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（Secret Image Sharing; 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（perceptual hash）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

医用画像や監視映像ではプライバシ侵害の可能性があるため，画像を秘密共有した状態で検索した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．そこで，秘密共有した状態で検索を可能にする暗号化方式を提案する．

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い．加えて，平文特徴の類似度計算を前提に設計されており，秘密共有や知覚暗号化された画像に対しては検索精度が低下するか，そもそも適用対象外になりやすい．段階的な情報開示も備えていない．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

本研究で用いる pHash は，32×32 画像の DCT 左上 8×8 の符号から 64bit を得る軽量特徴であり，低周波構造のみを保持する．二階層 Shamir 秘密分散は，同じシェア集合から k_1 で検索専用の情報，k_2 で原画像を復元する段階閾値を与える．本研究では，両者を組み合わせて三段階の情報開示を実現する．

2.1 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 $k_1 \leq r < k_2$ では pHash による検索のみ可能（$\text{pHash}(S_1) = \text{pHash}(I)$）とする．同じシェア集合から復元結果が段階的に変わる設計であり，**秘密分散のシェア計算を 3 回行うわけではない．**

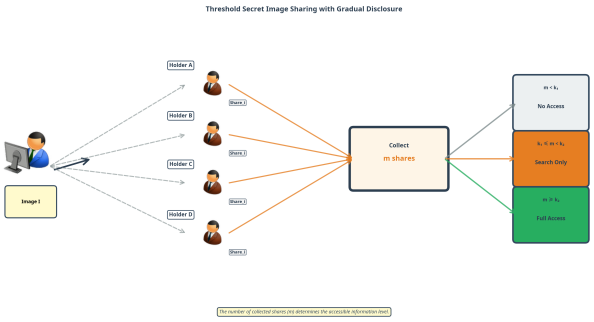

図 1: 三段階 SIS の概念図（k_1: 検索のみ，k_2: 完全復元）

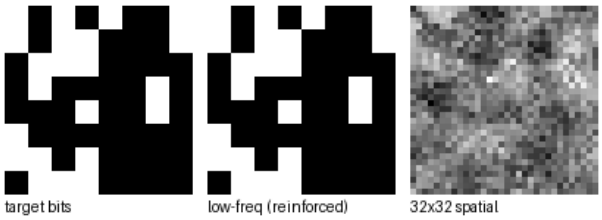

図 2: pHash 整合ダミー生成の流れ（符号抽出→低周波強調→ 32×32 空間）

2.2 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．図 2 に生成手順の要点を示す．

2.3 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．

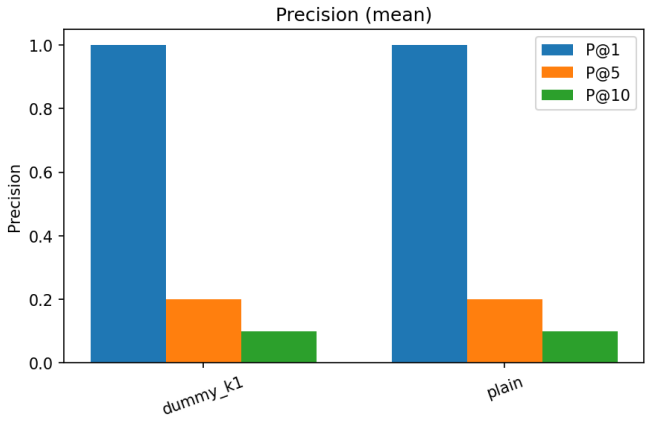

図 3: 検索精度（オリジナルのみ，plain vs dummy_k1）

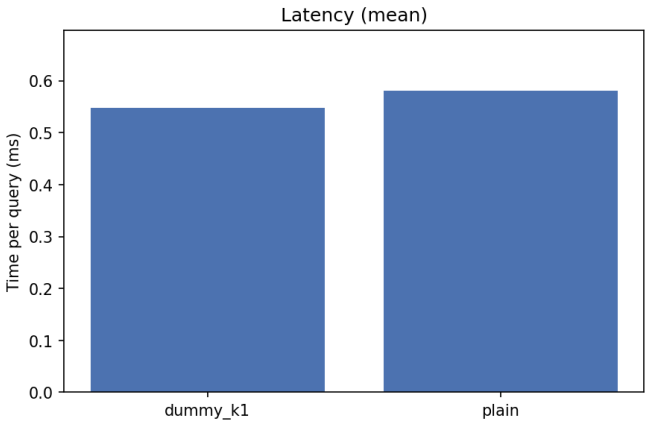

図 4: 検索時間（オリジナルのみ，plain vs dummy_k1）

3 実験

COCO val2017 公式配布[1]から seed=2025 で 500 枚を抽出し，JPEG 劣化・ガンマ/輝度/コントラスト・回転・クロップ・ノイズ・透かし等の 20 種変換を適用して派生データを作成した．各画像について，(1) 32×32 グレースケール化と pHash 計算，(2) 低周波符号を固定した pHash 整合ダミー生成，(3) $n = 5$, $k_1 = 2$, $k_2 = 4$ の二階層 Shamir によるシェア化を行い，平文 pHash と k_1 ダミー pHash の検索順位を比較した．

生成されたダミーは視覚的にはノイズだが pHash 符号は元画像と一致する．同一画像のシェアから k_1 復元した場合は Hamming 距離 0 近傍に集中し，異なる画像のシェア同士では距離が大きく分離した．一方 k_1 未満の組合せでは距離がランダム同等（平均 20.8）となり，pHash の漏洩が起きないことを確認した．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．図 3 と図 4 に，オリジナルのみの精度と時間の要約を示す．

[1] http://cocodataset.org/#download

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.