

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

第 1 章	はじめに	8
1.1	背景	8
1.2	目的	9
1.3	貢献	10
第 2 章	関連研究	12
2.1	類似画像検索に用いられる特徴量：深層特徴と知覚ハッシュ	12
2.2	秘密分散・MPC を用いたプライバシー保護検索	13
2.3	段階開示・多層 SIS に関する研究	13
2.4	段階開示・多層 SIS に関する研究	14
2.5	検索可能暗号 (SE) によるプライバシー保護検索	14
2.6	知覚ハッシュ (pHash) に関する研究	14
2.7	Shamir 秘密分散の基礎	15
第 3 章	提案手法	17
3.1	動機付け	17
3.2	問題設定と記号	18
3.3	Shamir 法の画像への適用 (データ表現)	19
3.4	二段閾値 SIS (検索用秘密と復元用秘密の同時分散)	20
3.5	pHash 整合ダミーの生成	21
3.6	安全性の扱い (Shamir の保証とダミーの評価)	21
3.7	検索パイプライン	22
3.8	実装	22
第 4 章	実験	26
4.1	条件・手順	26
4.2	実験条件・手順	26

4.3	結果・考察	28
第 5 章	おわりに	32
	参考文献	33

目次

3.1	pHash 距離の分布 (原画像平文 / k_1 ダミー / $r < k_1$ ノイズ)	24
3.2	PSNR の分布 (ダミーと原画像)	24
3.3	ダミー生成の途中出力例 (pHash 符号 \rightarrow 低周波補強 $\rightarrow 32 \times 32$ 空間画像)	25
4.1	三段階出力の可視化例 (複数画像の比較: 原画像 / ノイズ / pHash 整合ダミー 1, 2 / 復元)	27
4.2	Precision (平均値, オリジナル評価; 各クエリの正解は 1 件)	29
4.3	Latency (平均値, オリジナル評価)	30
4.4	Precision@1 (バリエント別, plain vs dummy_k1)	30
4.5	Latency (バリエント別, plain vs dummy_k1)	31

表目次

4.1	評価した 20 バリエントの例 (mapping.json)	30
-----	--------------------------------	----

概要

医療画像に代表される機微情報は、患者のプライバシーに直結するため、保存・伝送において暗号化やアクセス制御を施すことが一般的である。しかし、暗号化が行われていても、単一の保管先や鍵管理主体に依存した運用では、侵害時に被害が一括化し得るという構造的なリスクが残る。この課題に対し近年は、画像を複数のシェアへ分割して分散保持し、所定数 (k -of- n) のシェアが揃った場合にのみ復元を可能とする秘密画像共有 (Secret Image Sharing; SIS) に基づく方式が研究されている。これらは、保管先の分散や合意復元といった運用要件を自然に満たし、単一点の侵害に対する耐性を高める枠組みとして位置づけられる。

一方、従来の類似画像検索 (Content-Based Image Retrieval; CBIR) は、画像特徴量をサーバ側に保持し、平文特徴量間の比較により検索を行う構成が一般的である。しかしこの構成では、運用者による参照や外部侵入に加え、ログ等の副次情報を介して、画像内容に関する情報だけでなく画像間の類似関係 (近傍関係) までもが漏えいし得る。したがって、医療画像のような機微画像を対象とする CBIR においては、「画像を復元可能な状態で一箇所に集約しない」ことと「類似性の評価過程からの漏えいを抑制する」ことを同時に満たす枠組みが求められる。

本研究はこの問題意識に基づき、SIS による分散保持を前提とした環境下で、原画像を復元 (平文化) することなく類似画像検索を実現する手法を検討する。具体的には、分散保持されたシェアから直接得られる情報に基づいて候補を絞り込み、必要最小限の情報開示で類似性を評価することで、検索機能とプライバシー保護の両立を目指す。想定ユースケースは、医療・監視・個人写真などの機微画像を複数サーバに分散保管しつつ、必要時に「類似画像の検索のみ」を許可したい状況である。

しかし、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、原画像に対して用いられる従来の CBIR 手法をそのまま適用できない。一度原画像に復元すれば検索は可能であるが、その都度閾値以上のシェア収集と復元計算を要するため、コストや権限管理の観点で課題が残る。加えて、類似検索には比較のための情報開示が不可欠であるが、復元／非復元かの二択では「検索はさせたいが原画像は見せたくない」という要件を満たすことが困難である。

以上を踏まえ、本研究では「検索のみ許可／閲覧は禁止」という中間状態を導入し、収集したシェア数に応じて可能な処理 (権限) を段階的に切り替える方式を提案する。これにより、機微画像を平文化せずに検索可能性を確保しつつ、不要な情報開示を抑制することを目指す。

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、シェア画像にそのまま pHash を適用しても元画像の類似性は保証されない。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 フレームワーク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、関連技術として、複数のシェアを重ね合わせることで人間の視覚により像を得る Visual Secret Sharing (VSS, visual cryptography) がある。VSS の一部には、 k 枚以上のシェアを重ね合わせたとき、重ねる枚数が増えるほど復元像のコントラストが増し、段階的に見えやすくなる「progressive」な枠組み (progressive VSS) が提案されている。一方、本研究の三段階開示は、復元像の品質が連続的に改善することを目標とせず、第 1 閾値 k_1 と第 2 閾値 k_2 により、出力を「ノイズ / 検索用ダミー / 原画像」に離散的に切り替える点で progressive VSS とは異なる。

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。

COCO 派生データ (最大 500 クエリ) を用いた評価実験の結果、検索性能は Precision@K (検索結果上位 K 件に含まれる正解の割合) と Recall@K (正解集合のうち上位 K 件で回収できた割合) で評価した。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には，画像内容そのものを広く開示することなく，類似事例を検索して診断・治療方針の検討，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，症例参照型の意味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 [1-3]．一方で，こうした画像は患者情報や個人情報と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り得るため，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) をクラウド上のサーバで保持・照合する構成が一般的である．しかし本研究では，サーバ管理者による目的外の閲覧や，外部攻撃者によるデータ窃取のリスクを考慮し，サーバを完全には信頼しない脅威モデルを採用する．具体的には，サーバ (またはサーバへの侵入者) は計算手順 (プロトコル) には従う一方で，保持データや処理結果から画像内容の推測を試みる脅威 (semi-honest / honest-but-curious) を想定する．以下では，このようなサーバ運用主体をクラウドサービス提供者 (Cloud Service Provider; CSP) と呼ぶ．この状況では，(1) サーバが保持する特徴量，(2) 照合の中間結果や順位，(3) アクセスパターンやログといった周辺情報が攻撃面となり得る．これらが漏えいした場合，画像内容・属性の推測や，近傍関係 (どの画像がどれに似ているか) に基づくメタデータ露出が生じ得るため，CSP を含むサーバ側を完全には信頼しない前提でのプライバシー保護 CBIR が研究されてきた [4, 5]．

本研究では，さらに「サーバに原画像を置かない」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 個のシェアに分割し，所定数 (閾値) 以上のシェアが揃った場合にのみ復元できる一方，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 [6], 加えて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, 閾値未満のシェア画像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, SIS を前提にすると検索の実現は自明ではない. 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, 原画像を前提とする 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. したがって素朴な運用としては, 検索の都度, 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「復元してから検索」という手順は, 単に計算・通信コストが増大するだけでなく, セキュリティおよび運用上の大きな課題を抱える. 例えば, 広域監視や医療連携において「該当データが存在するか (ヒットするか)」をスクリーニングしたい段階で, 無関係なデータも含めて全て復元 (閲覧) しなければならない構成は, プライバシー侵害のリスクを不要に拡大させてしまう. また, 常時復元処理を伴う検索は, リアルタイム性が求められる場面では応答速度の致命的なボトルネックとなる. したがって, 「閲覧は許可しないが検索のみ行いたい」という要件を, 復元を前提とする設計のみ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離散コサイン変換 (Discrete Cosine Transform; DCT) を適用し, 低周波成分から 64bit のハッシュ値 (ビット列) を生成することで, 軽量のビット列比較 (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 [7]. 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・運用上の利点大きい. 一方で, 知覚ハッシュは, 攻撃者が生成した任意のクエリとハッシュとの照合結果 (距離や合否) を反復的に取得することで, 逆像を推定する判定器 (オラクル) として悪用され得ること, また実運用で用いられる PhotoDNA/PDQ/NeuralHash 等に対する脅威モデル・攻撃評価が議論されていることが報告されている [8,9]. 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, 本研究の課題は次の 3 点である.

1. SIS により保護された画像集合に対し, 秘密分散による保護状態を維持したまま検索を可能にすること.
2. 検索に必要な情報のみを, 収集シェア数に応じて段階的に制御して開示すること.
3. pHash に基づく高速な類似検索を成立させ, 実装・運用上の負担を抑えること.

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、検索用表現（特徴量やハッシュ値など）を比較に用いること自体は避けられない。しかし、サーバを信頼しない（semi-honest：プロトコルには従うが、観測できた情報から追加推測を試みる）環境では、上記オラクルが検索結果を反射的に、探索・推測し得ることが考えられる、検索用表現を無条件に露出させる設計は望ましくない [7,8]。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てから 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）と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。

これらの要件を同時に満たすため、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。以上を踏まえ、本研究は収集シェア数 r に応じて開示レベルを次の三段階に分離して制御する。

Level 0: $r < k_1$ のとき、検索に資する情報は開示せず、通常の SIS シェアのみを保持する。

Level 1: $k_1 \leq r < k_2$ のとき、検索のみを許可し、検索に必要な情報だけを含む検索専用出力を開示する。

Level 2: $r \geq k_2$ のとき、原画像の復元を許可する。

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」を両立させるために導入される中間段階である。

1.3 貢献

本研究は、秘密画像共有（Secret Image Sharing; SIS）で分散保持された画像集合に対して、原画像の復元（平文化）を前提とせずに類似画像検索を成立させるための設計指針と実装・評価を提示する。本研究の貢献は、次の三つの成果として整理できる。

まず、検索可能性と閲覧可能性を混同せずに制御するための段階開示モデルを提示した。具体的には、シェア収集数 r に応じて開示レベルを切り替える枠組みを定義し、 $r < k_1$ では検索に資する情報を開示せず（Level 0）、 $k_1 \leq r < k_2$ では検索のみを許可する出力（Level 1）を開示し、 $r \geq k_2$ で初めて復元（Level 2）を許可するという二つの閾値 k_1, k_2 に基づくアクセス構造として定式化した。これにより、「検索だけ許可したい」という運用要求を、復元許可（閲覧許可）と切り離して扱えることを明確化

した。

次に、Level 1 の検索専用出力として、pHash 検索に必要な情報のみを保持する pHash 整合ダミーを設計した。本設計は、pHash が参照する低周波成分に対応する符号を一致させる一方で、輪郭・文字・顔など内容推定に資する視覚情報を高周波成分のマスク／ノイズ化により意図的に劣化させることで、照合（検索）の可否と視覚的内容の復元（閲覧）を分離することを狙う。さらに、既存の pHash 計算（64bit ハッシュ値（ビット列）の生成と Hamming 距離比較）と同一の入出力で扱えるように構成し、既存の検索実装へ組み込みやすい形に整理した。

最後に、提案した段階開示方式を SIS 検索パイプラインとして実装し、COCO 派生データを用いて有効性を実験的に示した。原画像と pHash 整合ダミーの検索結果（Precision@k）および処理時間を比較し、検索精度の維持と計算コストの妥当性を確認した。また、Level 1（検索）から Level 2（復元）への切り替えに伴う処理時間の増加を測定し、段階開示として運用上分離できることを示した。

第 2 章

関連研究

本研究は、秘密画像共有 (Secret Image Sharing; SIS) により分散保持された画像集合に対して、原画像を復元 (平文化) せずに類似画像検索を成立させることを目的とする。第 1 章では背景と課題設定を述べたため、本章では提案法の位置づけに必要な既存研究を整理する。具体的には、類似画像検索で用いられる特徴量 (深層特徴と知覚ハッシュ)、暗号・秘密分散・多人数安全計算 (Multi-Party Computation; MPC) によるプライバシー保護検索、検索可能暗号 (Searchable Encryption; SE) を用いた検索、知覚ハッシュ (pHash) とその安全性・運用上の観点から関連研究を概観する。

2.1 類似画像検索に用いられる特徴量：深層特徴と知覚ハッシュ

高精度な類似画像検索では、Convolutional Neural Network (CNN) に基づく埋め込み (深層特徴) が広く用いられてきた。VGG (Visual Geometry Group) や ResNet (Residual Network) 等で抽出される特徴量は、画像の意味的類似をよく捉える一方で、次元数が数百から数千規模に及ぶことが多く、暗号化や秘密分散、MPC を併用して距離計算を行う場合、計算量・通信量が支配的になりやすいことが報告されている [20]。このため、プライバシー保護を要する設定では、コストを抑えるために次の工夫が検討されている。

- 特徴量自体を低次元化する。
- 距離計算を近似・簡略化する。
- 特徴量をバイナリ化し、ビット演算中心で照合する。

この文脈で、知覚ハッシュ (perceptual hash) は、画像を短いビット列へ写像し、Hamming 距離により高速比較できる点で実装・運用上の利点が多い。とりわけ pHash は、画像を小サイズに正規化した後に DCT を適用し、低周波成分の符号から 64bit 程度のハッシュ値 (ビット列) を生成する軽量手法として広く知られている [7, 26]。一方で、知覚ハッシュは「類似性を保存する」設計であるため、

照合の可否や距離が外部から反復的に観測できる状況では、検索機能がオラクルとして悪用される危険性がある（第 2.6 節参照）。したがって、pHash の軽量性を活かしつつ、どの情報をどの段階で開示するかまで含めた設計が重要となる。

2.2 秘密分散・MPC を用いたプライバシー保護検索

秘密分散や MPC を用いたプライバシー保護型の類似検索では、特徴量（多くは CNN 特徴）を暗号化・分散保持し、サーバ間で安全に距離計算を行う枠組みが提案されてきた。例えば、クラウド上の類似検索において、特徴量を秘匿化したまま比較処理を実行する方式が検討されている [20]。また、準同型暗号や MPC を用いて距離計算・近傍探索を実現する研究も多数存在し、暗号化ドメインや秘匿状態での比較処理そのものは可能になりつつある [22, 23]。

しかし、既存研究の多くは「特徴量ベクトル（平文特徴の秘匿表現）」を前提に、秘匿距離計算をどう成立させるかに主眼が置かれている。これに対して本研究は、

- 検索対象が SIS により「画像そのもの」として分散保持されていること
- 運用上「検索のみ許可／閲覧は禁止」という中間状態を明確に分離したいこと
- そのために検索用の出力形式自体を設計し直す必要があること

以上の設計により、本研究は機微画像の保護と画像検索の両立という課題に対し、SIS の枠組みを用いた具体的な解決策を確立した。

特に、SIS では閾値未満のシェア集合から意味情報が得られないよう設計されるため、復元を前提とする運用では「検索のたびに復元してから特徴抽出」という手順になりやすく、計算・通信コストと権限制御の両面で負担が大きい。このため、SIS の保護状態を維持したまま検索を成立させるには、距離計算の安全化だけでなく、「検索に必要な情報だけを制御して利用可能にする」ための表現設計が別途必要となる。

2.3 段階開示・多層 SIS に関する研究

秘密分散には、復元に必要な閾値が単一の (k -out-of- n) 型だけでなく、複数の閾値・アクセス構造を与えることで、異なる権限レベルに応じて復元可能な秘密を切り替える研究がある。たとえば multi-secret / multi-threshold 型の枠組みでは、参加者集合（あるいはシェア数）に応じて複数の秘密を復元できるようにアクセス構造を設計する [13, 14]。また、progressive（段階的）な復元を扱う系譜では、シェアの増加に伴って復元画像の品質が徐々に向上すること自体を目的とする研究がある [16, 18]。

本研究が狙うのは、画質が連続的に向上することそのものではなく、「検索専用の出力」と「閲覧可能な復元画像」を**離散的に**分離し、閾値に応じて**開示する情報の種類**を切り替える点にある。したがっ

て、既存の多層／多閾値アクセス構造の考え方に近い一方で、検索用表現 (pHash) と整合する「検索専用出力」を構成する設計は、既存研究では十分に整理されていない。

2.4 段階開示・多層 SIS に関する研究

秘密分散 (Secret Sharing) は、単一の (k, n) 閾値型に限らず、一般のアクセス構造を実現する枠組みや、多層 (階層) 構造を扱う拡張が研究されている。たとえば Benaloh-Leichter は、任意の単調アクセス構造を単調論理式として表現し、それに対応する秘密分散を構成する一般化手法を与えた [14]。また Tassa は、参加者が階層化された状況で、上位層の参加者を少数含むだけで復元可能になるような階層閾値アクセス構造に対して、理想的な秘密分散を設計している [13]。

一方、画像を対象とする秘密画像共有 (Secret Image Sharing; SIS) や視覚暗号 (Visual Cryptography; VC) では、シェア数の増加に伴って復元画像の視認性が向上する「progressive (段階的) 復元」を目的とする系譜がある。VC の代表例として Naor-Shamir の視覚暗号が知られ [15]、その拡張としてカラー画像に対する progressive 視覚暗号も提案されている [16]。また SIS 側でも、より多くのシェアを用いるほど復元品質が向上する PSIS (Progressive SIS) を扱う研究が報告されている [17]。これらの体系的整理として、視覚暗号を扱う書籍も存在する [18]。

本研究が狙うのは、復元品質が連続的に向上すること自体ではなく、「検索専用の出力」と「閲覧可能な復元画像」を**離散的に**分離し、閾値に応じて**開示する情報の種類**を切り替える点にある。特に、知覚ハッシュ (pHash) と整合する検索専用出力 (pHash 整合ダミー) を構成して検索を成立させつつ、閲覧につながる視覚情報を抑制する設計は、少なくとも上記の多層秘密分散／progressive SIS・VC の主要文献では明示的に議論されていない。

2.5 検索可能暗号 (SE) によるプライバシー保護検索

検索可能暗号 (SE) を用いて、暗号化したまま検索を行う研究も存在する。画像検索では、特徴量を暗号化してインデックスを構築し、暗号化状態で検索を行う方式が提案されている [24]。SE 系の枠組みは「検索はできるがデータ内容は隠す」という要請に整合しやすい反面、実装上は暗号化インデックスの構築・更新、検索トークン生成、アクセスパターン漏えい対策など、運用・性能の論点が複雑化しやすい。また、SIS のように画像自体が分散保持される状況や、閾値に応じて「検索専用出力／復元画像」を切り替える段階開示の要請を前提に設計された研究は多くない。

2.6 知覚ハッシュ (pHash) に関する研究

知覚ハッシュ (ロバストハッシュ) は、重複検出、改ざん検知、著作権管理等の文脈で研究・利用されてきた [26]。pHash はその代表例として広く普及しているが、本来は「類似性を保存するハッシュ値

(ビット列)」であるため、暗号学的ハッシュのような一方向性や耐推測性を保証するものではない [7]. このため、照合結果（距離やヒットの有無）を外部から反復的に観測できる環境では、検索機能がオラクルとして悪用されるという安全性・運用上の注意点が指摘されている [8].

以上を踏まえると、pHash をプライバシー保護設定で用いる場合は、単に「pHash を暗号化して比較する」だけでなく、どの情報をどの段階で開示するか（検索の可否と閲覧の可否をどう分離するか）まで含めて設計する必要がある。本研究は、SIS という「復元に閾値を要する分散保持」を前提に、pHash 整合な検索専用出力を導入して段階開示を実現する点に特徴がある。

2.7 Shamir 秘密分散の基礎

本節では、本研究で用いる Shamir 秘密分散の基本事項を整理する。Shamir 秘密分散は、有限体上の多項式補間に基づく (k, n) 閾値方式であり、「任意の k 個のシェアからは秘密を復元できるが、 $k - 1$ 個以下からは秘密に関する情報が得られない」という情報理論的性質をもつ [27]. 本研究ではこの性質を「閾値未満では復元できない」というアクセス制御の基盤として用いる。

2.7.1 Shamir 秘密分散の定義

総シェア数を n 、閾値を k ($1 \leq k \leq n$) とする。素数 p を法とする有限体 \mathbb{F}_p を用い、秘密（共有したい値）を $s \in \mathbb{F}_p$ として表す。Shamir 秘密分散では、次数 $k - 1$ 以下の多項式

$$f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_{k-1}x^{k-1} \quad (a_j \in \mathbb{F}_p) \quad (2.1)$$

を構成し、定数項を秘密に一致させる： $a_0 := s$ 。係数 a_1, \dots, a_{k-1} は \mathbb{F}_p 上で一様にランダムに選ぶ。

2.7.2 シェア生成手順

参加者（保持者） $i \in \{1, \dots, n\}$ に配布するシェアは、多項式の評価値として与える。評価点は 0 を避け、互いに相異なる $x_i \in \mathbb{F}_p \setminus \{0\}$ を選ぶ（本研究では実装の単純性のため $x_i := i$ を用いる）。このとき各参加者 i に配布するシェアは

$$\text{share}_i := (x_i, y_i), \quad y_i := f(x_i) \in \mathbb{F}_p \quad (2.2)$$

である。すなわち、秘密は多項式の定数項として埋め込まれ、シェアはそのサンプル点として配布される。

2.7.3 復元手順 (Lagrange 補間)

任意の k 個のシェア $\{(x_{i_1}, y_{i_1}), \dots, (x_{i_k}, y_{i_k})\}$ が与えられると、次数 $k-1$ 以下の多項式は一意に定まり、Lagrange 補間により $f(0) = s$ を直接計算できる。Lagrange 基底多項式を

$$\ell_j(x) = \prod_{\substack{m=1 \\ m \neq j}}^k \frac{x - x_{i_m}}{x_{i_j} - x_{i_m}} \pmod{p} \quad (2.3)$$

とすると、

$$f(x) = \sum_{j=1}^k y_{i_j} \ell_j(x) \pmod{p} \quad (2.4)$$

であり、特に復元したい秘密は

$$s = f(0) = \sum_{j=1}^k y_{i_j} \lambda_{i_j} \pmod{p}, \quad \lambda_{i_j} := \prod_{\substack{m=1 \\ m \neq j}}^k \frac{-x_{i_m}}{x_{i_j} - x_{i_m}} \quad (2.5)$$

として得られる。本研究の実装では、除算は \mathbb{F}_p 上の逆元計算（拡張 Euclid 等）により行い、復元は Lagrange 補間を用いて実装する。

2.7.4 情報理論的安全性（閾値未満で情報が漏れない理由）

Shamir 秘密分散の重要な性質は、閾値未満のシェア集合から秘密に関する情報が得られない点である。直観的には、 $t < k$ 個の点 $(x_{i_1}, y_{i_1}), \dots, (x_{i_t}, y_{i_t})$ が与えられても、それらを通る次数 $k-1$ 以下の多項式は多数存在し、定数項（秘密）も任意に取り得るためである。

より具体的には、任意の候補秘密 $s' \in \mathbb{F}_p$ に対して、「 $f(0) = s'$ かつ与えられた t 点を満たす」次数 $k-1$ 以下の多項式は少なくとも一つ存在し、さらに自由度が $k-1-t$ だけ残るため、その個数は同程度 (\mathbb{F}_p 上で一様) に分布する。したがって、観測者が得る $t (< k)$ 個のシェアは秘密 s の事後分布を変えず、秘密に関する相互情報量は 0 となる (perfect secrecy) [27]。この性質により、本研究では「 $r < k$ では当該秘密は復元できない」という前提を情報理論的に保証できる。

2.8 pHash の計算手順

pHash は標準的手順に従い、次の手順で 64bit のビット列 b を得る：

- (i) 画像を 32×32 のグレースケールに正規化する。
- (ii) DCT を適用する。
- (iii) 左上の低周波ブロック (8×8 相当) を取り出す。
- (iv) 係数の代表値（例：中央値）を閾値として 2 値化し、64bit のビット列 b を得る。

この低周波側の符号パターンを、以下「pHash の低周波符号」と呼ぶ。

2.9 Shamir 秘密分散の基礎

本節では、後続の二段閾値 SIS（第 3.4 節）を記述する準備として、本研究で用いる Shamir 秘密分散の基本事項を簡潔に整理する。Shamir 秘密分散は、有限体上の多項式補間に基づく (k, n) 閾値方式であり、「任意の k 個のシェアからは秘密を復元できるが、 $k - 1$ 個以下からは秘密に関する情報が得られない」という情報理論的性質をもつ [27]。本研究ではこの性質を「閾値未満では復元できない」というアクセス制御の基盤として用いる。

2.9.1 Shamir 秘密分散の定義

総シェア数を n 、閾値を k ($1 \leq k \leq n$) とする。素数 p を法とする有限体 \mathbb{F}_p を用い、秘密（共有したい値）を $s \in \mathbb{F}_p$ として表す。Shamir 秘密分散では、次数 $k - 1$ 以下の多項式

$$f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_{k-1}x^{k-1} \quad (a_j \in \mathbb{F}_p) \quad (2.6)$$

を構成し、定数項を秘密に一致させる： $a_0 := s$ 。係数 a_1, \dots, a_{k-1} は \mathbb{F}_p 上で一様にランダムに選ぶ。

次に、相異なる非ゼロの元 $x_1, \dots, x_n \in \mathbb{F}_p \setminus \{0\}$ （参加者 ID に相当）を選び、各参加者 i ($1 \leq i \leq n$) に対してシェア (x_i, y_i) を計算して配布する：

$$y_i = f(x_i) \pmod{p}. \quad (2.7)$$

ここで (x_i, y_i) が各参加者の保有するシェアとなる。画像への適用においては、画素値を s として扱うことが多い。

2.9.2 復元手順（Lagrange 補間）

任意の k 個のシェア $\{(x_{i_1}, y_{i_1}), \dots, (x_{i_k}, y_{i_k})\}$ が与えられると、次数 $k - 1$ 以下の多項式は一意に定まり、Lagrange 補間により $f(0) = s$ を直接計算できる。Lagrange 基底多項式を

$$\ell_j(x) = \prod_{\substack{m=1 \\ m \neq j}}^k \frac{x - x_{i_m}}{x_{i_j} - x_{i_m}} \pmod{p} \quad (2.8)$$

とすると、

$$f(x) = \sum_{j=1}^k y_{i_j} \ell_j(x) \pmod{p} \quad (2.9)$$

であり、特に復元したい秘密は

$$s = f(0) = \sum_{j=1}^k y_{i_j} \lambda_{i_j} \pmod{p}, \quad \lambda_{i_j} := \prod_{\substack{m=1 \\ m \neq j}}^k \frac{-x_{i_m}}{x_{i_j} - x_{i_m}} \quad (2.10)$$

として得られる。本研究の実装では、除算は \mathbb{F}_p 上の逆元計算（拡張 Euclid 等）により行い、復元は Lagrange 補間を用いて実装する。

2.9.3 情報理論的安全性（閾値未満で情報が漏れない理由）

Shamir 秘密分散の重要な性質は、閾値未満のシェア集合から秘密に関する情報が得られない点である。直観的には、 $t < k$ 個の点 $(x_{i_1}, y_{i_1}), \dots, (x_{i_t}, y_{i_t})$ が与えられても、それらを通る次数 $k - 1$ 以下の多項式は多数存在し、定数項（秘密）も任意に取り得るためである。

より具体的には、任意の候補秘密 $s' \in \mathbb{F}_p$ に対して、「 $f(0) = s'$ かつ与えられた t 点を満たす」次数 $k - 1$ 以下の多項式は少なくとも一つ存在し、さらに自由度が $k - 1 - t$ だけ残るため、その個数は同程度 (\mathbb{F}_p 上で一様) に分布する。したがって、観測者が得る $t (< k)$ 個のシェアは秘密 s の事後分布を変えず、秘密に関する相互情報量は 0 となる (perfect secrecy) [27]。この性質により、本研究では「 $r < k$ では当該秘密は復元できない」という前提を情報理論的に保証できる。

第 3 章

提案手法

3.1 動機付け

第 2 章で整理したように、プライバシー保護型 CBIR の多くは、高次元特徴量（CNN 埋め込み等）を暗号化・秘密分散し、距離計算そのものを安全計算化することで「復元せずに検索する」ことを目指してきた。一方で、本研究が扱うのは、そもそも原画像をサーバに置かず、画像自体を秘密画像共有（Secret Image Sharing; SIS）で分散保持する状況である。この状況では、検索のたびに閾値以上のシェアを集めて復元し、原画像に対して特徴抽出・照合を行う運用が素朴な解になるが、ボトルネックは次の 3 点である。

- 復元に伴う計算・通信コストが追加で発生しやすい。
- 復元には閲覧権限（復元許可）が必要となる。
- 復元には所定数のシェア収集が前提となり、「検索のみ許可したい」という要求と整合しにくい。

他方で、復元を避けるために、pHash 等の検索用表現を外部にそのまま露出させ、照合結果（距離や順位）を返す設計は、サーバを信頼しない（semi-honest）環境では、照合可否オラクルに悪用され得る。知覚ハッシュは暗号学的ハッシュのような方向性を目的としておらず、「似ているものは近い値になる」よう設計されているため、露出させ方を誤ると、オラクル自体が情報露出の手がかりになる。したがって本研究では、「検索を成立させるために必要な情報」と「閲覧（内容推定）につながる情報」を同一視せず、どの段階で何を開示するかを、閾値に基づいて明示的に分離する方針を採る。

本研究の要点は次の通りである。第一に、SIS の枠組みを保ったまま、シェア収集数に応じて出力の**種類**を切り替える三段階開示モデルを導入する。第二に、検索段階では、pHash 検索に必要な情報だけを満たす検索専用出力（pHash 整合ダミー）を生成し、閲覧に資する視覚情報は意図的に劣化させる。第三に、比較は 64bit 程度の軽量な pHash に限定し、検索処理を過度に重くしない設計を優先する。

3.2 問題設定と記号

本章では、提案手法を記述するために必要な問題設定、記号、および脅威モデルを定義する。具体的には、入力画像 I 、pHash 表現 b 、SIS のパラメータ (n, k) と収集シェア数 r を導入し、semi-honest なサーバ（結託を含む）が観測可能な情報の範囲と、本研究が前提とする安全性条件を明確化する。また、後続章で用いる段階的開示（Level 0/1/2）の定義を与える。

3.2.1 問題設定（システムモデル）

本研究では、画像の保持者（クライアント）が画像 I を秘密分散し、複数の保持者（サーバ群、あるいは分散保管ノード）にシェアを配布する状況を考える。検索要求が発生した際、収集可能なシェア数 r に応じて、検索に必要な最小限の出力のみを返す（閲覧はさせない）または、原画像 I の復元を許可する、という出力制御を行う。

3.2.2 記号

入力画像を I とし、pHash を 64bit のビット列 $b \in \{0, 1\}^{64}$ で表す。総シェア数を n 、収集したシェア数を r とする。段階的開示のために二つの閾値 k_1, k_2 ($k_1 < k_2$) を設ける。

pHash は知覚ハッシュの一種であり、画像を正規化して DCT に基づく低周波成分を要約し、得られた 64bit 列 b を Hamming 距離で比較する（詳細な計算手順は 3.2.4 で述べる）。

3.2.3 脅威モデル

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、観測できる情報（保持データ、出力、ログ、アクセスパターン等）から推測を試みる semi-honest を想定する。また、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が、閾値未満では復元できないことを前提とする。

3.3 三段階開示モデル（Level 0/1/2）

本研究は、シェア収集数に応じて「何ができるか」を三段階に分離する。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。

- **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、検索に資する情報を追加で開示しない。実装上は、外部に返す出力が必要な場合、秘密と独立なノイズ画像（プレースホルダ）を返す。
- **Level 1** ($k_1 \leq r < k_2$) : 検索のみを許可する段階であり、pHash 検索に必要な条件だけを満たす「検索専用出力」を生成して開示する。本研究ではこれを pHash 整合ダミーと呼ぶ。

- **Level 2** ($r \geq k_2$) : 復元（閲覧）を許可する段階であり，原画像 I の復元を可能にする．

この三段階は，「画像を三回別々に分割する」という意味ではない．同じ参加者に対して配布するシェアの中に，**検索段階に必要な秘密**と**復元段階に必要な秘密**を同居させ，集まったシェア数に応じて復元できる対象を切り替える，という設計である．開示規則は次式で表せる：

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

ここで $\text{dummy}(b)$ は，pHash が b と一致することを満たす一方で，視覚的内容が読み取りにくいように劣化させた画像である．（Level 1 は「pHash 一致は満たすが，閲覧に十分な視覚情報は保証しない」ことを狙う段階である．）

3.4 Shamir 法の画像への適用（データ表現）

本研究では，前述の Shamir 秘密分散法（第??節）を用いて画像を分散する．この際，画素集合やバイト列である画像データを，有限体 \mathbb{F}_p 上の計算で扱える形式（整数）へ適切に符号化する必要がある．本節では，本研究におけるデータ表現と Shamir 法の適用方法について述べる．

3.4.1 有限体とパラメータの選択

本研究では有限体として \mathbb{F}_p (p は十分大きな素数) を採用し，具体的には

$$p = 2^{521} - 1 \tag{3.1}$$

を用いる（一般化メルセンヌ形であり，楕円曲線 P-521 の法としても用いられる）[19]．これにより，画像をバイト列として扱い， p 未満に収まるよう固定長チャンクへ分割して各チャンクを整数 (\mathbb{F}_p の元) として分散する運用が容易になる．

3.4.2 画像の整数化とチャンク分割

画像 I をバイト列 $\text{bytes}(I)$ として取り出し，長さ L バイトのブロックに分割して，各ブロックをビッグエンディアンで整数化する：

$$m_j := \text{int}(\text{bytes}_j) \in [0, 256^L) \subset \mathbb{F}_p. \tag{3.2}$$

$256^L < p$ となるように L を選べばオーバーフローを避けられる．復元後に元のバイト列へ戻せるよう，総バイト長や最終ブロックの有効長をメタ情報として保持する．

また，本研究で低閾値側の秘密として用いる pHash ビット列 $b \in \{0, 1\}^{64}$ については，64bit 整数にパックしてそのまま $s \in \mathbb{F}_p$ として扱う．以上の符号化を前提として，次節では「検索用秘密」と「復元

用秘密」を別々に Shamir 分散し、同一参加者に束ねて配布する二段閾値 SIS の構成を述べる。

3.5 二段閾値 SIS（検索用秘密と復元用秘密の同時分散）

三段階開示を実現するための基本的な考え方は、各参加者に配るデータ（シェア）の中に、「検索用」と「完全復元用」という二つの独立したデータを埋め込んでおくことである。直観的には、集まったシェアの数に応じて、取り出せるデータの種類（深さ）が変わる構造を作る。具体的には、ある閾値 k_1 以上集まれば「検索用データ」だけが復元でき、これを用いて検索可能なノイズ画像（pHash 整合ダミー）を生成する。さらに多くの閾値 $k_2 (> k_1)$ 以上集まれば、「原画像データ」まで復元し、元の画像を取り戻せる。

これを形式化するため、本研究では二種類の秘密を定義する：低閾値側の秘密を s_L 、高閾値側の秘密を s_H とする。

$$s_L := b \in \{0, 1\}^{64}, \quad s_H := I$$

ここで s_L は閾値 k_1 で復元可能、 s_H は閾値 k_2 で復元可能となるように分散する。

具体的には、 s_L を定数項とする次数 $k_1 - 1$ の多項式 $f_L(x)$ と、 s_H を定数項とする次数 $k_2 - 1$ の多項式 $f_H(x)$ をそれぞれ独立に生成する（係数はランダムに選ぶ）。各参加者 i に対しては、それぞれの多項式の評価値を束ねて

$$\text{share}_i = (i, f_L(x_i), f_H(x_i))$$

を配布する。ここで $f_L(x_i)$ は s_L のシェア、 $f_H(x_i)$ は s_H のシェアに相当する。このとき、 $r < k_1$ では s_L, s_H はいずれも復元できず、 $k_1 \leq r < k_2$ では s_L のみ復元でき、 $r \geq k_2$ で初めて s_H が復元できる。すなわち「シェア数に応じて復元できる秘密が変わる」という意味で、多閾値（multi-threshold）／多層（multi-level）のアクセス構造として整理できる。

以降の実験では、具体例として $n=5$ 、 $(k_1, k_2) = (2, 4)$ を用いる。ただし本章の議論はこの値に依存しない。

3.6 pHash 整合ダミーの生成

本節では、Level 1 で開示する pHash 整合ダミー $\text{dummy}(b)$ の生成法を述べる。ここで重要なのは、Level 1 では原画像 I を復元しない点である。したがって、ダミー生成は、Level 1 で復元できる情報（本研究では $s_L = b$ ）から実行できなければならない。

直観的には、pHash が参照する低周波側の条件だけを満たすように周波数領域を構成し、それ以外（特に高周波成分）はランダム化することで、pHash 一致と視認性低下を両立させる。具体的な手順は次の通りである：

1. Level 1 で復元したビット列 b を入力として、 32×32 画像に対する DCT 係数行列のうち、低周

波ブロック (8×8 相当) に対応する係数に対し、ビット $b_i = 1$ ならば正の値、 $b_i = 0$ ならば負の値を割り当てることで、符号パターンが b と整合する目標係数 \tilde{C}_{LF} を構成する。

2. 逆 DCT 後の微小なゆらぎで符号が反転しないように、低周波係数に**マージン**を持たせるため、係数の絶対値を一定量以上に設定する（本論文ではこれを「低周波係数の強調」と呼ぶ）。
3. 高周波側の係数 \tilde{C}_{HF} は乱数で埋める。これにより、輪郭・文字・顔など閲覧に資する細部構造が再現されにくいようにする。
4. 構成した係数行列 \tilde{C} に逆 DCT (IDCT) を適用して空間画像 \tilde{I} を得る。
5. \tilde{I} から pHash を再計算し、 b と一致することを確認する。一致しない場合は低周波係数の強調量（マージン）を増やすなどして再生成する。

このようにして得られる \tilde{I} を pHash 整合ダミー $\text{dummy}(b)$ として用いる。ここで、pHash 整合ダミーは「pHash 一致」を満たすための検索専用出力であり、視覚的内容の復元（閲覧可能性）を保証しない点が本質である。以後の章では、ダミーの視認性低下を PSNR (Peak Signal-to-Noise Ratio) や SSIM (Structural Similarity) 等の指標で評価し、また検索段階 (Level 1) での偽一致（衝突）については Hamming 距離の閾値判定とあわせて実験で確認する。

3.7 安全性の扱い (Shamir の保証とダミーの評価)

Shamir 秘密分散は、閾値未満のシェア集合から秘密に関する情報を与えないという情報理論的安全性をもつ。したがって本研究の構成では、 $r < k_1$ で s_L (pHash) も s_H (原画像) も復元できないこと、および $k_1 \leq r < k_2$ で s_H が復元できないことは、分散方式の性質として保証される。

一方で、Level 1 では $s_L = b$ を用いて検索を成立させるため、低周波符号に関する情報露出が**ゼロ**であることは保証しない。本研究が主張するのは、(i) 閾値設計により「検索のために開示する情報」と「復元（閲覧）に必要な情報」を分離し、(ii) Level 1 の出力は検索に必要な条件 (pHash 一致) を満たしつつ、閲覧に資する視覚情報を劣化させるよう構成される、という設計上の性質である。そのうえで、「どの程度閲覧に耐えないか」「どの程度偽一致が起きないか」は、PSNR/SSIM や pHash 距離分布、Precision@k などの実験指標により評価する（詳細は第 4 章）。

3.8 検索パイプライン

本研究の検索パイプラインは、検索処理を必要最小限に保つため、比較は pHash (64bit) と Hamming 距離に限定する。シェア生成・復元はクライアント側で完結させ、サーバは検索用データベース (pHash の索引等) を保持し照合を行うが、サーバは semi-honest であり得るという前提のもと、開示レベルに応じて入力として与えるものを切り替える。

具体的には、 $r < k_1$ では検索自体を行わず（または秘密と独立なプレースホルダのみを扱い）、

$k_1 \leq r < k_2$ では復元した b から pHash 整合ダミーを生成して検索入力とし, $r \geq k_2$ では原画像 I を復元して必要に応じて平文側の処理へ移行する. このように, 閾値到達に応じて「検索専用の入力」と「復元入力」を切り替えることで, 検索と閲覧 (復元) の権限・コストを段階的に分離する.

3.9 実装

3.9.1 pHash 計算と DCT/IDCT

pHash は, 画像を 32×32 のグレースケールへ正規化した後, 2 次元 DCT を適用し, 低周波 8×8 ブロックの係数を基準値 (中央値) で 2 値化して 64bit のハッシュ値 (ビット列) を生成する. DCT/IDCT は DCT-II (および逆変換) に基づき, 2 次元変換は分離可能性を用いて 1 次元変換を縦横に適用することで実装した. 本研究では画像サイズを 32×32 に固定するため, cosine テーブル (変換行列) を事前計算して使い回し, 計算量と実装の単純性のバランスを取っている.

3.9.2 pHash 整合ダミー計算

Level 1 ($k_1 \leq r < k_2$) では, pHash 計算が参照する低周波成分が目標ビット列と整合するように構成した pHash 整合ダミーを出力する. ダミー生成は Level 1 で復元できる情報 ($s_L = b$) のみから実行されることが要件であり, 実装では以下の手順を採る.

低周波ブロックの構成

64bit ハッシュ値 (ビット列) $b \in \{0, 1\}^{64}$ を受け取り, 低周波 8×8 ブロックの各係数が b と整合するように振幅を割り当てる (`_build_lowfreq_from_bits`). 本実装では, 中央値を 0 近傍に保つ設計とし, $b_i = 1$ を正, $b_i = 0$ を負に対応させることで, pHash の 2 値化結果が一致するように構成する.

符号反転を避けるためのマージン補強

逆 DCT, および 0-255 への正規化・量子化により係数の符号が反転すると pHash 一致性が崩れるため, 低周波係数にマージンを持たせる補強処理を導入する (`_reinforce_margin`). 具体的には, 低周波係数の絶対値が所定の閾値を下回る場合に増幅し, 空間域の微小な揺らぎで符号が反転しにくい状態を作る.

高周波の無構造化とダミー画像の生成

高周波成分は平均 0・標準偏差 12 のガウスノイズで埋めることで無構造化し, 低周波のみを拘束した周波数領域表現を構成する. その後, IDCT により 32×32 の空間画像を得て, 0-255 に正規化し, 最終的に元解像度へ Bicubic で拡大する (`make_phash_preserving_dummy`). 乱数は NumPy の

`default_rng` を用い、評価時はシードを固定して再現可能性を担保する。また、生成後に pHash を再計算し、目標 b と一致しない場合は補強量（マージン）を増やして再生成する。

3.9.3 二段階 Shamir（低閾値・高閾値）の実装

本研究では、低閾値側の秘密 s_L と高閾値側の秘密 s_H を分離し、同一のインデックス i に対して 2 種類のシェアを束ねて配布する。低閾値側は $s_L := b$ (pHash の 64bit ハッシュ値 (ビット列))、高閾値側は $s_H := I$ (原画像データ) とする。各シェアは $\text{share}_i = (i, \text{share}_i^L, \text{share}_i^H)$ として保持する。

有限体と補間

Shamir 秘密分散は有限体 \mathbb{F}_p 上で実装し、復元は Lagrange 補間により行う (`_lagrange_interpolate`)。法 p には十分大きな素数が必要であるため、本実装では $p = 2^{521} - 1$ を採用した (一般化メルセンヌ形であり、P-521 の法としても用いられる) [19]。これにより、画像データを整数列へ符号化して分散する際にも十分な余裕が得られる。

秘密の符号化 (チャンク化)

画像 I はバイト列として扱い、 p 未満に収まるよう固定長チャンクへ分割して整数へ変換した上で分散する。復元時に元のバイト列へ復元できるよう、チャンク長 (および末尾の有効長) をメタ情報として保持する。pHash ハッシュ値 (ビット列) b は 64bit の整数にパックし、 s_L として分散する。

パラメータ設定

以降の評価では $n = 5$, $(k_1, k_2) = (2, 4)$ を用いる。すなわち、 $r < k_1$ では s_L, s_H のいずれも復元できず、 $k_1 \leq r < k_2$ では s_L のみ復元でき、 $r \geq k_2$ で初めて s_H を復元できる。二段階分散は `TwoLevelShamirScheme` として実装した。

3.9.4 評価に用いる指標の算出と可視化

提案方式の挙動確認として、原画像 (平文)、 k_1 到達時に得られるダミー、および $r < k_1$ のときに出力されるノイズについて、pHash 距離 (Hamming 距離) の分布を比較する (図 3.1)。また、ダミーと原画像の視覚的乖離の程度を定量化するため PSNR を算出する (図 3.2)。さらに、ダミー生成の内部分状態 (低周波構成と補強の効果) を確認するため、処理途中の 32×32 画像を出力する (図 3.3)。

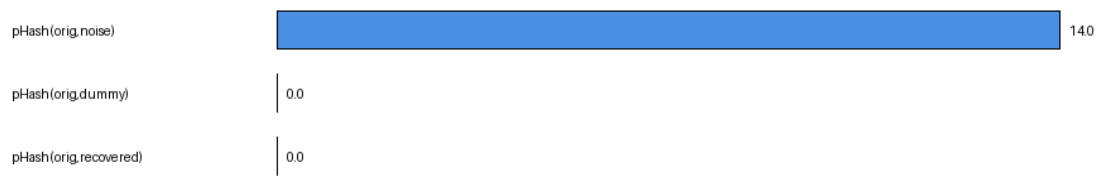


図 3.1 pHash 距離の分布 (原画像平文 / k_1 ダミー / $r < k_1$ ノイズ)



図 3.2 PSNR の分布 (ダミーと原画像)

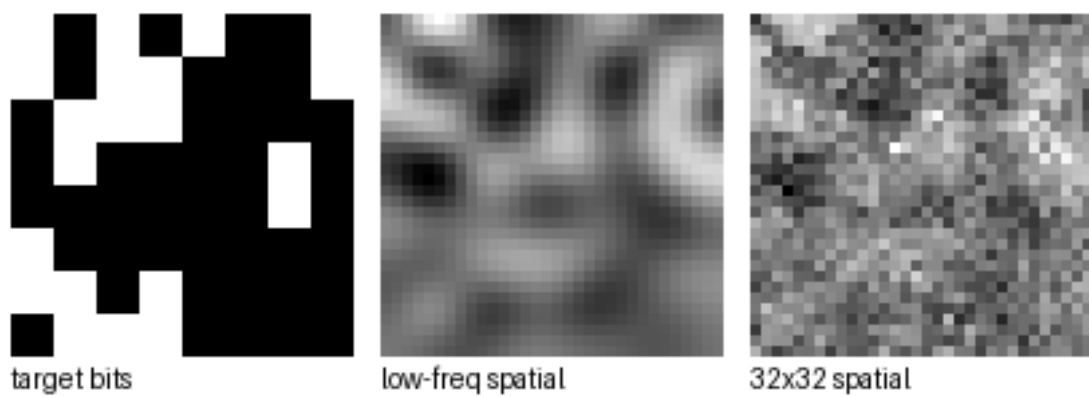


図 3.3 ダミー生成の途中出力例 (pHash 符号 → 低周波補強 → 32×32 空間画像)

第 4 章

実験

本章では、第 3 章で述べた三段階開示方式を、Python 実装と実験手順として具体化する。あわせて、評価で用いる実装上の設定（パラメータ、乱数の扱い、指標の算出方法）も本章で明確化する。本章の導入として、原画像・ノイズ ($r < k_1$)・pHash 整合ダミー ($k_1 \leq r < k_2$)・復元画像 ($r \geq k_2$) の代表例を図 4.1 に示す。

4.1 条件・手順

4.1.1 実装方針と依存関係

実装は Python 3 系で構築し、数値計算に NumPy、画像の入出力・リサイズに Pillow を用いた。提案方式の中核（pHash 計算、DCT/IDCT、Shamir 秘密分散、pHash 整合ダミー生成）は自前実装とし、SciPy / OpenCV などの外部画像処理ライブラリや暗号・秘密分散の専用ライブラリには依存しない。これは、環境構築の容易さと再現性を優先するためである。なお、可視化と集計は評価用スクリプト側で Matplotlib を用いて行い、中核アルゴリズムの依存関係とは分離した。

4.2 実験条件・手順

4.2.1 評価指標

本節では検索性能の評価指標として Precision@K と Recall@K を用いる。ここで K は評価する上位件数である。クエリ画像 q に対して検索結果上位 K 件を $\text{Top}K(q)$ 、正解集合を $G(q)$ とすると、

$$\text{Precision@}K(q) = \frac{|\text{Top}K(q) \cap G(q)|}{K}, \quad (4.1)$$

$$\text{Recall@}K(q) = \frac{|\text{Top}K(q) \cap G(q)|}{|G(q)|} \quad (4.2)$$

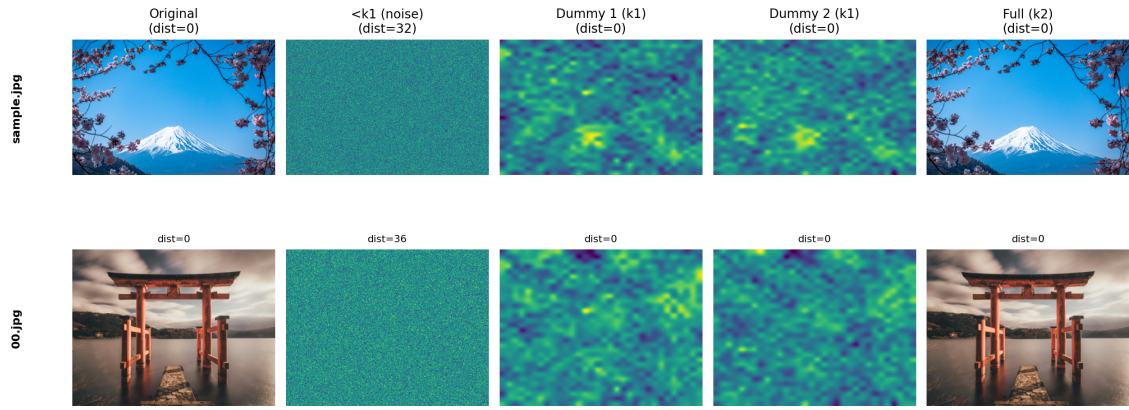


図 4.1 三段階出力の可視化例（複数画像の比較：原画像／ノイズ／pHash 整合ダミー 1, 2／復元）

で定義する．原画像のみを対象とする評価（以降「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 ($|G(q)| = 1$)，派生画像群を正解集合とする評価（以降「バリエーション評価」）では同一元画像から生成された派生画像群を $G(q)$ とする．

4.2.2 データと派生画像の生成

COCO val2017 から乱数シード 2025 により 500 枚をサンプリングし，これをクエリ集合とした．また，各原画像から固定パラメータの画像変換を適用し，派生セット `coco2017_derivatives` を作成した．派生の種類は original を含めて 20 種とし，対応関係を `mapping.json` に記録した．具体的には JPEG (q75, q60, q50+ サブサンプリング)，WebP (q70)，回転 $\pm 30^\circ$ （黒埋め），30% クロップ，台形射影，リサンプリング（双線形 \rightarrow 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，矩形遮蔽を用いた．

4.2.3 検索・比較の手順

各画像について次の処理を行った．

1. 32×32 グレースケール化と pHash 計算 (64bit)．
2. pHash 符号を保ったまま高周波成分をノイズ化した pHash 整合ダミーの生成 (k_1 到達時の検索用出力)．
3. 原画像（平文）とダミーを $n = 5, (k_1, k_2) = (2, 4)$ の二階層 Shamir によりシェア化し， $r < k_1$ では復元不能（ノイズ相当）， $k_1 \leq r < k_2$ ではダミーのみ出力可能， $r \geq k_2$ で原画像を復元可能とした．

検索性能の比較は，原画像の pHash による検索（plain）と， k_1 到達時に得られるダミー画像の pHash による検索（dummy.k1）の 2 条件で行った．探索では 64bit を 8 分割（bands=8）したパケッ

ト化により候補集合を絞り込み、候補に対して Hamming 距離を計算して順位付けを行った。さらに閾値 $\tau = 8$ を用い、距離が閾値以下の候補をヒットとして扱う設定とした。本設定により、各クエリについて上位 $K \in \{1, 5, 10\}$ の Precision@K/Recall@K と処理時間を集計した。

4.3 結果・考察

本節では、(i) pHash 距離分布、(ii) 検索精度 (Precision@K/Recall@K)、(iii) 処理時間を plain と dummy_k1 で比較し、 k_1 到達時の検索段階で平文と同等の挙動を維持できるかを確認する。

4.3.1 pHash 距離分布の確認

原画像 (平文) と、 k_1 到達時に得られるダミー (dummy_k1)、および $r < k_1$ の復元不能段階で出力されるノイズ相当画像について、pHash 距離の分布を比較した (図 3.1)。dummy_k1 と原画像の距離が小さく (もしくは同一に) 集中すれば、Hamming 距離に基づく順位付けが plain と整合し、検索結果 (上位 K 件) が一致しやすい。一方、 $r < k_1$ の段階が原画像と近い距離を頻繁に与える場合、「検索情報を開示していない段階でも検索が成立する」危険が生じる。本実験では $r < k_1$ の距離は無関係ペアと同程度の分布となり、候補として残りにくいことを確認した。

4.3.2 検索精度と時間 (オリジナル評価)

図 4.2 と図 4.3 に、オリジナル評価 (各クエリの正解が 1 件) に対する結果を示す。本条件では、正解が上位 1 件に入れば Precision@1=100% となり、上位 5 件に入れば Precision@5=20% ($= 1/5$)、上位 10 件に入れば Precision@10=10% ($= 1/10$) となるため、Precision@5 や Precision@10 は評価設定 ($|G(q)| = 1$) に依存して値が定まる点に注意が必要である。実験では plain/dummy_k1 ともに Precision@1=100% であり、Recall@10 も 100% であった。処理時間は 0.581 ms/query (plain) と 0.548 ms/query (dummy_k1) であり、同一の比較 API (pHash 計算と Hamming 距離比較) で処理できるため差は小さい。

4.3.3 バリエーション評価 (全 20 バリエーション)

次に、全 20 バリエーション条件では正解集合を「同一元画像から生成された派生画像群」とし、によりバリエーションごとの精度と時間を集計した。全バリエーション平均として Precision@1=100%, Precision@5=86.6%, Precision@10=84.82%, Recall@10=42.41% が得られ、これらの値は plain と dummy_k1 で一致した (図 4.4)。これは、dummy_k1 が pHash 計算に影響する低周波側の条件を一致させる設計であり、比較が pHash (Hamming 距離) のみで完結するため、候補生成と順位付けが一致し得ることを反映している。処理時間も 0.527 ms/query (plain) と 0.494 ms/query (dummy_k1)

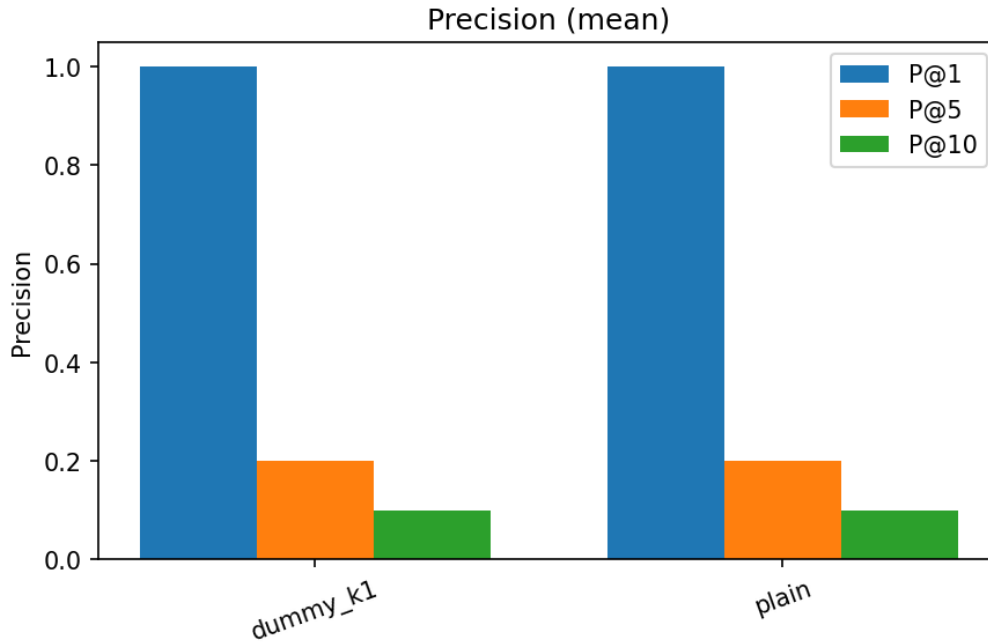


図 4.2 Precision (平均値, オリジナル評価; 各クエリの正解は 1 件)

で差が小さく (図 4.5), k_1 到達時の検索段階で計算負担を増やさずに適用できることを示している。

4.3.4 検索の実用性

本実装条件では, 「検索段階 (k_1 到達) において, 平文検索と同等のランキング結果・同等の処理時間を維持できる」ことを確認した。これは, 「復元 (閲覧) を許可せずに検索のみ行う」運用要求に対して, 復元ベースの検索手順を回避しつつ検索の実用性 (精度と時間) を確保できる可能性を示す。

4.3.5 安全性評価の範囲と課題

一方で, 本章の比較は pHash 検索 (距離分布とランキング一致) に限定されており, Level 1 で開示される情報 (pHash 符号や照合結果) が, 反復問い合わせ可能な判定器 (オラクル) としてどの程度推測に利用され得るかを直接評価するものではない。本研究の保証範囲は, Shamir の閾値性 ($r < k_2$ で原画像が復元不能) に基づく部分と, Level 1 の出力が視覚的内容推定に結びつきにくいという経験的評価に分かれる。したがって今後は, 攻撃者モデルを明示したうえで, 問い合わせ回数制限・監査ログ・探索戦略の評価などを含む追加検証が必要である。

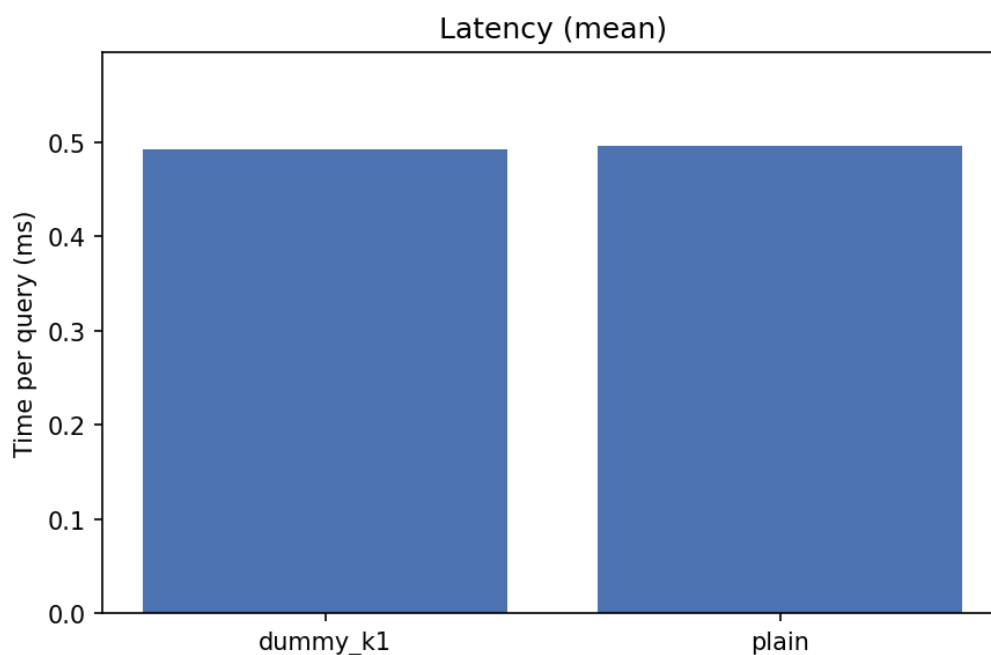


図 4.3 Latency (平均値, オリジナル評価)

表 4.1 評価した 20 バリエントの例 (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

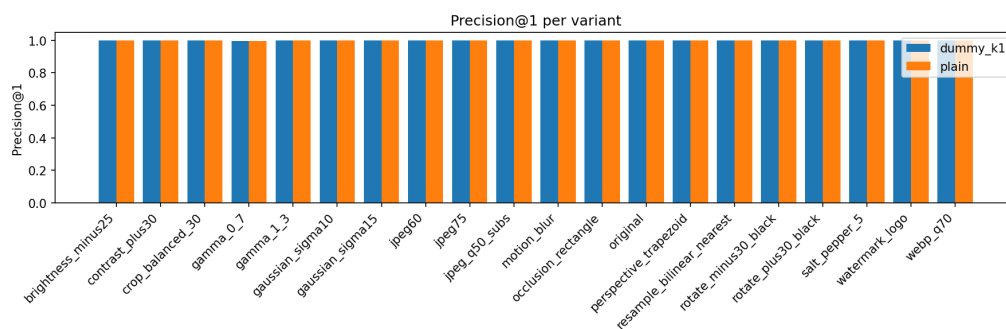


図 4.4 Precision@1 (バリエント別, plain vs dummy_k1)

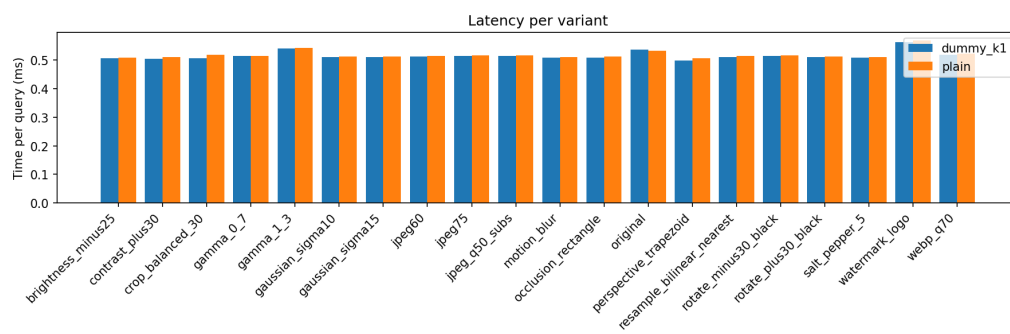


図 4.5 Latency (バリエーション別, plain vs dummy_k1)

第 5 章

おわりに

本研究は、秘密画像共有 (SIS) により分散保持された画像集合を対象として、原画像の復元 (平文化) を前提とせずに類似画像検索を成立させるための設計と実装・評価を示した。本研究の成果は以下のよう整理できる。

- 検索可能性と閲覧可能性を混同せずに制御するための段階開示モデルを提示した。
- 具体的には、シェア収集数 r に応じて開示レベルを切り替える枠組みを定義し、 $r < k_1$ では検索に資する情報を開示せず (Level 0)、 $k_1 \leq r < k_2$ では検索のみを許可する出力 (Level 1) を開示し、 $r \geq k_2$ で初めて復元 (Level 2) を許可するという二つの閾値 k_1, k_2 に基づくアクセス構造として定式化した。
- これにより、「検索だけ許可したい」という運用要求を、復元許可 (閲覧許可) と切り離して扱えることを明確化した。

実験では、pHash 整合ダミーにより平文 pHash と同等のランキング結果と処理時間を維持でき、また検索 (k_1) と復元 (k_2) で処理負担が段階化されることを確認した。

一方で、Level 1 では検索を成立させるために pHash の情報を開示しているため、これが安全性への懸念点として残る。具体的には、前述した「反復問い合わせ可能な判定器 (オラクル)」として機能することで元の画像情報を推測されるリスクや、どの画像を検索したかという履歴 (アクセスパターン) からの情報漏えいである。今後は、こうした漏えいを防ぐためのアクセスパターン秘匿技術の導入や、ダミー画像から具体的にどの程度元の内容が推測できてしまうかのより詳細な評価 (人手による判定や属性推定など) が必要である。また、pHash よりも頑健な特徴量の採用や、大規模なデータベースでの実用性検証も進めていく必要がある。

参考文献

- [1] H. Müller, “Medical Image Retrieval: Applications and Resources,” in *Proceedings of the ACM International Conference on Multimedia Retrieval (ICMR 2020)*, 2020. doi:10.1145/3372278.3390668.
- [2] C. G. Sotomayor, M. Mendoza, V. Castañeda, H. Farías, and others, “Content-Based Medical Image Retrieval and Intelligent Interactive Visual Browser for Medical Education, Research and Care,” *Diagnostics*, vol. 11, no. 8, 1470, 2021. doi:10.3390/diagnostics11081470.
- [3] M.-J. Su, Y.-C. Lin, Y.-C. Chen, and C.-M. Huang, “Diagnostic Decision Support by Intelligent Medical Image Retrieval with Electronic Medical Record for Enhance Dementia Treatment,” *Medical Imaging Technology*, vol. 25, no. 5, pp. 350–355, 2007.
- [4] Y. Xu, J. Gong, L. Xiong, Z. Xu, J. Wang, and X. Liu, “A Privacy-Preserving Content-Based Image Retrieval Method in Cloud Environment,” *Journal of Visual Communication and Image Representation*, vol. 43, pp. 35–43, 2017. doi:10.1016/j.jvcir.2017.01.006.
- [5] D. Ferreira, R. Rodrigues, P. Leitão, and D. Domingos, “Privacy-Preserving Content-Based Image Retrieval in the Cloud,” in *Proceedings of the 34th IEEE Symposium on Reliable Distributed Systems (SRDS 2015)*, pp. 11–20, 2015. doi:10.1109/SRDS.2015.27.
- [6] J. Katz and Y. Lindell, *Introduction to Modern Cryptography*, 3rd ed., Chapman and Hall/CRC, 2020.
- [7] N. Krawetz, “Looks Like It (Perceptual Hashing),” The Hacker Factor. <https://www.hackerfactor.com/blog/index.php/?archives/432-Looks-Like-It.html> (Accessed: 2026-01-05).
- [8] A. Jain and others, “SoK: Perceptual Hashing in the Adversarial Setting,” in *USENIX Security Symposium*, 2022.
- [9] H. Prokos, M. Christodorescu, and others, “Robustness and Trustworthiness of Perceptual Hashing in Adversarial Settings,” arXiv:2406.00918, 2024.
- [10] R. Guo, S. Liu, and X. Zheng, “Multi-threshold access structures for secret sharing schemes,” *Pattern Recognition Letters*, vol. 33, pp. 1594–1600, 2012.

- [11] W.-P. Fang, C.-C. Lin, and C.-C. Tsai, “Friendly progressive visual secret sharing,” *Pattern Recognition Letters*, vol. 29, no. 11, pp. 1582–1587, 2008.
- [12] A. Agarwal, S. S. Rana, and others, “Verifiable progressive visual cryptography,” *Pattern Analysis and Applications*, 2018. doi:10.1007/s10044-016-0571-x.
- [13] T. Tassa, “Hierarchical Threshold Secret Sharing,” *Journal of Cryptology*, vol. 20, no. 2, pp. 237–264, 2007. doi:10.1007/s00145-006-0334-8.
- [14] J. C. Benaloh and J. Leichter, “Generalized Secret Sharing and Monotone Functions,” in *Advances in Cryptology—CRYPTO ’88*, LNCS 403, pp. 27–35, Springer, 1988. doi:10.1007/0-387-34799-2_3.
- [15] M. Naor and A. Shamir, “Visual Cryptography,” in *Advances in Cryptology—EUROCRYPT ’94*, LNCS 950, pp. 1–12, Springer, 1994. doi:10.1007/BFb0053419.
- [16] D. Jin, W. Q. Yan, and M. S. Kankanhalli, “Progressive Color Visual Cryptography,” *Journal of Electronic Imaging*, vol. 14, no. 3, 033019, 2005. doi:10.1117/1.1993625.
- [17] L. Xiong, Z. Han, and M. Yang, “CP-PSIS: CRT and polynomial-based progressive secret image sharing scheme,” *Signal Processing*, vol. 185, 108064, 2021. doi:10.1016/j.sigpro.2021.108064.
- [18] F. Liu and W. Q. Yan (eds.), *Visual Cryptography for Image Processing and Security: Theory, Methods, and Applications, Second Edition*, Springer, 2015. doi:10.1007/978-3-319-23473-1.
- [19] L. Chen, D. Moody, A. Regenscheid, A. Robinson, and K. Randall, “Recommendations for Discrete Logarithm-based Cryptography: Elliptic Curve Domain Parameters,” NIST Special Publication 800-186, 2023. doi:10.6028/NIST.SP.800-186.
- [20] Z. Xia, X. Wang, L. Yao, et al., “A privacy-preserving CBIR scheme based on secret sharing,” *IEEE Access*, 2020.
- [21] C. Zhang, Y. Li, and Q. Liu, “SS-CNN: Secret sharing based secure image retrieval,” *Journal of Visual Communication and Image Representation*, 2024.
- [22] 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.
- [23] 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.
- [24] M. Tian, Y. Zhang, Y. Zhang, X. Xiao, and W. Wen, “A privacy-preserving image retrieval scheme with access control based on searchable encryption in media cloud,” *Cybersecurity*, vol. 7, Art. 22, 2024.

- [25] Z. Xia, Y. Zhu, X. Sun, and Q. Wang, “Searchable image encryption for privacy-preserving CBIR,” *IEEE Access*, 2021.
- [26] R. Venkatesan, S.-M. Koon, M. Jakubowski, and P. Moulin, “Robust image hashing,” in *Proc. IEEE ICIP*, 2000.
- [27] A. Shamir, “How to share a secret,” *Communications of the ACM*, vol. 22, no. 11, pp. 612–613, 1979. doi:10.1145/359168.359176.