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　８日現在

研究種目：基盤研究（C）
研究期間：２００７～２００８
課題番号：１９５６０３８２
研究課題名（和文）電子透かしの信頼性向上への応用を考慮した
誤り訂正符号の復号法・性能評価
研究課題名（英文）　Decoding Methods of Error Correcting Code for the Reliable Digital Watermarking and their Performance Analysis

研究代表者
藤原　融（FUJIWARA TORU）
大阪大学・大学院情報科学研究科・教授
研究者番号：７０１９００９８

研究成果の概要：電子透かしの信頼性向上を目指した符号化・復号法として，誤り訂正限界を超えた誤り訂正が行え，かつ復号誤りが少なくなるようにするため，2 重符号化を用い，OSD 復号法をベースにした復号法を用いるのがよいとの見通しを得た．電子透かし法は，パッチワーク法とし，輝度値に埋め込む場合と周波数成分に埋め込む場合について性能評価し，よい復号特性を得られることを確認した．特に，周波数成分の場合は信頼度の高いビットに誤りが発生しにくいため，OSD 復号法の特性がより生かされている．

交付額

（金額単位：円）

	直接経費	間接経費	合　計
２００７年度	2,300,000	690,000	2,990,000
２００８年度	1,200,000	360,000	1,560,000
年度			
年度			
年度			
総　計	3,500,000	1,050,000	4,550,000

研究分野：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：コンテンツ保護，電子透かし，誤り訂正符号，誤り検出，OSD 復号法

１．研究開始当初の背景

誤り訂正符号の性能解析や復号法については，さまざまな研究が行われている．最近では文献[1]をはじめとして，誤り訂正限界（最小距離の 1/2）を超えた誤り訂正の能力や復号法に関する研究も注目されている．

一方，電子透かし技術の研究も盛んに行われている．電子透かし技術は，主として画像や音声などのディジタルコンテンツ（以下，コンテンツ）のデータに微少な変更を加え，コンテンツを視聴する人に気づかれないように情報を埋め込む技術である．以下では埋め込んだ情報を透かし情報と呼ぶ．透かし情報として著作権情報を埋め込めば，著作権保護に利用できる．しかし，加える変更が微少である故，圧縮・伸張処理などのメディア処理，あるいは攻撃の影響を受け，透かし情報が正しく抽出されないことがある．この誤りは，誤りは著作権法違反の誤認につながりかねず，抽出した透かし情報の十分な信頼性をもつことが重要である．

これに対する方策としては，透かし情報の抽出の過程において最適な抽出を行うための工夫を行うこと，埋め込む情報に冗長を加えて抽出時に誤りを訂正すること等が考えられる．研究代表者は，統計量に基づく電子

透かしにおいて，抽出過程における工夫についての研究をこれまでに行ってきた[2]．最適な抽出である程度の成果を挙げることができるが，さらに信頼性を上げるためには，誤り訂正符号が必要である．特に，元のコンテンツの質を保つため，透かし情報をできるだけ少なくする必要がある．このため，誤り訂正限界を超えた誤り訂正の能力や復号法に関する研究が重要となる．

国内では文献[3]，[4]等で誤り訂正符号を用いた信頼性向上の研究がなされている．特に[4]では，(127，64)BCH 符号など実用的な符号について Chase 復号法を用いた場合の誤り率の分析が行われている．また，国外でも文献[5]等，研究成果が出始めている．しかし，限られた状況での評価であり，復号法についても十分検討されていない．

通常の通信路における誤り訂正では，訂正限界を超えた場合の訂正の研究は，訂正が主体であり，誤り検出と併用することはほとんど考慮されていない．本研究においてこれを考慮することが誤り訂正符号の研究として特色ある点である．

２．研究の目的

本研究では，誤り訂正符号を，電子透かしの信頼性向上に適用する方法に主眼をおいて，符号の復号法，性能評価についての研究を行う．具体的には，以下の(1)～(5)を行う．

(1) 誤りの解析：電子透かし法と圧縮・伸張などのメディア処理，代表的な攻撃について，生じる誤りについてデータを集め，分析する．

(2) 電子透かしにおける誤り訂正符号の性能評価：誤りがランダムに近い場合に，各種の誤り訂正符号とその復号法の性能を評価し，電子透かしの抽出において誤り率の低い復号法を見出す．特に，誤り訂正限界（最小距離の 1/2）を超えた誤り訂正・検出に重点をおく．

(3) 誤り検出を考慮した復号方法の考案：電子透かしの抽出においては，復号誤り率が低いことが重要である．これを達成するためには，訂正せずに誤りを検出するに留めることも，状況によっては重要である．最尤復号をはじめ既存の復号法では，訂正せずに誤りを検出することはあまり考慮されていない．誤り検出を考慮した復号法を考案する．

(4) ランダム性を保つ埋め込み：電子透かし法とメディア処理・攻撃により，誤りがランダムに近くないことがあり得ることが予想される．交錯法（インターリーブ）や記号の並べ替え等により，これを回避することを検討する．

(5) 性能評価：以上の(1)～(4)に基づき，各種の電子透かし法と誤り訂正符号・復号法の組み合わせについて，性能を評価し，本研究で考案した技術の総合評価を行う．

３．研究の方法

目的の項に記載の具体的目的に基づき，以下のように研究を行った．

(1) 誤りの解析：電子透かし法と圧縮・伸張などのメディア処理，代表的な攻撃について，生じる誤りについてデータを集め，分析する．電子透かし法としては画素置換法，パッチワーク法やその変形など，メディア処理としては，実用的な圧縮・伸張，ランダムノイズの付加，透かしテストツールを対象とする．メディア処理の強度と誤りの関係，特に誤り数やランダム性について分析する．

(2) 電子透かしにおける誤り訂正符号の性能評価：誤りがランダムに近い場合に，各種の誤り訂正符号とその復号法の性能を評価し，電子透かしの抽出において誤り率の低い復号法を見出す．まず，(1)の結果をふまえ，誤りがランダムに近い，電子透かし法とメディア処理・攻撃を対象とする．電子透かし法としてはパッチワーク法やその変形など，メディア処理としては，実用的な圧縮・伸張，ランダムノイズの付加のうちにそのようなものがあると考えている．符号としては，符号長が 64，128 や 256 で符号化率が 1/2 程度の符号を対象とする．復号法としては，Chase 復号法，OSD（Ordered Statistics Decoding）復号法[7]及びその拡張復号法，再帰的最尤復号法及び関連する準最尤復号法などを対象とする．これらのプログラムを作成し，復号誤り率を評価する．

(3) 誤り検出を考慮した復号方法の考案：電子透かしの抽出においては，復号誤り率が低いことが重要である．これを達成するためには，訂正せずに誤りを検出するに留めることも，状況によっては重要である．最尤復号をはじめ既存の復号法では，訂正せずに誤りを検出することはあまり考慮されていないが，これらの復号法に基づき，誤り検出を考慮した復号法について検討する．このために，誤り訂正せず誤り検出に留めるための基準を検討する．情報記号の一部に一定パターンを付加するとか，動画の場合，前後のフレームでの誤り訂正状況を考慮するなど，考えうる基準について，シミュレーションによりデータを収集し，適当な基準を見出す．

(4) ランダム性を保つ埋め込み：電子透かし法とメディア処理・攻撃により，誤りがランダムに近くないことがあり得ることが予想される．具体的ないくつかの透かし法について誤りがランダムになるかどうかを調べ，そうでない場合，交錯法や記号の並べ替え等により，これを回避する方法を見い出し，シミュレーションにより評価する．

(5) 性能評価：ここまでの研究成果に基づき，

ここまでに対象とした電子透かし法と誤り訂正符号・復号法の組み合わせについて，シミュレーションにより性能を評価し，本研究で考案した技術の総合評価を行う．

４．研究成果

いくつかの電子透かし法や誤り訂正符号について(1), (2)の評価を行った後，電子透かしに用いる符号化，復号法を検討した．

コンテンツの質を維持するために多くの情報を埋め込むことができないため，冗長ビットを多くとることができない．このため，誤りビット数が訂正限界を超え，限界距離復号法では正しく復号できないことが多い．そこで,OSD 復号法を用いて復号することを考える．しかし，コンテンツに所有者情報を埋め込み，不正者特定に用いる場合などのように，誤った透かし情報を抽出するよりも抽出せずに誤りの検出のみ行ったほうがよい応用もある．これに対応するものが復号失敗である．

本研究では２重符号化を用いることで復号失敗を導入している．与えられた透かし情報を情報ビットとして，ある符号（外符号）C を用いて符号化し，符号語を生成する．また，得られた符号語を情報ビットとして,別の符号（内符号）C'により符号化し，符号語を生成する（図 1）．

復号段階では,OSD 復号法を用いて内符号 C'について復号し，得られた復号結果の情報ビットを取り出し，符号 C の符号語と一致しているかどうかを確認する．もし一致していればそれを出力し，一致していなければ復号失敗とする．こうすることで，復号はできたが結果が誤っている復号誤りを減らすことができる．

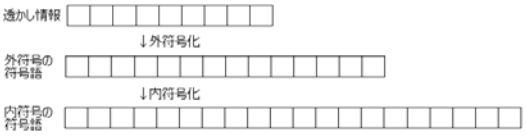

図１　２重符号化

次にこの復号法の性能評価を行うため，以下のような実験を実施した．

透かし情報は 64 ビットとし，それを 2 重符号化するための符号として，内符号の符号長（透かし情報に冗長ビットを加えて実際に埋め込む情報の長さ）は,127 ビットとした．そして，外符号と内符号への冗長ビットの分配を 3 通り考えた．外符号として，(71, 64)BCH 短縮符号,(78, 64)BCH 短縮符号,(85, 64)BCH 短縮符号を用いてそれぞれ符号長 71, 78, 85 の外符号とした．また，それぞれの外符号長に対して，内符号(127, 71, 19)BCH 符号，(127, 78, 15)BCH 符号，(127, 85, 13)BCH 符号をそれぞれ用いることで，埋め込みビット数を 127 となる．

電子透かし法としてパッチワーク法を選び，輝度値と周波数成分[8]に埋め込む方法を用いた．輝度値に埋め込む場合は以下のように行う．静止画像（動画のフレーム）に透かし情報としてビット 1 または 0 を埋め込むことを考える．ここで，埋め込み強度を正整数δとする．まず,画像から 2 つの画素をランダムに選び,それらの画素の輝度を(a_i, b_i)とする．透かし情報としてビット 1 を埋め込む場合，

$a_i \leftarrow a_i + \delta$

$b_i \leftarrow b_i - \delta$

また，透かし情報としてビット 0 を埋め込む場合，

$a_i \leftarrow a_i - \delta$

$b_i \leftarrow b_i + \delta$

とする．

ここで，画像中の画素を任意に選定して m 箇所に同じ透かし情報を埋め込む．

抽出の際，埋め込み時の乱数の種を用いて，情報を埋め込んだ場所を探す．$\Sigma(a_i - b_i)$が正ならば，ビット 1 が埋め込まれていると判断し，そうでなければ，ビット 0 が埋め込まれていると判断する．

周波数成分に埋め込む場合は，ウェーブレット変換により，周波数成分を抽出し，そこに同様の方法で埋め込む．

さらに，透かし情報を得られた符号語を画像に埋め込むサイズ 486×720 の画像フレームを n 枚用意し，各ビットをフレームに埋め込む．本研究では，シミュレーション時間の短縮のために，1 フレームに対して 4 ビットの情報を埋め込んでいる．この方法では，1 フレームに 1 ビットの情報を埋め込んだ場合よりも埋め込んだ箇所が 4 分の 1 となるため，正確でない可能性が高くなる．しかし，埋め込む箇所が 4 分の 1 に減少しても，十分除去や改ざんなどの攻撃に強く，1 フレームに 1 ビット埋め込む場合よりも多くのビットを埋め込むことができる．ここで，1 フレームに 4 つのビットを合計 m 箇所埋めるとするなら，1 つのビットを m/4 箇所に埋め込んだことになる．

本研究では，パッチワークでは透かし強度δ=4，選択画素ペア数 m=10,000 とし，離散ウェーブレット変換では透かし強度δ=4，選択画素ペア数 m=400 とした．このように埋め込みのパラメータが異なるが，誤り発生状況はほぼ同じとなる．図 2，3 に性能評価の結果を示す．

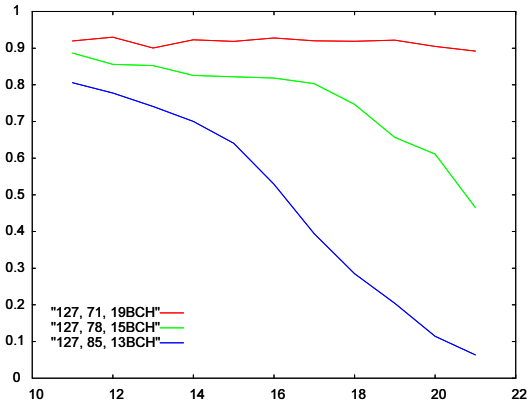

図２　輝度値への埋め込みの性能評価

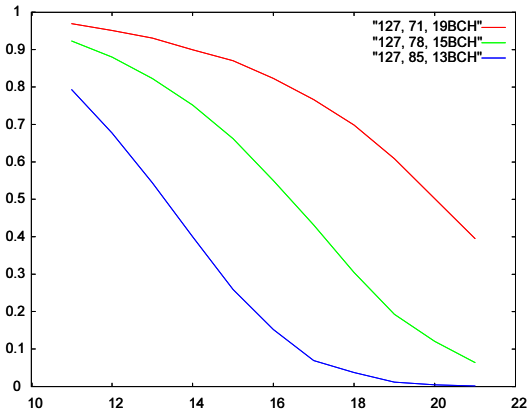

図３　周波数成分への埋め込みの性能評価

それぞれ横軸が復号前の誤りビット数，縦軸が正しく抽出する確率を表している．2 つの埋め込み法に共通して，外符号長が長くなるにつれ正しく抽出する確率は減少している．

しかし，2 つの結果を比べると，正しく抽出する確率が輝度値に埋め込む場合よりも，周波数成分に埋め込んだ場合のほうが大きい．これは，2 つの誤り特性について調べてみると，輝度値に埋め込んだ場合は信頼度が高くても誤りが発生することが多いのに対し，周波数成分に埋め込んだ場合信頼度が高いものに誤りがほぼ発生しないことがわかった．なお、透かし情報を誤って抽出する確率は、外符号が(n, k)符号の場合、ほぼ 2^{n-k} となり、外符号の符号化率で誤って抽出する確率を制御できる。

OSD 復号法では，信頼度の高いビットを情報ビットとみなし再符号化することで候補の符号語の集合を得ているために，信頼度の高いビットに誤りが少ないほど正しい透かし情報を抽出する確率が大きくなる．よって，周波数成分に埋め込んだ場合のほうがより OSD 復号法の特性を生かすことができていると考えられる．

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）

〔学会発表〕（計１件）
藤原　融：誤り訂正符号の性能評価，電子情報通信学会情報理論研究会，平成 21 年 3 月 9 日，函館市．

６．研究組織
(1)研究代表者
藤原　融（FUJIWARA TORU）
大阪大学・大学院情報科学研究科・教授
研究者番号：７０１９００９８

(2)研究分担者
なし

(3)連携研究者
なし

参考文献
[1] Error-Correction Capability of Binary Linear Codes, T. Helleseth, T.Klove and V.Levenshtein, IEEE Transactions on Information Theory, 51, 1408-1423, 2005.
[2] A New Scheme to Realize the Optimum Watermark Detection for the Additive Embedding Scheme with the Spatial Domain, Takaaki Fujita, Maki Yoshida, and Toru Fujiwara, IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, E90-A, 216-225, 2007.
[3] 誤り訂正符号を用いたアルゴリズム公開型電子透かし，　山口和彦，岩村恵市，今井秀樹，1999 年暗号と情報セキュリティシンポジウム，713-718，1999.
[4] 電子透かし検出に適した誤り訂正符号の拡張方式，藤井康広，越前功，山田隆亮，手塚悟，吉浦裕，情報処理学会論文誌，45，1980-1997，2004.
[5] Improving the Watermarking Process with Usage of Block Error-Correcting Codes, Todor Dotorov, Universite de Limoges, Report UMR CNRS 6090, 2005.
[6] A Trellis-Based Recursive Maximum Likelihood Decoding Algorithm for Linear Block Codes, Toru Fujiwara, Hiroshi Yamamoto, Tadao Kasami and Shu Lin, IEEE Transactions on Information Theory, 44, 714-729, 1998.

[7] Soft-Decision Decoding of Linear Block Codes Based on Ordered Statistics, Marc P. C. Fossorier and Shu Lin, IEEE Transaction on Information Theory, 41, 1379-1396, 1995.
[8] ウェーブレット変換を用いた動画像向け電子透かし方式, 荒木貴志, 宮崎明雄, 井上尚, 映像メディア学会誌, 54, 1606-1614, 2000.