Indonesian Journal of Computer Science
ISSN 2549-7286 (*online*)
Jln. Khatib Sulaiman Dalam No. 1, Padang, Indonesia
Website: ijcs.stmikindonesia.ac.id | E-mail: ijcs@stmikindonesia.ac.id

Image Copyright Protection Based on Blockchain Technology Review

Daban Ali Qadir[1], Shavan Askar[1], Mohammed A. Saleem[1], Mina Farooq[1], Saman M Omer[2]
shavan.askar@epu.edu.iq, daban.qadir@epu.edu.iq
[1]Department of Information System Engineering, Erbil Technical Engineering College, Erbil Polytechnic University, Erbil, Iraq.
[2]Department of Software and Informatics Engineering, University of Raparin, Kurdistan Region. Iraq

Article Information

Submitted : 20 Mar 2024
Reviewed: 24 Mar 2024
Accepted : 20 Apr 2024

Keywords

Blockchain, Decentralized Image Sharing, Image Copyright protection, Image Sharing

Abstract

On a daily basis, a significant number of individuals distribute several photos and videos that have been marginally modified from the original material produced by copyright owners, such as photographers, graphic designers, and video producers. Individuals that infringe upon the rights of others, lacking the legal authority to access multimedia content, employ various digital image and picture manipulation techniques, it involves converting to gray scale, trimming, rotating, contracting the frame, and adjusting the background speed, to modify said content. Blockchain technology obviates the necessity of an intermediary, hence circumventing the possibility of a singular point of failure. Infractions to copyright poses a significant barrier to protecting commercial image and video information. The IPFS blockchain technology offers on-chain preservation for copyright information and off-chain storing for distinct multimedia files. The enhanced perceptual hashing algorithm significantly enhances the precision of identifying connections to identify digital image piracy. The photographers and designers that submit their photographs on websites are experiencing significant dissatisfaction due to a prevalent practice in which others attempt to claim credit and profit from the initial creator's effort.

A. Introduction

In the present era of the internet, A significant number of photographers sustain their income by marketing and selling their images through online platforms, frequently via stock photo sources. Photographers are already facing intense competition as they strive to upload more photographs and boost the amount of downloading for their works, thanks to the free of charge and microstock revenue models provided by these platforms [1,2].

Lately, this conduct has resulted in a pervasive prevalence of image identification cheating, where some individuals who are not the original writers wrongfully claim credit for photographs created by others. This violates copyright laws and causes both psychological and financial damage to the rightful owner of the images. The photographs are acquired by another company, which incorporates them into one of its goods. In this case, there could have been a deliberate or accidental infringement of copyright. It is probable that the two companies will avoid discussing precise details with one other due to the assumption that they are rivals.

According to the digital forensics copyright protection legislation, which is enforced to some extent globally, it is unlawful to utilize a duplicate Unauthorized acquisition of data without the owner's consent. Consequently, scientists are formulating solutions to address this matter. Unfortunately, there has been minimal advancement [3,4].

Blockchain technology has increasingly expanded its use in various fields, including digital copyright protection, During the past few years. Blockchain technology is a distributed system that operates without central authority different entities work to uphold an unchangeable and genuine distributed ledger. This approach is utilized for the purpose of preserving copyright information. When this information is documented on the blockchain, it becomes difficult to make any modifications. This would greatly simplify the procedure for digital copyright certification bodies. One intrinsic advantage of blockchain technology is its capacity to enable data recording without the need for a centralized governing entity. Aside from Bitcoin, there are currently several significant operational blockchains, including the digital currency Ethereum, Ripple, which BigchainDB, Hyperledger, and various others. Each of these blockchains serves certain use cases.

B. Literature Review

Suggests a digital media distribution mechanism that employs blockchain technology and decentralized, peer-to-peer authentication methods for managing rights. The system's objective is to showcase the capabilities and opportunities of the blockchain in the delivery of content, using features like access control and encryption techniques. The article outlines the creation of an online content distribution system utilizing blockchain technology, with a specific emphasis on the design and presentation of an advanced video system capable of displaying super high-definition content (4K or 8K). The system employs a decentralized and peer-to-peer registration technique for managing rights. The encryption process entails altering the header portion of the H.265 compression data while also managing the encryption keys, so enabling the data to be decrypted and played back using the correct secret key. Additionally, it highlights the utilization of a permission control dashboard, which allows the licensor to regulate the authorization to see content based on its nature and the device used, even after it has been distributed. The current iteration of the system lacks an incentive system for mining calculation. However, the authors advise that this matter should be deliberated over in the business model. Future endeavors encompass the advancement of a more intricate system and the investigation of additional field applications. The blockchain-powered solution for distributing digital information was demonstrated and received feedback from more than 100 participants, encompassing producers, content owners, and stakeholders in digital content. The system's decentralized method was seen as the most remarkable and appealing characteristic, offering a replacement to the centralized design found in existing DRM solutions [5,6].

Present a groundbreaking technique for watermarking images. This methodology employs visual attention as a means to effectively incorporate watermarks of varying degrees of intensity in distinct areas of an image, while also taking into account visual saliency. This approach seeks to strike a balance between:

resilience and visibility of watermarks. The proposed model uses a new visual. simple attention strategy in the wavelet domain is a useful technique. effectiveness. This model performs much worse than the current ones. methods especially the ones related to saliency detection and also image susceptibility processing attacks on watermarks. The watermarking approach based on the wavelets is also known as without the Visual Attention Model (VAM), is short. However, our approach It integrates the visual attention force by using a saliency model. This enables the secretive usage of watermarks in the critical areas. Our team has made it easier to include and also remove the watermarks, therefore. the requirement of blind or visually impaired methods. To obtain an objective In the evaluation of our method, we employ different metrics including PSNR, SSIM and also the JND, to measure the efficiency of our system. Moreover, we also conduct subjective scores that consider the human factor in assessing the quality of visuals. Finally, the system is challenged against all kinds of attacks. such as image manipulation and filtering, to assess its reliability [7,8,9].

This revolutionary manuscript provides an innovative copyright management approach. The framework intends to provide improved copyright protection and also easier distribution through integrating the perceptual hashing, blockchain technology, digital watermarking, and also IPFS. Based on the timestamp's scrutiny, secure distribution and peer to peer technologies for copyrighted material dispersion of which reliance upon one controlling body is diminished [5].

This proposal is meant to revolutionize the method of leader selection in the consortium blockchains that are prevalent among data trading platforms. It outlines a dynamic process of assigning a numerical score to each transaction and uses this rank in identifying the leaders. Stability and security in the system will also be achieved using this revolutionary approach. To address this problem, our approach incorporates a component for dynamic leader selection that conducts the real-time and intelligent evaluation of transactions in order to make an appropriate peer choice. Moreover, the Hyperledger Fabric consensus mechanism has also evolved significantly to support the seamless integration with legacy data trade platforms. This advancement entails incorporating a punishment severity measure into the standardization process of the transaction data and behavioral assessment. In addition, a dynamic consensus mechanism has been added featuring transaction proposal submission, endorsement by the users on their basis and leader selection based on user ratings. Our proposed method includes user scores as one of the very crucial factors to select the top peer and thus a reflection on participants' credibility and transaction quality. This method helps to involve and create trust among all the stakeholders [10,11,12].

This research methodology uses the NSCT transform and image normalization to develop a trusted approach of zero watermarking. This technique serves the main purpose of ensuring that the watermark remains resilient to different kinds of attacks while at the same time, being inconspicuous. To achieve this very desirable result, geometric invariant space mapping and also block singular value decomposition are used. Through such an approach, it becomes impossible to produce a watermark that is very vulnerable to geometric distortions, noise filtering effect and so on. The first step is to normalize the cover image that involves invariant moments and thus leads us from one geometrically non-invariant space into a new, transformed system. After that, the square of the unit circle is calculated to retrieve a sufficient portion of the normalized picture. In addition, the use of Non-sampling Contourlet Transform (NSCT) helps in part of an image. On top of that, a block singular value decomposition is used to decompose the coefficient sub-band. We achieve zero watermarking by calculating the parity of the highest digit of the maximum unique value for each block. Image normalization methods based on invariant moments help the program to achieve geometric attack resistance by transforming images into a space that is rotationally and also translation-invariant. The selection of the NSCT is based on its ability to focus the energy in image into low-frequency region and capture a wide variety scales and orientations which are consistent with human visual characteristics. Surveying Singular Valley Decomposition (SDA) ensures the stability of watermark as it does not allow the largest singular value to remain same in the presence disturbance. Identifying the best areas of standard images for removal is also a problem recognized in this study that is currently under publication. These concerns including cutting assaults, filtering and disruption have been countered by several proposals. It shows that this method proves to be an very effective approach for combating the common image attacks, including noise attack, filtering and also compressed-JPEG [13,14].

This research study considers the increasing incidence of copyright infringements and violations in multimedia domain, particularly with regard to Game of Thrones television platform, wherein episodes were being illegally downloaded before official release. This research paper discusses the increasing cases of multimedia copyright infringements and weakness in light that it is needed to develop better methods for ensuring data protection and privacy. According to the principles of theoretical knowledge, it is possible to create a structured centralized data management framework using blockchain technology. This would empower people to have complete control over their data and at the same time ensure his privacy protection. The proposal does not include a solution involving blockchain technology for establishing a centralized data management system that protects the user privacy and also gives consumers ownership of their personal information. Thus, the authors propose an approach based on blockchain technology to grant the users full control over their multimedia resources without involving any mediators. The framework enables the easy archiving, retrieval; sharing and analysis of user information. Notable advantages of blockchain technology include the secure operations, decentralized connectivity and data privacy that are very valuable in the field where records access should be controlled [15,16].

This research study presents a digital copyright management system that has high security features. This system is very inefficient with the use of InterPlanetary File System and dum contracts that are destroyed under many layers on Ethereum blockchain. This study aims to develop the overall conceptual framework for the above-mentioned digital copyright management system. Notably, the framework mainly relies on the use of smart contracts and InterPlanetary File System with Ethereum blockchain being a very crucial element. To improve the security of the system, an advanced ELGamal encryption algorithm is implemented. This algorithm encrypts and also decrypts the digital content, along with session data. When this algorithm is incorporated into the system, its overall security level increases significantly. The authors of this paper perform a very comprehensive assessment to determine whether the augmented encryption algorithm is really effective. In addition, the article discusses a transaction watermark that is used specifically for imaging data. This watermark's main objective is to act as a physical proof of piracy while also retaining the feature for tracking unauthorized usage. The proposed solution for digital copyright management is highly reliable and traceable when it puts the improved version of ELGamal encryption to protect privacy, as well as include watermarking in transaction transactions into image data. This solution capitalizes on the blockchain technology combined with the encryption algorithms well [17,18].

The emergence of online technology has revolutionized the process of pictures sharing. On the other hand, it has also led to widespread and rampant unauthorized reproduction and use of images. Through the use of blockchain technology and the SIFT local feature method for extraction, Inter-Planetary File System (IPFS) has been implemented to decentralized storage of copyright information attributes on photos. Finally, copyright registration and transfer have been achieved using the Hyperledger Fabric as well as smart contracts (chain code). The system presents the strengths of automated detection for many similar violations, distributed storage, resistance to intrusion and also tracking activities well [19,20].

This study presents a developing strategy for controlling the digital rights associated with the design works via blockchain technology. This proposition aims to resolve the numerous issues associated with content protection, copyright preservation and also design work contracts' arrangement. This strategy in the study includes an on-chain integration of design work with its associated copyright record. In addition, the following aspects are considered in this approach: public display of the design effects; protection of all design details from disclosure and compliance with the applicable legislation. A novel proof-of-delivery strategy that is based on smart contracts and public key cryptography to avoid the active participation of the participants for a successful fair trade practices is presented. The effectiveness of the proposed solution is measured, by a comprehensive assessment through examination and also comparison against other methods. Moreover, a proof-of -concept study is conducted to demonstrate the security and fairness offered by the proposed plan with digital garment design as one good example. Finally, the study proposes a VoR method based on blockchain technology that eliminates upfront payment and also ensures trading integrity [21].

The present inquiry is dedicated to examining the obstacles connected to power measurement for virtual machines (VMs) in the framework of cloud computing. These challenges encompass a wide array of facets such as server models, sampling techniques, metering methods, and the evaluation of precision. Furthermore, the research examines topics that are presently open for exploration, which include VM service billing, power budgeting, and energy-saving scheduling. The objective of this examination is to stimulate novel research interests in this particular domain. The study explores diverse strategies for quantifying the power of VMs, covering server models, sampling techniques, and power metering methods. It provides a comprehensive explanation of the three primary stages involved in VM power measurement, namely data collection, modeling, and estimation. The investigation categorizes VM power measurement into two distinct approaches: the white-box method and the black-box method, and it offers extensive discussions on both methodologies. It underscores the significance of acquiring modeling information for VM power measurement and investigates methodologies for monitoring this information at the individual VM level. Additionally, the examination deliberates on the utilization of benchmarks to assess the accuracy of power consumption models and discusses commonly employed benchmarks [22].

A decentralized application utilizes Ethereum's robust smart contracts and perceptual hashes to automatically detect and reject modified images that have visual resemblance to photographs previously available for purchase. The marketplace we offer is characterized by complete absence of censorship, absence of any single point of failure, absence of any central authority overseeing it, and it ensures the protection of online user privacy due to the inherent attributes of blockchain technology. The authors have developed two separate data storage structures, namely IPFS Store and Eth Store, which effectively reduce the size of the Ethereum test chain. This is accomplished by utilizing the IPFS protocol to store both images and perceptual hashes. Any widely-used encryption algorithm can be employed to encrypt and decrypt data stored on IPFS. An effective hashing algorithm, capable of distinguishing between unaltered photos and those that have been modified, is demonstrated in the results and the system design is depicted in the Figure. 1 [1].

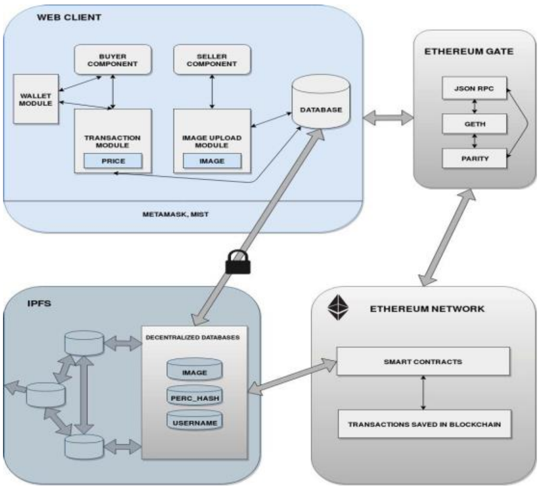

Figure 1. System design architecture [1]

Introduces a proposal for a blockchain-powered system that ensures secure storage and retrieval of data in industrial networks. This system utilizes local regenerative coding technology to effectively repair nodes that have been destroyed. Exhibits enhanced integrity and decreased resource usage, as evidenced by testing findings indicating a 9% rise in repair rate and an 8.6% increase in storage rate. Application of local regenerative code technology to repair and store data between broken nodes, while maintaining user data privacy. Comparative analysis of overhead performance when utilizing a fault-tolerant data storage and repair technique grounded on blockchain technology in relation to other approaches. Assess the repair quality of the regeneration code by choosing three comparable techniques within the field. The proposed approach involves the utilization of elliptic bilinear mapping and a third-party auditor (TPA) to implement an integrity authentication mechanism. The construction of a fault-tolerant local regeneration code is achieved by utilizing a Cauchy matrix in combination with multidimensional linear vector codes. An assessment of data recovery performance in industrial network systems, taking into account both safe data storage and repair rates [22].

Introduces a strong control method that utilizes Dual Surface Control (DSC) and Multi-Layer Perceptron (MLP) techniques to tackle the increasing complexity in backstepping design and minimize the number of adaptive parameters. The enhancement of the system's resilience is achieved by minimizing the impact resulting from approximations, modeling errors, and uncertainties. This objective is accomplished by integrating a robust compensator at each stage of the design process. The simplification of the estimation of continuous functions is achieved through the utilization of the Radial Basis Function Neural Network (RBFNN) is unlikely to be written by an AI when processed by an AI detection tool. The absence of reliable compensators at each stage of the backstepping design further compromises the durability of the system. In order to alleviate the spread of complexity in the backstepping design, the Dynamic Surface Control (DSC) technique is implemented. The Multi-Layer Perceptron (MLP) approach is mandated to decrease the quantity of adjustable parameters. The mean value theorem is employed in control strategies for nonaffine pure-feedback nonlinear systems [23].

The research article introduces a system based on blockchain technology to be used in the eBook market. This system allows for the exchange of self-published manuscripts and facilitates direct payments from readers to authors, thereby eliminating the need for a trusted intermediary. By eradicating the charges tied to intermediaries, this system aims to provide a more efficient and cost-effective solution. However, the absence of faith in this particular situation raises concerns regarding the genuineness, possession, and intellectual property of electronic content, as well as the security of purchase transactions. In order to address these concerns, the article proposes a secure and dependable system for eBook transactions. This system incorporates various features, including the assurance of safe direct purchases, prevention of illegal activities and unauthorized distribution of eBooks, preservation of the confidentiality of eBook content, authorization of reading rights, authentication of purchasers, verification of content validity and integrity, and several others. Additionally, the article evaluates the security and simulated efficiency of the proposed system and presents feasible cryptographic protocols. In conclusion, the article describes a marketplace for eBooks based on blockchain technology, which enables direct payments and self-published eBook trading. It in addition indicates the security requirements of the system, deliberates the cryptographic protocols employed, and assesses the security and functionality of the system. Moreover, the document supplies a summary of the important symbols employed in the eBook transaction protocols, which comprise of block hash values, sequence numbers, and the root hash value of the Merkle hash tree [24].

The paper introduces an innovative encryption technique for chaotic images that exhibits a correlation with fingerprinting. This technique utilizes the fingerprints of distributors to generate key streams, thereby ensuring security against chosen plaintext attacks and addressing concerns regarding key management. In order to verify and track the image, sender, and receiver, the proposed approach adopts the blockchain framework. The encryption method involves a substitution phase that employs a chaotic linear fractional transformation (LFT) S-box. This particular S-box is constructed through the action of PGL(2,GF(2^8)) on a finite field of order 2^8. To assess its efficacy, the proposed method is compared to four other recently developed encryption techniques that are associated with plaintext. Furthermore, the proposed image distribution technique encompasses a range of operations such as decryption, signature extraction, verification, tracing, fingerprint collusion, signature, reversible data hiding (RDH), and encryption. These operations are executed by different distributors in diverse distribution layers, and the encrypted images are transmitted through the public channel [25].

The implementation of digital medical images has markedly risen due to the rapid advancements in information technology and medical research. These photographs are presently being utilized in various applications, such as tele-diagnosis and tele-surgery. As a result, scientists are currently investigating the process of preparing, compressing, and safeguarding medical photographs to address their extensive utilization on cloud platforms. Throughout the transmission of these medical pictures, it is conceivable for them to be deliberately or accidentally modified by intruders. To ensure the purity of a medical image, one may assess the region of interest (ROI) for any tampering or alterations. In order to detect tampering and its subsequent restoration, scientists have developed multiple watermarking methods. Nevertheless, a drawback of established approaches, like LSB-based watermarking, is the potential loss of information in the cover image. Therefore, reversible watermarking is employed as a means to authenticate the medical image [26].

The proposed platform suggests the utilization of blockchain and IPFS as a method to ascertain copyright violation in multimedia content. This objective is attained through the implementation of perceptual hash algorithms, which guarantee the lawful acknowledgment of creators. The technology tackles the issue of manipulated image and video uploads and adopts a decentralized approach to discourage tampering and copyright infringements. The Intergalactic Document System (IPFS) is employed for the secure storage of multimedia objects and the generation of addressable hashes in a centralized manner. This program aims to accomplish the development and comparison of perceptual hash (pHash) for the purpose of detecting alterations in the original multimedia files. A comparative evaluation is carried out between pHash, dHash, and wHash, using a similarity metric that relies on the Hamming distance. The time required for block mining, block creation, and block access on the blockchain network is analyzed, considering different file sizes and the number of involved peers. Proof-of-work mechanisms are deployed to secure the consistency of blocks across the blockchain network. The Hamming distance is utilized to compare the hash values of video frames, while edge matching techniques are executed to eliminate redundant frames. Blockchain and IPFS obstruct the sharing of multimedia content while simultaneously promoting copyright infringement. The perceptual hash (pHash) algorithm proves to be highly effective in identifying copyright infringements in multimedia content, surpassing the performance of traditional hashing algorithms. The method successfully detects tampering in photos and videos, except for cases of video rotation and alterations in speed [27].

An adaptable and resilient approach is introduced to safeguard image copyrights, providing control over ownership and deterring improper utilization of image assets. The image is subjected to a multi-level lifting wavelet transform to convert it into the wavelet domain. To ensure resistance against cropping, the lowest frequency band is divided into multiple concentric rectangles. In order to guard against rotating attacks, the flag bits are embedded in the pixels of a rectangle selected by the user. The suggested embedding operation takes into consideration the high energy coefficient as a criterion for identifying suitable locations for the embedding procedure. This approach minimizes the overall error introduced during the embedding process and protects concealed data against both noise and jpeg-compression attacks. A reversible scrambling technique is implemented on a predetermined area of the watermarked image to impede unauthorized users from obtaining a watermarked image of superior quality. The functionality of the proposed picture copyright protection algorithm can be adapted to include video copyright protection. However, simplifying the complexity and reducing the duration of embedding in video media remains a significant challenge [28].

A novel approach for safeguarding the copyright of digital images was introduced, employing the characteristics of blockchain technology such as resistance to manipulation, decentralized nature, and ability to trace, along with perceptual hashing. The intelligent agreement employs the comparison of hash values to determine if the image is being used without proper authorization. Then, the encrypted image and the verified copyright details get uploaded to the InterPlanetary File System (IPFS) [29].

A method for creating zero-watermarks is presented that involves the use of a Linear Feedback Shift Register (LSFR) and the backpropagation algorithm to modify pretrained weights and biases. Using a stacked denoising autoencoder (SDAE), a highly improbable unsupervised neural network is constructed to extract deep-level properties from remote sensing photos. The SDAE is made up of multiple interconnected denoising autoencoders (DAEs) that allow for the handling of complex and high-dimensional datasets as well as the exploration of deep-level features in the data. Gluttonous layer-wise pretraining and finetuning for parameter optimization are the two phases in the training process. Every layer of the SDAE is trained separately during the greedy layer-wise pretraining phase. The output generated by the hidden layer of the previous DAE serves as the input for the input layer of the next DAE. Error backpropagation is used in the fine-tuning step to maximize all of the SDAE's parameters. The SDAE was applied in the zero-watermarking portion, and MATLAB R2022a was used as the software development platform. The suggested zero-watermarking approach effectively mitigated picture data distortion and accomplished effective copyright protection for high-resolution remote sensing photographs by merging blockchain technology with SDAE. Using a new zero-watermark registration technique based on blockchain technology, the algorithm increased uniqueness and improved copyright recognition accuracy for similar remote sensing photos taken in the same region. The program was able to extract deep-level properties from remote sensing images without the need for manual feature extraction by utilizing the SDAE model. The algorithm's accuracy and resilience were greatly enhanced by this feature [30].

C. Research Methodology

3.1 Secure Watermarking using Hashing

For grayscale photos in the frequency domains, the technique will enable image authentication utilizing watermarking and the blockchain of Ethereum. Figure 2 depicts and explains the watermark embedding process. The image required to be authenticated is first subjected to the third level's Discrete Wavelet Transform (DWT). The ID hash number of the picture owner is the watermark. The watermark is encrypted using the Advanced Encryption Standard, also known as AES, and a secret key before being incorporated into the center frequency wavelet coefficients. The user saves the identical watermark that is included in the image once it has been encrypted with SHA-256 and verified with their blockchain key. When adding a watermark to a picture or storing it on a blockchain, AES as well as

SHA-256 are combined to provide an additional layer of protection. The watermark is encrypted using AES before being embedded into the picture. The watermark is encrypted using SHA-256 before being saved to the blockchain. Since SHA-256 is a function that is one-way and since we don't want anyone to be able to access the watermark by obtaining the AES key, we utilize it [20].

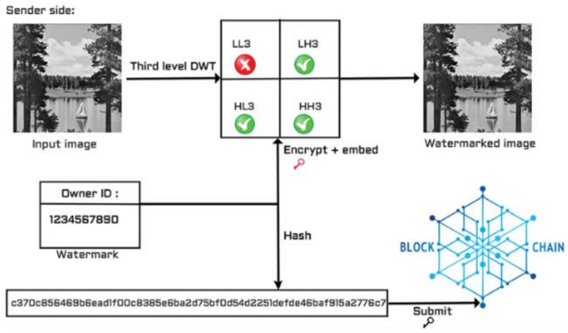

Figure 2. Embedding a secure watermark [10]

Blockchain is utilized to confirm the authenticity of a watermark so that no third party is engaged in the authentication procedure. As seen in Figure 1, the watermark is first encrypted using AES-128 encryption before being embedded into the input image.

3.2 Inter Planetary File System (IPFS)

The original image and their feature vector set of photos which have successfully registered copyrights are stored in the IPFS storage module, a decentralized storage network built on blockchain technology. A file sharing system called IPFS uses a file's content to identify files. File locations as well as node connection information are recovered using a hash table that is distributed (DHT). A file input to the IPFS system is split up into chunks, each of which can have up to 256 kb of information and/or connections with other chunks. Every chunk is identified by a content identification, which is derived from its content and is also known as a cryptographic hash [20].

D. Result and Discussion

The comparison of the outcomes of embedding into several wavelet sub-bands is displayed in Table 1. The comparison is done to find out how each region's watermark embedding affects the perceptibility measures.

Table 1. Blockchain Copyright Protection Comparison's

Reference	Year	Content Type	Algorithm
[3]	2015	HD Video	DRM
[4]	2017	Image	Watermarking
[8]	2018	HD Video	Encryption
[5]	2018	Image	Watermarking
[9]	2019	Image	Encryption+ Watermarking

[11]	2019	Image	DRM
[22]	2019	Document	Watermarking
[14]	2019	Image	Fingerprinting
[12]	2019	Image, Audio, Video	Fingerprinting
[15]	2020	Document	BCC-based encryption
[16]	2020	Image	Encryption+ Fingerprinting

The implementation of a Blockchain-based solution for an online stock picture marketplace offers numerous advantages compared to traditional marketplaces. The features encompass heightened security protocols, the implementation of permanent trade logs, the option to generate personalized permits and market prices for photographs, amplified earnings for participants, and the use of distributed storing for images via IPFS. Detecting violations of legal rights is a substantial barrier, particularly when dealing with multimedia artifacts. This paper outlines our utilization of blockchain and IPFS to facilitate the sharing of multimedia items among peers, while effectively circumventing copyright infringement The implementation of perceptual hash pHash is used to detect occurrences of copyright violation in multimedia content. Moreover, The IPFS hash corresponding to the original multimedia item is stored in the blockchain instead of the actual object itself to reduce the size of the blockchain network.

E. References

[1] Mehta, R., Kapoor, N., Sourav, S. and Shorey, R., 2019, January. Decentralised image sharing and copyright protection using blockchain and perceptual hashes. In 2019 11th International Conference on Communication Systems & Networks (COMSNETS) (pp. 1-6). IEEE.

[2] Yu, S. and Jiang, Z., 2015, August. Visual tracking perceptual image hash from a mobile robot. In 2015 IEEE International Conference on Information and Automation (pp. 1612-1616). IEEE.

[3] Kishigami, J., Fujimura, S., Watanabe, H., Nakadaira, A. and Akutsu, A., 2015, August. The blockchain-based digital content distribution system. In 2015 IEEE fifth international conference on big data and cloud computing (pp. 187-190). IEEE.

[4] Shavan Askar & Ibrahim Shamal Abdulkhaleq & Shahab Wahhab Kareem, 2021. "Blockchain systems: analysis, applications, & risks," International Journal of Science and Business, IJSAB International, vol. 5(6), pages 163-173.

[5] Shavan Askar & Zhwan Mohammed Khalid & Tarik A. Rashid, 2021. "Blockchain For Securing IoT Devices: A Review," International Journal of Science and Business, IJSAB International, vol. 5(6), pages 209-224.

[6] Bhowmik, D., Oakes, M. and Abhayaratne, C., 2016. Visual attention-based image watermarking. IEEE Access, 4, pp.8002-8018.

[7] Meng, Z., Morizumi, T., Miyata, S. and Kinoshita, H., 2018, July. Design scheme of copyright management system based on digital watermarking and blockchain. In 2018 IEEE 42nd Annual Computer Software and Applications Conference (COMPSAC) (Vol. 2, pp. 359-364). IEEE.

[8] Wang, X., Feng, Q. and Chai, J., 2018, December. The research of consortium blockchain dynamic consensus based on data transaction evaluation. In 2018

11th International Symposium on Computational Intelligence and Design (ISCID) (Vol. 2, pp. 214-217). IEEE.
[9] Yang, K., Wang, W., Yuan, Z. and Zhao, W., 2018, October. Strong robust zero watermarking algorithm based on NSCT transform and image normalization. In 2018 IEEE 3rd Advanced Information Technology, Electronic and Automation Control Conference (IAEAC) (pp. 236-240). IEEE.
[10] Vishwa, A. and Hussain, F.K., 2018, November. A blockchain based approach for multimedia privacy protection and provenance. In 2018 IEEE symposium series on computational intelligence (SSCI) (pp. 1941-1945). IEEE.
[11] Nashwan Maslah Fares, Shavan Askar, "A Novel Semi-symmetric Encryption Algorithm for Internet Applications", Journal of Duhok, Vol. 19, No.1, 2016.
[12] Omar Shirko; Shavan Askar , "A Novel Security Survival Model for Quantum Key Distribution Networks Enabled by Software-Defined Networking" IEEE Access, Volume 11, 2023.
[13] Peng, W., Yi, L., Fang, L., XinHua, D. and Ping, C., 2019, December. Secure and traceable copyright management system based on blockchain. In 2019 IEEE 5th International Conference on Computer and Communications (ICCC) (pp. 1243-1247). IEEE.
[14] Shi, J., Yi, D. and Kuang, J., 2019, October. Pharmaceutical supply chain management system with integration of iot and blockchain technology. In International Conference on Smart Blockchain (pp. 97-108). Cham: Springer International Publishing.
[15] Lu, Z., Shi, Y., Tao, R. and Zhang, Z., 2019, October. Blockchain for digital rights management of design works. In 2019 IEEE 10th international conference on software engineering and service science (ICSESS) (pp. 596-603). IEEE.
[16] Ibrahim Shamal Abdulkhaleq & Shavan Askar, 2021. "Evaluating the Impact of Network Latency on the Safety of Blockchain Transactions," International Journal of Science and Business, IJSAB International, vol. 5(3), pages 71-82.
[17] Zhwan Mohammed Khalid & Shavan Askar, 2021. "Resistant Blockchain Cryptography to Quantum Computing Attacks," International Journal of Science and Business, IJSAB International, vol. 5(3), pages 116-125.
[18] Qureshi, A. and Megías, D., 2019, November. Blockchain-based P2P multimedia content distribution using collusion-resistant fingerprinting. In 2019 Asia-Pacific Signal and Information Processing Association Annual Summit and Conference (APSIPA ASC) (pp. 1606-1615). IEEE.
[19] Liang, W., Fan, Y., Li, K.C., Zhang, D. and Gaudiot, J.L., 2020. Secure data storage and recovery in industrial blockchain network environments. IEEE Transactions on Industrial Informatics, 16(10), pp.6543-6552.
[20] Sun, J., Yao, X., Wang, S. and Wu, Y., 2020. Blockchain-based secure storage and access scheme for electronic medical records in IPFS. IEEE access, 8, pp.59389-59401.
[21] Chi, J., Lee, J., Kim, N., Choi, J. and Park, S., 2020. Secure and reliable blockchain-based eBook transaction system for self-published eBook trading. PloS one, 15(2), p.e0228418.
[22] Li, R., Wang, W., El-Sayed, E.S.M., Su, K., He, P. and Yuan, D., 2021. Ratiometric fluorescence detection of tetracycline antibiotic based on a polynuclear

lanthanide metal–organic framework. Sensors and Actuators B: Chemical, 330, p.129314.
[23] Janani, T., Darak, Y. and Brindha, M., 2021. Secure similar image search and copyright protection over encrypted medical image databases. IRBM, 42(2), pp.83-93.
[24] Salah M. Saleh Al-Majeed, Shavan K. Askar, Martin Fleury, "H.265 Codec over 4G Networks for Telemedicine System Application", UKSIM, Cambridge, UK, March, 2014.
[25] Saman M. Omer, Kayhan Z. Ghafoor & Shavan K. Askar , "Lightweight improved yolov5 model for cucumber leaf disease and pest detection based on deep learning" Journal of Signal, Image and Video Processing, 2023
[26] Kumar, R., Tripathi, R., Marchang, N., Srivastava, G., Gadekallu, T.R. and Xiong, N.N., 2021. A secured distributed detection system based on IPFS and blockchain for industrial image and video data security. Journal of Parallel and Distributed Computing, 152, pp.128-143.
[27] Shahadi, H.I., Thahab, A.T. and Farhan, H.R., 2022. A novel robust approach for image copyright protection based on concentric rectangles. Journal of King Saud University-Computer and Information Sciences, 34(4), pp.1263-1274.
[28] Zhang, Q.Y. and Wu, G.R., 2023. Digital Image Copyright Protection Method Based on Blockchain and Perceptual Hashing. International Journal of Network Security, 25(1), pp.10-24.
[29] D. Xu, N. Ren and C. Zhu, "High-Resolution Remote Sensing Image Zero-Watermarking Algorithm Based on Blockchain and SDAE," in IEEE Journal of Selected Topics in Applied Earth Observations and Remote Sensing, vol. 17, pp. 323-339, 2024, doi: 10.1109/JSTARS.2023.3329022.
[30] Baydaa Hassan Husain & Shavan Askar, 2021. "Survey on Edge Computing Security," International Journal of Science and Business, IJSAB International, vol. 5(3), pages 52-60.
[31] Kurdistan Ali & Shavan Askar, 2021. "Security Issues and Vulnerability of IoT Devices," International Journal of Science and Business, IJSAB International, vol. 5(3), pages 101-115.
[32] Mangipudi, E.V., Rao, K., Clark, J. and Kate, A., 2019, June. Towards automatically penalizing multimedia breaches. In 2019 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW) (pp. 340-346). IEEE.
[33] Steichen, M., Pontiveros, B.F., Norvill, R., Shbair, W., et al.: Blockchain based, decentralized access control for IPFS. In: The 2018 IEEE International Conference on Blockchain (Blockchain-2018), pp. 1499–1506. IEEE (2018)