CSE DEPARTMENT

GUIDE

Dr. K Lokeshwaran

Image Copyright Protection Based on Blockchain and Zero-Watermark

TEAM

Santhosh S - 510619104059
Mohammed Sufiyan TM - 510619104047
Mohammed Yusuf Khan K - 510619104048
Hari Prasanth S - 510619104701

ABSTRACT

- This project aims to explore the use of blockchain and zero-watermark technology for image copyright protection.
- The protection of digital images is crucial in the digital age, and the existing methods have limitations.
- Blockchain and zero-watermark technology have the potential to provide a secure and decentralized solution for image copyright protection.

INTRODUCTION

- The digital age has increased the risk of copyright infringement, particularly in the case of digital images.
- The current methods for image copyright protection, such as digital watermarks, have limitations in terms of security and scalability.
- Blockchain and zero-watermark technology offer a more secure and decentralized solution for image copyright protection.

ZERO-WATERMARK TECHNOLOGY

- Zero-watermark technology is a method of embedding an invisible and unique signature into an image.
- Unlike traditional digital watermarks, zero-watermarks are imperceptible and cannot be removed or altered.
- This technology provides a more secure and tamper-proof method of image copyright protection.

LITERATURE SURVEY - EXISTING PROBLEM

Title: Zero-Watermarking for Vector Maps Combining Spatial and Frequency Domain Based on Constrained Delaunay Triangulation Network and Discrete Fourier Transform

Author: Baoyuan Wu „ SiweiLyu. Bao-GangHu, QiangJi

Advantages:

- The vector map zero-watermarking scheme combines spatial and frequency domain methods, enhancing its robustness and security. The scheme is resistant to cropping attacks, compression, geometric attacks, and coordinate system transformations.

Disadvantages:

- The standard zero-watermarking algorithm is vulnerable to cropping attacks, and its robustness is not comprehensive enough. The proposed scheme requires feature point extraction and constraint Delaunay triangulation networks, which may increase computational complexity.

LITERATURE SURVEY – EXISTING PROBLEM

Title: Digital Image Copyright Protection Method Based on Blockchain and Perceptual Hashing

Author: Qiu-Yu Zhang and Guo-Rui Wu

Advantages:

- Enhanced transparency and credibility of digital image copyright information. Utilization of blockchain features such as tamper resistance, decentralization, and traceability.

Disadvantages:

- The need for additional computational resources and infrastructure for blockchain implementation.

LITERATURE SURVEY - EXISTING PROBLEM

Title: A Blockchain-Based Scheme for Secure Sharing of X-Ray Medical Images.

Author: Bing-qi Liu1, Ming-zhe Liu1* , Xin Jiang1, Fei-xiang Zhao1, Rui-li Wang2

Advantages:

- Secure sharing and trading of X-Ray medical image data based on blockchain. Protection against privacy disclosure, tampering, and data theft.

Disadvantages:

- Requires adherence to blockchain protocols and infrastructure for implementation

LITERATURE SURVEY – EXISTING PROBLEM

Title: PCPT and ACPT: Copyright Protection and Traceability Scheme for DNN Model

Author: Xuefeng Fan, Hangyu Gui, and Xiaoyi Zhou

Advantages:

- Copyright protection and traceability framework for DNN models. Improved traceability mechanism and stricter authorization control.

Disadvantages:

- Potential computational overhead due to an additional class of DNN models and authorization control mechanisms.

PROPOSED SYSTEM

Modules for the proposed system include:

1) Image uploading
2) Hashing process
3) Generation of Blockchain
4) QR code process
5) Generation of results & Verification

IMAGE UPLOADING

The first module of the proposed system is image uploading. Users can upload their images to the platform. The system will then store these images in a secure database. The image uploading module is the first step in the copyright protection system based on blockchain and zero watermark. The user uploads the digital image to the platform. The system will then store the image in a secure database. The image will be used later to generate the hash code and the QR code.

HASHING PROCESS

The second step in the proposed system is the hashing process. In this step, the digital image is transformed into a unique hash code using cryptographic algorithms. The hash code is a fixed-length alphanumeric string that is unique to the image. The hash code serves as the digital fingerprint of the image, and any changes made to the image will result in a different hash code.

There are different cryptographic algorithms that can be used to generate the hash code, such as SHA-256 or SHA-3. These algorithms are designed to be collision-resistant, meaning that it is computationally infeasible to find two different images with the same hash code. The hash code is stored on the blockchain network, along with the timestamp of the upload and other necessary details.

GENERATION OF BLOCKCHAIN

Once the hash code is generated, the system creates a new block on the blockchain network. The blockchain is a decentralized, distributed ledger that contains a growing list of records, called blocks. Each block contains the hash of the previous block, a timestamp, and transaction data. The hash of the previous block ensures the integrity and immutability of the blockchain.

In our system, the hash code generated in the hashing process is added to a new block on the blockchain network. This block contains the hash code, the timestamp of the upload, and other necessary details. Once the block is created, it is added to the existing blockchain network, creating a secure and transparent record of the image's existence.

QR CODE PROCESS

The next step in the proposed system is the generation of the QR code. QR code is a two-dimensional barcode that contains information about the image, such as the hash code and the timestamp of the upload. The QR code can be easily scanned using a mobile device to verify the authenticity of the image.

The QR code is generated based on the hash code and the timestamp of the upload. The QR code is stored on the platform and can be easily accessed by the user.

GENERATION OF RESULTS AND VERIFICATION

The final step in the proposed system is the generation of results and verification. Users can verify the authenticity of an image by scanning the QR code using their mobile devices. The system will retrieve the hash code and timestamp from the QR code and compare them with the hash code and timestamp stored on the blockchain network.

If the hash code and timestamp match, the system will display a message confirming the authenticity of the image. If the hash code and timestamp do not match, the system will display a message stating that the image is fraudulent. This provides a secure and transparent method for verifying the authenticity of digital images, which will be useful for artists, photographers, and other creators who want to protect their intellectual property rights.

SYSTEM METHODOLOGY

Implementation is the stage of the project when the theoretical design is turned out into a working system. Thus it can be considered to be the most critical stage in achieving a successful new system and in giving the user, confidence that the new system will work and be effective.

The implementation stage involves careful planning, investigation of the existing system and its constraints on implementation, designing of methods to achieve changeover, and evaluation of changeover methods.

WATERMARK BIT EMBEDDING AND DECODING:

Generally, watermarking involves the selection of a watermark carrier, and the design of two complementary processes: embedding and decoding. In the registration, we collect the watermark signature... The watermark embedding process inserts the information by a slight modification of some properties of the carrier.

The watermark decoding process detects and extracts the watermark (equivalently, determines the existence of a given watermark). To correlate encrypted connections, we propose to use inter-packet timing as the watermark carrier property of interest.

CORRELATION ANALYSIS:

In practice, the number of packets available is the fundamental Limiting factor to the achievable effectiveness of our watermark-based correlation. This set of experiments aims to compare and evaluate the correlation effectiveness of our proposed active watermark-based correlation and previous passive timing-based correlation under various timing perturbations.

By embedding a unique watermark into the inter-packet timing, with sufficient redundancy, we can make the correlation of encrypted flows substantially more robust against random timing.

WATERMARK TRACING MODEL:

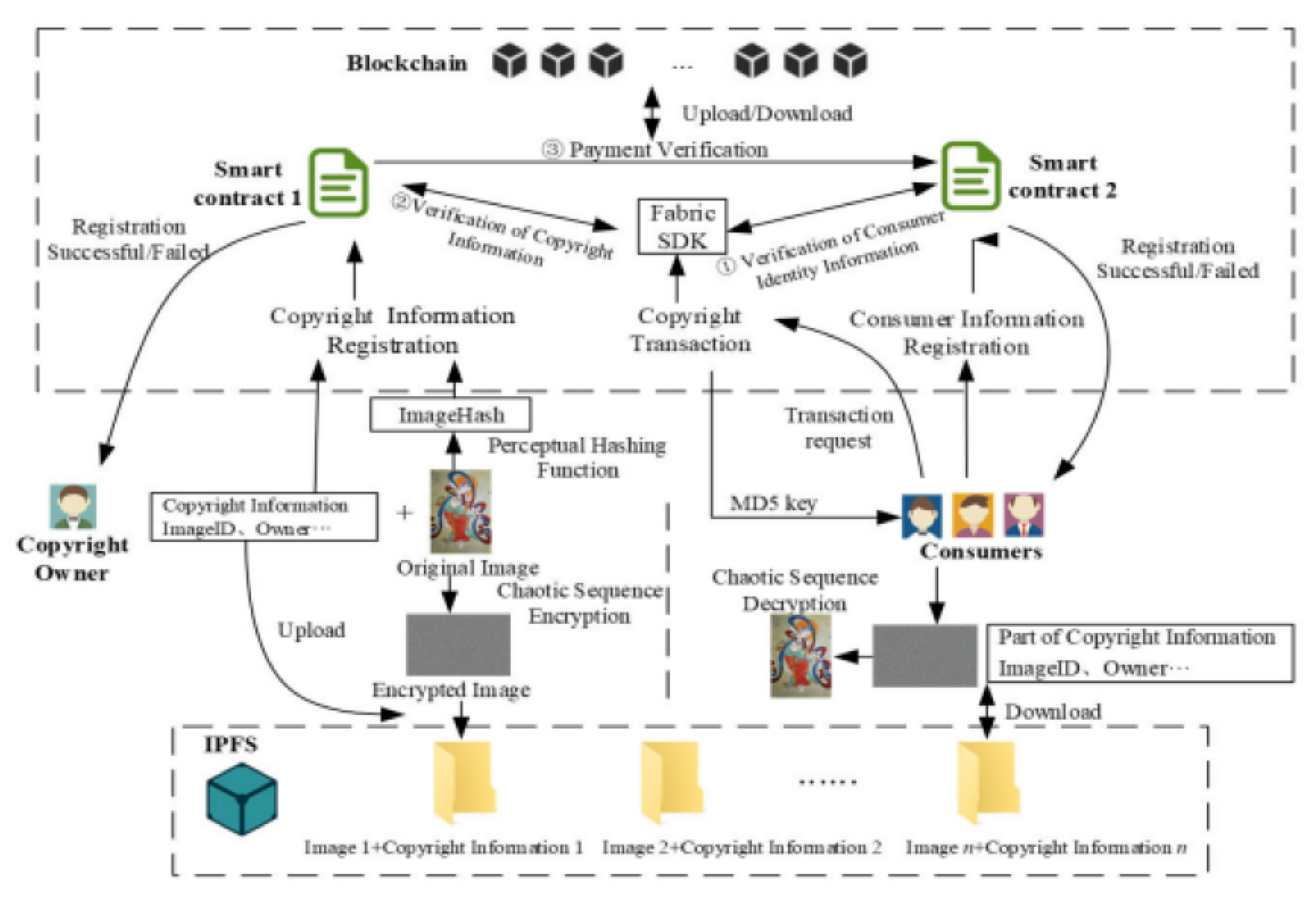
The watermark tracing approach exploits the observation that interactive connections are bidirectional. The idea is to watermark the backward traffic (from the victim back to the attacker) of the bidirectional attack connections by slightly adjusting the timing of selected packets. If the embedded watermark is both robust and unique, the watermarked back traffic can be effectively correlated and traced across stepping stones, from the victim all the way back to the attacker, assuming the attacker has not gained full control of the attack target, the attack Target will initiate the attack tracing after it has detected the attack.

PARAMETER & MAPPING RANDOMIZATION:

One simple technique to achieve this is to use a secret key to generate a pseudo-random sequence of numerical values and add them to either or both of and the pixels in the watermarking area. This technique is hereinafter referred to as parameter randomization. This parameter exchange does not affect the effectiveness of lossless recoverability, because we can now recover the original pixel values by the compound mappings.

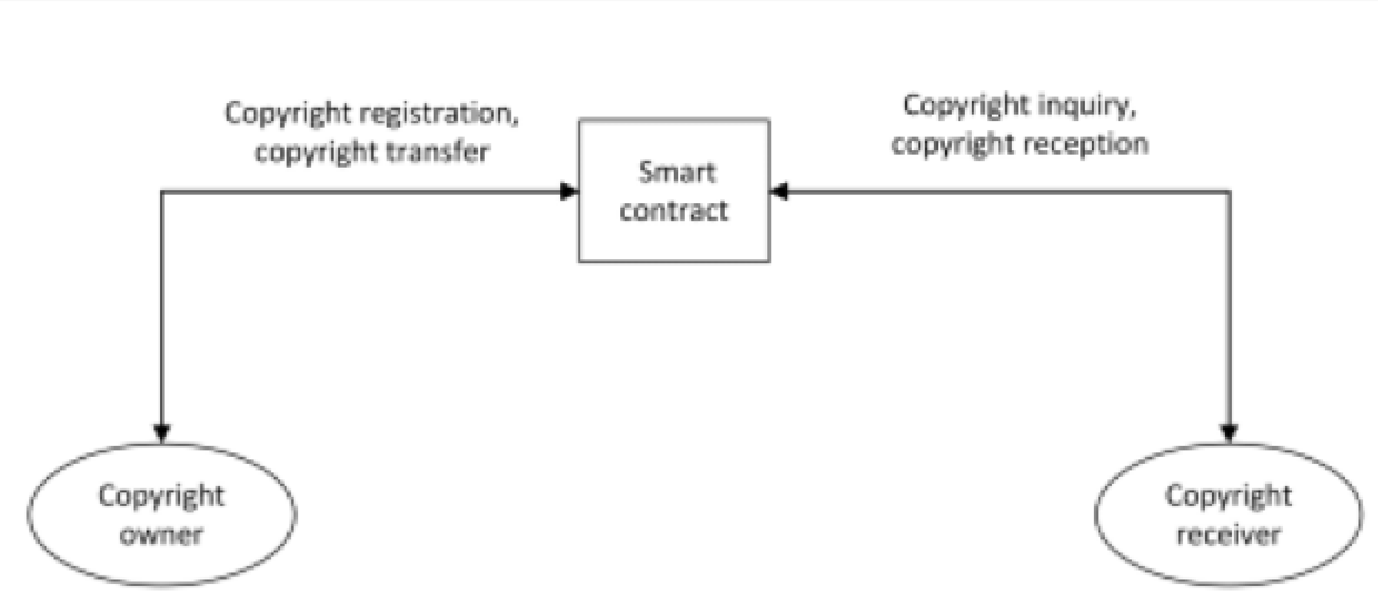
We will refer to this technique in the sequel as mapping randomization. We may also combine this technique with the parameter randomization technique to enhance security. Finally, the Authenticated user takes the file in zip format with the proper password.

SYSTEM DESIGN


Blockchain
...
Upload/Download
③ Payment Verification
Smart contract 1
Smart contract 2
②Verification of Copyright Information
Fabric SDK
① Verification of Consumer Identity Information
Registration Successful/Failed
Registration Successful/Failed
Copyright Information Registration
Copyright Transaction
Consumer Information Registration
ImageHash
Perceptual Hashing Function
Transaction request
MD5 key
Copyright Owner
Copyright Information
ImageID、Owner···
+
Original Image
Chaotic Sequence Encryption
Consumers
Chaotic Sequence Decryption
Upload
Encrypted Image
Part of Copyright Information
ImageID、Owner···
Download
IPFS
······
Image 1+Copyright Information 1
Image 2+Copyright Information 2
Image n+Copyright Information n

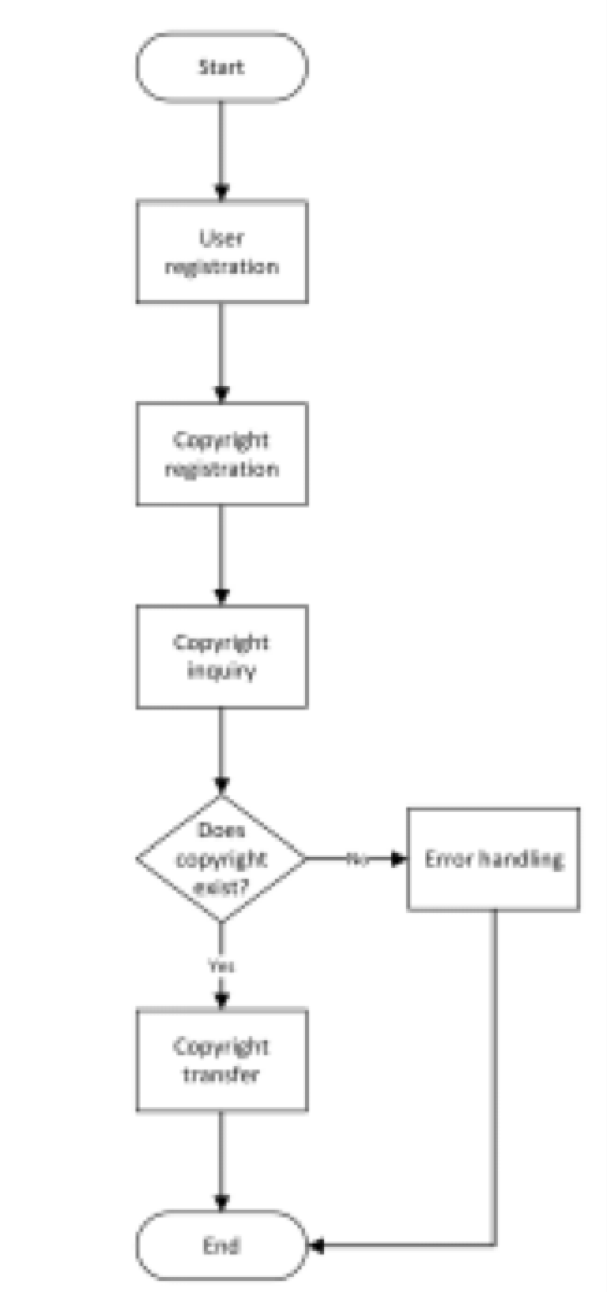
PROJECT PLANNING

LEVEL 0:



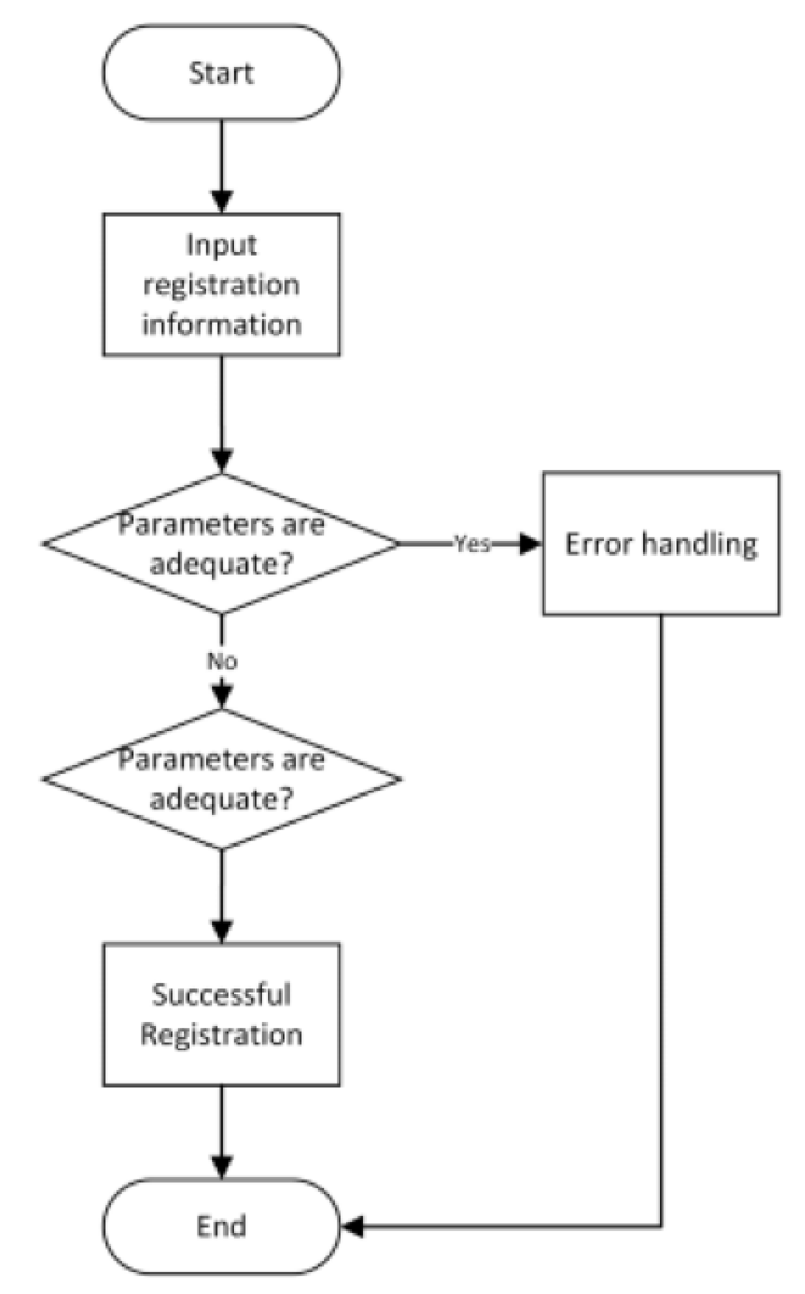
Copyright registration, copyright transfer
Smart contract
Copyright inquiry, copyright reception
Copyright owner
Copyright receiver

LEVEL 1:

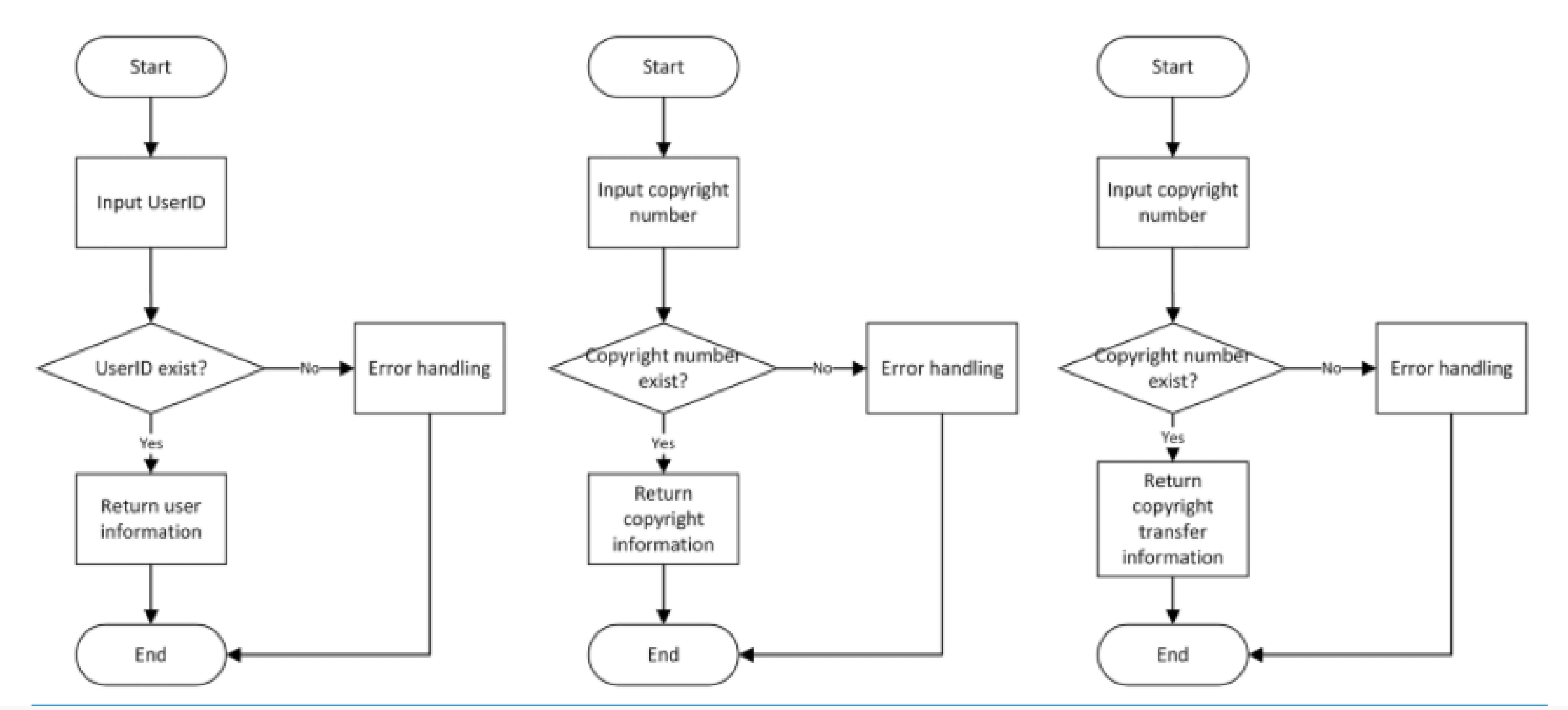


PROJECT PLANNING

LEVEL 2:



LEVEL 3:



ALGORITHM IMPLEMENTATION

Message-digest algorithm (MD5)

1. Algorithm 1 User registration

Input: username, userId, tel, address, password, gender

Output: if successful, return transaction data else throw an exception

Description: Before writing the user information to the blockchain, the user information is authenticated. If all the steps are passed normally, the user Register function will call the JSON. Marshal interface for the data sequence and then stub.PutState will be called to store the data on the blockchain.

ALGORITHM IMPLEMENTATION

2. Algorithm 2 Registration of copyright information

Input: digitalrightName, digitalrightId, digitalrightType, metadata, owner

Output: if successful, return transaction data else throw an exception

Description: Before writing the copyright information into the blockchain, it will first verify the legality of the copyright information and checks whether the copyright (digitalrightId) number already exists or not. If the copyright information is legal and valid, it will verify whether the copyright owner (owner) has been registered already. If so, the registered user will first serialize and then deserialize the user's copyright information to update user information.

ALGORITHM IMPLEMENTATION

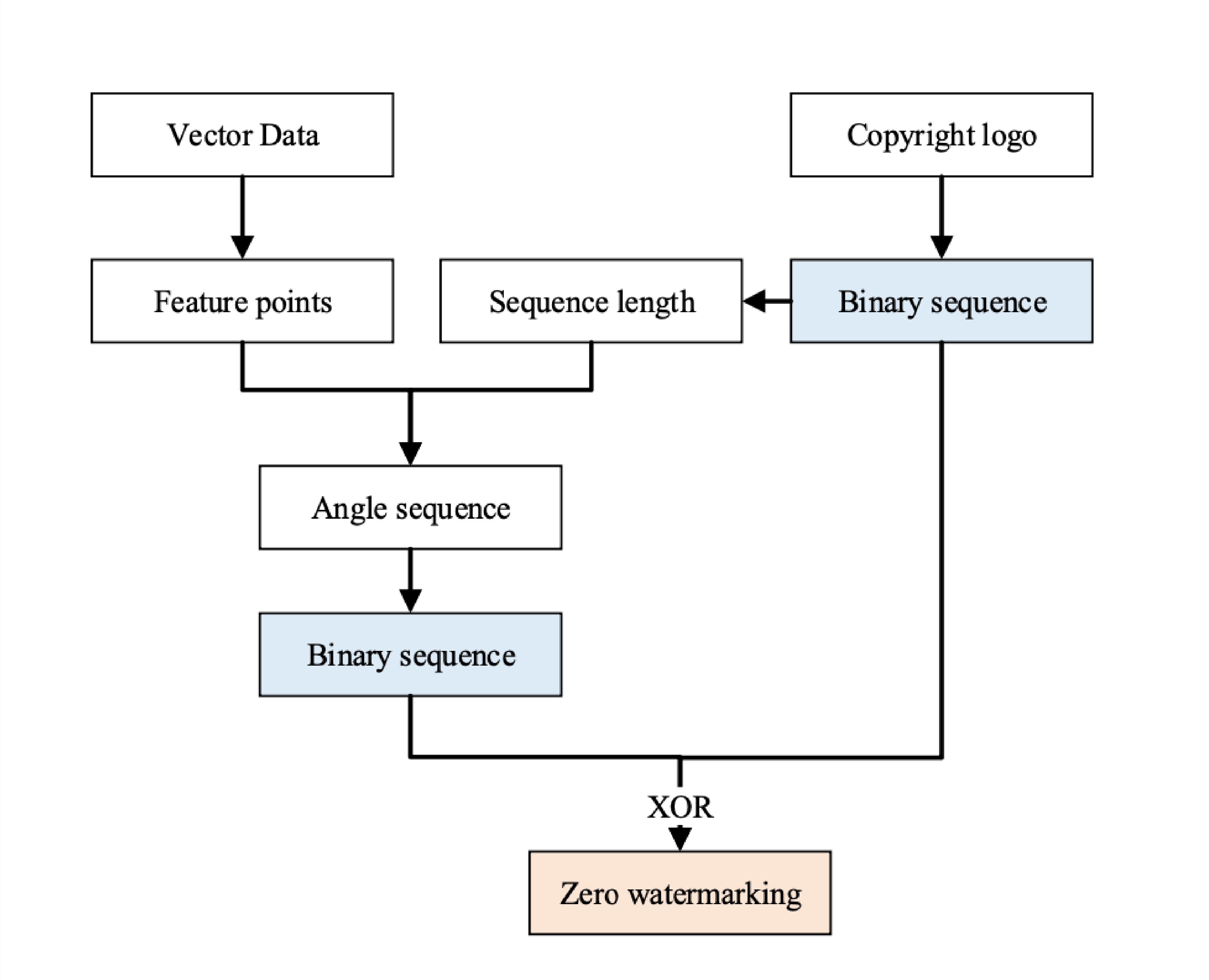
3. Algorithm 3 Copyright transfer

Input: digitalrightId, ownerId, currentownerId

Output: if success, return transaction data else throw an exception

Description: While performing the copyright transfer, it will first check whether the copyright number (digitalrightId) of the copyright to be transferred exists. If it exists, it will match whether the current owner is currently entered (ownerId) and whether the transaction user (currentownerId) is a registered user. After completing the verification, the acquired user information gets serialized and then deserialized to update the copyright information.

EMBEDDING ZERO-WATERMARK INTO THE IMAGE



STORING THE IMAGE AND SIGNATURE ON THE BLOCKCHAIN

- The image and its corresponding signature are stored on the blockchain, which is a distributed and tamper-proof system.
- The blockchain provides a decentralized and secure method of storing and managing digital assets, including images.
- The image and signature are linked to a unique identifier, making it easy to verify the ownership and authenticity of the image.

VERIFICATION OF IMAGE OWNERSHIP THROUGH SMART CONTRACTS

- Smart contracts are self-executing contracts that can automatically verify and enforce the terms of a transaction.

- In the proposed architecture, smart contracts are used to verify the ownership of the image and its corresponding signature.

- The smart contract checks the image and signature against the blockchain, ensuring that the image belongs to the rightful owner.

USE CASES OF IMAGE COPYRIGHT PROTECTION USING BLOCKCHAIN AND ZERO-WATERMARK

The proposed architecture for image copyright protection using blockchain and zero-watermark technology can be applied to various use cases, including:

- Protection of digital artwork and photography
- Protection of stock images and media content
- Protection of personal and corporate images

TECHNICAL IMPLEMENTATION

The technical implementation of the proposed architecture involves several steps, including:

- Embedding the zero-watermark into the image using a mathematical algorithm
- Storing the image and signature on the blockchain
- Verifying the ownership of the image through smart contracts
- Implementing a user interface for uploading and verifying images

LIMITATIONS

Although blockchain and zero-watermark technology offer significant advantages for image copyright protection, there are also limitations to their use, including:

- High computational requirements for embedding zero-watermarks into images
- Limitations in terms of the number of images that can be stored on the blockchain
- The need for a robust and secure smart contract system for verification and ownership checks

ADVANTAGES OF BLOCKCHAIN AND ZERO-WATERMARK OVER TRADITIONAL METHODS

The use of blockchain and zero-watermark technology for image copyright protection offers several advantages over traditional methods, including:

- Immutability: Once the zero-watermark is embedded in the digital content and stored on the blockchain, it becomes immutable and cannot be altered, ensuring the authenticity and ownership of the content.

- Ownership Verification: Zero-watermark technology helps verify the ownership of digital content, making it easier to track and prevent unauthorized use or distribution.

- Scalability: Blockchain has the potential to store and manage large amounts of digital content, making it more scalable.

FUTURE WORK AND RESEARCH

Future work and research on image copyright protection using blockchain and zero-watermark technology could include:

- Integrating AI, ML, and big data could enhance copyright protection.
- A legal and policy framework is needed to govern blockchain-based copyright protection.
- Performance can be optimized through parallel processing and data structure optimization.
- Exploring the use of other blockchain-based solutions, such as non-fungible tokens (NFTs)

CONCLUSION

- Image copyright protection is a crucial issue in the digital age, and existing methods have limitations in terms of security and scalability.

- The proposed architecture for image copyright protection using blockchain and zero-watermark technology offers a more secure and decentralized solution.

- The use of blockchain and zero-watermark technology has significant potential for protecting digital assets, including images.

THANK YOU