

博士論文

パイロット信号による攻撃推定を導入した
幾何攻撃に堅牢な電子透かし法

(Robust Digital Watermarking Method against
Geometric Attacks Using Pilot Signal-Based
Attack Estimation)

2026年 3月

河野綸華

山口大学大学院 創成科学研究科

目次

第 1 章	序論	5
1.1	背景	5
1.2	電子透かし法の分類	6
1.2.1	透かし情報	6
1.2.2	画像の可逆性	7
1.2.3	ブラインド方式	8
1.2.4	攻撃耐性	10
1.3	研究の位置付け	13
第 2 章	パイロット信号による拡大率推定を用いた拡大縮小に堅牢な電子透かし法	15
2.1	本研究の貢献	16
2.2	DFT の性質	17
2.3	透かし情報の埋め込み	17
2.3.1	透かし情報の構成	19
2.3.2	埋め込み領域	19
2.3.3	透かし情報の埋め込み	22
2.4	透かし情報の抽出	23
2.4.1	抽出領域と透かし候補	25
2.4.2	符号語の推定	26
2.5	パイロット信号を用いた拡大率の推定	26
2.5.1	パイロット信号の埋め込み	27
2.5.2	拡大率の推定	28
2.6	計算機シミュレーション	32
2.6.1	推定拡大率の評価	33
2.6.2	推定メッセージの評価	33
2.6.3	画質の評価	35
2.6.4	先行研究との比較	38
2.7	まとめ	38
第 3 章	パイロット信号を用いた幾何変換行列の推定	40
3.1	本研究の貢献	41
3.2	パイロット信号の埋め込み	41

3.3	変換行列の推定	42
3.3.1	抽出信号の検出	44
3.3.2	ラドン変換	44
3.3.3	検出角度の検出	45
3.3.4	検出間隔の特定	48
3.3.5	変換行列の推定	49
3.4	計算機シミュレーション	51
3.4.1	実験条件	52
3.4.2	格子間隔の決定	52
3.4.3	単一攻撃の推定変換行列	55
3.4.4	複合攻撃の推定行列	64
3.5	攻撃推定による透かし情報の評価	68
3.5.1	実験条件	72
3.5.2	画質評価	72
3.5.3	単一攻撃に対する評価	72
3.5.4	複合攻撃に対する評価	73
第4章	まとめ	79

目 次

1.1	一般的な電子透かし法における埋め込みの流れ	7
1.2	量子化ステップ $\Delta = 10$, 2 値の場合の QIM の埋め込み	9
1.3	量子化ステップ $\Delta = 10$, 2 値の場合の QIM の抽出	9
1.4	極値の探索方法	11
2.1	提案手法の概要	16
2.2	透かし情報の埋め込み手順	18
2.3	透かし情報の構成	20
2.4	SIFT 特徴量と埋め込み領域	21
2.5	トラックとセクタ	22
2.6	透かし情報の抽出手順	24
2.7	2 値のパイロット信号	28
2.8	パイロット信号の推定手順	29
2.9	スケーリング率の推定手順	30
2.10	拡大率が 0.5 – 3.0 倍のときの相対誤差	34
2.11	ステゴ画像を 0.7 – 1.3 倍に拡大縮小した後に Full HD サイズにトリミングした場合のメッセージの BER	36
2.12	トリミングサイズ毎のメッセージの BER	37
3.1	3 値のパイロット信号	42
3.2	攻撃の推定手順	43
3.3	3 値の抽出信号の例	44
3.4	ラドン係数の例	46
3.5	ラドン係数の模式図	46
3.6	ラドン係数の処理の例	47
3.7	変換行列による座標変換	50
3.8	線分 OA^0, OB^0 と検出間隔 γ_v, γ_h 及び角度 α, β の関係	51
3.9	高画素数画像 (4608 × 3456 画素)	53
3.10	低画素数画像 (768 × 512 画素または 512 × 768 画素)	54
3.11	高画素数画像における格子間隔 G 毎の相対誤差 E	56
3.12	低画素数画像における格子間隔 G 毎の相対誤差 E	57
3.13	格子間隔に対する PSNR	58

3.14	高画素数画像における拡大率 S_y 毎の相対誤差 E : : : : : :	60
3.15	低画素数画像における拡大率 S_y 毎の相対誤差 E : : : : : :	61
3.16	高画素数画像における回転角 θ_r 毎の相対誤差 E : : : : : :	62
3.17	低画素数画像における回転角 θ_r 毎の相対誤差 E : : : : ~~~~~	63
3.18	高画素数画像における剪断角 θ_y 毎の相対誤差 E : : : : ~~~~~	65
3.19	低画素数画像における剪断角 θ_y 毎の相対誤差 E : : : : ~~~~~	66
3.20	複合攻撃によって劣化した画像の例 : : : : ~~~~~	67
3.21	高画素数画像における複合攻撃毎の相対誤差 E : : : : ~~~~~	69
3.22	低画素数画像における複合攻撃毎の相対誤差 E : : : : ~~~~~	70
3.23	攻撃を受けた画像とその逆変換画像の例 : : : : ~~~~~	71
3.24	各拡大率毎の透かし情報の BER : : : : ~~~~~	74
3.25	各回転角毎の透かし情報の BER : : : : ~~~~~	75
3.26	各回転角毎の透かし情報の BER : : : : ~~~~~	76
3.27	複合攻撃に対する透かし情報の BER : : : : ~~~~~	78

第1章 序論

1.1 背景

SNSなどで画像の不正利用や海賊版の問題が深刻化している。これにより、デジタルコンテンツを保護するための技術である電子透かし法が注目されている。電子透かし法 [1] とは、静止画や動画、音声などのデジタルコンテンツに他の情報を秘密裏に埋め込む技術である。特に、画像に対して情報を埋め込む技術を画像電子透かし法と呼ぶ。SNSなどで投稿する画像に事前に所有者の ID や署名を埋め込むことによって、画像を保護することが可能である。このような埋め込む情報を透かし情報と呼び、透かし情報を埋め込んだ画像をステゴ画像と呼ぶ。例えば、不正利用された画像から情報を検出することによって、画像の真の所有権を主張することが可能になる。しかしながら、多くの海賊版コンテンツは原画像を拡大縮小や回転、剪断、さらに、トリミングといった加工によって原画像を劣化させることで不正利用の発覚を免れようとするほか、画像を保存する際に圧縮される場合がある。このような加工や圧縮といった画像への攻撃によって、透かし情報が消失してしまったり、検出が困難になる可能性がある。

透かし情報を埋め込む際に考慮する点として、透かし情報の堅牢性と透かし情報の埋め込み容量及び知覚困難性が挙げられる。一般的に、画像に対して透かし情報を強く埋め込むほど、ステゴ画像が劣化しても透かし情報が容易に抽出できる。しかしながら、透かし情報を強く埋め込むほど画質が劣化する。また、画像に埋め込む透かし情報の長さが長いほど画質が劣化する。これらの要因によって透かし情報の埋め込み位置が容易に知覚できるようになると、悪意あるユーザーによって透かし情報が消される可能性もある。そのため、これらの点を考慮しつつ、様々な攻撃に対して堅牢な電子透かし法を検討する必要がある。

図 1.1 に一般的な電子透かし法における埋め込み手順を示す。任意のメッセージを透かし情報として埋め込むことができる。埋め込み段階では、まず最初にメッセージから透かし情報を生成する。透かし情報は、メッセージを直接透かし情報として扱う場合や、誤り訂正符号などを用いてメッセージに冗長性を付加したものをを用いる場合がある [2, 3, 4]。次に、原画像において埋め込みドメインを決

定する。埋め込みドメインには主に空間領域または周波数領域が用いられる。電子透かし法において空間領域への埋め込みとは、画像の画素値への埋め込みを表す。空間領域へ透かし情報を埋め込むメリットとして処理が容易であることが挙げられるが、圧縮やフィルタリング等の処理によって埋め込んだ情報が容易に消えてしまう。また、幾何攻撃によって画像が劣化すると、埋め込み位置が攻撃強度に応じて変化するため、透かし情報を抽出するために位置同期が必要となる。更に、視覚的に埋め込み位置がわかりやすいというデメリットがある。一方で、周波数領域とは画像を離散コサイン変換 (Discrete Cosine Transform: DCT) [5, 6] や離散フーリエ変換 (Discrete Fourier Transform: DFT) [7] などを用いて周波数成分に変換した領域を表す。周波数領域へ透かし情報を埋め込むメリットとして、圧縮などの攻撃によって透かし情報が消えにくいことや、手法によっては幾何的に堅牢であることが挙げられる。しかしながら、空間領域と比較すると計算コストがかかる。また、幾何攻撃に対して堅牢とされる手法であっても、複数の攻撃を加えた場合には透かし情報を検出できない場合がある。次に、画像に対して透かし情報を埋め込むために加法的埋め込み [8] や量子化インデックス変調 (QIM) [9] などが用いられる。最終的に得られた画像のことをステゴ画像と呼ぶ。抽出段階では、ステゴ画像から抽出処理を経て透かし情報を得る。ここで、透かし情報を生成する際に誤り訂正符号などを用いていた場合は、復号することでメッセージを得る。

以降の節で電子透かし法の分類について述べる。

1.2 電子透かし法の分類

1.2.1 透かし情報

画像に埋め込む透かし情報の量に応じて異なる手法が適用される。透かし情報の有無の判別を行う手法を 1 ビット電子透かし法 [3, 10] と呼ぶ。この手法では透かし情報の抽出時に、あらかじめ保持している透かし情報が検出されるかどうかを判定することによって、画像の真贋を判定することが可能である。埋め込む際に 1 ビットの透かし情報を冗長化するため、透かし情報の劣化に堅牢であるというメリットがある。一方で、ID や署名などの複数ビットの情報を埋め込む手法を多ビット電子透かし法と呼ぶ。この手法では、画像が不正利用された際に流出元を追跡したり、画像の管理を行うことが可能である。ただし、1 ビット電子透かし法と比較すると埋め込む情報が多いため、画像がより劣化してしまうと言うデメリットがある。多ビット電子透かし法では、埋め込みたい情報をメッセージと呼び、符号化された情報を透かし情報と呼んで区別する。その他の手法として、透かし

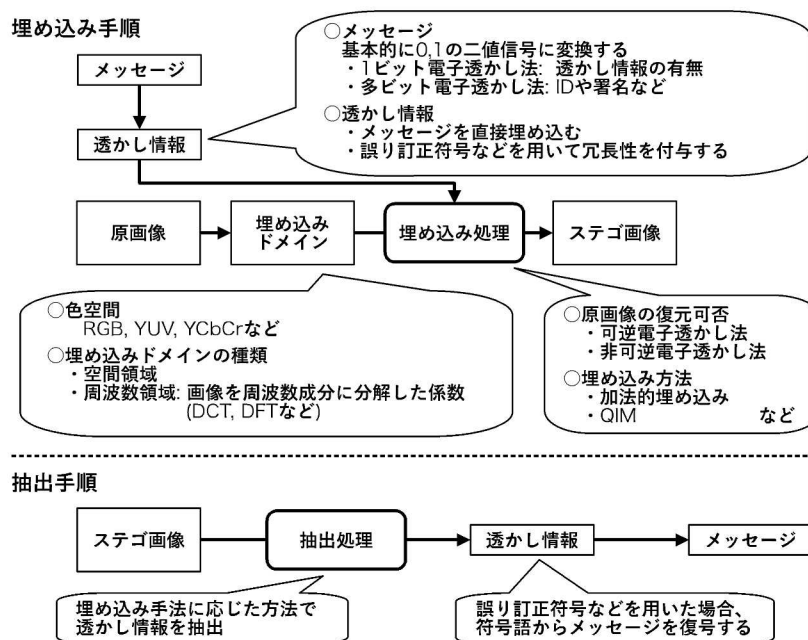


図 1.1: 一般的な電子透かし法における埋め込みの流れ

情報をコンテンツに直接埋め込まないゼロビット電子透かし法 [11, 12] がある。この手法では、画像の特徴量と透かし情報を組み合わせた情報を鍵として保持する。抽出時にはステゴ画像と鍵を用いて透かし情報を抽出する。ゼロビット電子透かし法のメリットとして、画像が劣化しないと言う点が挙げられる。したがって、医療用などの品質が重要となる画像の管理や保護に用いられる。しかしながら、画像毎に異なる鍵が必要となるため、大量の画像を管理する際には全ての鍵を保持する必要があると言うデメリットがある。この欠点を解決した連想電子透かし法 [13, 14] が提案されている。

1.2.2 画像の可逆性

一般的な電子透かし法では、一度画像に透かし情報を埋め込むと、ステゴ画像を埋め込み前の状態に戻すことはできない。そのため、医療用画像などの画像の品質が重要視される場合に可逆電子透かし法 [15] が用いられる。しかしながら、復元可能にするために埋め込み量が制限されてしまう点や、後述する攻撃に対して脆弱であると言う問題点がある。

SNSなどで画像を保護する際には、画質をなるべく維持する必要がある。一方で、不正利用され

る際に攻撃によって劣化するため、可逆電子透かし法は SNS などで投稿される画像の不正利用対策には不適である。

1.2.3 ブラインド方式

透かし情報を検出する方法には非ブラインド方式とブラインド方式の 2 種類がある。非ブラインド方式とは、透かし情報の抽出の際に原画像の情報を必要とする手法である。具体的には、透かし情報の埋め込み時に利用した、原画像の特徴点 [16] やウェーブレット係数 [17] などを透かし情報の抽出に用いる手法である。埋め込み手法には加法的な埋め込みが使われるため、透かし情報を容易に抽出可能である。非ブラインド方式の利点として、原画像情報を参照することによって、攻撃によって劣化したステゴ画像からも容易に透かし情報を抽出することが可能である。また、透かし情報を強く埋め込まなくても透かし情報を抽出可能なため、ブラインド方式よりも画質劣化を抑えられる。一方で、ブラインド方式とは透かし情報の抽出の際に原画像の情報を必要としない手法である。ブラインド方式の電子透かし法とは原画像を必要としない埋め込み手法の一つである。量子化インデックス変調 (Quantization Index Modulation: QIM) [9] 等を用いて透かし情報を埋め込む。QIM は画素値等を量子化することによって 0 以上の自然数を埋め込む手法である。図 1.2 に QIM の埋め込み処理を示す。画素値を I とし、透かし情報を w とし、ステップ幅を Δ とすると、埋め込み後の画素値 I^0 は

$$I^0 = 2\Delta \left(\left\lfloor \frac{I}{2\Delta} - \frac{w}{2} + 0.5 \right\rfloor + \frac{w}{2} \right); \quad (1.1)$$

で求められる。図のように、ステップ幅 Δ で画素値を量子化し、各ステップに対して交互に透かし情報の値を割り当てる。画素値を透かし情報 w に対応する最も近いステップの値にずらすことによって透かし情報を埋め込むことができる。図 1.3 に QIM の抽出処理を示す。画素値 $\hat{I}$ から抽出する場合、透かし情報 w^0 は

$$w^0 = \left\lfloor \frac{\hat{I}}{\Delta} + 0.5 \right\rfloor \bmod 2; \quad (1.2)$$

で表される。図のように、画素値の値がどのステップに属しているのかを判別することによって透かし情報を抽出する。非ブラインド方式では画像毎に対応した原画像情報を保持している必要があるため、大量の画像の管理には適していない。したがって、本研究ではブラインド方式に着目する。ブラインド方式の場合、特に幾何攻撃によって画像が劣化すると透かし情報の位置の検出が困難となるため、工夫が必要となる。

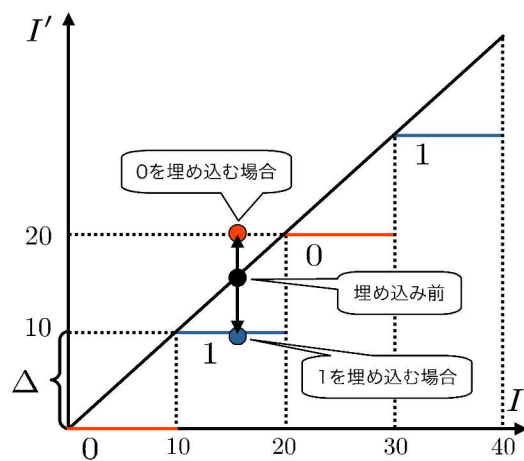


図 1.2: 量子化ステップ $\Delta = 10$, 2 値の場合の QIM の埋め込み

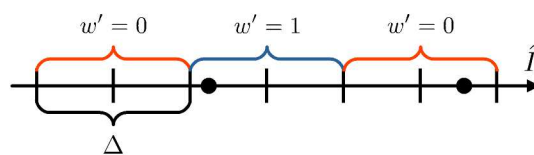


図 1.3: 量子化ステップ $\Delta = 10$, 2 値の場合の QIM の抽出

1.2.4 攻撃耐性

画像に対する攻撃は大別して非幾何攻撃と幾何攻撃に分けられる。非幾何攻撃とは、JPEG 圧縮やノイズ付加などのように画素値を変化させる攻撃を指す。ステゴ画像が非幾何攻撃によって劣化しても透かし情報が埋め込まれている座標は変化しない。この場合は透かし情報は元の座標から抽出することができるため、LDPC 符号 [18] などの誤り訂正符号 [2] やスペクトル拡散 [3, 4] を用いてメッセージを符号化していれば、透かし情報が劣化していても復号することが可能である。多くの従来手法は、これらの技術を導入することによって非幾何攻撃に対して堅牢である。

幾何攻撃は拡大縮小や回転、切り抜きのように画素の位置が変化する攻撃を指す。ステゴ画像が幾何攻撃によって劣化すると、埋め込まれた透かし情報の元の位置情報は失われる。そのため、透かし情報の位置の検出、つまり位置同期が必要である。

SIFT 特徴量 [19] などの特徴点を用いた電子透かし法は幾何攻撃に対して堅牢な手法の一つである。SIFT 特徴点とは、幾何攻撃に対して堅牢な特徴点である。画像が幾何攻撃によって歪んでも安定して特徴点を得ることができる。ここでは、ガウス分布の標準偏差を σ とする。最初に様々なスケールのガウス関数 $G(x, y, \sigma)$ と画像 $I(x; y)$ の畳み込みを行うことで DoG (Difference of Gaussian) 画像

$$D(x, y, \sigma) = G(x, y, k\sigma) * I(x; y) - G(x, y, \sigma) * I(x; y) \quad (1.3)$$

を生成する。ここで、 k は一定の乗数とし、 $*$ は畳み込みを表す。複数の DoG 画像の極値を求めることによって特徴点が決定される。図 1.4 に極値の探索方法を示す。注目するスケールの DoG 画像の画素値について、8 近傍の画素及び前後のスケールの DoG 画像の 9 近傍の画素値と比較して最大及び最小となる場合に極値とする。ここで、特徴量の一つであるスケール σ は、極値を検出した際の DoG 画像の標準偏差から求められる。複数の特徴点の周辺領域に同じ透かし情報を埋め込む手法 [20, 21] では、特徴点を検出することによって透かし情報が埋め込まれた領域の位置同期が可能である。

非ブラインド方式の場合は埋め込み時の特徴量を保存して、ステゴ画像の特徴点とマッチングを行うことで画像の歪みを補正する手法 [22] がある。しかしながら、わずかな位置ずれや回転検出の性能は依然として不十分であるという課題がある。

幾何攻撃の中で特に考慮すべきであるのが切り抜き攻撃である。切り抜きにはクリッピングとトリミング [23] がある。クリッピングとは、画像の一部の領域を 0 で埋めることによってその画素値の情報を削除する処理である。クリッピング画像の場合は画像全体の大きさは処理前後で変化しな

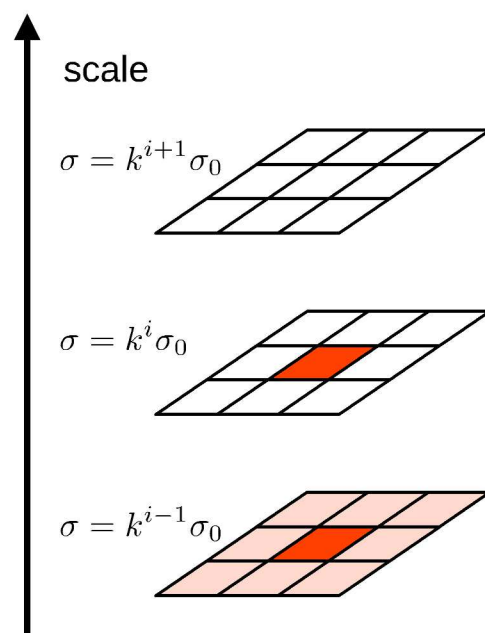


図 1.4: 極値の探索方法

いため、透かし情報の位置は既知である。一方で、トリミングとは画像の一部の領域を完全に除去することによって画素値の情報を削除する処理である。トリミング画像は画像領域が完全に除去されることによって画像サイズが変化するため、埋め込まれた透かし情報の位置を特定することが困難になる。多くの電子透かし法では、クリッピング攻撃に耐性があるが、トリミングには耐性がない。Hu と Xiang の手法 [24] では、透かし情報を Zernike モーメントの係数に埋め込む。Zernike モーメントは回転に対して不変であるという特性だけでなく、振幅を正規化することで拡大縮小にも堅牢になる。この手法では、多少のトリミングには堅牢である一方で、切り抜く領域が偏っていると検出が困難になる可能性がある。Lin らの手法 [23] では、フーリエ変換の対数極座標の振幅に対して透かし情報を埋め込む、RST 耐性のある手法を提案した。ここで、RST とは回転、拡大縮小、並進移動 (Rotation, Scaling, Translation) を表す。この手法は回転や拡大縮小、並進移動などに対して耐性がある一方で、トリミングには耐性がない。サーベイ論文 [25] の 7 章でも、トリミングを伴う幾何攻撃の問題は依然として困難であると述べられている。幾何攻撃の種類と強度を推定することができれば透かし情報の位置を正確に検出することができるため、検出誤りを減らすことが可能である。この考えに基づいて、我々はチャンネル推定の枠組みに焦点を当てた攻撃推定手法を導入する。チャンネル推定では、メッセージとは異なるパイロット信号で推定する手法が用いられている。パイロット信号はノイズのある通信路を通過すると劣化するため、この劣化に基づいて通信路のパラメータを推定する手法である。我々の電子透かし法では、このパイロット信号の概念を導入して、画像に埋め込む手法を提案する。パイロット信号を埋め込んだステゴ画像が幾何攻撃によって劣化すると、パイロット信号も劣化する。したがって、パイロット信号の歪みを分析することによって攻撃パラメータを推定することが可能である。

Su らの手法 [26] では、パイロット信号を用いた電子透かし法を提案した。彼らの手法では SIFT 特徴点の周辺の領域に透かし情報を埋め込む。透かし情報の位置を特定するための基準点としてパイロット信号を埋め込む。埋め込まれたパイロット信号に関連付けられた特徴点を検出することによって透かし情報の位置を特定することが可能である。しかし、この手法ではパイロット信号を同期目的で使用しているため、幾何攻撃のパラメータを推定することには用いていない。

Pereira と Pun の手法や Kang らの手法 [27, 28] では、原画像を固定サイズにパディングし、フーリエ変換を行って検出用のテンプレートと透かし情報の両方を埋め込む。透かし情報を抽出する際には、ステゴ画像からテンプレートを検出して、その劣化から変換行列を求める。次に、得られた推定変換行列を用いてステゴ画像を逆変換してから透かし情報を抽出する。これらの操作により、幾何

表 1.1: 研究の位置付け

画像電子透かし法			
	分類		
埋め込む透かし情報の長さ	ゼロビット電子透かし法 [11, 12]	1 ビット電子透かし法 [10]	多ビット電子透かし法
可逆/ 非可逆電子透かし法	可逆電子透かし法 [15]	非可逆電子透かし法	
抽出時の原画像情報の必要有無	非ブラインド方式 (原画像必要) [16, 17]	ブラインド方式 (原画像不必要) [32, 33]	
幾何攻撃耐性	あり (攻撃推定あり) [27, 28]	あり (攻撃推定なし) [20, 21, 23, 24, 26]	なし
非幾何攻撃耐性	あり [2, 3, 4]	なし	

攻撃やトリミングを受けた画像からでも透かし情報を正確に検出できると主張している。これらの手法は、トリミング画像からも幾何攻撃を推定可能である。しかしながら、透かし情報とテンプレートを画像全体の同じ係数値に埋め込むため、大量の透かし情報を埋め込むと画質が大きく劣化する。

1.3 研究の位置付け

本研究では、パイロット信号を用いて幾何攻撃のパラメータ推定を行う。推定パラメータを用いることによって、より正確に透かし情報を抽出することが可能である。パイロット信号を用いて画像に適用された幾何変換を推定するためには、適切な信号の形状を設計し、幾何変換の影響を正確に検出可能な埋め込み手法を選択する必要がある。特に、信号の形状は幾何攻撃の種類に応じて検討する必要がある。したがって、本研究では最初に拡大縮小と切り抜きの場合を考慮して推定手法を開発した [29]。また、SIFT 特徴点と DFT を用いた電子透かし法にパイロット信号による拡大率推定を導入した [30]。更に、複数種類の単体攻撃や複合攻撃の推定手法を開発し、電子透かし法に導入して性能を評価した [31]。

表 1.1 に本研究の位置付けをまとめる。本研究では、表の太字で示す要素をもつ電子透かし法を開発した。SNS などにおける画像の不正利用対策を想定していることから、ブラインド式の多ビット電子透かし法を用いた。しかしながら、1 ビット電子透かし法にも応用可能である。また、幾何攻撃を推定することで透かし情報を正確に検出可能にする。本手法は幾何攻撃耐性問題に着目しているため、非幾何攻撃については誤り訂正符号で対応すると仮定する。

本論文は以下のように構成される．2 章ではパイロット信号による拡大率推定手法と，攻撃推定を導入した電子透かし法を提案し，3 章では，幾何変換行列の推定手法を提案する．また，4 章で本論文を総括する．

第2章 パイロット信号による拡大率推定を用いた拡大縮小に堅牢な電子透かし法

Kawamura と Uchida の手法 [34] や Hayashi と Kawamura の手法 [20] では、画像から SIFT 特徴点 [19] を抽出し、特徴点の周辺領域を離散コサイン変換 (DCT) することで透かし情報を埋め込む。この手法は Su らの手法 [26] と同様に、透かし情報を埋め込む際に埋め込み領域を正規化することで、画像が拡大縮小されても透かし情報を抽出することが可能である。また、複数の特徴点に透かし情報を埋め込むため、画像がトリミングされても透かし情報を抽出することが可能である。しかしながら、埋め込み領域と正規化領域の大きさの差が大きいほど透かし情報が劣化する可能性がある。この問題を解決するために、本手法では幾何攻撃に対して堅牢である離散フーリエ変換 (DFT) ドメインを用いる。DFT 係数値には、画像を拡大縮小した際に攻撃前後で係数の座標が不変であるという特徴がある。この性質を利用することで、埋め込み領域の正規化無しに透かし情報を抽出可能である。ただし、DFT 係数は画像の拡大率に比例して変化してしまうという問題がある。したがって、格子状のパイロット信号を用いて拡大率を推定し、推定拡大率を用いて透かし情報を抽出する手法を提案する。

図 2.1 に提案手法の概要を示す。埋め込み処理では、RGB の原画像を YUV 色空間に分解し、Y 成分と U 成分にそれぞれ透かし情報とパイロット信号を埋め込む。抽出処理では、ステゴ画像を YUV 分解し、まず U 成分画像からパイロット信号を抽出して攻撃を推定する。次に、得られた推定拡大率を用いて Y 成分画像から透かし情報を抽出し、推定メッセージを得る。提案手法のパラメータは IHC [35] を参考に以下のように設定した。原画像は IHC 標準画像 (4608×3456 画素) とする。また、ステゴ画像は幾何攻撃によって劣化した後にトリミングされるものとする。ここで、ステゴ画像は中心座標が $(x \pm 700; y \pm 500)$ となるように 4 箇所の座標で Full HD サイズ (1920×1080 画素) にトリミングされる。また、本手法で想定する幾何攻撃はアスペクト比の変化しない拡大縮小である。

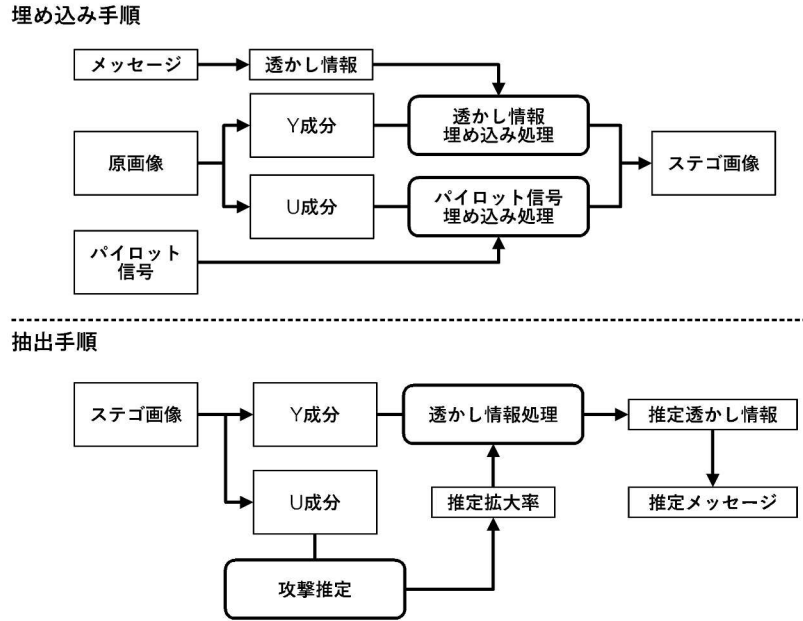


図 2.1: 提案手法の概要

2.1 本研究の貢献

本研究の貢献は大きく分けて2つである。一つ目は、DFTを用いた埋め込み領域の利用である。これによって、画像が拡大縮小されてもDFT係数上の透かし情報の埋め込み位置が不変となる。これに伴って従来法[34, 20]で必要だった埋め込み領域の正規化が不要となるため、透かし情報の劣化や画質の劣化を抑えることが可能である。二つ目は、格子状のパイロット信号による拡大率推定である。本研究の目的は、(1)パイロット信号による幾何攻撃の推定可否と、(2)攻撃の推定パラメータを用いた透かし情報の推定精度の向上の検証である。その結果として、パイロット信号によって幾何攻撃を推定することが可能であることを示した。加えて、推定拡大率を用いることでより正確に透かし情報を抽出することが可能であることを示した。本手法の特徴として、格子状のパイロット信号を用いることで画像がトリミングされても拡大率を推定可能であることが挙げられる。

2.2 DFT の性質

提案手法の透かし情報の埋め込みに用いる離散コサイン変換 (DFT) の性質について述べる. $h \times h$ 画素の画像 $Y(x; y)$ に DFT を適用すると, DFT 係数 $F(k_1; k_2)$ は

$$F(k_1; k_2) = F[Y(x; y)] \quad (2.1)$$

$$= \frac{1}{h} \sum_{x=0}^{h-1} \sum_{y=0}^{h-1} Y(x; y) e^{-2\pi j \frac{k_1 x + k_2 y}{h}}; \quad (2.2)$$

で表される. ここで j は虚数単位を表し, F は離散フーリエ変換を表す. 画像 Y を拡大率 μ [4, 36] で拡大縮小すると, DFT 係数は

$$F[Y(\mu x, \mu y)] = \frac{1}{\mu} F\left(\frac{1}{\mu} k_1; \frac{1}{\mu} k_2\right); \quad (2.3)$$

を満たすことが知られている. したがって, μ 倍に拡大した画像の DFT 係数は, 原画像の DFT 係数と同じ位置で検出することができる. DCT などの他の変換ではこのような不変性はないため, 透かし情報を抽出するためには拡大画像を元のサイズに逆変換する必要がある. DCT を用いる場合は, 埋め込み領域を正規化することで逆変換なしで透かし情報を抽出することが可能になる. しかし, 正規化は拡大縮小処理と等価であるため, 画質や透かし情報を劣化させる可能性がある. そこで提案手法では, 逆変換を必要としない DFT 領域に透かし情報を埋め込む. この場合の問題点は, 画像を拡大縮小すると DFT 係数値が拡大率に応じて変化することである. そのため, 画像を大きく拡大すると, 正しい係数の位置であっても正確な透かし情報が得られない可能性がある. そこで, 本章では画像の拡大率を推定し, 係数値を逆変換することでこの問題を解決する.

2.3 透かし情報の埋め込み

図 2.2 に透かし情報の埋め込み手順を示す. 透かし情報の手順は以下の通りである. (1) 符号化されたメッセージと判定ビットからなる透かし情報を生成する. (2) 原画像から SIFT 特徴点を抽出する. (3) SIFT 特徴量を基準に透かし情報を埋め込む特徴量を選択し, 埋め込み領域を生成する. (4) 埋め込み領域を DFT して, 係数からスペクトルを計算する. (5) 振幅スペクトルに透かし情報を埋め込む. (6) 逆 DFT をしてステゴ画像を生成する.

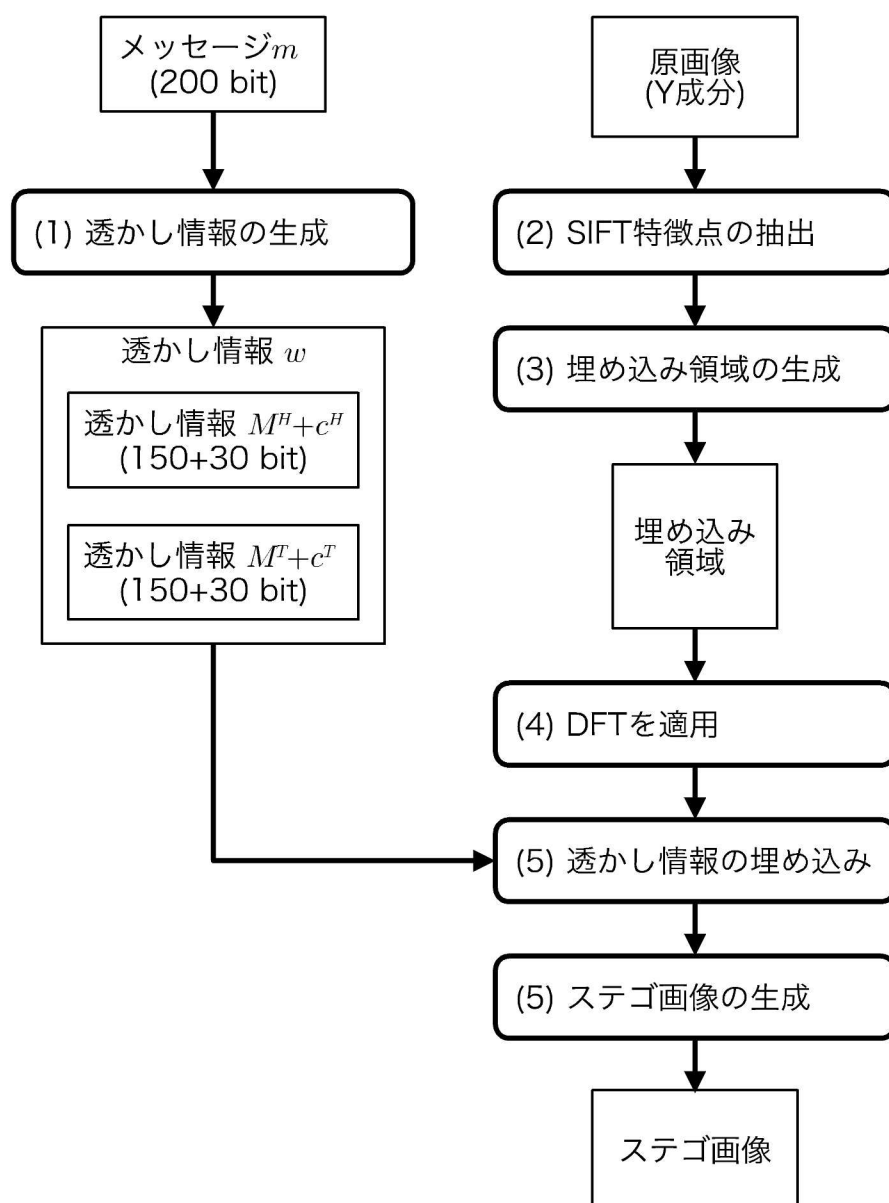


図 2.2: 透かし情報の埋め込み手順

2.3.1 透かし情報の構成

図 2.3 に透かし情報の構成を示す。画像には長さ $N_m = 200$ bit のメッセージ $\mathbf{m} = (m_1; m_2; \dots; m_{N_m})$ を m_i 2 f0; 1g を埋め込む。ステゴ画像が攻撃によって劣化するとメッセージが劣化する可能性がある。そのため、LDPC 符号 [18] を用いてメッセージを 297 bit に符号化して誤りを訂正できるようにする。ここで、符号語全体を一つの埋め込み領域に埋め込むと著しく劣化する。この劣化を抑えるために、符号語を 2 つに分割し、それぞれを異なる埋め込み領域に埋め込む。

1 つの埋め込み領域には $N_s = 150$ bit の情報を埋め込む。そのため、パディングして 300 bit にした符号語 $\mathbf{M}$ を 2 つに分割して埋め込む。パディングした符号語を $\mathbf{M}$ とし、分割した上位ビットと下位ビットをそれぞれ $\mathbf{M}^H; \mathbf{M}^T$ とする。更に、2 種類の符号語の検出及び判別を行うために各符号語と共に対応する判定ビットを埋め込む。判定ビットとは、得られた透かし情報が正しいのかを判別するために埋め込まれる情報である。本手法では、透かし情報の有無と、上位ビット及び下位ビットの判別のために用いる。

判定ビットの長さは $N_c = 30$ bit として、上位の判定ビット $\mathbf{c}^H$ と下位の判定ビット $\mathbf{c}^T$ は互いに直交するものとする。ここで、 $\mathbf{c}_1^H$ 2 f0; 1g, $\mathbf{c}_1^T$ 2 f0; 1g である。以上より、1 つの埋め込み領域に埋め込む符号語と判定ビットで構成される透かし情報 $\mathbf{w}^H; \mathbf{w}^T$ は次のように表される。

$$\mathbf{w}^H = fM_1^H; M_2^H; \dots; M_{N_s}^H; c_1^H; c_2^H; \dots; c_{N_c}^H g; \quad (2.4)$$

$$\mathbf{w}^T = fM_1^T; M_2^T; \dots; M_{N_s}^T; c_1^T; c_2^T; \dots; c_{N_c}^T g; \quad (2.5)$$

2.3.2 埋め込み領域

幾何攻撃に対して堅牢な埋め込み領域を生成するために、画像に SIFT 特徴器を適用する。これによって、特徴点とスケール σ が SIFT 特徴量として得られる。画像を拡大縮小すると、スケールが小さい特徴点は消えてしまう可能性がある。一方で、画像スケールが大きい特徴点は座標が変化する傾向がある。したがって、スケールの大きさが $4 \leq \sigma \leq 10$ [37] である特徴点に透かし情報を埋め込む。

図 2.4 に SIFT 特徴量と埋め込み領域の関係を表す。透かし情報の埋め込み領域は、特徴点を中心として半径がスケール σ に比例する円の外接矩形である。スケールによっては透かし情報を埋め込むために十分な埋め込み領域の大きさが確保できないため、拡大率 d を導入する。各特徴点から生成された埋め込み領域は重なり合う可能性がある。そのため、全ての埋め込み領域に透かし情報を

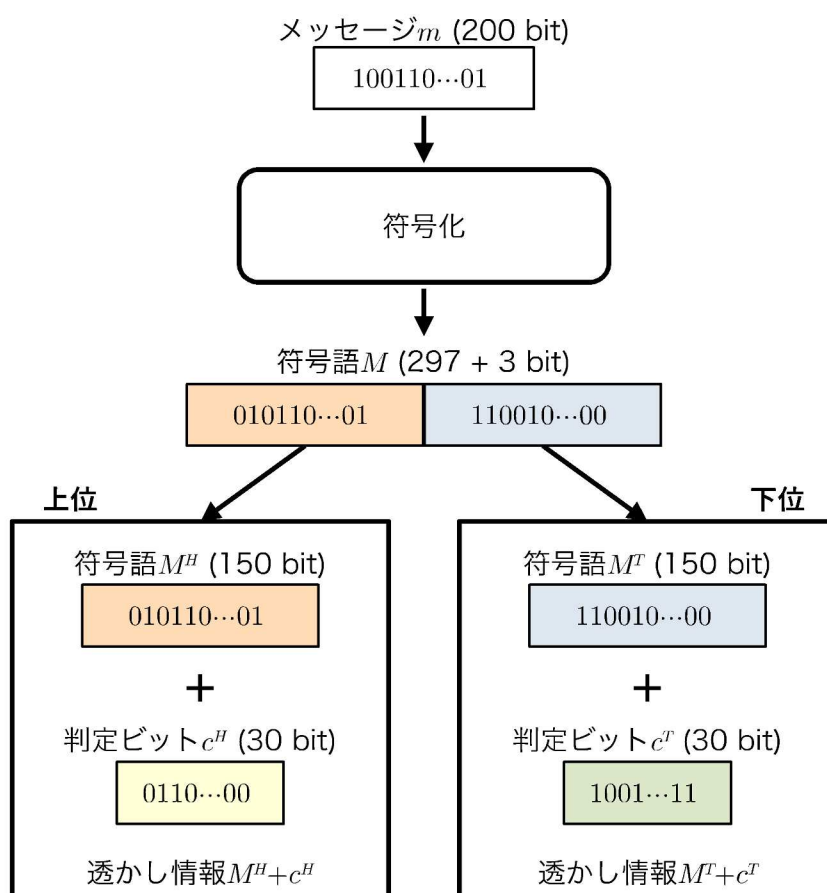


図 2.3: 透かし情報の構成

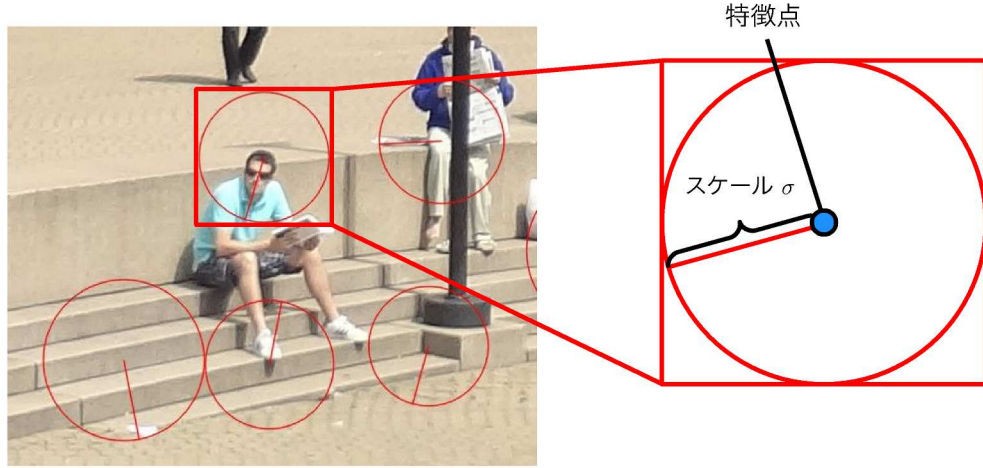


図 2.4: SIFT 特徴量と埋め込み領域

埋め込むと透かし情報が破損する可能性がある。これを回避するために、特徴点は重なり検出を用いて更に絞り込まれる。重なり検出は、ガウス分布 (DoG) 出力の差の順に特徴点を比較することによって行われる [34]。領域が重なり合う場合、DoG 出力が小さい特徴点が除外される。最終的に、2 種類の透かし情報 $\mathbf{w}^H; \mathbf{w}^T$ は一辺が $h = 2d\sigma$ の埋め込み領域に同量ずつ埋め込まれる。

ここで、拡大率 d について検討する。次の節で説明する埋め込み領域の直径は少なくとも 83 画素以上である必要がある。埋め込む特徴点のスケールの大きさは $4 \leq \sigma \leq 10$ と指定していることから、拡大前の埋め込み領域の一辺の長さは最小で 8 画素、最大でも 20 画素である。最小値の $\sigma = 4$ に合わせて拡大率を決定する場合、最低でも $d = 11$ にする必要がある。一方で、 $\sigma = 4$ の際に同様の拡大率を用いると埋め込み領域が過剰に大きくなってしまうため、透かし情報を正確に得るために十分な数の埋め込み領域を確保できない可能性がある。したがって、スケールの大きさに応じて異なる拡大率 d を導入する。ここでは拡大率 d を

$$d = \begin{cases} 15 & (4 \leq \sigma \leq 6) \\ 9 & (6 < \sigma \leq 10) \end{cases}; \quad (2.6)$$

と決定した。

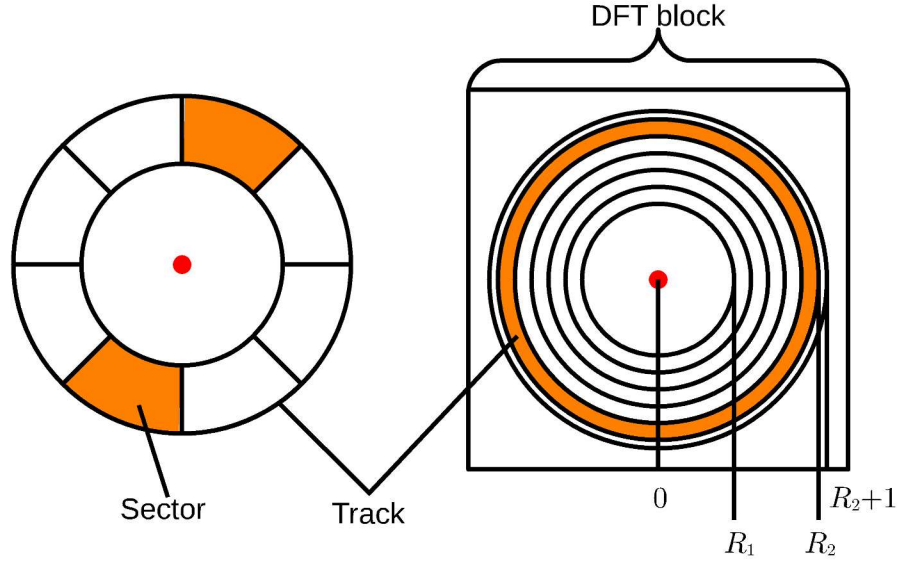


図 2.5: トラックとセクタ

2.3.3 透かし情報の埋め込み

透かし情報は埋め込み領域 $Y(x; y)$ を DFT して、得られた DFT 係数 $F(k_1; k_2)$ に対して埋め込まれる。DFT 係数 $F(k_1; k_2)$ は複素数であることから振幅スペクトル jFj と位相スペクトル $\angle F$ を求める。振幅スペクトルに変換した埋め込み領域を DFT ブロックと呼ぶ。各 DFT ブロックには、量子化インデックス変調 (QIM) [9] を用いて $N_s + N_c = 180$ bit の透かし情報を環状に埋め込む。図 2.5 に示すように、埋め込み領域は符号語領域と判定ビットトラックから構成される。符号語領域は半径 $R_1; R_2$ の同心円で囲まれた領域であり、判定ビットトラックは幅 1 の半径 R_2 の同心円で囲まれた領域である。符号語領域は半径方向に $t = 5$ 個のトラックに分割される。各トラックは角度方向に $2S$ 個のセクタに分割される。

透かし情報 w は内側のトラックから開始して、各セクタに 1 bit ずつ埋め込まれる。各セクタの全ての振幅スペクトル $jF(k_1; k_2)j$ に対して QIM を用いて i 番目の透かし情報 w_i を繰り返し埋め込む。埋め込まれた振幅スペクトルは

$$jF^0(k_1; k_2)j = 2\Delta_w \left(\left\lfloor \frac{jF(k_1; k_2)j}{2\Delta_w} - \frac{w_i}{2} + 0.5 \right\rfloor + \frac{w_i}{2} \right); \quad (2.7)$$

で表される。ここで、 Δ_w は床関数 Δ_w は埋め込み強度である。画像を DFT した直後は DFT 係

表 2.1: 各トラックにおけるセクタ数及び埋め込み強度 Δ_w

Track	1	2	3	4	5
Radius (R_1 - R_2)	15-20	20-25	25-30	30-35	35-40
sectors (s)	10	30	30	40	40
strength (Δ_w)	30	20	20	15	15

数の原点が四隅にあるため、原点が画像の中心となるように DFT 係数の位相をずらす必要がある。 $F^*(k_1; k_2)$ は $F(k_1; k_2)$ の複素共役であり、DFT 係数には

$$F(k_1; k_2) = F^*(h - k_1; h - k_2); \quad (2.8)$$

という対称性がある。したがって、 $F(k_1; k_2)$ と $F^*(h - k_1; h - k_2)$ の双方に同じ透かし情報 w_1 を埋め込む必要がある。

表 2.1 に各トラックに埋め込むビット数とそのトラックの埋め込み強度 Δ_w を示す。トラックが中心に近いほど埋め込みによって劣化しやすく、遠いほど透かし情報が劣化しやすくなることから、トラック毎に埋め込み強度を変更した。また、全てのトラックを同じセクタに分割した場合、中心に近いトラックほどセクタの大きさが小さくなってしまうため、トラック毎にセクタ数を変更した。

埋め込み後の振幅スペクトル $jF^Q(k_1; k_2)$ を用いると、埋め込み後の DFT 係数の実部 $\text{Re } F^Q(k_1; k_2)$ と虚部 $\text{Im } F^Q(k_1; k_2)$ は

$$\text{Re } F^Q(k_1; k_2) = jF^Q(k_1; k_2)j \cos \theta F(k_1; k_2); \quad (2.9)$$

$$\text{Im } F^Q(k_1; k_2) = jF^Q(k_1; k_2)j \sin \theta F(k_1; k_2); \quad (2.10)$$

で表される。この領域を逆変換することでステゴ画像が生成される。

2.4 透かし情報の抽出

図 2.6 に透かし情報の抽出手順を示す。抽出手順は以下の通りである。(1) ステゴ画像から SIFT 特徴点を検出する。(2) SIFT 特徴量を基準に抽出領域を生成する。(3) DFT と QIM を用いて透かし情報を抽出する。(4) 透かし情報に対して誤り訂正を行い、推定メッセージを決定する。

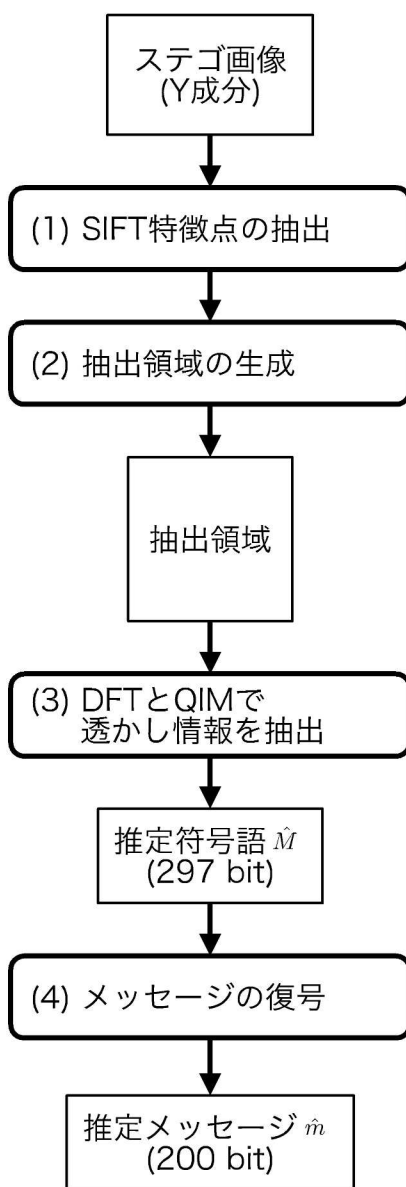


図 2.6: 透かし情報の抽出手順

2.4.1 抽出領域と透かし候補

ステゴ画像から SIFT 特徴点を検出して、スケールの大きさが一定の範囲の特徴点を得る。画像が拡大縮小されるとスケールの大きさも比例して変化するため、埋め込み時のスケールの大きさである $4 \leq \sigma \leq 10$ を用いると実際に埋め込まれた特徴点が検出できない可能性がある。一方で、全ての特徴点を参照すると計算コストがかかってしまう。したがって、0.7 倍から 1.3 倍の範囲の拡大縮小を考慮してスケールの大きさが $2.8 \leq \sigma \leq 13$ の範囲の特徴点を用いる。また、透かし情報が埋め込まれた特徴点を除外する可能性があるため、重なり検出は行わない。その代わりに 2 つの異なる拡大率である式 (2.6) を用いて各特徴点に対して 2 つの抽出領域を選択する。抽出領域は、特徴点を中心とする一辺が $h = 2d\sigma$ 画素の正方形である。ステゴ画像が拡大縮小されると、スケール σ の大きさも拡大率に応じて変化する。したがって、ステゴ画像が拡大縮小されても、埋め込み領域と同じ領域を得ることができる。 $h \times h$ 画素の領域に DFT を適用して振幅スペクトル jF_j を取得する。抽出された特徴点の数を $\hat{P}$ 個とする。透かし情報 w は得られた $\hat{P}$ 個の領域から抽出される。

ステゴ画像を拡大縮小すると、DFT 係数の値は埋め込み前の値に対する拡大率で変化する。したがって、DFT 係数を拡大率で割る必要がある。攻撃を推定することによって拡大率 μ が得られる場合、拡大率を係数で割ることで透かし情報が正確に得られる。拡大率を推定する方法は 2.5 節で説明する。

DFT 係数の半径方向は拡大縮小に対して不変であることから、透かし情報は埋め込み時と同じ符号語領域と判定ビットトラックから抽出する。埋め込み強度が Δ_w の時、振幅スペクトル $jF^{\hat{P}}(k_1; k_2)_j$ から得られる透かし情報候補 w_i は

$$w_i = \left\lfloor \frac{jF^{\hat{P}}(k_1; k_2)_j}{\Delta_w} + 0.5 \right\rfloor \bmod 2 \quad (2.11)$$

で表される。一つのセクタ内全体に同じ透かし情報が埋め込まれているため、透かし情報候補 w_i 2 $f_0; 1g$ は、それらの値の多数決 [20] によって求められる。得られた p 番目の特徴点の透かし情報候補 w^p は、符号語候補 $\hat{M}^p$ と判定ビット候補 c^p に分割される。その抽出領域に透かし情報が含まれているかどうかを符号語候補のみから判断することはできない。更に、透かし情報が含まれていたとしても、上位ビット $\hat{M}^H$ と下位ビット $\hat{M}^T$ のどちらであるかを判別することはできない。したがって、これらを判別するために真の判定ビット $c^H; c^T$ と判定ビット候補 c^p の一致率

$$r^{\lambda, p} = 1 - \frac{1}{N_c} \sum_{i=1}^{N_c} c_i^{\lambda} \oplus c_i^p, \lambda \in \{H, T\}; \quad (2.12)$$

を利用する．ここで， $\oplus$ は排他的論理和を表す．得られた一致率 $r^{\lambda,p}$ から上位ビットなのか下位ビットなのかを

$$\hat{\lambda}^p = \arg \max_{\lambda \in \Lambda^H; T_g} r^{\lambda,p}; \quad (2.13)$$

で判別する．以上より， P 個の符号語と判定ビットの組は $(\hat{M}^{H;p}; c^{H;p})$ または $(M^{T;p}; c^{T;p})$ として求められる．ここで，上位ビットの集合を $\Lambda^H = \{\hat{\lambda}^p = H_{jp} = 1; 2; \dots; P\}$ ，下位ビットの集合を $\Lambda^T = \{\hat{\lambda}^p = T_{jp} = 1; 2; \dots; P\}$ とする．

2.4.2 符号語の推定

P 個の符号語と判定ビットの組は，一致率によって得られる．しかし，これらの透かし情報はステゴ画像の拡大縮小によって劣化している可能性がある．そのため，重みつき多数決 [20] を用いて推定符号語を求める． i 番目の推定符号語 $\hat{M}_i^H; \hat{M}_i^T$ は，

$$\hat{M}_i^H = \Theta \left(\sum_{\lambda \in \Lambda^H} \alpha(r^{\lambda,p}) (\hat{M}_i^{\lambda,p} - 0.5) \right); \quad (2.14)$$

$$\hat{M}_i^T = \Theta \left(\sum_{\lambda \in \Lambda^T} \alpha(r^{\lambda,p}) (\hat{M}_i^{\lambda,p} - 0.5) \right); \quad (2.15)$$

で求められる．ここで，ステップ関数 Θ は

$$\Theta(x) = \begin{cases} 1 & (x \geq 0) \\ 0 & (x < 0) \end{cases}; \quad (2.16)$$

で定義される．また，重み関数 $\alpha(x)$ は

$$\alpha(x) = \begin{cases} 0.0 & (x < T) \\ \tanh(\beta(x - T)) & (T \leq x) \end{cases}; \quad (2.17)$$

で定義される． T は閾値を表し， β は重み係数を表す [34]．ここでは $T = 0.49$ ， $\beta = 7$ とする．以上より，推定符号語は $\hat{M} = (\hat{M}^H; \hat{M}^T)$ で表される．推定メッセージ $\hat{m}$ は推定符号語 $\hat{M}$ に対してノイズ GDBF 復号器 [38] を用いることで求められる．

2.5 パイロット信号を用いた拡大率の推定

幾何攻撃を推定するためにパイロット信号を用いる手法を提案する．本研究の目的は，(1) パイロット信号による幾何攻撃の推定可否と，(2) 攻撃の推定パラメータを用いた透かし情報の推定精度

の向上の検証である。全ての攻撃を一度で推定することは容易ではないため、本研究では画像の拡大率に焦点を当てる。

2.5.1 パイロット信号の埋め込み

パイロット信号を用いて攻撃を推定するためには、適切な (a) 埋め込み領域, (b) 埋め込み方法, (c) 信号の形状を決定する必要がある。

(a) 埋め込みドメイン

埋め込んだ透かし情報に影響を与えないように、パイロット信号を透かし情報とは異なる色空間に埋め込む。カラー画像を YUV 色空間に分解した時、多くの電子透かし法では輝度値である Y 成分に埋め込まれる。したがって、パイロット信号を V または U 成分に埋め込む。いずれの色空間に信号を埋め込んでも推定精度に影響はないため、本手法では U 成分を用いる。画像の大きさを $L_w \times L_h$ 画素とした時、座標 $(x; y)$ の U 成分の画素値は $U(x; y)$ で表される。

(b) 埋め込み方法

パイロット信号を埋め込むために、2.3.3 節で説明した QIM [9] を用いる。2 値のパイロット信号 $p \in \{0, 1\}$ が画素値 $U(x; y)$ に埋め込まれることに注意する。ここではパイロット信号の埋め込み強度を $\Delta_p = 10$ とする。

(c) 信号の形状

一般的に、テンプレートマッチングは拡大縮小された画像内の特定のパターンを見つけるために用いられる。しかし、この探索は非常に計算コストがかかる問題がある。パイロット信号の形状を格子状にして、格子間隔が埋め込み時と比較してどの程度変化したのかを検出することによって拡大率を推定することが可能である。本研究では格子状の 2 値のパイロット信号を用いる。図 2.7 に埋め込まれたパイロット信号の形状を示す。青とピンク色の部分には、それぞれパイロット信号の 1 と 0 の値が埋め込まれる。紫色で塗られた二色の格子の交差部分は 0 と 1 の値が交互に埋め込まれる。画像の格子以外の部分の値は変更しない。ここで、各値の格子線の間隔は $G = 100$ 画素、格子線幅は $B = 5$ 画素である。ここで、格子間隔は拡大率を推定するための秘密鍵である。攻撃者が画

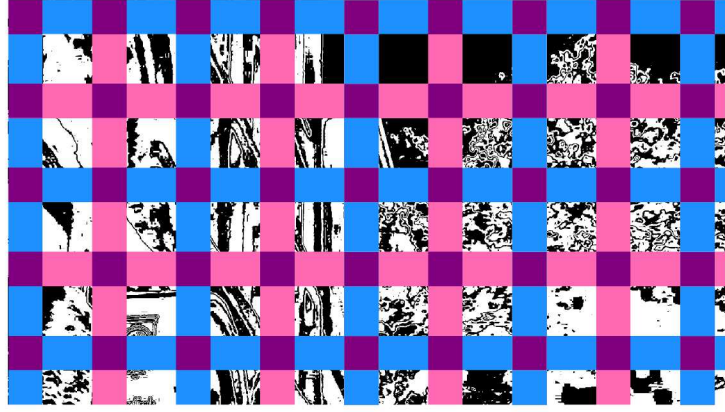


図 2.7: 2値のパイロット信号

像にパイロット信号が埋め込まれていることを知っていても、埋め込み時に使用された格子間隔を知らなければ拡大率を推定できない。

2.5.2 拡大率の推定

ステゴ画像が拡大縮小されると、パイロット信号の格子間隔も拡大率に比例して変化する。したがって、拡大縮小されたステゴ画像から得られた格子間隔の変化を検出することで拡大率を推定することが可能である。垂直方向と水平方向に同じ処理が適用されるため、ここでは水平方向のみにについて説明する。求めた拡大率は、透かし情報を抽出するために用いられる。図 2.8 に拡大率の推定手順を示す。拡大率を自動的に推定する手順は以下の通りである。(1) U成分画像から QIM を用いて 2 値のパイロット信号を得る。(2) 各列の総和を求める。(3) 総和系列から自己相関を求める。(4) 自己相関をフーリエ変換して格子間隔を求める。(5) 格子間隔から拡大率を推定する。

まず、ステゴ画像の U 成分画素値 $\hat{U}(x;y)$ から QIM を用いてパイロット信号 $p(x;y)$ を抽出する。次に、信号 $p(x;y)$ の垂直方向の総和を計算する。j 番目の列の合計は

$$S_j = \sum_{i=1}^{L_h^0} p(x;y); j = 1; 2; 3; \dots; L_w^0; \quad (2.18)$$

で表される。ここで L_w^0 と L_h^0 は拡大縮小されたステゴ画像の縦と横の長さを表す。また、 $S = fS_0; S_1; \dots; S_{M^0-1}g$ を総和の系列とする。ここで、図 2.9(a) に示すように、パイロット信号には 1

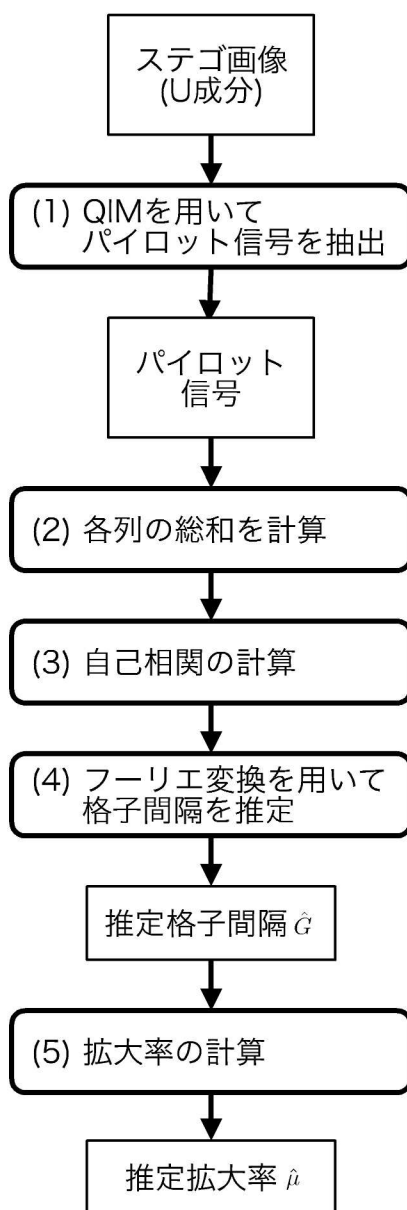
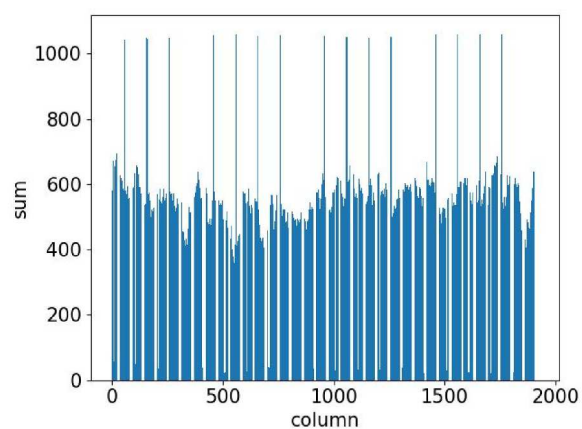
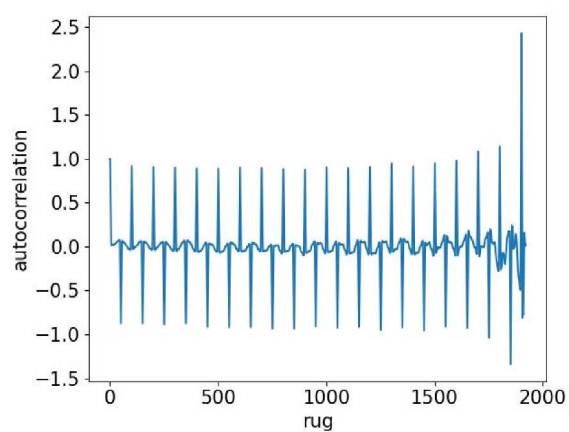


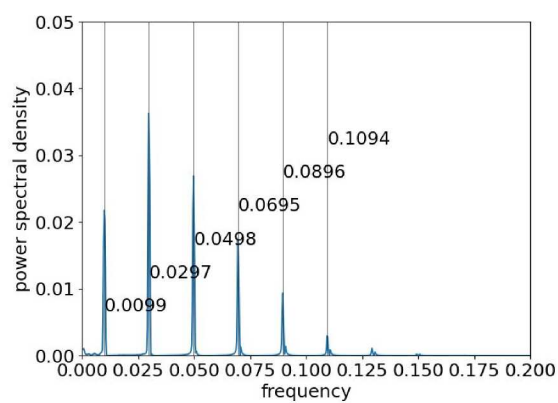
図 2.8: パイロット信号の推定手順



(a) 総和の系列



(b) 総和系列の自己相関



(c) 周波数に対する DFT パワースペクトル

図 2.9: スケーリング率の推定手順

と0の値が格子状に埋め込まれているため、系列Sは1と0の両方の格子線の位置でピークを持つ。したがって、系列Sから検出された格子間隔 $\hat{G}$ から拡大率を求めることが可能である。

系列Sの自己相関を計算することで、格子間隔 $\hat{G}$ を求める。ラグ τ における自己相関関数 $A(\tau)$, $\tau = 0; 1; \dots; M^0 - 1$ は

$$A(\tau) = \frac{1}{(M^0 - 1 - \tau)\sigma_s^2} \sum_{i=1}^{M^0 - 1 - \tau} (S_i - \bar{S})(S_{i+\tau} - \bar{S}); \quad (2.19)$$

で表される。ここで、 $\bar{S}$ と σ_s^2 はそれぞれ系列Sの平均と分散を表す。負のラグ τ を持つ自己相関は、

$$A(-\tau) = A(\tau), \tau < 0; \quad (2.20)$$

で表される。これは自己相関関数が偶関数であるためである。自己相関関数 $A(\tau)$ の範囲は $\tau = -M^0 + 1; -M^0 + 2; \dots; -1; 0; 1; \dots; M^0 - 1$ である。図2.9(b)に、系列Sの自己相関を表す。格子間隔は自己相関の周期的なピークから求められる。

次に、自己相関係数に対してDFTを適用することによって自己相関の周期を求める。この周期はDFTパワースペクトルから検出された周波数の逆数を計算することで得られる。図2.9(c)に周波数に対するDFTパワースペクトルを示す。拡大縮小や圧縮のような攻撃によってステゴ画像が劣化すると、パイロット信号以外の周期が検出される可能性がある。更に、データ長に該当する周期も検出されるため、自己相関に窓関数を適用した後にDFTが適用される。本手法ではフラットトップ窓関数 $W(x)$; $0 \leq x \leq 1$ を用いる。フラットトップ窓関数は

$$W(x) = 1 - 1.93 \cos(2\pi x) + 1.29 \cos(4\pi x) - 0.388 \cos(6\pi x) + 0.032 \cos(8\pi x); \quad (2.21)$$

で定義される。窓関数を適用することによってデータ長がDFTパワースペクトルに現れにくくなり、パイロット信号の周期をより検出しやすくなる。ここではフラットトップ窓関数のピークの位置と自己相関関数のラグ $\tau = 0$ が一致するように拡張される。窓関数をかけた自己相関関数 $A^Q(\tau)$ は

$$A^Q(\tau) = A(\tau)W\left(\frac{\tau + M^0 - 1}{2(M^0 - 1)}\right); \quad (2.22)$$

で表される。自己相関のピークは格子間隔 $\hat{G}$ の奇数倍の周期で現れる。つまり、周波数 $f_0 = 1/\hat{G}$ の奇数倍である周波数 $3f_0; 5f_0; \dots$ も同様に検出される。したがって、周波数 f_0 の奇数倍である周波数の組が検出できれば、この周波数 f_0 をパイロット信号の周波数とみなすことができる。格子間隔

$\hat{G}$ は

$$\hat{G} = \frac{1}{f_0}; \quad (2.23)$$

で求められる。パイロット信号は格子状に埋め込まれていることから、信号の埋め込まれていない領域から抽出される値はパイロット信号に対してノイズとなる。更に、画像が攻撃によって劣化するとパイロット信号が劣化するため、周波数の組が複数検出されたり、全く見つからない場合がある。複数の周波数の組が検出された場合、最も DFT パワースペクトルの大きい周波数 f_0 をパイロット信号の周波数とみなす。

最後に、推定拡大率 $\hat{\mu}$ は

$$\hat{\mu} = \frac{\hat{G}}{G}; \quad (2.24)$$

で求められる。攻撃によりアスペクト比が変化する場合、縦方向と横方向で2つの異なる拡大率が得られる。アスペクト比が変化する場合を想定しない時は2つの拡大率の平均を推定拡大率とする。本章ではアスペクト比が変化しない場合を想定する。

2.6 計算機シミュレーション

提案手法は、U成分画像に埋め込まれた2値のパイロット信号から推定拡大率を求め、推定拡大率を用いてY成分のDFT係数に埋め込まれた透かし情報を抽出する。提案手法にはOpenCVバージョン4.4.0のSIFT検出器を用いた。本手法の性能を評価する。

本手法のパラメータはIHC[35]を参考に決定した。しかし、性能を評価するために、ここでは以下の条件で提案手法を評価した。ステゴ画像への攻撃はIHCよりも広い範囲の拡大率で拡大縮小し、尚且つトリミングされることを想定する。拡大縮小されたステゴ画像はFull HD(1920×1080画素)サイズだけでなく、HDTV(1280×720画素)及びVGA(640×480画素)の大きさとトリミングした。

まず、パイロット信号から推定された拡大率の精度を相対誤差を用いて評価する。次に、推定拡大率を用いてメッセージを推定し、メッセージのビット誤り率(BER)とステゴ画像のピーク信号対雑音比(PSNR)を評価する。最後に提案手法とSIFT特徴点とDFTを用いた先行研究[39]を比較する。

2.6.1 推定拡大率の評価

推定拡大率を相対誤差の観点から評価する．真の拡大率を μ とし，推定拡大率を $\hat{\mu}$ とする．相対誤差 E は

$$E = \frac{|\mu - \hat{\mu}|}{\mu}; \quad (2.25)$$

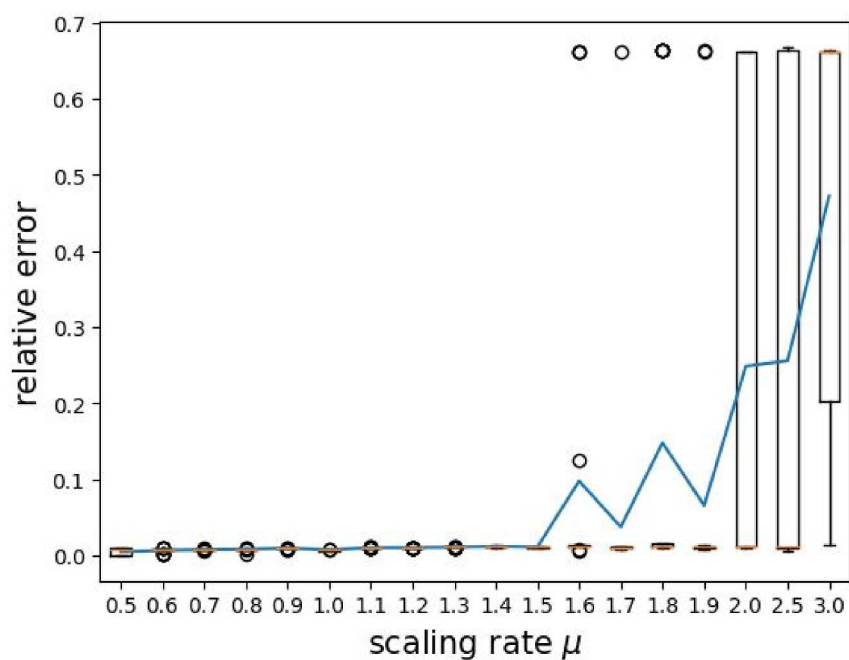
で与えられる．ステゴ画像は 0.1–3.0 倍の間で拡大縮小された後に Full HD サイズで切り抜かれることを想定する．拡大率は垂直方向 (1080 画素) から推定される．図 2.10(a) は各拡大率 μ ($0.5 \leq \mu \leq 3.0$) における推定拡大率 $\hat{\mu}$ の相対誤差 E を示している．また，図 2.10(b) には対数グラフを示す．グラフには，IHC 画像 6 枚を拡大縮小し，1 枚の画像につき 4 箇所から切り抜いた合計 24 枚の画像から得た結果を箱ひげ図と平均値で示している．青線は平均値，橙線は中央値を表し，箱ひげ図は四分位数を表す．図より，0.5 倍から 1.5 倍の拡大率では 0.02 以下の相対誤差で推定することができた．画像を縮小した場合は小さい相対誤差で推定することができた一方で，拡大率が 2 倍を超えると相対誤差が大きくなることがわかった．トリミング画像内に含まれるパイロット信号の格子線の数で攻撃を推定する際に重要となる．画像が縮小された場合は多くの格子線を検出することができる一方で，拡大された場合は画像中の格子線が少ない．格子間隔が 100 画素であることから，画像中の格子線が 5.5 本以下の場合には攻撃の推定が困難であることがわかった．これより，サイズの小さい画像では格子間隔を小さくする必要がある．

2.6.2 推定メッセージの評価

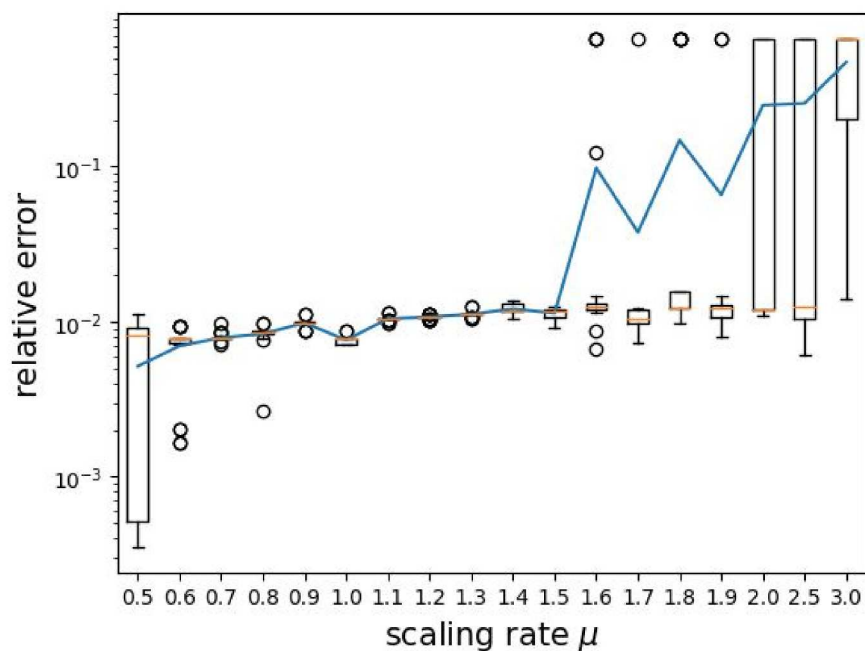
メッセージの BER を用いて提案手法を評価する．真のメッセージを $\mathbf{m}$ とし，抽出されたメッセージを $\hat{\mathbf{m}}$ とする．BER は

$$\text{BER} = \frac{1}{N_m} \sum_{i=1}^{N_m} \mathbf{m}_i \oplus \hat{\mathbf{m}}_i; \quad (2.26)$$

で表される．拡大率推定あり (SRE)，拡大率推定なし (without SRE)，及び既知の拡大率 (KSR) の場合で結果を比較する．図 2.11 にそれぞれの場合の透かし情報の BER の結果とその対数グラフを示す．ここではステゴ画像を 0.7–1.3 倍の拡大縮小した後に Full HD サイズにトリミングされた劣化画像を用いて評価した．横軸は拡大率，縦軸は BER を表している．青線は BER の平均値を，橙線は中央値を表す．これらの図より，拡大率既知と拡大率推定ありの結果は似ており，両手法共に全ての拡大率で BER の中央値が 0 になった．一方で，攻撃推定無しの場合には他の手法よりも BER が



(a) 拡大率毎の相対誤差 (線形スケール)



(b) 拡大率毎の相対誤差 (対数グラフ)

図 2.10: 拡大率が 0.5 – 3.0 倍のときの相対誤差

表 2.2: 画質評価 (PSNR)

	PSNR [dB]
透かし情報のみ	38.3
透かし情報とパイロット信号	34.9

大きくなった。したがって、提案された拡大率推定は効果があり、推定拡大率によってメッセージの誤りを減らせることがわかった。

次に、ステゴ画像を 0.5 – 1.5 倍に拡大縮小し、Full HD, HDTV, VGA サイズに切り抜いた場合の BER を評価した。図 2.12 に各トリミングサイズ毎の拡大率に対する透かし情報の BER とその対数グラフを示す。横軸は拡大率を表し、縦軸は BER を表す。青、橙、緑の線はそれぞれ拡大率既知、拡大率推定なし、拡大率推定ありの場合の平均 BER を表す。本実験で用いたパラメータは相対拡大率を 0.7 – 1.3 倍として設定している。そのため、拡大率が 0.7 未満及び 1.3 倍を超える場合に図 2.10 に示す拡大率推定段階では 0.7 – 1.3 倍と同程度の精度で推定できていたにも関わらず、BER が 0.1 より大きくなった。この原因は、拡大率が 0.7 未満の場合は埋め込み領域が小さくなり、透かし情報の抽出が困難になったためと考えられる。一方で、拡大率が 1.3 倍を超える場合はトリミング画像内に含まれる特徴点の数が少ないことによって正確に透かし情報が抽出できなかったと考えられる。各トリミングサイズを比較すると、画像サイズが小さいほど BER が増加することがわかった。拡大率が既知であっても BER が大きいことから、画像中の特徴点の数が少ないことが原因と考えられる。

2.6.3 画質の評価

パイロット信号の埋め込みによって画質が劣化するため、PSNR を用いて画質を評価する。表 2.2 は透かし情報のみを埋め込んだ場合と、透かし情報とパイロット信号の両方を埋め込んだ場合の 6 枚のステゴ画像の平均 PSNR を示す。パイロット信号を埋め込んだ場合、画質は 3.4 dB 低くなった。共に同じ埋め込み強度で透かし情報を埋め込んでいるため、画質の劣化はパイロット信号の埋め込みによる影響である。

拡大率を推定しない従来法では、透かし情報を正確に抽出するためには QIM の埋め込み強度 Δ_w を大きくする必要がある。比較として、提案手法の埋め込み強度は、パイロット信号を使用しない手法と同じである。しかし、提案手法は拡大率を推定することで、透かし情報を正確に抽出可能である。したがって、埋め込み強度 Δ_w が小さくても透かし情報を抽出できる可能性がある。

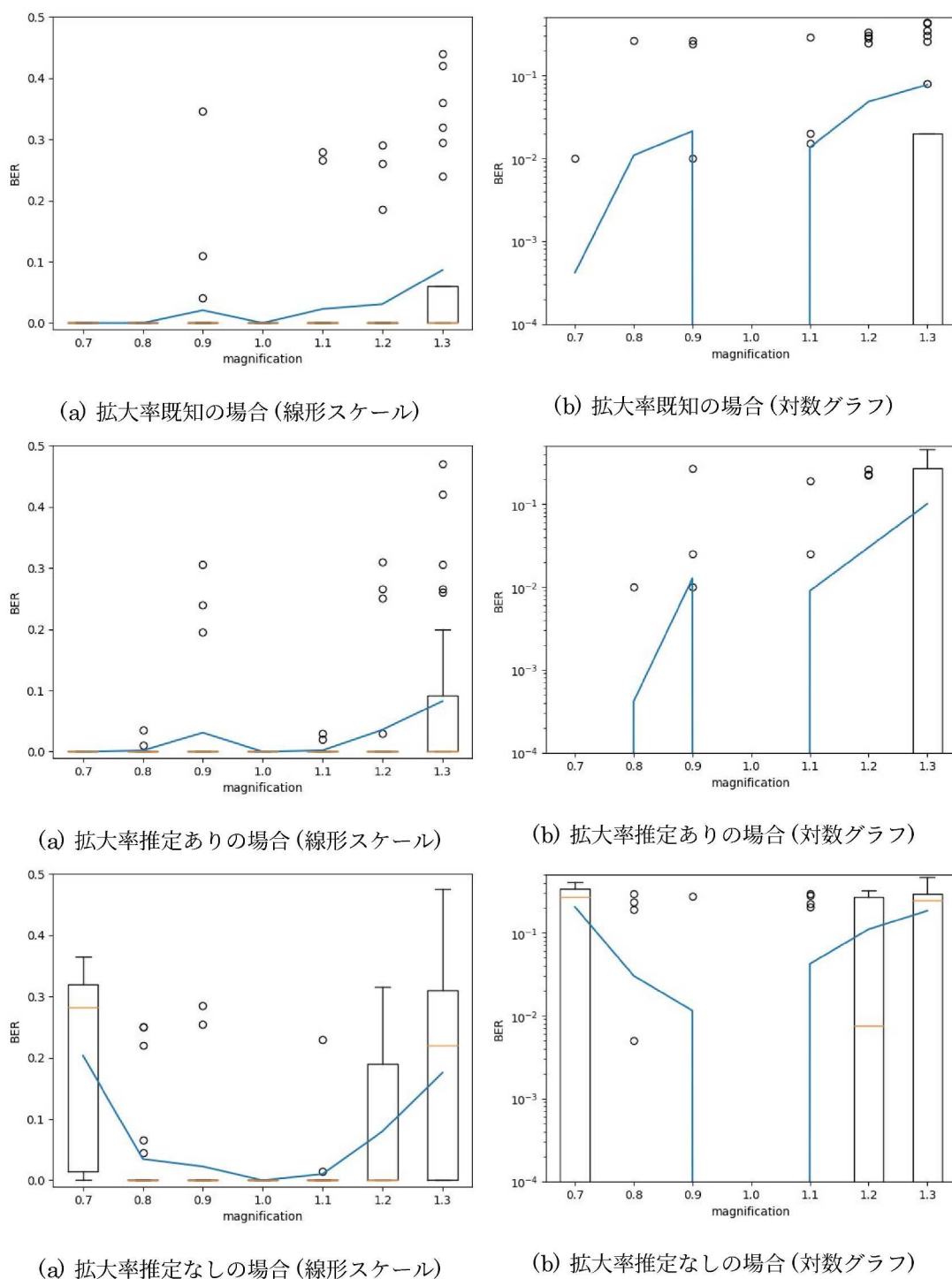
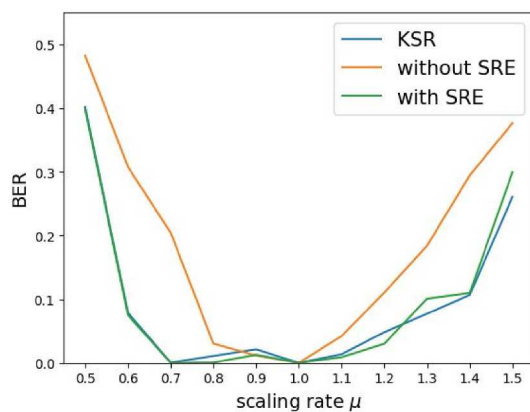
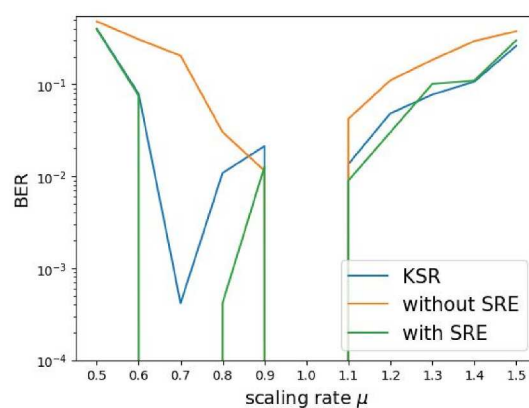


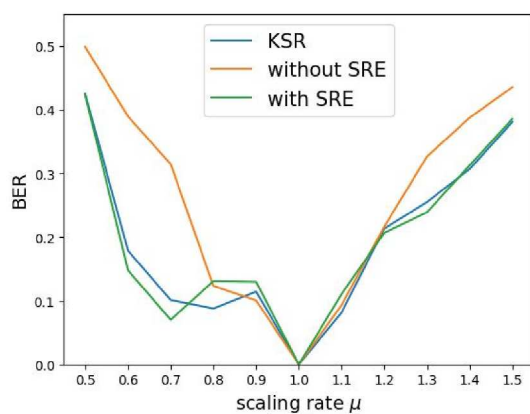
図 2.11: ステゴ画像を 0.7 – 1.3 倍に拡大縮小した後に Full HD サイズにトリミングした場合のメッセージの BER



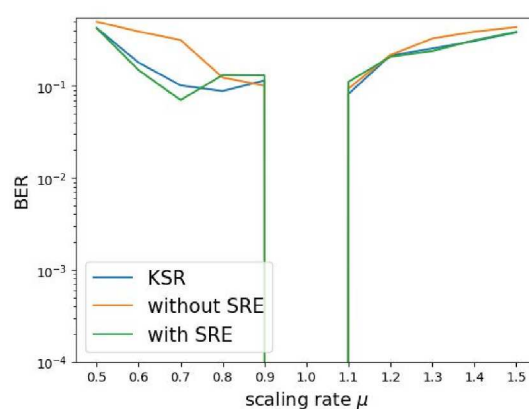
(a) Full HD サイズの場合 (線形スケール)



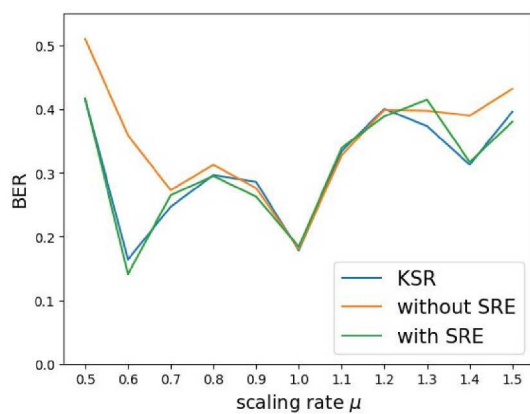
(b) Full HD サイズの場合 (対数グラフ)



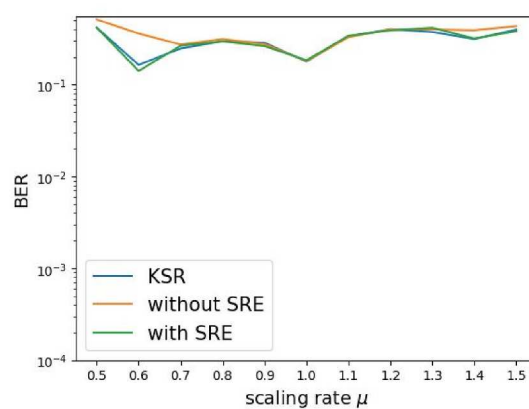
(a) HDTV サイズの場合 (線形スケール)



(b) HDTV サイズの場合 (対数グラフ)



(a) VGA サイズの場合 (線形スケール)



(b) VGA サイズの場合 (対数グラフ)

図 2.12: トリミングサイズ毎のメッセージの BER

表 2.3: 提案手法と Luo らの手法の比較

	透かしの長さ	PSNR	BER	
拡大率 μ			0.9	1.1
Luo らの手法	128	more than 42	0.060	0.103
提案手法 (透かし情報のみ)	180	38.3	0.023	0.010
提案手法 (透かし情報とパイロット信号)	180	34.9	0.031	0.002

2.6.4 先行研究との比較

Luo らの手法 [40] は, SIFT 特徴点の周囲の領域に対して DFT を行い, その DFT 係数に対して透かし情報を埋め込むという点で提案手法と類似している. したがって, 本研究と Luo らの手法を比較する. しかしながら, 彼らの手法では, 透かし情報を埋め込む特徴点の記述子を保存する必要がある. 言い換えると, 彼らの手法は完全なブラインド式電子透かし法ではない. さらに, 彼らの手法は 1 ビット電子透かし法である一方で, 提案手法はメッセージが 200 bit の多ビット電子透かし法である. そのため, 画質を評価する際にはメッセージの長さではなく, 埋め込まれる透かし情報のビット数の観点から 2 つの手法を比較する.

Luo らの手法と透かし情報のみを埋め込んだ提案手法, そして透かし情報とパイロット信号を埋め込んだ提案手法を透かし情報の長さ, 平均 PSNR, BER の観点で比較した. 表 2.3 に各手法の透かし情報のビット数, PSNR, BER を示している. 画像品質は透かし情報の長さによって変化する. 各手法の BER は, ステゴ画像を拡大率 $\mu = 0.9:1.1$ で拡大縮小した時に得られた結果の平均値として計算される. ここでは特徴点に生成された埋め込み領域に埋め込まれた透かし情報の長さを比較する. Luo らの手法では, 1 つの埋め込み領域に埋め込まれる透かし情報の長さは 128 bit であるが, 提案手法では 180 bit である. 透かし情報の長さが長くなると画質が劣化するため, Luo らの手法は提案手法よりも画質が高くなる. しかし, 提案手法は両方の拡大率でより BER が低いことから Luo らの手法よりも性能が良いと言える.

2.7 まとめ

本研究では, SIFT 特徴点と DFT を用いた電子透かし法と, 2 値のパイロット信号を用いた拡大率推定を組み合わせる幾何攻撃に対して堅牢な電子透かし法を開発した. 具体的には, Y 成分画像から SIFT 特徴点を抽出し, 特徴点周辺の埋め込み領域を DFT して透かし情報を埋め込んだ. また,

U成分画像に対して格子状のパイロット信号を埋め込み、格子間隔の変化を検出することによって拡大率を推定した。

本研究の貢献は、埋め込み領域へのDFTの適用と、パイロット信号による拡大率推定である。DFT係数を埋め込みに用いることによって、拡大縮小に対して幾何的に堅牢な埋め込み領域を生成することができた。また、パイロット信号による拡大率推定によって、(1)パイロット信号によって幾何攻撃を推定することが可能であることがわかった。また、(2)推定拡大率を用いて透かし情報の推定精度を高めることが可能であることがわかった。さらに、提案手法の攻撃推定ありと攻撃推定無し、そして先行研究[39]を比較した。その結果、パイロット信号の埋め込みによって画質は先行研究よりも劣化した。しかしながら、拡大率をほぼ正確に推定できたことによって、先行研究よりも低いBERで透かし情報を抽出することができた。

本手法の問題点として、拡大縮小以外の幾何攻撃(異方性拡大縮小や回転、剪断など)に対する堅牢性については対応していない。提案手法に限らず埋め込み領域の形状がこれらの幾何攻撃によって歪むと透かし情報の位置の検出が困難となる。したがって、汎用的な攻撃推定が可能なパイロット信号の形状及び推定方法を検討する必要がある。

第3章 パイロット信号を用いた幾何変換行列の推定

幾何攻撃に対して堅牢であると主張している多くの従来法では、画像を切り抜く際にクリッピング画像を前提としている。画像を切り抜く方法としてクリッピングとトリミングがある。クリッピングとは、特定の領域をパディングすることで画素値の情報を削除する処理である。クリッピングの場合、切り抜かれた領域の画像全体に対する座標は変化しない。一方で、トリミングとは一部の領域を完全に削除する処理である。トリミング処理を行うと画像サイズが変わるため、埋め込まれた透かし情報の位置を特定することが困難となる。例えば、Lin らの手法 [23] では、フーリエ変換の対数極座標の振幅に透かし情報を埋め込む RST 手法を提案した。この手法は回転や拡大縮小、並進移動に対して耐性がある一方でトリミングには耐性がない。Pereira と Pan の手法 [27] と Kang らの手法 [28] では、原画像を値 0 で固定サイズにパディングしてからフーリエ変換し、係数に幾何変換を検出するためのテンプレートと透かし情報の両方を埋め込んでいる。透かし情報を抽出する際にも同様にステゴ画像を固定サイズにパディングして、テンプレートから得られる変換行列に基づいて画像を逆変換する。彼らは、これらの操作によって幾何攻撃や切り抜きによって劣化した画像からも透かし情報を正確に検出可能であると主張している。さらに、Hu と Xiang の手法 [24] では、Zernike モーメントの係数に対して透かし情報を埋め込む。Zernike モーメントは回転に対して不変であるという性質を持つだけでなく、振幅を正規化することで拡大縮小にも堅牢になる。しかしながら、フーリエ変換や Zernike モーメントを用いる場合、トリミングによって攻撃を受けた画像の原点が変化すると、画像を同期させるために総当たり探索が必要となる。位置同期をするために総当たりアルゴリズムがよく用いられるが、このような手法は計算コストが高いという問題点がある。したがって、総当たりを用いる手法は幾何攻撃に対して真に堅牢であるとはいえない。

2 章で述べた SIFT 特徴点と DFT を用いた手法はトリミングに対して堅牢である。その一方で、剪断や複合攻撃等によって埋め込み領域の形状が歪んでしまった場合は正確な抽出領域が得られないという問題点がある。このように、トリミングを含む複数の幾何攻撃に対して効果的な手法は確立

されていない。2022年に出版されたサーベイ論文 [25] の第7節でもトリミングを含む幾何攻撃は依然として難しい問題であると述べられている。幾何攻撃の種類と強度を推定できれば、透かし情報の位置を正確に検出することが可能であるため、透かし情報の誤りを減らすことが可能である。したがって、パイロット信号を用いて拡大率だけでなくより汎用的な攻撃を推定する手法を提案する。

本手法では、格子状の3値のパイロット信号を用いてステゴ画像に加えられた幾何変換行列を推定する。格子状の信号が幾何攻撃によって歪められると格子線の傾きと間隔が変化する。これらの変化をラドン変換によって検出し、得られたパラメータから変換行列を推定する。

3.1 本研究の貢献

本研究の貢献は、格子の検出にラドン係数を用いたことと、画像に加えられた幾何変換行列を推定したことである。パイロット信号の形状は2章で述べた手法と同様に格子状にした。2章では2値のパイロット信号を用いていたため、縦方向と横方向の信号の判別ができなかった。本研究では3値用のQIMを用いて縦方向と横方向で異なる組み合わせの格子線を埋め込んだ。これにより、縦方向と横方向の判別が可能となる。しかしながら、直交した格子線が剪断などによって斜交すると同様の手法では格子を検出することができない。ラドン変換は、複数の角度毎に画像の端から線積分を行う。そのため、格子線の角度と間隔を容易に検出することが可能である。得られた格子の角度と間隔を用いて、異方性拡大縮小や回転、剪断などの幾何攻撃や、これらの複合攻撃を変換行列として推定することに成功した。また、得られた変換行列を用いて画像を逆変換することで透かし情報を正確に抽出可能であることがわかった。

3.2 パイロット信号の埋め込み

パイロット信号は2章で述べた手法と同様に、QIM [9] を用いて格子状に埋め込む。2章と異なる点として、パイロット信号は $-1; 0; 1$ の3値信号を3値用のQIMを用いて埋め込む。ここで、垂直方向と水平方向で異なる組み合わせの格子線を埋め込むことによって、垂直方向と水平方向の判別が可能になる。具体的には、垂直方向には $-1; 0$ の値を持つ格子線、水平方向には $0; +1$ の値を持つ格子線をそれぞれ交互に埋め込む。図3.1に3値のパイロット信号の埋め込み位置を示す。図の青、ピンク色、緑色の線はそれぞれ $-1; 0; 1$ の値の格子線を表す。紫色の部分は2種類の格子線の交差部

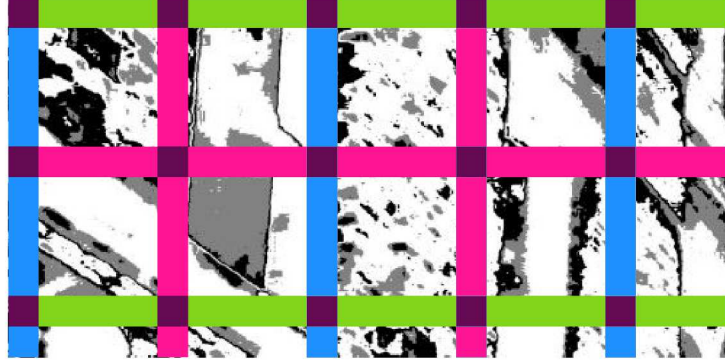


図 3.1: 3 値のパイロット信号

を表し, $-1:0:1$ の値を交互に埋め込んでいる. ここで, 各値の格子線の間隔は $G = 100$ 画素, 格子線幅は $B = 5$ 画素である.

画像サイズを $L_w \times L_h$ 画素として, 座標 $(x;y)$ における U 成分画像の画素値 $U(x;y)$ に対してパイロット信号 $p(x;y)$ を埋め込む時, 埋め込み後の画素値 $U^Q(x;y)$ は

$$U^Q(x;y) = \Delta_p \left(\left\lfloor \frac{U(x;y)}{\Delta_p} - \frac{p(x;y) + 1}{3} + 0.5 \right\rfloor + \frac{p(x;y) + 1}{3} \right); \quad (3.1)$$

で表される. ここで, QIM の埋め込み強度は $\Delta_p = 9$ とする. また, 通常の QIM の埋め込みでは埋め込む値 $p(x;y)$ に非負整数が用いられることから, ここでは -1 を埋め込むので修正版として $p(x;y) + 1$ の値を埋め込むように修正する.

3.3 変換行列の推定

図 3.2 に攻撃の推定手順を示す. 攻撃の推定手順は以下の通りである. (1) 画像の U 成分から QIM を用いて抽出信号を得る. (2) 抽出信号をラドン変換する. (3) 射影角度毎にラドン係数の分散を求め, 検出角度を求める. (4) 検出角度上のラドン係数から検出間隔を求める. (5) 求めた検出角度と検出間隔から変換行列を推定する.

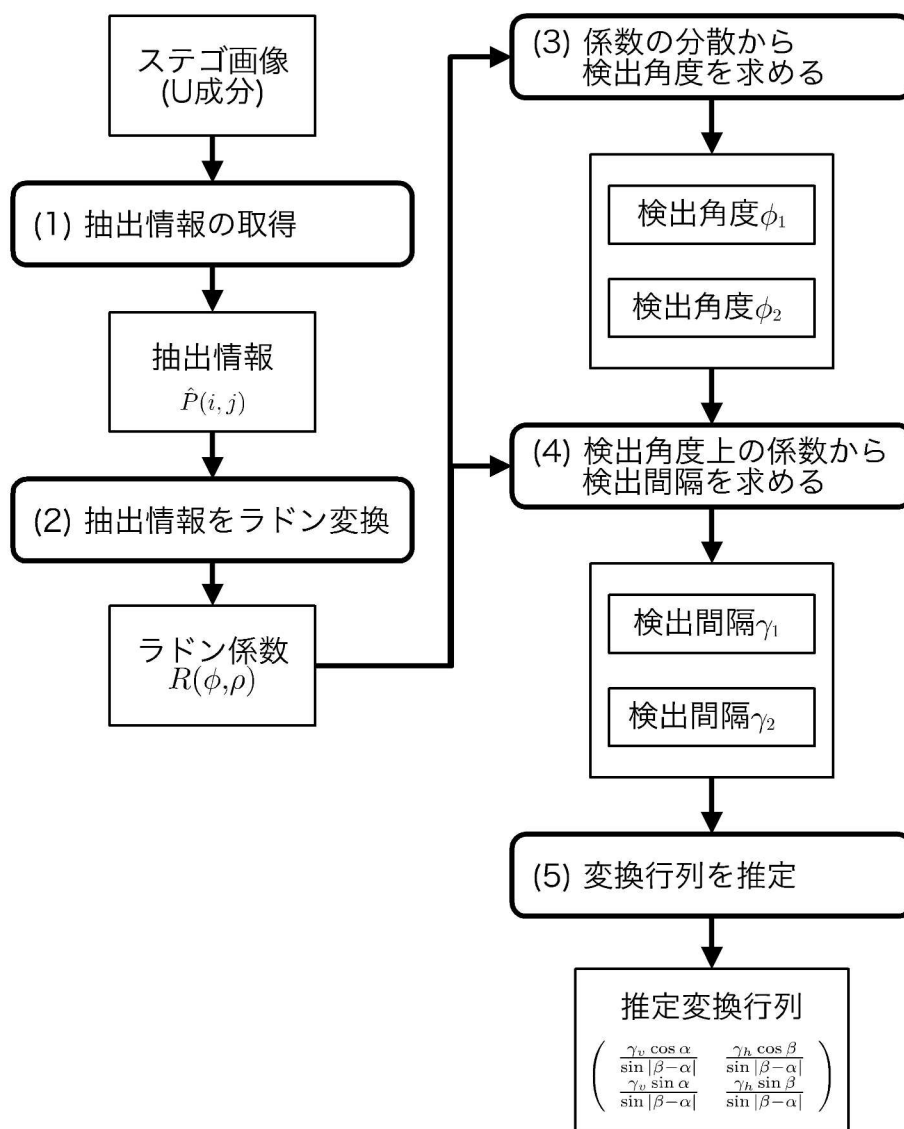


図 3.2: 攻撃の推定手順



図 3.3: 3 値の抽出信号の例

3.3.1 抽出信号の検出

抽出信号 $p(x; y) \in \{-1; 0; 1\}$ はステゴ画像の U 成分画素値 $\hat{U}(x; y)$ に 3 値用の QIM [9] を行うことで得られる。抽出信号 $p(x; y)$ は

$$q(x; y) = \left\lfloor \frac{3\hat{U}(x; y)}{\Delta_p} + 0.5 \right\rfloor \bmod 3; \quad (3.2)$$

$$p(x; y) = q(x; y) - 1; \quad (3.3)$$

で与えられる。ここでは、QIM の後に 1 を引く処理を追加している。これは埋め込み処理で $p(x; y) + 1$ の値を埋め込んだためである。

図 3.3 に抽出信号の例を示す。図中の黒、灰色、白はそれぞれ QIM によって抽出された $-1; 0; +1$ の値を示す。信号には格子状のパイロット信号と原画像成分の両方が含まれている。パイロット信号の格子線は直線として現れるため、これを検出することによって幾何変換を推定可能である。本手法では垂直方向と水平方向に異なる値の格子線が埋め込まれている。具体的には、垂直方向の格子線は $-1; 0$ の値を持ち、水平方向の格子線は $0; +1$ の値を持つ。そこで、抽出された信号を 2 つのグループに分けて格子線の傾きと間隔を検出する。これにより変換行列を推定することが可能である。

3.3.2 ラドン変換

抽出信号 $p(x; y)$ をラドン変換することで、パイロット信号の格子線の位置と傾きを検出することが可能である [41]。ラドン係数 $R(\phi, \rho)$ は

$$R(\phi, \rho) = \int_{-\infty}^1 p(\phi \cos \theta - u \sin \theta, \phi \sin \theta + u \cos \theta) du; \quad (3.4)$$

で求められる。ここで、 ρ は射影位置、 ϕ は射影角度である。ラドン変換の射影角度の範囲は、 $0 \leq \phi \leq 180$ 度で、 0.2 度刻みとする。これは強度分布が回転対称であるためである。提案手法ではパイ

ロット信号が格子状に埋め込まれていることから、格子線の向きに対して平行に線積分を行うことでラドン係数から強い強度が得られる。この性質を用いることで、回転角を推定することが可能である。

図 3.4 は抽出信号のラドン係数を示す。横軸と縦軸はそれぞれ射影角度と射影位置を表す。この例では図中の 60 度と 150 度の場合に一定間隔で強い係数値が見られる。この模式図を図 3.5 に示す。これらの強い係数値は、2 つの角度 ϕ_1, ϕ_2 ; ($\phi_1 < \phi_2$) で現れる。これらの角度を検出角度と呼び、2 方向の格子線の傾きを表している。さらに、各検出角度において、射影角度の方向に強い強度の係数が現れる。この間隔を検出間隔 γ_1, γ_2 と呼び、2 方向の格子線の間隔を表す。

3.3.3 検出角度の検出

まず、ラドン係数から検出角 ϕ_1, ϕ_2 を求める。ラドン係数 $R(\phi_1, \rho)$ と $R(\phi_2, \rho)$ の射影距離方向に着目すると強い強度の係数が等間隔で現れる。この性質を利用して、全ての射影角度 ϕ に対してラドン係数の分散を求めると、検出角 ϕ_1, ϕ_2 で局所的に分散が大きくなる。したがって、ラドン係数を数値微分し、導関数の値に対してゼロクロッシングを行うことによって検出角を求める。ここで、 $V_{\phi_i} = \text{Var}_\rho [R(\phi_i, \rho)]$ を i 番目の射影角度における ρ 方向のラドン係数の分散を表す。図 3.6(a) に、ラドン係数の分散 V_{ϕ_i} の例を示す。縦軸は分散、横軸は射影角度を表す。図より、2 箇所の射影角度で顕著なピークが現れていることがわかる。以下の条件を満たす角度 ϕ_i を検出角 ϕ_1, ϕ_2 とする。

$$dV_{\phi_{i-1}} dV_{\phi_{i+1}} < 0; \quad (3.5)$$

ここで、 dV_{ϕ_i} は射影角度 ϕ_i における分散 $V_{\phi_{i-1}}$ と $V_{\phi_{i+1}}$ の離散差分であり、

$$dV_{\phi_i} = \frac{V_{\phi_{i+1}} - V_{\phi_{i-1}}}{2}; \quad (3.6)$$

で定義される。

得られた検出角度 ϕ_1, ϕ_2 の一方は垂直方向の検出角度 ϕ_v を表し、もう一方は水平方向の検出角度 ϕ_h を表す。提案手法では、格子線は垂直方向と水平方向で異なる値を埋め込まれているので、区別が可能である。抽出信号 $p(x; y)$ には垂直方向及び水平方向のパイロット信号と原画像成分が含まれているため、区別をする必要がある。まず最初に検出角度 ϕ_1, ϕ_2 におけるラドン係数を正規化する。正規化ラドン係数 $R_n(\phi, \rho)$ は

$$R_n(\phi, \rho) = \frac{R(\phi, \rho) - \mu}{\sigma}; \quad (3.7)$$

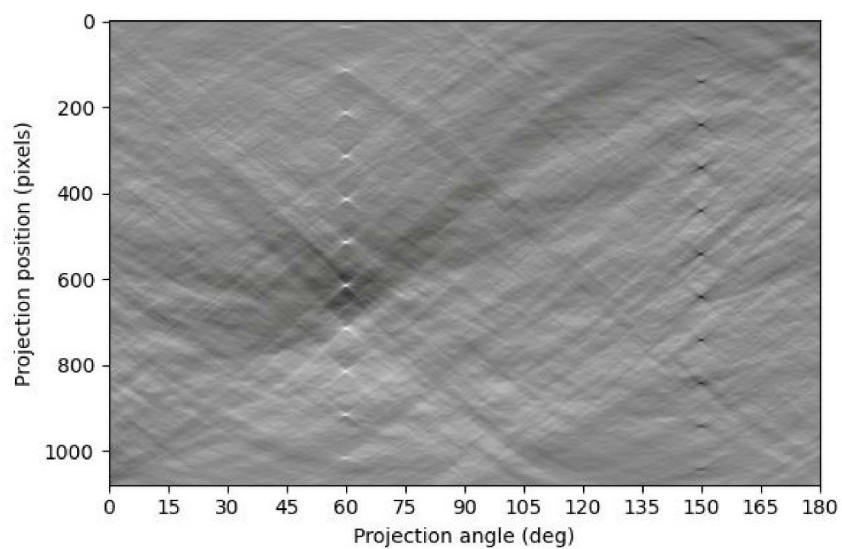


図 3.4: ラドン係数の例

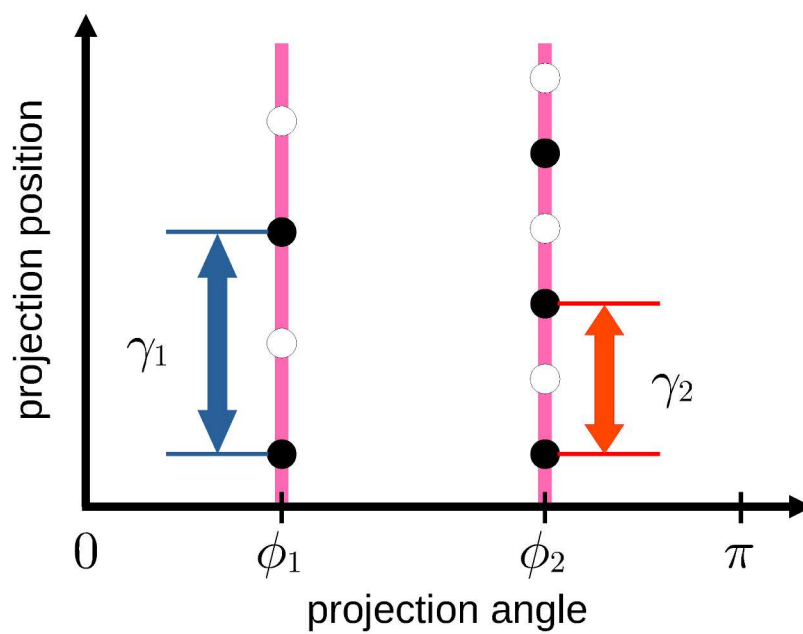
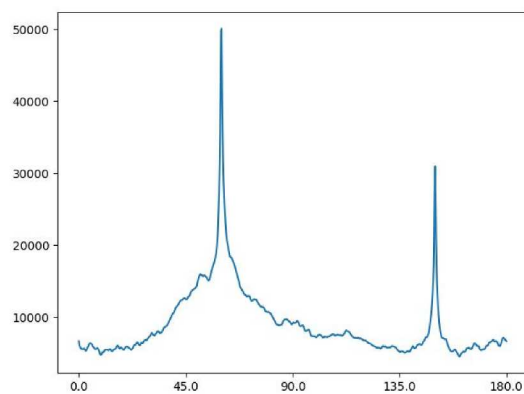
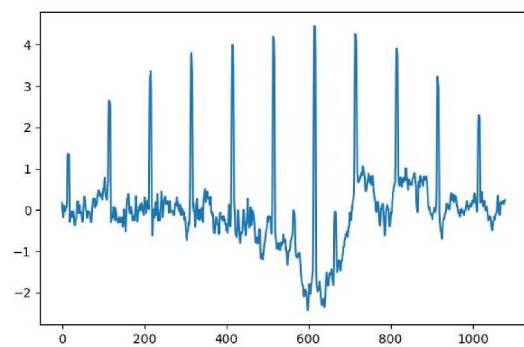


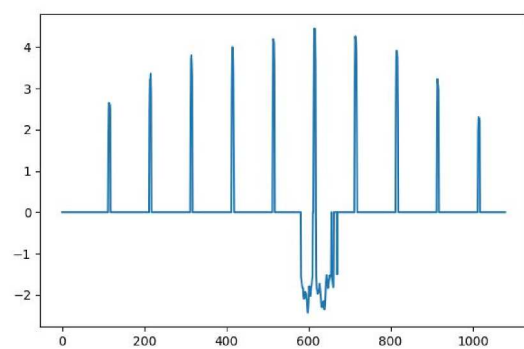
図 3.5: ラドン係数の模式図



(a) 各射影角度におけるラドン係数の分散



(b) 正規化された検出角のラドン係数



(c) 原画像成分除去後のラドン係数

図 3.6: ラドン係数の処理の例

で表される。ここで、 μ と σ はラドン係数の平均と標準偏差である。図 3.6(b) は検出角における正規化ラドン係数を示す。横軸は射影位置を表し、縦軸はラドン係数値を表す。パイロット信号上の係数値は局所的に強くなることから、絶対値の小さな係数は原画像成分とみなせる。したがって、絶対値が閾値以下の係数を 0 にすることで原画像成分を除去することができる。閾値を 1.5 とすると、原画像成分を除去したラドン係数 $\tilde{R}(\phi, \rho)$ は

$$\tilde{R}(\phi, \rho) = \begin{cases} 0; & |R_n(\phi, \rho)| \leq 1.5; \\ R_n(\phi, \rho); & \text{otherwise} \end{cases} \quad (3.8)$$

で表される。

垂直方向の格子線は $-1; 0$ の値で構成されており、水平方向の格子線は $0; +1$ の値で構成されている。言い換えると図 3.6 に示すように、垂直方向の検出角 ϕ_v におけるラドン係数は周期的に負のピークが現れ、水平方向の検出角 ϕ_h におけるラドン係数は周期的に正のピークが現れる。したがって、正のピークと負のピークの出現回数を比較することで判別することが可能である。

3.3.4 検出間隔の特定

次に、抽出信号 $p(x; y)$ から検出間隔 γ_v, γ_h を推定する。抽出信号は 3 値で構成されており、原画像成分を含んでいる。そのため、抽出信号を垂直方向 $p_v(x; y)$ と水平方向 $p_h(x; y)$ に分割してそれぞれで検出間隔を求める。垂直信号と水平方向は

$$p_v(x; y) = \begin{cases} -1; & p(x; y) = -1 \\ +1; & p(x; y) = 0; \\ 0; & p(x; y) = +1 \end{cases} \quad (3.9)$$

$$p_h(x; y) = \begin{cases} 0; & p(x; y) = -1 \\ -1; & p(x; y) = 0; \\ +1; & p(x; y) = +1 \end{cases} \quad (3.10)$$

で表される。垂直信号は $-1; 0$ の値をとる。この場合、 $+1$ の値を取る係数は原画像由来の成分である。これにより、式 (3.9) において原画像成分は $p_v(x; y) = 0$ に、格子線由来の成分は正と負の値をとるように変換される。一方で、水平方向では $0; +1$ の値をとる。同様に、式 (3.10) によって原画像成分は $p_h(x; y) = 0$ に、格子線由来の成分は正と負の値をとるように変換される。垂直信号と水平信号を $(p_v(x; y) - \mu_v) / \sigma_v$ で正規化すると原画像から得られる成分の多くが 0 に近づくため、信号対雑音比が改善される。ここで、 μ_v, σ_v はそれぞれ垂直信号の平均と標準偏差である。同様の性質は水平方向にも当てはまる。

以下は垂直信号に対する処理について述べる．水平信号の場合も処理は同様である．変換された垂直信号 $\hat{p}_v(x; y)$ は式 (3.4) でラドン変換されて、式 (3.7) で正規化する．更に、式 (3.8) で原画像成分を除去する．次に、ラドン係数 $\hat{R}_n(\rho, \phi)$ の自己相関を求める．最後に自己相関の周期的なピークから検出間隔 γ_v を求める．自己相関から格子間隔を求める方法は2章で述べた．同様の処理を水平信号でも行うことによって最終的に方向の検出間隔 γ_v, γ_h が得られる．

3.3.5 変換行列の推定

次に、検出角度 ϕ_v, ϕ_h と検出間隔 γ_v, γ_h を用いて変換行列 T を求める．注意すべき点として、ラドン係数の座標系と画像系は異なる．図 3.7 に検出間隔 ϕ_v, ϕ_h を示す．変換行列に関連する回転の向きは反時計回りであることに對して、ラドン変換における射影角度は時計回りに回転する．したがって、変換行列を推定する際にはこの違いを考慮する必要がある．図 3.7(a) に幾何変換前の格子の状態を示す．水平信号上の座標 $A(1; 0)$ と垂直信号上の座標 $B(0; 1)$ が変換行列 T で変換されたとき、変換後の座標を $A^0(x_a; y_a); B^0(x_b; y_b)$ と仮定する．この場合、変換行列 T は

$$T = \begin{pmatrix} x_a & x_b \\ y_a & y_b \end{pmatrix}; \quad (3.11)$$

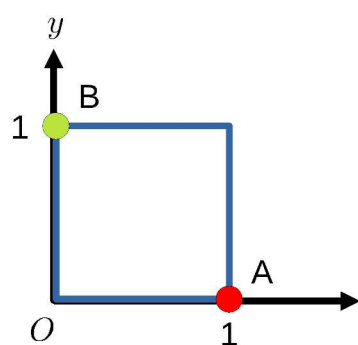
で与えられる．ここで x 軸と直線 OA^0 とのなす角を α 、 x 軸と直線 OB^0 とのなす角を β とする．これらの角度 α, β は行列 T によって変換された水平信号と垂直信号の角度に対応している．ここでラドン変換の射影角度の範囲は $0 - 180$ 度である．図 3.7(b) に示すように、角度 α, β が共に 0 度から 180 度の間の値を取る場合、角度 ϕ_v は検出角度 ϕ_h よりも小さくなる．図 3.7(c) に示すように、角度 β が 0 度未満の場合、検出角 ϕ_v は検出角 ϕ_h よりも大きくなる．したがって、なす角 α, β は

$$(\alpha, \beta) = \begin{cases} \left(\frac{\pi}{2} - \phi_v; \frac{\pi}{2} - \phi_h \right), & \phi_v < \phi_h \\ \left(\frac{3\pi}{2} - \phi_v; \frac{\pi}{2} - \phi_h \right); & \text{otherwise} \end{cases}; \quad (3.12)$$

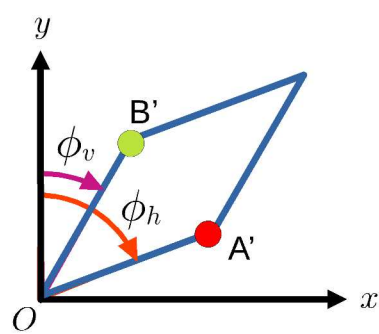
で求められる．

次に、検出間隔 γ_v, γ_h と角度 α, β を用いて座標 $A^0; B^0$ を計算する．図 3.8 に示すように、直線 OB^0 と A^0C 間の距離が検出間隔 γ_v を表し、直線 OA^0 と B^0C 間の距離が検出間隔 γ_h を表す．また、直線 OA^0 と OB^0 のなす角は $\beta - \alpha$ で与えられる．線分 OA^0 と OB^0 の長さは

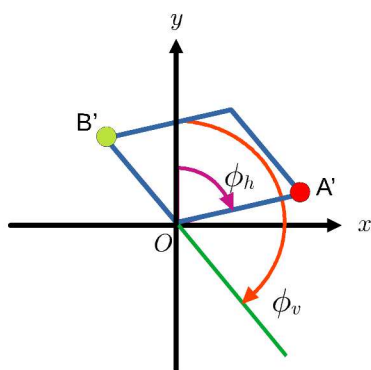
$$jOA^0 = \frac{\gamma_h}{\sin \beta - \alpha}; \quad jOB^0 = \frac{\gamma_v}{\sin \beta - \alpha}; \quad (3.13)$$



(a) 変換前の座標

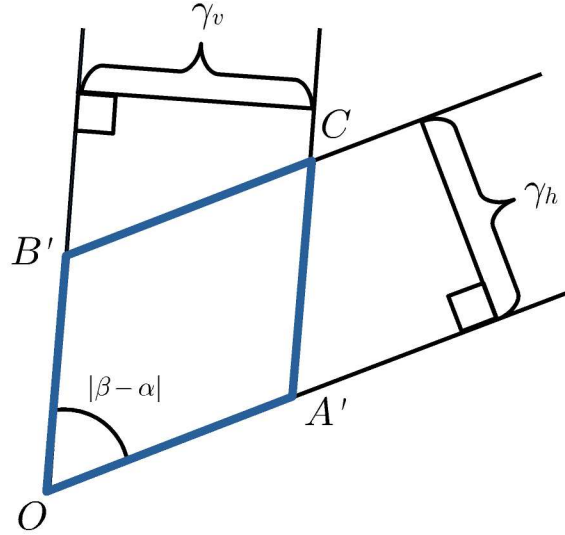


(b) 検出角度が $\phi_v < \phi_h$ となる場合の変換座標



(c) 検出角度が $\phi_h < \phi_v$ となる場合の変換座標

図 3.7: 変換行列による座標変換

図 3.8: 線分 OA^0, OB^0 と検出間隔 γ_v, γ_h 及び角度 α, β の関係

で与えられる。したがって、座標 $A^0(x_a; y_a); B^0(x_b; y_b)$ は

$$x_a = jOA^0 \cos \alpha = \frac{\gamma_v \cos \alpha}{\sin j\beta - \alpha j}; \quad (3.14)$$

$$y_a = jOA^0 \sin \alpha = \frac{\gamma_v \sin \alpha}{\sin j\beta - \alpha j}; \quad (3.15)$$

$$x_b = jOB^0 \cos \beta = \frac{\gamma_h \cos \beta}{\sin j\beta - \alpha j}; \quad (3.16)$$

$$y_b = jOB^0 \sin \beta = \frac{\gamma_h \sin \beta}{\sin j\beta - \alpha j}; \quad (3.17)$$

で与えられる。以上より、推定変換行列は

$$\hat{T} = \begin{pmatrix} \frac{\gamma_v \cos \alpha}{\sin j\beta - \alpha j} & \frac{\gamma_h \cos \beta}{\sin j\beta - \alpha j} \\ \frac{\gamma_v \sin \alpha}{\sin j\beta - \alpha j} & \frac{\gamma_h \sin \beta}{\sin j\beta - \alpha j} \end{pmatrix}; \quad (3.18)$$

と求められる。

3.4 計算機シミュレーション

推定変換行列 $\hat{T}$ の精度を推定変換行列の相対誤差

$$E(\hat{T}; T) = \frac{k\hat{T} - Tk_F}{kTk_F}; \quad (3.19)$$

で評価する．ここで $kT k_F$ は $m \times n$ の行列 $T = [t_{ij}]$ フロベニウスノルムであり，

$$kT k_F = \sqrt{\sum_{i=1}^m \sum_{j=1}^n |t_{ij}|^2}; \quad (3.20)$$

で定義される．

3.4.1 実験条件

本手法では，劣化画像のサイズに応じて攻撃の推定性能が異なる．従って，高画素数画像と低画素数画像を用いて性能を評価した．実験では高画素数画像として図 3.9 に示す 6 枚の IHC 標準画像 [35](4608 × 3456 画素) を用いる．また，低画素数画像として図 3.10 に示す 10 枚の Kodak Lossless True Color 画像 [42](768 × 512 画素または 512 × 768 画素) を用いる．

実験ではステゴ画像に対して変換行列 T で表す幾何攻撃を適用し，画像の中心でトリミングした．トリミングサイズは，画像サイズが原画像サイズの 4 分の 1 以下になるように IHC 標準画像は 1080 × 1080 画素，Kodak 画像は 256 × 256 画素とする．パイロット信号は点対称になるように設計されていることから，推定によって得られた角度と 180 度回転することで得られる角度の判別ができない．したがって，2 つの異なる変換行列を推定した後に，フロベニウスノルムに関して相対誤差が小さい方を推定変換行列として採用した．各攻撃において，これらの切り抜き画像における相対誤差に基づいて推定変換行列の精度を評価した．

3.4.2 格子間隔の決定

格子間隔は提案手法の性能に直接影響を与える重要な要素である．ステゴ画像が幾何攻撃によって変化し，トリミングされることによって格子線が失われる可能性があることから，適切な格子間隔は切り抜きサイズに依存する．格子間隔が狭いと攻撃後により多くの格子線を検出できるが，画質が下がってしまう．一方で，格子間隔が広いと推定するために十分な数の格子線を検出できない可能性がある．したがって，推定される変換行列の精度と結果として得られる画像品質を考慮して，画像サイズに応じて適切な格子間隔を決定する必要がある．

本実験では，20 から 120 画素までの様々な格子間隔のパイロット信号を埋め込み，最適な格子間隔を決定する．格子線幅は 5 画素とする．変換行列は単位行列とし，切り抜きのみを加えた画像から行列を推定した．図に異なる格子間隔における推定変換行列の相対誤差を示す．図 3.11(a) には高

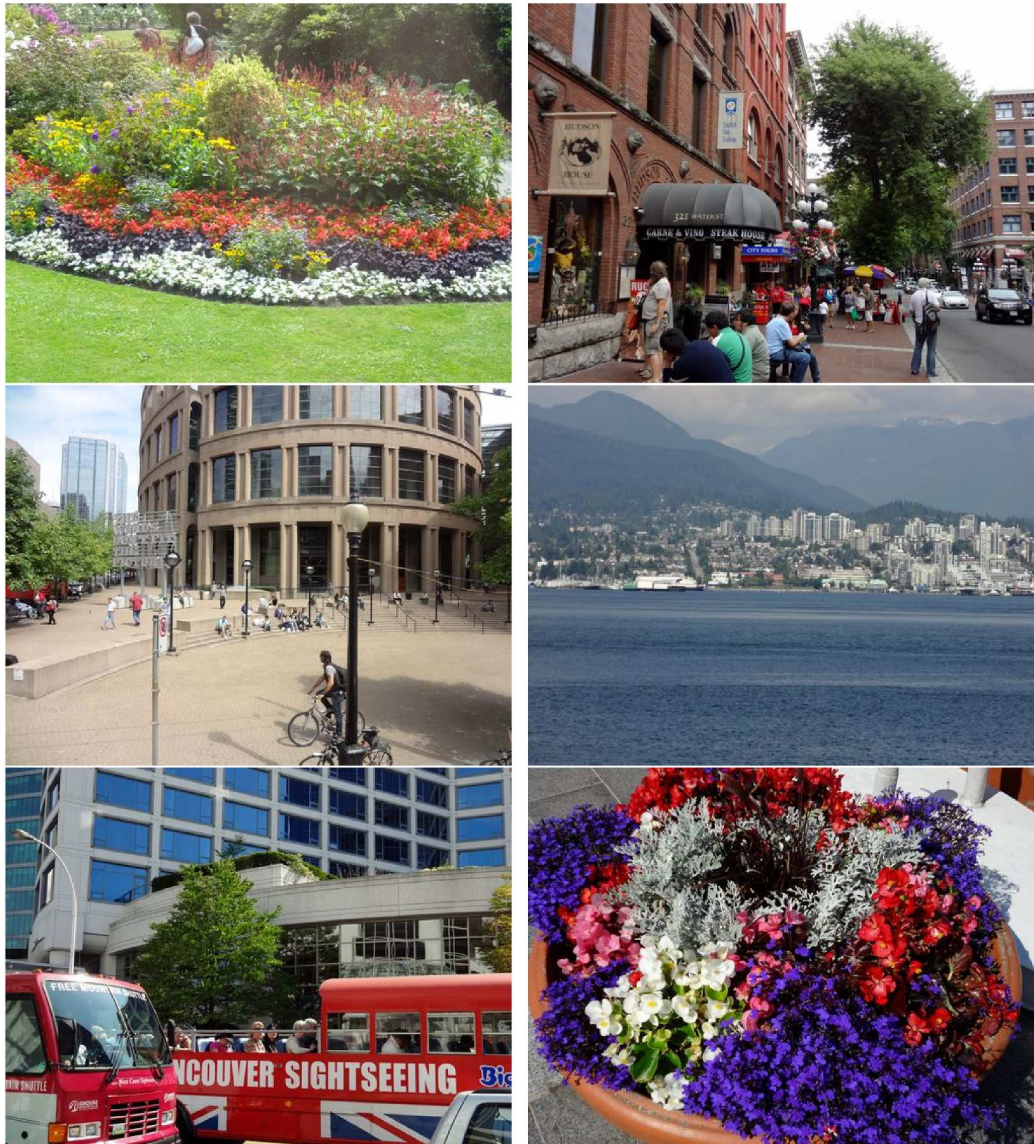


図 3.9: 高画素数画像 (4608 × 3456 画素)

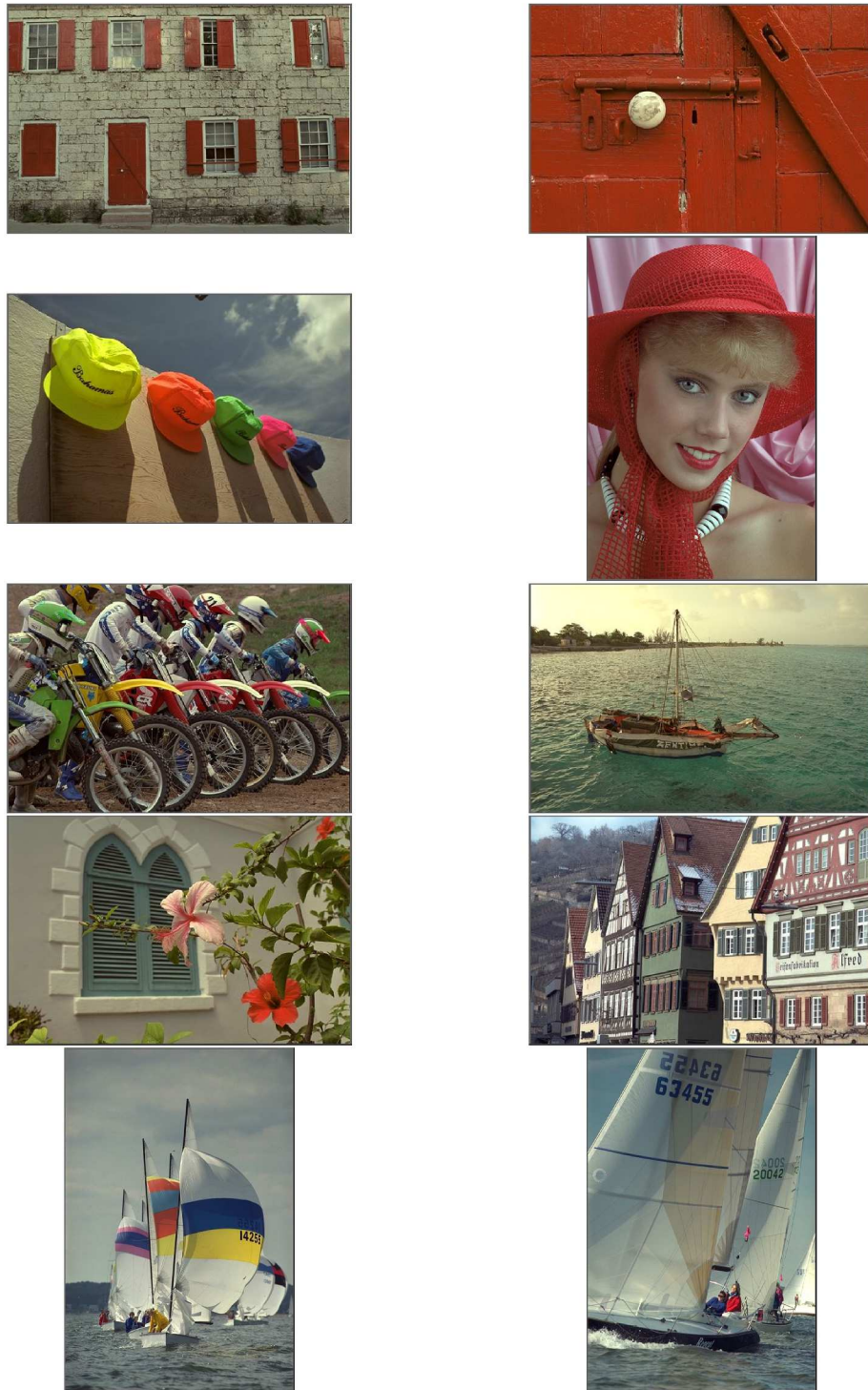


図 3.10: 低画素数画像 (768 × 512 画素または 512 × 768 画素)

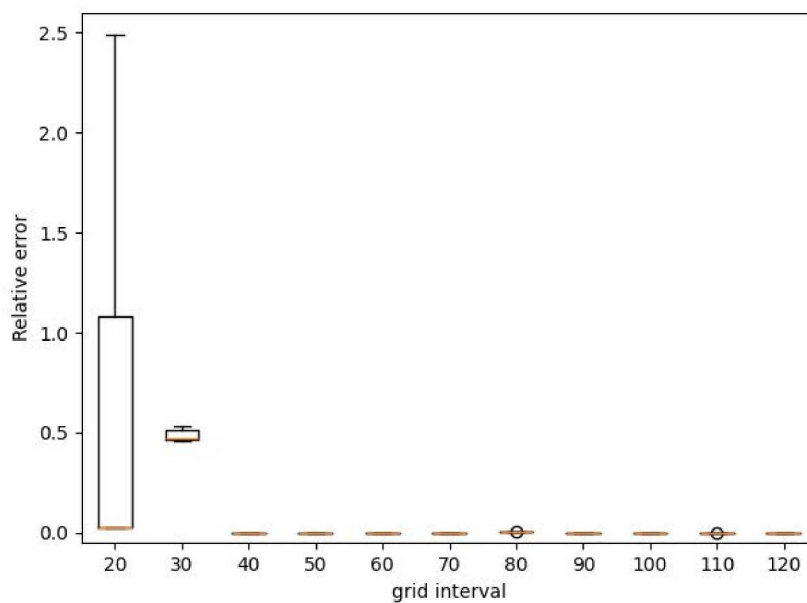
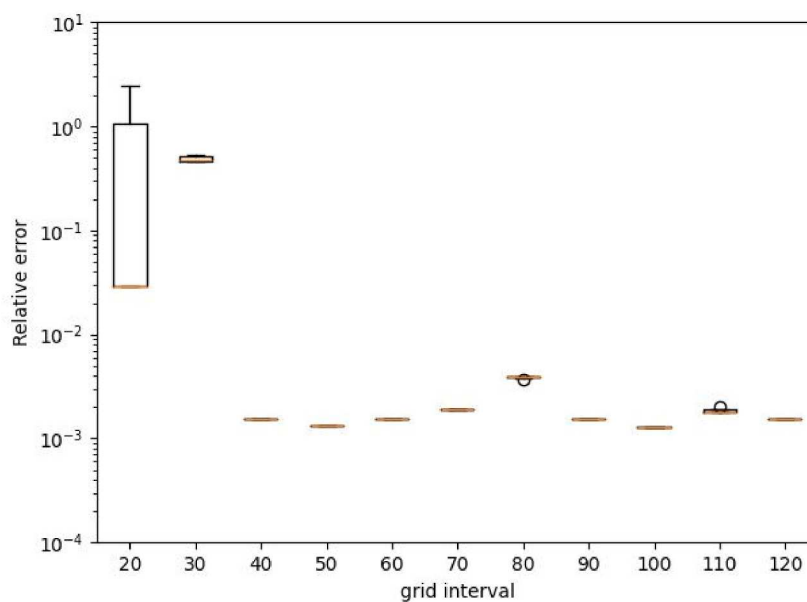
画素数画像の結果を、図 3.12(b) には低画素数画像の結果を示す。また、図 3.11(b), 図 3.12(b) はそれぞれの結果の常用対数グラフである。横軸は格子間隔を、縦軸は相対誤差を表す。箱ひげ図は、各格子間隔における全画像の結果の四分位数を表し、橙線は中央値を表す。トリミング画像からパイロット信号が検出されなかった場合、その結果は除外される。低画素数画像の場合は格子間隔 80 画素の画像 1 枚、120 画素の画像 2 枚でパイロット信号が検出できなかった。その他の画像についてはパイロット信号を検出することができた。

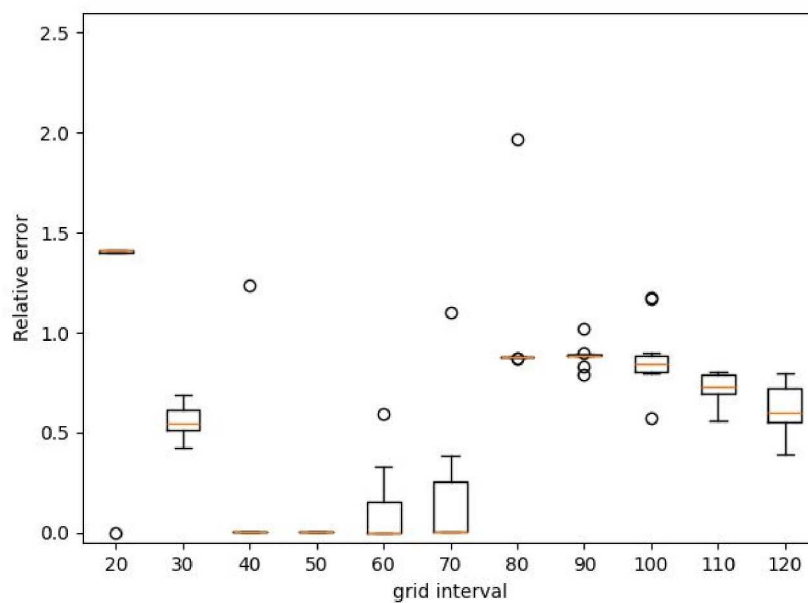
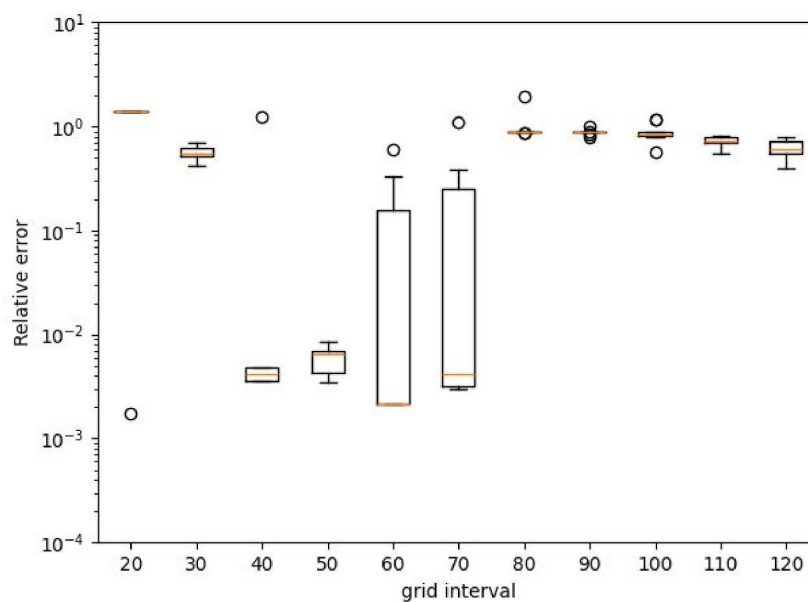
高画素数画像では格子間隔が 40 以上の場合に相対誤差が 0.01 未満で推定することができた。一方で、低画素数画像では格子間隔が 40 から 70 画素の場合に相対誤差の中央値が 0.01 未満で推定することができた。しかし、その他の格子間隔では相対誤差が大きくなった。高画素数画像では、格子間隔が大きい場合でも画像中に埋め込まれている格子線が多いため、低い相対誤差で推定することができた。しかし、低画素数画像の場合は格子線が少ないため、格子間隔が正確に検出できずに相対誤差が大きくなった。また、いずれの場合でも格子線幅が 5 画素であるため、格子間隔が 30 以下の場合にラドン係数のピークが鈍る様子が見られた。したがって、係数の特徴によって誤った角度や間隔を検出することがわかった。

図 3.13 に格子間隔毎のステゴ画像の PSNR を示す。図より、格子間隔が狭いほど埋め込まれる格子線の数が増えるため、画質が低下する。ただし、高画素数画像と低画素数画像を比較すると、単位面積あたりの埋め込まれた格子線の面積は等しいため、画像サイズに関わらず画質は一定である。ステゴ画像の画質をなるべく維持しつつ推定行列の相対誤差は十分小さくしなければならない。さらに、画像が幾何攻撃によって歪むことも想定する必要がある。そのため、実験により格子間隔の大きさは、高画素数画像では $G = 100$ 画素、低画素数画像では $G = 50$ 画素とした。このときの平均 PSNR は高画素数画像で 43.6 dB、低画素数画像で 40.6 dB であった。

3.4.3 単一攻撃の推定変換行列

単一攻撃における推定変換行列の精度を評価する。ステゴ画像には異方性拡大縮小 ($S_x; S_y$) と回転 θ_r 、剪断 θ_y のいずれかの攻撃を適用する。表 3.1 に各攻撃パラメータを示す。異方性拡大縮小の評価では x 軸の拡大率を $S_x = 1:0$ 倍に固定し、 y 軸方向の拡大率 S_y のみを変更する。同様に、剪断については y 軸方向の剪断のみを考慮する。

(a) 格子間隔 G 毎の相対誤差 E (線形スケール)(b) 格子間隔 G 毎の相対誤差 E (常用対数グラフ)図 3.11: 高画素数画像における格子間隔 G 毎の相対誤差 E

(a) 格子間隔 G 毎の相対誤差 E (線形スケール)(b) 格子間隔 G 毎の相対誤差 E (常用対数グラフ)図 3.12: 低画素数画像における格子間隔 G 毎の相対誤差 E

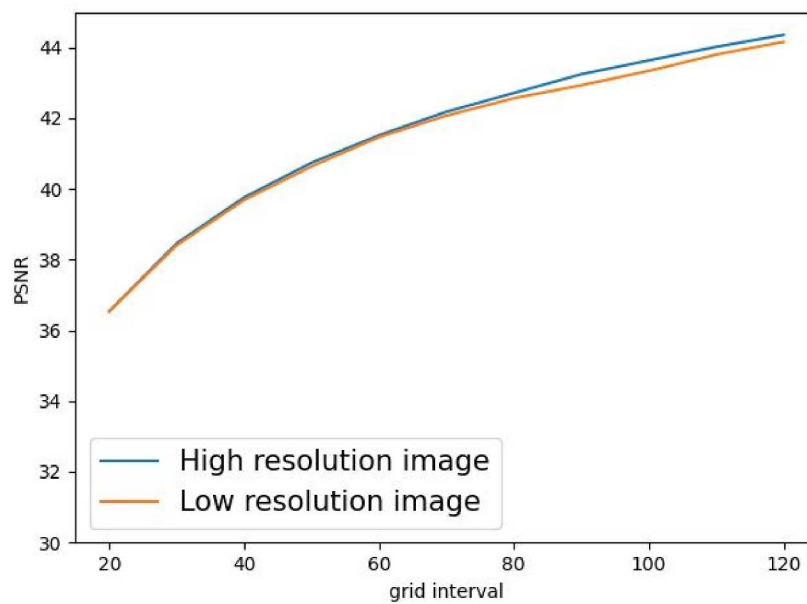


図 3.13: 格子間隔に対する PSNR

表 3.1: 変換行列推定時の攻撃パターン

攻撃の種類	パラメータ
異方性拡大縮小	$S_x = 1:0, S_y = 0:1:0:2:\dots:2:0$
回転角度	$\theta_r = 0:5:10:\dots:90$
剪断角度	$\theta_x = 0, \theta_y = 0:5:10:\dots:80$

異方性拡大縮小を適用するための変換行列は

$$T_m = \begin{pmatrix} S_x & 0 \\ 0 & S_y \end{pmatrix}; \quad (3.21)$$

で与えられる。この行列に対する相対誤差 $E(\hat{T}; T_m)$ で評価する。図 3.14(a) は高画素数画像の結果、図 3.15(a) は低画素数画像の結果を示す。また、図 3.14(b) と図 3.15(b) はそれぞれの結果の常用対数グラフを示す。横軸と縦軸はそれぞれ拡大率 S_y と相対誤差を表す。箱ひげ図は各拡大率 S_y における全画像の結果の四分位数を表す。ただし、パイロット信号が検出できなかった場合は統計量から除外されている。橙線は中央値を表している。高画素数画像の場合、拡大率が 0.2 – 1.9 倍の画像において相対誤差が 0.01 未満で推定できた。拡大率が小さい場合は格子間隔が細くなるため、検出間隔の推定が困難となってパイロット信号を検出できなくなる。拡大率が大きい場合にパイロット信号の検出に失敗する原因は、トリミング画像に含まれる格子線の数が減るためである。画像内に十分な格子線がない場合、元の画像成分によって検出角と検出間隔が不正確になる可能性がある。

低画素数画像では、拡大率が 0.4 – 1.3 倍の画像において相対誤差の中央値が 0.1 未満で推定できた。ただし、拡大率が 0.1; 0.2; 1.9; 2.0 倍の時、10 枚中 1 枚の画像で行列の推定に失敗した。低画素数画像ではトリミング画像内の格子線が少ないため、高画素数画像よりも行列の推定が困難となる。

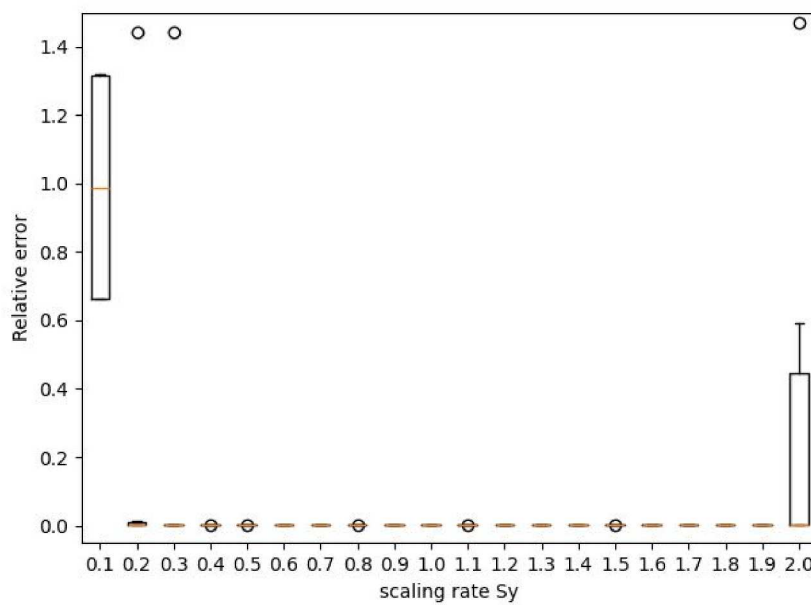
次に、回転攻撃の結果を示す。回転変換行列は

$$T_r = \begin{pmatrix} \cos \theta_r & -\sin \theta_r \\ \sin \theta_r & \cos \theta_r \end{pmatrix}; \quad (3.22)$$

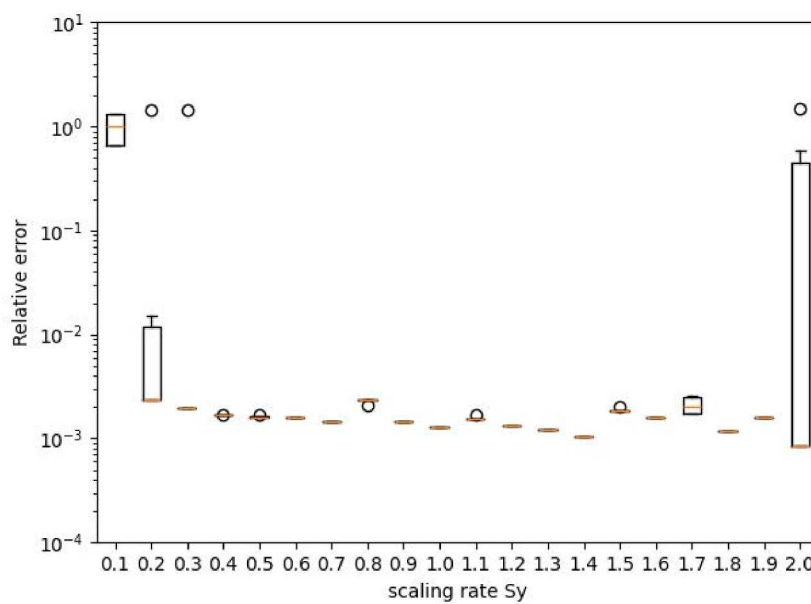
で与えられる。ここで、 θ_r は回転角度である。この行列に対する相対誤差 $E(\hat{T}; T_r)$ で評価する。図 3.16(a) は高画素数画像の結果、図 3.17(a) は低画素数画像の結果を示す。また、図 3.16(b) と図 3.17(b) はそれぞれの結果の常用対数グラフである。横軸と縦軸はそれぞれ回転角度 θ_r と相対誤差を表す。箱ひげ図は各回転角 θ_r における全画像の結果の四分位数を表し、橙線は中央値を表す。グラフより、高画素数画像の場合は全ての角度で相対誤差が 0.01 未満で推定できた。一方で、低画素数画像の場合は相対誤差の中央値が 0.02 未満で推定できた。言い換えると、少なくとも画像全体のうち半数において正しく推定することができた。しかし、高画素数画像と比較すると推定誤差が大きくなる場合が増えた。

次に、剪断の結果を示す。y 軸方向の剪断変換行列は

$$T_y = \begin{pmatrix} 1 & 0 \\ \tan \theta_y & 1 \end{pmatrix}; \quad (3.23)$$

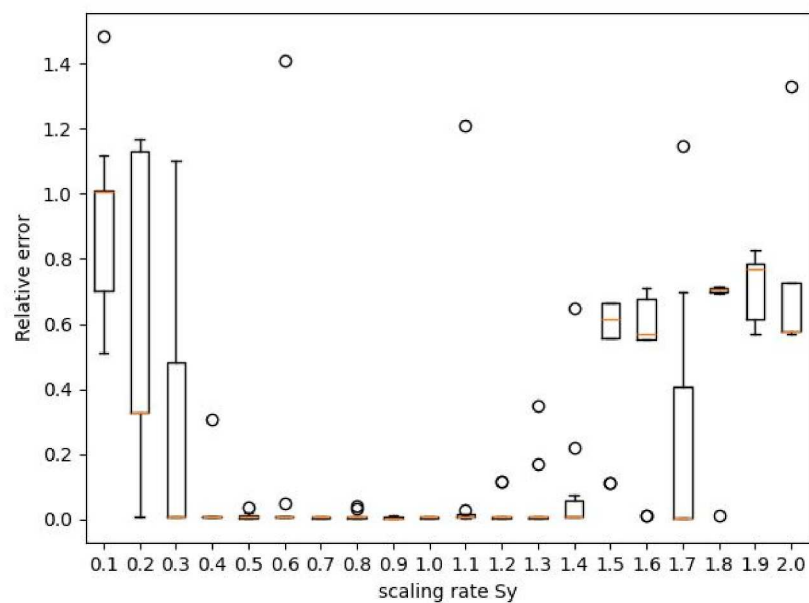


(a) 拡大率 S_y 毎の相対誤差 E (線形スケール)

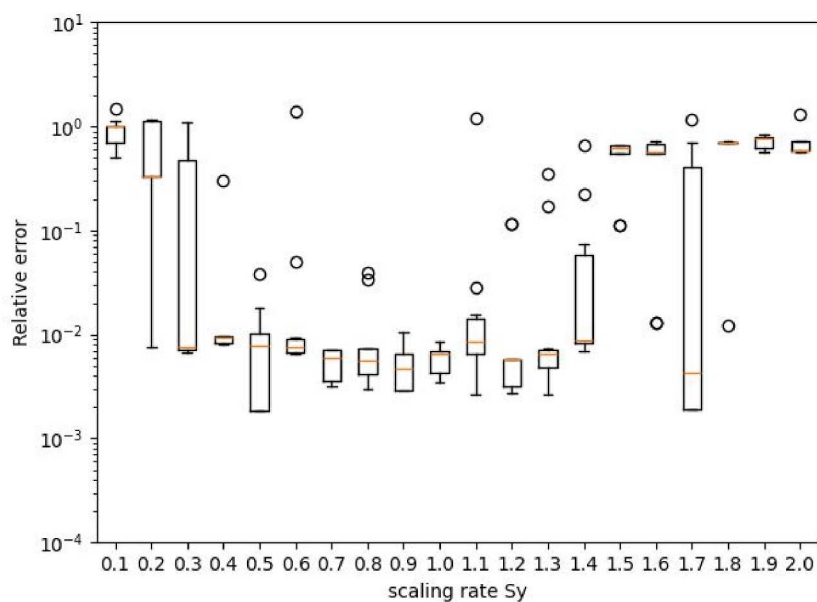


(b) 拡大率 S_y 毎の相対誤差 E (対数グラフ)

図 3.14: 高画素数画像における拡大率 S_y 毎の相対誤差 E

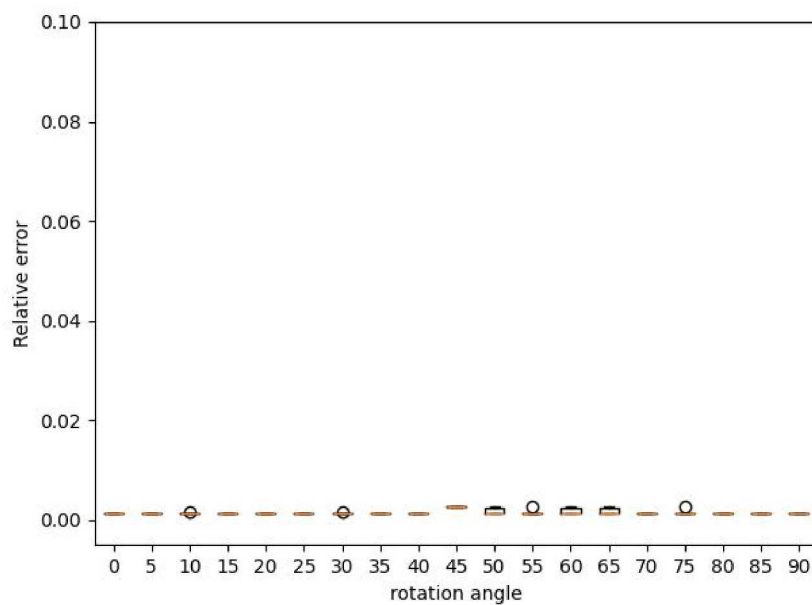


(a) 拡大率 S_y 毎の相対誤差 E (線形スケール)

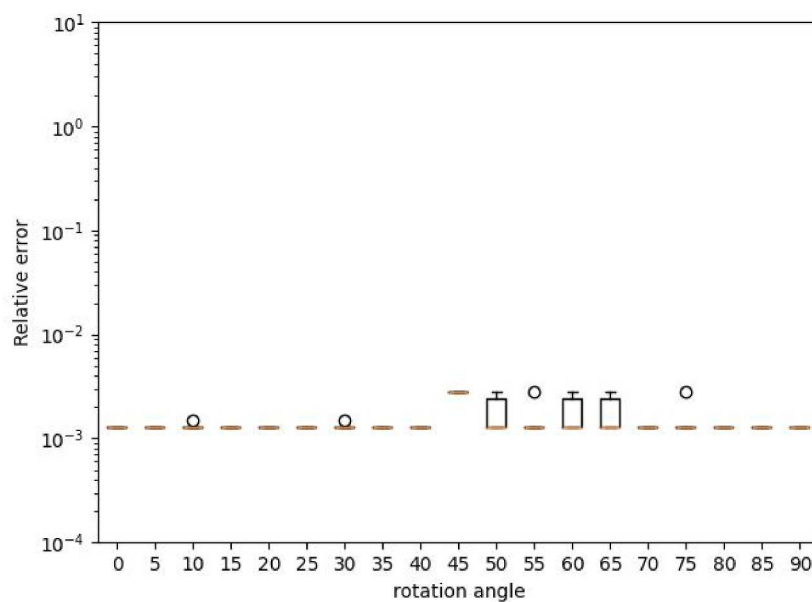


(b) 拡大率 S_y 毎の相対誤差 E (常用対数グラフ)

図 3.15: 低画素数画像における拡大率 S_y 毎の相対誤差 E

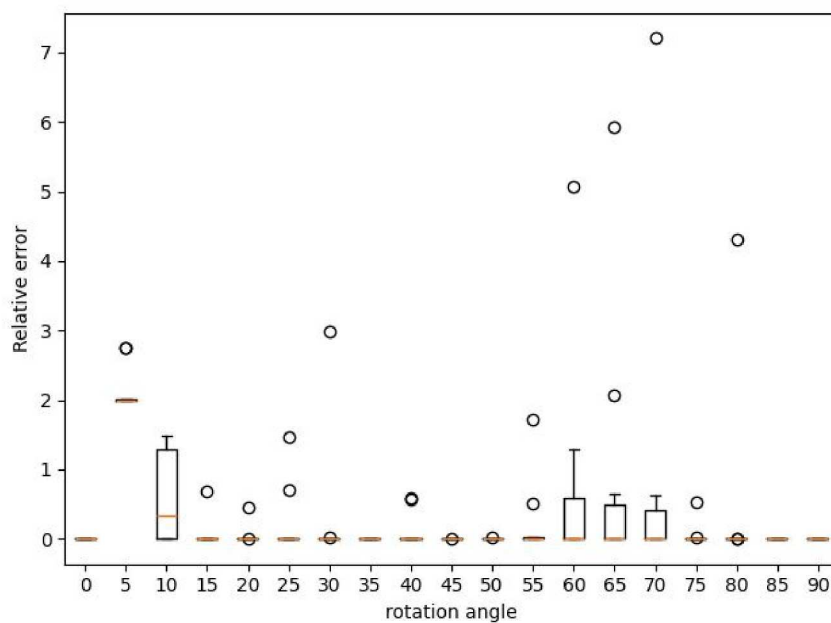
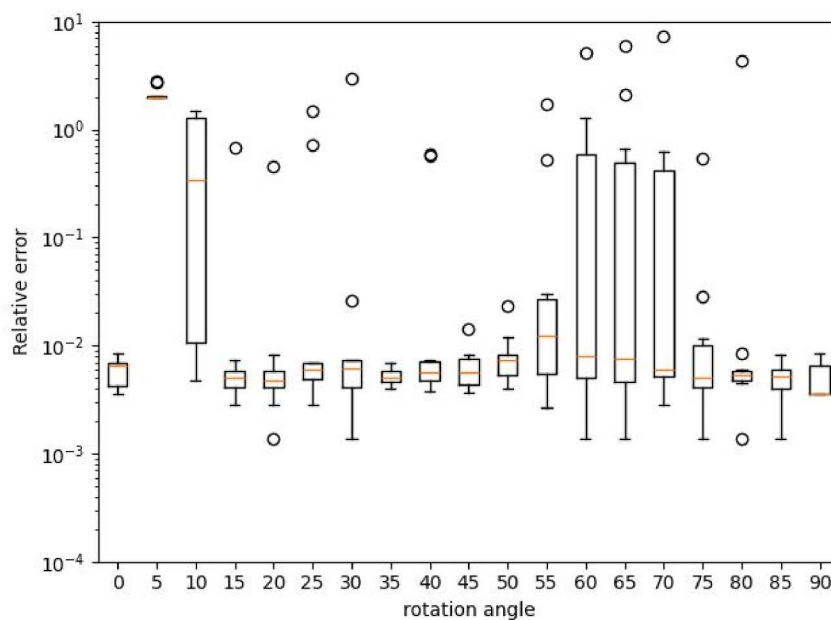


(a) 回転角 θ_r 毎の相対誤差 E (線形スケール)



(b) 回転角 θ_r 毎の相対誤差 E (常用対数グラフ)

図 3.16: 高画素数画像における回転角 θ_r 毎の相対誤差 E

(a) 回転角 θ_r 毎の相対誤差 E (線形スケール)(b) 回転角 θ_r 毎の相対誤差 E (常用対数グラフ)図 3.17: 低画素数画像における回転角 θ_r 毎の相対誤差 E

で与えられる．ここで， θ_y は y 軸方向の剪断角度を表す．同様に， x 軸方向の剪断角度は θ_x で表される．推定回転変換行列の相対誤差 $E(\hat{T}; T_y)$ を評価する．図 3.18(a) は高画素数画像の結果，図 3.19(a) は低画素数画像の結果を示す．また，図 3.18(b)，図 3.19(b) はそれぞれの結果の常用対数グラフを示す．横軸と縦軸はそれぞれ剪断角度 θ_y と相対誤差を表す．箱ひげ図は各剪断角度 θ_y における全画像の結果の四分位数を表し，橙線は中央値を表す．グラフより，高画素数画像では 70 度以下の剪断角度で相対誤差が 0.01 未満で推定できた．一方で，低画素数画像では 65 度未満の剪断角度で相対誤差の中央値が 0.01 未満で推定できた．

3.4.4 複合攻撃の推定行列

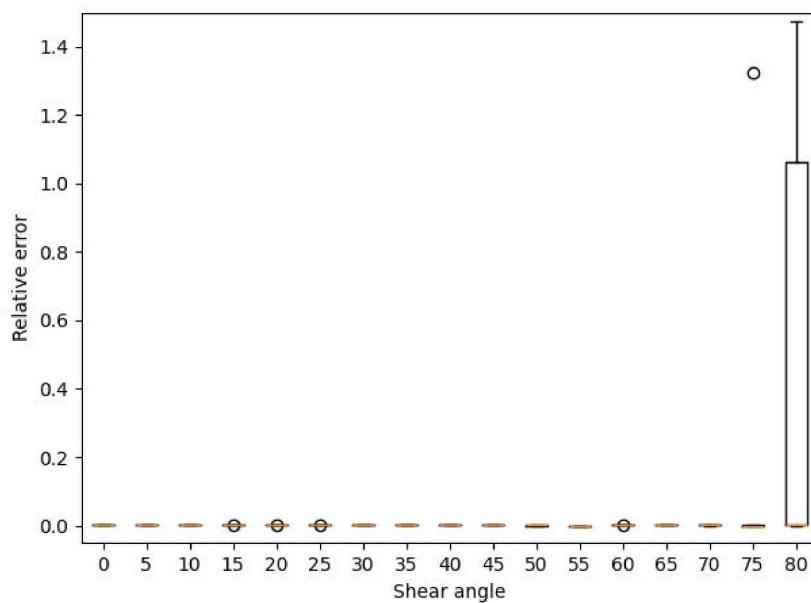
複合攻撃に対する推定変換行列の精度を評価する．拡大縮小，回転，剪断の複合攻撃を適用し，劣化画像をさらにトリミングした画像から変換行列を推定した．最初の攻撃は変換行列 T_1 で表される．同様に，2 番目と 3 番目の攻撃はそれぞれ行列 T_2, T_3 で表される．これらの複合攻撃は $T_c = T_3 T_2 T_1$ で与えられる．表 3.2 に変換行列 T_1, T_2, T_3 の組み合わせを示す．複合攻撃では変換の順序によって結果が異なることに注意する．攻撃の組み合わせは多数存在することから，本実験では表 3.2 で挙げた 12 パターンの複合攻撃を用いた．表中において拡大縮小は S_x, S_y ，回転攻撃は θ_r で表される．また，剪断攻撃は θ_x, θ_y で表される．パターン 1 の例では，まず T_1 で表される y 方向の剪断変換を行う．次に T_2 で表される拡大縮小変換を行い，最後に T_3 で表される x 方向の剪断変換によって変換される．これらの行列は

$$T_1 = \begin{pmatrix} 1:0 & 0:0 \\ \tan \frac{50\pi}{180} & 1:0 \end{pmatrix}; T_2 = \begin{pmatrix} 0:6 & 0:0 \\ 0:0 & 1:1 \end{pmatrix}; T_3 = \begin{pmatrix} 1:0 & \tan \frac{65\pi}{180} \\ 0:0 & 1:0 \end{pmatrix}; \quad (3.24)$$

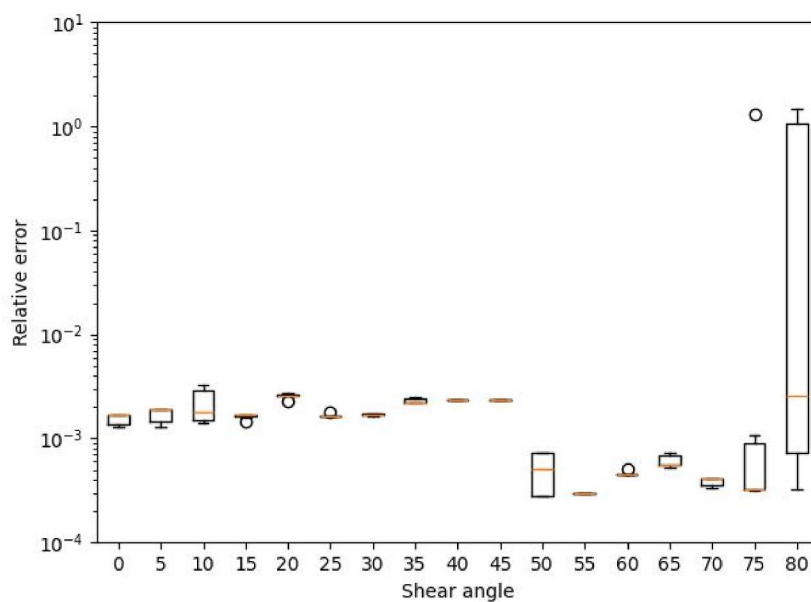
で表される．

図 3.20 に複合攻撃による劣化画像の例を示す．図 3.20(a) に格子線を含む原画像の例を示す．この画像に対してパターン 6 の変換行列を適用した結果を図 3.20(b) に，パターン 11 の変換行列を適用した結果を図 3.20(c) に示す．図のように画像変換によって格子線がより細くなり，線の検出が困難になる場合がある．

様々な複合攻撃に対する推定変換行列の相対誤差を示す．図 3.21(a) は高画素数画像の結果を，図 3.22(a) は低画素数画像の結果を示す．また，図 3.21(b) と図 3.22(b) はそれぞれの結果の常用対数グラフを示す．横軸と縦軸はそれぞれ攻撃パターン番号と相対誤差を表す．各攻撃の結果は箱ひげ図で示されている．図 3.20(c) に示すような強い複合攻撃を受けた結果も含め，高画素数画像の結果

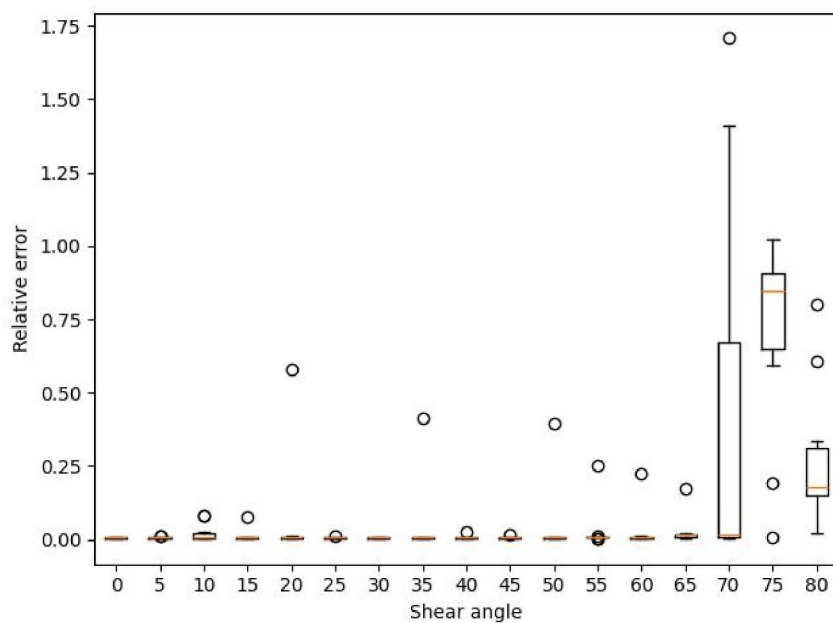
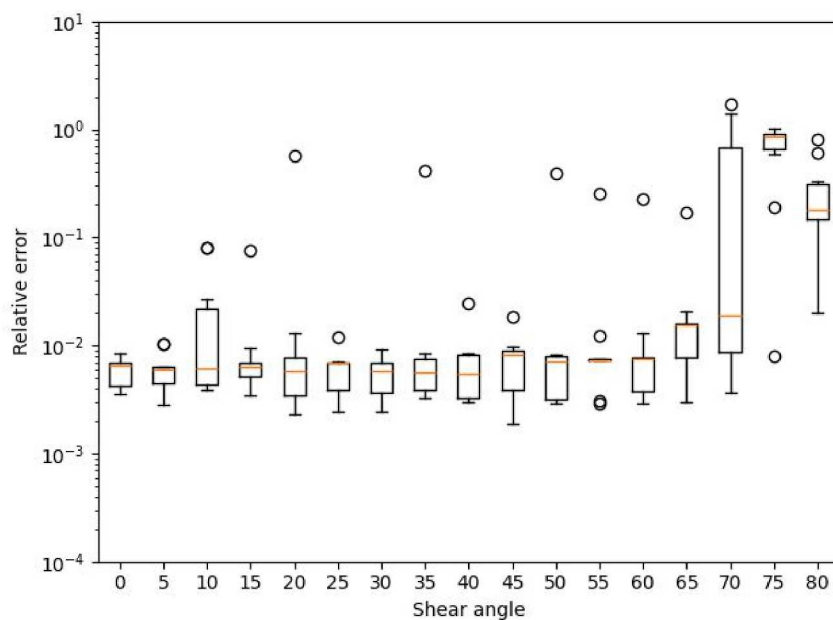


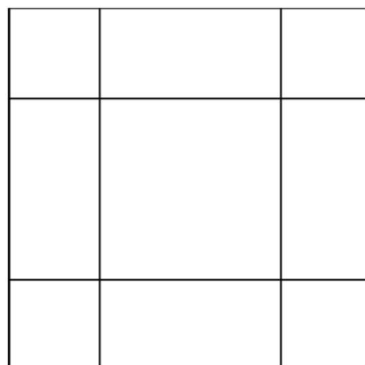
(a) 剪断角 θ_y 毎の相対誤差 E (線形スケール)



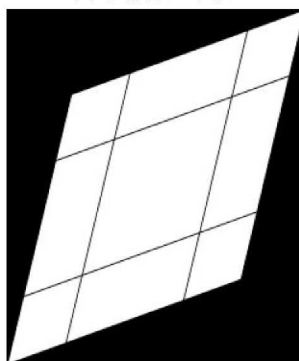
(b) 剪断角 θ_y 毎の相対誤差 E (常用対数グラフ)

図 3.18: 高画素数画像における剪断角 θ_y 毎の相対誤差 E

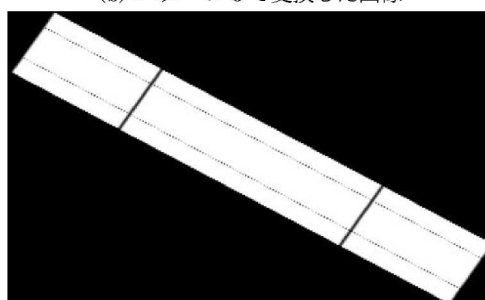
(a) 剪断角 θ_y 毎の相対誤差 E (線形スケール)(b) 剪断角 θ_y 毎の相対誤差 E (常用対数グラフ)図 3.19: 低画素数画像における剪断角 θ_y 毎の相対誤差 E



(a) 変換前の画像



(b) パターン 6 で変換した画像



(c) パターン 11 で変換した画像

図 3.20: 複合攻撃によって劣化した画像の例

表 3.2: 攻撃推定で用いた複合攻撃の組み合わせ

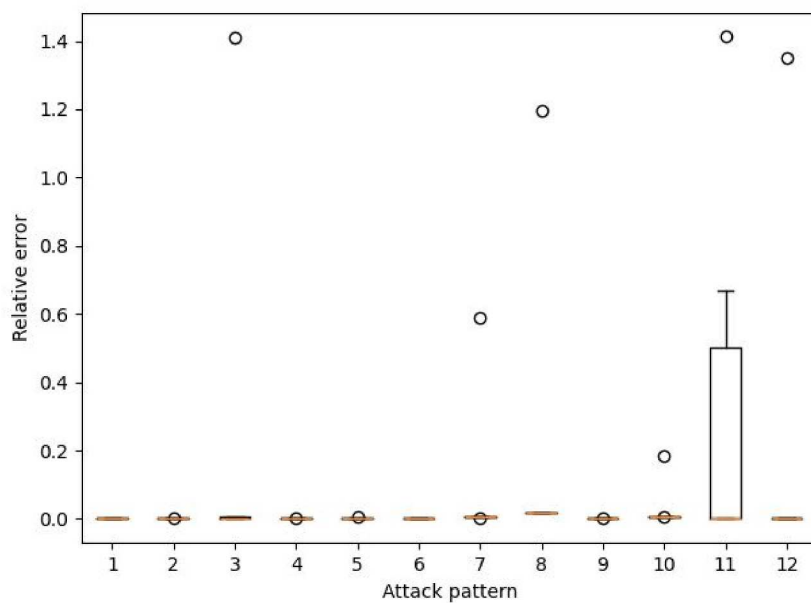
	pattern 1	pattern 2	pattern 3
T_1	$\theta_y = 50$	$\theta_r = 30$	$\theta_y = 40$
T_2	$S_x = 0:6; S_y = 1:1$	$\theta_x = 30$	$S_x = 1:5; S_y = 1:3$
T_3	$\theta_x = 65$	$\theta_y = 65$	$\theta_x = 25$
	pattern 4	pattern 5	pattern 6
T_1	$\theta_x = 60$	$S_x = 0:8; S_y = 1:4$	$\theta_y = 20$
T_2	$S_x = 1:3; S_y = 0:5$	$\theta_r = 250$	$\theta_x = 55$
T_3	$\theta_y = 70$	$\theta_y = 15$	$\theta_r = 355$
	pattern 7	pattern 8	pattern 9
T_1	$\theta_y = 70$	$S_x = 1:9; S_y = 1:5$	$S_x = 0:7; S_y = 1:1$
T_2	$\theta_r = 195$	$\theta_x = 45$	$\theta_r = 215$
T_3	$S_x = 1:2; S_y = 1:5$	$\theta_y = 55$	$\theta_x = 60$
	pattern 10	pattern 11	pattern 12
T_1	$\theta_y = 30$	$S_x = 0:9; S_y = 0:5$	$S_x = 0:6; S_y = 1:1$
T_2	$\theta_x = 65$	$\theta_r = 245$	$\theta_y = 60$
T_3	$\theta_r = 105$	$\theta_x = 20$	$\theta_y = 0$

は概ね良好であった．一方で，低画素数画像では相対誤差の中央値が 0.01 未満で推定できたパターンがある一方で，相対誤差が大きいパターンが多くみられた．加えて，パターン 8 では 10 枚中 7 枚，パターン 11 では 4 枚，パターン 12 では 2 枚の画像で変換行列の推定に失敗した．このように，画像サイズが小さい場合は複合攻撃の推定が困難である．

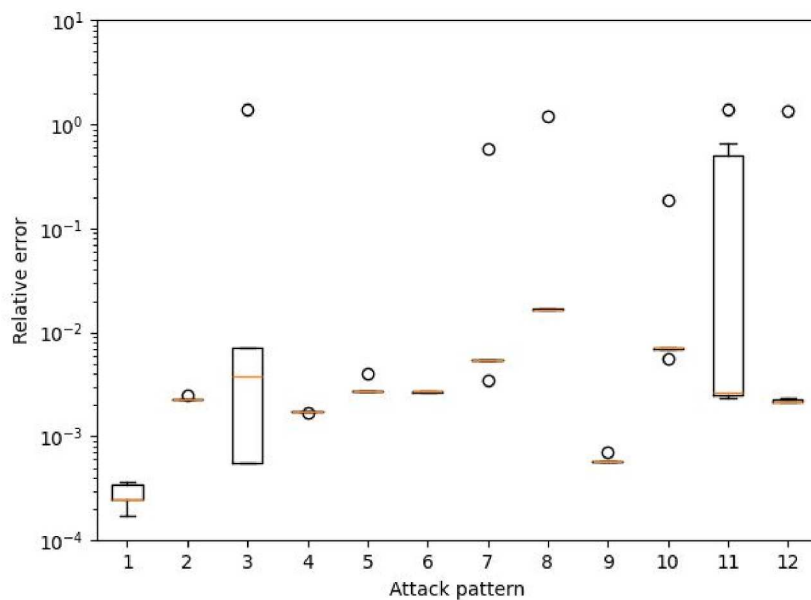
3.5 攻撃推定による透かし情報の評価

提案する幾何攻撃の推定手法は，従来の電子透かし法に導入することが可能である．本節では提案手法による攻撃推定を導入した電子透かし法を，透かし情報の誤り率で評価する．

従来の幾何攻撃に対して堅牢とされる電子透かし法の多くは，トリミングによって画像サイズが変化すると透かし情報の抽出が困難となる．トリミング攻撃に堅牢な電子透かし法として 2 章で述べた SIFT 特徴点を用いた手法が挙げられる．この手法では画像中の複数の SIFT 特徴点の周辺の領域を埋め込み領域として使用する．そのため，画像がトリミングされても特徴点が検出できれば透かし情報を抽出可能である．しかしながら，SIFT 特徴点を用いた手法では，剪断やその他の幾何攻撃によって埋め込み領域の形状が歪むと透かし情報の抽出が困難となる．この問題を解決するために，

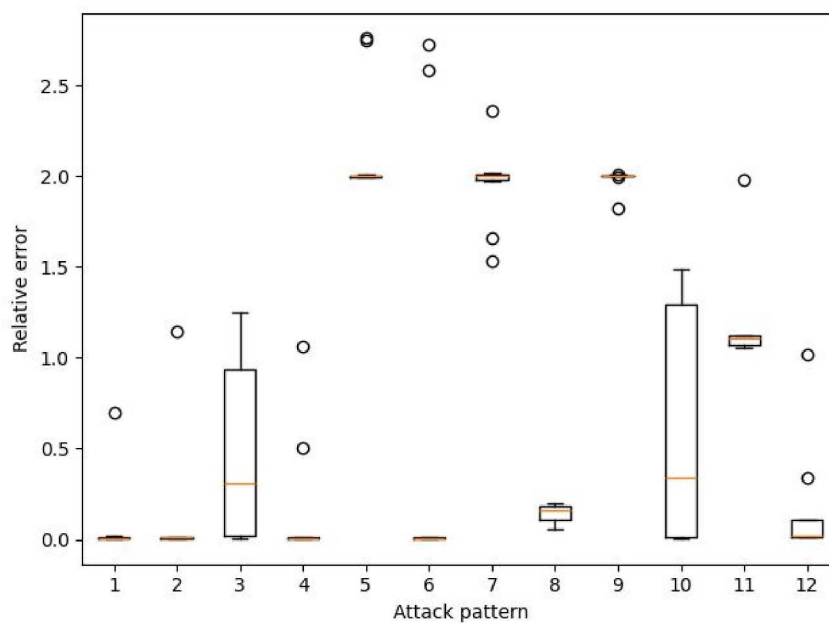
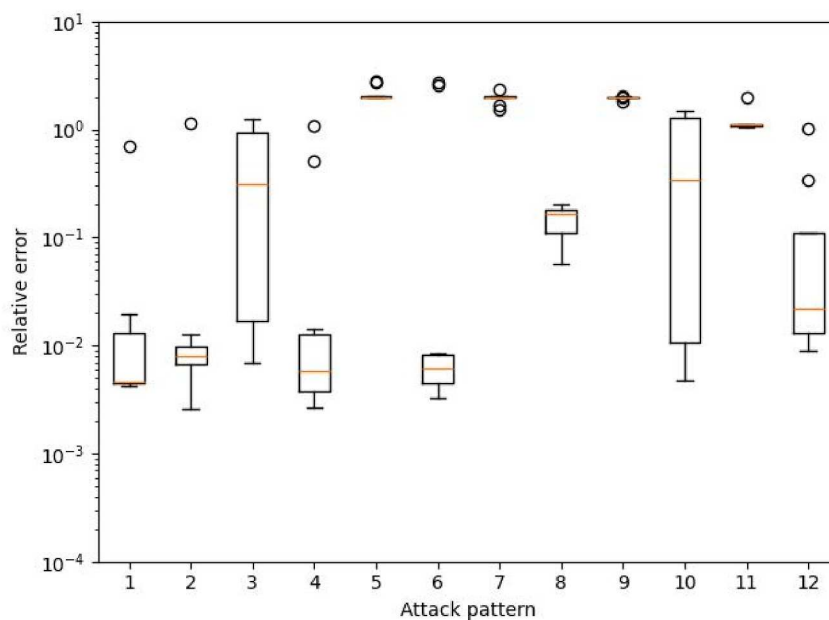


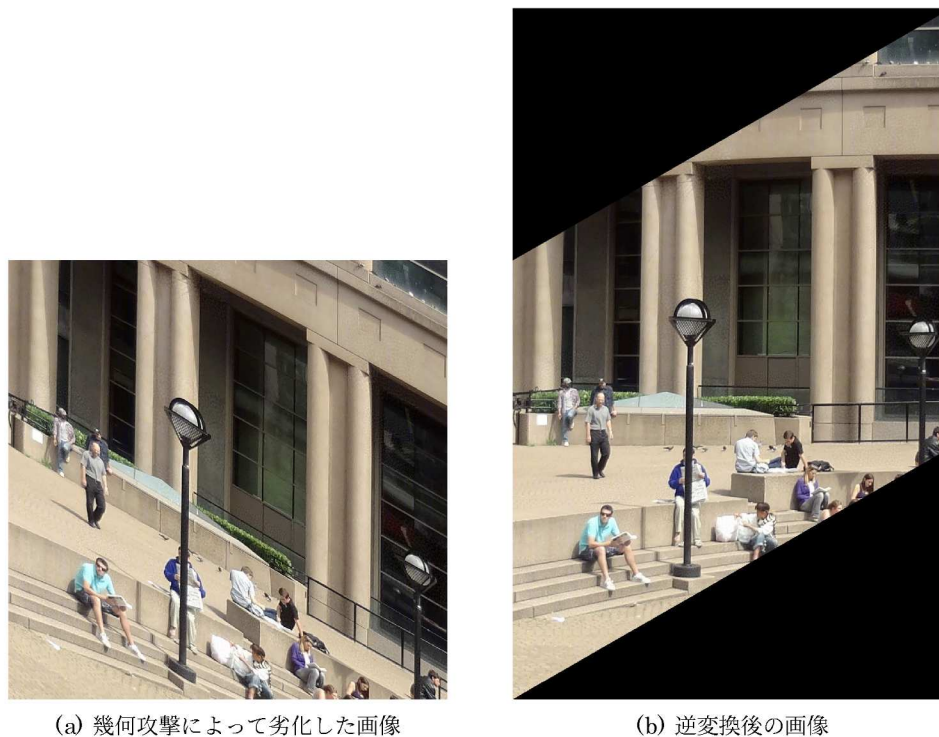
(a) 複合攻撃毎の相対誤差 E (線形スケール)



(b) 複合攻撃毎の相対誤差 E (常用対数グラフ)

図 3.21: 高画素数画像における複合攻撃毎の相対誤差 E

(a) 複合攻撃毎の相対誤差 E (線形スケール)(b) 複合攻撃毎の相対誤差 E (常用対数グラフ)図 3.22: 低画素数画像における複合攻撃毎の相対誤差 E



(a) 幾何攻撃によって劣化した画像

(b) 逆変換後の画像

図 3.23: 攻撃を受けた画像とその逆変換画像の例

我々は攻撃推定手法を導入する．まず，図 3.23(a) に示すような劣化画像から変換行列を推定し，逆行列を求める．次に，図 3.23(b) に示すように，画像を逆変換することで歪みを補正する．最後に逆変換画像から透かし情報を抽出する．提案手法を導入した電子透かし法を透かし情報のビット誤り率 (BER) で評価する．また，電子透かし法とパイロット信号の両方が埋め込まれている場合の画質を PSNR で評価する．

本実験では 2 章で述べた電子透かし法を用いる．この手法には画像サイズに対して埋め込める透かし情報の量に限界がある．透かし情報は SIFT 特徴点の中心として一辺 120 から 180 画素の正方形の領域に埋め込まれる．透かし情報を抽出するには 2 つ以上の透かし情報を含める必要がある．切り出しサイズを十分に大きくする必要があることから，本節ではこの手法を高画素数画像にのみ適用する．

3.5.1 実験条件

6枚の IHC 標準画像 [35](4608 × 3456 画素) を原画像として用い、これらの画像の U 成分にパイロット信号を埋め込む。また、2章で述べた手法を用いて Y 成分に 300 bit の透かし情報を埋め込む。ただし、ここでは透かし情報に誤り訂正を用いない。ステゴ画像は変換行列 T を用いた幾何攻撃を加えた後に、任意の位置から 1080 × 1080 画素にトリミングされる。このトリミングされた 6 枚の画像から抽出された透かし情報の平均 BER を各攻撃について評価する。

ここで、我々の攻撃推定手法では、1つの劣化画像から 2つの変換行列が推定される。これらの行列は 180 度回転することで一致すると言う点で関連している。これらを直接区別することはできないことから、本実験ではそれぞれの行列を用いて逆変換画像を生成する。これらの逆変換画像から得られた推定透かし情報のうち、より BER が低い方の行列が正しい結果として採用される。現在はどちらの推定透かし情報が正しいかを判断することはできない。しかし、この問題は透かし情報とは別に既知の判定ビットを埋め込むことで解決可能である [20]。2章に示す通り、本手法では透かし情報を DFT 係数に埋め込んだ。DFT 係数の性質として、画像が回転すると DFT 係数の座標は回転角と同じ角度で回転する。また、中心座標に対して点対象な座標同士の係数値は等しい。そのため、実際には 180 度回転は透かし情報の抽出時に考慮する必要はない。

3.5.2 画質評価

画質を PSNR で評価する。透かし情報のみを原画像に埋め込んだステゴ画像の平均 PSNR は 38.29 dB であった。一方、透かし情報とパイロット信号の両方を埋め込んだステゴ画像の平均 PSNR は 37.25 dB であった。したがって、パイロット信号による画質の平均劣化は 1.04 dB であった。

3.5.3 単一攻撃に対する評価

次に、パイロット信号と透かし情報が埋め込まれたステゴ画像に単一の攻撃を適用し、劣化画像から透かし情報を抽出する。ステゴ画像には異方性拡大縮小 ($S_x; S_y$) と回転 θ_r 、剪断 θ_y のいずれかの攻撃が加えられる。さらに、この劣化画像をトリミングする。表 3.3 に各攻撃のパラメータを示す。異方性拡大縮小の評価では x 軸方向の拡大率を $S_x = 1:0$ 倍に固定し、y 軸方向の拡大率のみを変化させる。また、剪断は y 軸方向のみを考慮する。

表 3.3: 透かし情報抽出時の攻撃の種類

攻撃の種類	パラメータ
異方性拡大縮小	$S_x = 1:0, S_y = 0:5; 0:8; 1:0; 1:3; 1:50$
回転角度	$\theta_r = 0; 30; 45; 60; 90$
剪断角度	$\theta_x = 0, \theta_y = 5; 20; 35; 50; 65$

図 3.24(a) に異方性拡大率に対する透かし情報の BER を示す。図 3.24(b) には常用対数グラフを示す。横軸と縦軸はそれぞれ拡大率 S_y と BER を表している。箱ひげ図は各拡大率における 6 枚のステゴ画像の結果を示している。橙線は中央値を表している。図に示すように、拡大率が 1.0 倍から離れるにつれて BER は増加する傾向がある。しかし、中央値はいずれの拡大率についても 0.1 未満で透かし情報を抽出することができた。

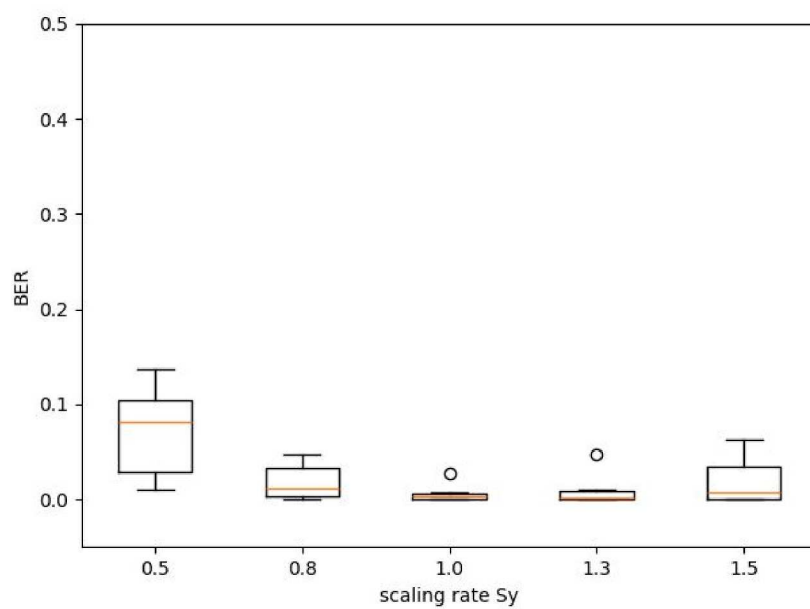
図 3.25(a) に回転角に対する透かし情報の BER を示す。図 3.25(b) には常用対数グラフを示す。横軸と縦軸はそれぞれ回転角 θ_r と BER を表している。箱ひげ図は各拡大率における 6 枚のステゴ画像の結果を示し、橙線は中央値を表している。図に示すように、0 度と 90 度の回転角度では BER が概ね 0.01 未満で抽出できる一方で、回転角が 45 度に近づくほど BER が大きくなることがわかった。しかし、BER の中央値は全ての角度において 0.04 未満で抽出できた。

図 3.26(a) に剪断角度に対する透かし情報の BER を示す。図 3.26(b) には常用対数グラフを示す。横軸と縦軸はそれぞれ剪断角度 θ_y と BER を表している。箱ひげ図は各拡大率における 6 枚のステゴ画像の結果を示している。橙線は中央値を表している。剪断角度 0 度から 35 度までの範囲では BER が概ね 0.05 未満で透かし情報を抽出することができた。逆に、剪断角が大きくなるにつれて BER は増加した。

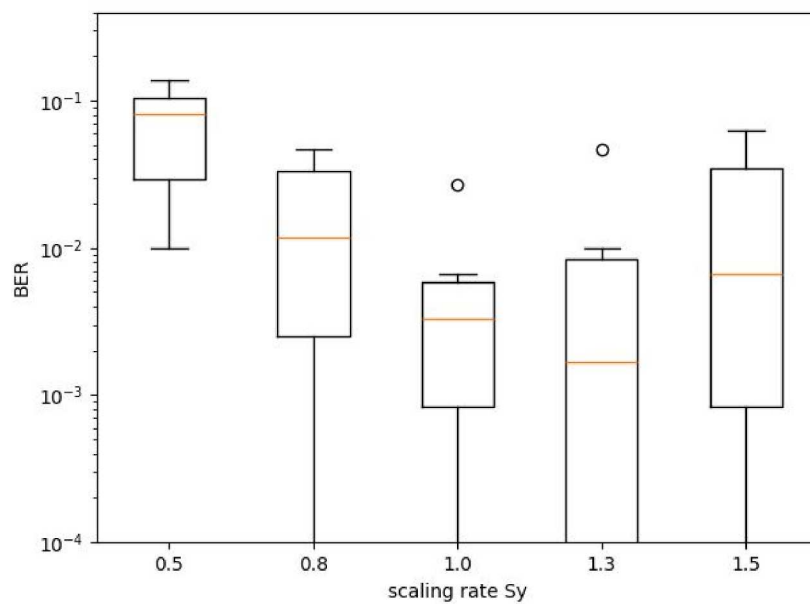
3.5.4 複合攻撃に対する評価

次に、複合攻撃に対する性能 BER を用いて評価した。ステゴ画像に 2 つの幾何攻撃を行い、その後トリミングした。表 3.4 に幾何攻撃 $T_1; T_2$ の組み合わせを示す。図 3.27(a) に、各攻撃パターンに対する透かし情報の BER を示す。また、図 3.27(b) に常用対数グラフを示す。横軸と縦軸はそれぞれ攻撃パターン、縦軸は BER を表している。透かし情報は全ての複合攻撃に対して中央値が 0.1 未満で推定することができた。

透かし情報の BER が大きくなる原因としては、透かし情報自体の消失が考えられる。例えば、図 3.18(a) に示した剪断角度 60 度における変換行列の相対誤差は小さいにも関わらず、図 3.26 の剪

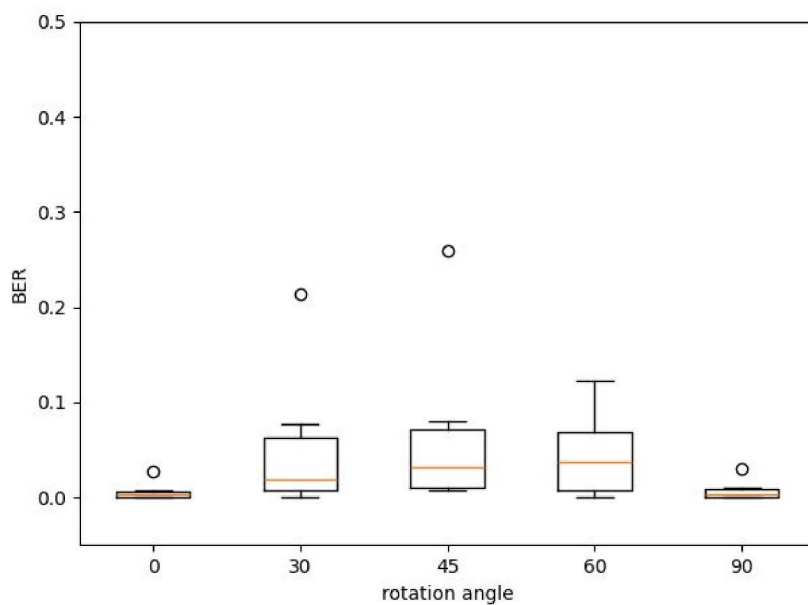


(a) 各拡大率毎の透かし情報の BER(線形スケール)

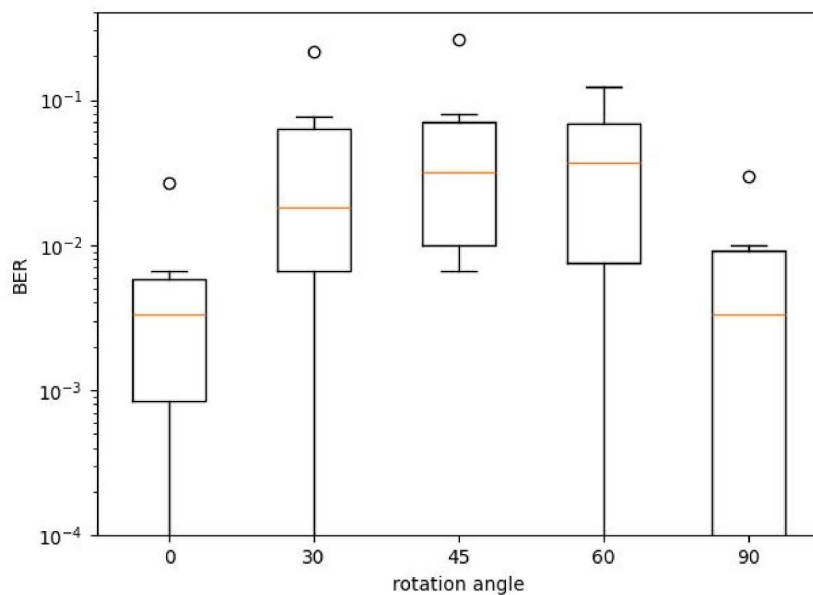


(b) 各拡大率毎の透かし情報の BER(対数グラフ)

図 3.24: 各拡大率毎の透かし情報の BER

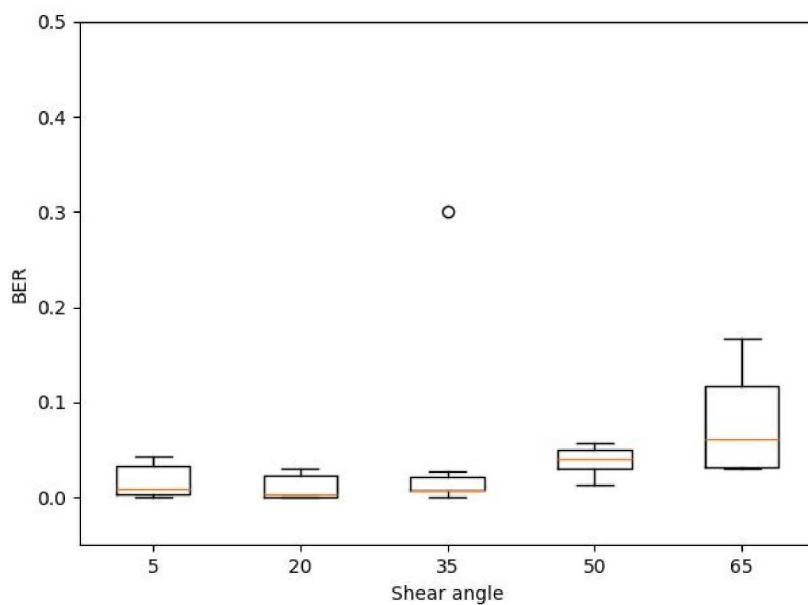


(a) 各回転角毎の透かし情報の BER(線形スケール)

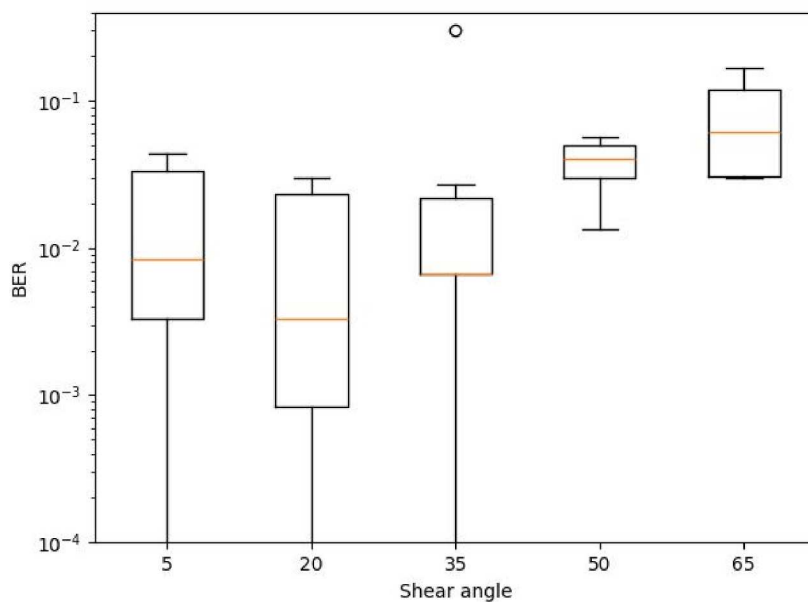


(b) 各回転角毎の透かし情報の BER(対数グラフ)

図 3.25: 各回転角毎の透かし情報の BER



(a) 各剪断角度毎の透かし情報の BER(線形スケール)



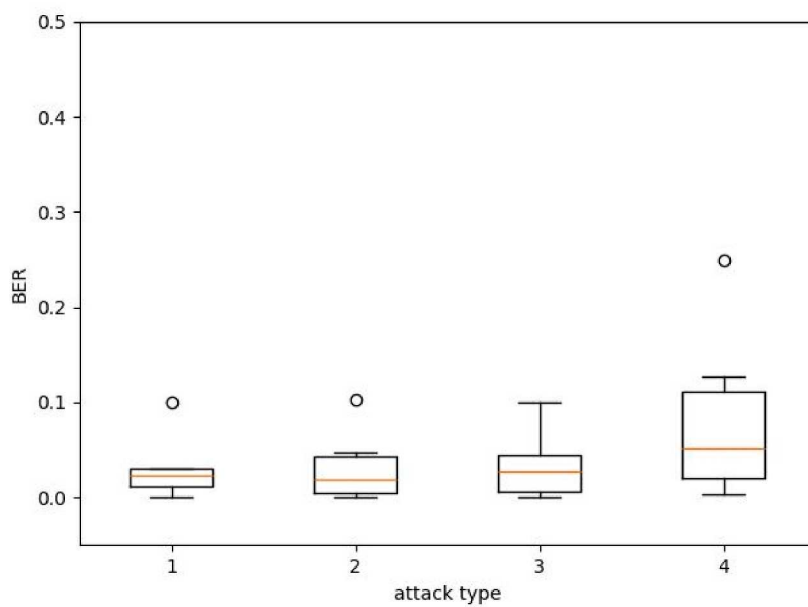
(b) 各剪断角度毎の透かし情報の BER(対数グラフ)

図 3.26: 各回転角毎の透かし情報の BER

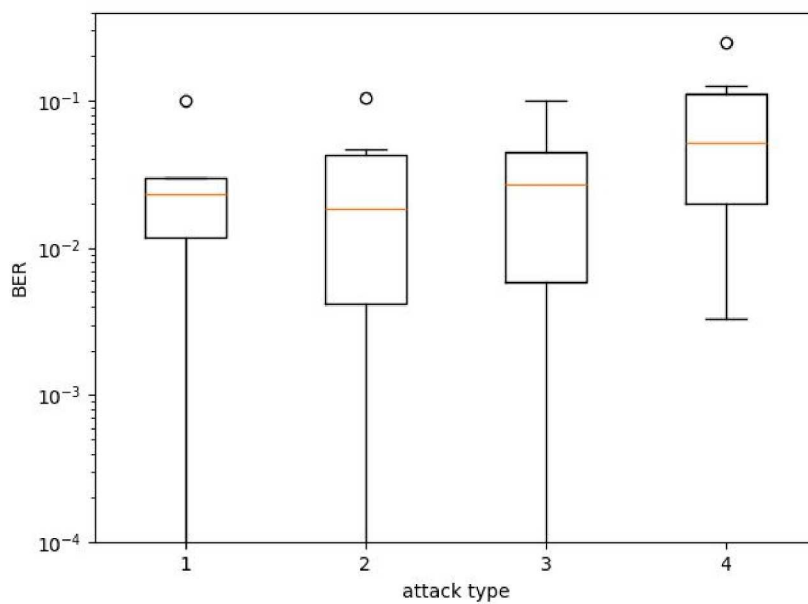
表 3.4: 攻撃推定で用いた複合攻撃の組み合わせ

	pattern 1	pattern 2
T_1	$\theta_y = 5$	$S_x = 1:0; S_y = 1:1$
T_2	$\theta_r = 10$	$\theta_r = 10$
	pattern 3	pattern 4
T_1	$\theta_r = 5$	$\theta_x = 10$
T_2	$S_x = 1:0; S_y = 1:2$	$\theta_y = 5$

断角度 60 度における透かし情報の BER は大きくなっている．このように，攻撃によって画像が大きく劣化すると，元の形状に逆変換できたとしても透かし情報の抽出は困難になる．これは他の電子透かし法についても同様に当てはまると考えられる．ただし，実際にはこのように強い幾何攻撃によって画像が劣化すると，画像自体の価値が失われる．



(a) 複合攻撃に対する透かし情報の BER(線形スケール)



(b) 複合攻撃に対する透かし情報の BER(対数グラフ)

図 3.27: 複合攻撃に対する透かし情報の BER

第4章 まとめ

SNS等で画像の不正利用が問題となっているため、不正利用対策のための技術として電子透かし法が注目されている。不正利用される際には圧縮等の非幾何攻撃や、拡大縮小やトリミング等の幾何攻撃によって画像が劣化する。多くの従来法では非幾何攻撃に対して堅牢である一方で、幾何攻撃に対して真に堅牢ではないという問題点があった。特に、トリミングによって画像が欠損した場合は透かし情報の抽出が困難となる。したがって、本研究ではパイロット信号による攻撃推定を導入した電子透かし法を提案した。本研究の貢献は、(1)パイロット信号を用いて幾何攻撃を推定する手法の開発及び、(2)トリミングを含む幾何攻撃に対して堅牢な電子透かし法の開発である。

2章では、パイロット信号を用いた拡大率推定を導入した電子透かし法を提案した。本手法では、画像のY成分からSIFT特徴点を検出し、SIFT特徴点の周辺領域を埋め込み領域とする。埋め込み領域をDFTすることで透かし情報を埋め込むことができる。また、画像のU成分輝度値に格子状の2値のパイロット信号を埋め込む。透かし情報の抽出時には拡大率を推定し、得られたパラメータを用いて透かし情報を抽出した。拡大率の推定では、パイロット信号の各行及び各列の総和を求めてその周期を検出することによって拡大率を推定した。実験では、拡大率の推定精度を相対誤差で評価した。その結果、0.5–1.5倍の拡大率で相対誤差が0.02以下で推定することができた。画像が更に拡大された場合、トリミング画像に含まれる格子線が少なかったことによって拡大率推定に失敗した。また、拡大率推定を導入した電子透かし法について、透かし情報の抽出精度をBERを用いて評価した。その結果、攻撃を推定した場合は0.7–1.3倍の範囲でBERの中央値は0になった。しかしながら、画像に加えた拡大率が大きいくほど透かし情報の抽出が困難になることがわかった。画像が拡大されるほどトリミング画像内に含まれる特徴点が少なくなるため、十分な数の透かし情報候補が得られなかったことが要因として考えられる。更に、透かし情報のみの画質と、透かし情報とパイロット信号を埋め込んだ場合の画質を比較した。その結果、パイロット信号を埋め込むことによって平均3.4 dB劣化することがわかった。

2章で述べた手法の問題点として、拡大縮小以外の攻撃（異方性拡大縮小や回転、剪断など）に対

する堅牢性は考慮していない点が挙げられる。そのため、埋め込み領域の形状がこれらの攻撃によって歪むと透かし情報の位置の検出が困難となる。したがって、3章では、3値のパイロット信号を用いた幾何変換行列の推定手法を提案した。本手法では、2章と同様に格子状のパイロット信号をU成分画像に埋め込む。2章と異なる点として、パイロット信号の垂直方向と水平方向を判別可能になるように設計した。また、パイロット信号をラドン変換することによって格子間隔と角度を検出し、得られたパラメータから変換行列を推定した。本手法は画像のサイズに応じて性能が変わるため、実験では高画素数画像と低画素数画像についてそれぞれ評価を行った。高画素数画像にはIHC画像を用い、低画素数画像にはKodak画像を用いた。画像サイズによって適切な格子間隔が異なることから、各画像サイズの格子間隔を相対誤差と画質の観点で決定した。格子間隔が狭いほど埋め込まれる格子線が増えるために検出しやすくなるが、画質が低下する。したがって、変換行列が推定可能な範囲でなるべく画質を維持できるように格子間隔を決定する必要がある。実験の結果、適切な格子間隔は高画素数画像では100画素、低画素数画像では50画素とした。また、単一攻撃の推定性能と複合攻撃の推定性能を相対誤差で評価した。いずれの結果についても高画素数画像では良好な結果が得られた。また、低画素数画像でも一部の弱い攻撃については低い相対誤差で推定することができた。しかしながら、低画素数画像では相対誤差が大きくなる傾向が見られた。

以上の結果より、画像サイズが小さいと、強度の強い攻撃、つまり画像の形状が原画像と比較して大きく変化する攻撃の推定が困難になることがわかった。さらに、本手法を2章で述べたSIFT特徴点とDFTを用いた電子透かし法に導入して透かし情報の抽出精度を評価した。高画素数画像で実験を行なった結果、単体攻撃と複合攻撃のいずれについてもBERの中央値が0.1未満で抽出することに成功した。しかしながら、変形度が大きい場合には透かし情報のBERが大きくなることがわかった。以上の結果より、変形度が小さい場合には透かし情報を抽出可能であることがわかった。

本研究では、トリミングに対して堅牢な電子透かし法及び、パイロット信号を用いて幾何攻撃を推定する手法を開発した。その結果、単体攻撃については概ね正確に攻撃推定及び正確な透かし情報の抽出に成功した。また、複合攻撃については変形度が小さい攻撃について推定および透かし情報の抽出に成功した。実際の不正利用を考慮した場合は、画像の価値を損なうほど変形度の大きい攻撃は行われないと考えられる。したがって、実用的な画質が維持される範囲内であれば、本手法によって十分な精度で透かし情報を抽出可能である。

謝辞

本研究は、JPSJ 科研費 JP20K11973, JP24K15106 と電気通信普及財団 (2023), 山口大学基金 (2023), 東北大学産業技術総合研究所 (RIEC) の共同研究プロジェクトプログラム R04/ B09, SCAT 研究費助成 (2024,2025) の支援を受けて実施された.

Bibliography

- [1] Fabien AP Petitcolas, Ross J Anderson, and Markus G Kuhn. "Information hiding-a survey". In: *Proceedings of the IEEE* 87.7 (1999), pp. 1062{1078.
- [2] Hyunho Kang and Keiichi Iwamura. "Watermarking based on the difference of discrete cosine transform coefficients and an error-correcting code". In: *Proceedings of the 1st international workshop on Information hiding and its criteria for evaluation*. 2014, pp. 9{17.
- [3] Ingemar J Cox, Joe Kilian, F Thomson Leighton, and Talal Shamoan. "Secure spread spectrum watermarking for multimedia". In: *IEEE transactions on image processing* 6.12 (1997), pp. 1673{1687.
- [4] Joseph JK O'Ruanaidh and Thierry Pun. "Rotation, scale and translation invariant spread spectrum digital image watermarking". In: *Signal processing* 66.3 (1998), pp. 303{317.
- [5] Roxana Yahya Abadi and Payman Moallem. "Robust and optimum color image watermarking method based on a combination of DWT and DCT". In: *Optik* 261 (2022).
- [6] Bin Bao and Yu Wang. "A robust blind color watermarking algorithm based on the Radon-DCT transform". In: *Multimedia Tools and Applications* 83.24 (2024), pp. 64663{64682.
- [7] Matthieu Urvoy, Dalila Goudia, and Florent Autrusseau. "Perceptual DFT watermarking with improved detection and robustness to geometrical distortions". In: *IEEE Transactions on Information Forensics and Security* 9.7 (2014), pp. 1108{1119.
- [8] Chih-Wei Tang and Hsueh-Ming Hang. "A feature-based robust digital image watermarking scheme". In: *IEEE transactions on signal processing* 51.4 (2003), pp. 950{959.
- [9] Brian Chen and Gregory W Wornell. "Quantization index modulation: A class of provably good methods for digital watermarking and information embedding". In: *IEEE Transactions on Information theory* 47.4 (2001), pp. 1423{1443.
- [10] Vassilios Solachidis and Ioannis Pitas. "Circularly symmetric watermark embedding in 2-D DFT domain". In: *IEEE transactions on image processing* 10.11 (2001), pp. 1741{1753.
- [11] HyoungDo Kim. "CRT-Based Color Image Zero-Watermarking on the DCT Domain." In: *International Journal of Contents* 11.3 (2015).

- [12] Yiyi Yuan, Jingbing Li, Jing Liu, Uzair Aslam Bhatti, Zilong Liu, and Yen-wei Chen. "Robust zero-watermarking algorithm based on discrete wavelet transform and daisy descriptors for encrypted medical image". In: *CAAI Transactions on Intelligence Technology* 9.1 (2024), pp. 40{53.
- [13] Ryoto Kanegae and Masaki Kawamura. "Proposal of associative watermarking method". In: *2022 Asia-Pacific Signal and Information Processing Association Annual Summit and Conference (APSIPA ASC)*. IEEE. 2022, pp. 1376{1381.
- [14] Ryoto Kanegae and Masaki Kawamura. "Performance Evaluation of Associative Watermarking Using Statistical Neurodynamics". In: *Journal of the Physical Society of Japan* 93.11 (2024).
- [15] Xiaoyi Zhou, Yue Ma, Qingquan Zhang, Mazin Abed Mohammed, and Robertas Damaševičius. "A reversible watermarking system for medical color images: balancing capacity, imperceptibility, and robustness". In: *Electronics* 10.9 (2021).
- [16] Toshihiko Yamasaki and Kiyoharu Aizawa. "SIFT-based non-blind watermarking robust to non-linear geometrical distortions". In: *IEICE TRANSACTIONS on Information and Systems* 96.6 (2013), pp. 1368{1375.
- [17] Deepayan Bhowmik, Matthew Oakes, and Charith Abhayaratne. "Visual Attention-Based Image Watermarking". In: *IEEE Access* 4 (2016), pp. 8002{8018. doi: 10.1109/ACCESS.2016.2627241.
- [18] Robert Gallager. "Low-density parity-check codes". In: *IRE Transactions on information theory* 8.1 (1962), pp. 21{28.
- [19] David G Lowe. "Distinctive image features from scale-invariant keypoints". In: *International journal of computer vision* 60.2 (2004), pp. 91{110.
- [20] Masato Hayashi and Masaki Kawamura. "Improved SIFT feature-based watermarking method for IHC ver. 5". In: *2018 Asia-Pacific Signal and Information Processing Association Annual Summit and Conference (APSIPA ASC)*. IEEE. 2018, pp. 1536{1543.
- [21] Jin S Seo and Chang D Yoo. "Localized image watermarking based on feature points of scale-space representation". In: *Pattern Recognition* 37.7 (2004), pp. 1365{1375.
- [22] Mohamed Hamidi, Mohamed El Haziti, Hocine Cherifi, and Mohammed El Hassouni. "A hybrid robust image watermarking method based on DWT-DCT and SIFT for copyright protection". In: *Journal of Imaging* 7.10 (2021).
- [23] C-Y Lin, Min Wu, Jeffrey A Bloom, Ingemar J Cox, Matthew L Miller, and Yui Man Lui. "Rotation, scale, and translation resilient watermarking for images". In: *IEEE Transactions on image processing* 10.5 (2001), pp. 767{782.
- [24] Runwen Hu and Shijun Xiang. "Cover-lossless robust image watermarking against geometric deformations". In: *IEEE Transactions on Image Processing* 30 (2021), pp. 318{331.

- [25] Wenbo Wan, Jun Wang, Yunming Zhang, Jing Li, Hui Yu, and Jiande Sun. "A comprehensive survey on robust image watermarking". In: *Neurocomputing* 488 (2022), pp. 226{247.
- [26] Po-Chyi Su, Yu-Chuan Chang, and Ching-Yu Wu. "Geometrically resilient digital image watermarking by using interest point extraction and extended pilot signals". In: *IEEE Transactions on Information Forensics and Security* 8.12 (2013), pp. 1897{1908.
- [27] Shelby Pereira and Thierry Pun. "Robust template matching for affine resistant image watermarks". In: *IEEE transactions on image Processing* 9.6 (2000), pp. 1123{1129.
- [28] Xiangui Kang, Jiwu Huang, Yun Q Shi, and Yan Lin. "A DWT-DFT composite watermarking scheme robust to both affine transform and JPEG compression". In: *IEEE transactions on circuits and systems for video technology* 13.8 (2003), pp. 776{786.
- [29] Rinka Kawano and Masaki Kawamura. "Detection of periodic pilot signal in image watermarking". In: *2021 Asia-Pacific Signal and Information Processing Association Annual Summit and Conference (APSIPA ASC)*. IEEE, 2021, pp. 1647{1652.
- [30] Rinka Kawano and Masaki Kawamura. "Watermarking method with scaling rate estimation using pilot signal". In: *IEICE TRANSACTIONS on Information and Systems* 107.9 (2024), pp. 1151{1160.
- [31] Rinka Kawano and Masaki Kawamura. "Estimation of Geometric Transformation Matrices Using Grid-shaped Pilot Signals". In: *APSIPA Transactions on Signal and Information Processing* 14.1 (2025).
- [32] Luis Rosales-Roldan, Jinhui Chao, Mariko Nakano-Miyatake, and Hector Perez-Meana. "Color image ownership protection based on spectral domain watermarking using QR codes and QIM". In: *Multimedia Tools and Applications* 77.13 (2018), pp. 16031{16052.
- [33] Zihan Yuan, Decheng Liu, Xueting Zhang, Huanying Wang, and Qingtang Su. "DCT-based color digital image blind watermarking method with variable steps". In: *Multimedia Tools and Applications* 79.41 (2020), pp. 30557{30581.
- [34] Masaki Kawamura and Kouta Uchida. "SIFT feature-based watermarking method aimed at achieving IHC ver. 5". In: *International Conference on Intelligent Information Hiding and Multimedia Signal Processing*. Springer, 2017, pp. 381{389.
- [35] Information Hiding and its Criteria for evaluation. Accessed: 2023-2-20. url: <https://www.ieice.org/iss/emmihc/en/image/image.php>.
- [36] Manuel Cedillo-Hernandez, Francisco Garcia-Ugalde, Mariko Nakano-Miyatake, and Hector Perez-Meana. "Robust object-based watermarking using SURF feature matching and DFT domain". In: *Radioengineering* 22.4 (2013), pp. 1057{1071.
- [37] Yanwei Yu, Hefei Ling, Fuhao Zou, Zhengding Lu, and Liyun Wang. "Robust localized image watermarking based on invariant regions". In: *Digital Signal Processing* 22.1 (2012), pp. 170{180.

- [38] Gopalakrishnan Sundararajan, Chris Winstead, and Emmanuel Boutillon. "Noisy gradient descent bit-flip decoding for LDPC codes". In: *IEEE Transactions on Communications* 62.10 (2014), pp. 3385{3400.
- [39] Yangxiu Fang, Jing Liu, Jingbing Li, Jieren Cheng, Jiabin Hu, Dan Yi, Xiliang Xiao, and Uzair Aslam Bhatti. "Robust zero-watermarking algorithm for medical images based on SIFT and Bandelet-DCT". In: *Multimedia Tools and Applications* 81.12 (2022), pp. 16863{16879.
- [40] Haijun Luo, Xingming Sun, Hengfu Yang, and Zhihua Xia. "A robust image watermarking based on image restoration using SIFT". In: *Radioengineering* 20.2 (2011), pp. 525{532.
- [41] Rinka Kawano and Masaki Kawamura. "Estimation of rotation angle and anisotropic scaling rate using pilot signals for watermarking". In: *2024 Asia Pacific Signal and Information Processing Association Annual Summit and Conference (APSIPA ASC)*. IEEE. 2024, pp. 1{6.
- [42] Kodak Lossless True Color Image Suite. Accessed: 2025-7-14. url: <https://www.kodak.com/ja/>.