様式 C-19

科学研究費補助金研究成果報告書

平成２１年　５月１９日現在

研究種目：基盤研究 (B)
研究期間：2006～2008
課題番号：１８３６０１８３
研究課題名（和文）　安全なＪＰＥＧ及びＪＰＥＧ２０００ステガノグラフィの研究開発

研究課題名（英文）　Research on Secure JPEG and JPEG2000 Steganography

研究代表者
野田　秀樹（NODA HIDEKI）
九州工業大学・大学院情報工学研究院・教授
研究者番号：80274554

研究成果の概要：
秘密情報の存在自体を隠すことを目的とするステガノグラフィでは，情報が埋め込まれていることを検出されないことが必要である．メディアデータは圧縮ファイルとして送受信されるのが普通である点を考慮して，JPEG 画像や JPEG2000 画像を用いた，埋め込み検出が困難な安全性の高いステガノグラフィを実現した．提案法では，離散コサイン変換係数や離散ウェーブレット変換係数の量子化時に，QIM （quantization index modulation）を適用して埋め込みを行っている．

交付額

（金額単位：円）

	直接経費	間接経費	合　計
２００６年度	5,000,000	1,500,000	6,500,000
２００７年度	1,700,000	510,000	2,210,000
２００８年度	4,000,000	1,200,000	5,200,000
年度			
年度			
総　計	10,700,000	3,210,000	13,910,000

研究分野：情報工学
科研費の分科・細目：電気電子工学・通信・ネットワーク工学
キーワード：情報保護，情報秘匿，ステガノグラフィ，ステガナリシス，埋め込み検出，JPEG，JPEG2000

１．研究開始当初の背景

暗号とは異なる情報保護技術として情報秘匿技術が関心を集めている．情報秘匿技術は，画像，ビデオ，音楽データ等のメディアデータ中に，第三者に知られたくない重要な情報を隠す技術であり，ステガノグラフィ技術と電子透かし技術に二分される．ステガノグラフィは，秘密情報や秘密通信の存在自体を隠す技術であり，暗号と併用することによって極めて強力な情報保護が実現できる．

ステガノグラフィでは，メディアデータは秘密情報を埋め込むための容器（ダミーデータ）として用いられる．ダミーデータ中に大量の秘密情報が隠されていても，そのことを第三者に気付かれないことが必要である．もし気付かれれば，秘密情報の存在自体を隠すことを目的とするステガノグラフィの意味がなくなる．例えば，ダミーデータが画像の場合，情報を埋め込む前と後の画像は，それぞれ，カバー画像，ステゴ画像と呼ばれる．どのような手段を用いてもステゴ画像とカバー画像とを区別できなければ，ステガノグ

ラフィは安全であるといえる．従来は，人間の主観判断によって両者が区別できないことを安全性の拠り所としていたが，最近は，統計的検定やパターン認識手法を用いた判定法が研究されている．その結果，従来の埋め込み法のかなりの部分は，埋め込み検出（情報が埋め込まれているか否かの判定）が可能であることがわかってきた．このような埋め込み検出に代表される，ステガノグラフィに対する攻撃は総称してステガナリシスと呼ばれている．

２．研究の目的

本研究の目的は，安全なステガノグラフィの実現を目指して，ステガナリシスに対して耐性を有するステガノグラフィを研究開発することである．各種メディアデータは圧縮ファイルとして送受信されるのが普通である．この点を考慮して，標準規格で非可逆圧縮されたメディアデータを用いる安全なステガノグラフィを実現する．具体的には，静止画像としては JPEG 規格と JPEG2000 規格，動画像としては MPEG 規格と Motion-JPEG2000（JPEG2000 規格の一部）による圧縮データを対象とする．JPEG と MPEG では離散コサイン変換（DCT）が，JPEG2000 と Motion-JPEG2000 では離散ウェーブレット変換（DWT）が用いられており，情報は DCT 係数や DWT 係数中へ埋め込むことになる．

これまでに提案されている JPEG 画像や JPEG2000 画像を用いるステガノグラフィ（それぞれ，JPEG ステガノグラフィ，JPEG2000 ステガノグラフィと呼ぶ）では，量子化された DCT 係数や DWT 係数を変化させることによって情報の埋め込みを行っている．JPEG ステガノグラフィに対するステガナリシスでは，埋め込み前後での量子化 DCT 係数の分布（ヒストグラム）の変化を捉えて埋め込み検出を行う場合が多い．このようなヒストグラム変化に基づく攻撃は，ヒストグラム攻撃と呼ばれる．

従来法とは違って本研究では，情報の埋め込みは DCT 係数や DWT 係数の量子化の際に（量子化後ではなく）行われる．埋め込みは，QIM （quantization index modulation）の枠組みで行う．QIM を用いた 2 値データの埋め込みでは，2 種類の量子化器を用意しておき，一方の量子化器で量子化することを 0 の埋め込みに，他方の量子化器を用いることを 1 の埋め込みに対応させる．このアプローチによって，埋め込み前後での係数の変化量を抑えることができ，情報を埋め込んだステゴ画像の品質低下を抑えることができる．この方法の直接的な適用では埋め込み前後でヒストグラムが変化するが，後述の工夫でヒストグラム変化を殆ど生じさせないことが可能であり，ヒストグラム攻撃に耐性を持たせることができる．本研究での提案法は，ヒストグラムの保存性を有すると共に高品質のステゴ画像を生成できるため，従来法と比べてステガナリシスに対する耐性が大きいことが期待できる．

３．研究の方法

(1) QIM を用いたステガノグラフィ

QIM を用いた JPEG ステガノグラフィ（QIM-JPEG ステガノグラフィ）は，QIM を DCT 係数の量子化に適用して情報を埋め込む方法である．QIM の直接的な適用は，埋め込み後のヒストグラムに顕著な変化をもたらすため，その変化を抑える工夫が必要となる．埋め込みによるヒストグラム変化は簡単な式で表現でき，絶対値の小さな（特に，0 と ±1 の）量子化 DCT 係数の頻度が大きく変化する．この問題は，量子化の際に，0 付近の DCT 係数に対して情報を埋め込まないデッドゾーンを設けることによって回避できる．デッドゾーンの範囲は，ヒストグラム変化を最小にするように設定できる．

QIM を用いた JPEG2000 ステガノグラフィ（QIM-JPEG2000 ステガノグラフィ）では，QIM を DWT 係数の量子化に適用して情報を埋め込む．JPEG2000 では，DWT 係数の量子化を行う時点で量子化幅を知ることができない（従って，量子化器を用意できない）問題点がある．それは，指定する圧縮率（ビットレート）での最適な量子化幅は，符号化の最終段階で決定される仕組みになっているためである．しかしこの問題は，埋め込み処理を復号化の途中から行うことによって解決できた．また，QIM-JPEG ステガノグラフィの場合と同様に，0 付近の DWT 係数に対してデッドゾーンを設けることによって，DWT 係数のヒストグラム変化の少ない埋め込みを実現できた．

QIM-JPEG2000 を含む大部分の JPEG2000 ステガノグラフィでは，情報の埋め込みによってファイルサイズが極端に増加する問題点がある．ファイルサイズの増加は，埋め込みによって DWT 係数 0 と ±1 の間で値が変化する場合に生じることを見出した．そのような変化を避ける埋め込みによって，ファイルサイズの増加を大幅に押さえる方法を開発した．この方法を改良 QIM-JPEG2000 と呼ぶ．

(2) ステガナリシスの方法

提案法の安全性は，ステガナリシス（埋め込み検出）実験によって評価した．埋め込み検出は，通常のパターン認識の枠組みで行うことができる．多数の学習用パターン（カバー画像とステゴ画像から抽出した特徴ベクトル）を用いて識別器の学習を行う．学習済みの識別器によって，未知画像がカバー画像とステゴ画像のいずれに属するかを判定する．ここでは，識別器としてフィッシャーの

線形識別器を用いた.

JPEG ステガノグラフィに対するステガナリシス(JPEG ステガナリシス)では,Fridrich らによる方法で特徴ベクトルを求めた. Fridrich 法によると,ステゴ画像のみからカバー画像の特徴量を推定できる特徴があるが,JPEG ステガナリシスに特化した方法である. 特徴ベクトルとして,直流成分を除く低周波の 5 つの DCT 係数のヒストグラムを用いた.

JPEG2000 ステガノグラフィに対するステガナリシス(JPEG2000 ステガナリシス)では,2 種類の特徴ベクトルを用いた. 第 1 の特徴ベクトルは, DWT 変換によって得られる各サブバンドの DWT 係数の高次統計量と, DWT 係数の線形予測誤差の高次統計量からなる 72 次元ベクトルである.第 2 の特徴ベクトルは, 5 レベルの DWT 変換で得られた各レベルのヒストグラムを表す 55 次元ベクトルとした.

４．研究成果

(1) JPEG ステガノグラフィの性能評価

408×306 画素, 8bpp (bit per pixel) のモノクロ濃淡画像 500 枚を用いて埋め込み性能評価とステガナリシス実験を行った. 提案法 (QIM-JPEG ステガノグラフィ) の性能評価は, WP (Wet Paper) 符号と F5 を用いた埋め込み法との比較によって行った. 情報埋め込み量は, 最も埋め込み量が少ない WP 符号の場合に合わせて 1036 byte とした. JPEG 圧縮における品質係数を種々変えて実験を行ったが, 一例として品質係数 90 の場合の結果を表 1 と表 2 に示す.表 1 中の PSNR(dB)値は, 画質の評価尺度である.KL ダイバージェンスは, 埋め込み前後のヒストグラムの違いを評価する尺度であり, 値が 0 に近いほどヒストグラムの保存性が良いことを表す. 表 1 の値は 500 枚の画像に対する埋め込み実験結果の平均である. WP との差は殆どないが, 提案法の埋め込み性能が良いことがわかる.

表 1　各種 JPEG ステガノグラフィの埋め込み性能

埋め込み方法	ファイルサイズ (byte)	PSNR(dB)	KL ダイバージェンス
埋め込みなし	36643	41.3	0.0
QIM	36666	41.0	0.0016
WP	36909	41.0	0.0018
F5	36250	40.8	0.0057

ステガナリシス実験では, 500 枚からランダムに選んだ 250 枚を学習用に, 残り 250 枚を評価用に用いた. 学習用や評価用に用いる画像をランダムに選択して行う実験を 100 回繰り返した平均の正解率を表 2 に示す. 判定の閾値は, 学習時に, カバー画像に対する正解判定率とステゴ画像に対する正解判定率が等しくなるように設定した. 表 2 から, WP との差は小さいが, 提案法が最も正解率が小さく, 安全性が高いことがわかる.

表 2　JPEG ステガナリシスにおける正解率 (%)

埋め込み方法	カバー画像	ステゴ画像
QIM	54.3	59.9
WP	55.3	60.4
F5	74.7	78.7

(2) JPEG2000 ステガノグラフィの性能評価

512×512 画素, 8bpp のモノクロ標準画像 8 枚 (Lena, Barbara, Mandrill, Airplane, Boat, Goldhill, Peppers, Zelda) を用いて埋め込み性能を評価した. JPEG2000 圧縮における目標ビットレートは 1bpp とした. 本研究で提案した QIM-JPEG2000 と改良 QIM-JPEG2000 (M-QIM) を, JPEG2000-BPCS, Lazy-JPEG2000 (Lazy モードの JPEG2000 圧縮時に埋め込む), LSB (最下位ビット置換) 埋め込みと比較した. 埋め込み量は, 最も埋め込み量が少ない Lazy-JPEG2000 の場合に合わせて 1866byte とした. 表 3 に埋め込み性能の比較結果を示す. これから, QIM と M-QIM は, 他の方法と比べて, ヒストグラムの保存性に優れていることがわかる. M-QIM は QIM と比べて, 埋め込みによるファイルサイズの増加が抑えられ, 埋め込み後の画質も非常に高いことがわかる. Lazy-JPEG2000 では, 算術符号化がバイパスされるビットにのみ埋め込むことから, ファイルサイズの増加は生じない.

JPEG2000 ステガナリシス実験では, 使用した特徴ベクトル以外は, JPEG の場合と同様に行った. 表 4 に実験結果を示す. これから, 全般的には, ウェーブレット特徴よりもヒストグラム特徴を用いる方が正解率が高いこと, M-QIM が最も正解率が小さく, 安全性が高いことがわかる.

表 3　各種 JPEG2000 ステガノグラフィの埋め込み性能

埋め込み方法	ファイルサイズ (byte)	PSNR(dB)	KL ダイバージェンス
埋め込みなし	32718	38.0	0.0
M-QIM	33144	37.4	0.0016
QIM	36221	36.4	0.0014
BPCS	35488	36.2	0.0041
Lazy	32756	33.0	0.0095
LSB	39138	35.2	0.0119

表 4　JPEG2000 ステガナリシスにおける正解率（%）

埋め込み方法	ウェーブレット特徴		ヒストグラム特徴	
	カバー画像	ステゴ画像	カバー画像	ステゴ画像
M-QIM	51.6	52.4	67.2	65.4
QIM	62.0	62.7	71.8	71.1
BPCS	73.3	73.5	88.8	87.7
Lazy	53.3	55.0	93.4	94.3
LSB	84.1	84.4	89.2	88.5

(3) まとめ

本研究では，JPEG 画像や JPEG2000 画像を用いたステガノグラフィにおいて，DCT 係数や DWT 係数の量子化時に，QIM を適用して埋め込みを行う方法を提案した．提案法は従来法と比べて，埋め込み検出が困難な安全性の高いステガノグラフィであることを確認した．現在のところ国内外で最も安全性の高いステガノグラフィの一つを提案できたものと確信している．MPEG や Motion-JPEG2000 動画像への適用も可能であることを確認したが，ステガナリシスによる安全性の検証は未実施である．

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１３件）

① T.Ishida, K.Yamawaki, H.Noda, M.Niimi, "An Improved JPEG2000 steganography using QIM and its evaluation by steganalysis", Proceedings of 2009 International Workshop on Advanced Image Technology, USB-ROM(2009), 査読有.

② M.Niimi, H.Noda, "Reversible information hiding for binary images based on selecting compressive pixels on noisy blocks", Proceedings of 2009 International Workshop on Advanced Image Technology, USB-ROM(2009), 査読有.

③ S.Ohyama, M.Niimi, K.Yamawaki, H.Noda, "Reversible data hiding of full color JPEG200 compressed bit-stream preserving bit-depth information", Proceedings of International Conference on Pattern Recognition, CD-ROM(2008), 査読有.

④ T.Ishida, K.Yamawaki, H.Noda, M.Niimi, "Performance improvement of JPEG2000 steganography using QIM", Proceedings of 2008 International Conference on Intelligent Information Hiding and Multimedia Signal Processing, pp.155-158(2008), 査読有.

⑤ S.Ohyama, M.Niimi, K.Yamawaki, H.Noda, "Lossless data hiding using bit-depth embedding for JPEG2000 compressed bit-stream", Proceedings of 2008 International Conference on Intelligent Information Hiding and Multimedia Signal Processing, pp.151-154(2008), 査読有.

⑥ S.Tanaka, M.Niimi, H.Noda, "A study on reversible information hiding using complexity measure for binary images", Proceedings of 2007 International Conference on Intelligent Information Hiding and Multimedia Signal Processing, Vol.2, pp.29-32(2007), 査読有.

⑦ H.Noda, Y.Tsukamizu, M.Niimi, "JPEG2000 steganography which preserves histograms of DWT coefficients", IEICE Trans. Information and Systems, Vol.E90-D, No.4, pp.783-786(2007), 査読有.

⑧ S.Tanaka, M.Niimi, H.Noda, "Reversible information hiding for binary images using complexity measure", Proceedings of 2007 International Workshop on Advanced Image Technology, pp.738-743(2007), 査読有.

⑨ K.Kozono, M.Niimi, H.Noda, "Information hiding for the color quantized images by Fibonacci lattice", Proceedings of 2007 International Workshop on Advanced Image Technology, pp.733-737(2007), 査読有.

⑩ H.Noda, Y.Tsukamizu, M.Niimi, "Steganography for JPEG2000 compressed images which preserves histograms of DWT coefficients", Proceedings of 2007 International Workshop on Advanced Image Technology, pp.61-65(2007), 査読有.

⑪ H.Noda, Y.Tsukamizu, M.Niimi, "JPEG2000 steganography possibly secure against histogram-based attack", Lecture Notes in Computer Science, Vol.4261, pp.80-87(2006), 査読有.

⑫ M.Niimi, T.Nakamura, H.Noda, "Application of complexity measure to reversible information hiding", Proceedings of the IEEE International Conference on Image Processing, pp.113-116(2006), 査読有.

⑬ H.Noda, M.Niimi, E.Kawaguchi, "High

performance JPEG steganography using quantization index modulation in DCT domain", Pattern Recognition Letters, Vol.27, pp.455-461(2006), 査読有.

〔学会発表〕(計９件)

① 新見道治, 野田心平, 野田秀樹, 2 値画像に対する可逆的情報ハイディング, 電子情報通信学会 2009 総合大会, 2009 年 3 月 20 日, 愛媛大学.
② 石田貴之, 山脇和美, 野田秀樹, 新見道治, JPEG2000 ステガノグラフィのステガナリシスによる評価, 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研究会, 2008 年 11 月 6 日, 東北大学.
③ 山脇和美, 野田秀樹, 新見道治, Wet Paper符号を用いたJPEG画像の改ざん検出, 平成 20 年度電気関係学会九州支部連合大会, 2008 年 9 月 25 日, 大分大学.
④ 向江勇気, 山脇和美, 野田秀樹, 新見道治, ステガナリシスへのAdaBoost適用の試み, 平成 20 年度電気関係学会九州支部連合大会, 2008 年 9 月 25 日, 大分大学.
⑤ 新見道治, 竹中雄太, 野田秀樹, ステガナリシスに対するスパースコーディングの効果, 平成 20 年度電気関係学会九州支部連合大会, 2008 年 9 月 25 日, 大分大学.
⑥ 石田貴之, 山脇和美, 野田秀樹, 新見道治, QIM-JPEG2000 ステガノグラフィの改良とステガナリシスによる評価, 平成20年度電気関係学会九州支部連合大会, 2008 年 9 月 25 日, 大分大学.
⑦ 大山承剛, 新見道治, 山脇和美, 野田秀樹, フルカラーJPEG2000 圧縮データに対する可逆的情報ハイディング, 2008 年映像情報メディア学会年次大会, 2008 年 8 月 29 日, 福岡工業大学.
⑧ 石田貴之, 山脇和美, 野田秀樹, 新見道治, QIMを用いたJPEG2000 ステガノグラフィの改良, 電子情報通信学会 2008 総合大会, 2008 年 3 月 21 日, 北九州学術研究都市.
⑨ 石田貴之, 野田秀樹, 新見道治, DWT係数のヒストグラム形状を保存するJPEG2000 ステガノグラフィ, 平成 19 年度電気関係学会九州支部連合大会, 2007 年 9 月 19 日, 琉球大学.

〔図書〕(計２件)

① 新見道治, 野田秀樹, 画像電子情報ハンドブック (画像電子学会編), 1.4.8 ステガノグラフィ, pp.521-526, 東京電機大学出版局 (2008).
② H.Noda, M.Niimi, E.Kawaguchi, "Steganographic methods focusing on BPCS steganography", Intelligent Multimedia Data Hiding, Springer, pp.189-229(2007).

６．研究組織

(1)研究代表者

野田　秀樹 (NODA　HIDEKI)

九州工業大学・大学院情報工学研究院・教授

研究者番号：80274554

(2)研究分担者

新見　道治 (NIIMI　MICHIHARU)

九州工業大学・大学院情報工学研究院・准教授

研究者番号：20269088

(3)連携研究者

なし