デジタルコンテンツの類似性に基づく権利保証のための新たなNFT方式

山中 圭[1,a)]　三村 昌裕[2]　面 和成[1]

概要：非代替性トークン（NFT）はデジタルコンテンツの所有権を保証する技術として注目されており，その市場は急速に拡大している．しかしながら，NFT はあらかじめ指定したデジタルコンテンツに対してのみ所有権を保証するという制限がある．たとえば，ある画像を NFT 化しても，その画像が解像度の削減やトリミングといった加工を受けた場合，NFT による保証の対象外となってしまう．本研究では，類似性の基準を導入することにより，特定の範囲に含まれる複数のデジタルコンテンツの所有権を一括で保証可能な新たな NFT 方式を提案する．本方式の核心は，従来の暗号学的ハッシュ関数を Image Hash 関数に置き換えることで，所有権の対象を「点」ではなく「領域」として指定可能にする点にある．これにより，個別のコンテンツを明示的に指定しなくても，類似性の高いコンテンツを自動的に NFT の保証範囲に含めることができる．さらに，本方式の実現可能性を検証するために，リサイズ及びクロッピングといった一般的な画像変換を対象とし，Polygom ブロックチェーン上で 4 種類の Image Hash を用いた実装評価を行った．その結果，Average Hash 及び Perceptual Hash が適しており，NFT の検証処理も効率的に実行できることを示した．本方式は，NFT の保証範囲を柔軟に拡張する革新的な技術であり，NFT の新たな応用可能性を切り拓くものである．

キーワード：ブロックチェーン，NFT，Image Hash，デジタルコンテンツ

A Novel NFT Scheme for Similarity-Based Ownership Guarantee of Digital Content

Kei Yamanaka[1,a)]　Masahiro Mimura[2]　Kazumasa Omote[1]

Abstract: This research proposes a new NFT scheme capable of guaranteeing ownership for multiple digital assets that fall within a specific range of similarity. The core of this method lies in replacing conventional cryptographic hash functions with Image Hash functions, which allows the scope of ownership to be defined as a “region” of similar content rather than a single “point” This enables highly similar content to be automatically included within the NFT’s scope of guarantee without explicit designation. To verify the feasibility of this scheme, we implemented and evaluated a prototype using four types of Image Hash functions against common image transformations, such as resolution reduction and trimming on the Polygon blockchain. The results indicate that both Average Hash and Perceptual Hash are suitable functions, and that the NFT verification process can be performed efficiently. This method represents an innovative technology that flexibly extends the scope of an NFT’s guarantee, paving the way for new potential applications for NFTs.

Keywords: blockchain, NFT, image Hash, digital content

1. はじめに

ブロックチェーン技術を基盤とした非代替性トークン

[1] 筑波大学
University of Tsukuba
[2] 株式会社ソーシャルパス
Social Path Co., Ltd.
[a)] s2420552@u.tsukuba.ac.jp

（NFT）は，デジタル資産の所有権[*1]を証明し取引するための革新的な枠組みとして登場した．従来のデジタルデータが無限に複製可能であったのに対し，NFT は個々のトークンに唯一無二の識別子を付与し，ブロックチェーン上にその所有権の履歴を記録することで，デジタルコンテンツに検証可能な希少性と真正性をもたらす [1]．この特性は，デジタルアートの世界に大きな変革をもたらし，クリエイターが仲介者を介さずに自身の作品を直接収益化し，世界中のコレクターと繋がる新たなクリエイターエコノミーを促進している [2].

しかし，NFT の市場が急速に拡大する一方で，その技術的・構造的な脆弱性も数多く指摘されている．NFT は多くの場合，デジタルコンテンツ本体ではなく，そのコンテンツが保存されている場所を示す URL のみをブロックチェーン上に記録している．この構造は，NFT とデジタル資産の永続的な接続を保証しないという根本的な脆弱性を内包している [3]．そのため，リンク切れやサーバの停止によって資産との接続が失われ，利用者が実質的に「空の NFT」を取得してしまう深刻なリスクがある [4]．さらに，Das ら [4] は，正規の作品を無断で NFT 化する偽造 NFT の発行，同一人物が売買を繰り返して価格を不当に吊り上げるウォッシュトレード，スマートコントラクトの脆弱性を悪用した所有権の窃取，NFT マーケットプレイス自体の不十分なユーザ認証プロセスに至るまで，主要なセキュリティ問題を特定し，その危険性を報告している．

中でも深刻な問題として，デジタルコンテンツ本体が分離している特性を悪用し，第三者がオリジナル作品の画像を無断でコピーし，それを用いて外見上は区別がつかない偽造 NFT を発行する事例が多発している．大手 NFT マーケットプレイスである OpenSea は，このような偽造行為をコピーミンティングと定義し，単純な複製だけでなく，画像の反転・回転，リサイズやクロッピング，テキストやロゴの追加，背景色や全体的な色調の変更，解像度低下など，視覚的に類似性が高いと判断される広範な改変を規約違反の対象としている [5]．偽造品を検出することは困難であり，多くの偽造 NFT が市場でオリジナル作品と区別なく流通している．結果として，利用者が意図せず価値のない偽造 NFT を購入してしまう金銭的被害や，オリジナルクリエイターの権利侵害といった深刻な問題を引き起こしている [6].

本研究で特に焦点を当てるのは，NFT が全く同一のデジタルコンテンツにしか所有権を保証できないという制限である．この制限は，NFT が SHA-256 のような暗号学的ハッシュ関数が用いられていることに起因する．暗号学的ハッシュ関数は，入力が 1 ビットでも異なれば出力値が完全に変化するように設計されている．そのため，ある画像を NFT 化しても，その画像の解像度を削減したり，一部をトリミングしたりといった視覚的には軽微な加工を施した場合，加工後の画像のハッシュ値は元の値とは全く異なるものとなり，加工後の画像は NFT の権利の対象外となってしまう．

本研究が着目する課題に関連して，これまでにも偽造 NFT を検出するための様々な研究が行われてきた．主要なアプローチとして，NFT 発行後に市場を監視し Image Hash で類似画像を検出する手法 [7] や，深層学習を用いて画像の盗用を高精度で判定する AI モデル [8] などが提案されている．しかし，これらのアプローチはいずれも「第三者による不正なコピー」の検出や追跡を目的としており，類似性の高いコンテンツを保証範囲に含めることできていない．

本研究の目的は，NFT の「保証範囲の限定性」という課題を解決する方法として，Image Hash を用いて所有権の対象を「点」から「領域」へと拡張する新たな NFT 方式を構築することである．本研究の主な貢献を以下に示す．

- Image Hash を用いて NFT の保証範囲を単一のコンテンツから類似コンテンツの集合へと拡張する，新たな NFT 方式を提案した．
- Polygon ブロックチェーンを用いたプロトタイプ評価により，約 18 万件規模のデータセットに対して，FPR（偽陽性率）を 0.5%未満に抑えながらリサイズ等の主要な加工で高い検知精度を達成し，かつ 1 検証あたり平均 0.8 秒という実用的な速度で動作することを実証した．
- 複数の Image Hash 関数の性能を定量的に比較評価し，リサイズやクロッピングといった基本的な画像変換において Average Hash (aHash) 及び Perceptual Hash (pHash) が適していることを実験的に示した．

2. 準備

2.1 NFT

NFT（Non-Fungible Token）とは，ブロックチェーン上で発行・管理される唯一無二の価値を持つデジタルトークンである．各トークンごとに異なる識別子（Token ID）が付与され，それぞれが固有の価値を持つため代替不可能という特徴を持つ．

NFT のスマートコントラクトは，(1) 所有者アドレス，(2)Token ID，(3) メタデータへのリンクである Token URI を主に記録する．デジタルコンテンツ本体は，データサイズや記録コストの問題から，改ざん耐性を持つ分散型ストレージ IPFS（Inter-Planetary File System）に保存されるのが一般的である．

この構造は，誰でも同じデジタルコンテンツを IPFS に

[*1] 本稿で用いる「所有権」という語は，NFT によって保証されるデジタルコンテンツの広義の権利を指すものとする．ただし，日本の法律では，「データの所有権」という文言は正式な法律用語としては認められていないことに留意する．

アップロードし，それに基づいて新たな NFT を発行できるという脆弱性を内包している．多くのスマートコントラクトは，同一の CID を用いた重複発行を制限するよう設計されているが，全てのプラットフォームがその制約を課しているわけではない．結果として，オリジナル作品とほとんど同一の偽造 NFT が市場に流通し，利用者が誤って価値のないトークンを購入し，オリジナル作品の価値が失われる問題が発生する [9].

2.2 Image Hash

Image Hash は，画像の視覚的な特徴を抽出し，短い固定長のハッシュ値に変換する技術である．元画像にリサイズや色の変更といった加工が加わっても，類似したハッシュ値を生成する特性を持つ．一般的な Image Hash のアルゴリズムは，以下の 4 段階の処理で構成される [7]:

(1) 前処理: 画像を固定の低解像度（例: 8x8 ピクセル）に変換し，色情報を除去してグレースケール化する．
(2) 特徴抽出: グレースケール化された画像から，ピクセルの輝度平均値や周波数成分など，画像の視覚的特徴を抽出する．
(3) ハッシュ値の計算: 抽出した特徴量を基に，各部分が平均値や中央値より大きいか小さいかを判定し，ビット列（'0' または'1'）に変換してハッシュ値を生成する．
(4) 類似度計算: 2 つの画像のハッシュ値を比較し，「ハミング距離」を計算する．この距離が事前に設定した閾値より小さい場合，2 つの画像は視覚的に類似していると判断される．

Image Hash には複数の手法が存在し，それぞれ特徴抽出の方法が異なる．主な手法として以下が挙げられる [7].

- aHash (Average Hash): ピクセル全体の輝度の平均値を算出し，各ピクセルの輝度が平均値より高いか低いかでビット値を決定する，最もシンプルな手法である．
- pHash (Perceptual Hash): 画像を DCT（離散コサイン変換）によって周波数成分に変換し，低周波成分を基にハッシュ値を生成する．人間の視覚特性を利用するため aHash より頑健性が高いとされる．
- dHash (Difference Hash): 隣接するピクセル間の輝度の差分（勾配）を基にハッシュ値を生成する．画像の細かなテクスチャよりも，輪郭などの変化に注目する手法である．
- wHash (Wavelet Hash): ウェーブレット変換で周波数成分を解析し，輝度の中央値との比較でハッシュ値を生成する．
- cHash (Color Hash): 画像の色相，彩度，明度といった色の情報を基にハッシュを生成する手法の総称である．例えば cHash では，画像を HSV 色空間に変換した後，各領域の色の統計的特徴からハッシュ値を計算する．
- sHash (Segmentation-based Hash): クロッピング耐性向上のため，画像セグメンテーションで識別した主要オブジェクトごとに個別のハッシュ値を計算する手法である．これにより，画像の一部が切り取られても，残ったオブジェクトのハッシュ値によって類似性を判定できる．

3. 関連研究

NFT の著作権保護・偽造防止に関する研究は，主に発行後の NFT を対象とするものと，機械学習を用いるものに大別される．

Kotzer らの研究 [7] では，NFT の複製・改変を検出する手法として，Image Hash の有効性を示した．この研究では，aHash や pHash など複数の Image Hash 関数を取り上げ，回転やリサイズといった改変パターンごとに各関数の性能を詳細に評価している．その上で，単一のハッシュ関数ですべての加工パターンに対応するのは困難であるとし，複数のハッシュを組み合わせた検出器が 97.5%の精度を達成するなど，高い有効性を示している．しかし，この手法はブロックチェーンに記録済みの NFT を対象とする事後的な検出を前提としている．そのため，悪意のある NFT が市場で発見・警告されるまでのタイムラグに利用者が偽造品を購入してしまうリスクは依然として残り，NFT 市場全体の信頼性低下という根本的な問題の解決には至らない．

画像の視覚的類似性とは別に，Chen ら [10] は，権利情報をオンチェーンで管理し著作権追跡を可能にする NFT モデルを提案した．このモデルは，デジタルコンテンツのハッシュ値や作者の署名といった権利情報をオンチェーンで記録・管理することにより，元データが複製・流出してもその著作権の帰属を追跡できる仕組みを構築している．

同様に，Bellagarda らの研究 [11] では，認証されたデジタルアイデンティティを NFT に紐付けることで詐欺を削減する Web アプリケーションを提案している．これらの研究は，本研究とは異なるアプローチで NFT エコシステムが抱える課題解決を目指すものである．

Prihatno らの研究 [8] では，深層学習を用いた NFT の画像盗用検出 AI モデルが提案されている．この手法は，EfficientNet をベースとした CNN モデルを用いて画像の特徴量を抽出し，Triplet Semi-Hard Loss と呼ばれる手法でモデルを学習させることで，微小な改変に対しても頑健な識別能力を獲得している．しかし，このような深層学習モデルは一般に推論に多くの計算資源を必要とする．この研究では pHash のような軽量な手法との性能比較がなく，NFT 発行前のリアルタイム検証に求められる速度やコストの実用性は検証されていない．そのため，本研究が目指す軽量化と所有権範囲の拡張への直接的な応用は困難である．

以上のように，既存研究は NFT 発行後の事後的な検出 [7] や，高い計算コストを要する機械学習モデル [8]，あるいはデータ構造の拡張による信頼性向上 [10][11] に焦点を当てている．しかし，これらのアプローチはいずれも不正なコピーの検出や追跡を目的としており，NFT の保証対象を「点」から「領域」へと拡張するという課題には取り組んでいない．したがって，NFT の保証範囲の限定性という問題を，実用的なコストと速度で解決する手法は未だ確立されていない．そこで本研究では，高速な Image Hash を NFT の発行プロセスに組み込むアーキテクチャを提案することで，NFT の保証範囲を拡張する．

4. 提案手法

4.1 概要

本研究では，NFT の「所有権の範囲の限定性」という問題を解決するため，Image Hash を用いて所有権の対象を「領域」として指定する新たな NFT 方式を提案する．

提案手法は，NFT の発行プロセスに Image Hash を用いた類似度検証を組み込むアーキテクチャである．発行ロジックと検証ロジックの 2 つに分離される．発行ロジックは，NFT を発行するトランザクションを生成する．検証ロジックは，入力された NFT が既存の NFT と視覚的に類似しているか否かを判定する．

4.2 構成要素

- 利用者
  NFT の新規発行を希望するユーザである．本稿で提案するクライアントシステムは，ユーザが操作する Web アプリケーションを想定しており，Image Hash の計算，既存ハッシュ群との類似度検証，トランザクションの生成といった本手法の核となる処理をオフチェーンで実行する．このシステムを用いて，NFT 化したい画像をアップロードし，発行をリクエストする．
- 検証者
  検証プロセスは特定の主体に限定されず，誰でも検証者となることができる．検証者は，クライアントシステムを用いて，発行をリクエストされた画像の Image Hash を計算し，ブロックチェーン上の Image Hash との類似度を検証する．
- ブロックチェーン
  検証済み NFT の所有権情報，IPFS の CID を含むメタデータ，Image Hash を永続的に記録する分散型台帳である．また，クライアントシステムが類似度検証を行う際に，記録済みの Image Hash 群を提供するデータソースとしても機能する．
- IPFS
  NFT の画像ファイル本体を保存する分散型ストレージネットワークである．アップロードされた画像は内容に基づいた一意の CID を付与され，永続的かつ改ざん困難な形で保持される．

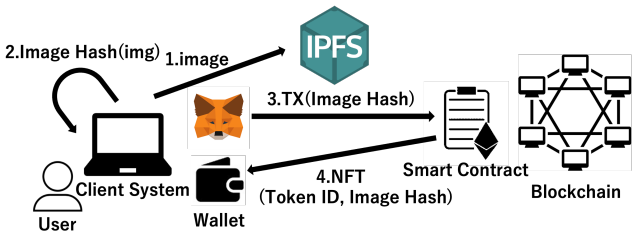

図 1: 提案 NFT 発行プロセスの構成図
Fig. 1 Overview of the Proposed NFT Minting Process.

4.3 攻撃モデル

提案手法における攻撃モデルとして，以下のような脅威を考える．

- 所有権回避攻撃（Ownership Evasion Attack）：攻撃者が標的画像のコピーに微小な改変を加える．これにより，人間の目には酷似しているが，システムの類似度判定の閾値をわずかに超える類似画像を意図的に作成し，すでに NFT 化されている権利範囲を回避する．
- 所有権妨害攻撃（Ownership Blocking Attack）：攻撃者が Image Hash アルゴリズムの特性を分析し，人間には全く異なって見えるにもかかわらずハッシュ値が極めて近くなる画像ペアを意図的に作成・登録することで，無関係な画像の NFT 発行を妨害する．

本研究では，画像の視覚的類似性に基づく権利範囲の拡張に焦点を当てているため，対策対象とする攻撃モデルを限定している．例えば，メタデータに著名なクリエイターの名前を偽って記載するなりすまし攻撃は，画像の視覚情報に依存しないため本稿の対象外とする．同様に，スマートコントラクトのアクセス制御の不備を突いて類似度検証プロセスを迂回する攻撃も，本稿の対象外とする．

4.4 手順

本節では，NFT を発行するためのプロセス及び Image Hash を用いた類似度検証のプロセスについて詳述する．本稿では，2 つの Image Hash 値のハミング距離を $D(ImageHash, ImageHash')$ で表し，類似度を判定するために用いる閾値を T で表す．

4.4.1 準備

利用者が NFT を発行する準備段階として，まずクライアントシステムに NFT 化したい画像ファイルを指定する．クライアントシステムは受け取った画像に対し，以下の 2 つの処理を並行して実行する．

- 画像の登録：画像ファイル本体を IPFS ネットワークへアップロードし，そのコンテンツ識別子である CID を取得する．この CID は，NFT のメタデータとして画像本体を指し示すために利用される．

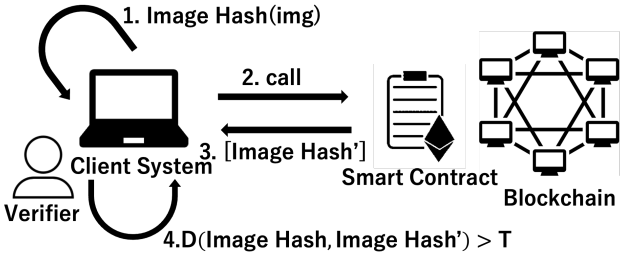

図 2: 提案 NFT 検証プロセスの構成図

Fig. 2 Overview of the Proposed NFT Similarity Verification Process.

- Image Hash の計算：権利範囲の拡張に用いるため，画像から Image Hash を計算する．このハッシュ値は，画像の視覚的な特徴を表現する一意のデータである．

4.4.2 NFT 発行プロセス

提案手法の NFT 発行の流れを**図 1** に示す．後述する 4.4.3 節の NFT 検証プロセスを通過した場合にのみ，クライアントシステムは NFT を発行するためのトランザクションデータを作成する．このトランザクションデータには，主に以下の情報が含まれる．

- to: NFT コントラクトのアドレス
- metadataURI: 画像の場所を示す IPFS の CID
- Image Hash: 権利範囲の拡張に用いた Image Hash
- gasPrice: ガス代
- gas: ガスの上限値

クライアントシステムがブロックチェーンネットワークに対して，署名済みトランザクションをブロードキャストする．トランザクションがネットワークに承認され，ブロックに記録されることで NFT の生成が完了する．これにより，NFT の所有権情報と共に，画像の実体を指す IPFS の CID と，その画像の唯一性を担保する Image Hash が，改ざん不可能な形でブロックチェーン上に記録される．

4.4.3 NFT 検証プロセス

提案手法の類似度の検証の流れを**図 2** に示す．特徴抽出後，検証者はクライアントシステムを用いてブロックチェーンネットワークに接続し，既存の全 NFT に記録されている Image Hash 群をローカル環境に取得する．そして，4.4.1 で計算した新規の Image Hash と，取得した既存のハッシュ群を一つずつ比較し，類似度を検証する．検証の結果，類似度が事前に設定した閾値以内の NFT が一つでも存在した場合，偽造の可能性が高いと判断し，プロセスを中止して利用者に警告する．

5. 実験評価

5.1 実験目的

本章では，Image Hash を用いて NFT の保証範囲を「領域」として拡張する新たな方式について，その有効性と実用性を検証する．実験の目的は，以下の二点である．第一に，提案方式の有効性を示すため，Image Hash が一般的な画像加工に対して NFT の保証範囲を適切に拡張できるかを，精度評価によって定量的に明らかにすることである．第二に，効率性の観点から提案方式の実用性を評価するため，大規模データに対する検証処理の速度を計測し，近似最近傍探索ライブラリ Faiss[*2]の導入による効果を実証することである．

5.2 実験環境

5.2.1 実行環境

ブロックチェーンには Polygon のテストネットワークである Amoy テストネットを利用し，IPFS への接続には Infura の API サービスを用いた．Polygon を用いた理由は，Ethereum と互換性があり，ガスコストが Ethereum に比べて大幅に低いためである．クライアントシステムの開発には JavaScript と Python を併用した．本実験におけるクライアントシステムは，MacBook Pro 上で実装および実行した．主なスペックは，CPU が Apple M1，メモリが 16GB，OS は macOS Sonoma バージョン 14.4.1 である．画像の類似度検証における Image Hash の計算には，Python の image hash ライブラリを利用した [12].

5.2.2 データセット

提案手法の検証精度を評価するため，本実験では公開データセットである Labeled Faces in the Wild (LFW) [13] をオリジナル画像のソースとして利用した．この LFW データセットから 14 点の顔写真をオリジナル画像としてランダムに選定し，それらに対して Python の画像処理ライブラリ Pillow [14] を用いて加工を施すことで，類似画像のデータセットを生成した．加工の基準は，NFT マーケットプレイスである OpenSea が定めるコピーミンティングの定義 [5] に従った．評価の網羅性を確保するため，データセットは以下の 3 種類の画像群で構成される．

(1) オリジナル画像：LFW データセットから選定した 14 点の顔画像.
(2) 類似画像：オリジナル画像に対し，トリミングや解像度低下といった加工を施した顔画像群.
(3) 無関係な画像：偽陽性率（FPR）の評価に用いる，オリジナル画像とは全く関連のない LFW データセットの 12,857 点の顔画像群.

5.2.3 評価の対象

Image Hash には多数の手法が存在するが，先行研究 [7] において，dHash および wHash は複製検出タスクに対する有効性が低いことが示されている．そのため，本研究ではそれらを除く主要な 4 つのハッシュ関数（aHash, pHash, cHash, sHash）を評価対象とする．画像の改変方法は，NFT の複製の画像の加工パターンである「リサイズ (Resize)[*3]」

[*2] https://github.com/facebookresearch/faiss
[*3] リサイズは画像の縦横比を維持したまま，その解像度（ピクセル

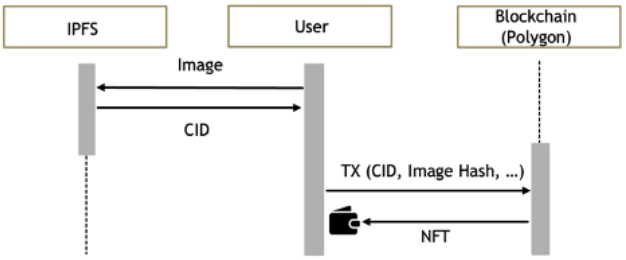

図 3: 提案手法の NFT 発行のシーケンス図
Fig. 3 Flowchart of the Proposed NFT Issuance Process.

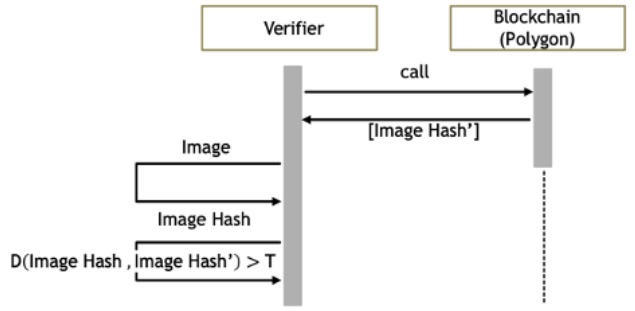

図 4: 提案手法の NFT 検証のシーケンス図
Fig. 4 Flowchart of the Proposed NFT Verification Process.

および「クロッピング (Crop)[*4]」に対する各手法の耐性を評価した．

評価指標には，真陽性率（TPR: True Positive Rate）と偽陽性率（FPR: False Positive Rate）を用いた．TPR は加工された同一人物の画像を正しく「類似コンテンツ」と判定した割合，FPR は別の人物の画像を「類似コンテンツ」と誤判定した割合を示す．理想的なハッシュ関数は，FPR を可能な限り低く抑えつつ，高い TPR を維持できるものである．本研究では，正規のクリエイターの所有権を侵害しないことを優先するため，FPR が 0.5%未満という保守的な水準になるよう，各ハッシュ関数のハミング距離の閾値を調整した．

5.3 実験評価の流れ

本節では，まず一連の発行プロセスを説明し，次節でその実行を制御する検証プロセスについて詳述する．

5.3.1 NFT 発行プロセス

NFT 発行プロセスのシーケンス図を**図 3** に示す．

(1) 5.3.2 節の類似度検証プロセスを通過した場合，最終的な NFT の発行プロセスを開始する．
(2) クライアントシステムは，検証を通過した画像を Infura の API 経由で IPFS へアップロードし，コンテンツ識別子である CID を取得する．

数）を変更する加工を指す．例えば，「Resize 25%」とは，元の画像の縦横の寸法をそれぞれ 25%に縮小することを意味する．

[*4] クロッピングは画像の外周部分を切り取り，中心部分などのみを抽出する加工を指す．例えば，「Crop 70%」とは，元の画像の面積や寸法が 70%になるように外周を切り取ることを意味する．

表 1: Image Hash の性能比較（FPR < 0.5%）
Table 1 Performance Comparison of Image Hash (FPR < 0.5%)

ハッシュ	閾値	Resize TPR [%]			Crop TPR [%]			FPR
		50%	25%	10%	90%	80%	70%	[%]
aHash	10	100.00	100.00	100.00	71.43	42.86	7.14	0.17
pHash	16	100.00	100.00	100.00	100.00	21.43	0.00	0.23
cHash	2.0	85.71	57.14	0.00	35.71	7.14	7.14	0.26
sHash	0.2	85.71	71.43	28.57	28.57	0.00	0.00	0.27

図 5: pHash により類似コンテンツと判定された改変画像
Fig. 5 Modified Images Detected as Similar Contents by pHash.

(3) 取得した CID と，検証に用いた Image Hash を含む NFT 発行トランザクション (TX) を作成し，利用者のウォレットで署名を行う．
(4) 署名済みのトランザクション (TX) をブロックチェーンに送信する．
(5) トランザクション (TX) がブロックチェーンに承認・記録されると，利用者のウォレットに新たな NFT が発行され，プロセスは完了する．

5.3.2 NFT 検証プロセス

NFT 検証プロセスのシーケンス図を**図 4** に示す．

(1) 検証者は，検証対象となる画像をクライアントシステムにアップロードする．
(2) Python の image hash ライブラリを用いて，検証対象の画像から新規の Image Hash を計算する．
(3) ブロックチェーンネットワークから既存の全 NFT に記録されている Image Hash 群を取得する．
(4) 取得した既存ハッシュ群と新規の Image Hash とのハミング距離を一つずつ比較する．
(5) 全てのハミング距離が閾値を超える場合のみ，プロセスは通過する．一つでも閾値以下のハッシュが存在した場合，類似・複製と判断し，プロセスは中止され，類似した NFT が存在することを検証者に通知する．

5.4 性能評価

5.4.1 類似度の計測

各ハッシュ関数の性能を公平に比較するため，偽陽性率（FPR）を 0.5%未満に抑制するという共通の制約を設けた．その制約内で，各加工に対する真陽性率（TPR）が最大となる最適な閾値を選定し，その時点での性能を比較した結

果を**表 1** に示す.

実験評価の結果，本研究で評価した 4 つのハッシュ関数（aHash, pHash, cHash, sHash）は，それぞれ異なる特性を持つことが明らかになった．その中でも，cHash および sHash は，検知精度（TPR）が aHash や pHash に及ばず，本研究の目的である広範な類似画像を保証するには性能が不十分であった．そのため，以降では，総合的に性能の高い aHash 及び pHash に焦点を絞って比較検討を行う.

aHash と pHash は，どちらも全てのリサイズに対して TPR 100%という高い性能を示した一方で，クロッピング耐性では異なる特性が見られた．pHash は Crop90%で TPR 100%という完璧な性能を示したが，より大きな Crop80%および 70%では，aHash が pHash を上回る検知性能を示し，画像の欠損に対する一定の頑健性が見られた.

図 5 は，pHash（閾値 16）が，実際に類似と判定した加工画像の例である．図の Resize50%・10%や Crop90%・80%といった，人間の目には同一コンテンツと認識される改変後の画像は，ハミング距離の閾値内に収まり，正しく類似と判定された．この結果は，リサイズや軽微なクロッピングといった加工を経ても，視覚的に類似したコンテンツを同一の「領域」内のものとして認識し，所有権の保証を継続できることを実証するものである.

5.4.2 実行速度の計測

本実験では，ローカル環境において，179,998 件（データサイズ：1439.984 KB）の Image Hash に対する類似度検証の実行速度を計測した．**表 2** に示す通り，総当たり比較では，aHash および pHash の検証にそれぞれ 133.47 秒，148.06 秒を要した．この結果は，リアルタイム性が求められるシステムにおいて，単純な線形探索が実用的ではないことを示している．pHash は類似度判定の閾値が高めに設定されるため，ハミング距離がある程度離れたものまで探索する必要があり，単純な線形探索では計算量が膨大になる.

この問題を解決するために、近似最近傍探索ライブラリである Faiss [15] を導入し、検証時間の大幅な短縮を図った。Faiss を用いた場合、比較件数の増加に伴い検証時間はほぼ線形に増加するに留まり、高い拡張性を示した。具体的には、1 万件の比較は約 0.005 秒、10 万件でも約 0.045 秒で完了し、本実験の最大規模である約 18 万件に対しても検証時間はわずか 0.08 秒であった。これは、総当たり比較で 148.06 秒を要した処理を大幅に高速化できたことを意味する。この結果は、Faiss のような最適化された探索手法を用いることで、精度面で優れる pHash を実用的な速度で運用可能であることを示しており、提案手法の核となる検証プロセスは Faiss の導入によって十分な実用性が担保されると結論付けられる。

表 2: 179,998 件の Image Hash の検証処理時間の比較

ハッシュ関数	比較方法	実行時間
aHash	総当たり	133.47 秒
	近似最近傍探索（Faiss [15]）	0.10 秒
pHash	総当たり	148.06 秒
	近似最近傍探索（Faiss [15]）	0.8 秒

6. 考察

6.1 提案手法の有効性と安全性

6.1.1 有効性に対する考察

実験結果は，提案手法が NFT の権利範囲の拡張の手段として有効であることを示している．5.4.1 の類似度評価では，aHash 及び pHash がリサイズとクロッピングといった一般的な画像加工に対して高い耐性を持つことが確認された．さらに 5.4.2 の速度評価では，pHash と近似最近傍探索ライブラリ Faiss を組み合わせることで，約 18 万件のデータに対する検証時間が 148 秒から 0.8 秒へと劇的に短縮されることが示された．これは，ユーザが NFT を発行する際の待ち時間をほとんど発生させることなく，リアルタイムで類似度検証が可能であることを意味する．これにより，本研究が目指す「NFT の保証範囲の拡張」が，実用的な性能で実現可能であることが実証された.

6.1.2 安全性に対する考察

提案手法の安全性について，4.3 節で定義した攻撃モデルに基づき考察する.

- 所有権回避攻撃（Ownership Evasion Attack）への対策：本手法は，この脅威に対し高い検知精度（TPR）で対抗する．実験結果より，FPR を 0.5%未満に抑制した条件下では，aHash（閾値 10）及び pHash（閾値 16）が全てのリサイズおよび 90%クロッピングされた画像に対して TPR 100%を達成した．これは，攻撃者が検知を回避するためには，単なる軽微な加工ではない改変を加える必要があることを意味しており，単純な閾値回避攻撃に対して耐性を持つことを実証している.
- 所有権妨害攻撃（Ownership Blocking Attack）への対策：偽陽性（False Positive）を狙うサービス妨害攻撃に対しては，低い偽陽性率（FPR）が有効な対策となる．本実験では，全てのリサイズおよび 90%クロッピングされた画像に対して高い精度を保ちつつも，pHash（閾値 16）で FPR を 0.23%に，aHash（閾値 10）では FPR を 0.17%に抑制することに成功した．これは，無関係な画像が誤って類似と判定されるケースが稀であることを示しており，発行妨害を目的とした攻撃の成功確率を低減できている.

図 6: pHash による偽陰性・偽陽性の判定例

Fig. 6 Examples of False Negative and False Positive Judgments.

6.2 制約

本提案手法の根幹をなす類似度判定は，ハミング距離の閾値に依存しており，この閾値の設定が本手法の制約となる．閾値の設定は，偽陽性率（FPR）と偽陰性率（FNR）[*5]の間にトレードオフの関係を生む．閾値を低く設定すればFPRを抑制できる一方で，**図 6** の左 2 枚のような加工された同一人物の画像を別の人物と誤判定する FNR のリスクが高まる．逆に，閾値を高くすれば FNR を低減できるものの，図 6 の右 2 枚のような全くの別作品を類似コンテンツと誤判定してしまう FPR のリスクが増加する．

本手法においては，この閾値の高さが，NFT が保証する権利の「領域」の広さと直結するという，より本質的な意味を持つ．閾値を不用意に高く設定すると，保証範囲が過度に広がり，クリエイターも意図しない別作品を自身の権利範囲に含んでしまう可能性がある．これは，新たなクリエイターの正当な NFT 発行を不当に妨げる，あるいは意図せぬ権利侵害を引き起こすリスクとなる．したがって，閾値の設定は，単なる検知精度だけでなく，この権利範囲の適切性を考慮して慎重に決定される必要がある．

7. まとめ

本研究は，NFT の保証範囲が単一のデジタルコンテンツ（点）に固定され，リサイズやクロッピンといった正当な改変でさえも保証対象外となる「保証範囲の限定性」という課題に着目した．この課題を解決するため，Image Hash 技術を用いて所有権の対象を類似画像の集合（領域）へと拡張する，新たな NFT 方式を提案した．プロトタイプ実装と性能評価を通じて，画像ハッシュとして aHash 及び pHash を，高速な類似探索に Faiss を組み合わせることで，本方式が大規模データに対しても高精度かつ実用的な速度で実現可能であることを実証した．本研究の成果は，NFT の利用価値と信頼性を向上させ，デジタル資産の権利保護における新たな応用可能性を拓くものである．

今後の課題としては，悪意のあるユーザによる検証回避リスクの低減や，画像に特定のパターンを埋め込み類似度を操作する攻撃など，より巧妙な画像の改変に対応するための検知精度の向上が挙げられる．

謝辞 本研究は JSPS 科研費 JP23K24844 の助成を受けたものである．

[*5] 本来，類似していると判定すべきコンテンツを類似していないと誤判定する確率

参考文献

[1] Q. Wang, R. Li, Q. Wang, and S. Chen, “Non-Fungible Token (NFT): Overview, Evaluation, Opportunities and Challenges,” *arXiv preprint arXiv:2105.07447*, 2021.

[2] J. Fairfield, “Tokenized: The Law of Non-Fungible Tokens and Unique Digital Property,” *Indiana Law Journal*, vol. 97, no. 4, pp. 1261–1314, 2022.

[3] S. Sanjaya and K. Omote, “Resolver Contract: Toward an NFT Verification Method with Enhanced Linkability,” in *IEEE ICBC Workshop 2025*. IEEE, 2025, pp. 1–7.

[4] L. Das, H.-H. Tu, Y. Wang, Y. Zhang, and J. Zhao, “Understanding Security Issues in the NFT Ecosystem,” in *ACM CCS 2022)*, 2022, pp. 3139–3152.

[5] A. Fauvre-Willis, “An Update on Verification and Copymint Prevention,” https://opensea.io/blog/articles/an-update-on-verification-and-copymint-prevention, accessed on 2024-12-02.

[6] ——, “We’re Improving the OpenSea Verification Process,” https://opensea.io/blog/articles/were-improving-the-opensea-verification-process, accessed on 2024-12-02.

[7] A. Kotzer, M. Naamneh, O. Rottenstreich, and P. Reviriego, “Detection of NFT Duplications with Image Hash Functions,” in *IEEE ICBC 2024*, 2024.

[8] A. T. Prihatno, N. Suryanto, S. Oh, T.-T.-H. Le, and H. Kim, “NFT Image Plagiarism Check Using EfficientNet-Based Deep Neural Network with Triplet Semi-Hard Loss,” *Applied Sciences*, vol. 13, no. 3, p. 1463, 2023.

[9] Z. Wang, J. Gao, and X. Wei, “Do nfts’owners really possess their assets? a first look at the nft-to-asset connection fragility,” in *WWW 2023*, 2023, pp. 2099–2109.

[10] Y. Chen, Z. Wang, X. Liu, and X. Wei, “A new nft model to enhance copyright traceability of the off-chain data,” in *CoST 2022*. IEEE, 2022, pp. 157–162.

[11] J. Bellagarda and A. M. Abu-Mahfouz, “Connect2NFT: A Web-Based, Blockchain Enabled NFT Application with the Aim of Reducing Fraud and Ensuring Authenticated Social, Non-Human Verified Digital Identity,” *Mathematics*, vol. 10, no. 21, p. 4047, 2022.

[12] J. Buchner, “An image hashing library written in Python,” https://github.com/JohannesBuchner/imagehash, 2023.

[13] G. B. Huang, M. Ramesh, T. Berg, and E. Learned-Miller, “Labeled Faces in the Wild: A Database for Studying Face Recognition in Unconstrained Environments,” University of Massachusetts, Amherst, Tech. Rep. 07-49, 2007.

[14] J. A. Clark, “Pillow (PIL Fork) documentation,” https://pillow.readthedocs.io/en/stable/, 2024.

[15] J. Johnson, M. Douze, and H. Jégou, “Billion-scale similarity search with GPUs,” *IEEE TBD*, 2019.