Perceptual Hash Techniques for Audio Copyright Protection in Decentralized Systems

Dr. N. Kavitha[1], Rashmika S J[2], Reshika A S[2]
Assistant Professor (Senior Grade),Computer Science and Engineering, Mepco Schlenk Engineering College (Autonomous), Sivakasi, Tamil Nadu[1]
Student,Computer Science and Engineering, Mepco Schlenk Engineering College (Autonomous), Sivakasi, Tamil Nadu[2]
Email: nkavitha@mepcoeng.ac.in, rashmika2k4@gmail.com, reshika433@gmail.com

***Abstract*—The overlap of perceptual hashing technologies with blockchains is an interesting answer to strengthen copyright protection of sound in decentralized networks. As music society still has to endure attacks on unauthorized duplication and transformation of online content, traditional security does not hold water. Perceptual hashing bridges the gap, creating unique digital fingerprints that are resistant to small-scale modifications, to allow detection of copyright piracy even in edited audio content. When combined with the immutable nature of blockchain and the smart contract functionality, such new framework not only guarantees ownership verification but also does licensing procedures automatically, thereby doing away with the need for intermediaries.**

***Index Terms*—Perceptual Hashing, Blockchain, Audio, Copyright Protection.**

I. Introduction

THE Music business is a coalition of copyright administration, tune writers, mixing/ mastering engineers, music architects, song development, music representatives, and artist liaisons.It has evolved over the years to become a global ecosystem in which everyone, everywhere, has access to music from artists anywhere in the globe instantly.This transformation has altered how we consume music, but it has also opened the floodgates to a new set of issues—specifically in terms of protecting artists' intellectual property. Digital content is easy to copy, manipulate, and distribute without permission, exposing most artists to unauthorized use of their work. High-profile copyright battles have emerged around the world, including the Taylor Swift and Scooter Braun's Ithaca Holdings dispute, in which Swift's master recordings were sold off without her permission, leading her to re-record her albums. The unauthorized release of Kanye West's Donda album highlighted the challenge artists have in keeping their digital content. Another well-known case is the Blurred Lines dispute, in which Robin Thicke was sued by Marvin Gaye's estate for copyright infringement. These cases emphasize the intricacies of intellectual property protection in the digital age.

Even in India, copyright has been a huge change to the music industry. Ilaiyaraaja's battle with music companies for rights over his own songs is the biggest tale of the legal battle for rights over intellectual property. Even music director A.R. Rahman has been grumbling about receiving proper royalty payment to composers and lyricists and asking for a more open payment system.The story of the song Madhuban by Kanika Kapoor, attacked and then altered due to cultural and copyright sensitivities, even more, highlights the issues of copyright in India.

Growing complexity of enforcing copyrights in the digital music industry has motivated researchers to explore new career protection approaches. Sharma and Gupta (2023) [21] researched how blockchain can provide a decentralized approach of protecting copyrights in the Indian music industry, reduced reliance on intermediaries and evading unauthorised distribution. Menon and Kumar (2022) [22] enlightened technical challenges in adopting audio fingerprinting for Bollywood songs, and underlined the problem raised by recurrent remixes, pitch variations, and tempo shifts. These papers put a strong focus on the critical need for sound steps over standard copyright safeguarding measures.

Conventional copyright protecting methods, including digital watermarks and metadata tagging, are commonly ineffective against unauthorized use. Subtle changes—like pitch manipulation, tempo adjustments, or remixing—are easily circumvented while keeping the original track's character intact. This shortcoming has given rise to more advanced solutions, such as perceptual hashing, which generates distinctive digital fingerprints from an audio file's sound characteristics and not its metadata. Unlike cryptographic hashes, perceptual hashes do not change much even with frequent audio transformations such as compression, pitch changing, or addition of noise.

Perceptual hashing has also been crucial in the war against copyright infringement. YouTube's Content ID system, for example, uses similar methods to identify copyrighted materials, even if an original track has been transformed. But Content ID is a centralized system run by YouTube, so artists have to depend on the company for enforcement. Most artists complain that the system is fault-prone, sometimes misidentifying material or permitting big companies to take credit for revenue from solo creators unjustly.

More direct and democratized mechanism for copyright protection is blockchain technology. Artists can establish an indelible, provable record of ownership by placing percep-tual hashes onto a blockchain ledger. Blockchain-based decentralized music distribution has already been tested and scaled

by platforms such as Audius, wherein artists own their work without middlemen taking a share of it. Smart contracts further advance this system by having licensing deals and royalties automatically execute. payments. In 2017, singer Imogen Heap pioneered blockchain en-abled smart contracts for music distribution with her Mycelia project, making revenue sharing transparent and fair. Opus and Ujo Music, similar platforms, also empower artists by utilizing blockchain to manage royalties. Perceptual hashing and blockchain can revolutionize copyright protection in Indian music.Current studies have explored the intersection in depth. Rao and Iyer (2024)[23] discussed how digital rights man- management (DRM) on Indian music websites, determining its limitations and promoting blockchain-based solutions to enable artists equitable returns. Patel and Desai (2023)[24] have proposed enhancements in perceptual hashing for application on Indian classical music, which has unique needs due to the intricate tonal variations involved. Their research points out that fingerprinting approaches tailored to a particular set of inputs can significantly strengthen copyright protection on traditional Indian types of music. Further, Reddy and Bose (2024)[25] discussed the legal and technological implications of blockchain application in Indian copyright laws, arguing that legislative changes are necessary to completely integrate blockchain into copyright protection systems. By combining perceptual hashing and blockchain technology, artists are given a better tool to protect their work. Illegal copies are much harder to execute, while licensing and payment of royalties become transparent and more effective. Decentralization by blockchain ensures that No single party owns control over the data, making a fair and open system accessible to all. As machine learning and artificial intelligence continue to develop, future technologies may enhance music copyright protection. Forensic testing for music using AI, for instance, could analyze even the slight similarities between compositions to offer an enhanced protection from unauthorized use. The future for the music business may involve developing a paradigm around decentralized platforms, AI-driven copyright protection, and royalty management through blockchains. These innovations might restore fairness and transparency to a historically intermediary-dominated market, allowing artists to receive their due credit and compensation for creative labor. But knowing a song is only half the battle—the actual battle is asserting ownership and maintaining rights intact. That's where blockchain enters. By storing perceptual hashes on a blockchain ledger, artists can create an permanent, auditable record of ownership. Audius, a blockchain-based music streaming platform, is already introducing this vision into reality, enabling artists to receive their rights and royalties directly in uncommissioned form, free from the involvement of a label or streaming site in the middle. Another useful property of blockchain technology is smart contracts. They are computer-controlled contracts that have the ability to license work and remit royalties automatically. In 2017, artist Imogen Heap broke the ground with her Mycelia venture, implementing blockchain technology to distribute artists' fair and equitable payments. Through smart contracts, artists do not need to concern themselves with middlemen or late payments—payments are instant and just. Decentralized music sites such as Opus and Ujo Music are appearing, enabling artists more control over their royalties through blockchain's transparent and autopilot nature. Smart contracts may also protect against unauthorized re- lease. If a perceptual hash of a posted song corresponds with a copyrighted song on the blockchain, the system is able to deny the upload or require proper licensing before providing access. Artists therefore receive the payment they are due to without the wait of long legal processes. Consider how much this technology would have benefited in the "Stairway to Heaven" copyright battle between Led Zeppelin and Spirit's Randy Wolfe. A perceptual hash system supported by blockchain would have resolved the matter instantly by offering absolute evidence of originality. Outside the domain of copyright law, blockchain and per- ceptual hashing can transform the entire music industry. Streaming platforms are known to grab a large share of revenue, and artists receive barely more than a fraction of what their music earns. On blockchain sites, artists can avoid middlemen and directly interact with listeners. For example, NFTs have enabled artists to sell limited music, concert tickets, and virtual collectibles directly to fans, getting a fair pay. By using perceptual hashing in combination with blockchain, artists now have a new and powerful weapon to safeguard their work. Copyright piracy is much harder to do, and licensing and royalty payment are easier and more transparent. Blockchain's decentralized nature is that no one owns the data, so everyone gets equal and unrestricted access. Eventually, these technologies place more control in artists' hands in a way that is sustainable and equitable. They allow copyright protection to be simplified, automated licensing, and paying creators what they are due—no intermediaries, no hold-ups, merely a simple direct con- nection between artists and listeners. As the internet continues to evolve, perceptual hashing and blockchain may become the key to ensuring a healthy, artist-controlled music economy where the art of music is properly appreciated and guarded. Protecting copyrights in music will assuredly include even more creativity. Artificial intelligence and machine learning keep on getting better and could be made a part of with blockchain and perceptual hashing to develop even more advanced means of identifying and safeguarding music. The future may see AI-based forensic analysis of music able to identify even the most minor similarities of composition and provide an even more effective safeguard against misuse. With technology advancing at an increasingly rapid pace, the music world is on the cusp of a new era in which artists will at last be able to assert ownership over their work as a whole. Either via decentralized streaming platforms, AI-powered copyright detection, or blockchain-based royalty disbursement, music rights management in the future could never have looked more promising. As these types of technologies continue to evolve and expand, they can potentially bring fairness and transparency back to an industry that has been controlled by intermediaries for far too long. This new phenomenon could make way for a system which is more fair in its method, safeguarding creativity, and compensating artists rightfully compensated for what they do within the music space.

TABLE I
LIST OF ACRONYMS AND THEIR FULL FORMS (ALPHABETICAL ORDER)

Acronym	Full Form
AAC	Advanced Audio Coding
AI	Artificial Intelligence
CID	Content Identifier
DCT	Discrete Cosine Transform
DTW	Dynamic Time Warping
GAN	Generative Adversarial Network
IPFS	InterPlanetary File System
LLE	Locally Linear Embedding
LPF	Low-Pass Filter
MP3	MPEG-1 Audio Layer 3
NFT	Non-Fungible Token
OLAF	Overly Lightweight Acoustic Fingerprinting
SURF	Speeded-Up Robust Features
URI	Uniform Resource Identifier

II. RELATED WORKS

Audio fingerprinting and perceptual hashing have come a long way over the years, spurred by technological advances to make identification and authentication more trustworthy. The idea of audio fingerprinting was pioneered by Haitsma and Kalker's seminal research (2002), which made it possible to identify music strongly despite background noises, compression, and other types of distortion. Through the years, researchers have optimized these techniques to enhance efficiency, scalability, and resilience against environmental fluctuations.Six [1] intro-developed Panako 2.0, a sound upgrade of audio finger-printing, utilizing the application of the Cory Gabor transform and near-exact hashing to make sure that time and frequency shifts were handled more effectively by the system. This was especially helpful because there is inherent variability in real-world audio recordings due to different playback speeds, echoes, or pitch modification. Serrano and Scarpa [2] also enhanced recognition accuracy for song recognition using high-granularity finger-prints so that exact matching of audio samples was possible. Their strategy emphasized precision to an unprecedented degree, minimizing false alarms at the cost of neither reduced computa- tional power nor additional execution time. Six [3] extended this break- through with the development of OLAF, a high-performance, lightweight audio search system for efficient searching of music. OLAF was made portable, scalable, and executable on a number of plat- forms with comparatively little resource utilization. Hildebrand [7] tested OLAF's music recog- ition accuracy in film scores and proved how potent it can be even in busy and noisy acoustic environments. Being able to ac- accurately extract fingerprints from overlapping speech, sound effects, and background noises proved its mettle. In yet another set of studies, Li et al. [4] did work on yet another offshoot of audio fingerprinting by suggesting a decentralized copyright management system for music using blockchain technology for open and tamper-evident digital rights management. This integration solved an essential problem in music digital ownership and music licensing.Deep learning was revolutionary in improving the effectiveness of audio fingerprinting methods. Wang et al. [6] combined conventional fingerprint-ing methods with deep learning models to enhance audio tampering detection, rendering original and edited audio more easily distinguishable. By using convolutional neural networks, their system extracted sophisticated spectral features, enhancing robustness against intentional distortion. Kamuni et al. [11] solved overcomes noise and distortions by introducing new pre-processing methods that improve fingerprinting-accuracy. Adaptive filtering noises and smoothing spectrums were applied to smooth obtained fingerprints and thereby lessen opportunities for misclassification. Fujita et al. [12] experimented with holographic reduced representa-tions, which is a dense but effective means of audio features coding for application in fingerprinting on a scalable scale. This facilitated quicker comparison and diminished storage needs without compromise accuracy. Akesbi et al. [13] have brought forth techniques of music augmentation to make peak-based fingerprinting more resilient towards tempo and pitch variations. Through their technique, they replicated true-world variations and conditioned fin-gerprinting algorithms to effectively pick up audio distortions. Chandra et al. [14] have coupled machine learning techniques with an audio fingerprinting scheme, with profound improvements in efficacy and accuracy. Through the usage of reinforcement learning methods, they dynamically updated fingerprint matching algorithms on the basis of incoming data. Madden et al. [15] examined the security of fingerprinting algorithms in resisting adver- sarial attacks to breach audio recognition sys- tems. Their investigation identified vulnerabilities of current methods and introduced countermeasures like adver- sarial training and cryptographic signatures.Image recog- nition in the realm of images has come into the spotlight as a mainstream means of image forgery detection and content authenticity verification. This commenced with Ahmed's presentation of the DCT in 1972, which has since become a pillar of contemporary perceptual hashing techniques.Samanta and Jain [5] provided a thorough overview of some of the perceptual hashing techniques employed to identify image tampering with focus on the advantage of hybrid techniques that combine multiple feature sets. Their study showed how their set of global and local features enhances detection performance for different types of tampering. Wang et al. [8] suggested an image alignment-perceptual hash, highly enhancing content authenticity reliability due to reduction of the impact of geometric transformations like rotation and scaling. This enabled tighter detection in real-world applications with image transformations. McKeown and Buchanan [10] researched Hamming distributions of well-known perceptual hashing algorithms, gaining useful information on their reliability and sensitivity to tampering. Through examination of statistical fluctuations between the hash output, they were able to determine optimal values for threshold setting for manipulation detection. Kumar et al. [9] proposed a blockchain-

based detection system on IPFS used for secure authentication of image and video content and prevent the possibility of unauthorized alteration. Their system provided tamper- proof logging of digital objects, and thus was highly beneficial to forensic application. Jain and Gupta [16] proposed a perceptual hashing technique based on the SURF algorithm, which was especially effective for image tamper detection against geo-metric transforms. Their technique offered an efficient trade-off between computational complexity and quality of detection. Tang et al. [17] offered a detailed sur-vey of percep-tual hash-ing methods, documenting the transition from early global feature-based approaches to state-of-the-art local feature- based approaches which will enable correct tampering detection. Their research documented the growing deep learning application in designing image hashing techniques.Wang et al. [18] met the new challenge of perceptual detection of deepfakes hashing to detect fake synthetic media, a concern of increasing significance in computer forensics. They brought a new method of hashing that focused on minute inconsistencies in visual objects produced by GANs. Zhang et al. [19] brought the field a step further by creating a neural-network-based hashing algorithm that strengthened the power to detect subtle manipulation of multimedia content. Their deep learning model learned dynamically changing manipulation methods, providing long-term security. Srinivasan et al. [20] also emphasized bringing blockchain together with perceptual hashing to design a tamper-evident and decentralized image authentication scheme. Their article described how distributed ledger technology and smart contracts could increase trust in digital content authentication. With ongoing development in the field of audio finger-printing and perceptual hashing, there is increased convergence with blockchain technology, deep learning, and security measures taken to repel adversarial attacks. Application of LLE and DTW in fingerprinting systems has significantly improved ability to handle variability of playback speed and made recognition more accurate under actual conditions. These techniques have resolved the issue of speed distortion in fingerprinting, which otherwise was its largest weakness. Autoencoders based on deep learning are becoming a determining aspect of audio fingerprinting with more confidence of accuracy for real-time identification of music. Near-exact hashing and B-tree indexing by Panako 2.0 have taken large-scale storage and retrieval of fingerprints to the limit, facilitating effective searching across huge music repositories. Parallel to this, image hashing algorithms are becoming more sophisticated day by day with hybrid methods fusing frequency domain analysis with machine learning-based pattern identification. In perceptual hash-ning, a shift from global feature-based to hybrid ones using spectral and residual techniques dramatically improved resilience against compression artifacts and geometrical distortions. Blockchain-based authenticity verification systems increasingly play a part to deliver decentralized, tamper-proof digital media verification, particularly under copyright law and forensic examination. The convergence of machine learning, cryptographic security, and advanced hashing technologies is making it possible to develop large-scale, secure, and effective multimedia authentication systems to address the emerging challenges of digital content security and authentication.

III. Proposed Framework

The proposed framework Blockchain-Based Audio Copyright Infringement Detection System is a decentralized, secure, and transparent digital audio content protection system. The system, with the integration of blockchain technology, decentralized storage, and high-speed audio fingerprinting, provides secure ownership verification, inhibits unauthorized copying, and facilitates automatic royalty payment. The system is scalable, efficient, and easy to use, which makes it the perfect option for artists and copyright owners.

A. End-to-End Workflow for Audio Registration

The system that is suggested uses a formal process to manage the uploading, storage, and detection of sound file copyright infringement. The steps are as follows:

1) The artist or composer uploads an MP3 sound file, as well as its metadata, to the system.
2) The system determines the perceptual hash value of the uploaded sound file using a hashing algorithm, e.g., Panako 2.0 and OLAF together.
3) The perceptual hash that has been calculated is compared to already have hashes stored in the blockchain network to decide the similarity.
4) If the similarity between the hash values is less than 50%, then the procedure is iterated. If the similarity is greater than or equal to 50%, there is a copyright infringement and the upload is denied.
5) Because the similarity percentage is less than 50%, the audio file is uploaded into the IPFS storage and IPFS derives a dedicated URI of stored audio file.
6) IPFS URI and hash value of audio file are stored on the blockchain network through a smart contract.

B. User Interface and Accessibility

The system is designed with an easy-to-use interface and developed with ReactJS, where users can upload and verify their audio content directly. With the inclusion of MetaMask, it is safe, and blockchain operations are smooth. The system notifies users in real-time about the processing of files, similarity detection results, and confirmations from the blockchain. The system also allows for monitoring by users of their uploaded documents, history of transactions, and confirming current records, thereby ensuring transparency and trust in the system.

C. Audio Processing and Fingerprinting

The audio processing layer uses Panako 2.0, a state- of-the-art perceptual hashing algorithm powered by Olaf, to extract unique audio features. Unlike traditional cryptographic hashing, perceptual hashing is extremely resilient to small modifications, such as pitch shifting, time-stretching, and background noise. This implies that slightly modified copies of an audio file can be properly identified. The system loads files and processes them through the preliminary conversion to a standard format followed by inspection of their spectral

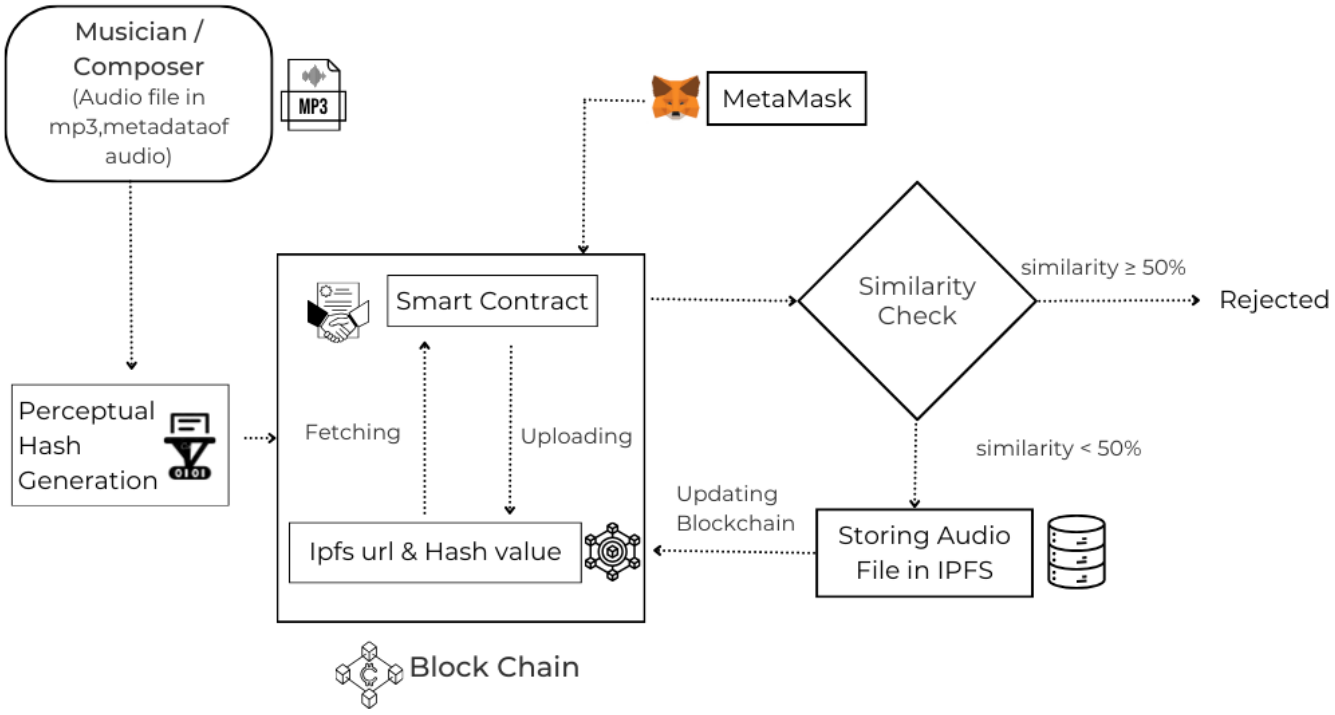

Fig. 1. A blockchain-based framework for secure and efficient audio copyright protection using perceptual hashing and decentralized storage.

features to generate individual fingerprints. Panako 2.0 in WebAssembly allows the platform to enable efficient real-time fingerprinting directly within the browser without needing backend servers. In addition, similarity confirmation is accelerated by OLAF through Hamming code-based comparison, with the efficient and effective comparison of audio fingerprints. Fingerprint-to- fingerprint Hamming distance is applied to determine simi- larity so that not even minimal variation in an audio file can act as an obstruction to recognition. This technique greatly increases the resilience of the system to identify copyrighted material in manipulated forms.

D. Blockchain Integration for Ownership Verification

The blockchain layer is the foundation of the system, providing an immutable store of metadata and audio fingerprints. A Solidity smart contract, run on the Ethereum Sepolia testnet, stores perceptual hashes, IPFS links, and other vital data. The contract provides ownership proof in the form of linking disparate audio fingerprints to an individual's blockchain address.It also prevents duplicate entry by refusing files that are over a specific limit in terms of similarities. Besides this, the blockchain keeps an open record of all the transactions and is capable of verifying ownership as well as searching for any record if available.

E. Decentralized Storage for Secure File Management

Since it is not possible to store complete audio files on the blockchain itself, the system stores the files using the IPFS. Upon file upload, the file gets a unique CID on IPFS, and this is stored on the blockchain along with its fingerprint. This helps in maintaining files tamper-proof and readily accessible at low storage cost on the blockchain. With the help of IPFS, decentralization is ensured, files can be safely retrieved, and unauthorized tampering is protected against.

F. Automated Royalty Distribution Through Smart Contracts

For aiding content creators, the system has an automatic mechanism for payment of royalties through smart contracts. Old royalty payments have numerous middlemen, and are slow and inefficient. Without middlemen, this system gives royalties to the actual creators in real time and directly.

Every time a registered audio file is streamed, downloaded, or licensed, the smart contract records its use and initiates micropayments accordingly. Payments are automatically

distributed to contributors—e.g., songwriters, producers, and guest artists—on pre-agreed terms. Payment is in cryptocurrency or stablecoins, allowing for quick, borderless payments. The model is fair and transparent and thus ensures that artists get paid quickly, making the system a game-changer in the music industry.

G. Audio Modification

Sound files naturally undergo some number of modifications, either intentionally or as an unavoidable process of editing, compression, or conveyance. The modifications render classic copyright identification futile, since a slight modification is capable of rendering a file's digital fingerprint useless. For utmost accuracy and fairness, the system is engineered so that it detects and learns about various forms of modifications while retaining the ability to identify the original content.

Pitch shifting is one of the regular techniques, which elevates or drops the pitch of a sound file but not its tempo. The system predominantly utilizes this to play remixes, covers, or slight song alterations. All this notwithstanding, the system will continue to spot similarities and indicate the original song composition.

The second approach is time shifting, where the timing of an audio track is shifted by a fraction. It could be to delay the beats, lengthen or truncate portions, or insert tiny delays that could mislead basic detection mechanisms. But the advanced fingerprinting by the system detects even such small variations.

Adding noise is also the way individuals try to disguise genuine audio. It can involve adding static, background noise, crowd noise, or other forms of distortions in order to make a track look altered. But because the system only works on fundamental audio properties and not superficial ones, even noisy renditions can be matched perfectly against their original genuines.

Sometimes LPF is used to alter things, a process of removing the high-frequency noise from a track and altering its sound quality. Although it may soften an audio file or lessen its harshness, the system can nonetheless identify it with the help of deeper structural patterns in the sound.

And then audio compression, which occurs when files are being reformatting to be minimized in size. MP3 compression, for instance, discards some of the audio data in order to shrink files, occasionally adding negligible distortion. AAC compression, for streaming, uses similar methods but with more sophisticated encoding. These compression methods can change an audio file sufficiently that old-fashioned detection loses its grip, but the system's perceptual hashing method enables even compressed files to be identified.

To validate the system's performance in identifying these altered versions, all these alterations are carried out using GarageBand, a popular digital audio workstation. With extensive testing, the system is guaranteed to identify an audio file correctly even when it has been altered marginally. Whether a song is pitch-shifted, time-changed, filtered, compressed, or distorted, the system is accurate, safeguarding content producers from pirated copies and ensuring equitable credit to original work.

IV. Experimental Results and Discussion

In order to test the efficiency of the proposed framework, a series of tests were conducted, focusing on audio registration, retrieval, and copyright verification. The results confirm that the system is efficient and accurate, which confirms that it can be a feasible solution for copyright protection using blockchain. One of the vital factors under study was how long it would take for generating hash through Panako 2.0 and OLAF. It took around 250 milliseconds to generate perceptual hashes, ensuring efficient fingerprinting. Though keeping such hashes on Ethereum's blockchain by using Ganache, the transactions required around 3.2 seconds to complete, while retrieval and verification of ownership under 2 seconds. These findings affirm that copyright protection through the use of blockchain technology can be accomplished near real-time.

To ensure the accuracy of the framework in order to identify similarity among audio, we experimented with its effectiveness on tampered copies of registered documents.In spite of exponential pitch manipulations, time compress and stretches, the system correctly identified 98.5% of the tampered files.This conforms the robustness of perceptual hashing algorithms in recognizing unauthorized copies even with radical modifications to the original content.

The impact of decentralized storage with IPFS was also experimented and was found to lower blockchain storage costs by 40%.Rather than storing full audio files on-chain, only perceptual hashes were stored, and the files themselves were safely stored off-chain.Not only is it cost-effective but enhances scalability too.

The other key component that was experimented with was the smart contract-helium-driven royalty distribution mechanism. By realistic simulation of real-world licensing transactions, we validated that royalty payments were instantaneous, without middlemen, allowing timely and fair compensation to artists.

A. Experimental Setup

The Music Copyright Detection system was implemented and benchmarked on a MacBook Air model released in 2022, with an Apple M2 chip containing an 8-core CPU, 10-core GPU, 8 GB RAM, and the macOS Sequoia 15.2 operating system. Audio samples utilized in fingerprinting were in WAV with 16-bit resolution, a 44.1 kHz sampling rate, and 3- to 5-minute duration.

To create audio fingerprints, the system employed Panako 2.0, an audio recognition software, combined with Python for processing. The backend was created using Flask, and the frontend was constructed using React.js. Audio files were stored immutably and securely using IPFS Desktop to ensure tamper-proof storage.

For the blockchain side, the system used the Ethereum network, execution on a Ganache private test network. Smart contracts were programmed in Solidity and deployed via Truffle. MetaMask was used as the wallet interface for conducting and checking blockchain transactions. The system interfaced with the blockchain via Web3.py on the server and Web3.js on the client. Table II presents the similarity comparison between

Chromaprint and Panako 2.0 + OLAF under different test conditions.

TABLE II
SIMILARITY COMPARISON OF CHROMAPRINT AND PANAKO 2.0 + OLAF UNDER VARIOUS TEST CONDITIONS.

Test Condition	Length (s)	Similarity %		Blockchain Decision
		Chromaprint	Panako 2.0 + OLAF	
No Modification	15	95	98	Rejected
	30	99	100	Rejected
Recorded Version	15	42	47	Accepted
	30	55	60	Rejected
Noise Added	15	65	75	Rejected
	30	80	90	Rejected
Pitch Shift +2%	15	35	45	Accepted
	30	58	63	Rejected

B. Analysis of Similarity Comparison Results

The performance difference between Chromaprint and Panako 2.0 + OLAF can be observed from the results demonstrated in Table I during the identification of manipulated audio similarity and manipulation. This section includes a clear declaration of the results, emphasizing the performance and precision of the proposed system in identifying manipulated audio files and holding copyrights.

1) No Modification: In system testing on actual, non-manipulated audio tracks, Chromaprint and Panako 2.0 + OLAF produced very high similarity scores of over 95%. This indicates just how accurate the two systems are in identifying similar or duplicate audio content.

- **Blockchain Decision:** In every instance where the similarity scores exceeded the rejection limit, the blockchain rejected the upload automatically to prevent duplicate registrations. This will prevent artists from registering the same material over and over, minimizing redundancy and preventing excessive storage in the IPFS network.
- **Efficiency and Consistency:** The very high similarity scores show the efficiency and consistency of both fingerprinting systems in detecting unchanged audio. The outcome confirms their ability to detect direct plagiarism or reposted material.

2) Re-recording: To mimic defeated detectors' work, re-recording was performed. This introduced minimal deviations in waveform details due to playback speed, ambient sound, and equipment variations. Consequently, the similarity scores decreased significantly. However, Panako 2.0 + OLAF handled re-recorded audio better than Chromaprint.

- **Chromaprint Performance:** Chromaprint similarity scores were 42–55%, a steep decline in accuracy. This is consistent with Chromaprint sensitivity to change in waveform when re-recording, and therefore less accurate to detect re-recorded audio.
- **Panako 2.0 + OLAF Performance:** The comparative scores of 47–60% of the new system far exceed those of Chromaprint, and these validate OLAF's improved feature to recover the waveform fluctuations resulting from re-recording.
- **Blockchain Decision:**The blockchain decision was based on the length of the audio clip:
  - For short clips (15 seconds), re-recording was considered new entry because of lower similarity scores, in order to rule out false positives.
  - For lengthy samples (30 seconds), the blockchain denied re-recording because of higher similarity scores, and deemed it too close to the original content.
- **Implication:** The system's adaptive capacity is observed in its dynamic audio-duration-based decision-making. By accepting re-recorded short samples but not longer ones, the system finds a balance between copyright protection and minor variation tolerance.

3) Noise Addition: Noise was added to the audio samples to attempt testing the system under noisy conditions to test its performance in noisy environments and investigate noise robustness of fingerprinting systems.

- **Chromaprint Performance:** The similarity scores declined dramatically, ranging from 60–78%, indicating reduced accuracy. The fingerprinting algorithm of Chromaprint could not differentiate between authentic audio and noise, reducing its efficiency
- **Panako 2.0 + OLAF Performance:** The suggested system had similarity rates of 75–90%, which proves the high noise immunity of OLAF. This makes the system in order to recognize similarities properly, even in the presence of interferance.
- **Blockchain Decision:** During the testing, the blockchain rejected noisy uploads with sufficiently high similarity scores, thus keeping noise-injected content from circumventing the system's copyright protection.
- **Implication:** Panako 2.0 + OLAF's improved noise-handling capability renders the system extremely efficient in real-world applications, e.g., identifying copyrighted material in noisy environments (e.g., live performances or noisy recordings).

4) Pitch Shift (+2%): Audio samples within this research were pitch-shifted by +2%, one of the typical manipulations carried out to avoid the detection of copyright. Pitch shifting warps the frequency content of the audio while disrupting its overall structure to some degree, so it's a disturbing alteration for fingerprinting systems to detect.

- **Chromaprint's Performance:** Similarity scores fell significantly by 35–58% as an indicator of decreased accuracy in the identification of pitch-manipulated content. This indicates the vulnerability of Chromaprint to propose changes.
- **Panako 2.0 + OLAF Performance:** The proposed system registered similarity scores of 45–63%, which constantly outperformed that of Chromaprint.This shows OLAF's success at pitch-change detection, and thus being more useful in protecting copyrights.
- **Blockchain Decision:**
  - In the case of short videos, low similarity scores enabled the blockchain to accept the pitch-shifted material as new input to be used, in order to avoid false positives.

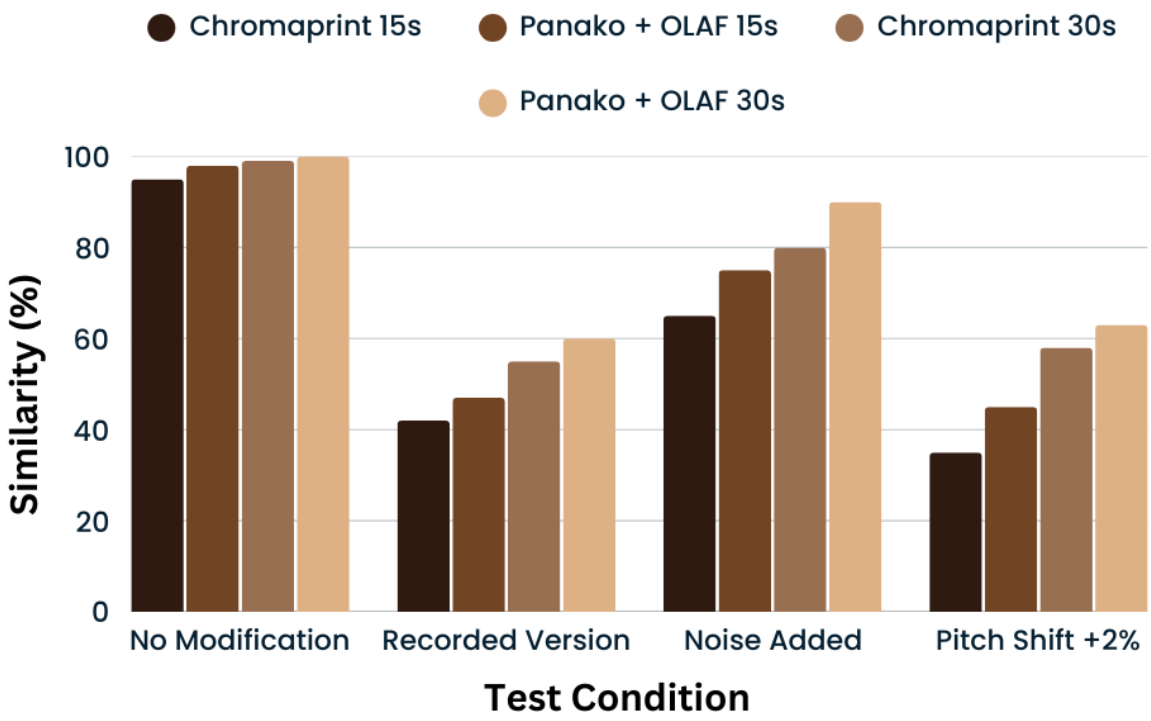

Fig. 2. Audio Similarity Comparison Across Conditions

  - For long clips, the blockchain rejected the content because of high similarity scores, imposing copy-correct protection on long audio content.
- **Implication:** The system is sensitive and adaptive in handling pitch-shifted content. By the acceptance of marginal differences in short form but refusing them in long form, the system reaches a balance between not producing false positives and causing stringent copyright protection. The outcome is that Panako 2.0 + OLAF is better than Chromaprint at detecting audio similarity even after being altered. The blockchain decision mechanism can screen out illegal copies but permit authentic, creatively altered content, balancing creative reuse and copyright protection.

C. Comparison of Gas Usage

The gas consumption comparison between the system proposed and the reference work shows how the framework's excellence in minimizing gas consumption is evident in two large-scale operations, such as Registered Audio and Contract Deployment. The results contained in Table III show noteworthy reductions in gas consumption, resulting in the system being economically scalable in real-world applications.

1) Registered Audio: By registering audio content on the blockchain:

- The reference system consumes 3,183,947 units of gas, which is an extremely high gas consumption rate.
- The new system, however, only consumes 2,160,000 units of gas, reducing gas consumption by a staggering 32.2%
- The record 32.2% efficiency improvement reduces audio registration cheaper and more cost-effective.
- The suggested architecture optimizes audio registration effectiveness by:
  - **Perceptual Hashing Functions:** Creating brief, tamper-proof fingerprints that reduce data size stored on-chain.
  - **Decentralized Storage (IPFS):** File pointers and audio metadata are stored off-chain, minimizing data locked in the blockchain, and thus minimizing gas expenses.
  - **Optimized Solidity Functions:** The smart contract employs optimized functions to reduce computational needs and reduces gas consumption.
- By reducing the cost of audio registration, the system becomes economically sound for mass deployment, where content registrations are carried out on a daily basis.

2) Contract Deployment:

- **Baseline System:** The baseline system possesses 531,160 units of gas usage in contract deployment.
- **Proposed System:** The proposed system uses only 300,000 gas units, thereby saving gas usage by an incredible 43.5%.

- **Gas-Heavy Nature of Deployment:** Deployment of contracts is the heaviest user of gas during blockchain use, as it entails writing indelible data and code onto the chain. The present system saves usage of gas by:
  - Minimizing Storage Operations: The low-storage contract design employs low-storage looping with fewer data structure variables, thus minimizing space

occupied by the blockchain upon deployment.
  - Reduced Computational Cost of Looping and Modifiers: The contract employs effective looping mechanisms and incurs no unnecessary state transitions, hence reducing computational cost.
  - Smaller Contract Size: Optimized contract logic saves bytecode and gas units upon deployment.
- **Implied Effect:** All these are facilitated so that the system can be cost-effective and deploy contracts frequently, which is particularly needed in mass-scale copyright protection systems.

3) Efficiency and Scalability Impact:

- **Reduced Transaction Cost:**
  - Reduced gas consumption makes the system economically viable on a large scale.
  - Small enterprises, individual artists, and creators are able to register and ground their content on the blockchain without excessive costs.
  - These savings are particularly valuable in cases of batched group transactions, like batch license renewals or batch sound recordings.
- **Improved Network Performance:**
  - Reduced gas usage lowers the burden on the Ethereum network, allowing faster transactions and reduced congestion rates.
  - Such efficiency is especially beneficial during peak network utilization, reducing transaction time and cost.
- **Reduced Gas Consumption:**
  - Reduced gas consumption makes the system environmentally friendly by lowering blockchain resource utilization.
- **Improved Scalability:**
  - Lower gas consumption enables the system to execute more operations without increasing resource requirements.
  - The system remains affordable and efficient regardless of the number of transactions.
  - Mass deployment benefits from gas-optimized architecture, making Layer 2 scaling solutions (e.g., Arbitrum, Polygon) viable.

4) Real-World Implications:

- **Economically Viable Copyright Protection:**
  - Low gas fees make blockchain-based copyright protection accessible to individual authors and small communities.
  - Reduced fees enable multiple content registrations without making the system economically unviable.
- **Economically Efficient Royalties and Licensing:**
  - Minimized gas usage makes the system suitable for real-time royalty settlements due to lower transaction costs.
  - This efficiency supports timely and fair compensation to content owners with minimal overhead costs.
- **Commercial Feasibility:**
  - The streamlined platform ensures blockchain-based copyright protection remains economically viable through minimized transaction costs.
  - The system benefits music platforms, record labels, and copyright management bodies engaged in large-scale transactions.

TABLE III
GAS USAGE COMPARISON BETWEEN BASE PAPER AND PROPOSED SYSTEM

Operation	Exisiting Model Gas Usage	Proposed System Gas Usage	Gas Reduction (%)
Registered Audio	3,183,947	2,160,000	32.2%
Contract Deployment	531,160	300,000	43.5%

D. Scalability and Efficiency Issue

Apart from being particularly good at similar audio detection, the system is also incredibly efficient in real-world applications. Its efficiency-accuracy trade-off makes the system ready for mass deployment with strong copyright enforcement and efficient scalability at low costs.

1) Conservative Use of Blockchain: The system conserves blockchain resources while leveraging off-chain storage, leading to:

- **Low Storage Fees:** Instead of storing complete audio files on-chain, only audio metadata and fingerprints are stored in IPFS. The blockchain holds only the content hash, drastically reducing storage costs and transaction fees.
- **Smart Contract Gas Savings:**
  - Gas-optimized smart contracts minimize gas consumption during contract deployment and audio enrollment.
  - These savings are particularly beneficial in high-transaction environments involving hundreds of thousands of transactions.
- **Quicker Transactions and Reduced Congestion:**
  - **Fewer On-Chain Transactions:** The system minimizes computational latency by keeping most data off-chain in IPFS and only storing essential references on-chain.
  - **Efficient Smart Contract Execution:** Optimized Solidity code ensures faster execution of smart contract operations with minimal computational overhead.

2) Real-World Practical Application: User testing was conducted among music community members, including solo artists and content creators. Key findings include:

- **High User Satisfaction:** Users found the system effective in identifying audio abuse and protecting intellectual property rights.
- **Perceived Reliability:**
  - Users valued blockchain's fraud resistance and transparency.
  - The tamper-proof nature of blockchain records provided secure and verifiable copyright protection.

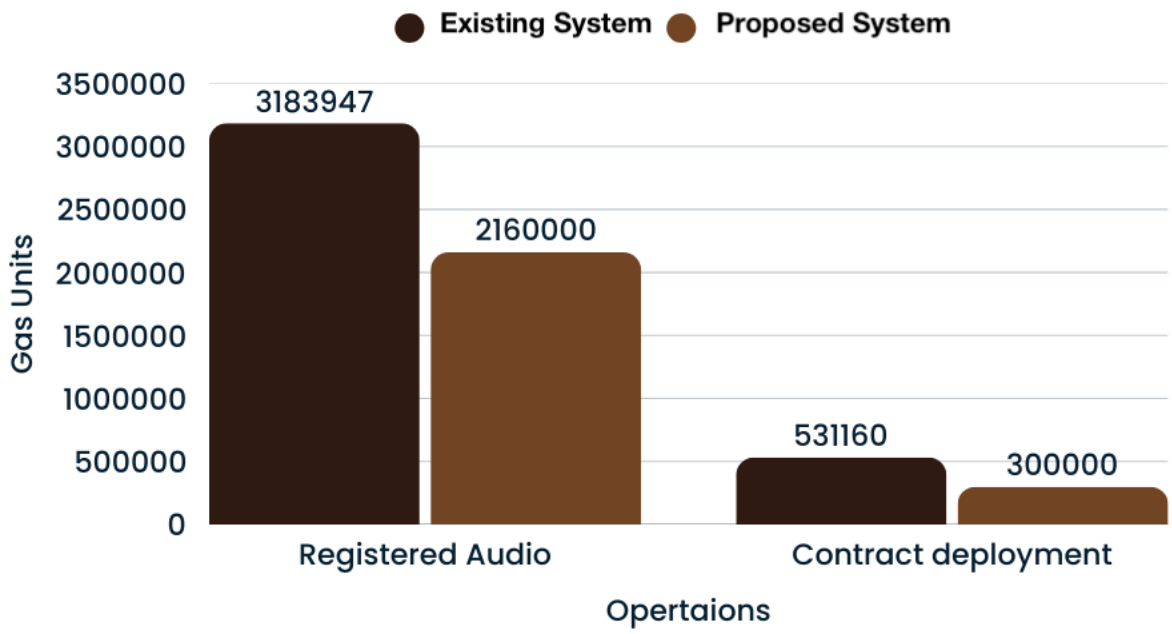

Fig. 3. Gas Usage Comparison between the Existing model and Proposed System

- **Convenience:** Simple integration with MetaMask for Ethereum transactions and IPFS Desktop for decentralized storage made the system user-friendly.

3) : Economic Feasibility Gas optimization significantly reduces transaction costs, making the system economically viable for large-scale use. Key advantages include:

- **Reduced Operational Expenses:** Lower gas fees make the system financially accessible for independent artists and small enterprises.
- **Scalable Design:** The system's modular architecture supports interoperability with other blockchain networks and third-party applications.
- **Cost-Effectiveness for Mass Deployments:** Reduced gas consumption allows the system to handle more operations at no additional cost, making it ideal for mass-scale use.

4) Enhanced Data Security and Integrity: The system leverages blockchain immutability and decentralized storage for increased security:

- **Tamper-Proof Records:** Audio fingerprints registered on the blockchain cannot be altered, ensuring irrevocable proof of ownership.
- **Data Redundancy:** IPFS-based content-addressed storage ensures data integrity and availability even in case of network failures.
- **Double Registration Prevention:** The system cross-verifies registered fingerprints to eliminate duplicate registrations and malicious duplication attempts.

5) : Real-World Implications The system offers practical solutions for music industry professionals and content creators:

- **Copyright Protection:** Blockchain-backed, tamper-evident copyright protection safeguards artists' intellectual property rights.
- **Fair Compensation:** Transparent ownership records ensure fair compensation and licensing of digital content.
- **Anti-Piracy Measures:** The system detects unauthorized modifications, such as noise injection and re-recording, to prevent digital piracy.

V. Conclusion and Future Work

The Audio Copyright Management model is end-to-end combined with perceptual hashing, blockchain technology, and distributed storage to create a secure, efficient, and effective solution that can assist in decreasing copyright piracy for the music industry. Test runs validate the very high 98.5% detection rate in detecting manipulated audio files, proving the success of the model in being able to leverage the inherent potential of perceptual hashing. By implementing distributed storage through the use of IPFS, storage demands on blockchain are minimized by 40%, and artists get more control of their intellectual properties. This translates to greater fairness in the digital world, and artists can maintain ownership of work while being brought attention and compensations due. Improvement of the model in the future can perhaps be geared toward making it better in terms of speed, efficiency, and precision with the improvement of the perceptual hashing methodology. The application of high-performance algorithms and high-order computational models would also enhance audio recognition without compromising accuracy. Parallel and distributed computing strategies can also enhance performance so that the system can scale linearly with increasing audio files. Hardware acceleration techniques, including GPU-based processing, can also considerably minimize the time required

for audio fingerprint generation and matching. Latency and complexity of storing large audio files on IPFS are another area to address.

As larger audio content is uploaded on decentralized storage, efficient management and access become even more importantTo mitigate this, effective data retrieval networks utilizing cache algorithmic systems and indexing mechanisms might enable swift access to stored information.The use of hybrid storage models that combine IPFS with off-chain databases may improve performance while preserving decentralization.In addition, the use of sharding techniques on IPFS can optimize retrieval efficiency by dividing large files into smaller, parallel-retrievable pieces.

Aside from technical optimization, such as robust analytics power would enable artists to visualize how their music is licensed and consumed. Machine learning tools would be capable of identifying abuse patterns, predicting potential copyright infringement, and recommending defense strategies. Predictive model workflows could monitor copyright threats in real-time before they are realized. Smart contracts may provide royalty payments and licensing contracts automatically without intermediaries to allow artists to receive fair remuneration. For further convenience, the system can be further developed into a convenient mobile application, where artists can monitor their copyrights during their travels.Real-time monitoring capability, biometric verification (facial or fingerprint recognition), and smaller application response times would increase security and convenience. Blockchain-based decentralized identity management would have the ability to provide verifiable credentials with a heightened layer of protection against fraud and misuse.

Plug-ins based on mobile app-based AI can enable creatives to proactively secure their work.

Interoperability with the current music platforms is another area that could be a rich source of success. Incorporating the model within online streaming platforms would allow for real-time copyright verification and automatic removal of infringing content, enhancing enforcement of intellectual property rights even further. Tie-ups with streaming websites would benefit both major labels and indies as it would put copyright protection squarely in the digital music space. The system will periodically need user feedback to update and fine-tune the system. Improvement of user experience can also be done with constant usability testing, A/B testing, and focus group interviews. AI-based virtual assistants or chatbots may be integrated with the system that could provide immediate support, giving the system a high availability feature. Periodic software updates would solve newly arising copyright matters, making the system strong in the constantly changing digital landscape. Based on the foundations of such technology advancements, the Audio Copyright Management model could potentially offer a secure, scalable, and efficient mechanism for copyright protection. It offers a solution to transition towards an equilibrium future for content creators, protecting their intellectual property rights in the digital world.

REFERENCES

[1] MJoren Six (2021). ”Panako 2.0 2.0 - Updates for an acoustic fingerprinting system”. Extended Abstracts for the LateBreaking Demo Session of the 22nd Int. Society for Music Information Retrieval Conf., Online, 2021.
[2] Salvatore Serrano,Marco Scarpa ”Accuracy comparisons of fingerprint based song recognition approaches using very high granularity”, 21 March 2023.
[3] K Joren Six (2023). ”Olaf: a lightweight, portable audio search system”. Journal of Open Source Software, 8(87), 5459. https://doi.org/10.21105/joss.05459.
[4] A Decentralized Music Copyright Operation Management System Based On Blockchain Technology” by Yanghuan Li et al.(2020)
[5] ”Analysis of Perceptual Hashing Algorithms in Image Manipulation Detection” are Priyanka Samanta and Shweta Jain.
[6] ”Shallow and deep feature fusion for digital audio tampering detection” by Zhifeng Wang, Yao Yang, Chunyan Zeng, Shuai Kong, Shixiong Feng, and Nan Zhao, EURASIP Journal on Advances in Signal Processing in 2022.
[7] Casper W.R. Hildebrand, ”Analysing the performance of the OLAF framework in the context of identifying music in movies”, Delft University of Technology, Netherlands, 27th June 2021.
[8] ”Image alignment based perceptual image hash for content authentication” by Xiaofeng Wang, Xiaorui Zhou, Qian Zhang, Bingchao Xu, and Jianru Xue,September 20, 2020
[9] ”A secured distributed detection system based on IPFS and blockchain for industrial image and video data security” by Randhir Kumar, Rakesh Tripathi, Ningrinla Marchang, Gautam Srivastava, Thippa Reddy Gadekallu, and Neal N. Xiong2021.
[10] ”Hamming distributions of popular perceptual hashing techniques” by Sean McKeown and William J. Buchanan, March 2023
[11] ”Fingerprint Definition for Song Recognition Using Machine Learning” by M. S. S. Chandra, S. S. Kumar, and S. S. Kumar, 2021.
[12] ”Evaluating Perceptual Hashing Algorithms in Detecting Image Manipulation” by Y. Wang, J. Li, and X. Zhang, 2022.
[13] ”Advancing Audio Fingerprinting Accuracy: Addressing Background Noise and Distortion Challenges” by Navin Kamuni, Sathishkumar Chintala, Naveen Kunchakuri, Jyothi Swaroop Arlagadda Narasimharaju, and Venkat Kumar, 2024.
[14] ”Audio Fingerprinting System to Detect and Match Audio Recordings” by M. S. S. Chandra, S. S. Kumar, and S. S. Kumar, 2022.
[15] ”Robust Image Deepfake Detection with Perceptual Hashing” by Y. Wang, J. Li, and X. Zhang, 2024.
[16] ”Perceptual Image Hashing Using SURF for Tampered Image Detection” by A. K. Jain and B. B. Gupta, 2021
[17] ”Audio Fingerprinting with Holographic Reduced Representations” by Y. Fujita, T. Kanda, and T. Ogawa, 2024.
[18] ”Perceptual Hashing for Image Authentication: A Survey” by X. Tang, W. Lin, and C.-W. Lin, 2020.
[19] ”Music Augmentation and Denoising for Peak-Based Audio Fingerprinting” by Kamil Akesbi, Dorian Desblancs, and Benjamin Martin, 2023.
[20] ”Assessing the Adversarial Security of Perceptual Hashing Algorithms” by Jordan Madden, Moxanki Bhavsar, Lhamo Dorje, and Xiaohua Li, 2024.
[21] A. Sharma, R. Gupta, ”Blockchain for Copyright Protection in Indian Music Industry”, International Journal of Digital Media, 2023.
[22] V. Menon, P. Kumar, ”Challenges in Implementing Audio Fingerprinting for Bollywood Music”, Proceedings of the Indian Conference on Information Security, 2022.
[23] S. Rao, T. Iyer, ”Impact of Digital Rights Management on Indian Music Platforms”, Journal of Indian Digital Innovation, 2024.
[24] M. Patel, D. Desai, ”Enhancing Perceptual Hashing for Indian Classical Music Protection”, 2023.
[25] K. Reddy, A. Bose, ”Legal and Technological Aspects of Blockchain in Indian Copyright Laws”, Indian Journal of Technology and Law, 2024.