2025 年度 卒業論文

秘密画像共有における pHash でのシェア収集を可能にする知覚暗号化の設計

指導教員：清水 恒輔

提出日：2026 年 2 月 6 日

玉城洵弥

工学部 電気電子・情報工学科 情報コース

1213033903

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．そこでまず，プライバシー保護の観点から秘密画像共有（Secret Image Sharing; SIS）が必要となる．検索には特徴量の露出が不可欠であり，復元／非復元の二択では不十分である．そこで「検索のみ許可／閲覧は禁止」という中間状態を設ける段階開示が必要となる．次に，シェアのまま類似検索を行うためには軽量でロバストで，Hamming 距離で高速検索できる特徴量である pHash を用いるのが適している．しかし，シェア画像は暗号化・分散されているため，通常の pHash 検索では精度が低下する恐れがある．そこで本研究では，pHash の検索精度を落とさずに SIS 上で検索を可能にする知覚暗号化方式を設計する．本方式では，収集したシェア数に応じて検索専用の出力から復元許可へ段階的に切り替える．具体的には，収集したシェア数 r が k_1 に達すると検索のみを許可し，k_2 に達すると復元を許可する（$k_1 < k_2$，r は収集したシェア数，k_1, k_2 は必要なシェア数）．k_1 では検索に必要な低周波符号が一致する pHash 整合ダミー（低周波符号のみ一致させ高周波をノイズ化した画像）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．COCO 派生データ（最大 500 クエリ）で評価した結果，オリジナル画像では Precision@1=100%，Precision@5=20%，Precision@10=10% で平文とダミーが一致し，全 20 バリアントでも Precision@1=100%，Precision@5=86.6%，Precision@10=84.82% で一致した．処理時間も 0.58/0.55 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）と同等，復元時間は k_1 到達時に 121 ms，k_2 到達時に 10.2 s となり，段階化できた．

1　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サーバに保持するため，検索のために中身をさらしてしまう．このため，画像内容を開示せずに検索を実現できるプライバシー保護技術が必要となる．本研究ではその手段として，暗号化により画像を分散保持できる秘密画像共有（Secret Image Sharing; SIS）を採用し，検索の特徴量には軽量な知覚ハッシュ（perceptual hash; pHash）を用いる．pHash は低次元でロバストかつ Hamming 距離で高速比較できるため，暗号化・分散環境でも検索コストを抑えやすい．

1.2　目的

本研究で扱う 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．pHash は低次元でロバストかつ Hamming 距離で高速比較できるため，暗号化・分散環境でも検索コストを抑えやすい．

以下，n を総シェア数，r を収集したシェア数，k_1, k_2 を検索許可・復元許可に必要なシェア数（閾値）とする．また，二階層 Shamir 秘密分散は （秘密を複数のシェアに分割し，所定数が揃うと復元できる Shamir 秘密分散を二段化したもの）所定の閾値で「k_1 は検索専用」「k_2 で原本復元」を分離する多段しきい値版 Shamir である．実験では n=5 を前提とし，検索の収集負担を抑えつつ復元には大半のシェアを要するよう k_1=2, k_2=4 とした．本研究で用いる 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る．この性質により，$r < k_1$ ではノイズのみ，$k_1 \le r < k_2$ では pHash 符号一致ダミー，$r \ge k_2$ で原画像を復元する三段階開示が可能になる．

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．このジレンマを避けるため，検索のみ許可する中間状態を用いた段階開示が必要となる．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，k_1 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．

1.3　貢献

本研究の貢献は次の三点に整理できる．第一に，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た．これにより，「pHash のみ開示／視覚情報非開示」を閾値で保証した．第二に，pHash 整合ダミーを平文 pHash と同じ API で検索できるようにし，k_1 でダミー（pHash のみ開示），k_2 で原本復元という段階開示を masked SIS パイプラインに実装した．第三に，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，オリジナルでは Precision@1=100%，Precision@5=20%，Precision@10=10%，全バリアントでも Precision@1=100%，

Precision@5=86.6%，Precision@10=84.82% と一致することを示した．さらに，処理時間も平文/ダミーで 0.58/0.55 ms（オリジナル），0.53/0.49 ms（全バリアント）と同等であり，復元コストが k_1=121 ms, k_2=10.2 s で段階化されることを実測した．

2　関連研究

本研究は，SIS 上で pHash 検索を可能にする知覚暗号化方式の設計を目的とする．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（Multi-Party Computation; 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 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限定的であり，軽量性を活かした実用的な設計は十分に整理されていない．

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（本研究の 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著者の調査範囲では限定的である．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については，著者の調査範囲では十分に整理されていない．

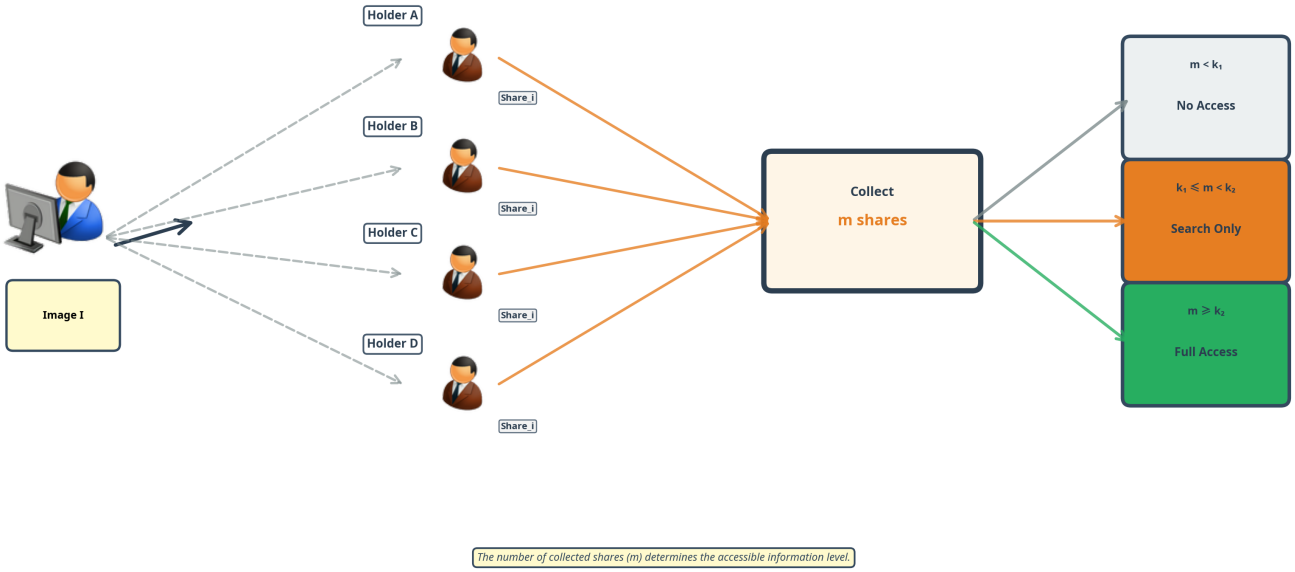

図 1: 三段階 SIS の概念図（k_1: 検索のみ，k_2: 完全復元）

3　提案手法

3.1　動機付け

第 2 章の関連研究を踏まえると，本研究は以下の点に特徴がある。(1) pHash の低周波符号構造のみに基づき、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。著者の調査範囲では，「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限定的であり，軽量知覚特徴と暗号技術を統合する方向性に本研究の特徴がある．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) 既存研究は高次元特徴を保ちながら距離計算を安全計算化する重い路線であり，段階開示を前提としていない．(b) 本研究は pHash に制約し，k_1 で検索のみ，k_2 で原本復元という役割分担で計算量を段階化する．

3.2　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，同じインデックスで低閾値用の秘密と高閾値用の秘密をそれぞれ Shamir 分散し，k_1 でダミー，k_2 で原画像を復元する多段しきい値構成である。以降の実験では n=5, $(k_1, k_2) = (2, 4)$ とする．言葉で言えば，収集シェア数 r が k_1 未満ならノイズのみ，$k_1 \le r < k_2$ なら pHash 整合ダミー，$r \ge k_2$ で原画像を復元する。この開示規則を次式で表す:

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

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

3.3　三段階開示

シェア数 r に応じて、$r < k_1$ はノイズ、$k_1 \le r < k_2$ は pHash 符号一致ダミー、$r \ge k_2$ 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。

図 2: pHash 距離の分布（原画像平文／ k_1 ダミー／ $r < k_1$ ノイズ）

3.4 pHash 整合ダミー

ダミー生成の流れを図 4 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。

3.5 理論的な安全性と復元不可性

低周波符号だけを拘束し高周波を完全ノイズ化することで、pHash は一致するが視覚情報は PSNR 10 dB 程度に落ち、画像内容の逆推定は本研究の評価範囲では困難と考えられる。k_1 未満ではそもそも符号も一致せず平均距離 20.8 とランダムノイズ並みで、pHash 漏洩も発生しない。

3.6 検索パイプライン

本研究では masked SIS に特化し、平文 pHash と同一 API で (a) k_1 で pHash 整合ダミー検索、(b) k_2 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。

4 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。

- **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 $p = 2^{521} - 1$ 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。

原画像（平文）と，SIS でシェア化して得られる k_1 ダミーおよび $r < k_1$ のノイズの pHash 距離を比較する（図 2）。

図 3: PSNR の分布（ダミーと原本）

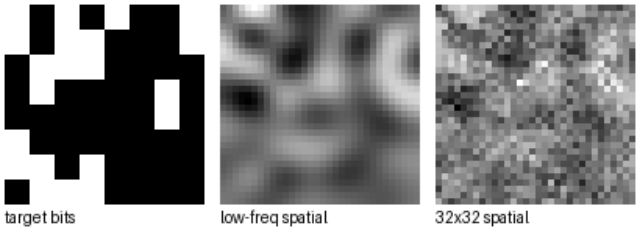

図 4: ダミー生成トップ 3（pHash 符号→強調低周波→ 32×32 空間）

5 実験

5.1 条件・手順

評価指標は Precision@k と Recall@k を用いる。オリジナル評価では各クエリの正解は同一原画像 1 件とし，バリアント評価では同一元画像から生成された派生画像群を正解集合とする。Precision@k は上位 k 件中の正解割合，Recall@k は正解集合のうち上位 k 件で回収できた割合である．

条件：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．変換は original を含め 20 種であり，具体的には JPEG（q75, q60, q50+サブサンプリング），WebP（q70），回転± 30° （黒埋め），30%クロップ，台形射影，リサンプリング（双線形→最近傍），ガンマ 0.7/1.3，明るさ -25，コントラスト +30，ガウシアンノイズ σ=10/15，ソルト&ペッパー 5%，モーションブラー，透かしロゴ，矩形遮蔽である．検索は 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/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．

手順：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 でシェア化した．平文 pHash（plain）と k_1 ダミー pHash（dummy_k1）の検索性能を比較し，復元時間と見えの指標を記録した．

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。$r < k_1$ は平均距離 20.8 で、無関係画像ペアの距離平均（約 20.8）と同程度（以下「ランダム同等」）のため候補に入らず、k_1 以上の候補は平文と同じ順位付けとなる。

5.3 検索精度と時間（オリジナル）

図 5, 図 6 はオリジナルのみの結果。Precision@1=100%, Precision@5=20%, Precision@10=10%となり、再現率@10 も 100% で plain/dummy_k1 とも同一、処理時間も 0.581 ms/query（plain）と 0.548 ms/query（dummy_k1）でほぼ同等だった。

5.4 バリアント別の精度と時間

`--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 Precision@1=100%，Precision@5=86.6%，Precision@10=84.82%となり、再現率@10 は 42.41% と平文／ダミーが一致し、処

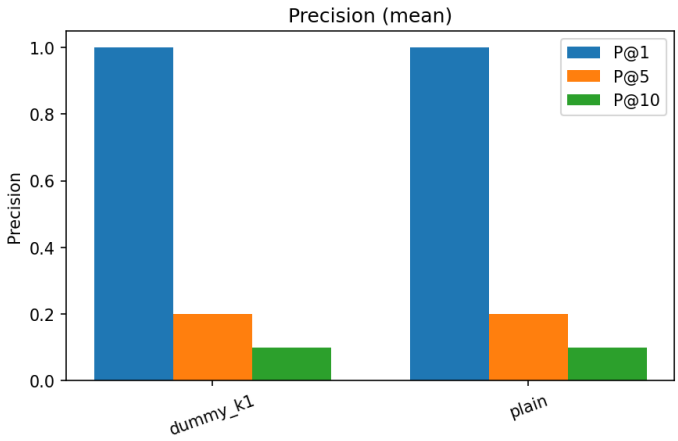

図 5: Precision（平均値、オリジナルのみ）

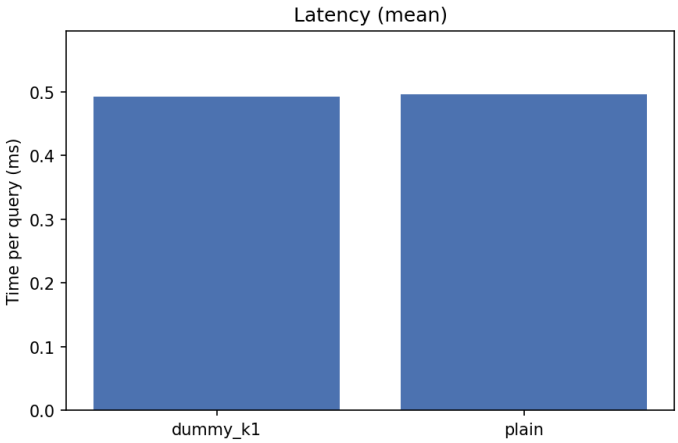

図 6: Latency（平均値、オリジナルのみ）

理時間も 0.527 ms/query（plain）と 0.494 ms/query（dummy_k1）で差が小さい（図 7, 8）。

6　考察

ダミーは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。

1. **視覚情報の漏えい**: pHash 整合ダミーは高周波をノイズ化するため PSNR は 10 dB 台まで低下し，視覚情報は大きく失われる．したがって内容の逆推定は本研究の評価範囲では困難と考えられる．

2. **pHash 距離の基準**: k_1 未満では pHash も一致せず距離平均 20.8 となり，無関係画像ペアの距離平均（約 20.8）と同程度である．ここで「ランダム同等」とはこの基準と同程度であることを指す．k_1/k_2 で権限分離し，検索と復元を分けて運用できる．

3. **アクセスパターン**: 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/TEE の導入や固定サーバ集合での一律送信が追加で必要である．

4. **pHash の弱さ**: 大回転や 30% 超の切り抜きで符号が崩れる弱点は残る．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．

7　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 上で平文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「画像を見せずに画像を検

表 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,	perspective_trapezoid
jpeg_q50_subs	
webp_q70	resample_bilinear_nearest
watermark_logo	gaussian_sigma10,15
	salt_pepper_5, motion_blur
	occlusion_rectangle

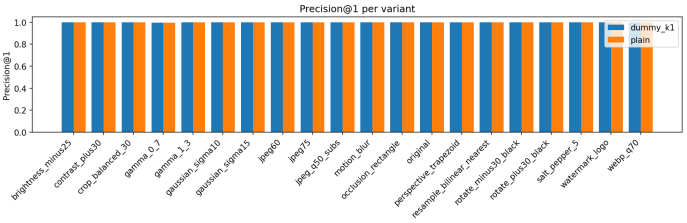

図 7: Precision@1（バリアント別、plain vs dummy_k1）

索する」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性を示した点に意義がある。今後は (1) 現在の処理時間（約 0.5 ms/query）と一般的な画像検索規模を踏まえ，まず 10 万件程度を現実的な初期ターゲットとしたスケールと索引・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。優先度としては，秘匿性への影響が大きいアクセスパターン秘匿を最優先とし，次に特徴量の頑健化，その後にスケール評価と閾値最適化を進める。

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.

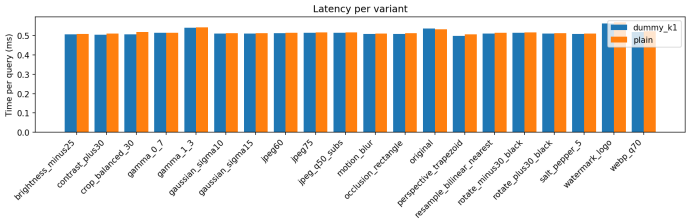

図 8: Latency（バリアント別、plain vs dummy_k1）