様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９　（共通）

科学研究費助成事業　　研究成果報告書

令和　６ 年　 ６ 月　 ５ 日現在

機関番号：１５５０１
研究種目：基盤研究(C)（一般）
研究期間：2020～2023
課題番号：２０Ｋ１１９７３

研究課題名（和文）連想記憶モデルを応用した情報ハイディング技術の高耐性化

研究課題名（英文）High-resistance information hiding method applied associative memory models

研究代表者
川村　正樹（Kawamura, Masaki）

山口大学・大学院創成科学研究科　・教授

研究者番号：６０３１４７９６

交付決定額（研究期間全体）：（直接経費）　　3,400,000円

研究成果の概要（和文）：個人がアップロードした写真を、他者が無断で使用するなど著作権を侵害する問題が起きている。この問題に対して、電子透かし法が有効である。本研究では、幾何変換に対する耐性として、パイロット信号を導入して、変換を推定する手法を提案した。また、JPEG圧縮への耐性として、量子化活性化関数を提案した。また、ゼロ電子透かし法の枠組みを連想記憶モデルで表現し、誤り率を改善した手法を提案した。いずれの手法も従来法よりも良好な結果を得ることができた。

研究成果の学術的意義や社会的意義
これまでの電子透かし法では、画像変換を推定する方法は行われていなかったが、本研究により、パイロット信号を導入することによって、攻撃推定が可能になった。また、畳み込みニューラルネットに対して量子化活性化関数を提案し、学習によりJEPG圧縮にも強いステゴ画像を生成できるようになった。また、透かしを埋め込むことができない医療画像などに対して、提案した連想電子透かしモデルにより、誤りがほとんど無い電子透かし法を提案することができた。

研究成果の概要（英文）：There is a problem of copyright piracy, i.e. illegal users using photos uploaded by people without their permission. Watermarking methods are effective against this problem. In this study, we proposed a method to estimate the geometric transformation by a pilot signal for resisting it. A quantisation activation function was also proposed for resistance to JPEG compression. A zero-watermarking framework was also proposed, which is represented by the associative memory models and improves the error rate. All the methods achieved better results than the conventional ones.

研究分野：情報科学

キーワード：情報ハイディング　電子透かし　ニューラルネットワーク　連想記憶モデル　パイロット信号

様　式　C−19、F−19−1、Z−19（共通）

1.研究開始当初の背景

漫画村のような著作物の不法配布サイトの出現や、個人がSNSにアップロードした写真が、他者に無断で使用される問題など、モラルに頼る著作権の保護では限界がきている。そのため、「著作物の保護をいかに行うか?」が社会的な課題となっており、「どのような情報保護技術が違法な利用を防止できるか?」が技術的な課題となっている。この問題に対して、情報ハイディング技術が有効である。情報ハイディング (Information Hiding) 技術とは、著作情報や購入者IDなどの透かし情報をコンテンツに埋め込む電子透かし技術と、情報を埋め込んだ痕跡を隠すステガノグラフィ技術などの総称である。IH技術はコンテンツの不正利用の防止や追跡のための中核技術として注目されている。しかしながら、デジタルコンテンツの加工や圧縮、変換は、いまやアプリを使って誰でも容易に行うことができる。従って、このような加工処理が行われても、透かし情報を取り出せる耐性を持っている必要がある。

電子情報通信学会情報ハイディング及びその評価基準 (IHC) 委員会は、IH技術の向上を目指すため発足した委員会である。本委員会では、どのような加工処理に対して、どの程度の耐性を持てばよいかを定めた評価基準を定義し、コンテストを実施することによって、評価基準のバージョンアップが行われてきた。JPEG圧縮に対しては、離散コサイン変換 (DCT) やウェーブレット変換 (DWT) などの周波数領域に透かしを埋め込むことで耐性を持たせることができる。切り出しには、画像をブロックに分割し、繰り返し透かしを埋め込むことで対応することができる。特に困難な攻撃が幾何変換である。拡大率や回転角が未知であるため、透かし情報を埋め込んだ埋め込み領域を決定することが難しい。これまでに、スケール不変特徴変換 (SIFT) を用いた手法によって拡大縮小には対応できている。回転角が既知であれば逆変換可能である。しかしながら、未知の場合は角度の推定が難しい。また、回転による画像の歪みが顕著に現れる問題がある。現在までに、評価基準 Ver.5以上を達成した手法は提案されていない。この点からも、回転攻撃への耐性が、如何に難しい課題であるかが理解できる。

回転攻撃への耐性がIH技術の向上のために必要不可欠であると認識し、本研究では、回転耐性に注目する。すなわち、本研究課題の学術的な問いは、回転攻撃を含むIHC評価基準の下で、「透かし情報を埋め込んだステゴ画像の画質を維持し、かつ、誤りなく透かし情報を抽出できるようにするには、どのような手法が可能か?」ということにある。

2.研究の目的

幾何変換が施された画像から一部が切り出され、その画像を圧縮率の高いJPEG圧縮で非可逆圧縮した画像から、誤り無く電子透かしを抽出できる手法がIHC評価基準で求められている。本研究では、回転耐性を向上させ、誤り無く透かしを抽出できる高耐性な手法を開発することを目的とする。そこで、(1) ニューラルネットに回転耐性の学習を導入すること。(2) 誤り訂正処理としての連想記憶モデルを導入すること。これらにより、評価基準を達成する手法を目指す。

高耐性な電子透かし手法の中で、近年、階層の深いニューラルネット (DNN) を使う手法が増えている。DNNは画像やパターンの認識や分類に高い性能を持っている。主な手法では、特定の画像が入力されると、対応する透かし情報を出力するように学習する。しかしながら、これらの方法では、透かし情報をDNNに保存しているだけなので、電子透かしを画像に埋め込んでおらず、復号時に対応するDNNを必要とする欠点がある。従って、任意の透かし情報と画像からステゴ画像を生成でき、ステゴ画像から透かし情報が抽出できる汎用性が必要である。これには、様々な画像を用いて学習する必要があり、学習に膨大な時間がかかるという問題がある。Zhu et al. はニューラルネットの内部に圧縮や拡大縮小、加法ノイズの擬似攻撃モジュールを持つ手法を提案している。内部で攻撃をシミュレートすることで、様々な攻撃

に耐性のあるステゴ画像を生成することができる。残念なことに、この手法も回転については対応がされていない。
次に、連想記憶モデルを導入する意義を述べる。従来の誤り訂正符号を用いた手法では、攻撃によって生じた誤りを訂正することができ、一定の成果を得ることができた。しかしながら、IHC評価基準はさらなる訂正能力を要求している。連想記憶モデルは、予め複数の符号語(ビット列)を連想パターンとして記憶することができる。多数のビットが反転し、元の連想パターンから遠ざかったとしても、記憶したパターンを想起することができる。すなわち、誤り訂正能力がある。この誤り訂正能力は連想記憶モデルの引き込み領域で表され、記憶パターン数(符号語数)が少ないほど広くなっている。少数の符号語のみをコンテンツに埋め込むので、誤り訂正処理として連想記憶モデルを用いれば、広い引き込み領域の恩恵を受けることができる。

3.研究の方法
本研究では、次の2つの課題に取組む。
課題 (1) ニューラルネットによる回転耐性の獲得
回転耐性ニューラルネットでは、内部で回転攻撃をシミュレートすることで、回転攻撃に強いステゴ画像を生成することができる。しかしながら、透かし情報の埋め込める量が少ないことと、回転による画質の低下が問題になっている。前者に対しては、埋め込み領域を大きくすることで情報量を増大できるかを検討する。また、ネットワークの構造を冗長化することも検討する。後者の画質の向上には、敵対的生成ネットワーク (GAN) の導入が有効である。GANを導入し、ステゴ画像の画質向上を目指す。また、回転以外の攻撃に対する擬似攻撃モジュールも Zhu et al. と同様に導入し、IHC評価基準で想定される攻撃に耐性を持つように改善を行う。
課題 (2) 連想記憶モデルによる誤り訂正能力の改善
従来の連想記憶モデルの引き込み領域の理論的な解析は、研究代表者のこれまでの研究で解明されている。電子透かしに用いるためには、ネットワークの構造を少し変更する必要がある。また、理論的な解析では、無相関なランダムノイズを仮定するが、画像処理の場合、人工的な加工が行われるので、この仮定が成り立たない。従って、電子透かしにおける連想記憶モデルの解析では、相関を考慮し、計算機シミュレーションによる評価も必要になる。また、その結果を従来の誤り訂正符号を用いた場合と比較する。

4.研究成果
課題 (1)　幾何変換が加えられたとしても、透かし情報の埋め込み領域を決定できる特徴抽出器を検討した。まず、回転や拡大縮小などの変換に強い特徴領域として、離散フーリエ変換（DFT）ドメインを用いる方法を検討した。DFTを用いると拡大縮小に対して堅牢になる。幾何変換に強いSIFT特徴点の周辺に埋め込み領域を決め、その領域をDFTする。このDFT係数に透かし情報を埋め込む手法に対して、性能評価を行った。その結果、拡大縮小が無い場合はほぼ誤り無く抽出が可能であった。また、拡大率が未知の場合、誤り率が大きくなる傾向が得られた。これより、拡大率の推定が必要であることが分かった。そこで、抽出した透かし情報の誤りを訂正するのではなく、攻撃自体を推定して、透かし情報の誤りを低減する手法を検討した。攻撃の種類と大きさを推定することができれば、誤りを低減することができる。まず、幾何攻撃を想定し、透かし情報とは別に攻撃を推定するためにパイロット信号を格子状に埋め込む。その格子間隔により攻撃の大きさを知ることができる。この手法より求めた推定拡大率を用いて、透かし情報の抽出を行った。その結果、誤り訂正する場合に比べ、十分に誤り率を小さくすることができた。この成果はEMM研究会などで口頭発表を行った。さらに、回転角を求める手法も検討した。ブロック分割し、ブロック平均を取ることにより、パイロット信号を先鋭化する方法と、ラドン変換を用いる方法を提案した。ラドン変

換を用いると、拡大率と回転角を同時に精度良く推定できることが分かった。この成果は、国際会議APSIPA2023とEMM研究会で成果発表を行った。

課題 (2)　電子透かしに用いる透かし情報を誤り訂正符号で訂正するのではなく、連想記憶モデルで訂正する方法を検討した。このテーマではゼロ電子透かし法と同様に、埋め込まない透かし法を考える。画像から抽出した特徴情報と透かし情報の対応を相互想起型連想記憶モデルに記憶し、特徴情報を与えることにより、透かし情報を想起することができる。このとき、画像が劣化し、特徴情報に誤りが含まれていても、連想記憶モデルで修復が可能である。これは従来のゼロ電子透かし法には無い機能である。劣化が大きい場合は、相互想起型連想記憶モデルでも誤り訂正が十分ではないため、さらに、自己想起型連想記憶モデルにより誤り訂正を行った。その結果、大きな劣化がある場合でも誤り無く透かし情報を抽出することが可能になった。この成果は、連想電子透かし法として、国際会議APSIPAで発表した。さらに、従来のゼロ電子透かし法を相互想起型連想記憶モデルと自己想起型連想記憶モデルで構成できることを示し、統計神経力学を用いて、巨視的状態方程式を導出した。ランダムな特徴量に関しては理論値と計算機シミュレーションの結果は良く一致した。しかしながら、画像から抽出した特徴量は若干の相関があり、理論値からのズレがみられた。これらの成果は、国際会議APSIPA2022で発表した。

（関連課題）　ニューラルネットワークを用いた電子透かし法では、階段状の量子化活性化関数を用いたモデルを提案した。従来のモデルではJPEG圧縮で用いられる量子化の過程が表現されておらず、学習によってのみ対応していた。オートエンコーダ（AE）型のネットワークに対して、提案した量子化活性化関数を用いることにより、量子化の効果を学習時に明示的に取り込むことができ、JPEG圧縮耐性が実現できた。この成果は国際会議APSIPAで発表した。さらに、畳み込みニューラルネット（CNN）型に対してもJPEG圧縮の量子化テーブルを模倣した量子化活性化関数を提案し、CNNの攻撃層に導入した。JPEG圧縮を忠実に模倣することにより、JPEG圧縮に耐性のあるステゴ画像を生成する埋め込み器と、劣化したステゴ画像から透かし情報を抽出する抽出器を学習によって構築することができた。これらの成果は、国際会議APSIPA2022で発表した。

ニューラルネットワークなどの学習モデルを構築する際は、モデルのパラメータを決定する必要がある。最適なパラメータを決定するためには、しばしば最適化問題を解く必要がある。そこで、効率的な解探索を行うアルゴリズムを検討した。また、標準的な最適化問題に適用し、その性能を評価した。その結果、比較的効率よく解探索を行えるアルゴリズムを提案できた。この成果は、学術論文として、Algorithmsと電子情報通信学会英文論文誌で発表した。

５．主な発表論文等

〔雑誌論文〕　計3件（うち査読付論文　3件／うち国際共著　0件／うちオープンアクセス　3件）

１．著者名 Rinka Kawano, Masaki Kawamura	４．巻 E107-D (9)
２．論文標題 Watermarking Method with Scaling Rate Estimation Using Pilot Signal	５．発行年 2024年
３．雑誌名 IEICE Transactions on Information and Systems	６．最初と最後の頁 -
掲載論文のDOI（デジタルオブジェクト識別子） 10.1587/transinf.2023EDP7222	査読の有無 有
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 －

１．著者名 Dhidhi Pambudi, Masaki Kawamura	４．巻 15
２．論文標題 Constructing the Neighborhood Structure of VNS Based on Binomial Distribution for Solving QUBO Problems	５．発行年 2022年
３．雑誌名 Algorithms	６．最初と最後の頁 192
掲載論文のDOI（デジタルオブジェクト識別子） 10.3390/a15060192	査読の有無 有
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 －

１．著者名 Dhidhi Pambudi, Masaki Kawamura	４．巻 E105.D
２．論文標題 Novel Metaheuristic: Spy Algorithm	５．発行年 2022年
３．雑誌名 IEICE Transactions on Information and Systems	６．最初と最後の頁 309～319
掲載論文のDOI（デジタルオブジェクト識別子） 10.1587/transinf.2021EDP7092	査読の有無 有
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 －

〔学会発表〕　計23件（うち招待講演　1件／うち国際学会　6件）

１．発表者名 Rinka Kawano, Masaki Kawamura
２．発表標題 Rotation Angle Detection Using a Pilot Signal from Rotated Stego-Image
３．学会等名 2023 Asia Pacific Signal and Information Processing Association Annual Summit and Conference（国際学会）
４．発表年 2023年

１．発表者名
Ayaka Sakamoto, Rinka Kawano, Masaki Kawamura

２．発表標題
Application for generating re-accessible screenshots of web pages using histogram shrinkage

３．学会等名
2023 Asia Pacific Signal and Information Processing Association Annual Summit and Conference（国際学会）

４．発表年
2023年

１．発表者名
Ryoto Kanegae, Masaki Kawamura

２．発表標題
Proposal of Associative Watermarking Method

３．学会等名
2022 Asia-Pacific Signal and Information Processing Association Annual Summit and Conference (APSIPA ASC)（国際学会）

４．発表年
2022年

１．発表者名
Shingo Yamauchi, Masaki Kawamura

２．発表標題
Neural Network Based Watermarking Trained with Quantized Activation Function

３．学会等名
2022 Asia-Pacific Signal and Information Processing Association Annual Summit and Conference (APSIPA ASC)（国際学会）

４．発表年
2022年

１．発表者名
Rinka Kawano, Masaki Kawamura

２．発表標題
Detection of Periodic Pilot Signal in Image Watermarking

３．学会等名
2021 Asia-Pacific Signal and Information Processing Association Annual Summit and Conference (APSIPA ASC)（国際学会）

４．発表年
2021年

１．発表者名
Akane Yokota, Masaki Kawamura

２．発表標題
BSS-Based Extraction For Additive Video Watermarking

３．学会等名
2021 Asia-Pacific Signal and Information Processing Association Annual Summit and Conference (APSIPA ASC)（国際学会）

４．発表年
2021年

１．発表者名
川村 正樹

２．発表標題
連想記憶モデルの電子透かしモデルへの応用

３．学会等名
電子情報通信学会 第６回EMM研究会（招待講演）

４．発表年
2024年

１．発表者名
河野 綸華，川村 正樹

２．発表標題
画像電子透かしのためのパイロット信号を用いた拡大率及び回転角の推定

３．学会等名
電子情報通信学会 第６回EMM研究会

４．発表年
2024年

１．発表者名
原田 奈央，河野 綸華，川村 正樹

２．発表標題
透かし情報を分散的に埋め込んだ加法的動画像電子透かし法の提案 ～ BSSとフレーム間差分を用いた抽出方法の性能比較 ～

３．学会等名
電子情報通信学会 第６回EMM研究会

４．発表年
2024年

１．発表者名
河野 綸華，川村 正樹

２．発表標題
画像電子透かしのためのパイロット信号を用いた回転角の推定

３．学会等名
電子情報通信学会 第２回EMM研究会

４．発表年
2023年

１．発表者名
阪本 彩佳，川村 正樹

２．発表標題
Swift標準ライブラリで構築したWebページの再表示が可能なスクリーンショットアプリの開発

３．学会等名
電子情報通信学会 第6回EMM研究会

４．発表年
2023年

１．発表者名
原田 奈央，河野 綸華，川村 正樹

２．発表標題
BSSを用いた電子透かしの抽出手法 ～ フレーム間差分を用いた画質の向上 ～

３．学会等名
電子情報通信学会 第6回EMM研究会

４．発表年
2023年

１．発表者名
河野 綸華，川村 正樹

２．発表標題
パイロット信号による拡大率推定を用いた電子透かし法の提案

３．学会等名
電子情報通信学会 第5回EMM研究会

４．発表年
2023年

１．発表者名
河野 綸華，川村 正樹

２．発表標題
電子透かしにおけるパイロット信号を用いた拡大率推定

３．学会等名
2022年度(第73 回) 電気・情報関連学会中国支部連合大会

４．発表年
2022年

１．発表者名
原田 奈央，河野 綸華，川村 正樹

２．発表標題
加法的動画像電子透かし法のBSSを用いた抽出方法

３．学会等名
2022年度(第73 回) 電気・情報関連学会中国支部連合大会

４．発表年
2022年

１．発表者名
山内 伸悟，川村 正樹

２．発表標題
量子化活性化関数で学習したJPEG圧縮耐性電子透かし法の検討

３．学会等名
電子情報通信学会 2021年度第6回EMM研究会

４．発表年
2022年

１．発表者名
Dhidhi Pambudi, Masaki Kawamura

２．発表標題
Modified VNS for Solving QUBO Problem

３．学会等名
電子情報通信学会総合大会

４．発表年
2022年

１．発表者名
鐘ヶ江諒人，川村 正樹

２．発表標題
相互想起モデルを用いたZero-Watermarking法への自己想起モデルの導入

３．学会等名
電子情報通信学会 2021年度 第5回EMM研究会

４．発表年
2022年

１．発表者名
河野 綸華，川村 正樹

２．発表標題
電子透かしのためのパイロット信号による拡大率の推定

３．学会等名
第20回情報科学技術フォーラム（FIT2021）

４．発表年
2021年

１．発表者名
横田 明音，川村 正樹

２．発表標題
BSSを用いた動画フレームからの電子透かしの抽出

３．学会等名
電子情報通信学会 2021年度 第3回EMM研究会

４．発表年
2021年

１．発表者名
河野 綸華，川村 正樹

２．発表標題
SIFT特徴点とDFTドメインを利用した電子透かし法の検討

３．学会等名
電子情報通信学会 第6回EMM研究会

４．発表年
2021年

１．発表者名
Dhidhi Pambudi, Masaki Kawamura

２．発表標題
Multimodal Optimization Using Spy Algorithm

３．学会等名
電子情報通信学会 総合大会

４．発表年
2021年

１．発表者名
Dhidhi Pambudi, Masaki Kawamura

２．発表標題
Spy Algorithm for Solving Continuous Optimization Problem

３．学会等名
電子情報通信学会 非線形問題研究会研究会

４．発表年
2020年

〔図書〕　計0件

〔産業財産権〕

〔その他〕
山口大学理学部数理情報科学研究室
https://www.is.sci.yamaguchi-u.ac.jp/Japanese/

６．研究組織

	氏名 （ローマ字氏名） （研究者番号）	所属研究機関・部局・職 （機関番号）	備考

７．科研費を使用して開催した国際研究集会

〔国際研究集会〕　計0件

８．本研究に関連して実施した国際共同研究の実施状況

共同研究相手国	相手方研究機関