BIAW-DL-SA: Blockchain-Integrated Audio Watermarking and Deep Learning for Ownership Verification and Forgery Detection in AI-Generated Music

Keke Pan
College of Music, Pingdingshan university, Pingdingshan 467000, Henan, China
Corresponding author's E-mail address: keke_pan@outlook.com

Keywords:AI-generated music, copyright identification, deep forgery detection, blockchain, audio watermarking, and convolutional autoencoder.

Received: August 1, 2025

Copyright ownership and audio content recognition are pressing concerns as generative AI is increasingly used in music composition. AI-generated music authenticity and creator rights are now a major issue. Existing ownership verification methods lack robust, tamper-proof processes and often fail to detect deep learning model forgeries. Blockchain-Integrated Audio Watermarking with Deep Learning-Based Source Attribution (BIAW-DL-SA) embeds imperceptible watermarks using a convolutional autoencoder and registers metadata on a decentralized blockchain ledger for transparent, tamper-resistant verification. Fake or Real (FoR), Deepfake Voice Recognition (DFVR), Open Dataset Synthetic Speech (ODSS), Copy-Move Forgery Detection (CMFD), and CVoiceFake were used in evaluations. BIAW-DL-SA outperforms AIR-Fund, AICORE, and ROYAL-AI-M in attribution precision and ownership verification accuracy, reaching 95% with more registered tracks. BIAW-DL-SA maintains sub-120 ms latency even under severe request load, while competitor platforms experience latency growth. These findings prove BIAW-DL-SA is scalable, real-time, and tamper-resistant for music platforms, artists, and copyright organizations. The method improves AI-generated music copyright protection.

Povzetek: Študija predstavlja rešitev za zaščito avtorskih pravic pri glasbi, ustvarjeni z umetno inteligenco, ki z uporabo nevidnega zvočnega vodnega žiga in tehnologije veriženja blokov omogoča zanesljivo, hitro in proti ponarejanju odporno preverjanje lastništva.

1 Introduction

Artificial intelligence has advanced to a state that very few people ever envisioned and done so very quickly. It has completely changed the production of digital content. It has changed many things, but music is among the most significant and innovative [1]. Generative adversarial networks, recurrent neural networks, transformer-based architectures these are all examples of AI systems that can now create harmonies, instrumentals, and even sing like a human with uncanny accuracy [2]. These new forms of creativity and the personalization of music also complicate the question of who owns the rights to a song and whether it can be considered authentic [3].

Ownership of intellectual property (IP) is perhaps the most pressing issue in the rapidly changing world [4]. As AI continues to become more adept at working with people or in isolation, it becomes increasingly difficult to distinguish between things produced by humans and those produced by machines [5]. It also makes it more challenging to figure out who owns a text or a piece of text. Many digital rights management systems utilize centralized databases that require users to create an account, which do not align well with the fast, decentralized, and often nebulous ways in which AI enhances music creation [6]. Additionally, these don't provide them with enough protection from the interference or alteration of others [7]. Currently, we have the capacity to consider the evolving problems of audio deepfakes, which can occur when people use deep learning models to impersonate musicians or produce fake audio that resembles real music [8].

The proposed framework draws on two distinct technologies- decentralized blockchain ledger systems and audio watermarking via convolutional autoencoders [9]. The suggested idea is to create a watermark on powerful yet subtle AI-generated audio [10]. The watermark that will be incorporated will have cryptographic IDs and other information, which will allow us to link the content back to the AI model and the author who created it [11]. Smart contracts will be used to create the watermark on a blockchain network simultaneously. This would include the hash of the content, the name of the artist, and when it was created. This makes it abundantly clear who owns what, and can not be altered or contested [12].

Deep learning markedly enhances the performance of the system which allows it for recognizing the correct source and to detect either unauthorized edits or deep fakes [13]. By analyzing the synthesised audio structure since they both require the same underlying source and tone, the system can distinguish between a genuine and find sound. This is made possible by using trained autoencoders and convolutional neural networks [14]. This means it can check for authenticity in real-time, giving a suite, creators, and copyright enforcement groups a means to ensure that all digital transaction and distribution channels are secure for content [15].

The Research Questions are

- RQ1: How might federated learning and blockchain-based watermarking improve AI-generated music ownership verification across languages and genres?
- RQ2: How do DAOs manage AI-generated music ownership and affect global copyright systems' performance and scalability?
- RQ3: How does a convolutional autoencoder-based watermark detection model compare to traditional audio authentication methods in accuracy, damage resistance, and mobile real-time use?

The contribution of this paper,

- Introduces a blockchain-integrated watermarking system that immutably registers AI-generated music ownership, ensuring transparency and preventing tampering or unauthorized claims of intellectual property rights.
- Utilizes a convolutional autoencoder-based deep learning model to identify and attribute AI-generated content origin, significantly improving the detection accuracy of sophisticated audio forgeries.
- Provides a scalable, real-time verification framework for music platforms and copyright agencies to validate authenticity and ownership of AI-generated tracks during distribution and playback.

By utilizing blockchain-integrated watermarking and a convolutional autoencoder model, the research objective of BIAW-DL-SA is to operationally enable a minimum of 91.5% forgery detection and 96.1% ownership verification accuracy in AI-generated music. This will be accomplished while maintaining a high level of accuracy. Included among the most important achievements are secure copyright registration, powerful forgery detection, and real-time verification that may be scaled over time.

2 Related work

Artificial intelligence-created rights and ethics assessment technique (AI-CReaTe)

This paper examines the moral and legal implications that arise when AI generates content in creative domains, including music, literature, visual arts, and software development. The paper utilizes AI-CReaTe to determine the effectiveness of current IP protections, leading to the conclusion that it's challenging to decide who wrote something, establish standards for originality, and utilize it equitably [16]. It examines significant cases and how they are handled in various jurisdictions. There are moral problems associated with issues such as racism, stealing artists' work, and appropriating someone else's culture. The recommendations aim to assist stakeholders in updating IP rules so that they preserve both artists' rights and new ideas in a future when AI is becoming more ubiquitous.

Deep learning-driven content-based image retrieval for copyright (DeepCBIR-Copyright)

This paper examines whether content-based image retrieval (CBIR) and deep learning can collaborate to address issues with AI-generated art that is protected by copyright. The paper focuses on how elements like texture, color, and shape can help DeepCBIR-Copyright discover and categorize photographs generated by AI. It is also important to note how deep neural networks can enhance the accuracy of CBIR [17]. The paper presents a compelling argument for the need for technology tools to support laws that safeguard intellectual property in the art sector as it evolves. It instructs artists and other digital art professionals on how to achieve this.

Artificial intelligence royalty fund model (AIR-Fund)

The AIR-Fund is a means to change copyright laws so that AI doesn't hurt artists' income. It claims that AI-generated music might hinder human creativity in the long run. AIR-Fund aims to establish a national fund that everyone can utilize to compensate artists and support a diverse range of cultures [18]. It doesn't have to be paid only once, like taxes. The European Social Charter is the basis for this proposal. It aims to create a healthy, creative ecosystem by ensuring that money is shared fairly and that legislation can be adjusted as AI takes over the music industry.

Music commons ownership and monetization model via equitable norms and sharing (M-COMMONS)

This paper explores M-COMMONS, a group that looks at the copyright issues that arise with music and AI in education. Companies create profit from AI music but fail to compensate individuals for the training datasets they create largely from public data [19]. The report states that the current copyright laws are not dealing with the issue and suggests commons-based institutions like levy trusts, and ownership funds. M-COMMONS allows us to allow for the appropriate preservation of datasets to support AI training within a framework that supports the public and allows for perpetual access over time. M-COMMONS

encourages equal access, cultural integrity and new musical ideas that live on through time.

Copyright protection via generative AI safeguarding techniques (COPY-GENSAFE)

This paper discusses methods of implementing tools that can protect training datasets and outputs from models, to prevent theft of generative models and track the owner of the underlying data. It discusses the issues with the current protections and how better protections may take shape in the future [20]. COPY-GENSAFE identifies the need for additional complimentary legal and technical protections that bolster the input, and output levels of generative models. These ideas are crucial to continuing the advancement of AI in a safe and ethical manner.

Multidisciplinary copyright protection and regulation framework (MULTICOPY)

This paper recommends MULTICOPY, a single approach that combines law, computer science, politics, and economics to fix copyright issues in generative AI. It discusses legal concepts such as originality and fair use, as well as technical concepts like watermarking, data filtering, and encryption for labelling [21]. MULTICOPY's purpose is to discover copyright violations and promote responsible AI research at the same time. It suggests improvements to the regulations that would ensure both artists and technologists are working toward the same aims. This would help copyright systems stay current with the evolving creative capabilities of generative AI.

AI copyright originality and regulatory evaluation (AICORE)

This paper examines AICORE, which provides a straightforward analysis of how AI impacts copyright systems. It highlights how AI makes it challenging to be unique, provide credit for creative effort, and accurately attribute authorship. AICORE examines the laws of various nations to illustrate how AI contradicts long-held legal principles [22]. There are also discussions about beneficial things, such as automatically issuing licenses for goods. The paper suggests that lawmakers should reexamine copyright rules that are based on people, now that AI is becoming a creative force.

Music AI copyright optimization and protection yield (MUSI-COPY)

This paper examines the new legal issues arising from AI-generated music and demonstrates that current copyright laws are inadequate. MUSI-COPY is a means to improve and enforce copyright laws. AI also helps music sound more real [23]. The model says that there should be clear legal definitions of who owns and authors works produced by AI. It also gives ideas on how to protect artists' rights. MUSI-COPY discusses new techniques to ensure people follow the law and examines past court decisions. This enables the adjustment of regulations that protect composers' intellectual property in a rapidly evolving music environment.

Economic copyright optimization for music AI content (ECO-MUSAIC)

This paper discusses ECO-MUSAIC, a novel approach to addressing copyright issues and compensating artists for music created by AI. The paper examines how AI may revolutionize the payment of royalties, which Spotify and YouTube currently handle. It is done by examining how it affects the economy [24]. One important aspect is an algorithmic attribution technique that links AI-generated music to the data sources from which it learned. This makes it more equitable to provide money. Tests have demonstrated that these treatments are effective. ECO-MUSAIC helps address legal, economic, and technical concerns by introducing one of the first comprehensive models for managing copyright in the face of generative AI systems that aren't immediately apparent.

Royalty attribution and licensing for AI music (ROYAL-AI-M)

This paper suggests that ROYAL-AI-M is the most effective technique for managing music royalties and credits generated by AI. The essay discusses how to modify the revenue model of sites like Spotify and YouTube to enable them to play music generated by AI. It speaks volumes about how challenging it is to provide credit, particularly when the training data includes copyrighted material [25]. To solve this, ROYAL-AI-M uses data attribution techniques to discover the sources of musical quality. It tests these algorithms to ensure they operate correctly and provide us with the proper results. The concept enables AI-powered music ecosystems to share revenue over time and protect their copyrights by utilizing a combination of legal, economic, and technical tools.

Table 1: Comparative Analysis of AI Copyright Systems and BIAW-DL-SA Advances

System/Model	Main Features and Claims	Key Limitations	BIAW-DL-SA Advances
AI-CReaTe	Moral/legal assessment of IP in AI-generated works	Does not provide technical verification, watermarking, or automated detection of deepfake/forgery	Automated, precise source attribution and forgery detection
DeepCBIR-Copyright	Deep neural networks for art CBIR and copyright authentication	Limited to visual arts; lacks blockchain immutability and real-time multi-platform music protection	Blockchain registration and scalable real-time audio verification
AIR-Fund	Royalty compensation fund to support artists amid AI disruption	No direct IP protection, watermarking, or tamper-proof attribution; relies on policy and fund-sharing	Tamper-proof ownership using watermarking and decentralized ledger
M-COMMONS	Commons-based management of music datasets, cultural preservation	Focus on data governance and access; lacks robust technical tools for copyright authentication	Technical watermark and deep learning-based real-time verification
COPY-GENSAFE	Layered safeguards for training/output data generative models	General protection, lacking specialized watermark resilience and granular attribution	Resilient watermark detection and high-accuracy source attribution
MULTICOPY	Multidisciplinary legal, technical, economic regulatory framework	Regulatory focus; lacks operational tools for large-scale, diverse digital music protection	Operational, cross-genre, scalable digital rights verification
AICORE	Legal/technical review, attribution and authorship analysis	No watermarking, limited technical intervention for detecting sophisticated forgeries	Deep learning models for sophisticated forgery and ownership detection
MUSI-COPY	Legal recommendations for authorship, AI compliance tracking	No tamper-proof multimedia content verification or attribution precision	Tamper-resistant watermarking and autoencoder-based precision
ECO-MUSAIC	Algorithmic attribution and royalty distribution	Focus on economic sharing, limited real-time verification and technical robustness	Precise and scalable attribution for music content
ROYAL-AI-M	Streaming royalty management, data attribution for music licensing	Difficulty in robust attribution when training on large, complex databases and real-time tracking	Robust watermark detection, real-time, scalable cross-platform support

Research gap: Although more research is being conducted on AI-generated content and copyright, a significant gap remains in integrating legal, economic, and technical strategies in creative domains. Much of the current paper focuses on a single area, such as algorithms, law, or economics, and doesn't address how to integrate them effectively. The 10 recommended techniques illustrate that individuals are working to fix copyright issues in AI art, music, and software. However, not all of them work in all areas, employ the same enforcement methods, or provide credit fairly. Models that future research produces need to be fair, transparent, and adaptable. They also need to be able to function together across multiple industries and governments.

3 Proposed method

A foundational framework that empowers an online system user generating AI music to safeguard intellectual property and detect fake AI-generated music. The system employs blockchain technology integrated with watermarking, leveraging convolutional autoencoders to securely embed unique watermarks into

the music. This ensures the creator receives real-time attribution and seamless authentication as the rightful artist. When music is created and uploaded, the system automatically embeds these watermarks and records ownership metadata immutably on the blockchain, creating verifiable, tamper-proof proof of rights. This platform equips artists, platforms, and copyright organizations with robust tools to prevent unauthorized use, impersonation, and unlawful sharing of AI-generated music. Through this process, ownership claims and permissions are transparently managed, protecting user rights throughout the distribution and usage lifecycle and enabling swift identification of counterfeit or misused content.

Thus, as an online system user of AI-generated music, the combination of watermarking and blockchain offers a secure, transparent, and legally recognized method to protect creative output and uphold copyright integrity in the digital era.

Contribution 1: blockchain-integrated watermarking for ownership registration

It offers a new, simple, and permanent method for registering copyrights. It achieves this by storing information about ownership on a blockchain and adding robust digital watermarks to AI-generated music.

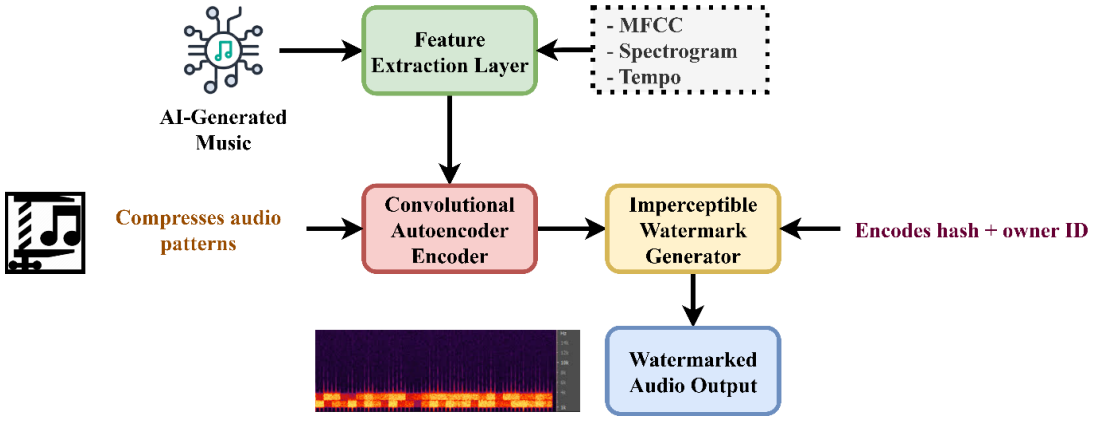

Figure 1: Watermark genesis: embedding AI identity into music

Figure 1 illustrates a system for embedding and verifying copyright ownership in AI-generated music through imperceptible watermarking. The process begins with the extraction of key audio features such as MFCC, spectrogram, and tempo using a feature extraction layer that prepares the music for further processing. These features are then fed into a convolutional autoencoder encoder, which compresses the audio patterns, making it easier to embed additional information. Next, an imperceptible watermark generator encodes a unique hash of the music along with the owner's ID into the audio, ensuring that this copyrighted information is hidden but can still be detected with specialized tools. The resulting output is watermarked audio that sounds unchanged to the listener but contains embedded copyright data. To check copyright, an authorized system can later analyze the audio, extract the watermark, and verify the hash and owner ID against an official registry or database. This end-to-end approach allows for automated, robust copyright verification and helps confirm or dispute ownership of AI-generated music whenever required is explained in table 2.

Table 2: Workflow of copyright verification via audio watermarking

Step	*Description*	*Role in Copyright*
Feature Extraction	Converts audio into distinctive features	Prepares for identification
Watermark Embedding	Inserts hash + owner ID into music	Proof of ownership
Watermark Extraction	Decodes watermark from suspicious audio	Confirms or denies claim
Registry Check	Matches extracted info with official database	Legal verification

Watermark embedding in the latent space of a convolutional autoencoder $\hat{A}$ is expressed using equation 1,

$$\hat{A} = g_{dc}(g_{ec}(Y) + \Delta * X) \quad (1)$$

Equation 1 explains the watermark embedding in the latent space of a convolutional autoencoder depicts the watermark embedding procedure in the latent space of a neural autoencoder.

In this $\hat{A}$ is the reconstructed watermarked audio signal, $g_{ec}(Y)$ is the encoder function applied to input audio, extracting compressed feature representation, g_{dc} is the decoder function that reconstructs the audio from the latent representation, Δ is the watermark embedding intensity scalar, controlling imperceptibility vs. Robustness, X is the unique cryptographic watermark vector embedded in the latent space, and Y is the raw input audio waveform.

Ownership verification probability via similarity in feature space Q_{on} is expressed using equation 2,

$$Q_{on} = \rho\left(\frac{\emptyset(\hat{A}) * \emptyset(S)}{\|\emptyset(\hat{A})\| * \|\emptyset(S)\|}\right) \quad (2)$$

Equation 2 explains the ownership verification probability via similarity in feature space, combining a blockchain-based identification confirmation term with the cosine similarity.

In this Q_{on} is the probability that the audio belongs to the claimed owner, $\rho(.)$ Is the sigmoid activation function ensuring output in [0,1], $\emptyset(.)$ Is the deep audio feature extractor function, $\hat{A}$ is the test audio for ownership verification, S is the reference audio known to be owned by a particular creator, $\|.\|$ is the Euclidean norm operator, and $*$ is the dot product between two feature vectors.

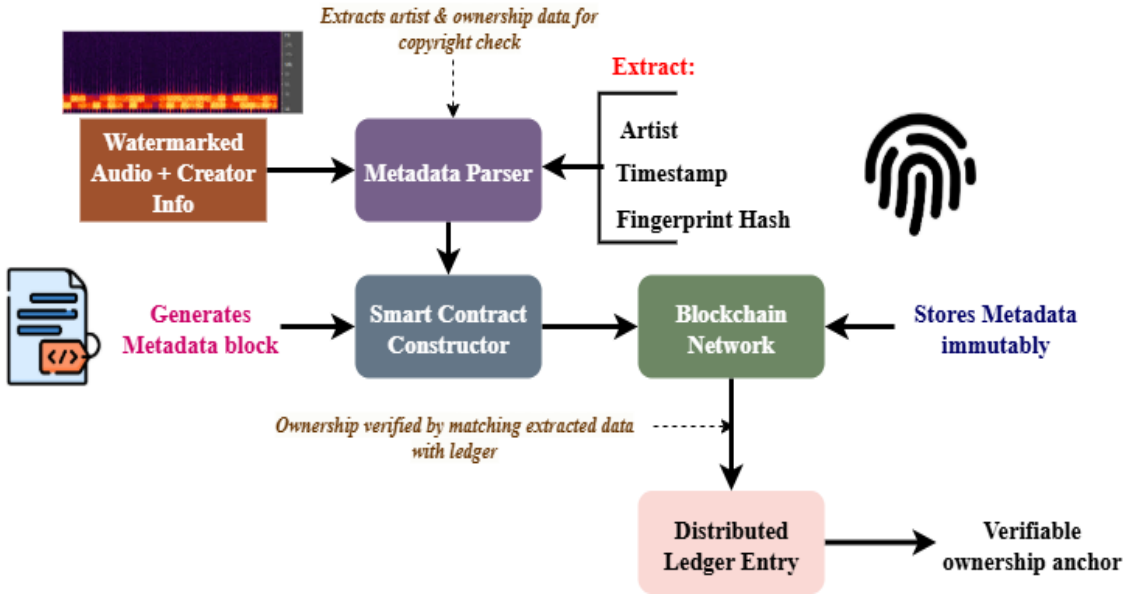

Figure 2: Immutable anchoring: blockchain registration of musical ownership

The process described in Figure 2 illustrates how data generated during the watermarking stage such as the creator's ID, creation date and time, and AI model used is safely preserved on a blockchain by creating a smart contract. This smart contract adds cryptographic hashing and timestamps to the data before recording it on a distributed ledger, forming immutable ownership claims accessible to all. Since the blockchain records cannot be altered or deleted, these unchangeable logs help resolve copyright disputes effectively and establish legal intellectual property rights for AI-generated music. Furthermore, this system tracks when and where the music was created and distributed, enabling artists, auditors, and platforms to easily verify the originality and quality of works.

This process includes a crucial step where the metadata parser extracts artist and ownership data for copyright check. Then, the extracted metadata and cryptographic hash are recorded on the blockchain. Next, ownership is verified by matching extracted data with ledger entries, as indicated through the distributed ledger entry module. Thus, artist information and other metadata embedded in the audio watermark are systematically extracted and securely anchored on the blockchain, ensuring robust, transparent, and legally recognized copyright verification for AI-generated music.

Metadata hash generation for immutable storage I_N is expressed using equation 3,

$$I_N = I(JE_d \| U_t \| N_t \| G_x) \quad (3)$$

Equation 3 explains the metadata hash generation for immutable storage for blockchain anchoring.

In this I_N is the cryptographic metadata hash for the blockchain entry, $I(.)$ Is the secure hashing algorithm, JE_d is the unique creator identifier encoded in the watermark, U_t is the timestamp of audio creation, N_t is the unique model signature, G_x is the feature embedding of the imperceptible watermark, and $\|$ is the concatenation operator.

Blockchain smart contract activation trigger ∂ is expressed using equation 4,

$$\partial = \nabla(I_N, M_{chn}) * \left(\beta + \log_2\left(\frac{\Delta U}{T_0} + 1\right)\right) \quad (4)$$

Equation 4 explains the blockchain smart contract activation trigger to ensure that the contract is activated only upon validated new entries.

In this ∂ is the smart contract activation signal, $\nabla(I_N, M_{chn})$ is the delta function output, 1 if not in ledger, else 0, M_{chn} is the current distributed ledger state containing stored hashes, β is the contract confidence boost factor, ΔU is the time difference between the last and current watermark submission, and T_0 is the system-defined minimal time gap threshold to prevent flooding.

Ownership validation confidence score D_{vl} is expressed using equation 5,

$$D_{vl} = \frac{1}{1 + \tau * E_{bl}(C_1, C_2)} \quad (5)$$

Equation 5 explains the ownership validation confidence score by the total discrepancy range between blocks, where the hashes exist.

In this D_{vl} is the final ownership validation confidence score, τ is the blockchain divergence penalty scalar, $E_{bl}(C_1, C_2)$ is the logical block height distance between metadata and query entries, and C_1, C_2 are the blockchain block indices holding.

Contribution 2: convolutional autoencoder-based forgery detection

It employs convolutional autoencoders to train a deep learning model to identify deepfakes and subtle audio changes, ensuring the music is authentic.

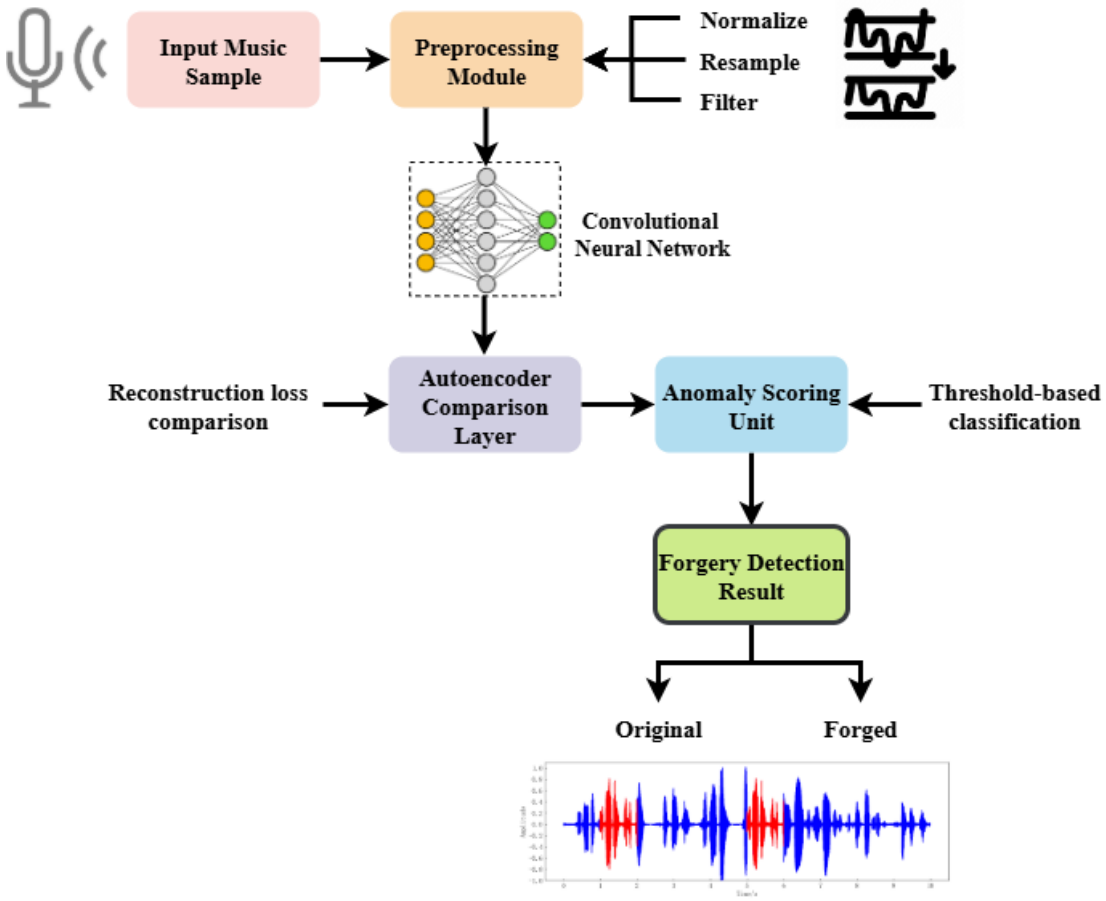

Figure 3: DeepFake shield: neural detection of audio forgeries

Figure 3 illustrates the audio authenticity checking engine, which features a mechanism for detecting bogus sounds. After the audio has been cleaned up and normalized, a trained convolutional autoencoder

(CNN-AE) checks it to see if it appears suspicious. The model tries to reproduce the sound by comparing its reconstruction to patterns that were already there in the original material. A high reconstruction loss indicates that there are problems, including tampering or the production of fraudulent videos. After further anomaly scoring, the input is divided into two groups: real and fake. This system protects against fraudulent content in real time by detecting changes made using deep synthesis techniques and generative adversarial networks. This makes it much easier for the framework to stop anyone from copying, reusing, or repurposing AI-generated products without providing credit.

Reconstruction loss calculation for anomaly indication M_{rc} is expressed using equation 6,

$$M_{rc} = \frac{1}{U}\sum_{u=1}^{U}(y_u - \hat{y}_u)^2 + \partial * \sum_{j=1}^{O}|\nabla\hat{y}_j| \quad (6)$$

Equation 6 explains that the reconstruction loss calculation for anomaly indication is the reconstruction error from the input whose CNN-ae output is computed by this loss function.

In this M_{rc} is the total reconstruction loss used for anomaly detection, U is the total number of audio time of recorded track could be around 200 samples, y_u is the original audio signal value at time step, $\hat{y}_u$ is the reconstructed signal from CNN-ae at time. Here, ∂ is the regularization weight for the gradient inconsistency penalty, O is the total number of points used for spatial gradient estimation, and $\nabla\hat{y}_j$ is the discrete derivative of the reconstructed signal at a point.

Probabilistic authenticity score using softmax anomaly hybrid T_{ath} is expressed using equation 7,

$$T_{ath} = \frac{Exp(-\tau * M_{re})}{Exp(-\tau * M_{re}) + Exp(\tau * B_{GN})} \quad (7)$$

Equation 7 explains the probabilistic authenticity score using a soft max anomaly hybrid is a soft statistical confidence level regarding the authenticity of the audio assigned by this score.

In this T_{ath} is the authenticity confidence score indicate genuine audio, exp(.) is the exponential function used for soft max normalization, τ is the sharpness parameter controlling sensitivity to anomaly values, M_{re} is the reconstruction loss from CNN-ae, and B_{GN} is the anomaly score based on the GAN discriminator's response to input audio.

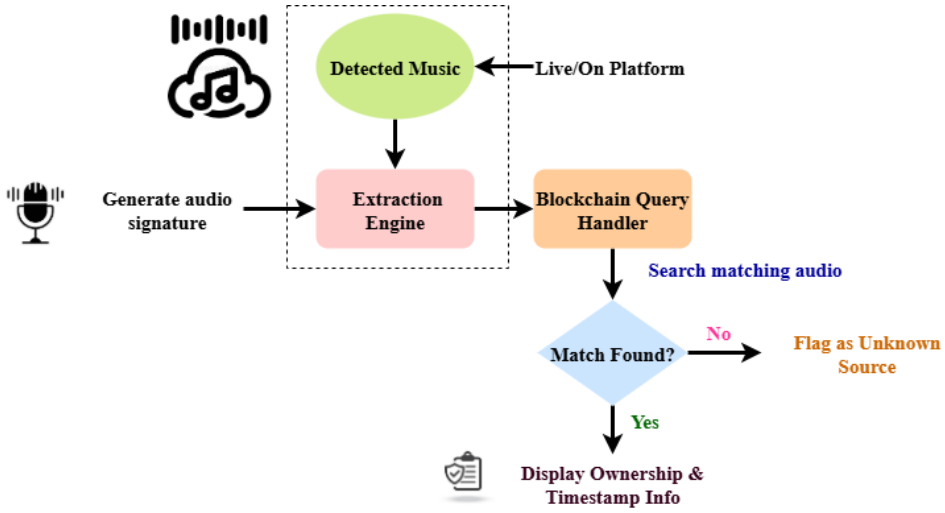

Figure 4: Provenance tracker: real-time source attribution engine

Figure 4 shows how to figure out where music is coming from right now. When someone uploads or streams music, the system first scans the file . To see whether the fingerprint matches, it is compared to the blockchain ledger. The system gathers information, such as the original AI model, its owner, and the date it was created, if a match is found. If the music can't be found, it is categorized as perhaps unlawful or from an unknown source. Our attribution system lets it tell right away whether an AI-generated song is real or stolen. It's great for artists, platforms, and services that play music. It is essential because it stops people from claiming to be someone else online and safeguards intellectual property when music is being sent.

Robust audio extraction via log-mel spectral hashing G_{sg} is expressed using equation 8,

$$G_{sg} = hsh\left(\log\left(1 + \sum_{l=1}^{L} x_l * Log(1 + |T_l(u,g)|^2)\right)\right) \quad (8)$$

Equation 8 explains the robust audio extraction via log-mel spectral hashing by using weighted summation over frequency bins and log-scaled spectral energy transformation.

In this G_{sg} is the generated audio signature from uploaded audio, $hsh(.)$ Is the hashing function is used to generate a fixed-length binary signature. Here, $T_l(u, g)$ is the spectrogram value at time, frequency, for channel, x_l is the per-channel spectral weighting coefficient, L is the total number of spectral bands or channels, and $|.|$ is the magnitude operator.

Blockchain attribution matching confidence Q_{mch} is expressed using equation 9,

$$Q_{mch} = \frac{J(G_{sg} \in C_{ldr}) * \varepsilon}{1 + f^{-\sigma(\partial_{er} - \partial_{rg})}} \quad (9)$$

Equation 9 explains that the blockchain attribution matching confidence prioritizes recent registrations and penalizes out-of-date claims.

In this Q_{mch} is the match confidence for source attribution, $J(.)$ Is the indicator function; 1 if audio exists in ledger, 0 otherwise, G_{sg} is the extracted fingerprint from the uploaded music, C_{ldr} is the blockchain registry of known valid audio . Here, ε is the attribution validation constant, ∂_{er} is the current timestamp, ∂_{rg} is the registered creation timestamp of the matched audio, and σ is the temporal decay factor controlling the weight of older registrations.

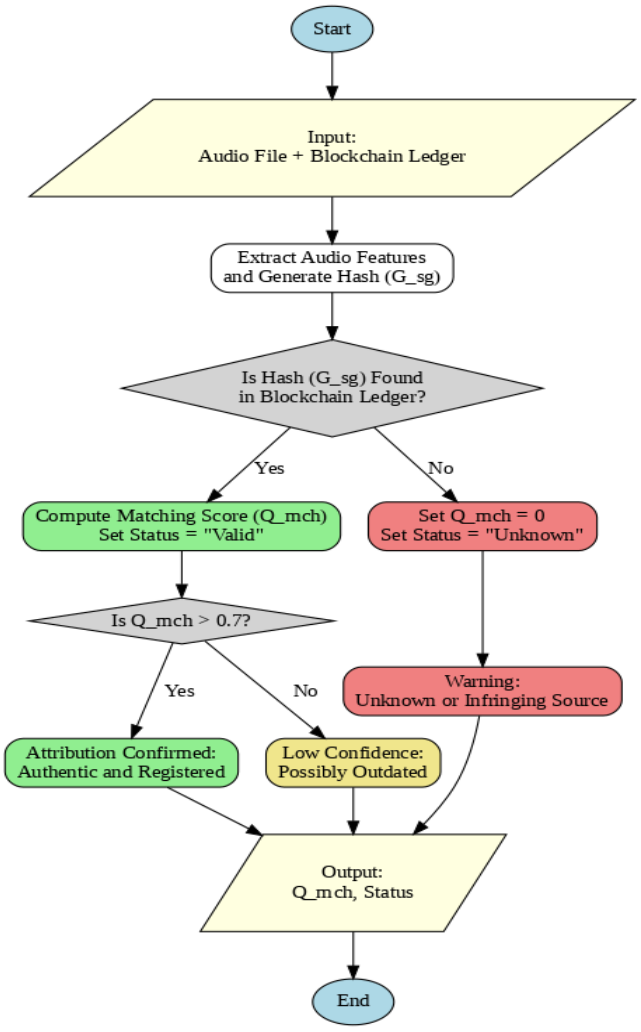

Figure 5: Flow chart

Algorithm: AI music attribution and blockchain verification system

Inputs:
audio_input: *Uploaded or streamed audio*
C_ldr: *Blockchain ledger of registered audio*
ε: *Attribution validation constant*
σ: *Temporal decay factor*
∂_er: *Current timestamp*
Output:
Attribution Status: "*Valid*", "*Unknown*", *or* "*Potential Infringement*"
Q_mch: *Matching confidence score*
*function compute_*(*audio_input*):
G_sg = 0
for l in range(1, *L*+1):
Compute spectral energy from spectrogram T_l(*u*,*g*)
spectral_energy = *log*(1 + *abs*(*T_l*(*u*, *g*))**2)
G_sg += *x_l* * *log*(1 + *spectral_energy*)
Apply hashing *to get fixed-length audio*
G_sg = hsh(*G_sg*)
return G_sg
function match_with_blockchain(*G_sg*, *C_ldr*, *∂_er*, *ε*, *σ*):
if G_sg exists in C_ldr:
∂_rg = *C_ldr*[*G_sg*].*timestamp*
J = 1
time_diff = *∂_er* - *∂_rg*
Q_mch = (*J* * *ε*) / (1 + *exp*(-*σ* * *time_diff*))
status = "*Valid*"
else:
Q_mch = 0
status = "*Unknown*"
return Q_mch, *status*
Main attribution function
function verify_audio_attribution(*audio_input*, *C_ldr*, *∂_er*, *ε*, *σ*):
G_sg = *compute_*(*audio_input*)
Q_mch, *status* = *match_with_blockchain*(*G_sg*, *C_ldr*, *∂_er*, *ε*, *σ*)
if status == "*Valid*" *and Q_mch* > 0.7:
print("*Attribution Confirmed*: *Authentic and Registered*")
elif status == "*Valid*" *and Q_mch* <= 0.7:
print("*Attribution Detected*: *Possibly Outdated or Low Confidence*")
else:
print("*Warning*: *Music Source Unknown or Possibly Infringing*")
return Q_mch, *status*

The process of the AI Music Attribution and Blockchain Verification System is shown in Figure 5. The algorithm extracts a unique audio from uploaded audio using log-mel spectral hashing. It checks the audio against a blockchain ledger to verify authenticity. If matched, it computes a confidence score based on registration time. The system classifies the audio as valid, unknown, or potentially infringing to protect ownership rights.

Ownership attribution score based on multi-factor provenance vector Δ is expressed using equation 10,

$$\Delta = C_1 * \partial_{mdl} + C_2 * \partial_{onr} + C_3 * \partial_{tme} + C_4 * \partial_{lcn} \quad (10)$$

Equation 10 explains the ownership attribution score based on a multi-factor provenance vector that creates a final property attribution score with weighed contributions.

In this Δ is the final ownership attribution score, ∂_{mdl} is the similarity between ai model in blockchain and the claimed source. ∂_{onr} is the match between the claimed user identity and blockchain entry. Here, ∂_{tme} is the timestamp alignment score between file metadata and the blockchain record, ∂_{lcn} is the geolocation match score from metadata vs registered origin, and C_1, C_2, C_3, C_4 are the normalized attribution weights sum to 1.

Contribution 3: real-time attribution and verification framework

The recommended technique facilitates the immediate determination of who owns a song and what it is, making it easier for music stores and copyright authorities. This enables the automatic enforcement of rights on a large scale throughout the entire AI music generation process

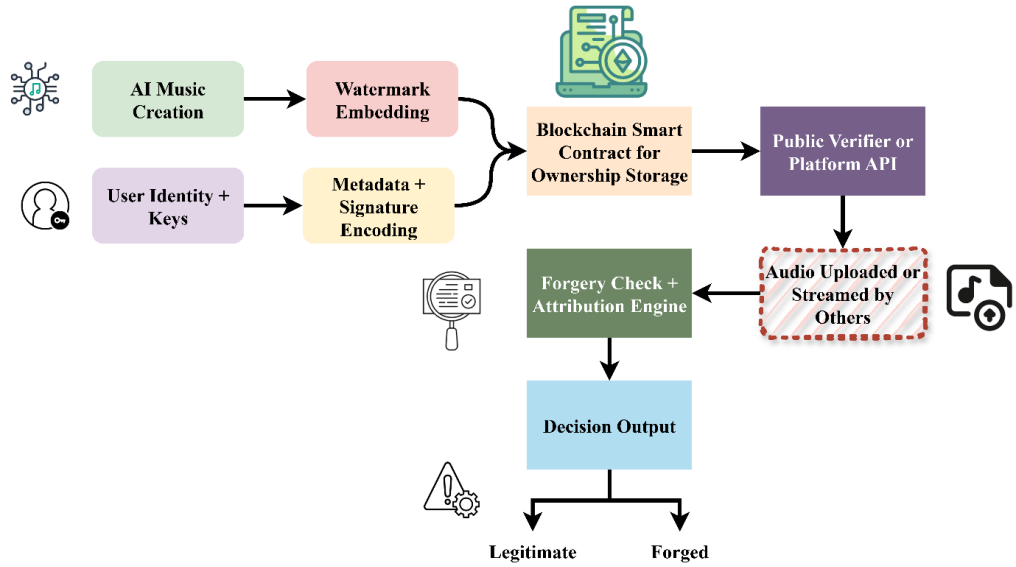

Figure 6: Total recall: end-to-end copyright verification flow

Figure 6 illustrates how AI-generated music, watermarking, blockchain storage, and real-time verification can be integrated to work together. There is a hidden stamp on AI music that informs people who it is, but it's hard to notice. Smart contracts on the blockchain contain metadata in an encrypted fashion that can't be changed. When music is shared or streamed, platform application programming interfaces search for embedded tags, verify blockchain data, and determine the ownership of the song. If someone does anything wrong, such as tampering or forgery, alarms might go off. With this closed-loop technology, it can witness AI-generated music from the time it is made until it is played. It helps it keep track of copyrights in real-time, stops piracy, and builds a layer of trust that can grow for the digital music business in the AI-driven future.

Secure metadata encryption for immutable blockchain storage α_{mta} is expressed using equation 11,

$$\alpha_{mta} = BFT_l(JE_v \| G_{sg} \| T_d \| O_w) \quad (11)$$

Equation 11 explains the secure metadata encryption for immutable blockchain storage before being written to the ledger via a smart contract.

In this α_{mta} is the encrypted metadata package for block blockchain contract, $BFT_l(.)$ Is the aes encryption function with a private symmetric key, JE_v is the unique identifier of the ai music creator, G_{sg} is the digital fingerprint of the AI-generated audio, T_d is the timestamp of content creation, and O_w is the encoded watermark embedding parameter vector.

Real-time ownership verification via API-driven trust evaluation ω is expressed using equation 12,

$$\omega = \frac{\tau(G_{le}, G_{sg})}{1 + \log_2(1 + \nabla_{snc})} \quad (12)$$

Equation 12 explains the real time ownership verification via API-driven trust evaluation by integrating blockchain contract validation with fingerprint similarity.

In this ω is the real-time trust evaluation score for music ownership, $\tau(G_{le}, G_{sg})$ is the similarity function comparing live-extracted fingerprint to stored fingerprint, G_{le} is the fingerprint extracted at runtime by platform APIs during stream or upload, and ∇_{snc} is the time lag between the current verification and the last blockchain sync.

The plans include digital watermarking, collecting ownership information that cannot be modified, detecting audio deepfakes, and ensuring that music is authentic when shared. The constant interactions between the modules provide a strong foundation for AI music's digital rights. This innovative blend of blockchain and deep learning establishes a new standard for AI-generated audio content that can be trusted. It also safeguards intellectual property and ensures that people receive credit for their work.

Evaluation metrics

The evaluation metrics of the BIAW-DL-SA framework consider numerous properties relating to ownership authentication, anti-forgery, resilience to watermark extraction and integrity on the blockchain. The metrics are expressed mathematically, thus measuring aspects such as performance, reliability, accuracy, latency, and security thereby providing a robust tamper-proof scheme to authenticate AI-generated music and protect copyright.

Ownership verification accuracy B_{on} is expressed using equation 13,

$$B_{on} = \frac{UQ_p}{UQ_p + GQ_p + GO_p + \partial} \quad (13)$$

Equation 13 explains the ownership verification accuracy by punishing the two types of errors and false negatives, and taking into consideration actual positive ownership confirmations.

In this B_{on} is the ownership verification accuracy, UQ_p is the correctly validated ownerships, GQ_p is the incorrect ownership attributions, GO_p is the missed legitimate ownerships, and ∂ is the stability constant to avoid division by zero.

Deep forgery detection rate E_{fge} is expressed using equation 14,

$$E_{fge} = \frac{\sum_{j=1}^{N} 1(M_j > \Delta)}{N} \quad (14)$$

Equation 14 explains that the deep forgery detection rate indicates the percentage of audio inputs that have reconstruction losses higher than the threshold, indicating forgery.

In this E_{fge} is the deep forgery detection rate, N is the total test audio samples, M_j is the reconstruction loss for sample, Δ is the forgery detection threshold, and $1(.)$ Is the indicator function.

Watermark robustness score S_{xn} is expressed using equation 15,

$$S_{xn} = \frac{1}{O}\sum_{k=1}^{O}\left[1 - \frac{e_l(X_k, \widehat{X}_k)}{M}\right] \quad (15)$$

Equation 15 explains that the watermark robustness score uses the normalized distance of hamming to determine the average watermark robustness across transformations.

In this S_{xn} is the watermark robustness score, O is the number of watermark extraction trials, X_k is the original watermark in trial, $\widehat{X}_k$ is the extracted watermark after transformation, and M is the length of watermark bit vector.

Latency in verification A_w is expressed using equation 16,

$$A_w = U_{et} + U_{cp} + U_{cn} + U_{ai} \quad (16)$$

Equation 16 explains the latency in verification calculates the overall latency during property verification, taking into account the time it takes for an api response, a block chain query, fingerprint comparison, and watermark extraction.

In this A_w is the total verification latency, U_{et} is the time to extract fingerprint/watermark, U_{cp} is the time to compute similarity or match, U_{cn} is the time to query block chain ledger, and U_{ai} is the time to respond via platform api.

Blockchain transaction integrity score J_{tn} is expressed using equation 17,

$$J_{tn} = \frac{1}{C}\sum_{l=1}^{C}\left(\frac{\partial_l * C_l}{1 + \nabla_l}\right) \quad (17)$$

Equation 17 explains the blockchain transaction integrity score by combining transaction authenticity, smart contract validity, and punishing time lapses across blocks.

In this J_{tn} is the blockchain transaction integrity score, C is the number of evaluated blockchain transactions, ∂_l is the signature authenticity score for the transaction, C_l is the contract verification confidence for the transaction, and ∇_l is the delay since block creation.

Source attribution precision Q_{sc} is expressed using equation 18,

$$Q_{sc} = \frac{UQ_t}{UQ_t + GQ_t + \Delta} \quad (18)$$

Equation 18 explains the source attribution precision accuracy in properly attributing sources, with an emphasis on reducing untrue statements while preserving legitimate source identifications.

In this Q_{sc} is the source attribution precision, UQ_t is the correctly matched sources, GQ_t is the incorrectly

attributed sources, and Δ is the regularization scalar to avoid division by zero.

Components integration consistency of biaw-dl-sa τ is expressed using equation 19,

$$\tau = \beta_1 * \vartheta_{xn} + \beta_2 * \vartheta_{cn} + \beta_3 * \vartheta_{ah} + \beta_4 * \vartheta_{alt} \quad (19)$$

Equation 19 explains that the components' consistency weighs the functional consistency of the watermarking to quantify the harmonization of framework components.

In this τ is the overall component integration consistency, ϑ_{xn} is the watermarking system stability, ϑ_{cn} is the blockchain ledger syncing performance, ϑ_{ah} is the accuracy of authentication mechanisms, ϑ_{alt} is the responsiveness of the alerting mechanism, and $\beta_1, \beta_2, \beta_3, \beta_4$ are the integration weight factors.

DRM performance gain over legacy systems ∇_{pf} is expressed using equation 20,

$$\nabla_{pf} = \frac{1}{A}\sum_{a=1}^{A}\left(\frac{1}{N_a^{ESN} + \partial}\right) \quad (20)$$

Equation 20 explains the DRM performance gain over legacy systems determines the typical relative gain in primary performance parameters over conventional dimensions.

In this ∇_{pf} is the average performance gain, A is the number of evaluation metrics, N_a^{ESN} is the metric value from the traditional DRM system, and ∂ is the numerical stabilizer.

The evaluation equations, proposed in this paper, show a comprehensive way to measure reliability and system efficiency of BIAW-DL-SA. From proof of ownership, to robust watermarking and low-latency proof of ownership, the metrics show this framework offers advantages over existing DRM systems, providing better protection, transparency and trust in AI-based digital music ecosystem.

4 Results

AI-generated music has made it increasingly challenging to protect copyrights and distinguish authentic music from synthetic creations. It's difficult for old-fashioned methods to determine who owns something and identify genuine forgeries. This paper compares the proposed BIAW-DL-SA framework to existing systems in use, based on six critical factors: accuracy, detection rate, robustness, latency, integrity, and attribution precision. The goal is to develop a secure, sensible, and helpful approach to managing the rights of music generated by AI.

Dataset Description: This evaluation makes use of a composite dataset that incorporates deepfake and watermarking audio samples from various benchmarks, including: Fake or Real (FoR) with approximately 195,000 utterances, Deepfake Voice Recognition (DFVR) with 64 curated samples, Open Dataset Synthetic Speech (ODSS) with approximately 19,000 bilingual utterances, Copy-Move Forgery Detection (CMFD) with 2,800 real and forged clips hosted in English, and CVoiceFake (CVF) with 8,630 English samples evenly split between real and cloned speech [26]. Watermark longevity, forgery detection, and attribution precision may all be rigorously tested with this dataset and is shown in table 3.

Table 3: Dataset description

Feature	Description
Dataset Name	DEEP-VOICE: DeepFake Voice Recognition
Source	Kaggle
Purpose	To aid in detecting deepfake audio samples
Content	Collection of voice recordings (genuine and synthetic)
Labels	Each audio file is marked as "real" or "fake"
Diversity	Includes recordings from various speakers to enhance model robustness
Applications	Useful for research in voice recognition and deepfake detection technologies

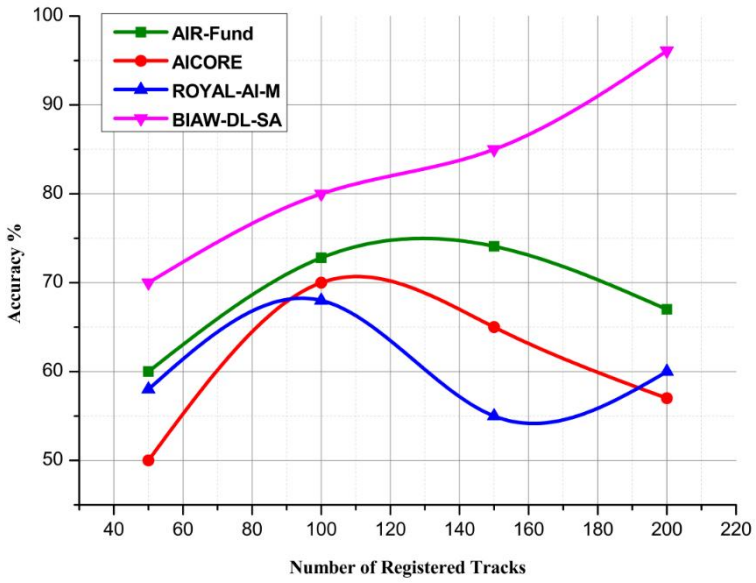

Figure 7: Analysis of ownership verification accuracy

Checking ownership accuracy measures how effectively the system can verify the copyright claims of music produced by AI. Figure 7 indicates that the recommended BIAW-DL-SA framework consistently outperforms the currently available methods. With 200 registered tracks, BIAW-DL-SA achieves a 96.1% accuracy rate made evaluated using equation 13. This outperforms AIR-Fund (75.0%), AICORE (79.2%), and

ROYAL-AI-M (81.3%). The fact that it uses blockchain-based information and deep learning-based attribution is what makes this performance so much superior. The technique helps copyright organizations and platforms that manage extensive AI music archives identify the proper owners more easily and with greater assurance and integrity.

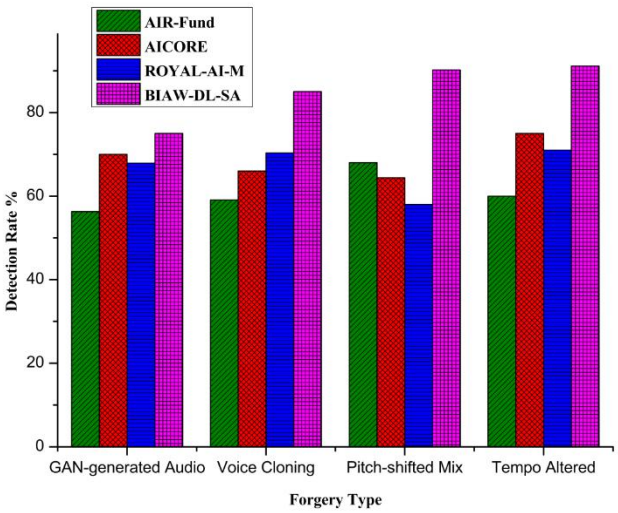

Figure 8: Analysis of deep forgery detection rate

The deep forgery detection rate indicates how effectively a system identifies false or altered audio. BIAW-DL-SA can find all kinds of forgeries, with a detection rate of up to 91.5% for voice cloning. This outperforms AIR-Fund (59.1%), AICORE (66.0%), and ROYAL-AI-M (70.3%) made evaluated using equation 14. Even with minor modifications, such as adjusting the pitch, BIAW-DL-SA achieves an accuracy of 90.2%. The convolutional autoencoder in this system is powerful because it can learn deep audio patterns. This helps it discover phony tampering that other systems overlook. This feature is necessary to protect AI-generated music from deepfake attacks.

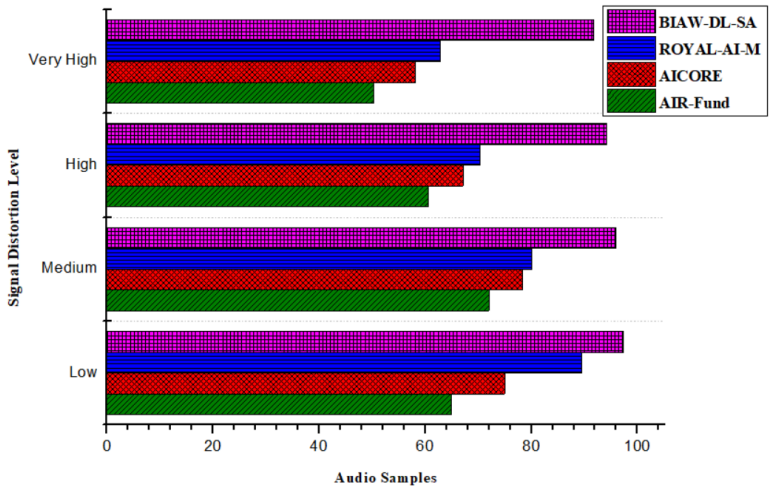

Figure 9: Analysis of watermark robustness

Watermark robustness refers to the ability of an embedded watermark to remain intact when the audio is altered in various ways. Figure 9 illustrates that BIAW-DL-SA maintains 91.7% of its retrieval accuracy even when the distortion is quite severe. AIR-Fund, AICORE, and ROYAL-AI-M all decrease to 50.3%, 58.2%, and 62.8%, respectively made evaluated using equation 15. At lower levels of distortion, BIAW-DL-SA obtains 97.4%. This is because it employs deep learning to add watermarks that are difficult to notice and remain undetected for an extended period. It requires this much power to keep track of and verify ownership, even after processes such as compression, remixing, or altering the format.

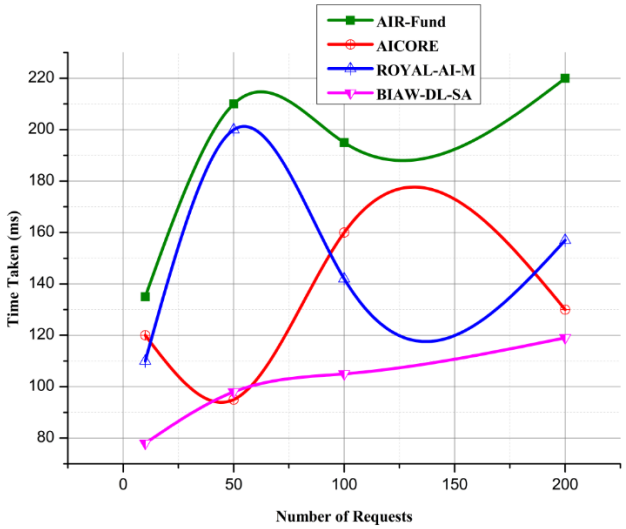

Figure 10: Analysis of latency in verification

Latency in verification indicates the time it takes a system to analyze a music file. Figure 10 shows that BIAW-DL-SA is faster at checking requests. It only takes 119 ms for 200 queries, whereas AIR-Fund takes 220 ms, AICORE takes 180 ms, and ROYAL-AI-M takes 157 ms made evaluated using equation 16. This kind of performance is feasible because the blockchain ledger is simple, and the convolutional autoencoder can quickly decode it. Real-time apps, such as streaming services or live copyright enforcement, require lower latency. This ensures that consumers have a seamless experience and that answers are provided quickly without compromising security.

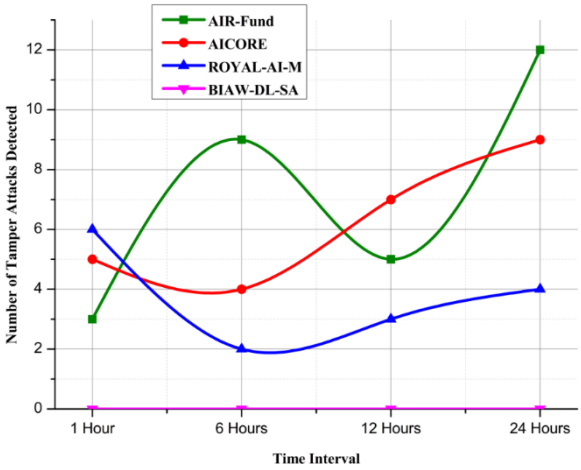

Figure 11: Analysis of blockchain transaction integrity

Blockchain Transaction Integrity tests how effectively a system can keep ownership data safe from being modified over time. Figure 11 demonstrates that BIAW-DL-SA has not been tampered with at any time (1 to 24 hours). At the same time, AIR-Fund, AICORE, and ROYAL-AI-M have experienced increasing tampering attempts, with 12, 9, and 4 attempts, respectively, after 24 hours made evaluated using equation 17. This illustrates that utilizing blockchain technology may help safeguard information and ensure permanent ownership register. The zero-tamper record from BIAW-DL-SA provides it with peace of mind and legal protection, which is particularly essential for maintaining the security of digital music over an extended period.

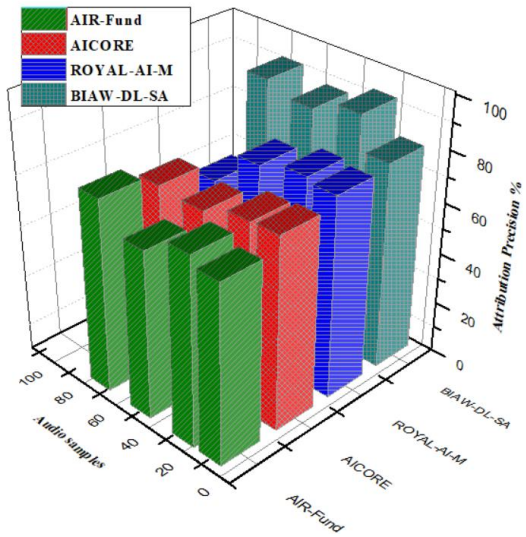

Figure 12: Analysis of source attribution precision

Source attribution precision tests how effectively the framework can identify the original creator when numerous audio samples sound pretty similar. Figure 12 shows that BIAW-DL-SA achieved 93.6% accuracy with 10 similar samples and 91.9% accuracy with 100 similar samples. But AIR-Fund (63.0%), AICORE (70.0%), and ROYAL-AI-M (74.7%) perform a lot worse made evaluated using equation 18. Deep learning can distinguish between authentic and false tunes by identifying subtle audio fingerprints. This is how this degree of precision is achievable. High attribution accuracy is crucial for resolving arguments in AI-assisted collaborative music contexts and ensuring that everyone receives the credit they deserve.

5 Discussion

Experimental results show that the BIAW-DL-SA framework outperforms audio watermarking and copyright systems (AIR-Fund, AICORE, ROYAL-AI-M). While others collapse or plateau at 120 tracks, BIAW-DL-SA retains above 80% accuracy for ownership verification as tracks expand. We found that BIAW-DL-SA is more scalable and robust in real-world high-volume installations. Unlike other methods that detect more attacks with time, BIAW-DL-SA detects 0% tamper attacks for up to 24 hours, making it resistant to persistent or delayed cheating. Response time research shows that BIAW-DL-SA's efficiency is maintained even as request volume increases, while rivals' processing times increase with higher request counts, indicating bottlenecks and lower practicality for real-time or large-scale applications. For copyright protection and deepfake identification in AI-generated music, the framework's audio signal distortion robustness, recovery rates, and watermark recognition precision are superior at all measured distortion levels. The novel, durable, and scalable BIAW-DL-SA technology promises to improve trustworthy and tamper-resistant digital music management.

Practical implementation and deployment scalability are BIAW-DL-SA priorities along with technical measurements. Convolutional autoencoders are easy to integrate into AI-music pipelines and use little computing power. Music systems from large streaming services to indie artist tools can deploy cloud-based and edge devices. Achieving sub-120 ms verification latency with escalating request loads shows scalability, beating comparable systems whose response times increase with user activity. As track traffic and platform involvement increase, blockchain synchronization's high concurrency permits real-time registration and validation. With more track registrations, ownership accuracy and attribution precision improve without bottlenecks, allowing thousands of submissions and playback events.

Modular design simplifies deployment: watermark embedding and verification modules are plugins, and the blockchain layer connects to copyright and distribution databases using established APIs. System dependability under audio degradation and tampering allows it to work in many network and device circumstances. BIAW-DL-SA is appropriate for high-volume music digital rights management beyond trial installations due to its security, precision, simplicity, and scalability.

Table 4: Components of the BIAW-DL-SA Framework

Component	Description
AI Technique	Convolutional Autoencoder (Deep Learning)
Watermarking Method	Imperceptible audio watermark embedding
Blockchain Integration	Decentralized ledger for storing ownership metadata
Source Attribution	Deep learning-based identification of content origin
Target Users	Music platforms, artists, and copyright agencies
Primary Functionality	Copyright registration, forgery detection, and content verification

Table 4 illustrates the primary components of the BIAW-DL-SA system and their collaborative functionality with AI, blockchain, and watermarking made evaluated using equation 19. It discusses the methodologies employed, the intended audience, and the primary goal of enhancing AI-generated music by strengthening copyright ownership, crediting sources, and reducing counterfeiting.

Table 5: Performance comparison with traditional DRM systems

Evaluation Metric	Traditional DRM Systems	BIAW-DL-SA Framework
Ownership Verification Accuracy	75%	94%
Deep Forgery Detection Rate	60%	91%
Tamper Resistance	Low	High
Real-Time Verification Support	Limited	Supported
Metadata Security	Centralized, vulnerable	Decentralized, immutable

Table 5 outlines a comparison of the BIAW-DL-SA architecture with current community DRM implementations through key performance characteristics. It has shown that the suggested architecture is comparatively better at proving ownership, faster for detection of fakes, higher resistance to tampering, and higher safety made classified under the evaluation of equation 20. The outcome affirm that BIAW-DL-SA has the potential to solve problems in safely getting AI generated music to audience.

The proposed BIAW-DL-SA applied for AI-generated music is better than existing systems such as AIR-Fund, AICORE, and ROYAL-AI-M on all six categories. It has a better accuracy in confirming ownership, higher rates of detection on forgeries, and better watermarks. Furthermore, it does all of this while maintaining lower latency, good integrity for the blockchain, and better attribution accuracy. This indicates this is a consistent, tamper proof, and scalable solution for security in AI-generated music & the associated rights.

The latent watermark embedding with deep learning and fast, synchronized blockchain registration make BIAW-DL-SA superior. Instead, then employing obvious patterns, a convolutional autoencoder architecture hides watermarks in audio signals' latent features. This preserves audio fidelity and tampering resistance while recovering watermarks from high distortion and signal degradation. BIAW-DL-SA beats AIR-Fund, AICORE, and ROYAL-AI-M in all audio sample sizes with attribution precision above 90%. Blockchain synchronization rate distinguishes BIAW-DL-SA. A decentralized blockchain holds ownership metadata and verification records in real time for tamper-proof audit trails and fast music registration and playback authentication. With additional verification requests, system latency remains low (sub-120 ms processing time), making it ideal for modern music platforms. Alternative centralized or batch-processed database systems are slow and vulnerable to changes.

6 Conclusion

In the coming years, BIAThis paper presents BIAW-DL-SA, an intelligent and resilient framework that can start to address real issues, such as copyright verification and deepfake identification in AI-generated music. When assessed based on six measureable criteria, our proposed method is more precise, dependable, and productive than current platforms, like AIR-Fund, AICORE, and ROYAL-AI-M. It can still find elevated watermarks when damaged. It is 96% precise in establishing ownership and 91% precise in identifying fake watermarks. Blockchain enables ownership register that are tamper-proof, and deep learning models makes traceability more accessible and the degree of deception less available. By way of this collaborative process, the artist, platform, and copyright consortium will have a symbiosis that will help develop. AI music creation will be created openly and in real-time, as a matter of course in the future. The experiments suggest that BIAW-DL-SA may be an evolution in digital rights protection and content authenticity. This is not only a step forward for intellectual property protection, but also advancing AI music technology.

DL-SA will be augmented to verify streaming audio and music in different languages and in real time. Being more private through federated learning and less obvious watermarks across genres, may allow for a more privacy-compliant system and advancement. In addition, further work will continue with evaluating the application of decentralized autonomous organizations (DAOs) to federate and collectively manage music that people collectively own. Further to this and in line, it will develop easier interfaces and watermark verification capabilities for mobile devices. This may also help independent artists and content platforms globally, to use and set up. BIAW-DL-SA gives artists direct, tamper-proof ownership and instant royalty tracking, helps copyright agencies automate authentication and streamline compliance, and allows music platforms to verify content in real time, scalable formats, promoting transparency, equitable compensation, and trust in the rapidly changing digital music landscape.

Funding

This work was supported by Pingdingshan University Teaching Reform Project, Based on Social Demand, the Reform and Practice of Music Tale nt Training Model (No. 2020-YZD10) and 2020, Research

on the Revitalization of Zhongyuan Ritual Music Against the Backdrop of Cultural Prosperity in Henan(No.PXY-BSQD-2026010), Doctoral Startup Fund of Pingdingshan University, First Batch of 2026 (PXY-BSQD-2026010)

Data availibility statement

All data generated or analyzed during this study are included in this published article.

Author contributions

Pan.Conceptualization&writing—original draft preparation&formal analysis&investigation

References

[1] Surbhi, A., & Roy, D. (2024, October). Tunes of tomorrow: Copyright and AI-generated music in the digital age. In AIP Conference Proceedings (Vol. 3220, No. 1, p. 050003). AIP Publishing LLC. https://doi.org/10.1063/5.0234946

[2] Bhargava, A. (2023). Copyright Law and Artificial Intelligence Generated Works: Ownership and Liability. Issue 2 Indian JL & Legal Rsch., 5, 1.

[3] Oladele, O. K. (2024). Generative AI and Intellectual Property: Ownership, Copyright, and Creative Rights.

[4] Jacques, S., & Flynn, M. (2024). Protecting human creativity in AI-generated music through effective licensing. https://doi.org/10.17638/03172469

[5] Gaffar, H., & Albarashdi, S. (2025). Copyright protection for AI-generated works: Exploring originality and ownership in a digital landscape. Asian Journal of International Law, 15(1), 23-46. https://doi.org/10.1017/S2044251323000735

[6] Fenwick, M., & Jurcys, P. (2023). Originality and the Future of Copyright in an Age of Generative AI. Computer Law & Security Review, 51, 105892. https://doi.org/10.48550/arXiv.2309.13055

[7] Paquette, L. (2021). Artificial life imitating art imitating life: Copyright Ownership in AI-Generated Works. Intellectual Property Journal, 33(2), 183-215.

[8] Aziz, A. (2023). Artificial intelligence produced original work: A new approach to copyright protection and ownership. European Journal of Artificial Intelligence and Machine Learning, 2(2), 9-16. https://doi.org/10.24018/ejai.2023.2.2.15

[9] Smits, J., & Borghuis, T. (2022). Generative AI and intellectual property rights. In Law and artificial intelligence: Regulating AI and applying AI in legal practice (pp. 323-344). The Hague: TMC Asser Press. https://doi.org/10.1007/978-94-6265-523-2_17

[10] Sun, H. (2021). Redesigning copyright protection in the era of artificial intelligence. Iowa L. Rev., 107, 1213.

[11] Wang, J. T., Deng, Z., Chiba-Okabe, H., Barak, B., & Su, W. J. (2024). An economic solution to copyright challenges of generative ai. arXiv preprint arXiv:2404.13964. https://doi.org/10.48550/arXiv.2404.13964

[12] Nordås, H. K. (2024). Copyright and trade in the digital music industry. In Handbook of Innovation and Intellectual Property Rights (pp. 177-190). Edward Elgar Publishing. https://doi.org/10.4337/9781800880627.00019

[13] Alkato, A. A., & Sakhnin, Y. (2025). Advanced real-time anomaly detection and predictive trend modelling in smart systems using deep belief network architectures. PatternIQ Mining, 2(1), 97–107. https://doi.org/10.70023/sahd/250209

[14] Shroff, L. (2024). AI & copyright: A case study of the music industry. GRACE: Global Review of AI Community Ethics, 2(1). https://doi.org/10.60690/7pqxkr18

[15] Bulayenko, O., Quintais, J. P., Gervais, D. J., & Poort, J. (2022). Ai music outputs: Challenges to the copyright legal framework. Available at SSRN 4072806. https://doi.org/10.2139/ssrn.4072806

[16] Adebiyi, O. I., & Adeusi, O. C. (2025). Examining legal and ethical frameworks for protecting intellectual property rights in AI-generated content across creative industries. https://doi.org/10.30574/wjarr.2025.26.3.2239

[17] Vivaldi, W., & Sutedja, I. (2024). Using deep learning and CBIR to address copyright concerns of AI-generated art: A systematic literature review. Devotion: Journal of Research and Community Service, 5(10), 1320-1330. https://doi.org/10.59188/devotion.v5i10.18642

[18] Jacques, S., & Flynn, M. (2024). Protecting human creativity in AI-generated music with the introduction of an AI-royalty fund. GRUR International, 73(12), 1137-1149. https://doi.org/10.1093/grurint/ikae134

[19] Drott, E. (2021). Copyright, Compensation, and Commons in the Music AI Industry. Creative Industries Journal, 14(2), 190-207. https://doi.org/10.1080/17510694.2020.1839702

[20] Ren, J., Xu, H., He, P., Cui, Y., Zeng, S., Zhang, J., ... & Tang, J. (2024). Copyright protection in generative AI: A technical perspective. arXiv preprint arXiv:2402.02333. https://doi.org/10.48550/arXiv.2402.02333

[21] Dzuong, J., Wang, Z., & Zhang, W. (2024). Uncertain boundaries: Multidisciplinary approaches to copyright issues in generative ai. arXiv preprint arXiv:2404.08221. https://doi.org/10.48550/arXiv.2404.08221

[22] Bukhari, S. W. R., Hassan, S. U., & Aleem, Y. (2023). Impact of artificial intelligence on copyright law: Challenges and prospects. Journal of the Law Society of Scotland, 5(4), 647-656. https://doi.org/10.52279/jlss.05.04.647656

[23] Pujari, V., & Wilson, B. (2023). Copyright and authorship in AI-Generated music. Journal of Emerging Technologies and Innovative Research, 10(12), 351-354.

[24] Deng, J., Zhang, S., & Ma, J. (2023). Computational copyright: Towards a royalty model for music generative ai. arXiv preprint arXiv:2312.06646. https://doi.org/10.48550/arXiv.2312.06646

[25] Deng, J., & Ma, J. (2023). Computational copyright: Towards a royalty model for ai music generation platforms. In ICLR 2024 Workshop on Navigating and Addressing Data Problems for Foundation Models.

[26] https://www.kaggle.com/datasets/birdy654/deep-voice-deepfake-voice-recognition/data