

# パイロット信号による攻撃推定を用いた画像電子透かし法

|       |    |    |         |         |        |
|-------|----|----|---------|---------|--------|
| 代表研究者 | 河野 | 綸華 | 山口大学大学院 | 創成科学研究科 | 博士後期課程 |
| 共同研究者 | 川村 | 正樹 | 山口大学大学院 | 創成科学研究科 | 教授     |

## 1 はじめに

SNS など画像の不正利用が問題となっている。そのため、デジタルコンテンツ保護のための技術として電子透かし法が注目されている[1]。電子透かし法とは、静止画像や動画、音声などのデジタルコンテンツに対して秘密裏に別の情報を埋め込む技術である。画像を対象とする場合、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。SNS などへ投稿する画像に事前に投稿者の ID や署名を埋め込むことで、コンテンツの管理を行うことができる。また、透かし情報を検出することによってコンテンツの不正利用を検出することができる。しかしながら、不正利用される画像の多くは拡大縮小や切り抜きなどの加工が行われる。また、画像を保存する際に、画像は圧縮される。ステゴ画像にこれらの加工や圧縮を加えると透かし情報が消えてしまったり、透かし情報の検出が困難となる可能性がある。これらの画像に対する加工や圧縮を攻撃と呼ぶ。不正利用のための電子透かし法を構築するためには様々な攻撃に対して堅牢な手法を考える必要がある。

画像への攻撃は非幾何攻撃と幾何攻撃に分類される。非幾何攻撃とは、JPEG 圧縮やノイズ付加などによって、画素値を変化させる攻撃である。ステゴ画像が非幾何攻撃によって加工された場合、埋め込まれた座標は変化しないが、埋め込まれた透かし情報は劣化する。そのため、埋め込む情報に対して誤り訂正符号を用いて透かし情報を構成したり[2]、スペクトル拡散を用いて埋め込んだり[3, 4]することで正確な透かし情報を得ることができる。多くの従来法では透かし情報に冗長性を導入することによって非幾何攻撃に対する堅牢性を持たせている。一方で、幾何攻撃は画像の拡大縮小や回転、切り抜きなどのような、画素の位置が変化する攻撃である。ステゴ画像が幾何攻撃によって劣化すると、透かし情報が埋め込まれた座標が変化する。そのため、透かし情報の位置を検出する必要がある。つまり、座標同期が必要である。幾何攻撃に堅牢な手法の例として、SIFT 特徴量[5]を用いた電子透かし法[6-8]がある。複数の SIFT 特徴点周辺に透かし情報を埋め込むことによって、幾何攻撃への耐性を持たせることができる。しかしながら、幾何攻撃の種類によっては埋め込み位置や領域を正確に検出できない可能性がある。

幾何攻撃に対して堅牢とされる多くの従来法では、クロッピング画像から透かし情報を検出している。クロッピング画像は一部の領域を 0 でパディングすることで構成される。つまり、クロッピングされた領域が非表示のマスク処理が行われるだけで、座標が変化しないため、座標同期が不要である。しかしながら、一般的に不正利用される画像はクロッピングされる。クロッピング画像は一部の領域が完全に除去・トリミングされるため、透かし情報の位置を検出することが困難である。そのため、総当たりなどの計算コストのかかる処理によって座標同期を必要とする手法が多いことから、幾何攻撃への耐性は十分ではない。もし幾何攻撃の種類や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できるため、透かし情報の誤りを減らすことができる。そこで、我々は通信路モデルの通信路推定の枠組みに着目して、攻撃の種類と強度を推定してきた[9]。通信路推定の方法の一つとして、パイロット信号と呼ばれるメッセージとは異なる信号を用いる手法がある。通信路に既知のパイロット信号を送信すると、信号の劣化具合から通信路を推定することができる。我々はこのアイデアを電子透かし法に導入した。つまり、既知のパイロット信号をあらかじめ画像に埋め込んでおき、画像が攻撃によって劣化したとき、信号の劣化を検出することによって攻撃を推定することができる。

パイロット信号を用いた電子透かし法の例として、Su らの手法[10]がある。SIFT 特徴量の一つである勾配方向を基に回転角を推定して勾配方向に回転した抽出領域を検出し、離散コサイン変換(DCT)を用いて透かし情報を抽出している。Su らの手法では、パイロット信号を座標同期のための同期信号として用いている。しかしながら、攻撃の内容を推定することはできない。

パイロット信号を用いて画像へ加えられた幾何攻撃を推定するためには、攻撃を推定可能な信号の形状と埋め込み手法を選択する必要がある。本手法では、画像に対して格子状のパイロット信号を埋め込む。

## 2 提案手法

我々は、画像に対して格子状のパイロット信号を埋め込む手法を提案した。画像が幾何攻撃によって歪むと格子の間隔や傾きが変化するため、これらのパラメータを検出することで幾何変換行列を推定することが可能である。格子の傾きと間隔は、ステゴ画像から抽出したパイロット信号をラドン変換することによって得られる。ラドン変換とは画像を様々な角度から線積分する積分変換の一つである。線が含まれる画像をラドン変換すると線と同じ角度で積分した際に係数に局所的なピークが現れることを利用して格子を検出することが可能である。

パイロット信号を用いて画像へ加えられた幾何攻撃を推定するためには、攻撃を推定可能な信号の形状と埋め込み手法を選択する必要がある。本手法では、画像に対して格子状のパイロット信号を埋め込む。

### 2-1 パイロット信号の埋め込み手順

多くの既存の電子透かし法では、画像の輝度値に透かし情報を埋め込んでいる。従って、ここでは画像を YUV 色空間に分解し、透かし情報が輝度値である Y 成分に埋め込まれると想定する。透かし情報と同じ色成分にパイロット信号を埋め込むと埋め込んだ情報が消えてしまう可能性があることから、Y 成分とは異なる成分にパイロット信号を埋め込む必要がある。パイロット信号の埋め込みが可能な色成分は U 成分と V 成分がある。いずれの成分に信号を埋め込んだ場合でも攻撃の推定精度に大きく影響はない。従って、本研究では U 成分にパイロット信号を埋め込む。

図 1 にパイロット信号の形状を示す。パイロット信号は -1、0、1 の 3 値の値をとる信号である。図のように、パイロット信号は U 成分画像全体に一定の間隔で格子状に埋め込む。これによって、画像が切り抜かれても部分的な格子間隔の変化や格子の傾きから攻撃を推定することが可能である。垂直線と水平線を区別するために、ここで、図のように垂直方向には -1 の値を持つ格子線と 0 の値を持つ格子線を交互に埋め込み、水平方向には 0 の値を持つ格子線と 1 の値を持つ格子線を交互に埋め込む。ただし、異なる値の格子線が交差する領域には -1、0、1 の値を交互に埋め込む。また、格子線以外の領域については埋め込み処理を行わない。格子間隔は 100 画素、格子線幅は 5 画素とする。

パイロット信号の埋め込みには量子化インデックス変調(Quantization Index modulation: QIM) [11]を用いている。QIM とは画素値を量子化することによって透かし情報を埋め込む手法であり、一般的にブラインド方式の画像電子透かし法で用いられる手法の一つである。

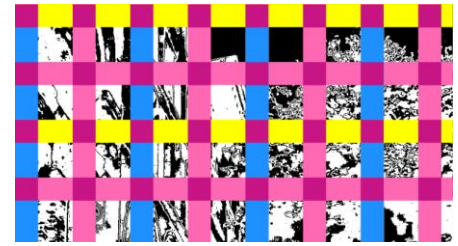


図 1 パイロット信号の形状

### 2-1 攻撃の推定手順

攻撃を推定するために、まずはステゴ画像の U 成分から QIM を用いて 3 値の抽出信号を得る。図 2 に抽出信号の例を示す。図の黒、白、灰色の線がパイロット信号である。図のように、抽出信号を見ると格子の位置や傾きは目視では判別可能である。しかしながら、原画像由来の成分がパイロット信号に対してノイズとなるため、一般的な電子透かし法に導入するためにはパイロット信号の検出から攻撃推定までの処理を行う必要がある。

格子線以外の領域には埋め込み処理を行わなかったため、QIM を用いて格子線以外の領域から値を抽出すると、原画像由来の模様が現れる。この原画像成分は格子検出の妨げになるが、格子が検出しやすいように格子以外の領域に一樣な値を埋め込むとステゴ画像の画質が大きく劣化してしまう。そのため、原画像成分を除去することで格子線を検出しやすくする。

次に、抽出情報から格子線の角度である検出角度を求める。検出角度は抽出情報をラドン変換することによって得られる。ラドン変換は画像を様々な角度から線積分する手法である。図 3 にラドン係数の模式図を示す。横軸は射影角度を表し、縦軸は射影位置を表す。抽出情報をラドン変換

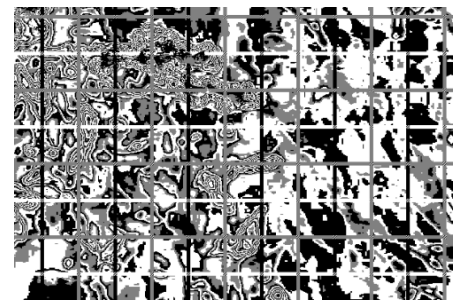


図 2 抽出信号の具体例

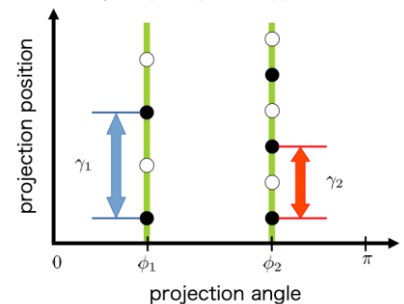


図 3 ラドン係数の模式図

すると格子の角度と同じ射影角度で、線の間隔と同じ周期で特徴的なピークが現れることが予備実験でわかった。従って、このピークを検出することによって検出角度と検出間隔を求めることができる。ここで問題となるのが原画像成分である。原画像によっては画像の模様によって格子線のピークが明瞭に表れない場合がある。従って、ラドン係数を標準化して絶対値が 1.5 以下となる係数値を 0 にすることで原画像成分をある程度除去することができた。検出角度は射影角度毎に係数の分散を求めると格子の角度と等しい射影角度で局所的に分散が大きくなることを利用して求められる。一般的にラドン変換では任意の範囲の角度で実行することが可能である。本手法では 0 度から 180 度までの範囲で実行する。従って、この処理によって検出角度は 2 つ得られる。しかしながら、この段階では格子の方向の判別ができない。ここで重要となるのが埋め込み時の格子線の値である。ラドン係数のピークは抽出信号の値に応じて決定される。値が 1 の格子線は係数値に正のピークとして現れ、-1 の格子線は負のピークとして現れる。従って、ラドン係数のピークの方から格子線の方を判別することが可能である。以上より、負のピークが多い場合は垂直方向の検出角度、正のピークが多い場合は水平方向の検出角度ということが分かる。

次に検出間隔を求める。得られた二種類の抽出信号について、求めた検出間隔のみでラドン変換すると、射影距離方向に周期的なピークが見られる。この周期に対して自己相関を求めた後にフーリエ変換することによって各方向の格子線に対応した射影間隔を求めることが可能である。

最後に、得られた垂直及び水平方向の検出角度と検出間隔を基に変換行列を推定する。図 4 に変換前の格子を、図 5 に変換後の格子の例を示す。変換行列の推定では、図 4 のような格子が変換行列によって図 5 のように変形したと仮定する。点 A(1, 0)、B(0, 1) の変換後の座標を点 A'、B' とすると、点 A'、B' の座標を検出角度と検出間隔を基に求めることで変換行列を推定することが可能である。ここで、一般的なアフィン変換では反時計回りに回転角を決定する。一方で、ラドン変換では +90 度ずれた位置を回転の軸として時計回りに回転角する。従って、得られた検出角度が格子の回転角と異なる。また、検出間隔は同じ方向の格子線の間隔を表す。従って、線 OA' 方向の検出間隔は線 OA' と線 B'C' の距離を表す。垂直及び水平方向の検出角度を  $\phi_v, \phi_h$ 、検出間隔を  $\gamma_v, \gamma_h$  とする。また、点 A' と x 軸のなす角を  $\alpha$ 、点 B' と x 軸のなす角を  $\beta$  とすると、点 A'(x<sub>a</sub>, y<sub>a</sub>)、B'(x<sub>b</sub>, y<sub>b</sub>) は次のように表される。

$$\begin{aligned} x_a &= |OA'| \cos \alpha = \frac{\gamma_v \cos \alpha}{\sin|\beta - \alpha|} \\ y_a &= |OA'| \sin \alpha = \frac{\gamma_v \sin \alpha}{\sin|\beta - \alpha|} \\ x_b &= |OB'| \cos \beta = \frac{\gamma_h \cos \alpha}{\sin|\beta - \alpha|} \\ y_b &= |OB'| \sin \beta = \frac{\gamma_h \sin \alpha}{\sin|\beta - \alpha|} \end{aligned}$$

得られた点 A'、B' の座標を基に変換行列を推定することが可能である。推定変換行列  $\hat{T}$  は次のように表される。

$$\hat{T} = \begin{pmatrix} x_a & x_b \\ y_a & y_b \end{pmatrix}$$

ここで注意すべき点として、本手法ではパイロット信号を点対称に設計したことにより、実際の角度と 180 度回転した場合の角度の判別をすることはできない。

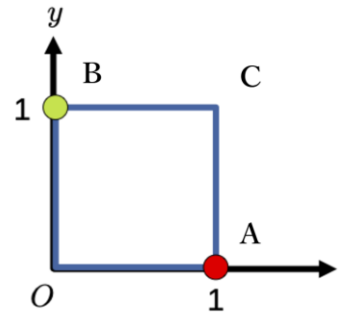


図 4 変換前の格子

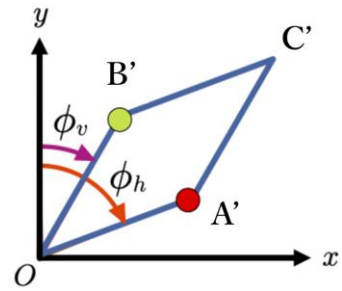


図 5 変換後の格子

### 3 計算機シミュレーション

本手法の性能を推定変換行列のフロベニウスノルムにおける相対誤差で評価した。変換行列 $T$ と推定変換行列 $\hat{T}$ のフロベニウスノルムの相対誤差は次のように表される。

$$\frac{|\hat{T} - T|_F}{|T|_F} = \frac{\sqrt{\sum_{i=1}^m \sum_{j=1}^n |t'_{ij} - t_{ij}|^2}}{\sqrt{\sum_{i=1}^m \sum_{j=1}^n |t_{ij}|^2}}$$

#### 3-1 実験条件

6 枚の IHC 標準画像 (4608×3456 画素) [12] の U 成分にパイロット信号を埋め込む。本実験ではパイロット信号を埋め込んだステゴ画像に対して変換行列を用いて幾何攻撃を加える。さらに、画像の中心座標を切り抜き画像の中心座標として、1080×1080 画素の大きさに切り抜く。本手法では、パイロット信号を点対称に設計したことにより、実際の角度と 180 度回転した場合の角度の判別をすることはできない。したがって、2 通りの変換行列を推定した後に、よりフロベニウスノルムにおける相対誤差が小さい方の変換行列を推定変換行列として評価した。

本手法では、ラドン係数から検出角度や検出間隔を得られなかった場合には攻撃を推定することはできない。従って、実験では推定に失敗した際にその結果を除外する。

#### 3-2 単体攻撃性能の評価

単体攻撃を行った場合の推定変換行列を評価する。攻撃の種類は異方性の拡大縮小と回転、そして剪断である。表 1 に各攻撃のパラメータを示す。ここで、異方性拡大縮小の評価については x 軸方向の拡大率を固定して軸方向の拡大率のみを変化させる。

表 1 各攻撃パラメータ

| 攻撃          | 強度                    |                    |
|-------------|-----------------------|--------------------|
| 異方性拡大縮小     | x 軸方向の拡大率             | 1.0                |
|             | y 軸方向の拡大率             | 0.1, 0.2, ..., 2.0 |
| 回転[度]       | 0, 5, 10, 15, ..., 90 |                    |
| y 軸方向の剪断[度] | 0, 5, 10, 15, ..., 80 |                    |

図 6 に異方性拡大縮小の結果を示す。横軸は y 軸方向の拡大率を表し、縦軸はフロベニウスノルムの相対誤差を表す。各拡大率について 6 枚の画像の結果を箱ひげ図として表す。橙線は中央値を表す。

図より、拡大率が 0.4 倍から 1.9 倍の時に相対誤差がほぼ 0 となった。また、推定変換行列を推定できなかった枚数を表 2 に示す。回転角が 0.3 倍以下の時に、検出角度を検出できなかったために変換行列の推定に失敗した。縮小時に推定に失敗または相対誤差が大きくなる事例が見られたのは、格子線が細くなったことによって検出間隔の推定が困難になったことが原因であると考えられる。一方で、画像を拡大したあとに一定の大きさに切り抜いた場合、縮小した場合と比較すると切り取り領域の抽出信号に含まれる格子線の本数が少なくなり、原画像成分の割合が高くなる。そのため、ラドン係数から原画像成分を除去しきれないと誤った間隔を検出してしまう場合がある。

表 2 異方性拡大縮小時の推定に失敗した画像数

| 攻撃  | 0.1 | 0.2 | 0.3 | 0.4-2.0 |
|-----|-----|-----|-----|---------|
| 失敗数 | 2   | 3   | 6   | 0       |

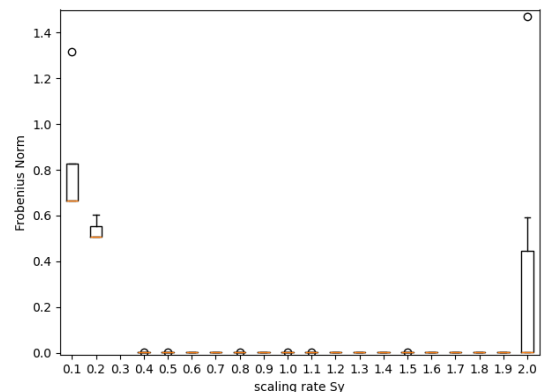


図 6 異方性拡大縮小の場合の相対誤差



次に、図 7 に回転の結果を示す。横軸は回転角を表し、縦軸はフロベニウスノルムの相対誤差を表す。各拡大率について 6 枚の画像の結果を箱ひげ図として表す。また、橙線は中央値を表す。図より、いずれの回転角についても相対誤差がほぼ 0 となった。

最後に、図 8 に y 軸方向の剪断の結果を示す。横軸は剪断角度を表し、縦軸はフロベニウスノルムの相対誤差を表す。各拡大率について 6 枚の画像の結果を箱ひげ図として表す。また、橙線は中央値を表す。図より、剪断角度が 70 度以下の場合に相対誤差がほぼ 0 となった。

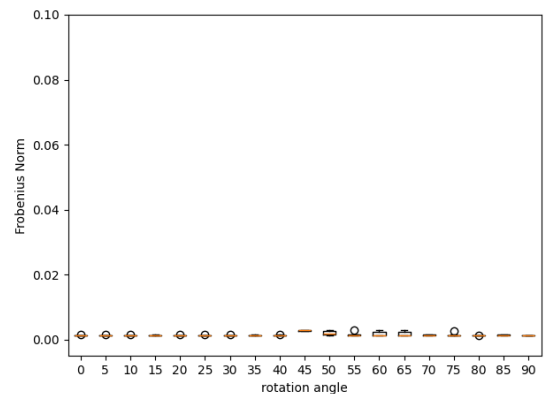


図 7 回転の場合の相対誤差

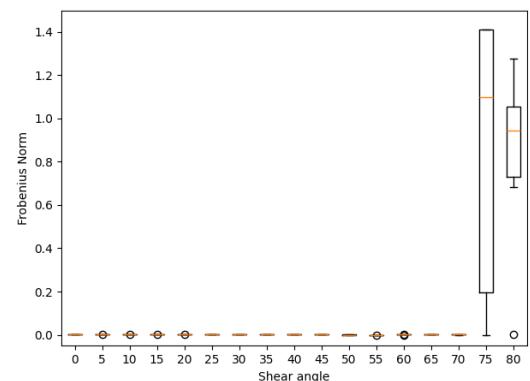


図 8 剪断の場合の相対誤差

#### 4 まとめ

ブラインド電子透かし法において画像の幾何変換と切り抜きを組み合わせると、透かし情報の埋め込み位置を正確に検出できない場合がある。そこで、本手法では格子状のパイロット信号を用いて変換行列を推定する手法を提案した。格子状のパイロット信号をラドン変換することによって検出角及び格子線の検出間隔が得られる。また、水平方向と垂直方向でパイロット信号を変えることによって、パイロット信号のおよその方向を検出することができる。これらのパラメータを用いて推定変換行列を推定した。

本手法の性能を、異方性の拡大縮小と回転、そして剪断の変換行列を推定して、フロベニウスノルムにおける相対誤差を求めることで評価した。異方性の拡大縮小の変換行列の推定については、0.4 倍から 1.9 倍の範囲で相対誤差がほぼ 0 となった。回転の変換行列の推定については、いずれの回転角についても誤差がほぼ 0 となった。また、剪断の変換行列の推定については、70 度以下で誤差がほぼ 0 となった。ただし、異方性の拡大縮小についてはパイロット信号を検出できずに推定に失敗する事例があった。これは、原画像成分によってラドン係数上の格子を表す係数値があまり強く現れなかったために分散が小さくなってしまったことが原因である。

極端に強い強度で攻撃を加えると視覚的に影響が現れる。特に、透かし情報を埋め込んだ画像に対して縮小や剪断等の領域がつぶれてしまうような攻撃を加えた場合、透かし情報が消えてしまう可能性がある。従って、本来の目的である電子透かし法のための攻撃推定という用途であれば問題ないと考えられる。

#### 【参考文献】

- [1] F. A. Petitcolas, R. J. Anderson, M. G. Kuhn, "Information hiding-a survey," Proceedings of the IEEE, vol.87, no.7, pp.1062--1078, 1999
- [2] H. Kang, K. Iwamura, "Watermarking based on the difference of discrete cosine transform coefficients and an error-correcting code," Proc. of IWIHC, pp. 9--17, 2014
- [3] I. J. Cox, J. Kilian, F. T. Leighton and T. Shamoon, "Secure spread spectrum watermarking for multimedia," in IEEE Transactions on Image Processing, vol. 6, no. 12, pp. 1673--1687, 1997
- [4] J. J.K.O. Ruanaidh, T. Pun, "Rotation, scale and translation invariant spread spectrum digital image watermarking," Signal Process., vol. 66, Issue 3, pp. 303--317, 1998

- [5] D. G. Lowe, "Distinctive image features from scale-invariant keypoints," International J. Compute Vision, vol. 60, no. 2, pp. 91--110, 2004
- [6] M. Hayashi, M. Kawamura, "Improved SIFT feature-based watermarking method for IHC ver. 5," Proc. of APSIPA ASC 2018, 2018
- [7] V. Solachidis, I. Pitas, "Circularly symmetric watermark embedding in 2-D DFT domain," IEEE Trans Image Process, vol. 10, no.11, pp.1741--1752, 2001
- [8] J. S. Seo, C. D. Yoo, "Localized image watermarking based on feature points of scale-space representation," Pattern Recognition, vol. 37, Issue 7, pp. 1365--1375, 2004
- [9] 河野綸華, 川村正樹, "パイロット信号を用いた回転角と異方性拡大率の推定,"電子情報通信学会 技術報告, 2024 年度 第 2 回 EMM 研究会, 札幌コンベンションセンター, vol.124, no. 125, pp. 158--163
- [10] P. C. Su, Y. C. Chang and C. Y. Wu, "Geometrically resilient digital image watermarking by using interest point extraction and extended pilot signals," IEEE Trans. Inf. Forensics Secur., vol. 8, no. 12, pp. 1897--1908, 2013,
- [11] B. Chen, G. W. Wornell, "Quantization index modulation: A class of provably good methods for digital watermarking and information embedding," IEEE Trans. Inf. Theory, vol.47, no.4, pp.1423--1443, 2001
- [12] Information Hiding and its Criteria for evaluation, <https://www.ieice.org/iss/emm/ihc/en/image/image.php> (20th February, 2023 access)

### 〈発 表 資 料〉

| 題 名                                                                                            | 掲載誌・学会名等                                                                                                  | 発表年月                 |
|------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------|----------------------|
| パイロット信号を用いた回転角と異方性拡大率の推定                                                                       | 電子情報通信学会 技術報告, 2024 年度 第 2 回 EMM 研究会                                                                      | 2024 年 7 月 22 日-23 日 |
| Estimation of rotation angle and anisotropic scaling rate using pilot signals for watermarking | Asia Pacific Signal and Information Processing Association Annual Summit and Conference 2024 (APSIPA ASC) | 2024 年 12 月 3 日-7 日  |
| 水平・垂直方向のパイロット信号による幾何変換行列の推定                                                                    | 電子情報通信学会 技術報告, 2024 年度 第 6 回 EMM 研究会                                                                      | 2025 年 3 月 5 日-6 日   |