

科学研究費助成事業（学術研究助成基金助成金）研究成果報告書

平成 25 年 6 月 7 日現在

機関番号：15401

研究種目：若手研究(B)

研究期間：2011～2012

課題番号：23700268

研究課題名（和文） 電子透かしのロバスト性強化に対する確率・統計的アプローチ

研究課題名（英文） Probability and statistical approaches to enhancement of robustness of digital watermarks

研究代表者

福光 昌由（中本 昌由）（FUKUMITSU MASAYOSHI (NAKAMOTO MASAYOSHI)）

広島大学・大学院工学研究院・助教

研究者番号：00403585

研究成果の概要（和文）：

本研究では、誤検出確率を埋め込み係数に基づいて理論的に計算することが可能であり、さらにビットパターンを埋め込み可能な電子透かし法を開発した。ここでは、秘密鍵を使用して透かし信号を反復してコンテンツに埋め込み、誤検出確率を保証した上で検出する方法を提案した。実験では、透かしの有無を誤検出率に基づいて判定可能なだけでなく、ビットパターンを復元できることを確認し、JPEG 圧縮、縮小、切り取りなどの各種攻撃に対して耐性があることを示した。

研究成果の概要（英文）：

This work treats the digital watermarking with considering the false positive probability and bit-pattern embedding. We propose an iterative embedding algorithm of watermarking signals which are generated by a secret key. Moreover, in the detection, the correlations between the watermarked coefficients and watermark signals are computed by using the secret key. In the experiment, we show the detection results with specified false positive probability and the bit-pattern recovery, and the comparison of the proposed method against JPEG compression, scaling down and cropping.

交付決定額

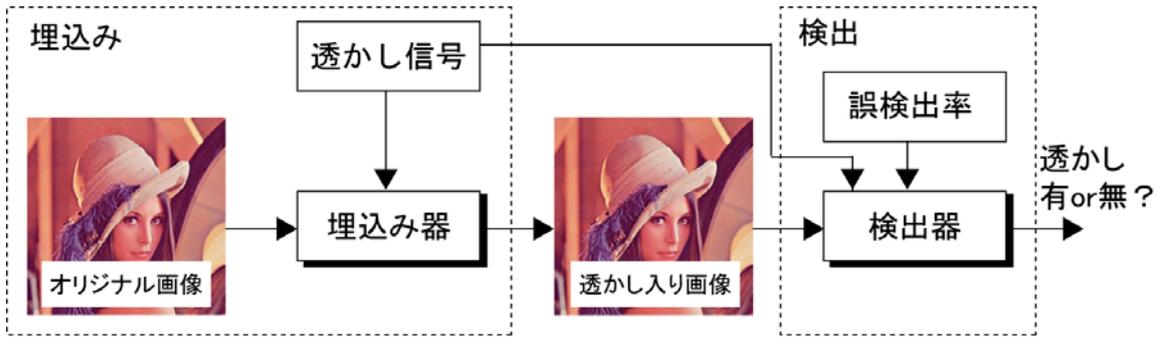
(金額単位：円)

	直接経費	間接経費	合計
交付決定額	2,600,000	780,000	3,380,000

研究分野：総合領域

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：確率的情報処理、電子透かし、著作権保護、ロバスト性、確率・統計、誤検出率、情報埋め込み、HVS、相関



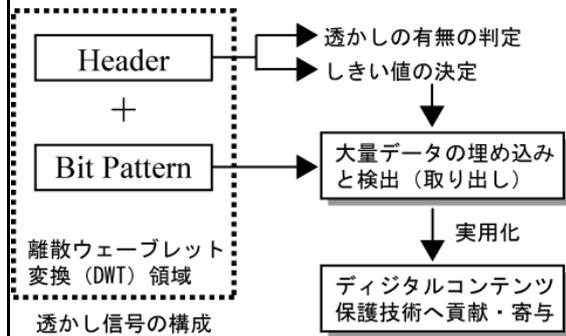
1. 研究開始当初の背景

近年、DVD やブルーレイディスクと言った大容量のデジタルコンテンツを記憶できる光学メディアが登場し、さらにインターネット網の整備とともに国内外のデジタルコンテンツ（音楽・画像・動画像など）が世界中に容易に配信・販売できるようになった。天然資源の乏しい我が国では、こういった「知的創作物」が今後の主要な輸出品の一つになると予想されている。その一方で、著作権・所有権を無視した複製が横行し、それにそれを不正に配布または販売すると言った違法行為が大きな社会問題となっている。絵画や陶器などの美術品と異なり、デジタルコンテンツは「完全な複製」を作成することが可能であり、その著作権や所有権を保護することは極めて難しいのが現状である。電子透かしと呼ばれる手法は、上記のような著作権保護における有力な手法として注目を集めており、現在、盛んに研究されている。電子透かしとは、音声・画像等のデジタルコンテンツの中に知覚できないような「透かし信号」を埋め込み、コンテンツに対して著作権・所有権や購入者に関する情報を付加するものである。上図は、(画像)電子透かし処理の一例である。埋込み処理では、疑似乱数列を透かし信号としてオリジナル画像に埋め込むことにより、透かし入り画像を得る。検出処理では、誤検出率を指定し、埋め込み時の透かし信号と透かし入り画像に基づいて検出を行う。すなわち、正当な所有者のみが透かし信号を正しく検出することができ、これがデジタルコンテンツの著作権・所有権の証となる。

2. 研究の目的

電子透かしはコンテンツの圧縮・切り取りなどの加工、および第三者による透かし信号の意図的な削除などの「攻撃」に対して頑強さを持つこと（ロバスト性）が要求される。一般に、電子透かしの埋め込みとして、画像の輝度領域に直接埋め込み方法と離散コサイン変換（DCT）領域や離散ウェーブレット（DWT）領域のような周波数領域に埋め込み

方法が知られているが、周波数領域に埋め込む方が透かしの攻撃に対する耐性が高いと言われている。本研究では、周波数領域の一つである DWT 領域に透かしを埋め込む方法を想定している。本研究課題は、攻撃を受けて透かし信号がダメージを受けた場合でも、高精度に透かしの検出が可能になるような新しい検出手法を開発し、確率・統計的な立場から電子透かしのロバスト性強化（検出性能向上）を目指す。これにより、知的創作物の著作権保護技術の発展に貢献することを目的とする（下図）。



3. 研究の方法

埋込み対象の DWT 係数を $y(i)$ 、埋め込む透かし信号 $x(i)$ を $\{-1, 1\}$ の 2 値をとる疑似乱数列、その重みを $w(i) (\geq 0)$ 、透かし埋め込み後の DWT 係数を $y'(i)$ とする。このとき、埋込みの式は次式のようになり、データ数を N とし、 $i=1, 2, \dots, N$ について繰り返す。

$$y'(i) = y(i) + w(i)x(i)$$

次に検出の原理を説明する。透かしの検出は、埋込み後の DWT 係数 $y'(i)$ と埋め込み時に用いた疑似乱数列 $x(i)$ を用いて以下の相関値 ρ を計算する。

$$\rho = \frac{1}{N} \sum_{i=1}^N y'(i)x(i)$$

$x(i)$ と $y(i)$ が無相関(透かし無し)なら相関は平均0に近く、相関有り(透かし有り)なら、相関値は0から離れた値をとる。したがって、誤検出率に基づいて計算されたしきい値によって透かしの有無を判定することができる。本研究では、透かしの検出時に、透かしが無いにもかかわらず「有り」と判断してしまう「陽誤検出の確率」を「誤検出確率」と呼ぶ。マルチビット埋め込みの原理は、埋め込み領域を K 分割してそれを $S_1, S_2 \dots S_K$ とし、各領域に1ビットの透かし信号を埋め込み、各領域の相関(局所相関)から透かし信号を検出することによって K ビットのデータを埋め込み・検出を可能としている。以上が従来の相関利用型電子透かしにおける埋め込み・検出手法である。埋め込み情報量の限界は埋め込み対象信号(ホスト信号)のサイズ(埋め込み領域の大きさ)に依存することが知られているが、相関利用型電子透かし法の場合、我々は相関値の分散にも依存すると予想し、既存の埋め込み手法の改良を行う。

4. 研究成果

本研究では、誤検出率を埋め込み係数の分散を元に理論的に計算し、検出した透かし信号の誤検出率を保証する電子透かし法を開発した。ここでは、透かし信号を反復してコンテンツ(画像)に埋め込み、誤検出確率を保証した上で検出する新たな方法を提案した。さらに、同時にコンテンツの中にビットパターンデータを埋め込みことにより、透かしの有無を誤検出率に基づいて判定できるだけでなく、様々な付加情報を埋め込むことが可能な手法を開発した。実験により、いくつかの静止画像に対してJPEG圧縮・縮小・クロッピング等の攻撃に対して十分な耐性を有することを確認した。

さらに、DWTされた領域に対して、人間の視覚特性(HVS)を考慮した上で透かし信号を埋め込む手法を開発した。従来法として、検出時に透かし入り係数と透かし信号の相関を計算し、相関値の正負符号に基づいてビット判定を行う手法が提案されているが、本研究では、この手法を改良し、より多くの情報を埋め込めるように埋め込み・検出方法を再構築した。従来法では、相関の正負符号によってビット判定を行っていたが、本研究では、埋め込み対象となるDWT係数と疑似乱数列の相関に応じて透かしの方向を決定し、相関の絶対値によってビット判定を行っている。このアイデアはこれまで我々が提案した手法をマルチビットに拡張したものである。ビット判定を行うための相関空間上の分割(しきい値の決定)を効率的に行う必要があるため、しきい値の決定方法が埋め込み情報量とロバスト性大きく影響する。ここでは、局所相関の絶対値の平均をしきい値として設定した。実験では、従来法と比べて2倍以上の情

報を埋め込み可能となることを確認した。また、電子透かしの安全性を向上させるため、情報の埋め込み空間を秘密鍵によって生成し、埋め込み空間を攻撃者から見つけにくくする方法についても検討した。提案法では、攻撃者が秘密鍵を相関計算によって特性するのは極めて困難となり、安全性が大幅に向上している。一方で、従来と同じようにHVSに基づいて透かしの埋め込みが可能であり、さらに、JPEG圧縮・縮小・クロッピング等に対するロバスト性もほぼ同等である。すなわち、従来の電子透かしの性能や利便性を損なうことなく、安全性のみを強化することに成功した。

本研究では、大学院生と共同で理論を構築して様々な角度から議論し、MATLABなどのソフトウェアを用いて実験的な検証を行った。電子透かしのロバスト性向上という目標に対し、確率・統計的視点という我々独自の立場からアプローチを行った。その結果、いくつかの興味深い結果が得られた。具体的には、透かしの検出に誤検出率を指定した上で、複数のビットを検出する方法や、従来よりも2倍以上ものデータ量(ビット長)を埋め込むことが可能な方法を提案することができた。上記研究課題に関連する研究成果は、査読付き論文、国際会議、国内査読付きワークショップおよびシンポジウム等で発表している。本研究課題に関連する研究成果は学会において高い評価を受け、後述するようにいくつかの賞を受賞している。また、研究成果のみならず、若手研究者(大学院生)を育成するという「教育成果」の面からも良好な成果が得られている。

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5件)

1. 藤井淳広, 中本昌由, 棟安実治, 大野修一: 人間の視覚特性を考慮したデジタル画像に対するデータ埋め込み法の改良, 電気学会論文誌 C, vol. 133, no. 1, 査読有, 2013, pp. 185-192.
2. 藪木直人, 中本昌由, 棟安実治, 大野修一: 鍵の解析攻撃に耐性のある画像電子透かし法, 第25回回路とシステムワークショップ論文集, pp. 121-126, 査読有, 巻無し, 2012. CD-ROM, 淡路市
3. N. Yabuki, M. Nakamoto, M. Muneyasu and S. Ohno: A secure image watermarking system with selecting embedding space, Proc of The 27th International

Technical Conference on Circuits/Systems, Computers and Communications (ITC-CSCC 2012), 査読有, 巻無し, 2012. CD-ROM, 札幌市

4. 左山紘平, 中本昌由, 棟安実治, 大野修一: 誤検出確率指定とビットパターン埋込みが可能な画像電子透かし法, 電気学会論文誌 C, vol. 132, no. 6, 査読有, 2012, pp. 932-939.
5. 中本昌由, 藤井淳広, 棟安実治, 大野修一: 相関検出器に基づく画像の離散ウェーブレット領域における情報埋込法, 第 24 回回路とシステムワークショップ論文集, pp. 116-121, 査読有, 巻無し, 2011. CD-ROM, 淡路市

[学会発表] (計 8 件)

1. 藤井淳広, 中本昌由, 棟安実治: 誤検出率を考慮したデジタル画像に対するデータ埋め込み法, 第 21 回計測自動制御学会中国支部学術講演会論文集, pp. 160-161, 2012 年 11 月 24 日, 広島市
2. 藪木直人, 中本昌由, 棟安実治: 直交変換行列の暗号化に基づくセキュア電子透かし法, 第 14 回 IEEE Hiroshima Student Symposium 論文集, pp. 487-490, 2012 年 11 月 17 日-11 月 18 日, 岡山県総社市
3. 左山紘平, 中本昌由, 棟安実治: 複数のビット埋込みが可能な誤検出率指定型電子透かし法, 第 13 回 IEEE Hiroshima Student Symposium 論文集, pp. 126-129, 2012 年 11 月 12 日-11 月 13 日, 東広島市
4. 藤井淳広, 中本昌由, 棟安実治: 人間の視覚特性を考慮した DWT 領域における情報埋め込み法の改良, 第 13 回 IEEE 広島支部学生シンポジウム論文集, pp. 130-133, 2012 年 11 月 12 日-11 月 13 日, 東広島市
5. 藪木直人, 中本昌由, 棟安実治, 大野修一: HVS を考慮した秘密鍵の解析攻撃に耐性のある画像電子透かし法, 平成 24 年度電気・情報関連学会中国支部第 62 回連合大会講演論文集, pp. 290-291, 2012 年 10 月 20 日, 鳥取市
6. 左山紘平, 中本昌由, 棟安実治, 大野修一: マルチビット埋込みと誤検出確率指

定による検出が可能な画像電子透かし法, 第 26 回信号処理シンポジウム, pp. 81-86, 2011 年 11 月 17 日, 札幌市

7. 左山紘平, 中本昌由, 棟安実治, 大野修一: マルチビット埋込みと誤検出率指定が可能な画像電子透かし法, 平成 23 年度電気・情報関連学会中国支部第 62 回連合大会講演論文集, pp. 86-87, 2011 年 10 月 22 日, 広島市
8. 藤井淳広, 中本昌由, 棟安実治, 大野修一: 相関情報に基づく離散ウェーブレット領域における情報埋め込み法, 平成 23 年度電気・情報関連学会中国支部第 62 回連合大会講演論文集, pp. 267-268, 2011 年 10 月 22 日, 広島市

[その他]

ホームページ等

本研究課題に関連した発表が, 以下の賞を受賞した.

- IEEE 広島支部学生シンポジウム優秀研究賞 (2 件)
- 情報処理学会中国支部 奨励賞 (2 件)
- 電子情報通信学会中国支部 連合大会奨励賞
- 電子情報通信学会 回路とシステムワークショップ奨励賞

6. 研究組織

(1) 研究代表者 福光 昌由 (中本 昌由)
(FUKUMITSU MASAYOSHI
(NAKAMOTO MASAYOSHI))
広島大学・大学院工学研究院・助教
研究者番号: 00403585

(2) 研究分担者 無
()

研究者番号:

(3) 連携研究者 無
()

研究者番号: