

科学研究費助成事業 研究成果報告書

平成 28 年 6 月 7 日現在

機関番号：15501

研究種目：基盤研究(C) (一般)

研究期間：2013～2015

課題番号：25330028

研究課題名(和文) 情報ハイディング技術の標準化と性能保証への基盤構築

研究課題名(英文) Standardization of information hiding techniques and infrastructure for their performance warranty

研究代表者

川村 正樹 (Kawamura, Masaki)

山口大学・理工学研究科・准教授

研究者番号：60314796

交付決定額(研究期間全体)：(直接経費) 2,600,000円

研究成果の概要(和文)：電子透かしの評価基準に基づいて、様々な電子透かし手法を提案し、評価してきた。スペクトル拡散型電子透かしでは、温度スケジューリングを適切に行うことにより、復号性能を向上させることができた。また、ステゴ画像に対する切り出し攻撃に対応するために、同期符号を用いる誤り訂正符号による手法と、同期符号を用いない特徴抽出による手法を検討した。前者はLDPC符号や接続符号を用いることにより、切り出し攻撃に対応する手法を確立できた。また、後者は拡大縮小や回転攻撃にも対応できる手法となった。

研究成果の概要(英文)：We proposed various types of watermarking methods in accordance with the evaluation criteria of the watermarking methods, and evaluated them. The spread spectrum watermarking method could achieve good performance by using suitable scheduling. Against clipping attack to stego-images, we considered two methods. One is the method using error correcting codes with a synchronization code, and the other is the method using feature extraction without the synchronization code. The former could counter the clipping attack by using LDPC and concatenated codes. The latter could have potential ability to counter the scaling and rotation attacks.

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 電子透かしコンテスト 誤り訂正符号 情報統計力学

1. 研究開始当初の背景

情報ハイディング(Information Hiding)技術とは、著作情報など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。インターネットの普及に伴い、著作権の保護を如何に行うかが重要な課題になっている。特に、音楽や映像などをダウンロード配信するニーズは急速に拡大しており、それらに対応する情報保護技術を構築していかなければならない。2012年、著作物をダウンロードすることも違法化されるなどの罰則の強化が行われているが、それを防止する情報技術の開発は遅れている。IH技術はマルチメディアコンテンツの認証や機密情報保護のための中核技術として注目されている。しかしながら、データの圧縮や改変、加工を含む攻撃への耐性が弱いことや、これらの攻撃耐性についての安全性の保証が課題であり、完全な実用化には至っていない。

著作権管理技術をはじめとするIH技術の向上を目指すために、平成23年度より、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)委員会が発足した。申請者も専門委員として参加している。本委員会では、評価基準を定め、コンテストを実施することによって、より良い情報ハイディング技術の開発を促している。第1回のコンテストでは、申請者が応募した手法が最も画質への影響が小さい埋め込み手法となり、高画質賞を受賞した(2012年[応募8件中1件受賞])。このように、技術開発の先頭に立って、研究を行っている。

電子透かしの埋め込み方法には、マトリックス埋め込み法[Fridrich & Soukal (2006)]や、Wet Paper符号を用いた埋め込み法、拡散符号を用いたスペクトル拡散[Cox et al. (1997)]が提案されている。これらの手法は、情報科学の分野で扱われてきたが、近年、申請者を含め、情報統計力学による評価が注目されている。

申請者は、電子透かしに対して情報統計力学を適用し、その復号性能を理論的に求めてきた。透かし情報の復号問題はNP困難であり、近似的な解法が必要である。そこで、最も適な復号方法を提案し、性能評価を行ってきた。また、原画像が未知の場合について、画像修復を行いながら復号を行う方法を提案し、統計力学の手法を用いて、理論的に性能限界を求めた。このように、アドホックに復号アルゴリズムを検討するのではなく、統計力学に立脚した数理モデルを構築することにより、電子透かしモデルの標準化を目指し、その性能を理論的に評価することに取組んできた。

2. 研究の目的

スペクトル拡散については、十分な成果が

得られつつあるが、他のIH技術は理論的な評価が行われていない。そこで、これらの手法についても情報統計力学を適用し、定式化するとともに理論評価を行っていく。

まず、Wet Paper符号を用いた電子透かしを取り上げる。これは、画質の変化が最小となるように透かしを埋め込む手法である。すなわち、変更画素が少ないスパースな解を求める問題である。近年、情報科学と統計物理学において、圧縮センシングが注目されている。これはスパースな未知ベクトル x を線形変換した観測ベクトル $y=Ax$ から求める手法である。このとき、観測ベクトル y の方が次元が小さく、一般的には、解を一意に定めることはできない。しかしながら、スパース性を考慮すると、 l_p -ノルム最適化問題として定式化でき、解を定めることができるのである。申請者はWet Paper符号に、圧縮センシングを利用できることを発見し、その解法に取組み始めている。

IHCのコンテストに対応しながら、復号アルゴリズムの改良を行う。また、最適化問題として定式化することにより、数理構造を明確化し、IHモデルを確立する。IHモデルの標準化を目指すと共に、情報統計力学による理論的な評価により、IHモデルの安全性・性能の保証を行えるようにする。このように、不正なユーザからの攻撃に耐性をもつ手法を提案し、理論的な保証を与えることによって、インターネット上でも安全な情報コンテンツの管理に貢献することが本研究の目的である。

3. 研究の方法

「電子透かしモデル」と呼ばれる統一モデルは、未だに存在しない。現在は、スペクトル拡散型のモデルや、線形符号を用いたモデルなどいくつかのモデルが提案されている。そこで、これらのモデル毎に標準的なモデルを構築し、その後、電子透かしコンテストで、優れたモデルを競わせることにより、統一モデルに近づけていくことができる。

様々なモデルの中で標準的な手法を検討する必要がある。したがって、以下の項目に取り組む。

- (1) スペクトル拡散型電子透かしモデル
- (2) Wet Paper符号によるモデル
- (3) 電子透かしコンテストへの応募

(1) スペクトル拡散型電子透かしモデルでは、申請者はいくつかの復号アルゴリズムを提案し、その性能評価を行ってきた。しかし、実用化に向けて、次の未解決の問題がある。

①ハイパーパラメータの推定

これまでの申請者の研究により、確率的な復号の方が復号性能が良いことがわかった。この場合、温度パラメータなどのハイパーパラメータを決める必要がある。つまり、通信路ノイズの推定を行う必要がある。これには、情報統計力学で用いられるハイパーパラメ

ータ推定を応用する。

②画素の同期の問題

スペクトル拡散では、透かしを埋め込む位置が揃っている必要がある。攻撃を受けた場合、画素位置がずれていることがある。従って、復号する前に同期させる必要がある。CDMA で用いられている技術を電子透かしに応用することを検討する。

(2) Wet Paper 符号[Fridrich *et al.* (2005)]の方法は、マトリックス埋め込みにも応用される基盤となるモデルである。この手法による埋め込みに、スパース推定を導入し、 l_1 -ノルム最適化問題として定式化する。また、得られる解を、従来法の解と比べ、その性能を評価する。

(3) 第1回の評価基準はかなり緩い制約であった。今後、この基準は引き上げられていくので、それに対応した埋め込み手法の開発を行い、性能評価する。毎年、継続的にコンテストへ応募し、他の技術を参考にしながら、技術の向上を目指す。

4. 研究成果

(1) スペクトル拡散型電子透かしモデルでは、確率的な復号法を提案した。ビット誤り率による評価を行った結果、提案手法の復号性能が従来法よりも良いことが分かった。そこで、ハイパーパラメータ推定を応用し、温度スケジューリングを導入した手法を提案した。この成果は、電子情報通信学会和文誌Aに掲載されている[論文③]。

第3回電子透かしコンテストでは、JPEG 圧縮と切り出し攻撃が想定された。そこで、評価基準に準拠し、切り出し攻撃に対応するために、画素同期の問題に取り組んだ。透かしを埋め込んだ位置を特定するために、透かし情報とは別にマーカー（同期符号）を導入した。マーカーを導入することによって、透かしの埋め込み位置を探索する時間を大幅に短縮させることができた。

一方、マーカーを導入することによって、埋め込み量が増大することにより、画質の低下が問題となった。また、マーカーの形状や配置を最適化することも必要となった。

スペクトル拡散型電子透かしは、拡散符号を用いてメッセージを拡散し、透かしとして画像に埋め込む。この拡散符号は、同期符号とみなすことができるので、切り出し攻撃を受けた画像から拡散符号との相関が高い位置を求めることにより、同期させることができる。その成果は、電子情報通信学会英文誌Dに掲載された[論文②]。

(2) Wet Paper 符号を用いた電子透かしの埋め込み法では、原画像とステゴ画像の差分が小さくなるように埋め込むことが可能である。差分が小さいと、高画質なステゴ画像を得ることができる。Wet Paper 符号による方法をスパース推定ができる形に定式化し、スパース解を求めることができた。しかしなが

ら、一部の係数を大きく変化させてしまうため、そのままではインパルス雑音のような雑音に乗ってしまうことが分かった。PSNRによる画質の評価では、30 dB 以上であっても、主観的评价では、雑音が気になるレベルであった。

この手法を改良し、ウェーブレット係数ではなく、離散コサイン変換係数に埋め込むことにした。また、複数の DCT 係数を利用し、雑音が目立たないような埋め込みを採用した。その結果、従来より画質が向上し、本手法の有効性が高まった。これらの成果は、EMM 研究会で発表を行っている。

(3) 切り出し攻撃に対して、マーカーを用いる方法も検討した。マーカーの分だけ埋め込み量が増大するため、メッセージを効率良く符号化する必要がある。そこで、低密度パリティチェック符号(LDPC)を導入した手法を提案した。また、マーカーの形状や配置を最適化し、マーカーを用いないスペクトル拡散型電子透かしよりも符号長を短くすることに成功した。本手法を第3回電子透かしコンテストに応募した結果、画質が最も良い高画質賞を得ることができた。この成果は、国際会議 IWIHC で発表した[学会発表⑨]。

第4回電子透かしコンテストでは、さらに、拡大縮小と回転攻撃が加えられた。拡大率と回転角は既知であったので、同期符号を用いる手法を応用することができた。しかしながら、拡大縮小と回転により、画像が大きく歪むため、さらに誤り訂正能力を上げる必要があった。そこで、接続符号を取り入れることにした。本手法では、多数の誤りを大幅に訂正できる LDPC 符号と、少数の誤りを確実に訂正できる BCH 符号を組み合わせた接続符号を用いた。その結果、符号効率の高い誤り訂正符号を構成することができ、コンテストの基準を達成することができた。この成果は、国際会議 IWDW2015 で発表し、Springer からレクチャーノートとして出版されている[論文①]。

拡大縮小と回転攻撃のパラメータが未知の場合、同期符号を用いた手法では対応できなくなると予想される。そこで、画像の特徴点を抽出し、その点の近傍に透かしを埋め込む手法を検討した。本手法では、拡大縮小に対して不変な SIFT 特徴量を用いた。ただし、回転攻撃に対しては、総当たりで検出する必要がある。この部分はまだ開発中である。この成果を情報科学フォーラム(FIT2015)で発表した結果、FIT 奨励賞を得ることができた。また、EMM 研究会においても、優秀ポスター賞を受賞した。

以上のように、IHC 委員会の定める電子透かしコンテストに基づき、様々な手法を提案し、評価してきた。同期の問題は、マーカーを導入することによって、解決できた。また、スペクトル拡散型電子透かしは拡散符号を同期符号として使うことができた。

5. 主な発表論文等

(研究代表者、研究分担者及び連携研究者には下線)

[雑誌論文] (計 3 件)

- ① Nobuhiro Hirata, Masaki Kawamura, "Watermarking method using concatenated code for scaling and rotation attacks," Lecture Notes in Computer Science, Digital-Forensics and Watermarking, Springer, vol. 9569, pp. 259-270, 2016. 査読あり
DOI: 10.1007/978-3-319-31960-5
- ② Takahiro Yamamoto, Masaki Kawamura, "Method of spread spectrum watermarking using quantization index modulation for cropped images," IEICE, Vol. E98-D, No. 7, pp. 1306-1315, 2015. 査読あり
DOI: 10.1587/transinf.2014EDP739
- ③ 寺西 直緒, 川村 正樹, "スペクトル拡散モデルにおける非同期確率アルゴリズムおよび温度スケジューリングによる復号の性能評価," 電子情報通信学会論文誌, Vol. J96-A, No. 7, pp. 452-461, 2013. 査読あり
http://search.ieice.org/bin/summary.php?id=j96-a_7_452

[学会発表] (計 17 件)

- ① 内田 洸太, 川村 正樹, "拡大縮小と回転攻撃に対する SIFT に基づく電子透かし法の評価," 電子情報通信学会, 第 6 回マルチメディア情報ハイディング・エンリッチメント (EMM) 研究会, 屋久島環境文化村センター (鹿児島県屋久島町), 2016 年 3 月 2 日-3 日.
- ② 東 友梨, 川村 正樹, "複数の DCT 係数を用いた wet paper 符号による埋め込み手法," 電子情報通信学会, 第 6 回マルチメディア情報ハイディング・エンリッチメント (EMM) 研究会, 屋久島環境文化村センター (鹿児島県屋久島町), 2016 年 3 月 2 日-3 日.
- ③ 内田 洸太, 川村 正樹, "スケール攻撃に対する SIFT に基づく電子透かし法の評価," 情報科学技術フォーラム (FIT2015), 愛媛大学 (愛媛県松山市), 2015 年 9 月 15-17 日.
- ④ 内田 洸太, 川村 正樹, "SIFT 特徴点周辺領域を用いた電子透かし法の検討," 電子情報通信学会, 第 6 回マルチメディア情報ハイディング・エンリッチメント (EMM) 研究会, 大濱信泉記念館 (沖縄県石垣市), 2015 年 3 月 12-13 日.
- ⑤ 岩本 拓也, 川村 正樹, "PDF 文書に対する動的な不可視透かし埋め込みシステムの開発," 電子情報通信学会, 第 6 回マルチメディア情報ハイディング・エンリッチメント (EMM) 研究会, 大濱信泉記念館 (沖縄県石垣市), 2015 年 3 月 12-13 日.
- ⑥ 山本 隆博, 川村 正樹, "FIST 法を用いた Wet paper 符号による埋め込み手法の提案," 電子情報通信学会, 第 5 回マルチメディア情報ハイディング・エンリッチメント (EMM) 研究会, 東北大学 (宮城県仙台市), 2015 年 1 月 29 日.
- ⑦ 平田 展裕, 川村 正樹, "電子透かしに対する接続符号の導入," 電子情報通信学会, 第 5 回マルチメディア情報ハイディング・エンリッチメント (EMM) 研究会, 東北大学 (宮城県仙台市), 2015 年 1 月 29 日.
- ⑧ 金森 雷太, 川村 正樹, "基底画像の置き換えによる 2 値の透かし情報の埋め込み法," 情報科学技術フォーラム (FIT2014), 筑波大学 (茨城県つくば市), 2014 年 9 月 3-5 日.
- ⑨ Nobuhiro Hirata, Masaki Kawamura, "Digital Watermarking Method using LDPC Code for Clipped Image," The First International Workshop on Information Hiding and its Criteria for evaluation (IWIHC 2014), 京都ガーデンパレス (京都府上京区), 2014 年 6 月 3 日.
- ⑩ 金森 雷太, 川村 正樹, "基底画像の置き換えによる電子透かしの埋め込み法の提案," 電子情報通信学会, 第 6 回マルチメディア情報ハイディング・エンリッチメント研究会 (EMM), 北陸先端大学 (石川県能美市), 2014 年 3 月 7-8 日.
- ⑪ 平田 展裕, 川村 正樹, "電子透かしに適したソーラス符号と LDPC 符号の誤り訂正能力の比較," 電子情報通信学会, 第 6 回マルチメディア情報ハイディング・エンリッチメント研究会 (EMM), 北陸先端大学 (石川県能美市), 2014 年 3 月 7-8 日.
- ⑫ 児玉 涼, 川村 正樹, "クリッピング画像からの透かし復号法とその IHC に基づく評価," 電子情報通信学会, 第 5 回マルチメディア情報ハイディング・エンリッチメント (EMM) 研究会, 東北大学 (宮城県仙台市), 2014 年 1 月 27-28 日.
- ⑬ 山本 隆博, 川村 正樹, "クリッピングを

考慮したスペクトル拡散型電子透かしの IHC に準拠する評価,” 第 64 回 電気・情報関連学会中国支部連合大会, 岡山大学 (岡山県岡山市), 2013 年 10 月 19 日.

- ⑭ 児玉 涼, 金森 雷太, 川村 正樹, “ウェーブレット変換を用いた電子透かしの IHC による評価,” 第 64 回 電気・情報関連学会中国支部連合大会, 岡山大学 (岡山県岡山市), 2013 年 10 月 19 日.
- ⑮ 平田 展裕, 川村 正樹, “ソーラス符号を用いた電子透かしの IHC に基づく評価,” 第 64 回 電気・情報関連学会中国支部連合大会, 岡山大学 (岡山県岡山市), 2013 年 10 月 19 日.
- ⑯ 平田展裕, 川村 正樹, “ソーラス符号を用いた電子透かしの提案,” 情報科学技術フォーラム(FIT2013), 鳥取大学 (鳥取県鳥取市), 2013 年 9 月 4 日.
- ⑰ 山本 隆博, 川村 正樹, “Wet Paper 符号に対する IST 法の導入とその問題点に関する検討,” 電子情報通信学会, 第 1 回 マルチメディア情報ハイディング・エンリッチメント研究会 (EMM), 高知城ホール (高知県高知市), 2013 年 5 月 24 日-25 日.

6. 研究組織

(1) 研究代表者

川村 正樹 (KAWAMURA, Masaki)

山口大学・大学院理工学研究科・准教授

研究者番号: 60314796