秘密画像共有における pHash 検索を可能にする知覚暗号化の設計

横田・清水研究室　玉城 洵弥

2025 年度 卒業論文審査会

概要

秘密画像共有（SIS）で分散保存した画像について，平文化せずに知覚ハッシュ pHash による類似画像検索を行う方式を提案する．シェア収集数 r に応じて「ノイズ」「pHash 整合ダミー」「原画像」の三段階で情報を開示し，**「検索はできるが中身は見えない」**という中間状態を実現する．COCO 派生データによる評価では，pHash 検索精度・処理時間ともに平文と同等であることを確認した．

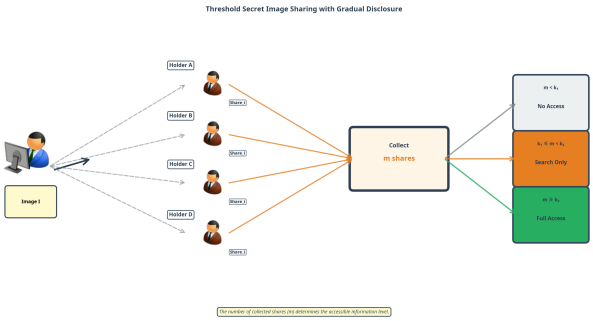

図 1: 三段階 SIS の概念図（k_1: 検索のみ，k_2: 完全復元）

1 はじめに

1.1 背景：利活用と保護のジレンマ

医療画像や個人写真などの機微データは，**「過去の類似症例を検索して診断支援に役立てたい」**という利活用の需要が高い．一方で，これらは患者のプライバシーに直結するため，極めて高度な安全管理も同時に求められる．しかし，既存のデータ管理手法ではこの両立が困難である．

- **オンプレミス管理**: 情報は守れるが，データ消失リスクや管理コストの問題がある．
- **クラウド管理**: 可用性は高いが，特定事業者に原本を預けることによる情報漏洩の懸念がある．

そこで，特定の管理主体に依存せず，可用性と機密性を同時に担保するアプローチとして，画像データを分散して無意味化する**秘密画像共有（SIS）**が注目されている．

1.2 課題：分散データの検索不可能性

SIS はセキュリティに優れる反面，シェア自体はランダムなデータ列であり視覚情報を持たない．「類似検索」を行いたくても，**シェアの状態のままでは画像の類似性を判定することが原理的に不可能**である．従来，「検索」を行うには一度シェアを集めて原画像を復元する必要があったが，これは以下の問題を生む．

1. **セキュリティ低下**: 検索のたびに機微な原画像を復元する必要があり，本来閲覧権限を持たない管理者にも内容が開示されてしまう．
2. **コスト増大**: 毎回復元処理を行う計算・通信コストが高い．

1.3 目的：三段階開示の必要性

本研究の目的は，SIS の安全性を維持しつつ検索を実現することである．しかし，単に検索用データを無条件に公開すると，それを手がかりに原画像の内容が推測されるリスクがある（オラクル攻撃）．したがって，**「検索はさせたいが，中身は見せたくない」**という矛盾する要求を満たすためには，以下の 3 つの状態を明確に区別し，制御する仕組みが不可欠となる．

1. **何もできない状態**（保管時）：データが漏洩しても安全．
2. **検索だけできる状態**（中間段階）：中身は見えないが，類似判定のみ可能．
3. **全てが見える状態**（復元時）：診断などで実際に画像を見る．

この「検索権限」と「閲覧権限」を技術的に分離・制御するために，本研究では新たな**三段階開示モデル**を提案する．

2 提案手法

2.1 三段階開示モデル

シェア収集数 r に対して 2 つの閾値 k_1, k_2（$k_1 < k_2$）を設定し，出力情報の質を段階的に制御する．

$$\mathrm{output}(r) = \begin{cases} \text{noise} & (r < k_1) \\ \text{pHash 整合ダミー} & (k_1 \le r < k_2) \\ \text{原画像} & (r \ge k_2) \end{cases}$$

- **Level 0** ($r < k_1$): 検索・閲覧不可．情報理論的安全性により，原画像に関する情報は一切漏洩しない．
- **Level 1** ($k_1 \le r < k_2$): 検索のみ許可．視覚的には内容が判別できない「pHash 整合ダミー画像」を出力する．
- **Level 2** ($r \ge k_2$): 閲覧・復元許可．原画像を完全復元する．

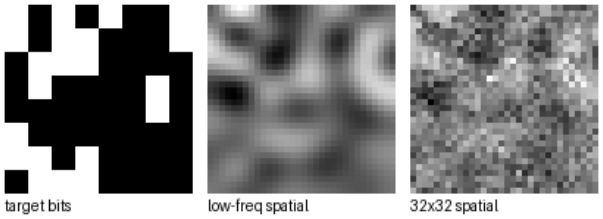

図 2: pHash 整合ダミー生成の流れ（符号抽出→低周波補強 → 32×32 空間像）

2.2 pHash 整合ダミーの生成

Level 1 で出力される「pHash 整合ダミー」は，本研究の核となる技術である．

- **知覚ハッシュ (pHash)**: 画像の低周波成分（DCT 係数）から生成される 64bit のハッシュ値．類似画像間でハッシュ間距離（Hamming 距離）が近くなる性質を持つ．
- **生成アルゴリズム**:
  1. 低周波成分: pHash のビット列と整合するように DCT 係数を操作・強調する．
  2. 高周波成分: ランダムなノイズで埋めることで，輪郭・顔・文字などの視覚情報を意図的に破壊する．
- **効果**: このダミー画像は，pHash による検索エンジンに対しては「原画像と同じもの」として認識されるが，人間の目にはノイズ画像にしか見えない．

3 実験

3.1 実験設定

- **データセット**: COCO val2017 から 500 枚を抽出．
- **派生条件**: 各画像に JPEG 圧縮，回転，クロップ，ノイズ付加など 20 種類の変換を適用（ロバスト性評価）．
- **比較条件**:
  - **plain**: 原画像から生成した pHash を用いた通常の検索（ベースライン）．
  - **dummy_k1**: 提案手法（Level 1）で生成したダミー画像を用いた検索．

3.2 結果：検索精度

Precision@K（検索結果上位 K 件に含まれる正解の割合）により評価を行った．

- **オリジナル評価**: 原画像そのものを探すタスクにおいて，**Precision@1 = 100%** を達成した．
- **ロバスト性評価**: 20 種類の変換画像を探すタスクにおいても，**Precision@1 = 100%, Precision@5 = 86.6%** となり，平文（plain）での検索結果と同等の性能を示した．

これは，提案手法が pHash の頑健性を損なわずに暗号化できていることを示す．

4 結論

SIS における「検索」と「閲覧」のジレンマを解消するため，pHash を用いた知覚暗号化と多段階 SIS を組み合わせた方式を設計・実装した．提案手法は，高い検索精度（平文と同等）を維持しつつ，検索段階での視覚的なプライバシー保護（閲覧抑止）を実現した．これにより，医療画像等の機微データに対して，内容を秘匿したまま類似症例検索を行うセキュアな運用が可能となる．

今後の課題として，ダミー画像からの推測耐性に対するより厳密な安全性評価や，pHash 以外の特徴量への拡張が挙げられる．

参考文献

[1] Z. Xia et al., “A privacy-preserving CBIR scheme based on secret sharing,” *IEEE Access*, 2020.