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 pHash による類似画像検索を行う方式を提案する。シェアのみを持つサーバでも検索できるよう，k_1 で **pHash の符号だけを開示し，視覚的にはノイズ化した pHash 整合ダミー画像だけを見せる**三段階開示モデルを設計した。ここで $1 < k_1 < k_2 \leq n$ とし，k_1 は検索のみ許可，k_2 は完全復元の閾値とする。シェア数に応じて「ノイズ」「pHash 整合ダミー」「原画像」の三段階で情報を開示し，検索精度と秘匿性の両立を図る。MS COCO（Common Objects in Context）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。

1 はじめに

医療画像や監視映像では「検索は必要だが中身は見せられない」という要求がある。既存の類似画像検索（CBIR: Content-Based Image Retrieval）は画像や特徴量を平文で保持するため，漏洩リスクが高い。pHash は軽量で実用的な知覚特徴量である一方，符号を平文で扱うと情報漏洩につながる。また，既存の秘密画像共有（SIS）は「復元する／しない」の二択であり，**復元せずに検索だけを許可する中間状態**を扱えないという課題がある。

プライバシ保護 CBIR では，CNN 特徴量を秘密分散や MPC により安全計算する方式が提案されている。しかし，高次元特徴を前提とするため計算コストが高く，段階的な情報開示は考慮されていない。一方，pHash は低次元で高速だが，暗号技術と統合した研究はほとんど存在しない。特に，**pHash 符号のみを保持したまま視覚情報を消去する設計**は未検討である。

2 提案法

本研究では，pHash の低周波符号構造と二階層 Shamir 秘密分散を組み合わせ，三段階の情報開示を実現する。

定式化（三段階 SIS）

閾値は $1 < k_1 < k_2 \leq n$ とし，k_1 は検索権限，k_2 は原画像復元権限を表す。配布した n 枚のシェア集合を A，$r = |A|$ とし，秘密を S_0, S_1, S_2 で定義する。

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

ここで S_0 は無意味なノイズ画像，S_1 は pHash 整合ダミー生成情報，S_2 は原画像復元情報を表す。安全性として $r < k_1$ で $I(S_1; A) = 0$，かつ $r < k_2$ で $I(S_2; A) = 0$ を要求する。また

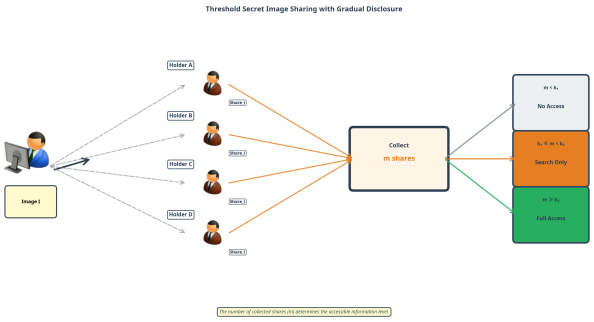

図 1: 三段階 SIS の概念図（k_1: 検索のみ，k_2: 完全復元）

$k_1 \leq r < k_2$ では pHash による検索のみ可能（$\text{pHash}(S_1) = \text{pHash}(I)$）とする。

pHash 整合ダミー

低周波 DCT 符号のみを一致させ，高周波成分をランダムノイズで置換することで，pHash は一致するが視覚情報は失われた画像を生成する。

二階層 Shamir

$n = 5$，$k_1 = 2$，$k_2 = 4$ とし，k_1 で検索権限，k_2 で原画像復元を許可する。

3 実験

COCO val2017 派生データ（500 クエリ，20 バリアント）を用いて評価した。その結果，

- 上位 1 件の検索精度は 100%（平文・ダミー一致）
- 上位 5 件 86.6%，上位 10 件 84.82%（全バリアント）
- 検索時間は約 0.5 ms/query と平文と同等

であり，pHash 整合ダミーが検索性能を劣化させないことを確認した。

4 おわりに

pHash 符号一致ダミーと二階層秘密分散を用いた段階的情報開示方式を提案した。本方式により，**画像を見せずに画像を検索する**という要求を軽量かつ実用的に実現できることを示した。今後は大規模データへの拡張や，CNN 特徴とのハイブリッド化を検討する。

参考文献

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