様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９　（共通）

科学研究費助成事業　　研究成果報告書

平成　２９　年　　６　月　　８　日現在

機関番号：　１５３０１
研究種目：　基盤研究(C)（一般）
研究期間：　2014～2016
課題番号：　２６３３０１５７

研究課題名（和文）線形符号の軟値復号法を応用した電子透かしの冤罪の確率の低減に関する研究

研究課題名（英文）Study on digital watermark without detection error using soft-decision decoding for linear codes

研究代表者

日下　卓也（甲本卓也）（Kusaka, Takuya）

岡山大学・自然科学研究科・講師

研究者番号：００３３６９１８

交付決定額（研究期間全体）：（直接経費）　　3,600,000円

研究成果の概要（和文）：電子透かしの透かし情報として二元線形符号のReed-Muller符号と拡大BCH符号の最小重み符号語だけを透かし情報として用い，かつ復号法の復号失敗を積極的に用いることで，透かし情報の取り出しにおける誤判定の確率を低減する手法を提案し，コンピュータシミュレーションにより有効性を確認した。
また，近年応用が進んでいる軟値入出力復号法において，浮動小数点数の加減算における量子化誤差の透かしの検出率への影響が実用上無視できることを確認した。
これらの符号と復号法を用いることで，電子透かしにおける冤罪の発生の抑制に効果があることを確認した。

研究成果の概要（英文）：A method which uses a set of the minimum weight codewords of Reed-Muller codes and extended BCH codes as an embedded information for digital watermark system is proposed. By using cases of decoding failure of decoding algorithms, the probability of erroneous detection can be reduced. The effectiveness of the proposed method is assured by computer simulations.
In addition, effects of quantization errors in the floating number operations in soft-in/soft-out decoding algorithms is evaluated by simulations. The simulation results show that effects are negligible for the digital watermarks. By using the proposed methods, the digital watermark systems which have small erroneous detection probability can be implemented.

研究分野：　符号理論

キーワード：　電子透かし　誤検出　線形符号　復号失敗　量子化誤差

１。研究開始当初の背景

電子透かしシステムにおいて誤り訂正符号を応用することで検出誤りの確率を低減できるが，その確率を非常に小さく抑えることは簡単ではない。誤検出確率の小さい手法を開発することで，デジタルコンテンツの不正使用に関する冤罪の発生を避けることが有用であると考えられるため，そのような方式の開発が求められている。

２。研究の目的

電子透かしシステムの透かし情報として，二元線形符号の最小重み符号語を用いることで，デジタルコンテンツへの透かし情報の埋め込みひずみの発生を抑えつつ，誤検出確率の低減の実現を目的とする。また，用いる軟判定復号法において，復号失敗を積極的に用いることでも誤検出の発生確率の低減を目的とする。

復号法の実装における誤り制御性能の評価を通して，電子透かしに適した符号と復号法の明確化も目的とする。

３。研究の方法

二元線形符号の中で，特に構造に関する研究が進んでいる Reed-Muller 符号と拡大 BCH 符号に関して，最小重み符号語の効率的な生成を行い，また誤り制御性能に優れた軟判定復号法のアルゴリズムを提案し，コンピュータシミュレーションにより，電子透かしに応用した場合の優れた誤り制御性能を確認する。長い符号長において，考案した復号法の実装を進めるとともに，画像の電子透かしシステムでの実験を行い，透かし情報の誤り率を取得する。特に，透かし情報の誤検出の確率を下げるために，復号失敗を生じる形式の復号法を複数調査し，得られる性能を調査する。用いる手法によって，透かし情報の正検出確率と誤検出確率がどのような関係になるかを明らかにする。

また，近年注目を集めている，軟値出力復号法を電子透かしに応用した場合の誤り制御性能に関してもコンピュータシミュレーションによる評価を行い，特に，実装面で，浮動小数点数の演算における量子化誤差に関する調査を行い，実用上，害にならないことを確認する。

４。研究成果

①電子透かしの透かし情報に用いる二元系列として，二元線形符号の符号語を用いることで，デジタルコンテンツの改変などの攻撃に対する耐性を持たせることができるが，透かしの埋め込みにおけるコンテンツの品質が，符号語のハミング重みの影響を受ける方式の場合，小さな重みの符号語だけを用いることで，コンテンツの品質の劣化を小さく抑えることができる。通常，誤り訂正符号の復号法は，全符号語の中で最尤な符号語を探索することを目的とするが，最小重みの符号語以外が埋め込まれていないことが明らかな場合，最小重みの符号語の中で最尤な符号語を効率的に探索する手法が有効である。

そこで，軟値受信系列に対して，一定の重みの二元系列を，その尤度の降順に逐次生成可能な再帰的な手法 Recursive Specific Weight Vector Generator(RSWVG)を考案し，AWGN通信路を想定した実験にて性能を評価した。長さ64で重み8のベクトルを生成する場合の加算回数と比較回数の結果を表1に示す。

表1 長さ64で重み8のベクトルを生成コスト

ベクトル本数	加算回数	比較回数
1	383	617
2	396	654
3	402	672
10	432	763
100	631	1672
1000	1960	10877
10000	12790	116001

また，RSWVGによって生成される一定の重みの二元系列に線形符号のパリティ検査を組み合わせることで，一定の重みの符号語の中で最尤な符号語を効率的に探索できる手法を考案し，(64,51,6)拡大BCH符号に対して，最小重み6と，その次に小さい重み8の符号語の探索手続を実装し，AWGN通信路を想定した実験にて性能を評価した。表2，3に結果を示す。

表2 (64.51.6)拡大BCH符号の最尤最小重み符号語の生成コスト

Eb/N0[dB]	0	2	4	6
ベクトル本数	3471	3493	3288	3265
加算回数	4642	4740	4604	4652
比較回数	36757	3793	35612	35627

拡大BCH符号の符号語の重み制御は簡単ではないことが知られており，一定の重みの符号語の探索手法の効率化により，長い符号長での実用的な復号法を実現できるため，電子透かしの攻撃耐性の強化が可能となった。

また，誤り制御性能が優れた復号法として知られている軟値出力型復号法を電子透かしに応用することも模索するため，軟値出力型復号法をブロックターボ復号法に適用する場合の，軟値出力に関する考察をし，復号法の効率化に関する検討をした。

表3 (64.51.6)拡大BCH符号の最尤の重み8の符号語の生成コスト

Eb/N0[dB]	0	2	4	6
ベクトル本数	4087	4003	3885	3892
加算回数	5639	5602	5565	5614
比較回数	46429	45748	44709	44830

②電子透かしの透かし情報に用いる二元系列として，二元線形符号の符号語を用いることで，デジタルコンテンツの改変などの攻撃に対する耐性を持たせることができるが，高い攻撃耐性を実現するためには，最小距離の大きい符号を用いて，誤り率を低く抑えることができる復号法を用いる必要がある。二元線形符号のReed-Muller符号は，多数決論理に基づく復号法で限界距離t(tは最小距離-1を2で割って少数を切り捨てたもの)復号法が容易に実装可能であり，限界距離t復号法を複数回用いる軟判定復号法は復号失敗を生じえる軟判定復号法として電子透かしに有用である。

そこで，限界距離t+2復号法に対して，符号の重み構造を用いて平均的な計算量を削減する手法と，Chase2復号法に関して，検査和の計算結果を再利用することと，無駄な計算を省略することで，平均的な計算量を削減する手法を考案して，AWGN通信路においてシミュレーションにより，有効性を確認した。(64,42,8)RM符号の限界距離t+2復号法の，既存法に対する提案法の平均計算量の相対値を表4に示す。

表4 限界距離t+2復号法の相対的計算量

Eb/N0[dB]	0	2	4	6
計算量	0.509	0.477	0.275	0.065

これにより，電子透かしにおいて正検出率を高くしつつ，誤検出を検出失敗と扱う目的で使用するための，復号誤りを生じえる軟判定復号法の選択の幅を広げることができた。電子透かしの透かし情報として二元線形符号の符号語を用いる場合，やみくもに復号語を生成しては，誤検出となる場合があるため，復号語のメトリックによっては，復号失敗とした方が，誤検出の確率を低減できると期待できる。平成 27 年度には，複数の軟判定復号法の計算量を削減する手法を考案し，ソフトウエア実装により有効性を確認し，正検出率と誤検出率のトレードオフ関係の中で，選択肢を広げることができた。

③拡大BCH符号の2次元積符号に対して，軟値入出力復号法を要素復号として用いるブロックターボ復号法により，高い誤り制御性能が得られることを確認した。一方で，軟値入出力復号法の復号器の実装において，軟値を浮動小数点数として扱う場合に，加減算における量子化誤差の誤り率への影響を調査し，量子化誤差による誤り率の悪化が実用上無視できることを確認した。図1に(64,16,16)積符号の4ステージブロックターボ復号法のビット誤り率(BER)を示す。

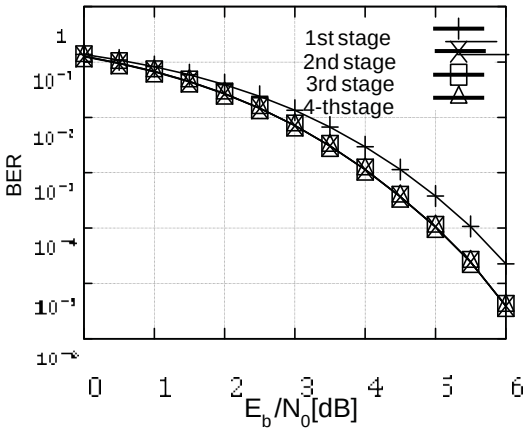

図1 ブロックターボ復号法の誤り率

また，各ステージにおいて軟値出力が0になるシンボル位置の発生する数を表5に示す。SN比が4[dB]付近では問題にならないことが確認できる。

表5 軟値が0となるシンボル位置の数

E_b/N_0	stage			
[dB]	1	2	3	4
0	0	1056	232	176
1	0	376	64	64
2	0	152	28	0
3	0	24	16	16
4	0	0	0	0

符号長64から1024程度の二元線形符号の符号語を透かこれらの符号と復号法を用いることで，埋め込まれた透かし情報を攻撃から守り，また，無理な復号でなく，復号誤りを積極的に用いることにより，電子透かしにおける冤罪の発生の抑制に効果があることを確認した。

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）

学会発表(計 3 件)
[1] S。 Fujimoto, T。 Kusaka and S。 Ueda, "A Study on Soft-out of Soft-in/Soft-out Decoding Algorithms for Binary Linear Codes," Proc. ISITA2016, pp.305-309, Monterey, USA, Nov. 1, 2016. (査読有)
[2] 田邉義直, 日下卓也, " Reed-Muller 符号の限界距離 t+2 復号法に関する研究," 平成 27 年度 電気・情報関連学会中国支部第 66 回連合大会, no. 18-6, 2015年10月17日.(査読無)
[3] T。 Kusaka, " Introduction of a Recursive Method for Specific Weight Binary Vector Generation in Decreasing Order of its Reliability Measure," Proc。 of ISITA2014, pp。 534-538, Melbourne, Australia, Oct. 29, 2014. (査読有)

６。研究組織
(1)研究代表者
日下　卓也(KUSAKA, Takuya)
岡山大学・大学院自然科学研究科・講師
研究者番号: 00336918