卒業論文

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

氏名：玉城洵弥

指導教員：清水 恒輔

工学部電気電子・情報工学科情報コース

岐阜大学

提出日：2025 年 2 月 6 日

概要

平文の画像特徴量をサーバに保持する従来の類似画像検索（Content-Based Image Retrieval; CBIR）は情報漏えいのリスクがある．そこで本研究は，秘密画像共有（Secret Image Sharing; SIS）によりシェア数 r に応じて k_1 で検索のみ，k_2 で復元を許可する二段閾値の知覚暗号化方式を提案する．k_1 では検索に必要な低周波符号が一致する知覚ハッシュ（perceptual hash; pHash）整合ダミーを返し，原画像の内容推定に資する視覚情報を開示しない中間状態を定義する．評価では同一 ID の派生群を正解集合とした Recall@k を主指標とし，オリジナルのみの 1 対 1 照合では Top-1 accuracy が 100%（plain/dummy 一致），全 20 バリアント平均で Recall@10=42.41%、Recall@5=21.65%（plain/dummy 一致）を得た．検索時間は 0.50/0.49 ms（オリジナル平文/ダミー），0.53/0.49 ms（全バリアント平文/ダミー）で同等であり，復元コストは k_1=121 ms，k_2=10.2 s に段階化できた．残る課題はアクセスパターン漏えいと pHash の頑健性である．

目次

図目次

表目次

第 1 章

はじめに

1.1 背景

医療画像や監視映像では，プライバシー侵害を避けつつ類似事例を検索したいという要求がある．しかし従来の Content-Based Image Retrieval (CBIR) は検索精度を優先し，画像や特徴量を平文で保持するため，検索のために中身をさらしてしまう．そこで本研究は，画像を秘密画像共有（Secret Image Sharing; SIS）したまま検索可能にする暗号化を設計し，原画像の内容推定に資する視覚情報を開示せずに照合を行うことを目指す．検索の特徴量としては軽量な知覚ハッシュ（perceptual hash; pHash）を用いるが，pHash を平文で扱えば符号から内容を推測される恐れがあるため，その漏洩も抑える必要がある．

1.2 目的

本稿で扱う pHash は，32×32 グレースケール画像の DCT 左上 8×8 の符号から 64bit を得る軽量特徴量であり，低周波構造だけを保持する．また，二階層 Shamir 秘密分散は n=5, $(k_1, k_2) = (2, 4)$ の閾値で「k1 は検索専用」「k2 で原本復元」を分離する多段しきい値版 Shamir である．本研究の目的は，「検索は許可するが閲覧はさせない」中間状態を閾値で保証し，検索のために平文を復元せずに済む SIS を構成することである．従来の SIS は「復元する／しない」の二択しかなく，検索段階で pHash を平文に再構成すれば符号が漏洩し，復元を禁じれば検索自体ができないというジレンマがあった．本研究では k_1 閾値で pHash 符号だけを開示し，k_2 閾値で初めて原画像を復元する二階層 Shamir を用い，k1 では pHash 整合ダミーを返して検索のみを安全に実行できるようにする．pHash 整合ダミーとは，低周波 8×8 DCT の符号だけを元画像と一致させ，高周波をランダムノイズに置き換えた画像であり，見た目はノイズだが pHash は原画像と一致する．

本稿で導入する主要用語をここで簡潔に示す．

- **pHash 整合ダミー (pHash-preserving dummy image)**: 本稿でいう「pHash 整合ダミー」とは，低周波 8×8 DCT の符号だけを元画像と一致させ，高周波をランダムノイズに置き換えた画像である．見た目はノイズだが pHash は原画像と同じになるため，サーバは中身を見ずにハッシュ検索だけを行える．
- **三段階開示モデル** (k_1/k_2): シェア数 r に応じて，$r < k_1$ はノイズ，$k_1 \leq r < k_2$ は pHash 符号一致ダミー，$r \geq k_2$ は原本を復元する． k_1 を検索専用，k_2 を閲覧許可の閾値として用いる．

1.3 貢献

- 低周波符号だけを一致させた pHash 整合ダミーと，二階層 Shamir $(k_1{=}2, k_2{=}4, n{=}5)$ による三段階開示モデルを設計し，「pHash の低周波符号のみ開示／原画像の内容推定に資する視覚情報は非開示」を閾値で保証.
- pHash 整合ダミーを平文 pHash と同じ API（Application Programming Interface）で検索できるようにし，k1 でダミー（低周波符号のみ開示），k2 で原本復元という段階開示を masked SIS パイプラインに実装.
- COCO 派生データ（500 クエリ，20 変換バリアント）で平文とダミーを比較し，オリジナルのみの 1 対 1 照合では Top-1 accuracy が 100%（plain/dummy 一致）となった．全 20 バリアントでは同一 ID の派生群を正解集合とした Recall@10=42.41%、Recall@5=21.65%（plain/dummy 一致）であり，処理時間も平文/ダミーで 0.50/0.49 ms（オリジナル），0.53/0.49 ms（全バリアント）と同等，復元コストは k_1=121 ms, k_2=10.2 s で段階化されることを実測した.

第 2 章

関連研究

近年，プライバシー保護を目的とした類似画像検索（Content-Based Image Retrieval; CBIR）の研究は，暗号技術，秘密分散，多人数安全計算（MPC），検索可能暗号（Searchable Encryption; SE）など，多様な手法を基盤として発展してきた．本章では，(1) 類似画像検索の特徴量，(2) 秘密分散・MPC によるプライバシー保護 CBIR，(3) 検索可能暗号による CBIR，(4) 知覚ハッシュ（pHash）に関する研究，の 4 つの観点から既存研究を整理し，本研究の位置づけを明確にする．

2.1 類似画像検索に用いられる特徴量：CNN と pHash

従来の高精度 CBIR では，VGG, ResNet, EfficientNet などの畳み込みニューラルネットワーク（CNN）による高次元特徴量（512〜4096 次元）が一般的に利用されている．しかしこれらは特徴量の次元数が大きく，暗号化や秘密分散を用いたプライバシー保護処理において計算負荷が高くなることが報告されている（Xia et al. [1]）．一方，pHash（Perceptual Hash）は，低周波領域 DCT の符号パターンから 64bit 程度のハッシュを算出する軽量な知覚特徴量であり，画像の大まかな構造に対してロバストである．しかし，pHash を暗号技術と統合し，プライバシーを保ったまま類似検索を可能にする枠組みはほとんど存在していない．

2.2 秘密分散・MPC を用いたプライバシー保護類似画像検索

秘密分散や MPC を用いたプライバシー保護 CBIR の研究は活発に行われている．Xia et al. [1] は，CNN 特徴量を加法的秘密分散により複数サーバへ分割し，サーバ間の MPC によって距離計算を実行する枠組みを提案した．検索処理は暗号化状態で行えるが，高次元特徴量を対象とするため処理が重い．また，Zhang et al. [2] は Shamir 型秘密分散を用いて CNN 特徴量を分散保持し，復元せずに検索する SS-CNN を提案したが，やはり高次元前提で段階的な情報開示は存在しない．画像特徴そのものを暗号化状態で計算する研究として，Barni et al. [3] は JPEG DCT 係数を暗号化し距離計算を行い，

Troncoso-Pastoriza et al. [4] は近似距離 MPC を提供したが，いずれも準同型暗号や高度な MPC を要し計算コストが高い．さらに，これらの手法は平文特徴や高次元ベクトルを前提としており，知覚暗号化された低次元特徴（本稿の pHash 整合ダミーや SIS シェア）にそのまま適用すると精度が低下するか，復号を伴うため本研究の要件（検索のみ許可・閲覧禁止）に適合しない．加えて，上記いずれの研究も (1) シェア数に応じて復元内容が段階的に変化する設計，(2) pHash の符号構造を用いたダミー画像生成，を備えていない．

2.3 検索可能暗号（SE）によるプライバシー保護 CBIR

検索可能暗号を画像検索に応用した研究も存在する．Tian et al. [5] は特徴量を暗号化し，ツリー構造インデックスに対して検索を行う SE ベースの CBIR を提案している．また，Xia et al. [6] は暗号化画像に対して近似検索を行う方式を示した．しかし，これらは (1) 特徴量または画像全体を暗号化する重い方式であり，(2) pHash を用いた軽量検索には向かず，(3) 段階開示モデル（k_1/k_2）を持たないという制約がある．したがって，SE は強力だが，軽量で実用的な pHash ベース検索のための暗号設計とは目的が異なる．

2.4 知覚ハッシュ（pHash）に関する研究

知覚ハッシュは, 画像同士の類似性を測るために広く利用されている．代表的手法として Venkatesan et al. [7] によるロバストハッシュ生成法が知られており，後続研究でも pHash は著作権管理や偽造検知に利用されてきた．しかし，pHash は本来 認証や重複検出が目的であり，プライバシー保護と結合する研究はほとんど存在しない．特に，(1) pHash の符号構造だけを保ちながら画像を視覚的ノイズに変換する研究，(2) pHash 再現可能なダミー画像を段階的復元モデルに統合した研究，(3) pHash を秘密分散と組み合わせて検索処理に活用する研究は見当たらない．

2.5 本研究の位置づけ

以上の比較から，本研究は以下の点で既存研究とは異なる独自の位置づけを持つ。(1) pHash の低周波符号構造のみに基づき、原画像の内容推定に資する視覚情報を欠く pHash 整合ダミー画像を生成できる点。(2) 秘密分散（SIS）を用い、シェア数に応じて「ノイズ」「pHash 整合ダミー」「原画像」という三段階の開示を実現した点。(3) 検索は軽量な pHash のみで実行し、プライバシーは段階的な復元制御によって保証する枠組みを確立した点。著者が調査した範囲では、「pHash × 秘密分散 × 段階開示」を組み合わせた類似画像検索方式はこれまでに提案されておらず、軽量知覚特徴と暗号技術を統合する新しいアプローチを提供する。さらに，既存研究との対比で強調すべき点は次の 2 つである。(a) Barni, Xia, Zhang, Troncoso らは「高次元特徴を保持したまま距離計算を安全計算化する」重い路線

であり，復元内容を段階開示する設計はない。これに対し本研究は特徴量を pHash に制約し，k_1 で低周波符号のみ開示する極めて軽量な中間状態と，k_2 で原本を復元する高コスト状態を分離した。(b) 既存路線では常に安全計算の重さを支払うが，本研究は「検索は軽量 pHash」「復元は閾値到達時のみ」という役割分担で計算量を段階化し，実験でも 0.5 ms/件（検索）と 10 s（完全復元）のコスト差を実証した。このように特徴量次元の削減と段階開示設計により，MPC/SE 系より大幅に小さい計算量で運用できることを第 5 章の結果（平均 0.5 ms/query）で確認した。

第 3 章

提案手法

3.1 記号と定義

入力画像をグレースケール 32×32 に縮小し DCT を取る。低周波 8×8 ブロック C_{LF} の符号で 64bit の pHash $b \in \{0,1\}^{64}$ を定義し、$b_i = 1$ は正、0 は負の符号を表す。二階層 Shamir は n=5, $(k_1, k_2) = (2, 4)$ とし、$1 < k_1 < k_2 \leq n$ **で** k_1 **は検索のみ許可、**k_2 **は原画像復元許可の閾値**としてシェア数 r に応じた段階開示を次のように定義する:

$$\mathrm{output}(r) = \begin{cases} \mathrm{noise} & (r < k_1) \\ \mathrm{dummy}(b) & (k_1 \leq r < k_2) \\ \mathrm{original} & (r \geq k_2) \end{cases}$$

ここで dummy(b) は pHash 符号が b と一致するノイズ画像である。

3.2 三段階開示

シェア数 r に応じて、$r < k_1$ はノイズ、$k_1 \leq r < k_2$ は pHash 符号一致ダミー、$r \geq k_2$ は原本を復元する。この三段階は一度生成した同じ Shamir シェアを閾値で切り替えて出力するものであり，画像を 3 回別々に分割するわけではない。

3.3 pHash 整合ダミー

ダミー生成の流れを図 4.3 に示す。(1) 元画像を 32×32 に縮小し DCT から target bits（低周波 8×8 の符号）を抽出、(2) 符号が反転しないようマージンを持たせて低周波ブロックを強調（reinforced low-freq)、(3) 高周波をランダムノイズで埋めて逆 DCT し 32×32 空間画像を得る。逆 DCT 後の符号が目標値からずれないよう、低周波振幅を複数回補強し、空間域でのわずかな変動では符号が反転しないマージンを確保する。

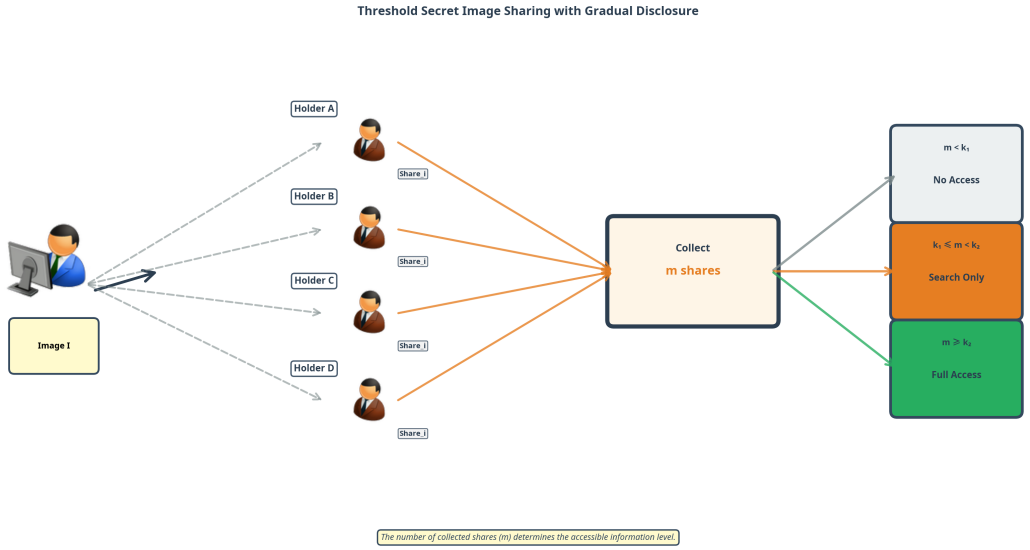

図 3.1　三段階 SIS の概念図（k_1: 検索のみ，k_2: 完全復元）

3.4　攻撃モデルと漏えい評価

本稿では honest-but-curious なサーバを想定し，攻撃者が得る情報を (i) k_1 で復元される pHash 整合ダミー画像，(ii) pHash の低周波符号（64bit），(iii) k_1 未満のシェア断片，(iv) アクセスパターン（検索トークンのヒット構造）とする。攻撃目標は (a) カテゴリ/シーン推定，(b) 人物・文字の有無推定，(c) メンバーシップ推定，(d) 原画像復元である。漏えい評価は PSNR などの画質指標だけでは不十分であり，分類器による推定精度や AUC（Area Under the Curve）などの相互情報量の代理指標，復元攻撃の成功率，メンバーシップ推定の優位度で測定する必要がある。PSNR は視覚的劣化の補助指標としてのみ用い，k_1 未満では pHash 距離がランダム同等であることを確認する。

3.5　検索パイプライン

本稿では masked SIS に特化し、平文 pHash と同一 API で (a) k1 で pHash 整合ダミー検索、(b) k2 で原本復元検索を切り替えるシンプルなパイプラインのみを実装する。シェアは k_1=2, k_2=4, n=5 の Shamir で分割し、生成・復元はクライアント側で完結する。

第 4 章

実装

実装は Python 3 系で構築し、数値計算に NumPy、画像処理に Pillow を用いた。外部依存は最小限とし、DCT/IDCT や Shamir 分散は自前実装で完結させている。

- **pHash 計算**: 32×32 グレースケールへ Bicubic 縮小後、正規直交 DCT-II を行列表現で計算（`dct2`, `idct2`）。左上 8×8 の符号を平均閾値で 64bit ベクトルにする（`compute_phash`）。
- **ダミー生成**: 64bit 符号を `_build_lowfreq_from_bits` で低周波振幅に写像し、`_reinforce_margin` で符号反転を防ぐマージンを強制。高周波は平均 0・分散 12^2 のガウスノイズで埋め、IDCT → 0–255 正規化→元サイズへ Bicubic 拡大（`make_phash_preserving_dummy`）。NumPy の `default_rng` でシード制御。
- **二階層 Shamir**: 大素数 $p = 2^{521}-1$（Mersenne 素数）上で Lagrange 補間（`_lagrange_interpolate`）を行う Shamir を実装し、$n = 5, k_1 = 2, k_2 = 4$ の二層分散（`TwoLevelShamirScheme`）。秘密は p に収まる長さにチャンク分割して多項式係数を乱数生成し、結合時はチャンク長も保持して復元。

可視化は Matplotlib で描画し、精度・時間の集計も同一環境で自動出力している。

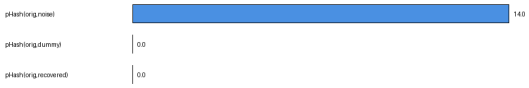

図 4.1　pHash 距離（ダミー、原本、$< k_1$）

図 4.2　PSNR の分布（ダミーと原本）

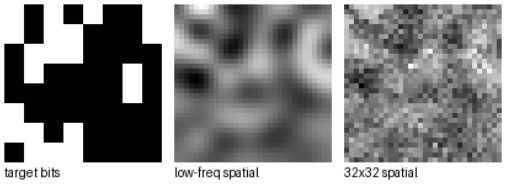

図 4.3　ダミー生成トップ 3（pHash 符号→低周波のみの空間像→ 32×32 空間）

第 5 章

実験

5.1 設定

COCO val2017 公式配布からシード 2025 で 500 枚をサンプリングし，20 種の固定パラメータ変換（JPEG 品質劣化，ガンマ・輝度・コントラスト，±30 度回転，リサンプリング，クロップ，ノイズ，透かし等）を適用して派生セット `coco2017_derivatives` を作成し，パスを `mapping.json` に記録した。各画像について (1) 32×32 グレースケール化と pHash 計算，(2) pHash 符号を保ったまま高周波をノイズ化したダミー生成，(3) 原本・ダミーを n=5, $(k_1, k_2) = (2, 4)$ の二階層 Shamir でシェア化，を行い，平文 pHash（plain）と k1 ダミー pHash（dummy_k1）の検索性能を比較した。検索では bands=8, k=3, n=5, τ=8 を用い，オリジナルのみと全 20 バリアントの 2 条件で評価した。復元評価は最大 50 枚で pHash/PSNR（Peak Signal-to-Noise Ratio）/復元時間を測定し，500 クエリは約 0.5 ms/query で実行可能な規模として設定した。生成されたダミー画像（図 4.3）は視覚的にはノイズだが pHash 符号が元と一致し，k_1 で復元したときの Hamming 距離は 0 となる。一方 k_1 未満のシェア組み合わせでは平均距離 20.8 とランダム同等で，pHash 漏洩は生じない。異なる画像のシェア同士では pHash 距離が離れるため誤マージは起きず，同一画像の原本シェア／ダミーシェアでは符号が一致することを確認した。ここでの評価指標は次の通りである。本稿では同一 ID の派生群を正解集合とし，Recall@k（再現率）を主指標に用いる。Recall@k は「正解全体のうち上位 k 件に何件含まれるか」の割合であり，参考として Precision@k は「上位 k 件のうち正解が何件含まれるか」の割合を表す。ダミー（k_1）の pHash 距離は平均 0、$< k_1$ は平均 20.8、ダミー PSNR は平均 10.76 dB と視覚的な劣化は大きい。PSNR は漏えい量の直接指標ではなく補助指標であり，漏えい評価は分類器の推定精度や復元攻撃の成功率などで測定する必要がある。復元時間は k_1 が平均 121 ms、k_2 が平均 10.2 s で閾値ごとにコストが段階化された（図 4.1, 4.2）。k_2 が重いのは、元画像を大きな秘密長（64KB）で Shamir 復元するため計算量が増えることによる。分布の詳細を図 5.1, 図 5.2, 図 5.3 に示す。

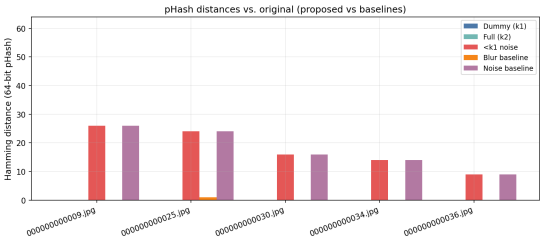

図 5.1　pHash 距離の分布（plain/dummy/$< k_1$）

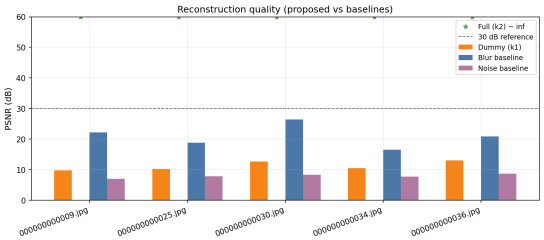

図 5.2　PSNR の分布（ダミーと原本）

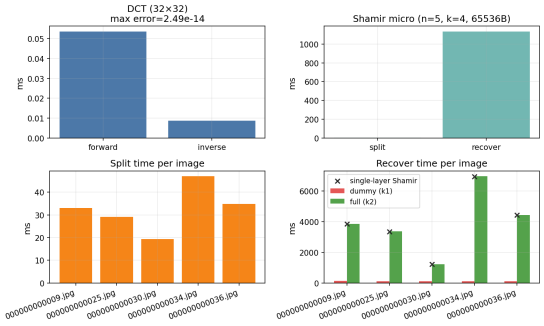

図 5.3　復元時間の分布（k_1/k_2）

5.2　pHash 距離分布と精度維持の理由

dummy_k1 でも精度が落ちないのは、pHash 符号を一致させているため Hamming 距離のランキングが平文と同一になるからである。$< k_1$ は平均距離 20.8 とランダム同等で候補に入らず、k1 以上の候補は平文と同じ順位付けとなる。

5.3　検索再現率と時間（オリジナル）

図 5.4，図 5.5 はオリジナルのみの結果。1 対 1 照合では Top-1 accuracy が 100% で plain/dummy_k1 とも一致し，Recall@10 も 100%（正解 1 件）だった。処理時間も 0.496 ms/query（plain）と 0.493 ms/query（dummy_k1）でほぼ同等だった。

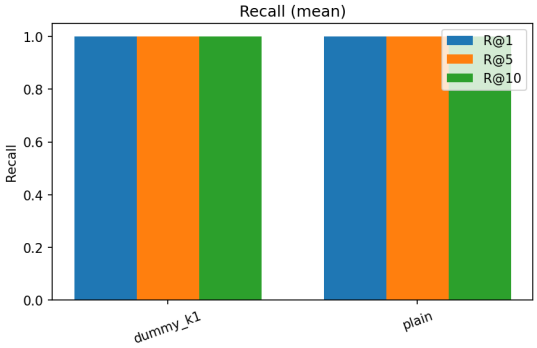

図 5.4　Recall（平均値、オリジナルのみ）

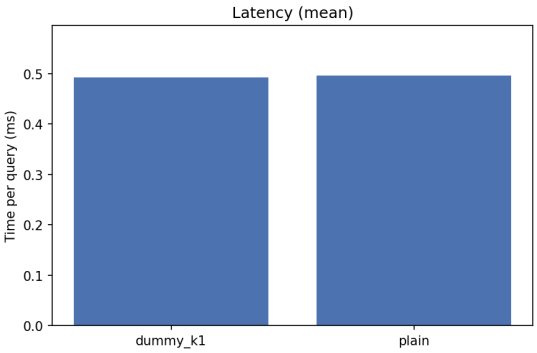

図 5.5　Latency（平均値、オリジナルのみ）

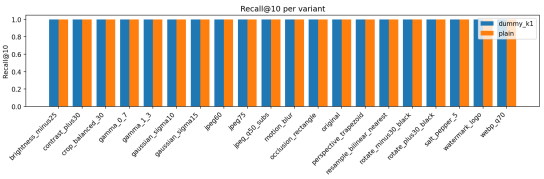

図 5.6　Recall@10（バリアント別、plain vs dummy_k1）

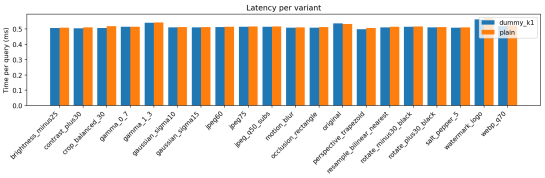

図 5.7　Latency（バリアント別、plain vs dummy_k1）

5.4　バリアント別の再現率と時間

`--per_variant_plots` で全 20 バリアントを自動ループし、平文 vs ダミーの精度と時間を集計した。全バリアントの平均で同一 ID の派生群を正解集合とした Recall@10=42.41%、Recall@5=21.65% と平文／ダミーが一致し、処理時間も 0.527 ms/query（plain）と 0.494 ms/query（dummy_k1）で差が小さい（図 5.6, 5.7）。

表 5.1　評価した 20 バリアントの例（mapping.json）

フォトメトリック系	幾何・ノイズ系
brightness_minus25	rotate_plus30_black
contrast_plus30	rotate_minus30_black
gamma_0_7, gamma_1_3	crop_balanced_30
jpeg60, jpeg75, jpeg_q50_subs	perspective_trapezoid
webp_q70	resample_bilinear_nearest
watermark_logo	gaussian_sigma10,15
	salt_pepper_5, motion_blur
	occlusion_rectangle

第 6 章

考察

ダミーは原画像の内容推定に資する視覚情報を開示せずに pHash を一致させ、平文 pHash と同等の検索精度・時間を維持できた。一方で以下の安全性・限界を整理する。

k_2 復元が 10 秒超となる主因は、原画像の秘密長が大きく（PNG バイト列をそのまま分散）、Shamir の補間をチャンク数分だけ繰り返す必要がある点にある。改善策としては、(1) 秘密長を短縮するための画像圧縮／表現削減、(2) 固定の share index に対する Lagrange 係数の事前計算とバッチ化、(3) 大整数演算の最適化（gmpy2 等）や有限体の選択（高速な素数体や GF(2^8) 系）による演算コスト削減、(4) 並列化によるチャンク復元の高速化、が考えられる。これらは段階復元の運用（必要時のみ k_2）と組み合わせることで実用性が向上する。

- PSNR は視覚的劣化の指標に留まり，漏えい量の直接指標ではない。カテゴリ推定・人物/文字の有無・メンバーシップ推定に対する推定精度や優位度で評価する必要がある。
- k_1 未満では pHash も一致せず距離平均 20.8 とランダムノイズ並みで、pHash 漏洩も発生しない。k_1/k_2 で権限分離し、k1 は検索専用、k2 は復元許可の運用が可能。
- アクセスパターンは固定長バッチとダミーで平滑化するが完全には隠せない。VOPRF（Verifiable Oblivious Pseudorandom Function）/TEE（Trusted Execution Environment）の導入や固定サーバ集合での一律送信でさらなる緩和が必要。
- pHash の弱さ（大回転や 30% 超の切り抜きで符号が崩れる）は残る。必要に応じて CNN 特徴や多視点 pHash とのハイブリッド化を検討する。

第 7 章

おわりに

pHash 符号一致ダミーと二階層 Shamir に基づく三段階開示モデルを提案し、SIS 上で原画像の内容推定に資する情報を開示せずに類似検索を実現した。平文と同等の検索性能を保ちつつ、復元コストを閾値で段階化できることを確認した。本研究は「原画像を復元せずに類似検索を可能にする」という従来は両立しなかった要請に対し、pHash の知覚特性と SIS の暗号特性を統合することで実装可能な解法を提示した点に意義がある。今後は (1) 10 万件規模へのスケールと索引・通信コストの評価、(2) pHash と CNN 特徴のハイブリッド化や頑健な知覚ハッシュとの接続、(3) クエリごとの最適 τ を動的に調整する閾値制御、(4) アクセスパターン秘匿のさらなる強化（VOPRF/TEE）を進める。

参考文献

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

[2] C. Zhang, Y. Li, and Q. Liu, “SS-CNN: Secret sharing based secure image retrieval,” *Journal of Visual Communication and Image Representation*, 2024.

[3] M. Barni, P. Failla, R. Lazzeretti, et al., “A privacy-preserving framework for JPEG-based image retrieval,” *IEEE Transactions on Information Forensics and Security*, 2010.

[4] J. R. Troncoso-Pastoriza, S. Katzenbeisser, and M. Celik, “Privacy-preserving approximate search for multimedia,” *IEEE Transactions on Circuits and Systems for Video Technology*, 2017.

[5] Y. Tian, X. Wang, and D. He, “Secure image retrieval based on feature index tree searchable encryption,” *Information Sciences*, 2024.

[6] Z. Xia, Y. Zhu, X. Sun, and Q. Wang, “Searchable image encryption for privacy-preserving CBIR,” *IEEE Access*, 2021.

[7] R. Venkatesan, S.-M. Koon, M. Jakubowski, and P. Moulin, “Robust image hashing,” in *Proc. IEEE ICIP*, 2000.