

ステガノグラフィ (ANGO) の特性と テンプレートマッチングへの応用に関する研究

石塚 裕一^{1,a)} 越前 功² 岩村 恵市³ 櫻井 幸一¹

受付日 2015年12月3日, 採録日 2016年6月2日

概要: 原画像に手を加えず, 原画像の特徴と強く結びついたデータを, その原画像の真贋性の保証や透かし情報として利用するハッシュ関数や Zero-watermarking といった技術がある. 我々が提案するステガノグラフィ技術は Zero-watermarking の一種と見なされることがあるが, 復号時に特徴抽出などの前処理が必要ないといった Zero-watermarking などにはない特徴を持っている. そのため復号処理が高速に行え, ステガノグラフィとしての利用に加えて, 類似画像の検索や類似度順のソートにも応用できる. 今回, 提案方式の計算量の評価およびノイズ・圧縮耐性試験および, 類似画像検索について実験を行い, その有効性を確認したので報告する.

キーワード: ステガノグラフィ, 電子透かし, 類似画像検索, テンプレートマッチング, 周波数解析

Study of the Characteristics of Steganography ANGO and its Template Matching Application

HIROKAZU ISHIZUKA^{1,a)} ISAO ECHIZEN² KEIICHI IWAMURA³ KOICHI SAKURAI¹

Received: December 3, 2015, Accepted: June 2, 2016

Abstract: Without adding a hand to an original image, there are some technologies such as hash function, fingerprinting or zero-watermarking which utilize the data strongly tied to the characteristics of the original image as the authenticity of the original image. We proposed a steganography that can also be classified as a kind of zero-watermarking. Our steganography has a remarkable feature at the time of decoding compared with zero-watermarking. The feature is that our method does not need pre-processing at the feature extraction. Therefore, the decoding can be done at high speed, and it is possible to apply to similar image searching or similar image sorting, besides using as steganography. This time, we investigated noise and compression resistance of our method, and conducted experiments for similar image searching and confirmed its effectiveness.

Keywords: steganography, digital watermark, similar image search, template matching, frequency analysis

1. はじめに

近年, 有線・無線ネットワークを流れるデータ量は指数関数的に増大している. 特にマルチメディアデータは, デー

タ量が大きく, 暗号などで処理するには時間がかかり過ぎる. また, 暗号は一度ほどくと, ほどいたデータには何も残っておらず, 複製が作られても出所が分からなくなってしまう. これに対して透かし技術は, オリジナルデータを若干書き換えて透かしを埋め込むか [8], [11], 我々が提案するステガノグラフィ (ANGO [5], [21]) のようにオリジナルデータと切り離せないデータを, 認証機関に登録して著作権を保護する.

埋め込み型の電子透かしは原画像や元データの輝度や色, スペクトルなどに透かし情報を埋め込むため, コンテンツも必ず変更を受ける.

¹ 九州大学

Kyushu University, Fukuoka 819-0395, Japan

² 国立情報学研究所

National Institute of Informatics, Chiyoda, Tokyo 100-0003, Japan

³ 東京理科大学

Tokyo Science University, Katsushika, Tokyo 125-8585, Japan

^{a)} hirokazu.ishizuka@inf.kyushu-u.or.jp

これに対し、ANGO は、「原画像」とは別に「情報抽出ファイル」を用いて、原画像と情報抽出ファイル間の「演算」により「秘密情報」を取り出すもので（図 2 参照）、コンテンツの変更はいっさいない。

ANGO は Zero-watermarking [7], [9], [10] や、フィンガープリンティングの中でも Perceptual (Image) Hash [18], [19] との類似性が指摘されるが、それらにない特徴がある。

Zero-watermarking や Perceptual Hash は一般にまず、コンテンツの特徴を抽出する。その特徴と秘密情報から（2 値パターンの）透かしを生成するのが Zero-watermarking であり、特徴そのもののハッシュ値を抽出するのが Perceptual Hash である^{*1}。

これに対して ANGO の復号は情報抽出ファイルで指定された 2 点の周辺画素の平均値を比較するだけであり、いわゆる特徴抽出処理は行わない。別のいい方をすれば、情報抽出ファイルで指定した画素の座標がすでに特徴を含んだ点であるため、復号が高速に実施できる。この高速性は、4K, 8K テレビなどの高精細な画像や膨大な数のテンプレートマッチングに ANGO を適用した場合に効果がある。また、ステガノグラフィとテンプレートマッチングを同時に実行できることも、最近のビッグデータ処理において有利である。

ステガノグラフィ作成後は Zero-watermarking 同様、認証局に画像、情報抽出ファイルを登録し、画像を公開する。なお、Perceptual Hash に関しては、秘匿（暗号）の役割は暗号化関数（たとえば SHA などのハッシュ関数）に委ねられている [19]。

2. 提案方式の背景

本論文はステガノグラフィ ANGO の紹介とそのノイズ耐性などの特性評価、および ANGO をテンプレートマッチングに応用するという 2 つ事柄を記載する。そのため背景もステガノグラフィ技術の背景と、テンプレートマッチング技術の背景に分けて記載し、最後に両者を同時利用した場合のメリットと利用上の補足事項について述べる。

2.1 ステガノグラフィとしての ANGO

ANGO の類似技術として、フィンガープリンティング技術 [20] の中でも画像を目的とした Perceptual (Image) Hashing, および透かし技術として提案されている Zero-watermarking について述べる。

Perceptual Image Hashing は主に特徴抽出ステージと

認証方法の違いにより、統計ベース手法、関係ベース手法、粗い表現手法、低レベル特徴手法の 4 つのスキームに分類することができる [19]。これらのうち、統計ベース手法以外は、DCT や DWT 変換などの特徴抽出が必要であり、統計ベース手法も、画像の空間領域における統計、たとえば平均値や分散、画像ブロックとヒストグラムの高次モーメントなどの特徴抽出がハッシュ計算時に必要である。ハッシュの計算は入力画像をグレースケールに変換し、それを小さいサイズの画像に圧縮してから DCT などの特徴抽出処理を行うため、計算量は削減されるが、検索対象のすべての画像に対して計算しなければならない [18]。ただし、前もってハッシュ値を計算しデータベース化してあれば、ハッシュ値の比較だけで類似画像が高速に検索できる。Perceptual Hash も一般のフィンガープリンティング技術も、任意のデータを埋め込むのではなく、データのハッシュ値（人間にとってハッシュ値自体の意味はない）を比較して、同じ画像か否かを判別したり、データの改ざんがないことの証明にしたりする。また通常の電子透かしも、マークなどの透かし画像がノイズがあっても判別できるというものであって、それ以上の機能はない。これに対し ANGO は、任意の文章などの傷つきやすい秘密情報を、透かしとして頑健に抽出できる点が他のものと異なる（2.3 節参照）。

Zero-watermarking の具体的方式についていくつか説明する。Zhang ら [9] の方式は、Discrete Wavelet Transform (DWT) により、低解像度成分を抽出しエッジ抽出を行う。次にそのエッジ抽出画像を 3×3 画素ずつに分け、縦、横、斜めのエッジ部分をそれぞれ、01, 00, 10 とし、エッジがない部分を 11 とする符号化を行う。こうして 3×3 画素が 2 ビットずつに符号化された行列を得る。これと、透かし画像をユーザ鍵でスクランブルした行列（彼らは情報行列と呼んでいる）をビットごとに XOR して、疑似透かし行列 (PM) を得る。PM を第三者機関（センタ）に登録して完了する。復号には原画像と PM とユーザ鍵が必要で、まず、符号化行列を得るまで同様に DWT 変換、エッジ抽出を実行する。符号化行列と PM を XOR すれば、情報行列が得られ、それとユーザ鍵から透かし画像を得る。特徴抽出に相当する、DWT 変換、エッジ抽出処理が復号時にも必要である。

Hu ら [10] は、CDMA をベースとした Zero-watermarking を提案している。画像の特徴量として、全ユーザの入力信号とユーザの鍵から抽出されるスペクトル拡散符号の線形和を用いている。具体的には画像を DWT 変換し、その高周波成分の 1 次元アレイを作り、ユーザ鍵をもとにロジスティック写像により生成した番号の Walsh 行列の「行」をスペクトル拡散符号として用いている。特徴抽出としては DWT 変換が必要であり、また前処理としてロジスティック写像の行の選択が必要である。そのほか、Sang ら [7] は、

^{*1} ハッシュは単なるコンテンツのダイジェストであるのに対して、透かしやステガノグラフィはコンテンツに加えて、もう 1 つ、人間が理解できる情報がある点が異なる。一般に、その情報が主でコンテンツがカムフラージュ、つまり副のものをステガノグラフィと呼び、反対にコンテンツが主で、もう 1 つの情報が副のものを透かしと呼んでいる。ANGO はカムフラージュと主情報という分類はできないが、Cardan grille と呼ばれるステガノグラフィ法に近いので、ステガノグラフィに分類してある。

選択した画素値と、対応する空間領域のニューラルネットワークの出力を使って2値パターンを生成している。これもニューラルネットワークが特徴抽出処理に相当し、復号時にも必要である。このように、Zero-watermarkingは、通常、復号時にも作成時同様の特徴抽出処理が必要となる。

ANGOの復号は直接画像中の2点の画素値（もしくはその近傍の画素の平均値）を読み出し比較するだけであり、実質的に特徴抽出の必要がない。

2.2 テンプレートマッチングへのANGOの応用

ステガノグラフィとしてANGOのノイズ耐性実験を実行中、ANGOのノイズ耐性の頑健さにより、ほとんど同じ画像からほぼ同じ秘密情報が抽出されることに気が付いた。これは画像ハッシングの概念とよく似ており、このことからANGOが類似画像検索やテンプレートマッチングに利用できると考えた。しかも画像ハッシングにはない秘密情報を抽出する過程で、同時にその画像が類似しているかどうかを判別できるメリットがある。

テンプレートマッチングは画像解析、画像処理、コンピュータビジョンの中でも重要な技術であり、様々な分野で使われている。たとえば、工場の生産ラインでの製品検査をはじめ、衛星写真や航空写真を元にした飛翔体ナビゲーション技術、顔画像の認識などがすぐに思いつく。

テンプレートマッチング技術はこれまで数多くの方式が提案されており領域ベースマッチングと、特徴ベースマッチングに大別できる[14], [15]。先に説明したPerceptual Hashも利用でき、特徴ベースマッチングの一種と考えることができる。画像の拡大・縮小などに頑健な特徴ベースマッチングがさかんに研究されてきたが、近年、ステレオ立体視や3D画像への応用から領域ベースマッチングにも関心が集まっている[16]。

Xuら[13]は、領域ベースマッチングとして、ランダムにサンプリング点をとるSSDA法[12]を改良し、サンプリング点をあらかじめ固定された点とし、その点のテンプレートと対象画像の比較した結果の誤差を積み上げ、あらかじめノイズなどの状況から決めた閾値と比較することで一致可否かを判断するアルゴリズムを提案している。サンプリング点を固定し、探索間隔を適切に広げることで高速性とノイズに対する頑健性を獲得した述べているが、具体的なサンプリング点の決め方は記載されていない。

Yueら[17]は、フィルタの中央からX状に対称に固定されたサンプリング点を採用し、かつ、それぞれの点は中心から段階的に小さくなる重みを与えた領域ベースのマッチングアルゴリズムを提案している。また、画像の部分的に支配的な色を特徴点として取り入れたり、大まかなマッチングと精細なマッチングを2段階で利用したりして検索を高速化する技術を提案している。これらの技術はテンプレートの画像と検索対象画像の対応する箇所どうしの1対

1の比較が基本である。これに対して、我々が提案する方式は、テンプレートを周波数分析したうえで、そのテンプレートの低周波成分が支配的な点をサンプリング点として抽出し、かつ、サンプリング点単独の比較ではなく、複数のサンプリング点間の相対的な輝度や色の差を比較してマッチングをはかる。

一方、特徴ベースマッチングの1つ、SIFT(Scale-Invariant Feature Transform)を用いて、画像の拡大・縮小に対して不変な特徴としてエッジの頂点部分を抽出し、その周辺を含めベクトル化し、テンプレートマッチングを図る類のものがいくつか提案されている（たとえば文献[14]）。

ANGOは領域ベースのマッチングであり、直接比較はできないが、エッジなどの画像の輪郭を利用するのではなく、大まかな構造物の相対的な形状や輝度（およびカラー）の差異を用いてマッチングを行う。

一般に低周波成分の抽出には時間がかかるが、提案方式は次に示すように前処理としてテンプレート上での解析のみであり、検索対象画像に対しては特徴抽出などの事前処理の必要はない。なお、テンプレートの解析にも3.2節に述べるように高速な手法を提案している。

2.3 ANGOの利用に関する補足

通常、類似画像検索と秘密情報の抽出は2つの別の処理だが、これをANGOは同時に行うことができる。駅や空港などの個人認証において、テンプレートとなる対象者の顔を識別しながら、同時にテンプレートから秘密情報をチェックすることができ、衛星写真をもとに対象地点を特定する際に、同時に検索中の写真の秘密情報を表示することができ、またAR(Aergument Reality)などで現実の背景と、3D地図情報をマッチングをはかりつつ、同時にバイブラインなどの秘密情報を抽出できたりする。

従来の埋め込み型透かしと、ANGOやZero-watermarkingは、著作権保護という目的のためにお互いに補完し合うべきであり、両方を使うことで著作権の強固な保護が可能となる。

一般に画像などのコンテンツでは、複雑な部分は高周波成分が支配的であり、何かが紛れていても気づかれにくい。別の見方をすれば、類似した複雑なパターンに置き換えるなどしても気づかれにくい部分であり、透かしを取り除きやすい部分といえる。反対に低周波成分が支配的な部分は、輝度変化が緩やかな部分で、少しの変化も目立つため、仮に透かしを目立つことなく埋め込めたとしたら、その透かしは取り除きにくくなる。埋め込み型透かしという技術は、こうしたトレードオフの上に成り立つ技術であり[1], [3], [4], [6], Zhangら[9]が指摘しているように、多くの場合、取り除きにくい低周波空間への透かしの埋め込み量は、画像にもよるが十分とはいえない。これに対しANGOやZero-watermarkingは、原画像とは別に情報を

用意することで、画像の低周波空間と結びついた隠蔽情報をいくらでも作成できるため、画像の大部分をひどく破壊しない限り、秘密情報が取り出せなくなることはない。つまり埋め込み型透かしと一緒に利用することで埋め込み型透かしの弱点を補うことができる。

原画像を直接配布することは、ANGO や Zero-watermarking にとって、透かしを上書きされ、不当に著作権を主張される可能性が生じる。また ANGO の場合、完全ではなく、類似した画像からも透かしが抽出できてしまうため、完全性を保証する必要がある場合は、埋め込み型の透かしとの連携が必要となる。一般配布用のコンテンツは埋め込み型透かしを入れたものを使い、著作権を保護する認証局には、原画像と、埋め込み型透かし画像と、情報抽出ファイルとその抽出方法を登録し、認証局に証明してもらおう^{*2}。なお、認証局への登録を安全に行う手段は、信頼できる人物によるハンドキャリーか、暗号通信などの別の安全策が必要である。このように埋め込み型透かしと ANGO などの透かし、暗号通信の3つを組み合わせることで、著作権を強固に保護することができる。

以下、3章では、ANGO のアルゴリズム、要素技術アルゴリズム、復号アルゴリズム、画像検索応用アルゴリズムの4つを紹介し、4章ではこれらアルゴリズムを適用したノイズや圧縮耐性実験および、Caltech 標準画像を用いた類似画像検索実験、テンプレートマッチングの実験結果について報告する。最終5章では、まとめと今後の課題について述べる。

3. 提案アルゴリズム

3.1 ANGO アルゴリズム

ステガノグラフィ・アルゴリズム ANGO は、坂口安吾の小説「アンゴウ」に登場する秘密通信の方式をヒントに提案したもので、「アンゴウ」では、2人が所有する共通の本を介して、ページ番号、行番号、上から何文字目という数字の組が記載された紙片から、秘密の文章を抽出する。(図1)。共通の本があれば、数字の書かれた紙片を交換することで、秘密の通信を次々に行うことができる。これに対して提案方式は、本の代わりに共通の原画像を持つ2者間などで行い、別ファイルで指定された座標の原画像の輝度や色情報を読み出し、指定された演算により秘密情報を抽出するもので、原画像 O と情報抽出ファイル E から、隠ぺい情報 S を抽出するものである (図2)。

ANGO アルゴリズムを以下に記す。ただし、下記 (1-2) では低周波空間を抽出後の2次元画像中の点列を1次元のリストで表現している。つまり1次元リスト $[A, B, C, \dots]$ の

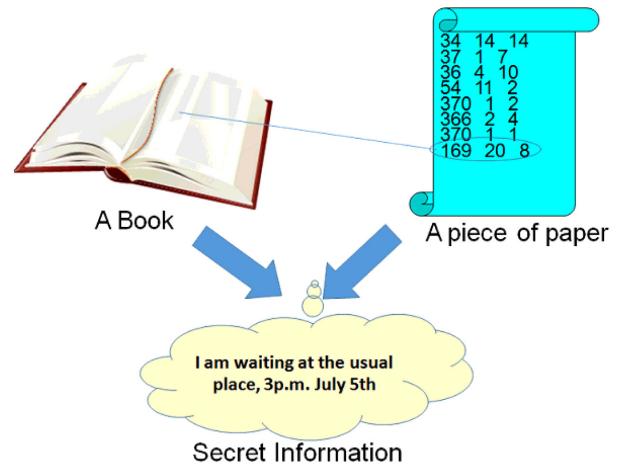


図1 小説中の方法

Fig. 1 Method of the novel.

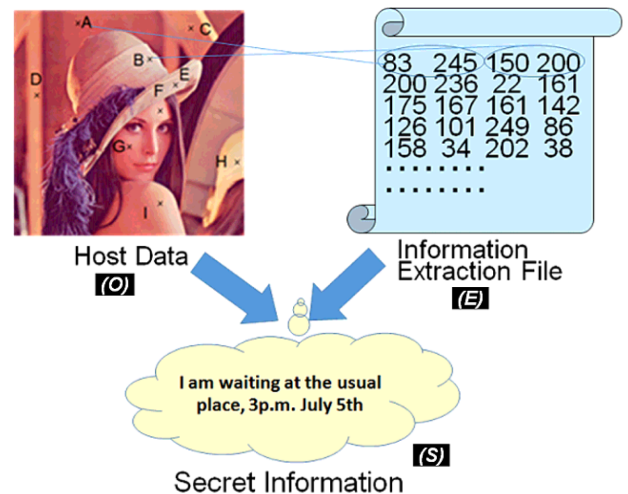


図2 ANGO アルゴリズム

Fig. 2 ANGO algorithm.

A 点は実際には、画像中の (x_1, y_1) で表せ、B 点は (x_2, y_2) で表せる。以下同様にリスト1文字が画像中の1点を表しているものとする。

ANGO アルゴリズム (*1)

- (1-1) 画像と紐付する隠蔽情報を1ビット (b_i) 取り出す。
- (1-2) 乱数を2つ ($R1, R2$) 発生させ、低周波空間の1次元リストから乱数に対応する2点 A, B を選ぶ。
- (1-3) 2点の輝度値の差 $I(A) - I(B) \equiv d$ の絶対値 $|d|$ が、閾値 θ より小さい場合は (1-2) に戻り、そうでなければ (1-4) に進む。
- (1-4) $b_i = 1$ の場合、 $d \geq 0$ なら情報抽出ファイルに A, B と記し、そうでないなら、情報抽出ファイルに B, A と記す。 $b_i = 0$ の場合、 $d < 0$ なら情報抽出ファイルに B, A と記し、そうでないなら、A, B と記す。
- (1-5) (1-1)~(1-4) の処理を隠蔽情報がなくなるまで続ける。

ポイントは、画像の輝度変化の少ない比較的広い低周波空間の内部の点を隠蔽場所として選ぶ点であり、隠蔽情報

^{*2} 埋め込み型の透かしであっても、すでに透かしが埋め込まれているコンテンツに別の透かしを上書きされた場合、埋め込まれた順序は通常は区別できない。しかし原画像があれば、どちらの埋め込みが先かを証明できる。

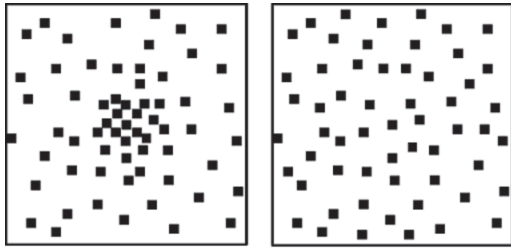


図 3 ガウシアンサンプリングフィルタ (左) と
ランダムサンプリングフィルタ (右)

Fig. 3 Gaussian sampling filter (left) and random sampling filter (right).

を大きな構造どうしの形状と輝度関係に対応させている点である。ここでは記載していないが、輝度の代わりに色情報を利用することもできる。低周波空間の抽出は次節で述べる。

3.2 低周波空間抽出アルゴリズム

広範な低周波空間を見つける方法で、ただちに思いつのが画像をフーリエ変換などで周波数成分に分解する方法である。もしくはそれと同等な空間フィルタ処理（コンボリューション）を行うか、あるいは逆に高周波空間を求め、それを原画像から差し引く方法がある。しかしこれらの方法は 3.3 節に示すように、計算量が多く、時間がかかる^{*3}。

我々が提案する低周波空間の抽出は、図 3 のようなランダムに穴の開いたスパースフィルタを用いるもので、穴の開いた場所の画素値とフィルタ中心の画素値を比較し、その値が近ければカウントアップする。カウンタがあらかじめ設定した閾値を超えたら、フィルタの中央の点を低周波空間と見做す。

白黒画像の場合のアルゴリズムを以下に記す。画像 $I(i, j)$ 、フィルタ $F(x, y)$ とも左上を原点とし、フィルタは簡単のため正方形でサイズは S (奇数) とする。 N 点穴が開いており、フィルタの k 番目の穴の開いた点を (x_k, y_k) とし、カウンタを Co 、閾値を Θ とする。

低周波空間抽出アルゴリズム (*2)

- (2-1) 画像 I の点 (i, j) にフィルタ F の原点を重ね、フィルタの中央にあたる画像 I の輝度値を読み込む ($I(i + \lfloor S/2 + 1 \rfloor, j + \lfloor S/2 + 1 \rfloor)$)。ただし、 S は奇数。
- (2-2) フィルタ上で k 番目の 1 の立つ箇所 (x_k, y_k) に対応する画像 I の輝度値を読み込む ($I(i + x_k, j + y_k)$)。
- (2-3) $I(i + x_k, j + y_k) \approx I(i + \lfloor S/2 + 1 \rfloor, j + \lfloor S/2 + 1 \rfloor)$ ならば $Co = Co + 1$ 、そうでない場合はなにもしない。
- (2-4) もし $(Co > \Theta)$ なら、点 $(i + \lfloor S/2 + 1 \rfloor, j + \lfloor S/2 + 1 \rfloor)$ を低周波空間中の点と見なしファイルに記録し (2-5) へ、そうでなければ (2-1) ~ (2-4) を k が 1 から N (=

^{*3} 最後の高周波空間を用いる方法は、基本的には高速であるが、ある帯域以上のすべての低周波成分が含まれるため、広範な低周波空間を切り出すには、やはり計算量が増加する。

フィルタ上 1 のある箇所の数) になるまで繰り返す。
なお、 N まで計算しても Θ を超えなければ、そこは低周波空間ではないとして (2-5) へ。

(2-5) フィルタを移動し、(2-1) ~ (2-5) の処理を画像 I 全体に施す。

3.3 様々な低周波空間抽出方法の比較

様々な低周波空間の抽出方法の計算量は以下のとおりである。 N をサンプリング数として、時間計算量の見積りはそれぞれ次のとおり。ただし、比較演算は $O(1)$ とした。

- 通常の 2 次元離散フーリエ変換の場合 (たとえば文献 [2] を参照)
- $DFT(N) \propto O(N^4)$
- 入力 2 のべき乗という制約があるが、高速フーリエ変換 (FFT) を適用した場合 (文献 [2] 参照)
- $FFT(N) \propto O((N \log N)^2) = O(2N^2 \log N)$
- コンボリューション法の場合
- $CONV(N) \propto O(N^3)$
- 提案方式
- $ANGO(N) \propto O(N^2)$

これらを比べると提案方式の計算量が小さいことが分かる。8K 映像ではフレームレートも最大 120 fps となり、現在のフル HD の 64 倍のデータを処理しなければならない。画像の特徴抽出という意味では、FFT と提案方式では、約 4 倍 FFT の方が処理が重くなる。また空間計算量としても提案方式は、途中結果を保持するメモリを他の 3 つに比べ大幅に削減でき、ハードウェア資源の消費も少ない。さらに提案方式は、符号化されたデータであっても同様のアルゴリズムを適用し、特徴抽出ファイルが作成できる。一般に低周波空間の検出精度 (位置の正確な精度) と速度はトレードオフの関係にあるが、提案方法は検出した低周波空間の相対的な位置関係のみが重要であり、また多くの場合、低周波空間の比較的中央部分が抽出されるので、検出精度にあまり影響しない。

図 4, 図 5 は、フーリエ変換により抽出された低周波画像を 2 値化したものと、提案方式で抽出した低周波空間を 2 値化したものである。カットした周波数やフィルタ径などが異なり一概に比較はできないが、提案方式が効果的に低周波空間を抽出していることが分かる。

3.4 復号アルゴリズム

復号、すなわち透かし抽出アルゴリズムは以下のとおり (図 6)。

復号アルゴリズム (*3)

- (3-1) 画像と情報抽出ファイルを用意。
- (3-2) 情報抽出ファイルの先頭から 1 行 (2 点) 座標を読み



図 4 帯域通過 FFT 後 2 値化 図 5 提案フィルタの結果
Fig. 4 Binarization after FFT. Fig. 5 Applied our filter.

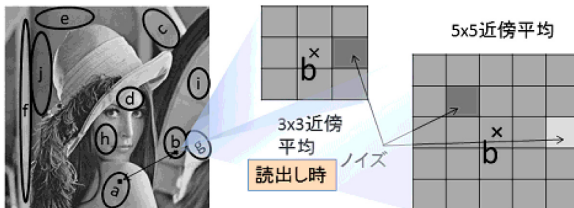


図 6 復号方法の説明
Fig. 6 Explanation of our decoding method.

込む $A(x_1, y_1)$, $B(x_2, y_2)$.

(3-3) ノイズ耐性向上のため, A , B 点およびその周辺 (Ex. 8 近傍とすると) の点の画素値を読み込み平均をとる.

$$\bar{A} = [A(x_1 - 1, y_1 - 1) + A(x_1 - 1, y_1) + A(x_1 - 1, y_1 + 1) + A(x_1, y_1 - 1) + A(x_1, y_1) + A(x_1, y_1 + 1) + A(x_1 + 1, y_1 - 1) + A(x_1 + 1, y_1) + A(x_1 + 1, y_1 + 1)] / 9,$$

$$\bar{B} = [B(x_2 - 1, y_2 - 1) + B(x_2 - 1, y_2) + B(x_2 - 1, y_2 + 1) + B(x_2, y_2 - 1) + B(x_2, y_2) + B(x_2, y_2 + 1) + B(x_2 + 1, y_2 - 1) + B(x_2 + 1, y_2) + B(x_2 + 1, y_2 + 1)] / 9$$

(3-4) $\bar{A} - \bar{B}$ が正なら, 隠蔽情報は 1, 負なら 0. これを情報抽出ファイルをすべて処理するまで実施.

(3-5) 抽出された 0, 1 の情報を文字コードに変換.

復号アルゴリズムで重要なのは, 情報抽出ファイルに書かれた座標の画素値だけでなく, その周辺画素の輝度値 (またはカラー情報) を読み込んで平均値をとることにある. 情報抽出ファイルに記された座標は, 比較的広い低周波空間の内部の点なので, その周辺画素を読み込んで平均をとれば (ex. 3×3 画素平均や, 5×5 画素平均), ノイズに対する耐性を持たせることができる. ただし, 平均値をとる領域が広がれば, 計算量は増加する.

また, 作成される情報抽出ファイルは, 1 行に独立した座標 (数字) が 2 つずつ記載され, それぞれ隠蔽情報 1 ビットに対応するが, 各行すべて独立に座標を選ぶ必然性はない. 前の行の座標との関係で次の点を選ぶようにすれば, n 点の隠蔽情報の関係づけには, $n + 1$ 点の “独立した座標” があるだけでよい.

提案方式の特徴として, 2 点間の輝度差の符号 (正負) で 1 ビットの隠蔽情報が決まるので, 画像全体が一定量輝度

変化した場合も, 秘密情報は取り出せる.

画像全体に作用する拡大, 縮小, 回転などの幾何学変換に対しては, 相対的な輝度や色情報の変更も追従して変化するため, 拡大・縮小係数, 回転角などのパラメータが分かれば, そのパラメータによる変換を施したうえで透かし情報が検出できると考えられる.

提案アルゴリズムは, 画素値の大小により順番を入れ替える単純なものだが, これをより複雑な演算, たとえばアルゴリズム (1-3) の計算を $c\sqrt{I(A)^2 + I(B)^2} \geq 128$ (ただし c は定数) などに変更しても, 情報抽出ファイルを作成できるし, 2 点ではなく 3 点以上の低周波領域の関係 (例: $I(A) - I(B) + 2I(C) \geq 0$ など) に変更しても, 同様な方式が成り立つ. すなわち, 原画像と埋め込み型透かし入り画像, 情報抽出ファイルに, 抽出アルゴリズム加えることで, 秘匿情報をより強固に守ることができる.

3.5 テンプレートマッチングとしての応用

ANGO のテンプレートマッチング応用は, ユーザがテンプレートから抽出した情報を正として他の画像データから抽出した情報と比較し, ビット正解率から類似度を出せばよい. 類似度のメトリックとしては以下の確率 $S(i, j)$ を使用する.

$$S(i, j) = \frac{\#\{\text{total correct relations} : R\}}{\#\{\text{all relations} : W\}} \quad (1)$$

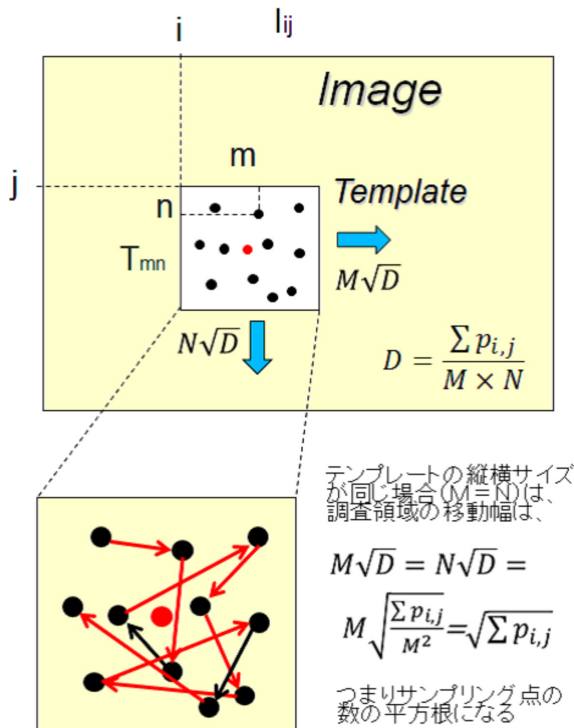
図 7 を用いて説明する.

テンプレート画像を T_{mn} , 調べる対象画像を I_{ij} として, テンプレート上で実施した透かし抽出点を黒いドットで示す. また下の図はテンプレートの拡大図を示し, 赤いリンクと黒いリンクは情報抽出ファイルに照らし合わせた結果として, 正しい関係かそうでないかを表している.

画像の中から, 類似部分を高精度に見つけるには, 1 画素ごとに対象領域を移動して透かし抽出アルゴリズム (*3) を計算すればよいが, 無駄な計算が多くなってしまふ. そこで, 式 (2) で提案するように, 秘密情報量に基づく調査領域のサンプリング密度によって決まる移動幅で調査領域を移動させながら, 大まかに類似箇所候補を選び, 次にその候補をより細かい移動幅で調べるといった 2 段階のアルゴリズムを採用する*4. これは文献 [17] などでも用いられているものだが, 我々の方式は, 調査領域のサンプリング密度から式 (2) によって移動幅を一意に決められる点異なる.

2 次元画像の場合, サンプリング定理から, 提案するランダムサンプリング調査の計算間隔は, 調査領域のサンプリング密度の平方根に比例すると考えられる (比例定数は省略). そこで, 調査領域の移動幅 SW は, サンプリング密度を D , 縦横方向のテンプレートサイズを同じとし

*4 段階的に復号する秘密情報を制限すれば多段階のアルゴリズムも構成できる.



($M = N$), 位置 i, j にあるサンプリング点を $p_{i,j}$ とすると, 以下の式で与えられる.

$$SW \approx M\sqrt{D} = N\sqrt{D} = M\sqrt{\frac{\sum p_{i,j}}{M^2}} = \sqrt{\sum p_{i,j}} \quad (2)$$

つまりテンプレート上の全サンプリング点の総数の平方根を調査領域の移動幅とする.

テンプレートマッチングアルゴリズムは以下のとおり. ただし, あらかじめ透かしが作成され, 式 (2) によってシフト幅 (SW) が決まっていると仮定する.

テンプレートマッチングアルゴリズム (*4)

(4-1) 類似度を調べる領域を定め復号アルゴリズム (*3) を実行し, 類似度 (式 (1)) を計算.

(4-2) 領域を式 (2) に従い SW ずらし, (4-1) を実行. 縦横 SW ずつ離れた間隔で画像全体を調べる.

(4-3) ソートして類似度の大きいところを抽出.

(4-4) (4-3) で求めた類似度の大きい点周辺を, 縦横に微小距離: $\frac{SW}{2}(\frac{SW}{4}, \dots)$ 移動し, 類似度 (式 (1)) を計算し確認.

4. 評価

本章以降は提案方式の性能評価について述べる. まず画質の基準となる PSNR の定義を確認する. サイズ $m \times n$ の原画像 P とノイズが乗った画像 Q があるとき, 平均 2 乗誤差 (Mean Square Error) を次のとおり定義する. i, j は画像中の点の座標であり, $P(i, j), Q(i, j)$ はその点の画像の値 (輝度値) とする.

表 1 ランダムノイズ強度と PSNR

Table 1 Random noise intensity and PSNR.

Random Noise	LENA PSNR	Cameraman PSNR
20	16.24	15.34
30	14.42	13.63
40	13.22	12.35
50	12.24	11.38
60	11.44	10.60
70	10.82	9.93
80	10.18	9.36



図 8 左から原画像, ランダムノイズ印加 30, 50, 80

Fig. 8 Original, random noise applied 30%, 50%, 80% from left.

$$MSE = \frac{1}{mn} \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} [P(i, j) - Q(i, j)]^2 \quad (3)$$

$$PSNR = 10 \log_{10} \frac{MAX_P^2}{MSE} = 20 \log_{10} \frac{MAX_P}{\sqrt{MSE}} \quad (4)$$

MAX_P : 画像の画素データがとりうる最大値. 白黒濃淡画像で 1 ピクセル 8 ビットで表現されているならば, $MAX_P = 255$. 今回実験した画像も 1 ピクセル 8 ビットの BMP 画像を使用した.

ノイズ指標と PSNR の関係は以下の表のとおり. ランダムノイズは, 画像のランダムな場所に, 0~255 階調のノイズをランダムに乗せたものである. たとえばランダムノイズの 80 は画素のうち 80 パーセントがランダムノイズに置き換わったもので, 図 8 の右端にあるように原画像がほぼ分からない状態になる.

4.1 ランダムノイズ耐性

図 8 のランダムノイズの 80 の場合を見てみると, 画像自体が大きくダメージを受けている. しかし, 5×5 画素の平均による読み出しを行うと, なおも 90% 近くのビットが抽出できる. さらに読み出しフィルタのサイズを大きくすれば, ノイズ耐性が向上するものと予想され (図 9), 隠蔽データに誤り訂正符号をつければ, ビット正解率はさらに向上すると考えられる.

4.2 圧縮耐性

次に提案方式の圧縮耐性を評価した. 表 2 に結果を示したように, JPEG により元の画像データを 1.26% に圧縮しても 100% 近く秘密情報が抽出できた (図 11). 表 2 中, BAR (= Bit Accuracy Ratio) (1) と BAR(2) の違いは,

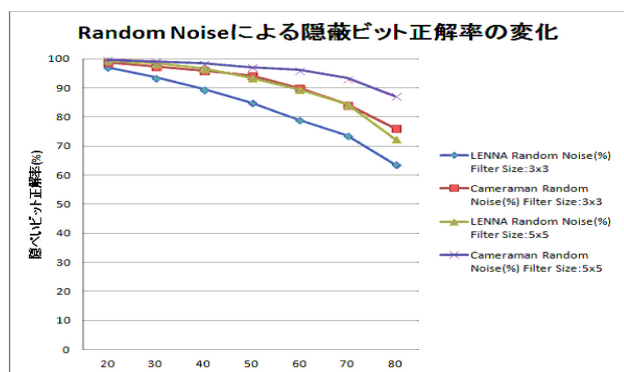


図 9 ランダムノイズと隠蔽ビット正解率の関係

Fig. 9 Relationship of hiding bit accuracy and random noise quantity.



図 10 Lenna の圧縮画像 (左から L1, L3, L7)

Fig. 10 Various compression ratios (L1, L3, L7 from left).

表 2 提案方式の画像圧縮耐性 (BAR(1): 3×3 , BAR(2): 5×5 近傍抽出)Table 2 Image compression resistance (BAR(1): 3×3 , BAR(2): 5×5 neighbors extraction).

ID	サイズ (KB)	圧縮率 (%)	BAR(1)	BAR(2)
L1	0.830	1.26	99.50	99.53
L2	0.966	1.46	99.78	99.44
L3	1.72	2.61	99.69	100.00
L4	2.40	3.64	100.00	100.00
L5	3.91	5.92	99.86	99.87
L6	4.92	7.45	100.00	100.00
L7	5.11	7.74	100.00	100.00
L8	6.95	10.53	99.86	100.00
L9	9.88	14.97	100.00	100.00
L10	11.6	17.58	100.00	100.00
L11	14.3	21.67	100.00	100.00
L12	27.6	41.82	100.00	100.00
L13	40.1	60.76	100.00	100.00
L14	42.8	64.85	100.00	100.00

読み出すときの平均をとる領域サイズが 3×3 か 5×5 の違いである。

4.3 類似画像検索への応用

ANGO の類似画像検索性能を調べるため、標準画像、Caltech-101 中の図 14 に示した 50 種の自動車画像から類似画像を抽出する実験を行い、その結果をグラフにまとめたのが、図 12, 図 13 である。図 12 は図 14 の 15 番目の画像をテンプレートとして、他の画像との類似度を式

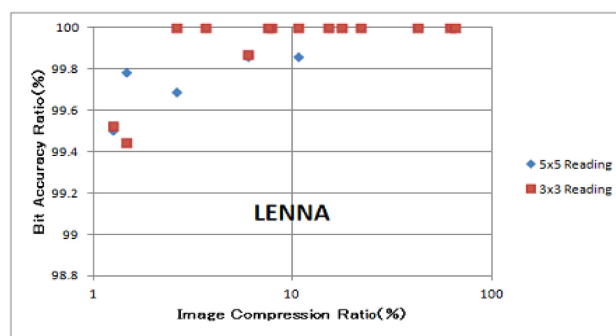


図 11 様々な圧縮率における秘密情報のビット抽出精度

Fig. 11 Bit extraction accuracy of secret information in various compression ratios.

(1) で計算したものである。また図 13 は図 14 の 1 番目の画像をテンプレートとして同様に評価したものである。なお、図 14 は左上から右下へ順番に 1~50 番とする。グラフの中の点線は平均値, $\pm 1\sigma$, $\pm 2\sigma$ を表す。前者は平均 48.44, 標準偏差 11.40, 後者は平均 50.23, 標準偏差は 18.39 であった。画像によって大きく標準偏差が異なるが、正解の画像は両者とも 2σ 以上離れており、上位 2% 以内の類似度として抽出できた。

4.4 テンプレートマッチング

画像 Lenna 中の部分画像によるテンプレートマッチングを実施した。これはテンプレート画像 (図 16, サイズ: 80×80 画素, 8 ビット) を対象画像 (図 15, サイズ: 256×256 画素, 8 ビット) の中から探すというもので、式 (2) で与えた調査領域の移動幅についての検証を行う目的もある。図 17 がその結果であり、x, y 軸は画像の横縦方向に対応しており、z 軸 (縦軸) は部分画像が一致した確率である。図 17 の上に 1 点突き出た赤い点 (矢印の先) がマッチングポイントである。アルゴリズムの 2 段階目の詳細確認作業により、当該点が正しく抽出できていることを確認した。このとき、画像全体の中のテンプレート画像の一致確率の平均は 0.5251 であり、標準偏差は 0.1178 であった。

一方、OpenCV の matchTemplate 関数を使って同様の評価を実施した [23] (正確には OpenCV 関数を画像処理ソフトウェア ImageJ を通して実施した)。ただし、テンプレート画像は表 3 の左端のものであり、Lenna の右上の帽子のあたりを切り取ったものである。同関数は一致度として、差の 2 乗和や差の絶対値和など次の 6 つのメトリックが利用できる。

1. SD: Square Difference
2. NSD: Normalized Square Difference
3. CC: Cross Correlation
4. NCC: Normalized Cross Correlation

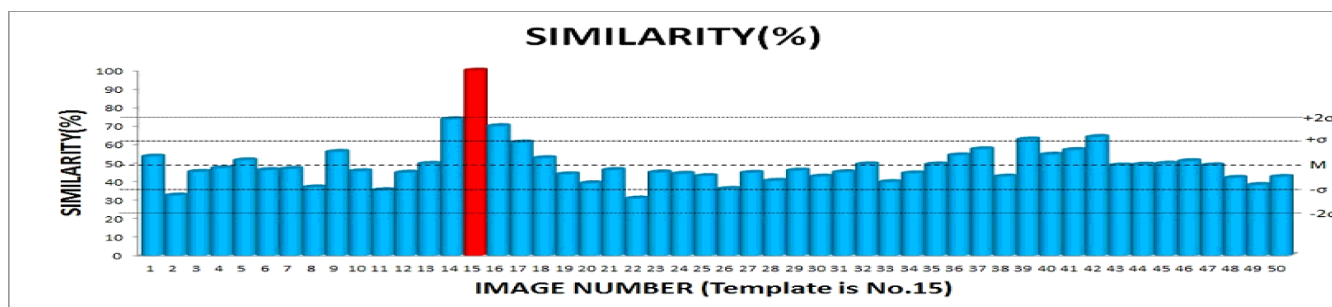


図 12 15 番の画像から見た一致確率
Fig. 12 Matching probability viewed from No.15.

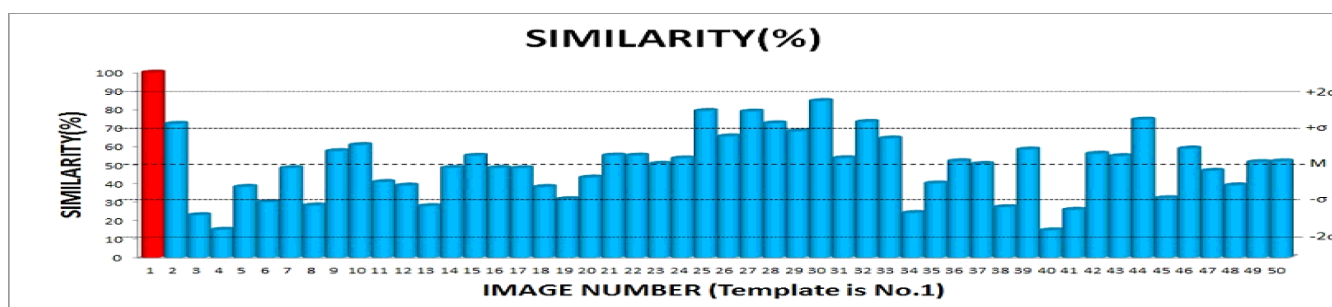


図 13 1 番の画像から見た一致確率
Fig. 13 Matching probability viewed from No.1.



図 14 Caltech-101 標準画像（白黒の車画像）：50 画像
Fig. 14 Caltech-101 standard images (car_side): 50 images.



図 15 検索対象画像
Fig. 15 Source image.



図 16 テンプレート画像
Fig. 16 Template image.

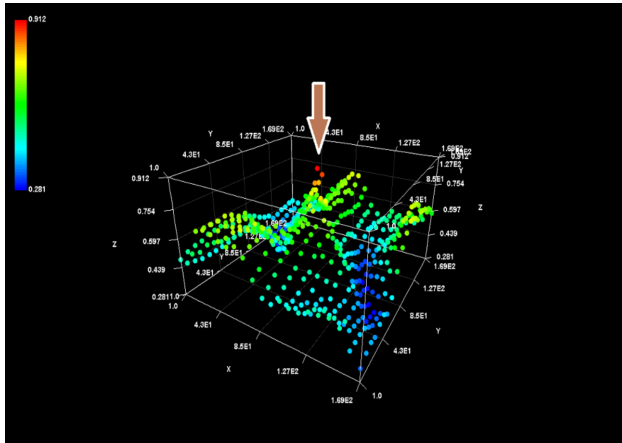


図 17 部分画像の一致確率
Fig. 17 Matching probability of the partial image.

5. CCC: Correlation Coefficient
6. NCCC: Normalized Correlation Coefficient

それぞれの定義は以下のとおり．ただし，検索対象画像とテンプレートの輝度値を $I(x, y)$, $T(x', y')$ ，テンプレートの縦横サイズを h , w とする．

$$SD(x, y) = \sum_{x', y'} (T(x', y') - I(x + x', y + y'))^2 \quad (5)$$

$$NSD(x, y) = \frac{\sum_{x', y'} (T(x', y') - I(x + x', y + y'))^2}{\sqrt{\sum_{x', y'} T(x', y')^2 \cdot \sum_{x', y'} I(x + x', y + y')^2}} \quad (6)$$

$$CC(x, y) = \sum_{x', y'} (T(x', y') \cdot I(x + x', y + y')) \quad (7)$$

$$NCC(x, y) = \frac{\sum_{x', y'} (T(x', y') \cdot I(x + x', y + y'))}{\sqrt{\sum_{x', y'} T(x', y')^2 \cdot \sum_{x', y'} I(x + x', y + y')^2}} \quad (8)$$

$$CCC(x, y) = \sum_{x', y'} (T'(x', y') \cdot I(x + x', y + y')) \quad (9)$$

ただし，

$$T'(x', y') = T(x', y') - \frac{1}{w \cdot h} \cdot \sum_{x'', y''} T(x'', y'') \quad (10)$$

表 3 ノイズのある部分画像（Lenna 右上帽子周辺）の検出実験
Table 3 Detecting experimentation of partial noisy images.

Image	Noise	Square Difference	Normalized Square Difference	Normalized Cross Correlation	Correlation Coefficient	Normalized Correlation Coefficient	Our Method
	0	○	○	○	○	○	○
	10	○	○	○	○	○	○
	30	○	○	○	○	○	○
	50	○	○	○	○	○	○
	60	×	○	×	○	○	○
	70	×	×	×	○	○	○
	80	×	×	×	○	○	—
	90	×	×	×	○	○	—

$$I'(x + x', y + y') = I(x + x', y + y') - \frac{1}{w \cdot h} \cdot \sum_{x'', y''} I(x + x'', y + y'') \quad (11)$$

そして最後，NCCC は，

$$NCCC(x, y) = \frac{\sum_{x', y'} (T'(x', y') \cdot I'(x + x', y + y'))}{\sqrt{\sum_{x', y'} T'(x', y')^2 \cdot \sum_{x', y'} I'(x + x', y + y')^2}} \quad (12)$$

というメトリックを使って評価される．なお，CC: Cross Correlation が不自然な結果のため，実験から除外した．

テンプレート画像にノイズが乗った場合について，表 3 に結果を示している．左端の画像がノイズの乗った画像であり，各メトリックを使った結果および，ANGO の結果を表示した．

表 3 から，提案方式は OpenCV のテンプレートマッチング関数 6 種のうち（実験できたのは 5 種），Square Difference, Normalized Square Difference, Normalized Cross Correlation 以上で，Correlation Coefficient や Normalized Correlation Coefficient と同程度かそれ以下と判明した．ただし，表中の提案方式の“—”は，判別の前段階でランダムノイズが 80%以上になると，高周波成分が強くなり，フィルタが低周波成分を検出できないことに起因する．低周波検出フィルタの判別閾値を下げ，さらに読み出し時の周辺領域のサイズを広げると頑健性を改善できると予想される．しかし，80%以上のランダムノイズが乗った画像はほぼ判読は不可能なため，そもそも類似しているかどうかを判別すること自体に意味がないとの議論もある．

5. まとめと今後の研究について

提案方式のアルゴリズムについて述べ，Perceptual Hash や Zero-watermarking との違いについて述べた．さらに提

案方式のノイズ、圧縮耐性を示した。また提案方式の要素技術について、ランダムもしくはガウシアン分布状にサンプリング点をとるフィルタを提案し、サンプリング点の輝度値の比較だけで低周波空間が把握できることを述べた。厳密な周波数解析に比べ、計算量的に軽く、電子透かしやステガノグラフィの要素技術として利用できることを示した。

一方、フーリエ変換のような複雑な演算を神経回路網の構造で実現するのは難しいが、提案方式はスパースな比較演算だけで低周波空間を把握でき、神経回路網としても簡単に構成できる。近年画像認識で注目されているディープラーニング[22]の中で、最大値を保持するプーリング層・畳込み層の機能と構造に関して提案フィルタの機能と構造との関係を今後調べていく予定である。

さらに、ステガノグラフィアルゴリズムとして提案していたANGOを、テンプレートマッチングに応用することを提案した。実験はテンプレートマッチング単独で実施したが、ステガノグラフィとの同時利用のメリットについても述べた。テンプレートマッチングとしては復号アルゴリズムにおいて、調査領域をサンプリング密度の平方根に比例した量だけ移動させ、2段階目で詳細に調べる効率的なアルゴリズムを提案した。実験の結果、少なくとも同じ画像が含まれている場合は、正解の画像は平均から $2\sim 2.5\sigma$ 以上離れており、誤り率は2%以下であり、また部分画像のマッチング実験でも、OpenCVなどの標準的な領域ベースマッチングと比べても同等の抽出精度が得られることが確認できた。

謝辞 本研究は、国立情報学研究所の「公募型共同研究・（自由型）研究課題番号22」の成果として実施したものである。また本論文を査読いただいた方からは、貴重な時間を割いて丁寧に読んでいただき、大変有益なコメントをいただいた。ここに感謝申し上げます。

参考文献

- [1] Lancini, R., Mapelli, F. and Tubaro, S.: A Robust Video Watermarking Technique in the Spatial Domain, *VIPromCom-2002, 4th EURASIP*, pp.251–256 (2002).
- [2] 金谷健一：これなら分かる応用数学教室，共立出版(2003).
- [3] Suhail, M.A. and Obaidat, M.S.: Digital Watermarking-Based DCT and JPEG Model, *IEEE Trans. instrumentation and measurement*, Vol.52, No.5 (2003).
- [4] Nikolaidis, A. and Pitas, I.: Asymptotically Optimal Detection for Additive Watermarking in the DCT and DWT Domains, *IEEE Trans. image processing*, Vol.12, No.5 (2003).
- [5] Ishizuka, H., Nishioka, T., Hasegawa, T. and Tsurumaru, T.: An Evaluation of a Digital Steganographic Method (ANGO), *SCIS2005* (in Japanese) (2005).
- [6] Bao, P. and Ma, X.: Image Adaptive Watermarking Using Wavelet Domain Singular Value Decomposition, *IEEE Trans. Circuits and Systems for Video Technology*, Vol.15, No.1 (2005).
- [7] Sang, J., Liao, X. and Alam, M.S.: Neural network based zero-watermarking scheme for digital images, *Optical Engineering*, Vol.45, No.9 (2006).
- [8] Cheddad, A., Condell, J., Curran, K. and Kevitt, P.M.: Digital image steganography: Survey and analysis of current methods, *Signal Processing*, pp.727–752 (2010).
- [9] Zhang, L., Cai, P., Tian, X. and Xia, S.: A Novel Zero-watermarking Algorithm Based on DWT and Edge Detection, *4th International Congress on Image and Signal Processing* (2011).
- [10] Hu, M., Tian, X. and Xia, S.: Robust Digital Image Zero-watermarking Based on CDMA Technology, *Proc. 4th International Congress on Image and Signal Processing* (2011).
- [11] Chanu, Y.J., Singh, K.M. and Tuithung, T.: Image Steganography and Steganalysis: A Survey, *International Journal of Computer Applications*, Vol.52, No.2 (2012).
- [12] Barnea, D.I. and Silverman, H.F.: A Class of Algorithm for Fast Digital Image Registration, *IEEE Trans. Comput.*, Vol.c-21, No.2 (1972).
- [13] Xu, X. and Zhang, J.: The Method of Image Matching by Taking Every Fixed Match Pixel, *5th International Symposium on Computational Intelligence and Design (ISCID)* (2012).
- [14] 伊藤康一，高橋 徹，青木孝文：高精度な画像マッチング手法の検討，第25回信号処理シンポジウム(2010).
- [15] Babbar, G., Bajaj, P., Chawla, A. and Gogna, M.: Comparative study of image matching algorithm, *International Journal of Information Technology and Knowledge Management*, Vol.2, No.2 (2010).
- [16] Joglekar, J. and Gedam, S.S.: Area Based Image Matching Methods - A Survey, *International Journal of Emerging Technology and Advanced Engineering*, Vol.2, No.1 (2012).
- [17] Yue, G. and Y.X.: An Aera based Image Matching Algorithm and Its Implementation, *3rd World Congress on Software Engineering* (2012).
- [18] Zauner, C.: Implementation and Benchmarking of Perceptual Image Hash Functions, eingereicht am Fachhochschul-Masterstudiengang (2010), available from <http://www.phash.org/docs/pubs/thesis.zauner.pdf>.
- [19] Hadmi, A., Puech, W., Sad, B.A.E. and Ouahman, A.A.: Perceptual Image Hashing, Watermarking, Vol.2, Dr. Gupta, M.D. (Ed.), ISBN: 978-953-51-0619-7, 2012, available from <http://cdn.intechopen.com/pdfs/36921.pdf>.
- [20] 古賀久志：ハッシュを用いた類似検索技術とその応用，2014, *IEICE Fundamentals Review*, Vol.7, No.3 (2014).
- [21] Ishizuka, H., Echizen, I., Iwamura, K. and Sakurai, K.: A Zero-watermarking-like Steganography and Potential Applications, *Proc. 10th International Conference on Intelligent Information Hiding and Multimedia Signal Processing (IIHMSP2014)*, pp.459–462 (Aug. 2014).
- [22] Zeiler, M.D. and Fergus, R.: Visualizing and Understanding Convolutional Networks, LNCS 8689, *2014 International Conference on Engineering of Intelligent Systems* (2006).
- [23] available from http://docs.opencv.org/2.4/doc/tutorials/imgproc/histograms/template_matching/template_matching.html



石塚 裕一

1986 年東京理科大学理学部一部物理学専攻卒業，同年三菱電機株式会社入社，情報電子研究所，通信・放送機構，情報通信研究機構出向を経て，現在，情報技術総合研究所所属．2011 年より九州大学大学院システム情報科学府

博士課程にも在籍．ニューラルネットワーク，画像認識，電子透かし，量子暗号等の開発に従事．電子情報通信学会会員．



越前 功（正会員）

1997 年東京工業大学大学院理工学研究科修士課程修了（応用物理学）．同年日立製作所入社，システム開発研究所を経て，現在，国立情報学研究所コンテンツ科学研究系教授．総合研究大学院大学複合科学研究科情報学専攻

教授を兼務．2010 年ドイツ・フライブルグ大学客員教授．2011 年ドイツ・マルティン・ルター大学（ハレ大学）客員教授．コンテンツセキュリティの教育研究に従事．博士（工学）．2005 年・2014 年情報処理学会論文賞，2006 年 IEEE IHH-MSP06, Best Paper Award, 2010 年映像情報メディア学会藤尾フロンティア賞，画像電子学会画像電子技術賞，2011 年情報処理学会長尾真記念特別賞，2014 年ドコモ・モバイル・サイエンス賞，2016 年情報セキュリティ文化賞各受賞．IEEE, ACM, 映像情報メディア学会，画像電子学会各会員．



岩村 恵市（正会員）

1958 年生．1980 年九州大学工学部情報工学科卒業．1982 年同大学大学院情報工学研究科修士課程修了．同年キャノン（株）入社．1994 年東京大学博士（工学）．現在，東京理科大学工学部電気工学科教授．主に符号理論，

並列処理，情報セキュリティ，電子透かしの研究に従事．IEEE, 電子情報通信学会，情報ハイディングおよびその評価基準（IHC）研究会委員長．本会フェロー．



櫻井 幸一（正会員）

1988 年九州大学大学院工学研究科応用物理学専攻修士課程修了．同年三菱電機（株）入社．現在，九州大学大学院システム情報科学研究院情報学部門教授．2004 年より九州システム情報技術研究所第 2 研究室（現，九州先端

科学技術研究所・情報セキュリティ研究室）室長兼任．博士（工学）．2000 年情報処理学会坂井特別記念賞．2000 年，2004 年情報処理学会論文賞．2005 年第 1 回 IPA 賞受賞．2012 年第 26 回独創性を拓く先端技術大賞経済産業大臣賞（企業・産・学部門最優秀賞）受賞．日本数学会，応用数理学会，電子情報通信学会，IACR, ACM, IEEE 各会員．