ingegneria sismica
International Journal of Earthquake Engineering
Anno XLIII - Num. 1 - 2026

Algorithm Design and Implementation of Blockchain in Folk Music Copyright Protection

Lili Tian[1,*]

[1] Art College, Zhaotong University, Zhaotong 657000, Yunnan Province, China

SUMMARY: *In order to solve the problems of decentralized copyright registration, hidden content tampering and difficulty in source tracking in the process of digital transmission of folk music, a blockchain-supported algorithm framework for copyright protection of folk music was proposed. This method coupled robust audio watermarking, convolutional autoencoder and alliance chain certificate storage mechanism, and constructed a technical link covering copyright registration, forgery detection, real-time traceability and online verification. In the implementation, the system completed the identity binding of the work through time-frequency feature extraction and latent space watermark embedding, and then used the reconstruction error of the convolutional autoencoder to identify the forgery behaviors such as segment splicing, pitch sandaling, speed variation and deep imitation singing. The on-chain hash index and smart contract were combined to realize ownership verification and evidence retention. Experimental results show that on 4800 folk music audio samples, the accuracy of copyright confirmation of the proposed method reaches 95.8%, the average detection rate of forged samples reaches 94.0%, the success rate of watermark extraction remains above 93.6%, the accuracy of source attribution reaches 91.1%, and the average delay under 100 concurrent verification requests is 138 ms. The research shows that the collaborative design of blockchain and deep learning can effectively improve the credibility, real-time performance and enforceability of folk music copyright protection, and provide a feasible computer technology path for the standardized circulation and long-term protection of folk music digital resources.*

KEYWORDS: *Blockchain; Folk music; Copyright protection; Convolutional autoencoders*

1 Introduction

The continuous expansion of the digital communication environment is reshaping the production, circulation and reuse of folk music. Relying on short video platforms, streaming media platforms and intelligent audio editing tools, the original folk music with distinct regional characteristics, oral transmission and performance scene dependence has been rapidly transformed into digital content that can be copied, spliced and reprocessed. Although the improvement of communication efficiency has expanded the social visibility of folk music, it also makes copyright ownership, communication authorization and infringement forensics more complex. A segment of national music audio that has been edited, remixed or rearranged is often repeatedly reprinted between multiple platforms, and the rights and responsibilities boundaries between its creators, collectors, orchestrators and communicators are constantly diluted. For many folk music resources still in the early stage of digital arrangement, this imbalance state of "dissemination first, right confirmation lag" has become a prominent

*13885502050@163.com
https://doi.org/10.65102/is2026083
Published: 30 April, 2026

problem in copyright protection.

From the existing practice, digital rights management mostly still relies on centralized databases, platform filing or manual registration mechanisms. Such methods have certain operability in general works management, but in the face of national music copyright scenes, they often expose defects such as link fragmentation, evidence dispersion, difficult to detect tampering and inefficient traceability. On the one hand, the source of folk music material is complex, including the original singing recording, digital restoration version, teaching adaptation version and performance re-creation version. There are strong associations between different versions but lack of unified identification. On the other hand, the traditional right confirmation process pays more attention to the registration results, and lacks the real-time response ability to content tampering, fragment theft and forged signature in the dissemination process. Especially in the context of the rapid development of deep learning audio generation technology, the threshold for forging timbres, imitating melodies and synthesizing performance fragments has been significantly reduced. It is difficult to meet the actual needs of authenticity identification and infringement determination by simply relying on manual comparison or static file storage.

Blockchain technology provides a new solution to this problem. Its distributed ledger, tamper-resistant record and smart contract automatic execution mechanism can build a trusted foundation for folk music copyright registration, authorization records and transaction traces. However, only on-chain storage is still not enough to solve the key issues such as "whether the content is authentic", "whether the version has been rewritten" and "whether the transmission fragment originates from the original work". In other words, copyright protection requires not only trusted records, but also computable content verification capabilities. Based on this, this paper combines blockchain with audio watermarking and deep learning forgery detection method, and tries to construct an algorithm framework for folk music copyright protection. In the copyright registration stage, the unique binding of work identity is realized by embedding robust audio watermarking and synchronizing the hash and ownership metadata on the chain. In the content recognition stage, the convolutional autoencoder is used to extract the time-frequency structure features, and the difference between editing, compression, resampling and imitation generated audio is distinguished. In the phase of circulation verification, with the help of on-chain index, smart contract and real-time comparison module, the source tracking of works, ownership verification and propagation evidence writeback are completed, forming a closed-loop mechanism of "registration - detection - traceability - verification".

The core problem of this paper is not only to simply superpose the blockchain as a storage tool into the music copyright management process, but also to try to answer several questions with more computer implementation significance: for the audio objects with diverse structures and significant differences in singing styles such as folk music, how to design a blockchain integrated watermarking mechanism with concealment, robustness and identifiability. In the face of forged clips, secondary splicing and deep generated audio, how to establish an effective feature reconstruction and anomaly recognition model? In the platform-based transmission scenario, how to realize low-latency and scalable real-time right confirmation and verification. Focusing on these problems, this paper studies from two aspects of algorithm design and system implementation, and tries to improve the automatic judgment ability of the authenticity and source consistency of folk music audio while ensuring the credible registration of copyright information. In the following, this paper will discuss the related research basis, blockchain algorithm design method, experimental results and performance analysis in turn, and further explain the application value and realistic boundary of this method in the digital protection of folk music.

2 Related work

In recent years, the research of digital music copyright protection has obviously presented a trend of technology integration, and the research focus has gradually shifted from a single file storage to the integrated processing of "right confirmation, identification, trace-verification". In terms of existing achievements, blockchain, digital watermarking, audio fingerprinting and deep learning recognition are four relatively active technical paths, but their adaptation degrees in folk music copyright protection are not the same, and the advantages and limitations of the methods are also relatively clear.

The research of blockchain mainly focuses on trusted registration, authorization execution and transaction trace. Bodo et al. [1] and Ma et al. [2] pointed out earlier that distributed ledger can improve the problems of traditional digital rights management, such as too strong central node, easily split records, and incomplete right confirmation chain. Liu et al. [3] and Heo et al. [4] further introduced the consortium blockchain structure into the digital content management scenario, emphasizing the importance of on-chain identity authentication, hash mapping and rights control for copyright registration. The contribution of such research is to provide an immutable timestamp and ownership record for digital works, so that copyright ownership no longer completely depends on platform credit or manual recording. However, the simple on-chain storage certificate cannot directly answer the question "whether the current circulating audio is still the original work". For folk music, it is difficult to cover content-level tampering identification by only relying on hash registration because of the differences in singing versions, frequent instrumental adaptations, and widespread segment transmission.

The research of digital watermarking is closer to content protection. Katzenbeisser et al. [5], Bianchi et al. [6] and Hua et al. [7] systematically discussed the robustness, invisibility and detectability of watermark embedding from the perspective of multimedia security. Wu et al. [8] verified the feasibility of robust watermarking in the early audio copyright protection scene. In recent years, Zhao et al. [9] and Frattolillo[10] have tried to combine watermark management with smart contracts, so that the watermark is no longer just a hidden mark attached to the internal audio, but a computational object that can be synchronously associated with the ownership metadata on the chain. These methods have direct value for copyright claim, infringement forensics and content traceback, but their shortcomings are also obvious. When audio undergoes compression, cropping, variable speed, reverberation or partial re-recording, the performance of traditional watermark detection is often degraded. In the face of forged samples with high similarity, only relying on watermark extraction may still lead to misjudgment.

Developed in parallel with the watermarking mechanism are audio fingerprinting and deep learning authentication techniques. Serrano et al. [11, 12] constructed a higher- granularity audio fingerprint description method around song recognition, which provided an effective tool for segment matching and source search. Costa et al. [13] and Nasridinov et al. [14] show that convolutional neural networks based on spectrograms can better capture the time-frequency structural features of music and have strong performance in classification and recognition tasks. Related research shows that deep models are not limited to music style classification, but also applicable to copyright forgery detection, source attribution and abnormal sample discrimination. However, the existing models mostly serve the general music data sets, and less consider the characteristics of folk music such as drab, glide, free rhythm and complex grace note. This makes some effective discriminative models on popular music may have the problem of insufficient feature expression after being transferred to the folk music scene.

The research of folk music itself focuses more on classification recognition, style analysis

and educational application. Wang[15] discussed the problem of folk music recognition based on feature extraction algorithm, and Xu[16] applied deep learning to the construction of an intelligent recognition and learning platform for folk music types. These works lay the foundation for the digital processing of folk music, and also show that its audio structure can be effectively represented by computational models. However, the main goal of such research is still "identify what" rather than "prove who" or "determine whether it has been tampered with". When folk music comes into the context of copyright protection, the focus of the problem has expanded from general classification to ownership binding, version association, infringement tracking and real-time verification, and the technical requirements are obviously higher.

To more clearly compare the differences between the existing research paths and the work in this paper, the related results can be summarized as Table 1. It can be seen from the table that most of the existing methods perform well in a certain link, but the cross-link collaboration ability is insufficient. However, the copyright protection of folk music requires a stable connection between registration mechanism, content identification and traceability verification.

Table 1: Related research paths and their implications for this paper

Research Direction	Representative Technologies/Studies	Main Function	Existing Limitations	Implications for This Study
Blockchain-based Copyright Management	Blockchain registration, smart contract authorization [1–4, 17, 19–20, 23–24]	Provides trusted evidence storage and tamper-resistant records	Emphasizes registration but pays less attention to content verification, making audio tampering difficult to detect	On-chain rights confirmation should be integrated with content-level detection
Digital Audio Watermarking	Robust watermarking, smart contract-linked watermarking [5–10, 25]	Enables copyright mark embedding and infringement evidence collection	Limited adaptability to complex editing operations and forged samples	The stability of watermarking under compression and editing scenarios needs to be improved
Audio Fingerprinting	Fine-grained fingerprint matching [20–21]	Supports song fragment retrieval and source tracing	More oriented toward similarity retrieval, with limited capability in copyright ownership representation	It can serve as an important supplement to the traceability module
Deep Learning-based Audio Analysis	CNN, spectrogram feature learning [22, 25]	Improves forgery detection and feature discrimination capability	Usually designed for general music, with insufficient adaptation to ethnic music	A detection model tailored to ethnic music characteristics should be developed
Intelligent Recognition of Ethnic Music	Feature extraction, genre recognition, and platform applications [23–24]	Demonstrates that ethnic music can be effectively represented by computational models	Focuses mainly on classification and teaching, with limited attention to copyright protection	Recognition results should be extended to copyright verification scenarios

In general, the existing research has answered the questions of "how to credibly register", "how to embed copyright tags", "how to perform audio matching" and "how to carry out deep recognition" respectively, but the response to the complex scene of folk music copyright protection is still insufficient. What is really missing is not a single point of technology, but a

collaborative scheme for the transmission chain of folk music: it can not only complete the binding on the chain when the copyright is registered, but also detect the forgery and identify the rewrite in the process of audio circulation, and write the verification results back to the trusted ledger in real time. It is in this sense that this paper incorporates the blockchain integrated audio watermarking, convolutional autoencoder forgery detection and real-time traceability verification framework into the unified design, hoping to establish a more stable technical connection between content authenticity, copyright confirmation efficiency and cross-platform tracking ability.

3 Blockchain algorithm design method for folk music copyright protection

Aiming at the problems that folk music is easy to be edited and rewritten, replaced by signature and transferred across platforms in the process of digital transmission, this paper constructs a set of blockchain algorithm design methods for copyright registration, forgery identification and source verification. Instead of using blockchain as a storage tool alone, this method combines audio watermarking, deep feature extraction and on-chain verification mechanism to form a technical framework for simultaneous operation of content protection and ownership management. When a folk music work is uploaded, the original audio is preprocessed and feature encoded, and the copyright data including work identity, author information and timestamp is embedded into the robust audio watermark. Then the key metadata is written into the consortium blockchain ledger through hash mapping to complete the copyright registration that cannot be tampered with. For the audio samples in the subsequent propagation, the system uses the convolutional autoencoder to extract the time-spectrum structure features, detects the abnormal situations such as compression, cropping, resampling and forgery generation, and combines the on-chain index to complete the source comparison and ownership verification. In this way, the copyright protection of folk music no longer stays at the static registration level, but can realize real-time identification, fast traceability and result retention in the process of circulation of works. Based on this overall design, this paper further elaborates on four aspects of blockchain integrated audio watermarking mechanism, copyright forgery detection model, real-time traceability verification framework and evaluation indicators.

3.1 Blockchain integrated audio watermarking mechanism for copyright registration

Aiming at the copyright registration of folk music, this paper designs a blockchain-based integrated audio watermarking mechanism. The goal is not limited to completing one-time registration, but to establish a stable binding relationship between the content characteristics and author identity information of the work and the ownership records on the chain, so that the copyright registration results can continue to play a role in the subsequent transmission, comparison and forensics process. Considering that folk music has strong differences in melody decoration, rhythm expansion, singing timbre and accompaniment morphology, if only file hash is used as the copyright identifier, the audio may lose comparability after compression, editing or resampling. To this end, the robust watermark is embedded into the deep audio feature space, and the creator's identity, registration time, work abstract and model signature are written into the consortium chain, forming a dual registration structure of "content implicit marking + explicit storage on the chain".

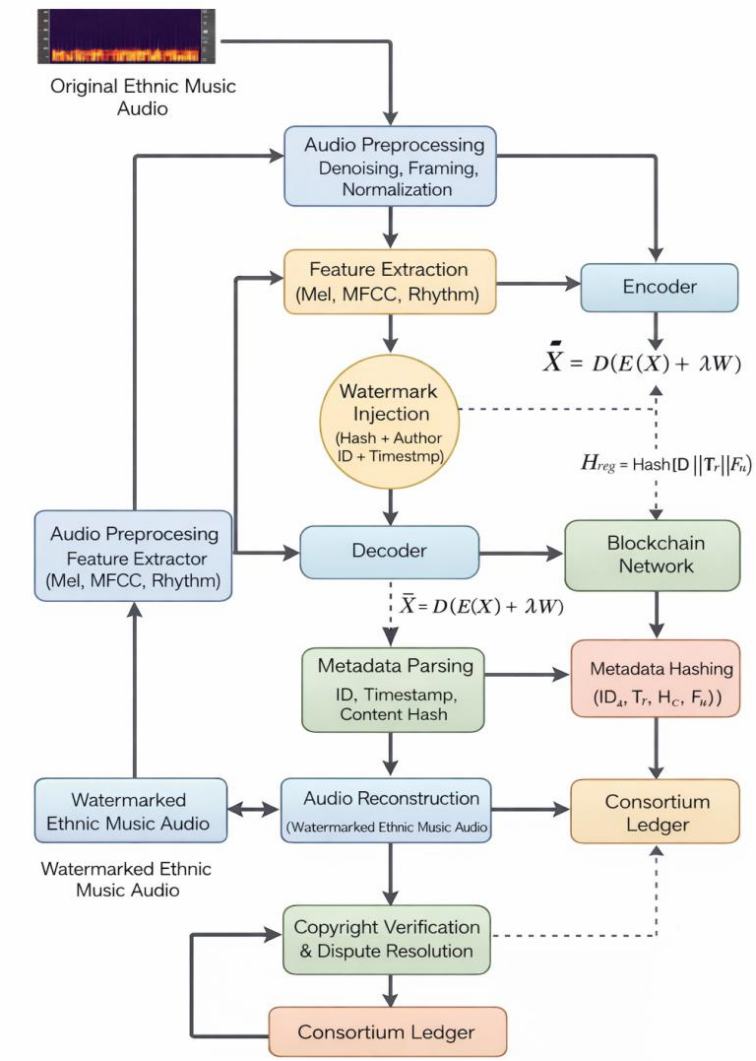

Figure 1: Blockchain integrated audio watermarking mechanism for copyright registration

As shown in Figure 1, after uploading the folk music work, the system firstly preprocesses and extracts features, and converts the original waveform into multi-dimensional representations such as MEL spectrum, MFCC parameters and rhythm contour, which are used to describe the singing changes, timbrel details and melody trend. Then, the encoder compressed the time-frequency features, injected the watermark vector composed of the work hash, the author ID and the timestamp into the latent space, and reconstructed the watermarked audio by the decoder. The process tries to keep the listening sense unchanged, so that the watermark is imperceptible to ordinary listeners, but can be stably extracted by the authorized system. After embedding, the system parsed the copyright metadata into structured fields, generated an on-chain registration digest through hash operation, and triggered the smart contract to write it into the blockchain ledger, so as to obtain an immutable registration certificate. After this process, the folk music works not only retain content-level identity tags, but also have on-chain registration records that can be publicly verified. The watermark embedding process can be expressed as follows.

$$\hat{X} = D(E(X) + \lambda W) \tag{1}$$

where, X represents the time-frequency feature matrix of the input folk music audio, E(·) is the

encoder mapping function, D(·) is the decoder reconstruction function, W is the watermark vector formed by concatenating the hash of the work, the author identity and the registration time, λ is the embedding strength coefficient, and $\widehat{X}$ is the generated watermarked audio feature. The meaning of Equation (1) is that the copyright information is written into the potential representation rather than directly attached to the prominent position of the waveform, so as to achieve a relatively balanced result between concealment and robustness. The on-chain memorial can be further defined as follows.

$$H_{reg} = \mathrm{Hash}(ID_a \parallel T_r \parallel H_c \parallel F_w) \tag{2}$$

Among them, H_{reg} is the copyright registration abstract, ID_a represents the author identity identifier, T_r represents the registration timestamp, H_c represents the content Hash of the work, F_w represents the watermark feature summary, $\parallel$ is the field splicing operation, and Hash(·) is the secure hash function. After the abstract is written into the blockchain by the smart contract, it can be used as a unified index for copyright registration and subsequent verification.

The value of this mechanism is that it changes the traditional practice of "separating registration information from audio content". For folk music, there are often cases such as different singing of the same song, fragment dissemination, performance adaptation and cross-platform reprint. A single database filing can only prove the existence of a certain declaration, but it is difficult to prove the real association between circulation samples and registered works. Through the linkage of watermark vector and the abstract on the chain, the proposed method makes the copyright registration transform from static filing to dynamic binding process that can be calculated, tracked and reviewed. Once the infringement dispute occurs, the system can not only extract the watermark information from the suspicious audio, but also retrieve the corresponding registration records on the chain, so as to improve the credibility and enforceability of the folk music copyright registration.

3.2 Copyright Forgery Detection Model based on Convolutional Autoencoder

In the copyright protection scenario of folk music, the forgery behavior is not always represented by substantial tampering. Most of the time, the original audio segments are spliced, rhythm fine-tuning, pitch shift, reverberation coverage, and even the simulation of specific singing voice and timbre with the help of generative models. Such changes often do not completely destroy the overall sound sense, but they are enough to change the source judgment of the work and bring significant interference to the copyright verification. Based on this reality, in addition to the blockchain registration and watermarking mechanism, this paper introduces a convolutional autoencoder to construct a copyright forgery detection model, so that the system can identify fine-grained anomalies from the audio time-frequency structure, and then determine whether the circulation sample deviates from the real feature distribution of registered folk music works.

The model takes the original folk music samples that pass the right confirmation on the chain as the training subject, and learns the stable representation of normal works in spectrum texture, formant direction, rhythm fluctuation and local energy distribution through the convolutional encoder. Considering the common complex phenomena in folk music such as togue, glissia, appoggionic and free beats, this paper does not directly take the original waveform as the only input, but jointly codes the logarithmic Mel spectrum, MFCC parameters and their first-order difference to enhance the model's ability to perceive melody decoration and timbre details. The autoencoder only contacts the real registered samples in the training phase,

so it can form a low-dimensional representation of the "normal folk music feature space". If the internal structure of the audio to be detected is consistent with the real sample, the model reconstruction error is usually low. On the contrary, if the audio is forged, spliced or illegally re-recorded, there will be deviations in the local continuity of spectrum, energy transfer relationship and potential feature distribution, which will cause the reconstruction error and potential deviation to rise synchronously.

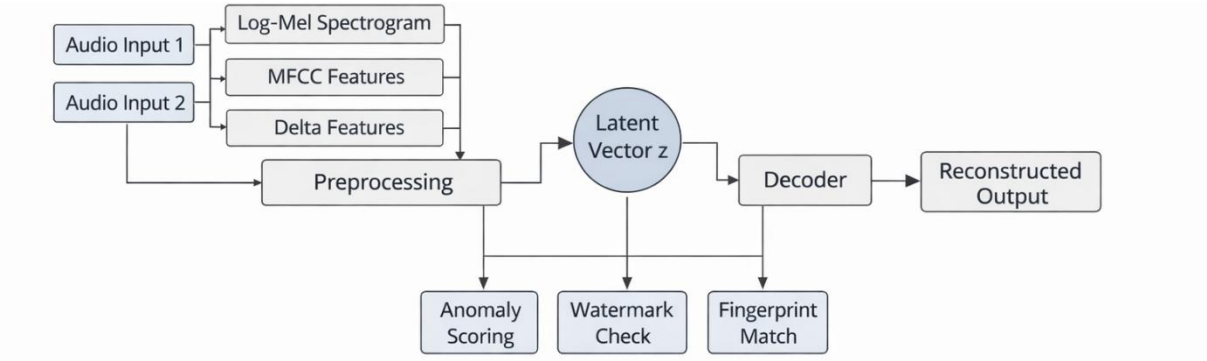

Figure 2: Framework for copyright forgery detection of folk music based on convolutional autoencoder

As shown in Figure 2, the running process of the model is composed of "preprocessing - feature extraction - coding compression - reconstruction and recovery - anomaly scoring - on-chain writeback". The preprocessing module is responsible for noise reduction, framing, normalization and silent segment elimination to reduce the interference caused by the difference of acquisition equipment. The feature extraction module converted the audio into a two-dimensional time-frequency matrix suitable for convolutional network processing. The encoder extracts the local harmonic texture and time dependence information layer by layer to form the latent vector z. The decoder then reconstructs the input features according to the latent representation, and the system calculates the anomaly degree of the audio by comparing the difference between the input and output. If the abnormal score exceeds the threshold, the sample is marked as suspected forgery and further linked with the copyright record on the chain to trigger the subsequent traceability and manual review process.

In order to improve the stability of detection, reconstruction error, spectral gradient error and latent space similarity are incorporated into the loss function. The refactoring goal is defined as follows.

$$L_{rec} = \frac{1}{N}\sum_{i=1}^{N} \| X_i - \hat{X}_i \|_2^2 + \alpha \frac{1}{N}\sum_{i=1}^{N} \| \nabla X_i - \nabla \hat{X}_i \|_2^2 + \beta(1 - \cos(z_i, \hat{z}_i)) \quad (3)$$

where, X_i represents the joint time-frequency feature of the ith input audio clip, $\hat{X}_i$ is the model reconstruction result, ∇ represents the spectrogram gradient operator, z_i and $\hat{z}_i$ represent the coding vectors of the input feature and the reconstructed feature in the latent space, N is the number of sample segments, α and β are the weight coefficients. The meaning of this formula is that it not only compares the overall difference before and after reconstruction, but also pays attention to the change of spectrum edge and the consistency of potential representation, so as to avoid the model being only sensitive to the surface energy distribution and ignoring the more recognizable detail structure in folk music. In the detection phase, the authenticity score function is further defined as follows.

$$P_{auth} = \sigma\left(-\gamma L_{rec} - \eta A_{wm} + \mu C_{fp}\right) \quad (4)$$

where P_{auth} is the authenticity confidence of the audio to be detected, $\sigma(\cdot)$ is the Sigmoid function, A_{wm} represents the watermark extraction error, C_{fp} represents the matching coefficient between the sample to be detected and the registered fingerprint on the chain, γ, η, μ are the adjustment parameters. The design combines the depth reconstruction results with the watermark consistency and fingerprint matching information, so that the forgery determination no longer depends on a single index. If the sample is illegally edited but part of the original watermark remains, the model can still identify the risk through reconstruction anomaly and fingerprint offset. If the sample is the imitation result of the generative model, although it may imitate the melody contour, it is usually difficult to meet the three constraints of spectrum reconstruction, watermark extraction and on-chain fingerprint matching at the same time, so the overall authenticity score will be significantly reduced. In order to facilitate the system implementation, this paper writes the detection process into an executable pseudo-code structure, and the code is shown below.

Algorithm 1 ForgeryDetectionByCNN_AE

```
Input:
    audio_suspect
    AE_model
    watermark_decoder
    blockchain_fingerprint_db
    tau
Output:
    label, P_auth

features = extract_features(audio_suspect)      # log-Mel, MFCC, delta
recon_features = AE_model(features)
loss_rec = mse(features, recon_features) \
            + alpha * gradient_mse(features, recon_features) \
            + beta * latent_distance(features, recon_features)

wm_error = watermark_decoder(audio_suspect)
fp_score = match_fingerprint(audio_suspect, blockchain_fingerprint_db)

P_auth = sigmoid(-gamma * loss_rec - eta * wm_error + mu * fp_score)

if P_auth >= tau:
    label = "Genuine"
else:
    label = "Forged or Suspected"
write_result_to_chain(audio_suspect, P_auth, label)
return label, P_auth
```

The implementation logic corresponding to the code is relatively straightforward: the system first extracts the multi-dimensional features of the audio to be tested, and then uses the trained convolutional autoencoder to reconstruct it. Then, the comprehensive reconstruction loss is calculated, and the authenticity confidence is output by linking the watermark decoding error and the on-chain fingerprint matching score. Once the detection result is generated, it is written back to the on-chain recording module to form a continuous and traceable copyright

verification log. The benefit of this design is that the model output no longer stays at the offline recognition level, but can be truly embedded in the copyright protection business process.

3.3 Implementation framework of real-time traceability and verification for copyright confirmation

In the digital transmission chain of folk music, copyright registration is not equal to copyright implementation. Once a work enters the links of platform uploading, segment reprinting, secondary editing and cross-terminal playback, what really affects the efficiency of right confirmation is often not whether there is registration on the chain, but whether the system can quickly determine the source of the audio, verify the consistency of ownership, and make a traceable response to abnormal samples at the moment of circulation. Based on this requirement, this paper constructs a real-time traceability and verification implementation framework for copyright confirmation, which integrates embedded watermark extraction, audio fingerprint matching, metadata verification on the chain and platform interface call into a unified process, so that the folk music has the computing ability of instant verification, dynamic tracking and automatic retention in the transmission process.

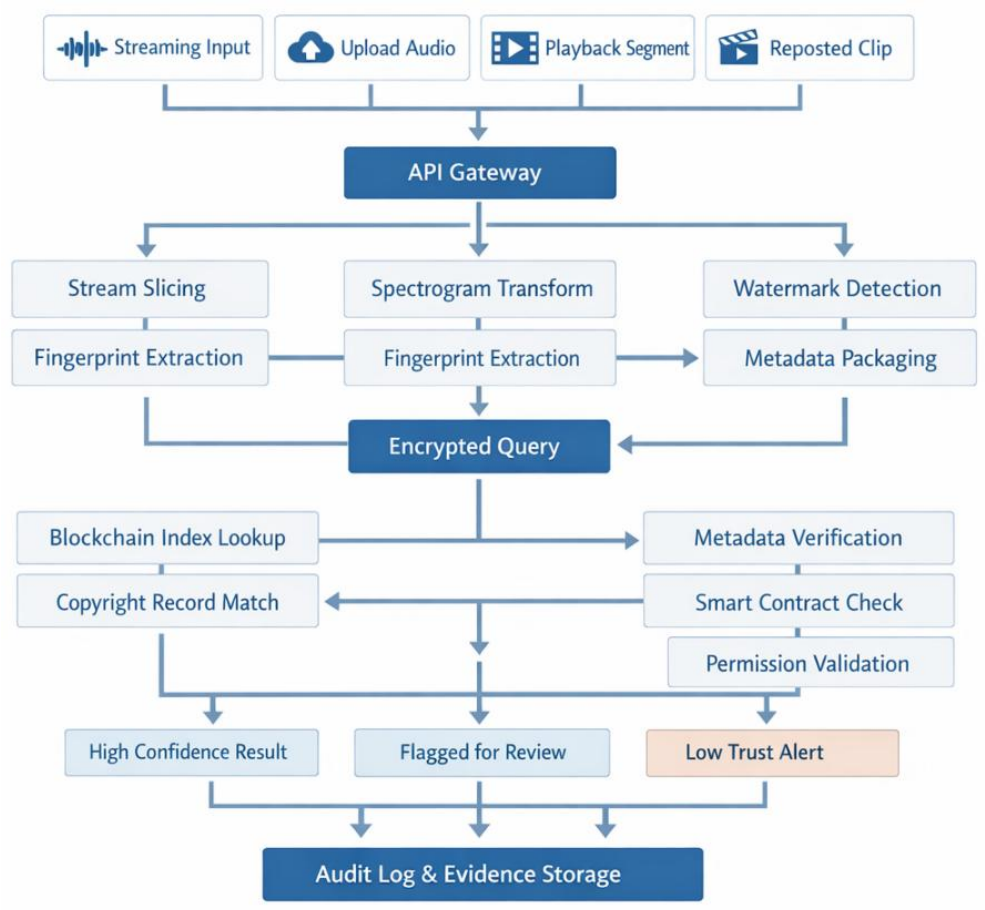

Figure 3: Implementation framework of real-time traceability and verification for copyright confirmation

As shown in Figure 3, the framework is composed of stream access layer, feature parsing layer, trusted comparison layer and result writeback layer. After receiving the uploaded audio or playing clip, the platform calls the real-time analysis interface to complete the audio slicing, spectrum transformation and fingerprint extraction, and synchronously detects the existence

and completeness of the implicit watermark. Then, according to the extracted fingerprint abstract, author identification fragment and time information, the system retrieved the corresponding copyright records in the alliance link citation table. If the retrieval is successful, it will further verify whether the registration metadata, smart contract status and the current propagation permission are consistent on the chain. If the retrieval fails, or there is a significant deviation in the comparison results, the audio will be marked as a low confidence sample, triggering abnormal warning and evidence retention. In this way, the copyright confirmation of folk music no longer relies on artificial proof afterwards, but can complete the source judgment and responsibility positioning at the moment of content circulation.

In order to ensure the security of on-chain records in the calling process, this paper encapsulates the metadata to be verified and then performs encryption mapping. The expression is:

$$M_{enc} = Enc_k\left(ID_u \parallel F_q \parallel T_q \parallel W_q \parallel P_s\right) \tag{5}$$

where, M_{enc} represents the encrypted meta data packet to be linked or verified, Enck(·) represents the symmetric encryption function based on key k, ID_u is the identity of the right holder, F_q is the real-time extracted audio fingerprint summary, T_q is the current verification timestamp, W_q is the watermark extraction vector, P_s is the propagation permission state, $\parallel$ represents the field splicing operation. The function of Equation (5) is to encapsulate the key fields required for real-time verification, avoid directly exposing copyright sensitive information under plaintext conditions on the platform side, and provide standard input for on-chain retrieval and contract invocation.

On this basis, this paper defines a real-time right confirmation credibility scoring function to comprehensively reflect the degree of consistency between sample sources and registration records:

$$R_{tv} = \lambda_1 \, Sim(F_q, F_r) + \lambda_2 V_w + \lambda_3 C_a - \lambda_4 \frac{\Delta t}{\Theta} \tag{6}$$

where R_{tv} is the credibility of real-time traceability verification, $Sim(F_q, F_r)$ is the similarity between real-time fingerprint F_q and the registered fingerprint F_r on the chain, V_w is the watermark verification pass degree, C_a is the authorization consistency result returned by the smart contract, Δt is the difference between the current verification time and the latest on-chain synchronization time, Θ is the time normalization constant. The $\lambda_1 - \lambda_4$ are the weight parameters, and $\sum \lambda_i = 1$ is satisfied. The formula shows that the right confirmation result is not only determined by a single matching value, but by the content similarity, the integrity of copyright mark, the authorization status and the synchronization prescription. For the content with complex communication forms such as folk music, this multi-factor fusion method is more suitable for the actual situation of the coexistence of fragmented circulation and version variants.

At the engineering implementation level, the platform interface can directly map the R_{tv} calculated by formula (6) into three types of output states. When the score is higher than the threshold, the system determines that the sample is registered and authorized. When the score is in the middle range, the sample is marked as low-confidence content that needs to be further checked. When the score is significantly low, the system identifies it as potential infringement or unknown source audio, and writes the fingerprint, watermark residual, and call time into the on-chain audit module together with the user side request record. In this way, real-time verification not only completes the current right confirmation task, but also saves a continuous evidence chain for subsequent dispute processing.

3.4 Evaluation Metrics

In order to objectively test the applicability of the blockchain copyright protection method constructed in this paper in the ethnic music scene, the evaluation system should not only stay on a single recognition accuracy, but also cover multiple dimensions such as copyright confirmation, forgery detection, watermark stability, real-time response efficiency and on-chain record credibility. Folk music audio has the characteristics of rich melody decoration, large rhythm flexibility, and obvious differences in singing versions. If the evaluation index design is too dependent on the single accuracy in the general classification task, it is difficult to reflect the actual performance of the system in the real copyright protection environment. Based on this, this paper constructs a set of comprehensive evaluation indicators for copyright protection process, which are used to describe the operation quality of the model in the whole process of "registration, detection, traceability, verification". Copyright right confirmation accuracy is used to measure the system's ability to identify the ownership of legal works, which is defined as:

$$A_{own} = \frac{N_{tp}}{N_{tp} + N_{fp} + N_{fn} + \varepsilon} \tag{7}$$

where, A_{own} represents the accuracy of copyright confirmation, N_{tp} is the number of samples whose ownership is correctly confirmed, N_{fp} is the number of samples whose ownership is incorrectly attributed, N_{fn} is the number of legal samples that have not been identified, and ε is the smoothing term that prevents the denominator from being zero. This index reflects whether the system can stably complete the accurate binding between the work and the right holder after the folk music copyright registration. The copyright forgery detection rate is used to measure the ability of the model to identify illegal clips, synthetic counterfeits and tampered samples, which can be expressed as:

$$R_{for} = \frac{1}{N}\sum_{i=1}^{N} \mathbb{I}\left(E_i \geq \delta\right) \tag{8}$$

Here, R_{for} is the forgery detection rate, N is the total number of test samples, E_i represents the comprehensive anomaly score of the ith sample, δ is the forgery determination threshold, and I(·) is the indicative function. This formula essentially counts the proportion of samples whose abnormal scores exceed the threshold to evaluate the sensitivity of the convolutional autoencoder to forged audio.

The robustness of watermark is an important factor in copyright protection. Folk music often undergoes compression coding, bit-rate adjustment, segment interception and noise pollution in the transmission process. Therefore, this paper uses the normalized bit consistency rate to measure the stability of watermark extraction:

$$S_{wm} = 1 - \frac{1}{KL}\sum_{k=1}^{K}\sum_{j=1}^{L}\left|w_{k,j} - \hat{w}_{k,j}\right| \tag{9}$$

where, S_{wm} represents the watermark robustness score, K is the test round, L is the watermark bit length, $w_{k,j}$ is the JTH bit of the KTH round of the original watermark, and $\hat{w}_{k,j}$ is the corresponding extraction result. The closer this index is to 1, the better the system can recover the copyright logo after experiencing multiple propagation perturbations.

Real-time verification performance directly affects the effect of platform application. If the verification process is too slow, even if the model accuracy is high, it is difficult to support large-scale upload and online distribution scenarios. Therefore, in this paper, the total system delay is defined as:

$$T_{ver} = T_{ext} + T_{mat} + T_{qry} + T_{api} \tag{10}$$

where, T_{ver} is the total time consumption of a complete copyright verification, T_{ext} is the audio feature and watermark extraction time, T_{mat} is the similarity matching time, T_{qry} is the blockchain ledger query time, and T_{api} is the platform interface return time. The smaller the index is, the more suitable the system is to be deployed in the real-time copyright auditing and online playing environment.

Considering that blockchain assumes the supporting role of trusted registration and audit in this paper, it is not sufficient to only report the identification accuracy, and it is also necessary to measure the integrity and reliability of transactions on the chain. In this regard, this paper defines the integrity score of on-chain records as:

$$I_{bc} = \frac{1}{M}\sum_{m=1}^{M}(\alpha s_m + \beta c_m - \gamma d_m) \tag{11}$$

where, I_{bc} represents the integrity score of blockchain records, M is the total number of on-chain transactions evaluated, s_m is the signature validity of the MTH transaction, cm is the smart contract execution consistency, d_m is the time delay penalty term of the transaction, α, β, γ are weight parameters. This index comprehensively reflects whether copyright registration, state synchronization and contract call are stable and credible.

Source attribution accuracy is used to evaluate the system's ability to identify true sources in multi-version folk music samples and can be expressed as:

$$P_{src} = \frac{N_{cm}}{N_{cm} + N_{wm} + \eta} \tag{12}$$

Here, P_{src} is the source attribution accuracy, N_{cm} is the number of samples from correctly matched sources, N_{wm} is the number of samples from incorrectly matched sources, and η is the smoothness constant. Compared with the general classification accuracy, this index emphasizes "attribution correctness", which is especially suitable for the copyright scenes of folk music in which the same song is sung differently, the same source is adapted and the fragments are spliced frequently. This paper further constructs the comprehensive performance index as follows.

$$C_{all} = \omega_1 A_{own} + \omega_2 R_{for} + \omega_3 S_{wm} + \omega_4 P_{src} + \omega_5 I_{bc} - \omega_6 \widetilde{T}_{ver} \tag{13}$$

where, C_{all} is the comprehensive performance index, ω_i is the normalized weight coefficient, and $\widetilde{T}_{ver}$ is the normalized verification delay. This formula integrates the right confirmation ability, forgery detection ability, watermark stability, source attribution ability, on-chain credibility and response efficiency into an evaluation framework, which facilitates the horizontal comparison between different models, different parameter combinations and different experimental Settings.

4 Experimental results and analysis

In order to test the effectiveness of the proposed method in the folk music copyright protection scenario, the experiment is carried out around six indicators: copyright confirmation accuracy, forgery detection rate, watermark robustness, real-time verification delay, on-chain record integrity and source attribution accuracy, and compared with three common schemes: The traditional centralized rights management method (C-DRM), the method only using blockchain to store certificates (BC-Only), and the method combining blockchain with conventional audio fingerprinting (BC-FP). Different from general music data, ethnic music is more complex in melody decoration, rhythm freedom, singing timbre and accompaniment structure. Therefore, the construction of experimental data sets also emphasizes multi-source and variant coverage.

The dataset consists of recorded folk song clips, public folk instrumental music samples, and artificially generated copyright perturbation samples, covering four types of audio: folk song singing, instrumental solo, ensemble clips, and teaching-curated versions. On this basis, 1200 legal transmission samples are constructed, which are processed by compression, cropping, variable speed, pitch sandaling and noise pollution, and 1200 forged or counterfeit samples are generated, totaling 4800 audio recordings. A 7:2:1 training, validation and test ratio was used for data partitioning, in which the convolutional autoencoder was mainly trained on real registered samples and mildly perturbed samples, and the forged samples were used for evaluating the anomaly recognition ability in the testing phase. The experimental platform uses Python and PyTorch to realize model training, the consortium blockchain environment uses Hyperledger Fabric, and the on-chain index module communicates with the platform interface through REST API. See Table II for the relevant Settings.

Table 2: Experimental data sets and test Settings

Item	Content
Total Data Volume	4,800 ethnic music audio samples
Original Registered Samples	2,400
Legitimate Dissemination Variants	1,200
Forged/Imitated Samples	1,200
Audio Types	Folk song singing, ethnic instrumental music, ensemble excerpts, and curated teaching versions
Perturbation Types	Compression, cropping, resampling, time-stretching, pitch-shifting, and noise contamination
Training Framework	Python + PyTorch
Blockchain Environment	Hyperledger Fabric
Comparison Methods	C-DRM, BC-Only, BC-FP, Proposed Method

From the perspective of the accuracy of copyright confirmation, the proposed method maintains high stability under different registration scales. As shown in Figure 4, when the number of works registered on the chain increases from 200 to 1000, the accuracy of the right confirmation of the proposed method decreases from 97.2% to 95.8%, with a small fluctuation. In contrast, C-DRM decreases from 84.6% to 79.5%, BC-Only decreases from 88.3% to 84.1%, and BC-FP decreases from 92.1% to 89.4%. This shows that relying only on on-chain registration can improve the credibility of records, but it is not enough to deal with the ownership discrimination of a large number of similar audio samples. In this paper, through the joint verification of watermarking, deep features and metadata on the chain, the copyright verification does not stop at the text-level comparison, but enters the content-level verification

level, so it still maintains strong discrimination when the sample size is expanded.

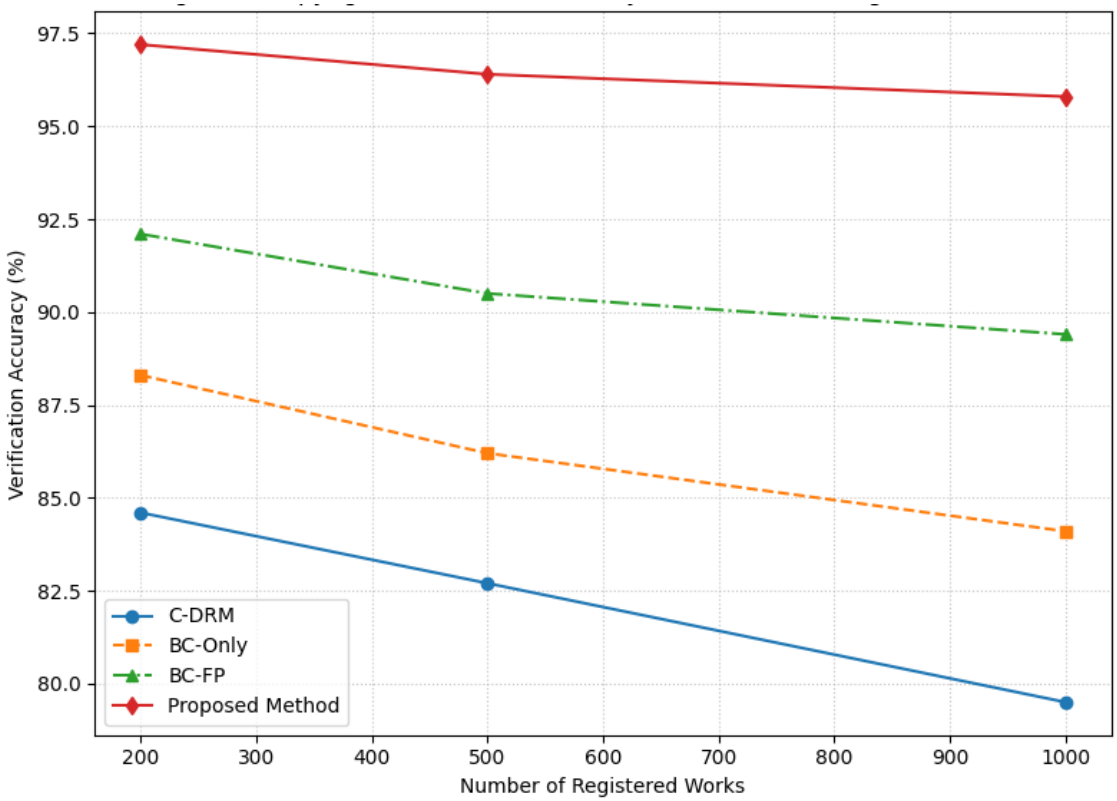

Figure 4: Accuracy of copyright confirmation /% under different registration scales

As shown in Figure 5, the forgery detection results further reflect the role of the convolutional autoencoder. The average detection rate of the proposed method is 94.0% for four kinds of common forgery methods, including pitch deviation, speed disturbance, segment splicing and depth parody, and the recognition rate of depth parody samples is 96.3%. The average detection rate was 84.7% for BC-FP, 73.6% for BC-Only and 65.9% for C-DRM. The reason is that the forgery of folk music is not always represented by the overall structure distortion, and many infringe samples only make fine adjustments at the local melody or timbre level. The traditional fingerprint method is more suitable for matching, but not good at identifying deep structure shifts.

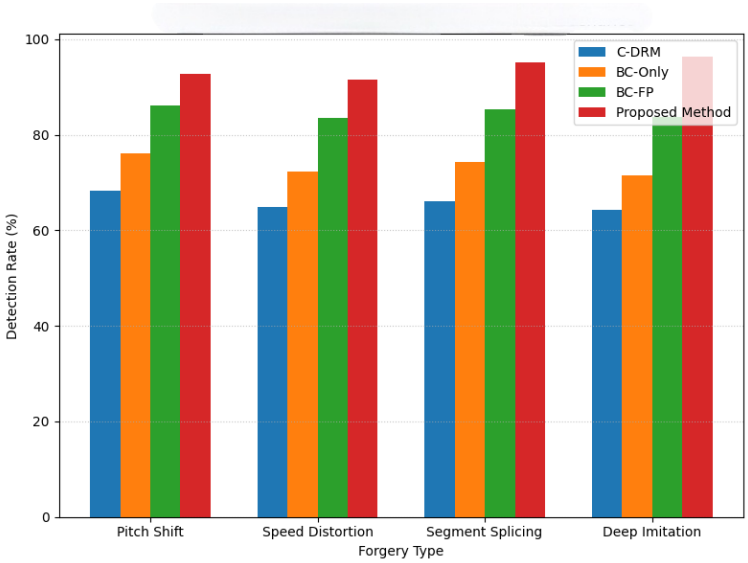

Figure 5: Detection rate /% for different forgery scenarios

As shown in Figure 6, the watermark robustness was tested using four propagation perturbations: 128 kbps compression, 16 kHz resampling, 20 dB noise stacking, and 10% random cropping. Experiments show that the success rates of watermark extraction of the proposed method in four types of scenes are 96.8%, 95.7%, 94.9%and 93.6%, respectively, which are higher than other comparison schemes as a whole. Especially under the condition of random cropping, the extraction rate of traditional watermarking scheme decreases rapidly, while the proposed method can still maintain an effective recovery of more than 90%, which indicates that the latent space embedding strategy has a good balance between invisibility and robustness. For the copyright protection of folk music, this is particularly critical, because many platforms transmit not the complete work, but the cropped highlight fragments or secondary edited fragments. If the watermark becomes invalid quickly in this kind of processing, the storage certificate on the chain is difficult to really play a role.

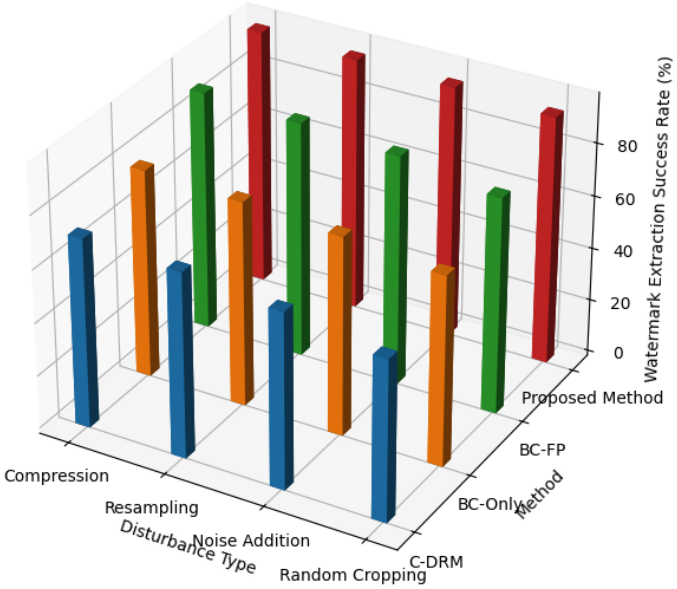

Figure 6: Success rate of watermark extraction /% under different disturbance conditions

In terms of real-time verification efficiency, the proposed method does not significantly sacrifice response speed due to the introduction of deep models and on-chain interactions. Taking 100 concurrent verification requests as an example, the average verification delay of the proposed scheme is 138 ms, 167 ms for BC-FP, 204 ms for BC-Only, and 151 ms for C-DRM. Although C-DRM does not need on-chain query and its latency is not high, its accuracy and traceability ability are obviously insufficient. BC-Only is affected by on-chain retrieval and metadata transmission, and its response speed is slow. By establishing a lightweight on-chain index and a local cache mechanism, the method in this paper separates the feature comparison and the ledger query, so that the delay is controlled within the acceptable range of the platform while ensuring the integrity of the verification. The on-chain integrity test shows that after 24 hours of continuous pressure operation, the on-chain record integrity score of the proposed method reaches 0.988, which is higher than 0.961 of BC-Only and 0.954 of BC-FP, indicating that the process of smart contract triggering and state synchronization is relatively stable.

The test setup of source attribution accuracy is closer to the real application scenario. In the experiment, different singing methods, different mode versions and different Musical Instruments under the same melody theme were mixed into the system to investigate the source judgment ability under the condition of high similarity. When the number of candidate approximate samples is 50, the source attribution accuracy of the proposed method is 93.4%. When the approximate sample is extended to 200, the value still remains at 91.1%. In contrast, BC-FP drops to 83.6%, BC-Only to 77.4%, and C-DRM to 70.8%. This result indicates that the proposed framework has a good ability to distinguish "similar but not identical" folk music samples, and will not easily be misclassified because of different sung versions of the same tune. For folk music copyright management, this ability is more important than simply identifying "whether the same fragment exists", because its copyright disputes often occur at the variant boundary rather than the full copy level.

5 Discussion

The experimental results show that the blockchain copyright protection framework constructed in this paper has good comprehensive adaptability in the folk music scene. Compared with the schemes that only rely on centralized registration, on-chain storage or conventional audio fingerprinting, the advantage of the proposed method does not simply come from the performance improvement of a certain module, but lies in the synergistic relationship formed between blockchain, watermark embedding, convolutional autoencoder and real-time verification interface. The audio watermarking completes the implicit binding between the content of the work and the ownership information. The convolutional autoencoder is responsible for identifying the deep time-frequency anomalies, and the real-time traceability module converts the model output into executable copyright verification results in time. This structure makes the copyright protection of folk music change from static recording to dynamic calculation, which better responds to the practical problems of fragmentary transmission, frequent version variation and increasing concealment forgery. From the experimental performance, the method in this paper still maintains high right confirmation accuracy and source attribution accuracy under the condition of high similar samples, indicating that it has a strong ability to distinguish the "homologous different singing" and "local rewrite" of folk music. This is particularly important. Folk music is often accompanied by reinterpretation, reorchestration and rhythm arrangement in the transmission process. If the copyright system can only recognize the exact same audio files, it is difficult to adapt to the real use situation. In this paper, the latent space watermarking is combined with the metadata index on the chain, which not only improves the recognition ability of the original work, but also enhances the

ability to associate and determine the propagated variants. At the same time, the convolutional autoencoder shows strong sensitivity to imitation singing, splicing and deep synthesis samples, indicating that the anomaly detection idea based on reconstruction error is suitable for the analysis of copyright forgery of folk music. The method in this paper still needs to be further improved. On the one hand, different ethnic music has significant differences in scale organization, vocalization mode and instrument spectrum characteristics. Although the existing models have certain cross-genre adaptability, they may still have the problem of unbalanced feature expression under more complex cross-regional corpus conditions. On the other hand, the advantage of trusted registration brought by blockchain is also accompanied by the increase of on-chain storage overhead and system synchronization cost. If the application scale continues to expand in the future, more detailed engineering design is still needed in terms of on-chain data compression, edge computing collaboration and high-concurrent index optimization. In addition, copyright protection is not only a problem of technical identification, but also involves the definition of ownership, authorization boundaries and cultural sharing norms. Especially in folk music resources, collective inheritance and individual creation are often intertwined, and a single technical framework cannot replace further clarification of the system level.

6 Conclusions

Focusing on the problems faced by folk music in digital transmission, such as decentralized copyright registration, hidden content tampering, and difficulty in source tracking, this paper constructs a copyright protection algorithm framework supported by blockchain. In this study, audio watermarking, convolutional autoencoder and consortium blockchain registration mechanism are combined to form a complete technical link covering copyright registration, forgery detection, real-time traceability and online verification. Compared with traditional methods that rely on centralized recording or single fingerprint matching, the proposed framework not only improves the credibility of ownership confirmation, but also enhances the identification ability of clip editing, deep imitation singing and transmission variants, which makes the copyright protection of folk music move from static storage to content-oriented dynamic verification. The experimental results show that the proposed method has better comprehensive performance in copyright confirmation accuracy, forgery detection rate, watermark robustness, source attribution accuracy and real-time verification efficiency. This shows that blockchain can not only assume the role of a registration tool, but also form a more stable and credible support in the copyright management of folk music when it runs in coordination with deep feature modeling and implicit copyright tagging. Especially under the condition of the coexistence of high similarity samples and complex propagation disturbances, the framework still maintains strong adaptability, showing certain application and promotion value. The copyright protection of folk music is not only a legal proposition, but also an engineering problem that requires continuous intervention of computer technology. The follow-up work can further expand the cross-regional, multi-lingual and multi-style folk music corpus, optimize the on-chain index and edge verification mechanism, and improve the real-time deployment ability in the mobile terminal and platform audit scenario, so as to provide a more solid technical foundation for the long-term protection, standardized circulation and credible utilization of folk music digital resources.

Funding

General Project of National Social Science Foundation, Survey and Research on "Jia Li" of

Miao Nationality in Leigong Mountain, Guizhou Province, 19BMZ093

References

[1] Bodó B, Gervais D, Quintais J P. Blockchain and smart contracts: the missing link in copyright licensing?[J]. International Journal of Law and Information Technology, 2018, 26(4): 311-336.

[2] Ma Z, Jiang M, Gao H, et al. Blockchain for digital rights management[J]. Future Generation Computer Systems, 2018, 89: 746-764.

[3] Liu Y, Zhang J, Wu S, et al. Research on digital copyright protection based on the hyperledger fabric blockchain network technology[J]. PeerJ Computer Science, 2021, 7: e709.

[4] Heo G, Yang D, Doh I, et al. Efficient and secure blockchain system for digital content trading[J]. IEEE Access, 2021, 9: 77438-77450.

[5] Katzenbeisser S, Lemma A, Celik M U, et al. A buyer–seller watermarking protocol based on secure embedding[J]. IEEE Transactions on Information Forensics and Security, 2008, 3(4): 783-786.

[6] Bianchi T, Piva A. Secure watermarking for multimedia content protection: A review of its benefits and open issues[J]. IEEE signal processing magazine, 2013, 30(2): 87-96.

[7] Hua G, Huang J, Shi Y Q, et al. Twenty years of digital audio watermarking—a comprehensive review[J]. Signal processing, 2016, 128: 222-242.

[8] Wu C P, Su P C, Kuo C C J. Robust audio watermarking for copyright protection[C]// Advanced Signal Processing Algorithms, Architectures, and Implementations IX. SPIE, 1999, 3807: 387-397.

[9] Zhao B, Fang L, Zhang H, et al. Y-DWMS: A digital watermark management system based on smart contracts[J]. Sensors, 2019, 19(14): 3091.

[10] Frattolillo F. A watermarking protocol based on blockchain[J]. Applied Sciences, 2020, 10(21): 7746.

[11] Serrano S, Sahbudin M A B, Chaouch C, et al. A new fingerprint definition for effective song recognition[J]. Pattern Recognition Letters, 2022, 160: 135-141.

[12] Serrano S, Scarpa M. Accuracy comparisons of fingerprint based song recognition approaches using very high granularity[J]. Multimedia Tools and Applications, 2023, 82(20): 31591-31606.

[13] Costa Y M G, Oliveira L S, Silla Jr C N. An evaluation of convolutional neural networks for music classification using spectrograms[J]. Applied soft computing, 2017, 52: 28-38.

[14] Nasridinov A, Park Y H. A study on music genre recognition and classification techniques[J]. International Journal of Multimedia and Ubiquitous Engineering, 2014, 9(4): 31-42.

[15] Wang X. Research on recognition and classification of folk music based on feature extraction algorithm[J]. Informatica, 2020, 44(4).

[16] Xu Z. Construction of intelligent recognition and learning education platform of national music genre under deep learning[J]. Frontiers in Psychology, 2022, 13: 843427.

[17] Ciriello R F, Torbensen A C G, Hansen M R P, et al. Blockchain-based digital rights management systems: Design principles for the music industry[J]. Electronic markets, 2023, 33(1): 5.

[18] Li N. Combination of blockchain and AI for music intellectual property protection[J]. Computational intelligence and neuroscience, 2022, 2022(1): 4482217.

[19] Zhao S, O'Mahony D. Bmcprotector: A blockchain and smart contract based application for music copyright protection[C]//Proceedings of the 2018 international conference on blockchain technology and application. 2018: 1-5.

[20] Frattolillo F. Blockchain and smart contracts for digital copyright protection[J]. Future Internet, 2024, 16(5): 169.

[21] Qureshi A, Megias Jimenez D. Blockchain-based multimedia content protection: Review and open challenges[J]. Applied Sciences, 2020, 11(1): 1.

[22] Xiao X, Zhang Y, Zhu Y, et al. FingerChain: Copyrighted multi-owner media sharing by introducing asymmetric fingerprinting into blockchain[J]. IEEE Transactions on Network and Service Management, 2023, 20(3): 2869-2885.

[23] Islam M M, In H P. Decentralized global copyright system based on consortium blockchain with proof of authority[J]. IEEE Access, 2023, 11: 43101-43115.

[24] Zhaofeng M, Weihua H, Hongmin G. A new blockchain-based trusted DRM scheme for built-in content protection[J]. EURASIP Journal on Image and Video Processing, 2018, 2018(1): 91.

[25] Kowalczuk Y, Holub J. Evaluation of digital watermarking on subjective speech quality[J]. Scientific Reports, 2021, 11(1): 20185.