second, it discusses application scenarios and existing challenges. Finally, it describes the recent advances of smart contracts and presents its future development trends. This 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.

Basic concept:

- Smart contracts are programs within decentralized Blockchains that get executed automatically when specified conditions are fulfilled
- Negates the need for a third party
- Ethereum platform - Solidity, Hyperledger fabric - Golang
- Use cases : financial transactions, market prediction, voting systems



Programmable Currency | Programmable Finance | Programmable Societies

Application Layer

Script Code | Algorithm Mechanisms | Smart Contracts

Contract Layer

Issuing Mechanisms | Allocation Mechanisms

Incentive Layer

PoW | PoS | DPoS

Consensus Layer

P2P Network | Propagation Mechanisms | Validation Mechanisms

Network Layer

Data Block | Chain Structure | Time Stamp

Hash Function | Merkle Tree | Asymmetric Encryption

Data Layer

Figure 1. A basic framework of blockchain.

Figure: cited from: "An Overview of Smart Contract: Architecture, Applications, and Future Trends"

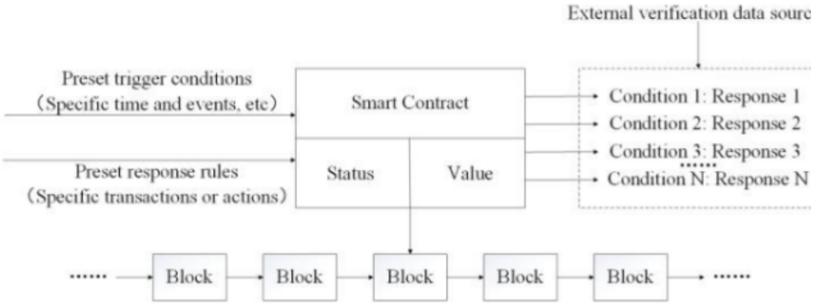


Figure 2. The operating mechanisms of smart contract.

Figure: cited from: "An Overview of Smart Contract: Architecture, Applications, and Future Trends"

Advantages:

- **Autonomy**: After launch and execution, the contracts and the initiating agents need not be in further contact
- **Self-sufficient**: Ability to find resources
- **Decentralized**: They do not subsist on a single centralized server, they are distributed and self-executed across network nodes

Disadvantages:

- **Reentrancy vulnerability:** Utilizing recursive call function to conduct multiple repetitive withdrawals from transactions, while their balances are only deduced once, leads to unexpected behaviours
- **Transaction-Ordering Dependence:** When several dependent transactions occur, miners can set arbitrary order between transactions and can also modify them for exploitation
- **Lacking of trustworthy data feeds:** Smart contracts sometimes require information from external resources. However, the reliability of the information can not be guaranteed.
- Due to the **immutable nature** of blockchain, contracts cannot be modified once they are deployed, so hackers can exploit this vulnerability to attack.

Benet, Juan, "IPFS: Content addressed, Versioned, P2P File System", Research Gate, 2014

Summary:
First, this paper explains about HTTP and Git, the two earliest versions of a global distributed system. It also discusses about how a global distributed file system is needed for handling large multimedia content as well as large datasets and for file sharing. Then, this paper talks 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.

Basic concept:

- HTTP : basic file sharing distributed system, but not all advancements have been utilised properly
- Git : the distributed source code version control system, developed many useful ways to model and implement distributed data operations
- IPFS : Peer-to-peer distributed file system that seeks to connect all computing devices with the same system of files
  - Principle: modeling all data as part of the same Merkle DAG
  - Peer-to-peer-no special privileges for any node
  - Nodes store IPFS objects in local storage, connect to each other and transfer objects.
- IPFS Usecase : Encrypted file or data sharing system, as a database.

Advantages:

- This system can be used as an encrypted file or data sharing system.
- Content addressing - All data stored in IPFS has a specific hash value, which is unique, and content can be searched through the hash value.
- Tamper-proof - Data is verified with its checksum, so if the hash changes, then IPFS will know the data is tampered with.
- Elimination of redundancy - The same files in the IPFS network will only be stored once, saving storage space.

Disadvantages:

- IPFS installation has a lot of hassles, it is not very user friendly.
- IPFS consumes a lot of bandwidth which is not appreciated by metered internet users.

Sarohi, Harsh Kumar, and Farhat Ullah Khan, "Image Retrieval Using Perceptual Hashing", IOSR Journal of Computer Engineering (IOSR-JCE), 2013

Summary:
This paper mainly focuses on retrieving image from content. It proposes 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 paper also proposes a hash algorithm that is robust and secure to non-malicious manipulation and sensitive to the malicious tampering.

Basic concept:

- For searching in large image data sets, two solutions are available:
    - **Image annotation:** Images are tagged and meta-data is attached to images, then keywords are used in search interface for getting specific image. Tagging of images is time consuming, leads to inefficient data storage and every image cannot be described in the form of keywords.
    - **Content Based Image Retrieval:** Images are retrieved based on content of an image. Two major steps - Feature extraction algorithm, Matching algorithm
      Feature extraction algorithm processes the image and compute feature vector, which is used for the extraction of information from data set
      Matching algorithm performs comparison between extracted features of images to check whether they are similar or not and up to what extent they match

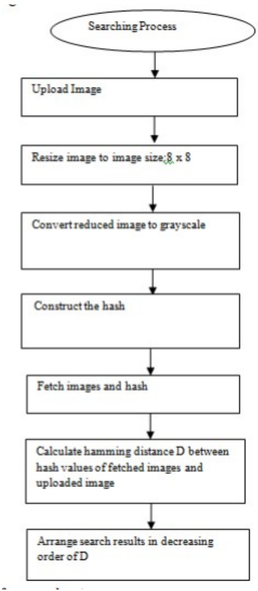

Searching Process
Upload Image
Resize image to image size:8 x 8
Convert reduced image to grayscale
Construct the hash
Fetch images and hash
Calculate hamming distance D between hash values of fetched images and uploaded image
Arrange search results in decreasing order of D

Figure: Cited from "Image Retrieval Using Perceptual Hashing"

Advantages:

- The paper focuses only on efficient retrieval based on color, it uses color spaces and hamming distance to construct hash
- The process requires low computation cost and satisfactory performance.
- Compared to cryptographic hashes, perceptual hashes are better since they do not have avalanche effect

Disadvantages:

- Storage mentioned in the paper does not provide a safe storage
- This system focuses on only image retrieval
- This is a subset of our proposed solution
- dHash algorithm is better than aHash

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

Summary:
This paper proposes 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.

Proposed System

- **Generation and Uploading of the Watermark**
  - First, the image is processed by compressed sensing. Then, generate a feature watermark.
  - Designing an actual watermark
  - Uploaded to IPFS
- **Extraction and Detection of the Watermark**
  - Entering the contract address to find the corresponding contract, and downloading the uploaded blockchain watermark from the IPFS network
  - The actual watermark can be obtained by combining the blockchain watermark and the feature watermark.
  - Comparing the obtained actual watermark with the original actual watermark, the tampered area can be found

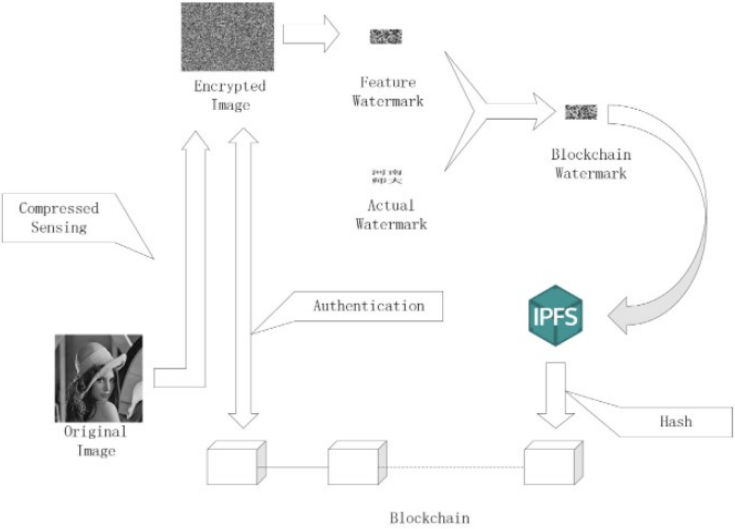


FIGURE 3. **Schematic diagram of the process.**

Figure: Cited from "Blockchain-Watermarking for Compressive Sensed Images"

Advantages:

- Blockchain watermark is introduced which combines the feature watermark(extracted from the features of the image) and actual watermark of the owner.
- Uses IPFS to store the watermark thereby reducing the storage cost.
- By a smart contract, the file is uploaded to the blockchain, and a string of hash values will be generated. The hash value is the contract address of the transaction.That'll be saved in the IPFS.

Disadvantages:

- This system doesn't detect copyright violations only creates watermark for content

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
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
Digital Watermarking with Copyright Authentication for Image Communication	Digital Watermarking based on DCT-DWT watermarking	DCT-DWT joint transform algorithm improves the performance of the watermarking	It increases the potential for unauthorized distribution of info.
Encryption-then-Compression-Based Copyright- and Privacy-Protected Image Trading System	ECT Techniques and Fingerprinting	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

Paper	Methodology	Advantages	Disadvantages
Real Time Copyright Protection and Implementation of Image	Watermarking on android or embedded platforms	Efficiency of watermarking is high.The visible text watermark is also resilient to be removed by common image processing algorithms .The watermark embedding process is automatic	Increase in computational complexity is compensated by the speed of implementation.
Blockchain: The Perfect Data Protection Tool	Blockchain technology	Transactions are verified and trackable.Distributing control among all peers in the transaction chain	Privacy is a big concern. Main question that arises is who should have access to the data

Paper	Methodology	Advantages	Disadvantages
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
IPFS - Content Addressed, Versioned, P2P File System	IPFS with P2P File System	System can be used as an encrypted file or data sharing system and is a linked communications platform,Content addressing ,Tamper-proof ,Elimination of redundancy	IPFS installation has a lot of hassles, it is not at all user friendly. IPFS consumes a lot of bandwidth

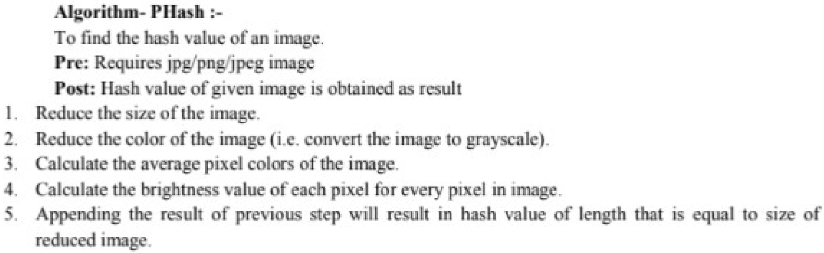
Paper	Methodology	Advantages	Disadvantages
Image Retrieval using Perceptual Hashing	Perceptual Hashing	The process requires low computation cost and satisfactory performance.Compared to cryptographic hashes, perceptual hashes are better since they do not have avalanche effect	The hashing algorithm is primitive, dhash is the better option.It only focuses on image retrievals
Blockchain-Watermarking for Compressive Sensed Images	Blockchain watermarking and IPFS	Blockchain watermark is introduced which combines the feature watermark(extracted from the features of the image) and actual watermark of the owner.Uses IPFS to store the watermark thereby reducing the storage cost	This system doesn't detect copyright violations only creates watermark for content

Omkar Dedge,Rohit Shingade, Abhiraj Jagtap, Apurva Yadav , Asmita Kamble *Image Copyright Protection System Using Blockchain* International Journal of Future Generation Communication and Networking, July 2020

Summary:
This paper has proposed a model of image copyright protection using blockchain. There are many methods to protect the images such as disabling right clicks, disabling external linking of websites, digital watermarking and many more. Adding a digital watermark makes it easier to identify that the image is copyrighted. Blockchain stores the images securely and also provides the proof-of-property for the copyright holder. This system also provides a cross-check functionality for commercial users to avoid copyright issue by checking whether the image is copyrighted or not.

To provide copyright protection to an image there are three steps to follow:

- **Image Uploading**
  - Uploading of the images is facilitated by the use of web portal where the user can either claim the copyright or check the image for any copyright issues if the images is to be used commercially.
- **Image Verification**
  - In this step the image hash will be calculated and cross-verified with all the blockchain records and thus giving the result whether the image already exists in blockchain or not.
  - By using the following algorithm, the images are compared and they get the same hash values if the images are equal. By using hamming distance of these hash values we will be able to determine how similar these images are.



Algorithm- PHash :-

To find the hash value of an image.

Pre: Requires jpg/png/jpeg image

Post: Hash value of given image is obtained as result

1. Reduce the size of the image.
2. Reduce the color of the image (i.e. convert the image to grayscale).
3. Calculate the average pixel colors of the image.
4. Calculate the brightness value of each pixel for every pixel in image.
5. Appending the result of previous step will result in hash value of length that is equal to size of reduced image.

- **Acknowledge Copyright**
  - If the similarity is above the threshold value, image is rejected and the user gets acknowledgement about the request or else if the image is accepted then it is added to all the blockchains as a new record and image is digitally watermarked implying that the image is now copyrighted.
  - User get a receipt containing the unique id to claim copyright on the system.

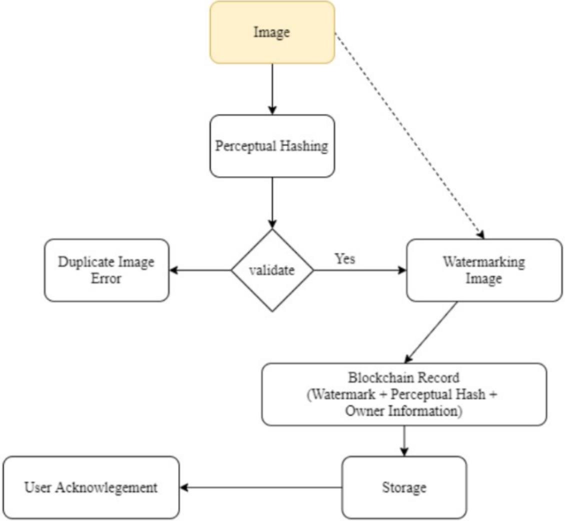


Figure: Cited from "Image Copyright Protection System Using Blockchain"

Problem statement

- With the evolution of the 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 drastic change in output value.
- Inorder to better accomplish the task of copyright protection and violation detection, we analyzed papers and have come to the conclusion that there is a need for a **global system for copyright protection and violation detection using blockchain technology along with IPFS and utilizing DCT watermarking technique and Perceptual Hashing Algorithms.**

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

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, Avinash. *Real Time Copyright Protection and Implementation of Image and Video Processing on Android and Embedded Platform*, December 2015

References

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

[7] 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

[8] Benet, 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*, in IEEE Access, April 2021

Thank You!