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

氏名：玉城洵弥
学生番号：1213033903
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

2026 年 2 月 6 日

# 目次

# 図目次

# 表目次

# 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）には，運用者・侵入者・ログ等を経由して画像内容や画像間の類似関係が漏えいし得るため，機微画像を扱う場面ではリスクがある．そこで本研究では，プライバシー保護のために画像を秘密画像共有（Secret Image Sharing; SIS）で分散保持したうえで，原画像を復元（平文化）せずに類似画像検索を実現したい状況を想定する．本研究は，サーバを信頼しない（semi-honest：プロトコルには従うが得られる情報から推測を試みる）脅威モデルを想定する．例えば，医療・監視・個人写真などの機微画像を複数主体（複数サーバ／複数保持者）に分散保管しつつ，必要時に類似画像の検索だけを許可したいといったユースケースである．このときシェアは暗号化画像のようにランダムに見えるため，平文画像に対する CBIR をそのまま適用できない．

しかし，類似検索には比較に用いる情報の露出が不可欠であり，復元／非復元の二択では運用上不十分である．そこで本研究では「検索のみ許可／閲覧は禁止」という中間状態を設け，収集したシェア数に応じて権限を段階的に切り替える方式を提案する．

シェアのまま高速に類似性判定を行うために，知覚ハッシュの一種である pHash を用いる．pHash は画像を低次元のビット列に写像し，Hamming 距離（XOR とビットカウント）で高速比較できるため，大規模データベースに対しても検索コストと保存コストを小さくできる．一方で，SIS のシェアは暗号化画像のようにランダムに見えるため，シェア画像そのものに pHash を適用しても元画像の類似性は保持されない．そこで本研究では，pHash が主に低周波構造に依存する点に着目し，閲覧に資する高周波成分は劣化させつつ pHash に必要な低周波符号を一致させることで，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．具体的には，本研究は SIS における多層（multi-level）／多閾値（multi-threshold）アクセス構造に基づき，収集したシェア数 $r$ に応じて開示する情報（出力）を段階的に切り替える．多閾値 SIS では，複数の閾値をもつアクセス構造をあらかじめ定義し，満たされた閾値に応じて復元可能性や得られる情報を制御する [**?**, **?**]．本研究ではその最小構成として 2 段の閾値を設定し，$r$ が第 1 閾値 $k_1$ に達すると検索のみを許可し，$r$ が第 2 閾値 $k_2$ に達すると原画像の復元を許可する（$k_1 < k_2$）．なお，これはシェア数の増加に伴い復元画像が徐々に鮮明化する progressive VSS の「画質が連続的に向上する」設計とは異なり，本研究では「検索専用の出力」と「復元可能な出力」を閾値で離散的に分離する点に特徴がある [**?**].

$k_1$ 到達時には，検索に必要な低周波符号が平文 pHash と一致するように合成したダミー画像（pHash 整合ダミー）を返す．このダミーは，高周波成分をノイズ化して輪郭・文字・顔などの可読性を低下させ，内容推定に資する手掛かりを弱める一方で，検索に必要な低周波符号は保持する．また，異画像との衝突（偽一致）を抑えるため，Hamming 距離の閾値判定も併用し，偽一致については評価により確認する（詳細は実験章）．

COCO 派生データ（最大 500 クエリ）で評価した結果，元画像では Precision@1=100% となり，平文 pHash と同等の検索結果を維持した．また，回転・切り抜き等の 20 種類の変換画像を含む条件でも Precision@1=100%，Precision@5=86.6%，Precision@10=84.82% であり，平文との差は小さかった．処理時間も約 0.5ms/件と平文と同等であり，復元時間は $k_1$ 到達時に 121ms，$k_2$ 到達時に 10.2s となり，段階化できた．

# 第 1 章

# はじめに

## 1.1 背景

医療画像や監視映像，個人写真などの機微画像では，画像内容を開示せずに類似事例を検索し，診断・治療方針の検討や臨床教育，研究用途に活用したいという要求がある．実際，医療分野では Content-Based Medical Image Retrieval（CBMIR/CBIR）が，症例参照型の意思決定支援や教育支援のための基盤技術として位置づけられてきた [?, ?, ?]．しかし，これらの画像は患者情報や個人情報と強く結びつくことが多く，「検索できる」こと自体が情報露出の入口になるため，利便性とプライバシーの両立が課題となる．

従来のコンテンツベース画像検索（Content-Based Image Retrieval; CBIR）は，検索精度と運用容易性を優先し，画像特徴量（埋め込みやハッシュ等）をサーバ側で保持・照合する構成が一般的である．ところがサーバを信頼しない（semi-honest / honest-but-curious）状況では，サーバが保持する特徴量，照合の中間結果，アクセスパターンやログ等が攻撃面となり得る．特徴量が漏えいした場合，画像内容・属性の推測（機微カテゴリの推定）や，検索結果（近傍関係・ヒットの有無）を介したメタデータ漏えいが生じ得るため，honest-but-curious なクラウド（CSP）を想定したプライバシー保護 CBIR が研究されてきた [?, ?]．

本研究では，さらに踏み込んで「サーバに平文画像を置かない」だけでなく，画像そのものを秘密画像共有（Secret Image Sharing; SIS）により分散保持した画像集合を検索対象とする状況を扱う．SIS は画像を $n$ 個のシェアへ分割し，所定数（閾値）以上のシェアが揃った場合にのみ復元でき，閾値未満では原画像に関する意味情報が得られないよう設計される（閾値型 SIS）．脅威モデルとしては，サーバ（および一部の保持者）はプロトコルには従うが，保持データや観測可能な計算結果から推測を試みる semi-honest を想定し [?]，複数主体が結託して観測情報を統合する可能性も考慮する．このとき，閾値未満のシェア集合からは原画像を復元できないことを安全性の前提とする．

しかし，ここで新たな問題が生じる．一般的な SIS では各シェアが単独では意味情報を与えないよう

生成されるため，平文画像を前提とする CBIR（特徴抽出・比較）をシェアに直接適用しても，原画像間の類似関係を反映した比較結果は得られない．したがって素朴には，検索の都度，(i) 閾値以上のシェアを収集して復元（平文化）し，その後に特徴抽出・類似度計算を行う手順が必要となる．ところがこの復元ベース手順は，計算・通信の追加コストを伴うだけでなく，復元許可（閲覧権限）と閾値を満たすシェア収集を前提とするため運用上の制約が大きい．すなわち，「閲覧は許可しないが検索のみ行いたい」という要求を，復元を前提とする設計だけで満たすことは難しい．このため，秘密分散による保護状態を維持したまま，検索に必要な情報のみを制御して利用可能とする検索方式が必要となる．

本研究では，検索の特徴量として知覚ハッシュ（perceptual hash; pHash）を採用する．pHash は画像を小サイズに正規化した後に DCT を適用し，低周波成分から 64bit の指紋を生成することで，軽量なビット列比較（Hamming 距離：XOR とビットカウント）で高速に近似類似検索を行える [**?**]．このような（低次元・ビット演算中心の）比較は，大規模データベースに対しても計算資源と保存容量を抑えやすく，本研究が想定する「サーバを信頼しない」環境下での実装・運用上の利点が大きい．一方で，知覚ハッシュは照合結果がブラックボックス・オラクルとして悪用され得ることや，実運用の PHAs（PhotoDNA/PDQ/NeuralHash 等）に対する攻撃評価も報告されている [**?**, **?**]．したがって，検索機能を提供する場合でも，どの情報をどの段階で開示するかは慎重に設計しなければならない．

以上より，本研究の課題は，SIS により保護された画像集合に対し，(1) 秘密分散による保護状態を維持しつつ，(2) 検索に必要な情報のみを段階的に制御して開示し，(3) pHash に基づく高速な類似検索を成立させる方式を設計することである．

## 1.2 目的

本研究が対象とするのは，SIS で分散保持された機微画像集合に対し，原画像を復元（平文化）せずに類似検索を成立させたい状況である．類似検索を行う以上，何らかの検索用表現（特徴量，指紋，ハッシュ等）を比較に用いることは避けられない．しかし，検索用表現をそのまま外部に露出させて照合を行う設計は，サーバを信頼しない（semi-honest）環境では，照合結果（ヒットの有無，距離，順位）が反復問い合わせ可能な**判定器**として機能し，探索・推測の手掛かり（オラクル）となり得る点で望ましくない．特に知覚ハッシュは暗号学的ハッシュのような一方向性を目的としておらず，**類似性を保存する指紋**として設計されているため，照合可否や距離情報の露出それ自体が情報露出の窓口になり得る [**?**]．

一方で，SIS の素朴な運用として「検索のたびに閾値以上のシェアを収集して復元し，平文画像に対して CBIR を実行する」手順を採ると，復元処理に計算・通信コストが発生するだけでなく，復元許可（閲覧権限）や所定数のシェア収集が前提となるため，「閲覧は許可しないが検索だけ行いたい」という要求と整合しない．すなわち，**復元ベースの手順だけでは運用要求を満たしにくい**一方で，**検索用表現を無条件に露出させる設計も安全ではない**という緊張関係が生じる．

そこで本研究は，検索可能性と閲覧可能性を同一視せず，開示レベルを三段階に分離して制御する

方式を確立することを目的とする．総シェア数を $n$，収集したシェア数を $r$ とし，二つの閾値 $k_1, k_2$（$k_1 < k_2$）を設ける．本研究が定義する開示レベルは次の三段階である．

1. **Level 0（$r < k_1$）**：通常の SIS シェアのみが得られている段階であり，検索に用いる情報は開示しない．
2. **Level 1（$k_1 \leq r < k_2$）**：検索のみを許可する段階であり，検索に必要な情報だけを含む検索専用出力を開示する．
3. **Level 2（$r \geq k_2$）**：原画像の復元を許可する段階である．

Level 1 では，pHash 計算で参照される低周波成分に対応する符号が平文 pHash と一致するように合成したダミー画像（pHash 整合ダミー）を出力する．pHash 整合ダミーは検索のための一致（pHash の一致）を満たす一方で，輪郭・文字・顔など内容推定に資する視覚情報は高周波成分のマスク／ノイズ化により意図的に劣化させ，閲覧可能性（内容の可読性）を抑制する．すなわち本研究の Level 1 は，「検索の成立」と「閲覧の抑止」を同時に満たすために導入される中間段階である．

このように，閾値に応じて開示する情報の**種類**を切り替える点は，多層（multi-level）／多閾値（multi-threshold）アクセス構造に基づく段階開示として位置づけられる [**?**]．これに対し，シェア数の増加に伴い復元画像の画質が段階的に向上すること自体を主眼とする progressive 型（PVC/Progressive VSS）とは狙いが異なり [**?**,**?**]，本研究は「検索専用出力」と「復元可能出力」を離散的に分離し，検索可能性と閲覧可能性を分けて制御する点に特徴がある．

## 1.3 貢献

本研究の貢献は次の三点である．

1. **段階開示モデルの定義**：SIS で分散保持された機微画像集合に対する類似検索において，復元閾値とは独立に検索許可を扱うという観点から，三段階（Level 0/1/2）の開示レベルと二つの閾値（$k_1, k_2$）を導入し，「検索に必要な情報」と「閲覧（内容推定）に資する情報」を分離して制御する枠組みを提示した．これにより，復元ベース運用では満たしにくい「検索のみ許可」という要求を，アクセス構造として明示的に扱えるようにした．
2. **pHash 整合ダミーと切替処理系の設計・実装**：Level 1 の検索専用出力として pHash 整合ダミーを設計し，既存の pHash 検索（64bit 指紋生成と Hamming 距離比較）と同一の入出力形式で扱えるようにした．これにより，検索時に原画像の復元（平文化）を行わずとも，$r$ に応じて（Level 0：非開示／ Level 1：検索／ Level 2：復元）を切り替える検索パイプラインを実装可能とした．さらに，低周波符号の一致を満たしつつ高周波成分を制御するという設計により，「検索の成立」と「閲覧の抑止」を両立させるための具体的な設計指針を与えた．

3. **実験による有効性の検証**：COCO 派生データを用いて，平文画像と pHash 整合ダミーの検索結果（Precision@k）および処理時間を比較し，検索精度と処理コストの観点から提案方式の有効性を実験的に示した．あわせて，閾値設定や距離判定が検索結果へ与える影響を整理し，段階開示を導入した際の挙動を定量的に評価した．

# 第 2 章

# 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．ただし，既存の SE ベース CBIR は暗号処理が重く，pHash の軽量性や段階開示（$k_1/k_2$）を前提としていないため，本研究の要件（検索のみ許可／閲覧抑止）には適合しない．

## 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「pHash 符号を保ったまま視覚情報を失わせる変換」や「段階開示／秘密分散と pHash 検索の統合」については，著者の調査範囲では体系的整理が少ない．

# 第 3 章

# 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 $C_{\mathrm{LF}}$ 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。本研究では秘密を 2 種類に分ける。低閾値側の秘密を $s_L := b$（pHash の 64bit 符号）、高閾値側の秘密を $s_H := I$（原画像データ）とする。各シェア番号 $i$ について、$s_L$ を閾値 $k_1$ の Shamir 秘密分散で、$s_H$ を閾値 $k_2$ の Shamir 秘密分散で、それぞれ同一の有限体 $\mathbb{F}_p$ 上で分散し、配布するシェアを $\mathrm{share}_i = (i, \mathrm{share}_i^L, \mathrm{share}_i^H)$ としてまとめる。したがって $r < k_1$ では $s_L, s_H$ のいずれも復元できず、$k_1 \le r < k_2$ では $s_L$ のみ復元できる一方で $s_H$ は情報理論的に秘匿される。$r \ge k_2$ で初めて $s_H$ が復元される。以降の実験では $n$=5, $(k_1, k_2) = (2, 4)$ とする．言葉

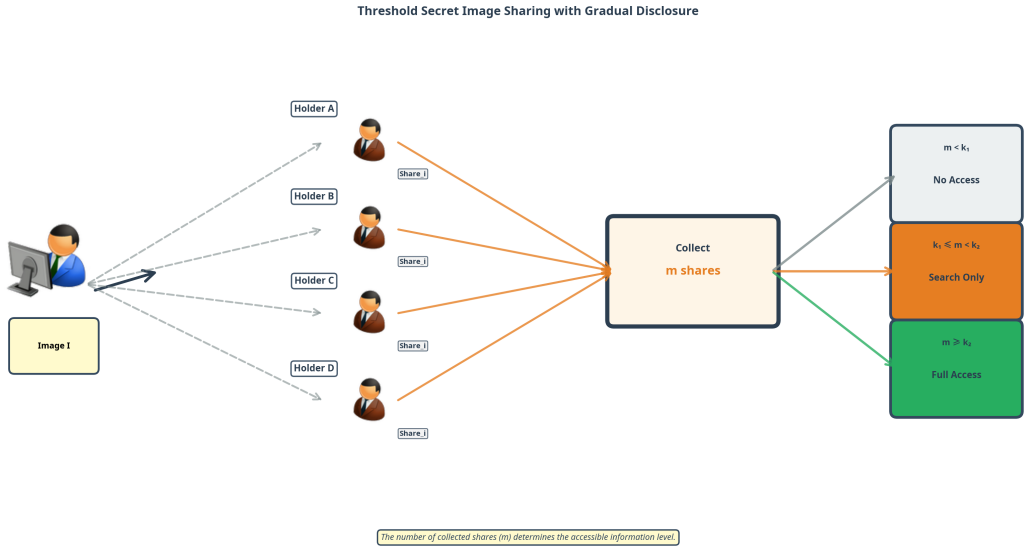


図 3.1　三段階 SIS の概念図（$k_1$: 検索のみ，$k_2$: 完全復元）

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:

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

ここで $\text{dummy}(b)$ 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。

## 3.4　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。

## 3.5 安全性の保証範囲と評価（Shamir の保証／ダミーの可視性）

Shamir 秘密分散は閾値未満のシェアから秘密に関する情報を与えない（情報理論的安全性）。したがって本研究では，$r < k_1$ では $s_L$（pHash 符号）と $s_H$（原画像）の双方が復元不能であること、また $k_1 \leq r < k_2$ では $s_H$ が復元不能であることは Shamir の性質として保証される。一方で $k_1$ 到達時に $s_L = b$ を開示するため、低周波符号情報の漏えいが“ゼロ”であることは保証しない。以下では、開示される情報が画像内容の視認につながりにくいことを実験的指標（PSNR 等）で評価する。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、$r < k_1$ では Shamir の性質により $b$ に関する情報は得られず、設計上も秘密と独立なノイズのみを出力する。

## 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。

# 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．外部依存はこの 2 つに限定し，SciPy ／ OpenCV や暗号・秘密分散の専用ライブラリには依存しない（環境構築の容易さと再現性を優先するため）．DCT/IDCT および Shamir 秘密分散は自前実装で補完した．

- **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 4.1）。


図 4.1　pHash 距離の分布（原画像平文／ $k_1$ ダミー／ $r < k_1$ ノイズ）


図 4.2　PSNR の分布（ダミーと原本）

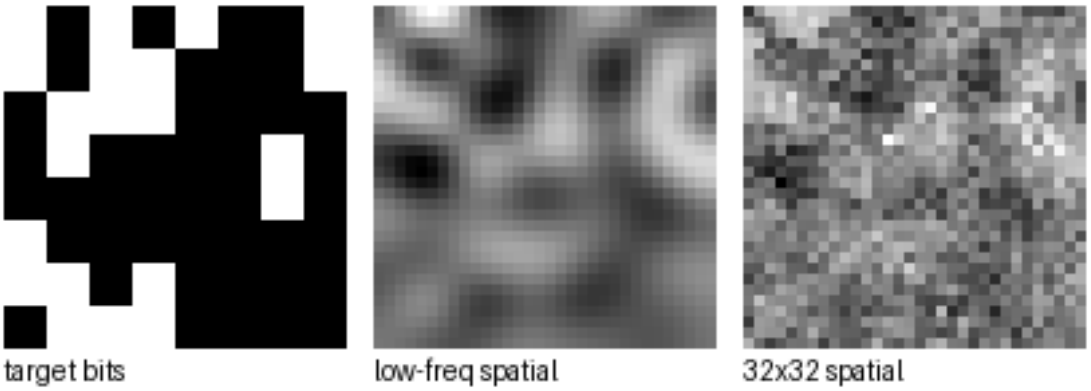


図 4.3　ダミー生成トップ 3（pHash 符号→強調低周波→ 32×32 空間）

# 第 5 章

# 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 $\sigma$=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, $\tau$=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）

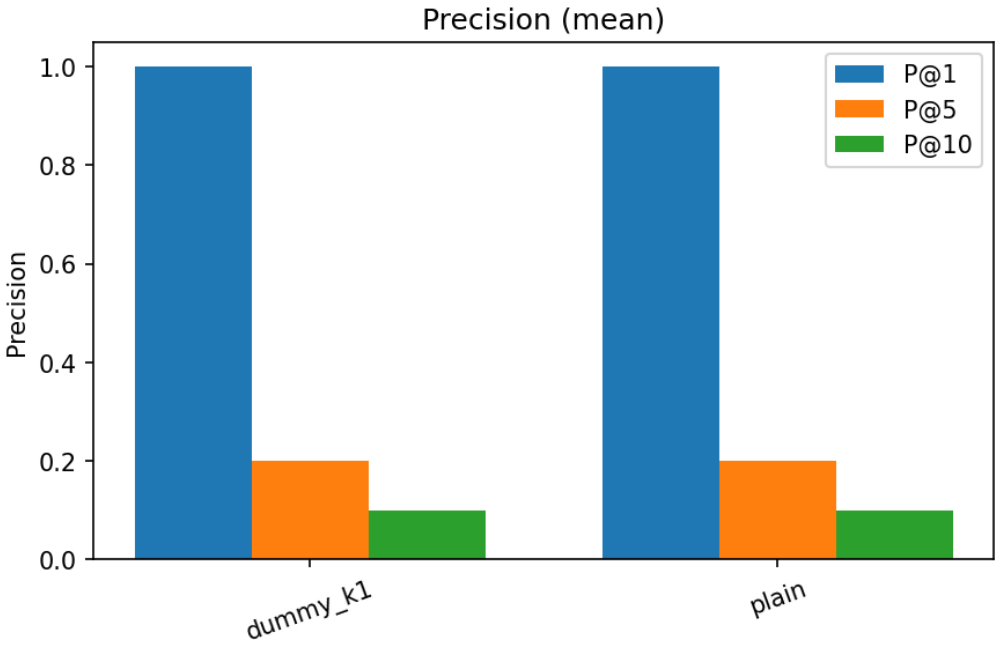


図 5.1　Precision（平均値、オリジナルのみ）

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 5.1，図 5.2 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、処理時間も 0.527 ms/query（plain）と 0.494 ms/query（dummy_k1）で差が小さい（図 5.3, 5.4）。

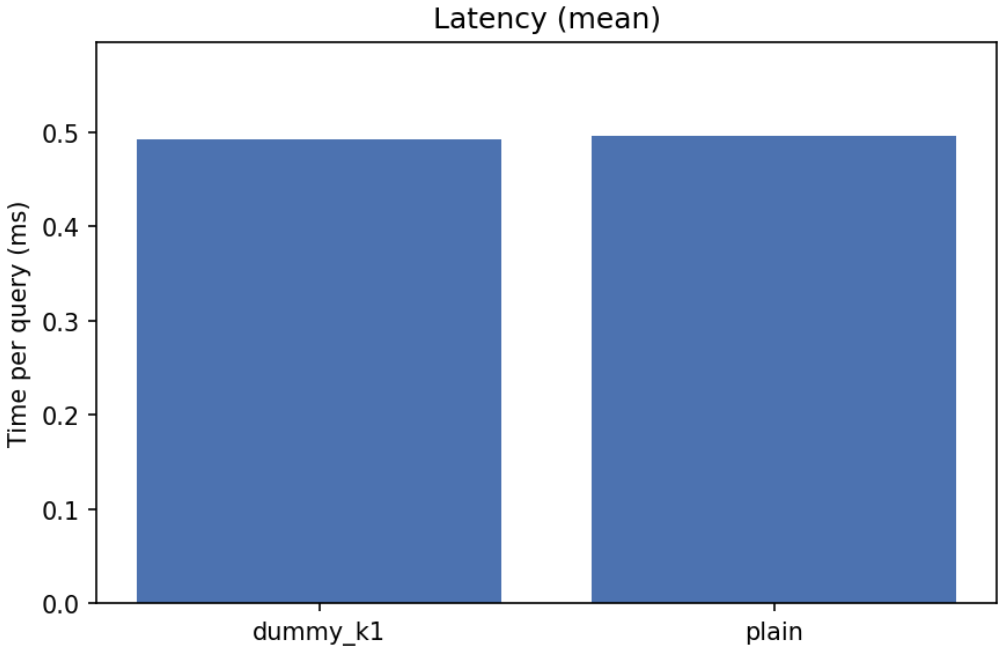


図 5.2　Latency（平均値、オリジナルのみ）

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

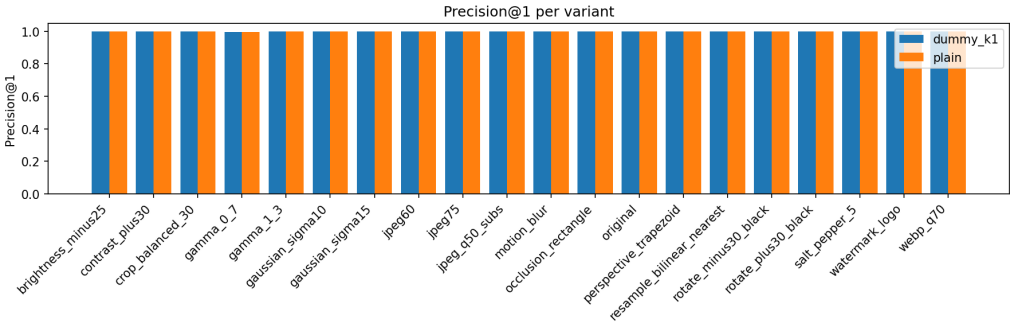


図 5.3　Precision@1（バリアント別、plain vs dummy_k1）

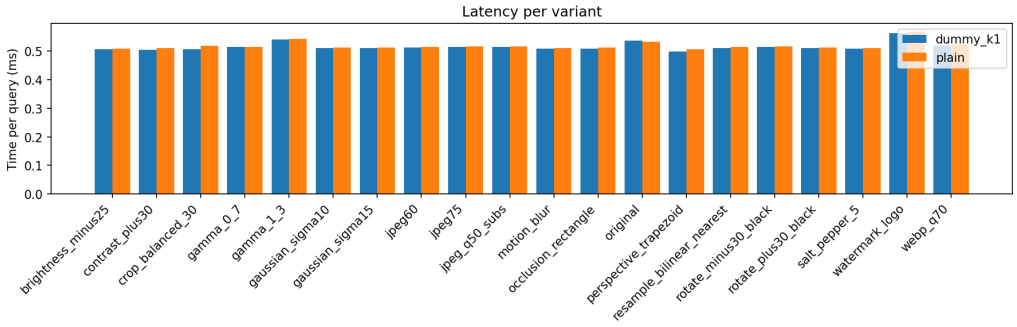


図 5.4　Latency（バリアント別、plain vs dummy_k1）

# 第 6 章

# 考察

ダミーは、pHash を一致させつつも人が内容を視認・推測できる情報を大きく低減した状態で検索を可能にし、平文 pHash と同等の検索精度・時間を維持できた。なお $k_1$ 到達時には pHash 符号 $b$ を開示するため、低周波の符号情報が漏えいしうる点は前提として残る。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．ただし、開示されるのは低周波符号 $b$ に限定され、原画像データ $I$ の復元は $k_2$ 未満では保証されない.
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.

# 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 $\tau$ 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.