様式Ｃ－１９

科学研究費助成事業（科学研究費補助金）研究成果報告書

平成２５年４月１６日現在

機関番号：１５５０１
研究種目： 若手研究(B)
研究期間： 2009～2012
課題番号： 21700255
研究課題名（和文） 拡散符号を用いた多重化した電子透かし法の確立と復号アルゴリズムの開発
研究課題名（英文） Establishing multiplexed watermarking method using spread code and development of its decoding algorithm
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

研究成果の概要（和文）：電子透かしに対して、最適な復号アルゴリズムを提案することが目的である。ベイズ最適な復号は計算困難であるので、復号アルゴリズムを工夫する必要がある。透かし間干渉を低減する方法や攻撃等によって生じるノイズの性質を調べ、様々な復号アルゴリズムを提案し、評価した。その結果、同期更新よりも非同期更新で復号する方が良いことがわかった。また、決定論的に推定するよりも、確率的な推定方法がよいことがわかった。

研究成果の概要（英文）：Our goal is to propose optimal decoding algorithms for digital watermarking. Since it is hard to obtain Bayes optimal solutions, we need to devise decoding algorithms. We studied both methods reducing interference between the watermarks and property of noises caused by attacks, and then, we proposed various algorithms and evaluated them. As a result, we found asynchronous update is better than synchronous one, and stochastic estimation is better than deterministic one.

交付決定額

（金額単位：円）

	直接経費	間接経費	合　計
2009 年度	1,000,000	300,000	1,300,000
2010 年度	900,000	270,000	1,170,000
2011 年度	600,000	180,000	780,000
2012 年度	600000	180000	780000
年度			
総　計	3,100,000	930,000	4,030,000

研究分野：情報科学
科研費の分科・細目： 情報学、感性情報学・ソフトコンピューティング
キーワード：電子透かし、 スペクトル拡散， 復号アルゴリズム， ベイズ推定，情報統計力学

１．研究開始当初の背景

情報セキュリティの分野では、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、それに対応するセキュリティ技術も構築していかなければならない。その中で、情報ハイディング技術は暗号と併用可能な技術であり、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、以前から注目されていた。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が課題であり、完全な実用化には至っていない。経済産業省の技術戦略マップによると、電子透かし検出技術の開発が今後１０年間で求められている。電子透かしを埋め込む際に、誤り訂正機能（冗長性）を持たせることにより、耐性を持たせることが可能である。この手法には、シンドローム復号を用いたマトリックス埋め込み法[Fridrich & Soukal (2006)]や、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。マトリックス埋め込み法は情報理論の分野で研究が進んでいる。一方、スペクトル拡散は CDMA でも用いられていることから、情報統計力学による評価が行われている。
情報統計力学を用いた研究によって、確率的画像処理など情報処理の分野に対して、統計力学が適用可能であること、そして、新しい計算アルゴリズムの提案が可能であることが示されてきた。我々は、情報統計力学を用いてCDMAの通信容量を解析してきた[川村，岡田(2006)]。ベイズ最適な解を求めるためには、周辺事後確率を最大にする解を求めればよい。しかしながら、周辺事後確率を求めることは NP 困難であり、近似的な解法が必要である。これまでに、復号アルゴリズムに、連続時間・非同期・同期更新などを検討し、アルゴリズムによって達成できる性能が異なることを示してきた[武富,川村 (2006)]。すなわち、通信容量の解析だけではなく、復号アルゴリズムが極めて重要であることを示した。
本研究では、情報ハイディング技術の中でも電子透かしに注目する。特に、スペクトル拡散を用いた電子透かしは、拡散符号を用いるため、その冗長性により誤り訂正機能をもつ。また、ランダムな符号を用いるため、秘匿性に優れており、電子透かしの用途に適している。ただし、電子透かしを拡散するため、埋め込める情報量は大幅に減少してしまう。そこで、多重化した電子透かしに焦点を当てる。スペクトル拡散型電子透かしは、CDMA と同様な数理構造を持っている。具体的には、CDMA の送信情報が電子透かしに対応し、通信路ノイズが不正なユーザによる攻撃や埋め込み誤差とみなすことができる。しかしながら、電子透かし固有の問題がある。
問題点(1). 透かしを多重化して埋め込む場合、透かし間干渉を生じる。
問題点(2). 電子透かしに対して、コンテンツ（画像、映像等）はノイズとみなされる。
問題点(3). 攻撃や埋め込み誤差には、独立性や無相関性を仮定することができない。
これらの問題点を解決する必要がある。

２．研究の目的
本研究では、情報ハイディング技術の中でも電子透かしに注目する。電子透かしに対して、主に圧縮耐性をもつ新しい復号アルゴリズムを提案する。画像や映像は非可逆圧縮を伴う変換が流通時に行われるため、圧縮耐性を持つことが必須である。スペクトル拡散型電子透かしは、CDMA と同様な数理構造を持っている。しかしながら、前節で述べたように、電子透かし固有の問題点がある。これらの問題点を解決していく。
問題点(1)に対しては、CDMA の技術を元に、推定透かし情報を用いながら、透かし間干渉を除去するアルゴリズムを提案し、評価していく。また、様々な負荷や埋め込み誤差による影響を定量的に評価する。
問題点(2)に対しては、元コンテンツ（画像）が利用できない場合、元コンテンツを推定しながら透かし情報を復号しなければならない。しかしながら、元コンテンツはガウス分布のような単純な確率分布に従うことはなく、その扱いが難しい。そこで、情報統計力学が適用されている画像修復の手法（ベイズ推定に基づく事後確率最大化）を取り入れて、その復号性能を評価する。
問題点(3)は、データ圧縮では必ず発生する問題である。ブロック単位で圧縮処理を行うため、ブロック内では独立性を仮定することはできない。攻撃で生じるノイズを混合ガウス分布で近似を試み、その近似性能を評価することによって、より良い分布を求める。

３．研究の方法
各問題点を順次解決するために、次の方法を試みていく。
透かし間干渉の低減（問題点(1)）
透かし間干渉を低減させるアルゴリズムを検討する。CDMA では、マルチステージ復調[T. Tanaka (2001)]や部分干渉除去法[水谷, 田中, 岡田 (2004)]などが知られているので、電子透かしに対して有効であるかを評価する。さらに、同期と非同期のダイナミクスの違いを検討する。また、決定論的な方法と確率的な方法を比較していく。確率的な方法では、一定温度(確率)の場合やシミュレーテッド・アニーリング(SA)を考える。
画像のノイズ性の評価（問題点(2)）
原画像が既知の場合と未知の場合を計算機シミュレーションで評価し、原画像が電子透かしに与える影響の大きさを見積もる。また、ベイズ推定を応用し、原画像に対する事前確率を仮定することによって、劣化画像からメッセージと画像の両方を推定する定式化を行う。
ノイズの独立性、相関性を考慮した評価（問題点(3)）
JPEG や JPEG2000 などの標準的なデータ形式

を想定した場合、一般的に非可逆圧縮が用いられる。この処理は画像ブロック単位に行われるため、生じる誤差は独立ではなく、ブロック内で相関を生じる。すなわち、この影響を考慮した理論を構築する必要がある。まず、どのような分布になるのかを定量的に評価する。
復号アルゴリズムと評価方法の確立を目指すので、数値計算用の計算機システムを導入する。ベイズ最適な復号を行うには、周辺事後確率の計算が必要であり、これは NP 困難である。近似的な復号アルゴリズムを用いる場合、反復計算を伴い、計算量は多い。そのため、高性能な計算機を導入する。

４．研究成果
透かし間干渉の低減（問題点(1)）
計算機シミュレーションにより、様々な復号アルゴリズムを評価した結果、非同期更新で、確率的なアルゴリズムの復号性能が高いことがわかった[Senda, Kawamura (2009]他]。また、従来と同様に零度に収束させる SA に対して、西森温度で止める SA を提案し、その性能評価を行った結果、提案した復号アルゴリズムが良好な性能を有していることがわかった[寺西,川村(2013)他]。
画像のノイズ性の評価（問題点(2)）
画像の影響を排除するために、ベイズ推定を用いて、メッセージと原画像を推定する手法を提案した。レプリカ法を用いて、鞍点方程式を求めた結果、この方法は、CDMA モデルと画像修復モデルを結合したモデルになることがわかった。また、理論と計算機シミュレーションの結果はよく一致した。
ノイズの独立性、相関性を考慮した評価（問題点(3)）
理論評価する際には、ノイズ（攻撃）がガウス分布に従うと仮定する。しかしながら、実際の画像を用いた場合、必ずしもガウス仮定が成り立つかどうかは自明ではない。そこで、様々な拡散符号長に対してノイズ分布のガウス性を検定した。その結果、ガウス性が成り立つためには、かなり長い拡散符号長が必要であり、実用的な範囲ではガウス性は成り立たないことが明らかになった。この分布がどのような分布に従うかは、依然として未解決である。
画素置換による埋め込みの場合は、原画像の影響をガウス分布で近似することによって、理論値を求めることができた。しかしながら、DCT 係数に埋め込む場合は、ダブルピークを持つ分布となることがわかった。本研究では、混合ガウス分布で近似し、EM アルゴリズムを用いてパラメータを決定した。その結果、理論値と計算機シミュレーションとの誤差をより小さくすることに成功した。
電子情報通信学会情報ハイディング及びその評価基準委員会が開催した電子透かしコンテストに応募した結果、我々の手法が最も画質の高い埋め込み方法として、高画質賞を受賞した。

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 2 件）

① 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, A, (2013), 査読有り, 採録
② Kazuhiro Senda, Masaki Kawamura, ″Statistical-mechanical approach for multiple watermarks using spectrum spreading,″ Lecture Notes in Computer Science - Information Theoretic Security, Springer Berlin / Heidelberg, vol.5973, pp.231-247 (2010), 査読有り.
DOI: 10.1007/978-3-642-14496-7_18

〔学会発表〕（計 25 件）

① 寺西直緒, 川村正樹, ″スペクトル拡散型電子透かしにおける通信路推定を用いた復号法,″ 電子情報通信学会 技術報告, 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), ATR(京都), Vol.112, No.467, pp.65-70, 2013 年 3 月 7 日-8 日.
② 合志清, 栗林稔, 越前功, 岩田基, 川村正樹, 岩村惠市, ″画像・映像信号用電子透かし評価基準 2013 の提案,″ 暗号と情報セキュリティシンポジウム(SCIS 2013), ウェスティン都ホテル京都(京都), 3F1-1, 2013 年 1 月 22 日-25 日.
③ 山本隆博, 川村正樹, ″スペクトル拡散型電子透かしの IHC に基づく評価の報告,″ 電子情報通信学会 技術報告, 第 4 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), 大分大学(大分), Vol.112, No.293, pp.135-140, 2012 年 11 月 17 日.
④ 寺西直緒, 川村正樹, "スペクトル拡散型電子透かしにおける焼きなまし法のスケジューリング,″ 第 63 回電気・情報関連学会中国支部連合大会, 島根大学(島根), pp.317-318, 2012 年 10 月 20 日.
⑤ 山本隆博, 川村正樹, ″IHC 評価基準を満たす電子透かし方式,″ 第 63 回電気・情報関連学会中国支部連合大会, 島根大学(島根), pp.281-282, 2012 年 10 月 20 日.
⑥ 川村正樹, 上江洌達也, 岡田真人, ″画像修復を行う電子透かしモデルの性能評価 ～二次元イジングモデルによる画像修復～,″ 電子情報通信学会 技術報告, 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，北海道工業大学(札幌)，Vol.112，No.129，pp.29-34，2012年7月19日-20日.
⑦ 川村正樹，上江洌達也，岡田真人，″二次元イジング模型による画像修復を行う電子透かしモデルの性能,″日本物理学会 第67回年次大会，Vol.67，Issue 1，Part 2，関西学院大学(兵庫)，p.378，2012年3月27日.
⑧ 宮嵜翔太，川村正樹，″電子透かしにおけるノイズの混合ガウス分布近似,″電子情報通信学会 2012 年総合大会，D-21-2，岡山大学(岡山)，2012年3月20日.
⑨ 寺西直緒，川村正樹，″スペクトル拡散型電子透かしにおける焼きなまし法による復号の性能評価,″電子情報通信学会技術報告，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），大阪大学(大阪)，Vol.111，No.496，pp.49-54，2012年3月16日.
⑩ 川村正樹，上江洌達也，岡田真人，″画像修復ありスペクトル拡散型電子透かしモデルの統計力学的評価,″電子情報通信学会第 4 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，東北大学(仙台)，Vol.111，No.287，pp.53-58，2011 年 11 月 14 日-15 日.
⑪ Nao Teranishi，Masaki Kawamura，″Asynchronous stochastic decoder for spread spectrum digital watermarking,″ The Seventh International Conference on Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP 2011)，DUT International Convention Center，Dalian，China，Oct. 13-16，2011. DOI: 10.1109/IIHMSP.2011.41
⑫ 川村正樹，上江洌達也，岡田真人，″電子透かしモデルのレプリカ解析,″日本物理学会 第66回秋季大会，Vol.66，Issue 2，Part 2，富山大学(富山)，p.217，2011 年 9 月 22 日.
⑬ 川村正樹，上江洌達也，岡田真人，″レプリカ法による電子透かしモデルのRS解,″日本物理学会 第66回年次大会，Vol.66，Issue 1，Part 2，新潟大学(新潟)，p.340，2011年3月28日.
⑭ 宮嵜翔太，川村正樹，″画像推定誤差のガウス仮定の妥当性,″第12回マルチメディア情報ハイディング研究会，東北大学(仙台)，pp.11-16，2011年1月13日.
⑮ 宮嵜翔太，川村正樹，″画像推定誤差に対するガウス性の評価,″第 61 回 電気・情報関連学会中国支部連合大会，岡山県立大学(岡山)，pp.48-49，2010月10日23日.
⑯ 寺西直緒，川村正樹，″スペクトル拡散型電子透かしにおける確率的復号法の提案,″第61回 電気・情報関連学会中国支部連合大会，岡山県立大学(岡山)，p.298，2010年10月23日.
⑰ 寺西直緒，川村正樹，″スペクトル拡散型電子透かしの確率ダイナミクスの導入,″第11 回マルチメディア情報ハイディング研究会，長崎大学(長崎)，pp.7-12，2010年10 月8日.
⑱ 川村正樹，岡田真人，″SCSNA による電子透かしの評価,″日本物理学会 第 65 回年次大会 ，Vol.65，Issue 1，Part 2，岡山大学(岡山)，p.263，2010年3月20日.
⑲ 川村正樹，岡田真人，″スペクトル拡散型電子透かしの復号アルゴリズム,″電子情報通信学会 総合大会 ，東北大学(仙台)，pp.S23-S24，2010年3月16日-19日.
⑳ Kazuhiro Senda，Masaki Kawamura，″Statistical-mechanical approach for multiple watermarks using spectrum spreading,″ The 4th International Conference on Information Theoretic Security (ICITS 2009)，Granship，Shizuoka，Japan，Dec. 3-6，2009.
㉑ 川村正樹，岡田真人，″スペクトル拡散型電子透かしのブラインド復号器,″第 8 回マルチメディア情報ハイディング研究会，国立情報学研究所(東京)，pp.27-32，2009 年 11 月 27 日.
㉒ 川村正樹，玉井悠揮，仙田和丈，岡田真人，″画像推定を伴う電子透かしの復号法,″日本物理学会 2009 年秋季大会，熊本大学(熊本)，Vol.64，Issue 2，Part 2，pp.157，2009年9月25日-28日.
他３件

〔その他〕
ホームページ等
http://www.is.sci.yamaguchi-u.ac.jp/~kawamura/Japanese/papers/

６．研究組織
(1)研究代表者
川村　正樹　(MASAKI KAWAMURA)
山口大学・大学院理工学研究科・准教授
研究者番号： 60314796

(2)研究分担者
なし　　(　　)
研究者番号：

(3)連携研究者
なし　　(　　)
研究者番号：