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[††]

コンテンツに埋め込まれた電子透かし情報は微弱であるうえ，制作，流通の過程および不正者の意図による様々なメディア処理が加えられるため，その検出では誤りが生じやすい．ところが，一般に電子透かしでは多くのビット数を埋め込むことができないので，誤りを訂正する冗長な検査ビットは多くとれない．そのため，誤り訂正符号を用いた従来の電子透かし検出方式では，ビット誤り数が訂正限界を超え，情報を復号できないことが多かった．そこで本論文では，訂正限界以上の誤り訂正を行う軟判定復号法を取り上げ，電子透かし検出への適用を提案する．ただし，現実の電子透かし検出では，軟判定復号法の前提となる各ビットの信頼度を正確に算出できない場合が多いので，軟判定復号法を拡張し，各ビットの信頼度の代わりに，同じ情報が何回復号されたかという復号回数に基づく方式を提案する．実情報 64 ビット，訂正限界 10 ビットの $(127, 64, 21)$ BCH 符号を用いて提案方式を実装し，提案方式の検出能力は復号誤り確率 10^{-30} 以下を達成することを証明する．さらに，実際のサンプル画像に JPEG 圧縮に施して誤りを発生させることで誤り訂正能力を実測し，従来 10 ビットまでの誤りしか訂正できなかった検出能力が平均 13.92 ビットにまで向上することを明らかにする．

An Improvement of Error Correction Coding for Digital Watermarking

Yasuhiro Fujii,[†] Isao Echizen,[†] Takaaki Yamada,[†]
Satoru Tezuka[†] and Hiroshi Yoshiura[††]

Error correction coding is necessary for detection of digital watermarking because some bits of information embedded into digital contents are apt to be eliminated by media processes. The number of error bits, however, exceeds the error correction bound because large number of bits, especially check bits for correcting, can not be embedded into digital contents. This paper proposes a detection method of watermarking with higher bound and lower probability of error decoding by making use of the number of times that each information is decoded by the soft-decoding. Experimental evaluation showed that the error correction bound of the proposed method was improved to be 13.92 bits at average and the probability of error decoding achieved below 10^{-30} for $(127, 64, 21)$ BCH code with 64 bits information and 10 bits bound.

1. はじめに

絵画や音楽，映画などのコンテンツをデジタル化して配信するコンテンツビジネスがさかんになっている．デジタルコンテンツは取扱いが容易で使用による劣化がない反面，不正コピーにより著作権が侵害されやすいという問題がある．そのため，コンテンツ所有者や配布先などの情報をコンテンツ自体に埋め込むことで著作権の保護を可能にする電子透かしの技術が注目されている[1),2)]．

電子透かしでは，コンテンツの価値を損なわないという制約により，元のコンテンツの値に比べて微弱な信号を埋め込む．たとえば，静止画コンテンツの輝度を変更する電子透かし方式では，透かしの強度を輝度の値域の 1/100 程度にする必要があることが知られている[3)]．また，情報が埋め込まれたコンテンツには，制作や流通の過程で様々なメディア処理が加えられ，さらに，不正者によって意図的な処理が施される場合もある．これらの処理の後にコンテンツから微弱な電子透かし信号を正確に検出することは容易ではない．しかしながら，電子透かし情報は著作権の主張，不正者の特定，機器の制御など，重要な役割を果たすので，検出誤りは重大な問題を引き起こす可能性がある．そ

† 株式会社日立製作所システム開発研究所
Systems Development Laboratory, Hitachi, Ltd.
†† 電気通信大学電気通信学部
Department of Electro-Communications, The University of Electro-Communications

のため，電子透かし検出においては，誤りの発生を防止するだけではなく，万一検出誤りが生じた場合でも，それを検知し，正しく復元する技術が重要となる．

透かし情報復元の従来方式として，誤り訂正符号を用いる方法が知られている[1),4)~10)]．ただし，電子透かしにおいてはコンテンツ価値を維持するために，誤り訂正のための冗長な検査ビット列を多く埋め込むことができず，その分訂正能力が低くなってしまう．そのため，誤りビット数が誤り訂正符号の訂正能力を超過するという問題がしばしば起こる．このとき，従来の誤り訂正符号を用いた検出方式では，いっさいの情報が検出できなくなることがある．

誤り訂正符号の訂正限界の問題は，符号理論一般の重要な問題であり，これまでに訂正限界を拡張する様々な方式が提案されている．その代表的な方式として，軟判定復号法がある[22)~28)]．軟判定復号法は，信頼度の低いビットを消失と見なし，すべての消失ビットに 0 または 1 を割り当てた組合せについて誤り訂正を繰り返し行い，復号できた情報を訂正結果とする復号方法である．

そこでまず，本論文では，消失の概念が電子透かし検出に適することを明らかにして，軟判定復号法を用いた電子透かし検出方式を提案する．

しかし，電子透かしにおいては，コンテンツに様々なメディア処理が加えられた結果，消失ビットの選択に誤りが生じる可能性がある．また，対象となるコンテンツが十分な大きさを持たない，もしくは二値画像など特殊なコンテンツであるといった理由によって，消失ビットの正確な選択自体が困難である場合もある．このような場合，本来消失として扱うべきビットを正しいビットとして誤り訂正を繰り返してしまい，本来埋め込まれた情報と異なる情報を誤って復号してしまう．

そこで次に本論文では，誤り訂正を繰り返したことである同一の情報を何回も復号できた場合，その復号回数に着目することで軟判定復号法の高い検出率を保ったまま復号誤りを回避できる，新しい電子透かし検出方法を提案する．透かし検出実験を行い，提案方式の効果を明らかにする．

本論文は以下のように構成される．2 章で従来の電子透かしの検出方式とその問題点についてまとめる．3 章で軟判定復号法を用いた電子透かし検出方式を提案する．4 章で，復号回数を用いて復号誤りを防止する新しい電子透かし検出方式を提案する．5 章で静止画像を用いて提案方式を評価し，提案方式が従来の検出方式と比べて電子透かし検出に適していることを明らかにする．6 章で本論文の内容をまとめる．

2. 従来の電子透かし検出方式とその問題点

1 章で述べたように，電子透かしの信号が元のコンテンツの値に比べて微弱であること，および電子透かしを埋め込んだコンテンツに様々なメディア処理が施されることから，電子透かし情報の正確な検出は容易ではない．そのため，電子透かしの検出誤りを防止するために，正規分布などの確率モデルを用いて誤り確率を求める方法[12)~16)]，多数決などの冗長性を用いる方法[17)]，人間の視覚モデルを用いてコンテンツの劣化を防止しながら透かしを強く埋め込むことで，検出誤りを防止する方法[18)~20)] などが提案，利用されている．

しかし，電子透かしの検出に関わる上記の厳しい条件のため，これらの方法を用いたとしても，検出誤りを完全に防止できない場合が多い．そのため，検出が誤った場合でも，これから正しい情報を復元することが重要となる．

誤りを復元するような電子透かし検出方式として，誤り訂正符号を用いる方法が提案されている[1),4)~10)]．これらの方式は，いずれも本来埋め込みたい情報に検査ビット列を余分に付加することで検出情報の訂正を行う方式である．誤り訂正符号の訂正能力は検査ビット列を多くとるほど向上するため[29),30)]，もし誤りが生じやすい環境下にあるのならば，その分検査ビット列を多くとることで情報を正確に検出できる．

しかし，電子透かしにおいては，コンテンツ価値維持の観点から，検査ビット列，すなわち訂正可能なビット数（訂正限界）を多くとることができないという固有の問題がある．

このことを明らかにするために，透かし情報としてコンテンツの識別番号の表現に必要とされる 64 ビットを用いる例について考察する[21)]．文献 17) では，電子透かしに適した誤り訂正符号として，実情報と同程度の大きさの検査ビット列を持つ BCH 符号を採用して透かし検出実験を行い，その有用性を実証している．この結果をもとにすると，実情報 64 ビットと同程度の大きさの検査ビット列を持つ（127, 64, 21）BCH 符号が，64 ビットの電子透かし情報の検出にとって適していると考えられる．この符号では訂正限界 10 ビットまでの誤りを訂正できるが，実情報とほぼ同量の検査ビット列を用いたことでコンテンツに埋め込む情報は 2 倍に増大してしまう．

ところが，5.3 節で明らかにするように，この符号を用いて訂正を試みたとしても，静止画の JPEG 圧

縮などによって 10 ビットを超える誤りが発生することが多い．このとき，実情報の 2 倍の透かし情報を埋め込んだにもかかわらず，通常の誤り訂正符号を用いるだけでは，透かし情報がいっさい検出できなくなってしまう．

訂正限界を向上させることは符号理論一般における重要な研究課題であり，これまで様々な方式が提案されてきた．その代表的な手法として，各ビットの信頼度を援用することで訂正限界を超えた復号を行う軟判定復号法が知られている[22)~28)]．その基本的な概念は，信頼度が低いビットをビット値が判断できない消失として扱い，すべての消失ビットにあらゆる組合せで 0, 1 を割り当て何回も誤り訂正を繰り返すことで，訂正が成功した組合せを訂正結果とする復号方法である．軟判定復号法によって訂正限界が 1〜2 割程度向上することが知られている[29),30)]．

そこでまず本論文では，軟判定復号法を用いた電子透かし検出方式を提案し，その方式によって訂正限界が向上することを示す．

3. 軟判定復号法を用いた検出方式

3.1 軟判定復号法の電子透かしへの適合性

一般に，電子透かし検出時においては，透かし情報の各ビットとともに，そのビットの信頼性も評価でき，消失の概念を導入することが可能である．このことを示すため，輝度といったコンテンツの特徴量を微妙に変更することで情報を埋め込む例について考察する[12),13)]．この方式では，コンテンツから評価値を計算し，しきい値との大小関係でビット値を割り当てることで，埋め込まれた透かし情報を検出する．すなわち，評価値を z，しきい値を $\tau > 0$ とかくと，

$$b = \begin{cases} 0 & (\tau < z) \\ \text{未検出} & (-\tau \le z \le \tau) \\ 1 & (z < -\tau) \end{cases} \qquad (1)$$

とビット値 b を判定できる．

このとき，$-\tau \le z \le \tau$ に対応するビットを消失と見なすことができ，かつ，しきい値 τ を調節することで，消失ビットの個数を変更することも可能となる．

この方式は電子透かしにおける典型的な手法であり，他の方式でも同様に，情報ビットは評価値としきい値との大小関係で割り当てられるため，式 (1) のようにしきい値を調節することで消失ビットを導入できる．たとえば，多数決を用いる検出方法[17)]では，ビット 0 の個数 N_0 とビット 1 の個数 N_1 を算出し，$N_0 > N_1$ のときビット 0 を，$N_0 < N_1$ のときビット 1 を割り当てるが，このとき評価値を $z = N_0 - N_1$ とすることで，式 (1) でビット値を判定することができる．

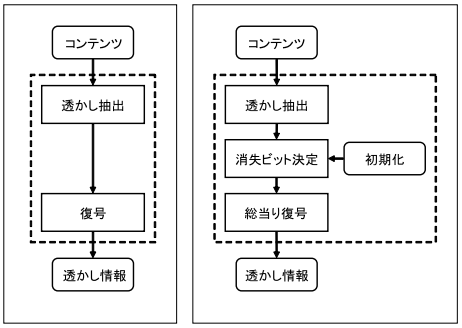


図 1 従来の検出方式と軟判定復号法を用いた検出方式の処理手順
Fig. 1 Detection processes of previous method and primitive method based on soft-decoding.

3.2 基本方式

上記のように，電子透かし検出では，しきい値との大小関係から消失ビットも導入できる．そこで本章では，この電子透かし特有の事実に着目して，軟判定復号法を用いた電子透かし検出方式を提案する．

誤り訂正符号を用いた電子透かしの典型例として，以下，符号長 n，情報ビット長 k，最小距離 d の二元 (n, k, d) 線形符号を埋め込む場合について考察する．透かし情報として有効なのは k ビットであり，残りの $n-k$ ビットは検査ビットとなる．この符号の訂正限界は $t = \lfloor (d-1)/2 \rfloor$ で与えられる．

軟判定復号法には様々な方式が知られているが，その代表的手法であり，他の方式のベースとなっているチェイス復号法を採用する[23)]．この復号法を用いた電子透かし検出方式は次の手順からなる（**図 1**）．

Step 1 （透かし抽出）
コンテンツから透かしを抽出して評価値を算出する．

Step 2 （消失ビット決定）
消失ビット数 N をあらかじめ決めておく．式 (1) に従いしきい値 τ を調節することで N 個の消失ビットとビット 0，1 を割り当てる．

Step 3 （総当たり復号）
取り出した N 個の消失ビットそれぞれに 0，1 を割り当てて得られる 2^N 個のビット列に誤り訂正を施す．復号できたビット列を出力する．

軟判定復号法を電子透かし検出に用い，消失ビットに 0，1 を割り当て誤り訂正を繰り返すことで，検出率が 1〜2 割程度向上することが期待できる[29),30)]．また，この検出方式は，コンテンツの種類や電子透かし方式の詳細によらないため，検出能力を向上させる汎

用的な方法となる．

3.3 基本方式の問題点

上記提案した基本方式では，消失ビットを導入することで訂正能力の改善を試みた．しかし，電子透かし検出においては，以下の理由から消失ビットの選択に誤差が生じる可能性がある．

(1) コンテンツの劣化による影響
(2) 信頼度算出のためのモデルが不成立
(3) もともと信頼度の厳密な算出が不可能

(1) の根拠を示すため，3.1 節でとりあげたコンテンツの特徴量を微小に変更することで情報を埋め込む方式[12),13)]について考察する．埋め込まれた情報は，式 (1) に従ってコンテンツから算出した評価値 z としきい値 τ との大小関係を調べることで検出できる．ところが，透かし入り画像にたとえば JPEG 圧縮が施された場合，画像上にブロック歪みが発生し，このノイズの影響を受けて，もともと $-\tau \leq z \leq \tau$ にあった評価値が $z < -\tau$ もしくは $\tau < z$ にずれる場合がある．このとき，本来消失とすべきビットが正しいビットと判断され，消失ビットの選択に誤りが生じてしまう．5.3 節で実験を行いこれを実証する（図 10〜図 13 参照）．

(2) の根拠を示すため，信頼度算出のモデルの例として，2 章であげた正規分布といった確率モデルを用いて各ビットの信頼度を求める方法[12)〜16)]をとりあげて説明する．この方式は，中心極限定理をもとにコンテンツから算出した評価値を正規分布にあてはめ，その平均や分散を評価することで，式 (1) 以上に各ビットの信頼度を精密に算出する方法である．この方式によって，JPEG などのメディア処理が施されても信頼度を正しく算出できる可能性が高まる．しかしながら，実際に評価値が正規分布に従うには，同一の透かし情報を 4000 回以上重畳しなければならないことが知られている[15),16)]．それゆえ，たとえば 8×8 の単位ブロックをコンテンツのいたるところに埋め込み 64 ビットの透かし情報を挿入した場合には，正規分布をもとにビットの信頼度を正しく算出するためには，最低限 500×500 程度の大きさのコンテンツが要求される．したがって，これよりも小さいコンテンツに対しては，信頼度算出の前提とした正規分布からの誤差が大きくなり，消失ビットを正しく選択できなくなるおそれがある．

(3) についても同様である．正規分布が成立するコンテンツは自然画像など限られており，たとえば二値白黒画像に対してはまだ適切な確率モデルが知られていない．このようなコンテンツに対しては信頼度を式 (1) 以上に精密に算出することがもともと不可能であり，誤差が生じやすい．その結果，消失ビットの選択を誤る可能性がある．

3.2 節で提案した基本方式の場合，消失ビットの選別を誤っているにもかかわらず誤り訂正を繰り返すと，本来埋め込まれた情報と異なる情報を復号する可能性が増大してしまう．したがって，基本方式を，コンテンツの劣化度合いや大きさ，種類に依存しない，汎用的な検出方式とするためには，各ビットの信頼度を精密に計算できない場合の対処方法が要求される．

3.4 信頼度を用いない従来の復号方式とその問題点

基本方式の問題点は，訂正限界向上のために各ビットの信頼度が要求されるところにある．信頼度を精密に計算できない場合にも訂正限界を向上させる復号方式として，以下が知られている．

(1) 誤り位置を求めるアルゴリズムのステップ数を増やすことで，訂正限界を超える誤りを訂正する方式[31),32)]．
(2) 誤り訂正処理を，二次元平面内の複数の点を通る曲線を求める問題に帰着させることで，候補となる複数の符号語のすべてを多項式時間で求めるリスト復号法[33),34)]．

しかし，これらの復号方式には以下の問題があるために，電子透かし検出には適さない．

- 訂正限界は復号結果の唯一性を保障するために設けられた指標であるため，訂正限界以上の誤りを訂正した場合，複数の符号語が訂正結果の候補となる場合がある．しかし (1) は通常の誤り訂正のステップを増やすことで訂正限界を向上させる方式であるため，通常の誤り訂正同様，符号語が複数あるにもかかわらずただ 1 つの符号語しか復号することができない．よってこの方式では，通常の誤り訂正と比較して，本来と異なる符号語を得る復号誤りの可能性が高くなる．1 章で述べたように，電子透かしにおいては復号誤りを防止することが重要な要件であるため，この復号方式をそのまま電子透かし検出に適用することはできない．
- (2) のリスト復号法は，訂正の候補となる複数の符号語すべてを多項式時間で求めることができる復号法である．しかし，複数の符号語が得られた場合，これらの中から最も確からしい透かし情報をただ 1 つ選別するためには，結局各ビットの信頼度を用いて判断するほか方法がない．したがって，信頼度の精密な計算が困難である場合，リスト復号法を用いたとしても，複数の情報から誤った情報を選んでしまうことによる復号誤りの可能

性は回避できない．

- 符号長を n，通常の誤り訂正の訂正限界 d とした場合，(2) のリスト復号法によって，

$$n - \sqrt{n(n-d)} \tag{2}$$

以下の誤りを訂正できることが知られている[34]．式 (2) はリスト復号法によって拡張された訂正限界が n に比例することを意味するが，コンテンツ価値維持の観点から，電子透かしには符号長 n を大きくとれないという固有の問題があるため，電子透かし検出においてはこの拡張の効果は薄いと考えられる．たとえば，2 章であげた $(127, 64, 21)$ BCH 符号について式 (2) を評価すると 10.9741 となり，元の訂正限界 10 ビットと比較して拡張の効果が薄いことが分かる．

以上のように，従来知られている復号方法では，電子透かし検出の固有の条件により効果が薄く，また，復号誤りを防止することも困難である．そこで本論文では，次章で基本方式を改良し，各ビットの信頼度だけではなく，誤り訂正を繰り返す間に復号できた情報の復号できた回数に着目することで，復号誤りを回避しつつ訂正限界を改善できる，新しい誤り訂正方式を提案する．

4. 復号回数に着目した改良方式

4.1 復号回数の特徴

前述の基本方式では，N 個の消失ビットそれぞれに 0，1 を割り当てて 2^N 個のビット列を用意し，それぞれに誤り訂正を施すことで情報の復号を試みた．実際には，**図 2** に示すように，2^N 回誤り訂正を施した結果，本来埋め込まれた情報だけが復号できるとは限らず，それと異なる情報が復号される可能性がある．ところが，誤り訂正だけでは，復号情報のどれが本来埋め込まれた情報であるか判断できない．

2^N 回の誤り訂正によって L 個の情報 $I_1, I_2, \ldots, I_L$ が復号できたとする．2^N 個の訂正前のビット列のうち，誤り訂正によって情報 I_k に復号されるビット列の個数 N_k を I_k の復号回数とよぶ（$k = 1, \ldots, L$）．

復号に失敗した回数を N_E としたとき，すべての復号回数の和に対して

$$\sum_{r=1}^{L} N_r + N_E = 2^N \tag{3}$$

が成立するのは明らかである．実際にはもっと強く，復号回数に関して以下の補題が成り立つことが証明できる．

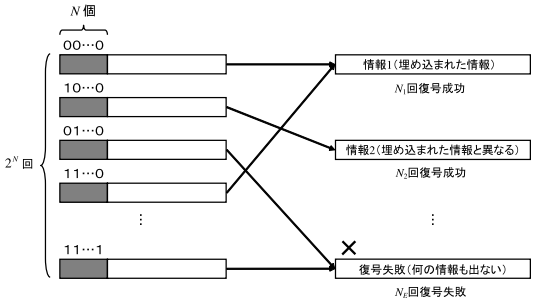


図 2 誤り訂正を繰り返して復号できた各情報の復号回数
どの情報が正しいかは判断できない．

Fig. 2 The number of times that each information is decoded. It is indeterminable which information is correct.

補題 消失として 0，1 を割り当てるビットの個数を N とする．N 個のビットそれぞれに 0，1 を割り当てて 2^N 個のビット列を求め，それぞれに対して誤り訂正を施す．2^N 回の誤り訂正の間に L 個の情報 $I_1, \ldots, I_L$ が復号できたとき，各情報 I_k の復号回数 N_k は，二項係数の和

$$\begin{aligned}
&\sum_{i=0}^{0} {}_N\mathrm{C}_i = 1 \\
&\sum_{i=0}^{1} {}_N\mathrm{C}_i = N + 1 \\
&\qquad\vdots \\
&\sum_{i=0}^{t+N-m} {}_N\mathrm{C}_i = \frac{N!}{(t+N-m)!(m-t)!} \\
&\qquad\qquad + \cdots + N + 1
\end{aligned} \tag{4}$$

のいずれかで与えられる．ここで，t は訂正限界，m は実際に誤っているビットの個数である．

証明は後の 4.3.2 項で与える．この補題より，2^N 回の総当たり復号によってある情報が復号できた場合，それぞれの復号情報に対して，その復号回数は必ず 1 か，$N + 1$ 以上になることが分かる．

一方，本来の情報と異なる偽の情報はランダムに散らばっており，同一の偽の情報を $N + 1$ 回以上復号できる確率は，N が大きくなるにつれ小さくなると考えられる．このような予想に基づいて，本論文では，$N + 1$ 回以上復号できた情報を正規の情報と見なすことで復号誤りの回避を試みる，新しい電子透かしの検出方式を提案する．後の 4.4 節で，実際に BCH 符号を用いて復号誤り確率を計算し，これが低減することを証明する．

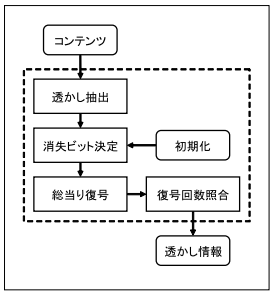


図 3 改良方式の処理手順
Fig. 3 Detection process of improved method.

4.2 改良方式

3.2 節で提案した電子透かし検出の基本方式の改良方式として，以下を提案する（**図 3**）．

Step 1（透かし抽出）
コンテンツから透かしを抽出して評価値を算出する．

Step 2（消失ビット決定）
消失ビット数 N をあらかじめ決めておく．式 (1) に従いしきい値 τ を調節することで N 個の消失ビットを取り出し，ほかにビット 0，1 を割り当てる．

Step 3（総当たり復号）
取り出した N 個の消失ビットそれぞれに 0，1 を割り当てて得られる 2^N 個のビット列に誤り訂正を施す．復号できたビット列それぞれに対してその復号回数を求める．

Step 4（復号回数照合）
$N+1$ 回以上復号に成功した復号ビット列のうち最も復号回数が大きいビット列を透かし情報として出力する．

この改良方式は Step 4 を除いて 3.2 節であげた基本方式と同様であり，コンテンツの種類や電子透かし方式の詳細によらず，検出能力を改善することができる．

なお，これら提案方式のもととなったチェイス復号法には，計算量が N に関して指数関数的に増大するという問題があるが，計算量削減の観点からこれまで様々な研究がなされており[25)~28)]，提案方式の計算量もこれらの改良方式を援用することで削減できると考えられる．本論文では，復号回数に着目した新しい電子透かし検出方式を提案することを優先し，計算量削減については今後の課題とする．

4.3 改良方式の特性

本来埋め込まれた透かし情報を正しく検出できる正復号確率と，それと異なる情報を誤って復号する復号誤り確率について解析し，改良方式が復号誤りを回避できることを明らかにする．ただし，3.3 節で述べたように，電子透かし検出においては，各ビットの信頼度を厳密に計算して N 個の消失ビットを正確に選択することは容易ではない．そこで，以下の解析では，まず最悪の場合を想定し，各ビットの信頼度の算出が正しくなく，消失ビットがまったくランダムに選択されると仮定して，正復号確率および訂正限界の最悪値を導出する．

4.3.1 準　　備

以下，論理を明確にするため，二元線形符号に限定して解析する．一般の q 元線形符号に関しても同様である．

二項係数 ${}_i\mathrm{C}_j$ を，

$$ {}_i\mathrm{C}_j = \begin{cases} \dfrac{i!}{j!(i-j)!} & (i \geq j \geq 0 \text{ が整数}) \\ 0 & (\text{それ以外}) \end{cases} \tag{5} $$

と定める．また，$\delta_{i,j}$ を，

$$ \delta_{i,j} = \begin{cases} 1 & (i=j) \\ 0 & (i \neq j) \end{cases} \tag{6} $$

と定める．

ビット列内の誤っているビットの総数を重みという．情報ビットに誤り訂正のための検査ビットを付加したビット列を符号語という．

改良方式の正復号確率を，「2^N 回の誤り訂正によって同一の情報を $N+1$ 回以上復号し，かつその情報が本来埋め込まれた情報に一致する確率」として定義する．

また，改良方式の復号誤り確率を，「2^N 回の誤り訂正によって同一の情報を $N+1$ 回以上復号し，かつその情報が本来埋め込まれた情報に一致しない確率」として定義する．

まず，重み u のビット列が誤り訂正によって重み v のある符号語に訂正される確率 $p_{u,v}$ について考察する．付録の証明より，重み v の符号語が存在するとき，確率 $p_{u,v}$ は，

$$ p_{u,v} = \frac{1}{{}_n\mathrm{C}_v} \sum_{s=0}^{t} {}_v\mathrm{C}_x \cdot {}_{n-v}\mathrm{C}_{s-x}, \tag{7} $$

と求まる．また，存在しない場合は $p_{u,v}=0$ となる．ここで $x=(v-u+s)/2$ である．さらに，$0<v<d$ のときには，符号語が存在しないため，式 (7) は簡単にまとめられて，

$$ p_{u,v} = \begin{cases} \delta_{v,0} & (0 \leq u \leq t) \\ 0 & (t < u \leq n) \end{cases} \tag{8} $$

が成立する．さらに，符号語をビット反転したものも符号語になる場合には，重み分布は $\lfloor n/2 \rfloor$ を中心に対称となり[35]，重み 0 の符号語をビット反転することで重み n が得られるため，$n-d<v<n$ のときも同様に，

$$p_{u,v}=\begin{cases}\delta_{v,n} & (n-t\le u\le n)\\ 0 & (0\le u<n-t)\end{cases} \tag{9}$$

が成立する．

次に，N 個の消失ビットを除いたビット列の重みを u とする．これに 2^N 回の総当たり復号を施したとき，重み v の同一の符号語を r 回復号できる確率を $P_{u,v}(r)$ とかく．これは以下で与えられる．

$$P_{u,v}(r)=\sum_{k_0+\cdots+k_N=r}\prod_{i=0}^{N}{}_{R_i}\mathrm{C}_{k_i} \times {p_{u+i,v}}^{k_i}(1-p_{u+i,v})^{R_i-k_i}. \tag{10}$$

ここで

$$R_i={}_N\mathrm{C}_i \tag{11}$$

であり，各 k_i は $k_i=0,\ldots,R_i$ について和をとる．付録でこれを証明する．

最後に，N 個の消失ビットのうち，実際に誤っているビットが M 個含まれる確率について考察する．n 個のビットから N 個とりだす組合せの数が ${}_n\mathrm{C}_N$，m 個の誤りビットから M 個取り出す組合せの数が ${}_m\mathrm{C}_M\cdot{}_{n-m}\mathrm{C}_{N-M}$ だから，求める確率を $\alpha_m(M)$ とかくと，

$$\alpha_m(M)=\frac{{}_m\mathrm{C}_M\cdot{}_{n-m}\mathrm{C}_{N-M}}{{}_n\mathrm{C}_N} \tag{12}$$

が成立する．この $\alpha_m(M)$ は本来ビットの信頼度に依存する量であるが，本節では消失ビットがまったくランダムに選択されると仮定しているため，組合せの数だけに依存することに注意する．

以上の準備のもと，改良方式の正復号確率と復号誤り確率を計算する．

4.3.2 正復号確率

以下，n ビット中誤っているビットの個数を m とおき，改良方式の正復号確率を $P_C(m)$，本来埋め込まれた情報を r 回復号する確率を $P_C(m,r)$ とかく．まず，この $P_C(m,r)$ の計算を通じて，4.1 節であげた補題を証明する．

$P_C(m,r)$ は，$\alpha_m(M)$ に重み 0 の符号語が r 回復号できる確率 $P_{m-M,0}(r)$ を乗じて，M に関する和をとったものになる：

$$P_C(m,r)=\sum_{M=0}^{N}\alpha(M)P_{m-M,0}(r). \tag{13}$$

式 (8) を式 (10)，(13) に代入して整理すると次式が得られる．

$$P_C\left(m,\sum_{i=0}^{K}{}_N\mathrm{C}_i\right)=\alpha_m(m-t+K). \tag{14}$$

ただし $K=0,\ldots,t+N-m$ で，他の P_C は 0 である．式展開の詳細については付録で与える．ここで，式 (14) 以外の P_C は 0 であることに注意する．このことより，正しく復号できる回数は必ず

$$\sum_{i=0}^{K}{}_N\mathrm{C}_i \qquad (K=0,\ldots,t+N-m) \tag{15}$$

の形でかけることが明らかとなった．これより 4.1 節であげた補題が証明された．

また，式 (14) より $P_C(m)$ は，

$$P_C(m)=\sum_{M=m-t+1}^{N}\alpha_m(M) \tag{16}$$

と求められる．この式を用いれば，改良方式によって向上する訂正限界の期待値 $\langle t(N)\rangle$ は，

$$\langle t(N)\rangle=t+\sum_{m=t+1}^{n}P_C(m) \tag{17}$$

と計算できる．

ただしこれらの導出では，3.3 節で述べたように，消失ビットを全体の n ビットからランダムに取り出すと仮定している．そのため，実際の適用においては，正復号確率，訂正限界の期待値は，それぞれ式 (16)，(17) よりも高いと考えられる．これに関しては 5.3 節で実際に静止画像を用いて電子透かし検出実験を行い，実証する．

4.3.3 復号誤り確率

各 m について改良方式の復号誤り確率を $P_E(m)$ とかく．重み v を持つ符号語の個数を A_v とすると，$P_E(m)$ は以下のようにかける．

$$P_E(m)=\sum_{M=0}^{N}\alpha_m(M)\sum_{v=d}^{n}A_v \times\sum_{K=1}^{t+N-m}P_{m-M,v}\left(\sum_{i=0}^{K}{}_N\mathrm{C}_i\right). \tag{18}$$

これを厳密に評価することは困難であるため，代わりに復号誤り確率の上限を評価する．

式 (7) で与えた確率 $p_{u,v}$ の最大値を p とかく．式

(10) に現れる $p_{u,v}$ すべてを p で置き換えたとき，その分復号誤りが起こりやすくなるため，$P_{m-M,v}(r)$ は最大値を与える．定義より，これは確率 p で起こる事象を 2^N 回試行したとき r 回起こる確率にほかならないから，

$$P_{m-M,v}(r) \leq {}_{2^N}\mathrm{C}_r \cdot p^r (1-p)^{2^N-r} \qquad (19)$$

が成立する．

これは重み v に依存しないため，式 (18) において v に関する和を独立にとることが可能になる．重みの定義より $A_0 = 1$，$A_1 = \cdots = A_{d-1} = 0$ が成立するため，情報ビット長 k を用いて $\sum_{v=d}^{n} A_v = 2^k - 1$ となる．

また，$m - M > t$ のときに限り，誤りが t を超過して復号誤りが生じる．以上まとめると，

$$P_E(m) \leq \sum_{M=0}^{m-t-1} \alpha_m(M)(2^k - 1) \times \sum_{r=N+1}^{2^N} {}_{2^N}\mathrm{C}_r \cdot p^r (1-p)^{2^N-r} \qquad (20)$$

が得られる．

4.3.4 基本方式の特性

次の 4.4 節で改良方式と基本方式の特性を比較するために，基本方式の正復号確率 $P'_C(m)$ と復号誤り確率 $P'_E(m)$ についても厳密に解析する．

基本方式の正復号確率 $P'_C(m)$ は，式 (14) から容易に導出できて，

$$P'_C(m) = \sum_{M=m-t}^{N} \alpha_m(M) \qquad (21)$$

となる．

基本方式の復号誤り確率 $P'_E(m)$ は，重み d 以上の情報を 1 回でも復号する確率にほかならない．重み u のビット列から重み d 以上の符号語を 1 回以上復号する確率 P_u は，重み u のビット列を重み d 以上の符号語に訂正できない確率 $1 - \sum_{v=d}^{n} A_v p_{u,v}$ の余事象

$$P_u = 1 - \prod_{i=0}^{N} \left(1 - \sum_{v=d}^{n} A_v p_{u+i,v}\right)^{R_i} \qquad (22)$$

で計算できる．ここで R_i は式 (11) で与えられる．

これを用いて復号誤り確率 $P'_E(m)$ は，

$$P'_E(m) = \sum_{M=0}^{N} \alpha_m(M) P_{m-M} \qquad (23)$$

と求められる．

4.4 正復号確率，復号誤り確率の評価

4.4.1 （127,64,21）BCH 符号の評価

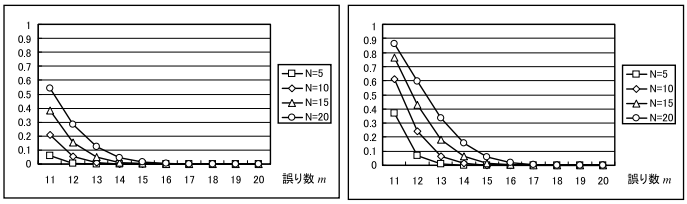
4.3 節の解析結果をもとに，具体的な符号について正復号確率および復号誤り確率を評価し，改良方式と基本方式とを比較する．

誤り訂正符号として，まず，これまで例としてあげてきた，符号長 $n = 127$，情報ビット長 $k = 64$，最小距離 $d = 21$ の（$127, 64, 21$）BCH 符号を採用する．この符号は訂正限界 $t = 10$ ビットの誤りを訂正できる．

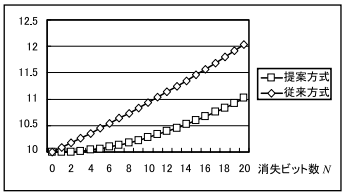
式 (16)，(21)，(17)，(20)，(23) から，改良方式および基本方式の，正復号確率，訂正限界の期待値，および復号誤り確率は**図 4** のように評価できる．なお，式 (23) を評価するには（$127, 64, 21$）BCH 符号の重み分布 $\{A_v\}$ が必要であるが，これに関しては文献 35) を参照した．

これらの結果より以下の結論が導かれる．

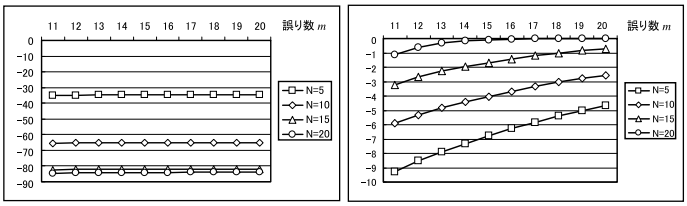
- 復号回数を $N + 1$ 回以上に制限したことによって，同一の N，m で比較した場合，改良方式の正復号確率は基本方式よりも減少した．N，m がともに小さいほどその差が顕著になり，$m = 11$，$N = 5$ のとき改良方式の正復号確率は基本方式の 16.1%に減少した．
- 復号回数を制限したことによって，$5 \leq N \leq 20$ で改良方式の復号誤り確率はいずれも 10^{-30} 以下を達成した．なお，ビット列が符号語に訂正できる確率の最大値 p は 1.35×10^{-10} であった．
- 基本方式の復号誤り確率は改良方式と比較して非常に大きく，特に $N = 20$，$m = 20$ のときには復号誤り確率は 99%に達し，実用的ではない．復号誤りを回避するために N を，たとえば 10 以下に限定したとしても，復号誤り確率は 10^{-5} から 10^{-3} のオーダとなる．これは消失ビットをランダムに選択した結果である．このような環境下では，改良方式の方が復号誤りを防止できると結論される．
- 改良方式の復号誤り確率が $5 \leq N \leq 20$ で 10^{-30} 以下を達成したことから，本来の情報と異なる偽の情報はランダムにちらばっており，この N に関しては，同一の偽情報を $N + 1$ 回以上復号することはほとんどおこりえないといえる．
- 改良方式では N が大きくなるほど復号誤り確率が減少しているが，その原因として，総当たり復号の回数が増加した効果よりも，復号回数のしきい値が大きくなることで同一の偽情報を復号しにくくなった効果のほうが優勢であったためである．



(A)改良方式の正復号確立 $P_C(m)$ (B)基本方式の正復号確立 $P'_C(m)$



(C)訂正限界$\langle t(N)\rangle$



(D)改良方式の復号誤り確率 $\log_{10} P_E(m)$ (E)基本方式の復号誤り確率 $\log_{10} P'_E(m)$

図 4 $(127, 64, 21)$ BCH 符号に対する改良方式，基本方式の評価結果
Fig. 4 Performances for $(127, 64, 21)$ BCH code by improved method and primitive method.

しかし，たとえば $N = n - t$ と符号長に近い数をとった場合には，ビット列が符号語に訂正できる確率の最大値が，式 (9) より 1 になるため，この関係が崩れて復号誤りが増大する．

改良方式は 3.2 節で提案した基本方式より訂正能力が低いが，消失ビット数 N を $5 \leq N \leq 20$ にとれば，復号誤り確率を 10^{-30} 乗以下に低減できることが示された．

4.4.2 他の訂正符号に対する評価

他の誤り訂正符号に対しても，改良方式によって復号誤りを回避できることを明らかにするために，

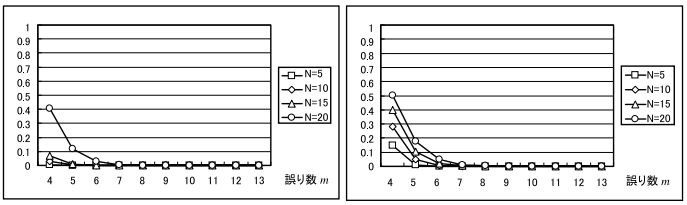
(1) 実情報ビットがより多い $(127, 106, 7)$ BCH 符号

(2) 訂正限界がより大きい $(127, 36, 31)$ BCH 符号

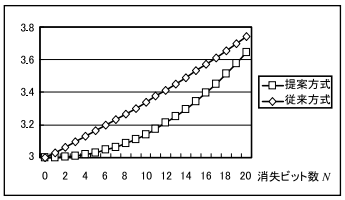
(3) 全体の符号長がより短い $(63, 36, 11)$ BCH 符号

についても改良方式と基本方式の評価を行う．評価結果を**図 5**，**図 6**，**図 7** にまとめる．これらの評価結果より，以下の結論が導かれる．

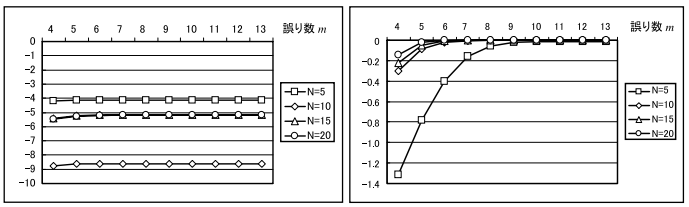
- 復号回数を制限したことによって，改良方式の正復号確率は基本方式よりも減少した．N，m がともに小さいほど減少の度合いが大きくなり，$(127, 106, 7)$ BCH 符号の場合には $N = 5$，$m = 4$ のとき基本方式の 4.8%に，$(127, 36, 31)$ BCH 符号の場合には $N = 5$，$m = 16$ のとき 24.0%に，$(63, 36, 11)$ BCH 符号の場合には $N = 5$，$m = 6$ のとき 16.6%に減少した．
- 改良方式の復号誤り確率は，$5 \leq N \leq 20$ において，$(127, 106, 7)$ BCH 符号のとき 10^{-4} 以下，$(127, 36, 31)$ BCH 符号のとき 10^{-79} 以下，$(63, 36, 11)$ BCH 符号のとき 10^{-8} 以下を達成した．なお，ビット列が符号語に訂正できる確率の最大値は，それぞれ 3.14×10^{-6}，1.679×10^{-16}，4.87×10^{-6} であった．
- 基本方式の復号誤り確率は，$5 \leq N \leq 20$ において，$(127, 106, 7)$ BCH 符号，および $(63, 36, 11)$ BCH 符号のとき 10^{-1} 以上，$(127, 36, 31)$ BCH 符号のとき 10^{-2} 以下となった．これは消失ビットをランダムに選択した結果である．このような環境下では，基本方式は，改良方式と比較して正復号確率が大きい反面，復号誤り確率も大きく，電子透かし検出において実用的でないと結論される．
- $(127, 106, 7)$ BCH 符号に対する改良方式の復号誤り確率は，$N = 10$ を境に増大している．この



(A)改良方式の正復号確立 $P_C(m)$ (B)基本方式の正復号確立 $P'_C(m)$



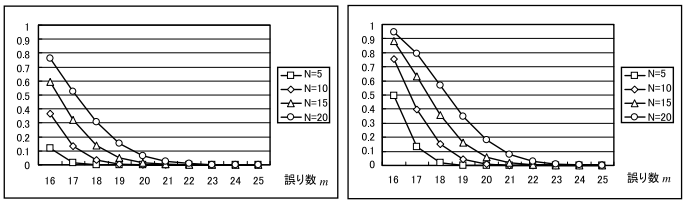
(C)訂正限界$\langle t(N)\rangle$



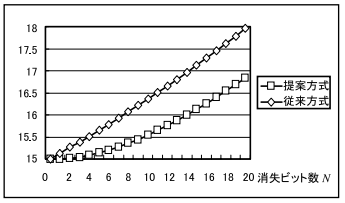
(D)改良方式の復号誤り確率 $\log_{10} P_E(m)$ (E)基本方式の復号誤り確率 $\log_{10} P'_E(m)$

図 5 (127, 106, 7) BCH 符号に対する改良方式，基本方式の評価結果

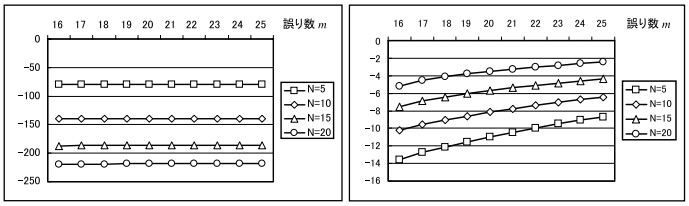
Fig. 5 Performances for (127, 106, 7) BCH code by improved method and primitive method.



(A)改良方式の正復号確立 $P_C(m)$ (B)基本方式の正復号確立 $P'_C(m)$



(C)訂正限界$\langle t(N)\rangle$



(D)改良方式の復号誤り確率 $\log_{10} P_E(m)$ (E)基本方式の復号誤り確率 $\log_{10} P'_E(m)$

図 6 (127, 36, 31) BCH 符号に対する改良方式，基本方式の評価結果

Fig. 6 Performances for (127, 36, 31) BCH code by improved method and primitive method.

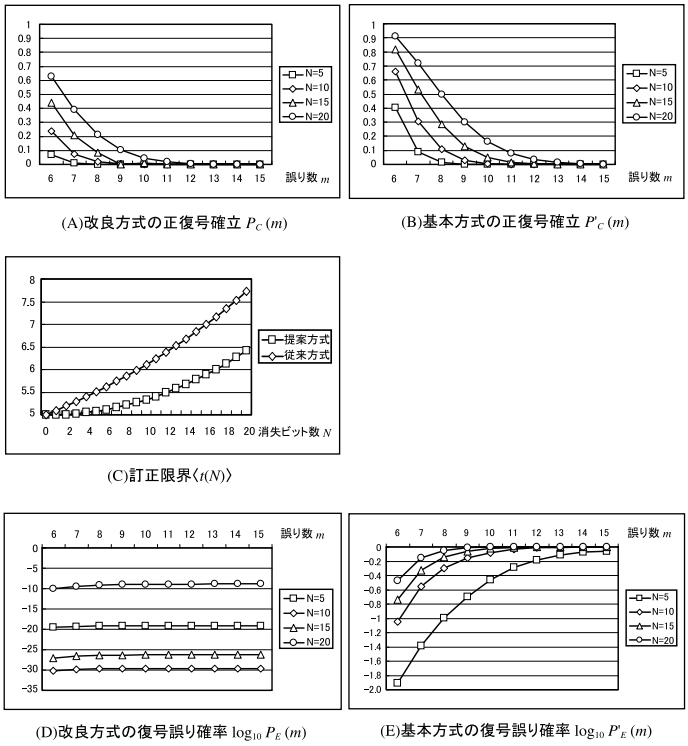


図 7 (64, 36, 11) BCH 符号に対する改良方式，基本方式の評価結果
Fig. 7 Performances for (64, 36, 11) BCH code by improved method and primitive method.

符号は（127, 64, 21）BCH 符号よりも多くの符号語を持つため，N に制限を加えて復号誤りを防止する効果よりも，誤り訂正を繰り返すことで本来と異なる符号語にヒットする確率のほうが優勢になったためと考えられる．

- （63, 36, 11）BCH 符号のときも同様に，復号誤り確率は $N = 10$ を境に増大している．この符号は（127, 64, 21）BCH 符号よりも符号長が短いため，誤り訂正を繰り返す回数が 64 ビット列そのものの組合せにより近づき，本来と異なる符号語にヒットする確率が大きくなったためと考えられる．

いずれの符号でも，改良方式によって復号回数に制限を加えることで，復号誤りを回避できることが明らかになった．

4.5 拡　　張

以上の解析によって，改良方式によって復号誤りが回避できることが示された．しかし，もともとの誤りビット数が少ない場合，改良方式の正復号確率は基本方式より低いことも明らかになった．これは，復号回数が $N+1$ 未満であった復号情報を破棄したことによる．

基本方式のもととなったチェイス復号法では，復号誤りを回避するために，N を訂正限界 t 以下にとることが推奨される[23]．そこで，t 以下の N に対しては，復号回数による制限をなくすことで，改良方式の正復号確率を向上させられると考えられる．

また，改良方式および基本方式双方とも，適用の際には，あらかじめ消失ビット数 N を固定しておく必要がある．ところが実際コンテンツの劣化度合いに応じてとるべき N が変わるのだから，自動的に N を調節できることが好ましい．

以上の観点から改良方式をさらに拡張し，復号誤りを回避しつつ基本方式とほぼ同等の訂正能力を有する電子透かし検出方式を，以下のように提案する（**図 8**）．

Step 1（設定）
消失ビット数 N を 0 に，N のしきい値 T を訂正限界 t 以下に設定する．また，N の上限 $\bar{N}$ を設定する．

Step 2（透かし抽出）
コンテンツから透かしを抽出し，埋め込まれているビット列と各ビットの信頼度を算出する．

Step 3（消失ビット決定）
信頼度が低い N 個の消失ビットを取り出す．

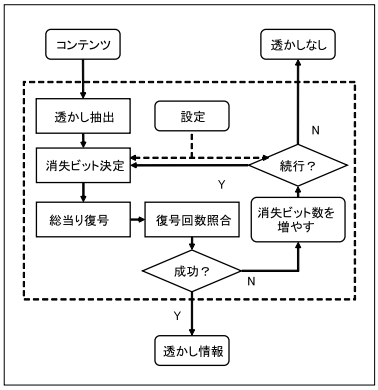


図 8 提案方式を拡張した検出処理手順
Fig. 8 Detection process for extended method.

Step 4 （総当たり復号）
取り出した N 個の各ビットに 0，1 を割り当てて得られる 2^N 個のビット列それぞれに対して誤り訂正を施す．

Step 5 （復号回数照合）
$N \leq T$ のとき，得られた復号情報のうち最も復号回数が大きい情報を出力する．$N > T$ のとき，$N+1$ 回以上復号できたビット列のうち最も復号回数が大きいものを出力する．

Step 6 （判断）
出力情報を透かし情報として採択する．何も出力できなかった場合，N を 1 増やして Step 3 に戻る．N が $\bar{N}$ を超過したとき，透かし情報が検出できなかったとして処理を終了する．

コンテンツの誤りビット数が少ない場合には，T より小さい N に対して復号が成功する可能性が高い．この確率は基本方式の正復号確率 (21) で与えられる．しかし，その反面，コンテンツの誤りビット数が多い場合には，改良方式よりも高い，基本方式の復号誤り確率 (23) で誤った情報を復号する可能性も増大してしまう．たとえば，各ビットの信頼度が正しく算出できないコンテンツに対して拡張方式を適用した場合には，$(127, 64, 21)$ BCH 符号の場合，図 4 (E) より，復号誤り確率は 10^{-3} 程度と評価される．同様に他の符号に対する拡張方式の復号誤り確率の最悪値は，図 5–図 7 の (E) より，$(127, 106, 7)$，$(63, 36, 7)$ BCH 符号のとき 10^{-1} 以上，$(127, 36, 31)$ BCH 符号のとき 10^{-2} 程度と評価される．したがって，劣化が著しく，信頼度が正しく算出できないコンテンツに対して復号誤り確率を低く抑える必要がある場合には，基本方式の復号誤り確率 (23) を評価して T の値を t よりも小さく設定し，小さな N に対して改良方式が適用されやすいようにする必要がある．なお，もともと透かしが埋め込まれていないコンテンツに対してこの拡張方式を適用した場合，無限ループに陥るため，終了条件として，N が $\bar{N}$ を超過した場合には透かしなしとして検出処理を終了する．

上記の電子透かし検出方式によって，従来の誤り訂正を用いた検出方式では何の情報も検出できなかった劣化コンテンツからも，復号誤りを回避しつつ，情報を復元できる可能性が向上する．次章で電子透かし検出実験を行い，このことを実証する．

5. 実　　験

5.1 電子透かしの定式化

4.4 節の結果は，消失ビットをランダムに選択した場合の結果である．実際の電子透かしでは，消失ビットの選択がある程度は正しいと予想されるため，透かし情報の検出精度はより高いと考えられる．そこで本章では電子透かし検出の評価実験を行い，4.5 節で提案した拡張方式と通常の誤り訂正を用いた検出方式の電子透かし検出能力を評価し，比較する．

誤り訂正方式は透かし情報の誤りを訂正するためだけに用いられ，透かし情報の埋め込み方式に依存しない．そこで本論文では，比較評価のために静止画像を対象とし，誤り訂正符号を用いた最も単純かつ一般性の高い方式として，次の埋め込み方式を採用する．なおこの方式は文献 9) の方式を簡略化したものに相当する．

Step 1 （透かし情報画像作成）
ビット 0，1 をそれぞれ輝度 I，$-I$ の $b_x \times b_y$ ブロックに対応させる．透かし情報に誤り訂正用の検査ビットを付加し，得られたビット列に対応するように $b_x \times b_y$ ブロックを横一列に並べる．得られた画像を透かし情報画像とよぶ．

Step 2 （透かし埋め込み）
透かし情報画像を透かし埋め込み対象の画像全体に隙間なく足し合わせる．

なお，文献 9) の方式では，透かし情報が除去されないようにビットプレーンを巧妙に操作するが，本論文の目的は検出能力を評価することにあるので，ビットプレーンの代わりに直接輝度を上げ下げすることで情報を埋め込む．

こうして埋め込まれた情報は次の手順で検出できる．

Step 1 （差分画像作成）
透かしが埋め込まれた画像から元の画像を引き，得られた差分画像を透かし情報画像の大きさにまとめあげることで，透かし情報画像を再現する．

Step 2 （透かし検出）

得られた透かし情報画像を構成する $b_x \times b_y$ ブロックそれぞれについて輝度の平均値を計算し，埋め込んだビット列に対応する評価値を求める．各評価値 z_i に対して，ビット値 b_i を

$$b_i = \begin{cases} 0 & (\tau < z_i) \\ \text{消失} & (-\tau \leq z_i \leq \tau) \\ 1 & (z_i < -\tau) \end{cases} \qquad (24)$$

と割り当てる．得られたビット列に誤り訂正を施すことで透かし情報を検出する．

このような電子透かし方式を用いて実際に透かし情報を静止画に埋め込み，画像処理を加えた後，4.5 節であげた提案方式と，通常の誤り訂正を用いる従来方式とで透かし情報を検出して，検出能力を比較する．

5.2 透かし検出における条件

透かし検出実験を行うにあたり以下の条件を設けた．

(1) 提案方式
提案方式として 4.5 項で述べた拡張方式を採用する．N の上限 $\bar{N}$ として，計算量の観点から $\bar{N} = 20$ とした．また，復号誤りを回避するために，T を 0 にして通常のチェイス復号法を用いないようにし，さらに $N = 5$ から誤り訂正を開始した．

(2) 誤り訂正符号
誤り訂正符号として，まず 4.4.1 項であげた $(127, 64, 21)$ BCH 符号を採用し，透かし検出実験を行う．次に 4.4.2 項であげた他の訂正符号についても同様の実験を行い，実験結果を比較検証する．

(3) 消失ビット
提案方式を適用するには，N に応じてしきい値 τ を調節する必要があるが，式 (24) によれば，これは絶対値が小さい評価値を N 個取り出したものにほかならない．そこで，評価値を絶対値でソートすることで提案方式を実装した．また，通常の誤り訂正を適用するにあたっては，$\tau = 0$ として消失ビットが現れないようにした．

(4) 画像処理
画像処理として JPEG 圧縮を採用した．圧縮率を変えながら透かしが埋め込まれた画像に JPEG 圧縮を施すことで，誤りビット数が 11 から 20 になる圧縮画像を作成した．JPEG 圧縮画像の例を**図 9** にあげる．圧縮によってブロック歪みが発生し，これが透かし情報の誤りを引き起こす．

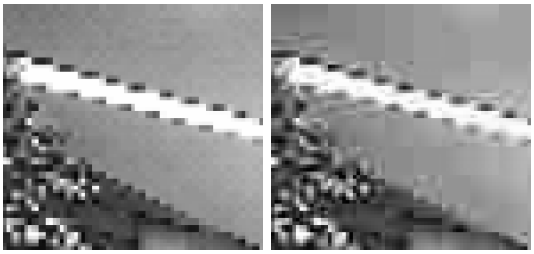


図 9 JPEG 圧縮によりブロック歪みが発生した圧縮画像（右）
Fig. 9 The right image is a compressed image—JPEG compression causes block distortion.

(5) 透かし情報画像
透かし情報画像を構成するブロックの大きさを，予備実験の結果誤りビット数の調整が容易であった 2×2 に固定した．同様に，透かし情報画像の輝度 I を，予備実験の結果 $I = 2$ に固定した．

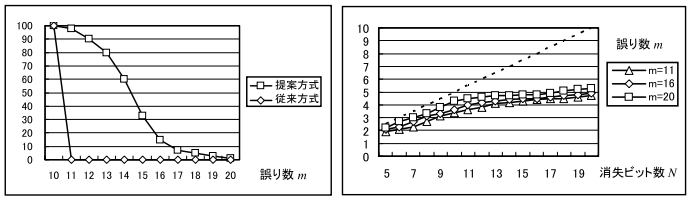
(6) 透かし検出画像
透かし情報画像を 256 回埋め込むことができる大きさの画像を 100 枚用意し，それぞれについて画像処理を加えた後，透かし検出を試みた．100 枚中検出に成功した枚数から検出能力を測定した．

5.3 電子透かし検出の比較実験

5.3.1 （127,64,21）BCH 符号に対する実験結果

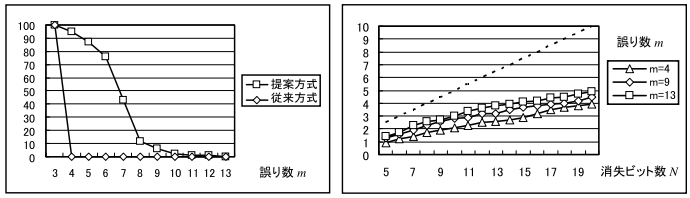
透かし検出に成功した画像数を**図 10** (A) に，また，本実験において，N 個の消失ビットのうち実際に取り出すことができた誤りビット数の平均値を図 10 (B) にまとめる．これらの結果より以下の結論が導かれる．

- $(127, 64, 21)$ BCH 符号の訂正限界は 10 ビットであり，従来の誤り訂正方式では，これ以上の誤りが生じた場合まったく情報を復号できなかった．一方，提案方式の訂正限界は図 10 (A) のように向上し，提案方式を適用することで，誤りビット数が 20 の圧縮画像からも情報が検出できる場合があることが示された．提案方式の訂正限界の平均値は 13.92 となった．なお，4.4.1 項の結果より，復号誤り確率は 10^{-30} 以下である．
- JPEG の圧縮率はクオリティファクタ Q で調節でき，Q が小さいほど圧縮率が高くなる．ただし，同じ Q でも劣化の度合いは 100 枚のコンテンツによって異なったため，本実験では実験を定量的に行うために，Q ではなく誤りビット数を対象とした．おおよその結果として，提案方式では $Q = 20$ 前後，通常の誤り訂正を用いた検出方式では $Q = 30$ 前後の圧縮コンテンツから情報が検



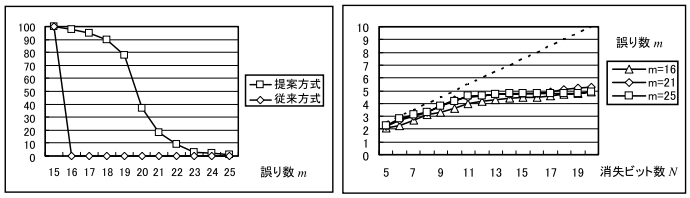
(A)透かし検出に成功した画像数　　(B)抽出できた誤りビット数の平均値

図 10（127, 64, 21）BCH 符号によって検出できた画像数と抽出できた誤りビット数の平均値
Fig. 10 The number of images correctly detected and averages of the numbers of error bits for (127, 64, 21) BCH code.



(A)透かし検出に成功した画像数　　(B)抽出できた誤りビット数の平均値

図 11（127, 106, 7）BCH 符号によって検出できた画像数と抽出できた誤りビット数の平均値
Fig. 11 The number of images correctly detected and averages of the numbers of error bits for (127, 106, 7) BCH code.



(A)透かし検出に成功した画像数　　(B)抽出できた誤りビット数の平均値

図 12（127, 36, 31）BCH 符号によって検出できた画像数と抽出できた誤りビット数の平均値
Fig. 12 The number of images correctly detected and averages of the numbers of error bits for (127, 36, 21) BCH code.

出できた．

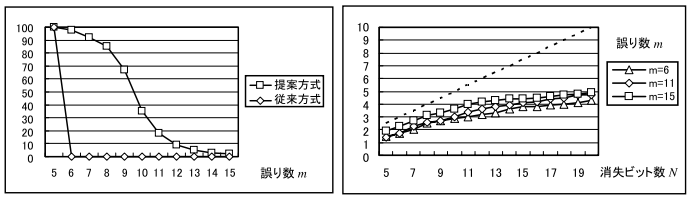
- 図 10 (A) で示された検出能力は図 4 (C) の結果より高いが，これは評価値をもとにした結果，127 ビット全体からランダムに選定するよりもある程度効率良く，消失ビットを選択できたためと考えられる．
- 図 10 (B) より，消失ビット数 N，もしくは 127 ビット全体の誤りビット数 m が大きくなるにつれて，抽出できた誤りビット数の平均が増加することが分かる．もし各ビットの信頼度を正しく見積もることが可能であれば，消失ビットとして選択したビットが実際に誤っている確率は 1/2 に近づくので，抽出できた誤りビット数の平均値は $N/2$ に達するはずである（図中点線）．しかし，実際に抽出できた消失ビット数は $N/2$ より小さい．JPEG 圧縮によって発生したブロック歪みの影響を受けた結果，式 (24) では各ビットの信頼度を正しく評価できず，消失ビットをとりこぼしやすかったと結論される．

以上の結果より，提案方式によって，(127, 64, 21) BCH 符号の訂正限界 10 ビットが，復号誤り確率 10^{-30} 以下を保ちつつ，13.92 ビットにまで向上し，電子透かし検出能力が改善されることが実証された．

5.3.2 他の訂正符号に関する実験結果

他の誤り訂正符号に対しても，提案方式によって電子透かしの検出能力が向上することを明らかにするために，4.4.2 項であげた（127, 106, 7），(127, 36, 31)，および（63, 36, 11）BCH 符号についても同様の検出実験を行った．その結果を**図 11**，**図 12**，**図 13** にまとめる．これらの評価結果より，以下の結論が導かれる．

(1) （127, 106, 7）BCH 符号に対しては，訂正限界 3 ビットが 5.71 ビットに向上した．4.4.2 項の



(A)透かし検出に成功した画像数　　(B)抽出できた誤りビット数の平均値

図 13 $(64, 36, 11)$ BCH 符号によって検出できた画像数と抽出できた誤りビット数の平均値
Fig. 13 The number of images correctly detected and averages of the numbers of error bits for $(63, 36, 11)$ BCH code.

結果より，復号誤り確率は 10^{-4} 以下である．抽出できた消失ビット数は $N/2$ から離れているが，これは，もともと誤りビット数が少ないため，消失ビットの捕捉に失敗したためと考えられる．誤りを発生させるために用いた JPEG 圧縮のクオリティファクタは，100 枚のコンテンツでおおよそ 30 であった．

(2) $(127, 36, 31)$ BCH 符号に対しては，訂正限界 15 ビットが 19.31 ビットに向上した．復号誤り確率は 10^{-79} 以下である．誤りビット数 $m = 25$ ビットのとき，ブロック歪みの影響が大きくなり，$m = 21$ のときよりも抽出できた消失ビット数が少ない．JPEG のクオリティファクタは 15 程度であった．

(3) $(63, 36, 11)$ BCH 符号に対しては，訂正限界 5 ビットが 9.14 ビットに向上した．復号誤り確率は 10^{-8} 以下である．符号長 127 ビットの場合と同様，$N = 10$ 付近でブロックノイズの影響を受け消失ビットをとりこぼしはじめた．JPEG のクオリティファクタは 20 程度であった．

いずれの符号でも提案方式によって，復号誤り確率を低減させつつ，電子透かしの検出能力が改善されることが明らかになった．

6. ま と め

本論文では，電子透かしの検出における誤り訂正能力の向上について述べた．電子透かし情報は微弱であるうえ，制作，流通の過程および不正者の意図による様々なメディア処理が加えられるため，その検出では誤りビット数が多数となる．ところが，コンテンツの価値維持からの制約により，誤りを訂正する余分な検査ビット列を多く埋め込むことはできない．そのため，誤り訂正符号を用いた従来の電子透かし検出方式では，ビット誤り数が訂正限界を超え，情報を復号できないことが多かった．

そこで，訂正限界以上の誤り訂正を行う方式として，符号理論の分野で知られている軟判定復号法を取り上げ，電子透かし検出への適用を提案した．現実の電子透かし検出では，メディア処理の影響などにより，軟判定復号法の前提となる各ビットの信頼度を正確に算出できない場合が多い．そこで，軟判定復号法を拡張し，ビットの信頼度の代わりに，同じ情報が何回復号されるかという復号回数に基づいて，訂正限界以上の誤りに対応する方式を考案した．

符号長 127 ビット，実情報 64 ビット，最小距離 21 ビットの，訂正限界 10 ビットまでの誤りを訂正できる $(127, 64, 21)$ BCH 符号を用いて提案方式を実装し，消失ビット数が 20 以下のとき，提案方式の復号誤り確率は 10^{-30} 以下を達成することを証明した．また，実際のサンプル画像に電子透かしを埋め込み，JPEG 圧縮によって訂正限界以上の誤りを発生させた後，提案方式の誤り訂正能力を実測することで，通常の誤り訂正を用いた検出方式の訂正限界 10 ビットが，提案方式を適用することによって平均 13.92 ビットにまで向上することを明らかにした．さらに，他の訂正符号に対しても同様の透かし検出実験を行い，$(127, 106, 7)$ BCH 符号の訂正限界 3 ビットが 5.71 ビットに，$(127, 36, 31)$ BCH 符号の訂正限界 15 ビットが 19.31 ビットに，$(64, 36, 11)$ BCH 符号の訂正限界 5 ビットが 9.14 ビットに向上することを明らかにした．

なお，本論文では電子透かしの検出方式について論じたが，これに限らず，各ビットの信頼度を厳密に算出することが困難で，かつ復号誤りをできるだけ低減しなければならない環境下において，本論文で提案した復号回数を用いた誤り訂正方式は広く有効であると考えられる．

謝辞 本論文 5 章の比較実験は，平成 15 年度 NEDO（新エネルギー・産業技術総合開発機構）の委託研究「クロスメディアコンテンツ基盤技術の研究開発」を通じて着想を得た．

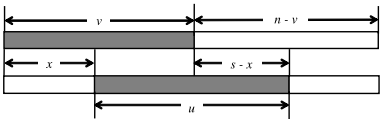


図 14 u, v, x の関係
Fig. 14 Relation among u, v, x.

付　　録

A.1 式 (7)，(10)，(14) の導出

まず式 (7) を導出する．**図 14** に見るように，ある重み v の符号語から s だけ離れた重み u のビット列の総数は，v 個から x 個とり，$n-v$ 個から $s-x$ 個とる組合せの数 ${}_vC_x \cdot {}_{n-v}C_{s-x}$ に等しい．ここで x は，関係式 $x+(u-(s-x))=v$ より $x=(v-u+s)/2$ と計算できる．したがって，重み u のビット列が重み v のある符号語に訂正される確率は，重み v の符号語が存在する場合には，${}_vC_x \cdot {}_{n-v}C_{s-x}$ の和を $s=0,\ldots,t$ についてとり，重み v のビット列の総数 ${}_nC_v$ で割ることで得られる．x が整数でない場合，二項係数の定義式 (5) から ${}_vC_x \cdot {}_{n-v}C_{s-x}$ は 0 になることに注意する．また，重み v の符号語が存在しない場合には，求めるべき確率は 0 である．なお，以上の導出に関しては文献 29) を参照した．

次に，式 (10) を導出する．N 個の判別ビットを除いたビット列の重みを u とすると，総当たり復号によって重みは $u+i$（$i=0,\ldots,N$）になり，各 i について $R_i = {}_NC_i$ 回誤り訂正を施すことになる．R_i 回施して重み v のある符号語に k_i 回訂正できる確率は ${}_{R_i}C_{k_i} \cdot {p_{u+i,v}}^{k_i}(1-p_{u+i,v})^{R_i-k_i}$ だから，和 $k_0+\cdots+k_N$ を r に制限して，式 (10) が得られる．

最後に，式 (14) を証明する．式 (8) を式 (10) に代入すると，

$$P_{u,0}(r) = \sum_{k_0+\cdots+k_N=r} \prod_{i=0}^{t-u} \delta_{k_i,R_i} \prod_{i=t-u+1}^{N} \delta_{k_i,0} \tag{25}$$

が得られる．$u=t+1,\ldots,t-N$ について計算すると，0 にならない $P_{u,0}(r)$ は

$$\begin{aligned} P_{t+1,0}(r) &= \delta_{r,0} \\ P_{t,0}(r) &= \delta_{r,R_0} \\ P_{t-1,0}(r) &= \delta_{r,R_0+R_1} \\ &\vdots \\ P_{t-N,0}(r) &= \delta_{r,R_0+\cdots+R_N} \end{aligned} \tag{26}$$

に限られる．関係式 $u=m-M$，$R_i = {}_NC_i$，および M の上限が N であることに気をつけて，式 (14) が証明される．

参　考　文　献

1) Cox, I.J., Miller, M.L. and Bloom, J.A.: *Digital Watermarking*, Morgan Kaufmann Publishers (2001).
2) 松井甲子雄：電子透かしの基礎，森北出版 (1998).
3) 大西淳児，松井甲子雄：多重解像度解析と PN 系列を利用した電子透かし法，電子情報通信学会論文誌 D-II，Vol.J80-D-II, No.7, pp.3020–3028 (1997).
4) Ó Ruanaidh, J.J.K., Dowling, W.J. and Boland, F.M.: Watermarking Digital Images for Copyright Protection, *IEEE Proc. Vision, Signal and Image Processing*, Vol.143, No.4, pp.250–256 (1996).
5) Marvel, L.M., Boncelet Jr., C.G. and Retter, C.T.: Reliable Blind Information Hiding for Images, *Proc. Information Hiding*, Lecture Notes in Computer Science, Vol.1525, pp.48–61 (1998).
6) Kutter, M. and Petitcolas, F.A.P.: A Fair Benchmark for Image Watermarking Systems, *Proc. SPIE Security and Watermarking of Multimedia Contents*, Vol.3657, pp.226–239 (1999).
7) 山口和彦，岩村恵市，今井秀樹：誤り訂正符号を用いたアルゴリズム公開型電子透かし，1999 年暗号と情報セキュリティシンポジウム SCIS'99-T4-2.2，pp.713–718 (1999).
8) 角野英之，稲葉宏幸，笠原正雄：改ざんを考慮した動画像の電子透かしに関する二，三の考察，映像情報メディア学会誌，Vol.54, No.4, pp.593–600 (2000).
9) 平田弘毅，池原雅章：誤り訂正符号を用いた電子透かし，信学技報 CS2000-144，pp.95–102 (2001).
10) Bradley, B.A. and Brunk, H.: Comparative Performance of Watermarking Schemes Using M-ary Modulation with Binary Schemes Employing Error Correction Coding, *Proc. SPIE Security and Watermarking of Multimedia Contents III*, Vol.4314, pp.629–642 (2001).
11) Eggers, J.J., Bäuml, R. and Girod, B.: A Communications Approach to Image Steganography, *Proc. SPIE Security and Watermarking of Multimedia Contents IV*, Vol.4675, pp.26–37 (2002).
12) Bender, W., Gruhl, D. and Morimoto, N.: Techniques for Data Hiding, *Proc. SPIE*, Vol.2020, pp.2420–2440 (1995).
13) 小林誠士，上條浩一，清水周一：近傍ピクセルの性質を用いたデータハイディング—近傍ピクセルの統計的性質，第 56 回情報処理学会全国大会論文集，1V-03 (1998).

14) Linnartz, J.P., Kalker, T. and Depovere, G.: Modeling the False Alarm and Missed Detection Rate for Electronic Watermarks, *Proc. Information Hiding*, Lecture Notes in Computer Science, Vol.1525, pp.329–343 (1998).
15) Gruhl, D. and Bender, W.: Information Hiding to Foil the Casual Counterfeiter, *Proc. Information Hiding*, Lecture Notes in Computer Science, Vol.1525, pp.1–15 (1998).
16) 越前 功，吉浦 裕，安細康介，佐々木良一：分布推定手法を用いた電子透かしの検出誤り確率推定方式，情報処理学会論文誌，Vol.42, No.8, pp.2006–2016 (2001).
17) 小川 宏，中村高雄，高嶋洋一：フレーム間を考慮した電子透かし方式の有効性，電子情報通信学会，基礎境界ソサイエティ大会講演論文集，pp.252–253 (1997).
18) Swanson, M.D., Zhu, B. and Tewfik, A.H.: Transparent Robust Image Watermarking, *Proc. International Conference on Image Processing*, Vol.3, pp.211–214 (1996).
19) Delaigle, J.F., De Vleeschouwer, C. and Macq, B.: Watermarking Algorithm Based on a Human Visual Model, *IEEE Signal Processing*, Vol.66, pp.319–335 (1998).
20) Bony, L., Tewfik, A.H. and Hamdy, K.N.: Digital Watermarks for Audio Signals, *IEEE Proc. International Conference on Multimedia Computing and Systems*, Session 17, pp.473–480 (1996).
21) コンテンツ ID フォーラム（編）：cIDf Specification 1.1.
22) Forney Jr., G.D.: Generalized Minimum Distance Decoding, *IEEE Trans. Inf. Theory*, Vol.IT-12, No.2, pp.125–131 (1966).
23) Chase, D.: A Class of Algorithms for Decoding Block Codes with Channel Measurement Information, *IEEE Trans. Inf. Theory*, Vol.IT-18, No.1, pp.170–182 (1972).
24) Tanaka, H. and Kakigahara, K.: Simplified Correlation Decoding by Selecting Possible Codewords Using Erasure Information, *IEEE Trans. Inf. Theory*, Vol.IT-29, No.5, pp.743–748 (1983).
25) Taipale, D.J. and Pursley, M.B.: An Improvement to Generalized-Minimum-Distance Decoding, *IEEE Trans. Inf. Theory*, Vol.37, No.1, pp.167–172 (1991).
26) Kaneko, T., Nishijima, T., Inazumi, H. and Hirasawa, S.: An Efficient Maximum-Likelihood-Decoding Algorithm for Linear Block Codes with Algebraic Decoder, *IEEE Trans. Inf. Theory*, Vol.40, No.2, pp.320–327 (1994).
27) Moorthy, H.T., Lin, S. and Kasami, T.: Soft-Decision Decoding of Binary Linear Block Codes Based on an Iterative Search Algorithm, *IEEE Trans. Inf. Theory*, Vol.43, No.3, pp.1030–1040 (1997).
28) Kasami, T., Tang, Y., Koumoto, T. and Fujiwara, T.: Sufficient Conditions for Ruling-Out Useless Iterative Steps in a Class of Iterative Decoding Algorithms, *IEICE Trans. A*, Vol.E82-A, No.10, pp.2061–2073 (1999).
29) 今井秀樹：符号理論，電子通信情報学会 (1990).
30) Lin, S. and Costello, D.J.: *Error Control Coding: Fundamentals and Applications*, Prentice Hall (1983).
31) 堀口敏男：ユークリッド復号法を用いたリードソロモン符号の BCH 限界以上の復号，電子情報通信学会論文誌 A，Vol.J78-A, No.5, pp.626–638 (1995).
32) 小林 学，松島敏泰，平澤茂一：BCH 限界を超える復号法とその軟判定復号法への応用，電子情報通信学会論文誌 A，Vol.J81-A, No.4, pp.751–762 (1998).
33) Sudan, M.: Decoding of Reed-Solomon Codes Beyond the Error-Correction Bound, *J. Complexity*, Vol.13, No.1, pp.180–193 (1997).
34) Guruswami, V. and Sudan, M.: Improved Decoding of Reed-Solomon and Algebraic-Geometry Codes, *IEEE Trans. Inf. Theory*, Vol.45, No.6, pp.1757–1767 (1999).
35) http://www.infsys.cne.okayama-u.ac.jp/~koumoto/wd/

(平成 15 年 12 月 2 日受付)
(平成 16 年 6 月 8 日採録)

藤井 康広（正会員）

2001 年東京大学大学院理学系研究科博士課程修了（物理学）．同年日立製作所入社．現在，システム開発研究所第 7 部（セキュリティシステム研究部）研究員．情報セキュリティ技術，著作権保護技術，機密情報管理システムの研究開発に従事．博士（理学）．電子情報通信学会会員．

越前　功（正会員）

1997 年東京工業大学大学院修士課程修了（応用物理学）．同年日立製作所入社，システム開発研究所配属．情報セキュリティ技術，画像用電子透かし技術の研究開発を担当．現在，同研究所第 7 部（セキュリティシステム研究部）研究員．博士（工学）．映像情報メディア学会会員．

山田　隆亮（正会員）

1988 年京都大学工学部資源工学科卒業．同年日立製作所に入社．大森ソフトウェア工場を経て，現在，システム開発研究所第 7 部（セキュリティシステム研究部）主任研究員．マルチメディア応用，コンテンツ流通システムの研究に従事．映像情報メディア学会会員．

手塚　悟（正会員）

1984 年慶應義塾大学工学部数理工学科卒業．同年日立製作所入社，マイクロエレクトロニクス機器開発研究所を経て，現在，システム開発研究所セキュリティシステム研究センタ勤務．オペレーティングシステム，デバイスドライバ，LAN システムの研究を経て，現在，セキュリティシステム，特に電子認証の研究開発に従事．工学博士．

吉浦　裕（正会員）

1981 年東京大学理学部情報科学科卒業．同年日立製作所入社．日立研究所，システム開発研究所を経て．現在，電気通信大学電気通信学部人間コミュニケーション学科助教授．自然言語処理，知識処理，情報セキュリティ，著作権保護の研究に従事．理学博士．電子情報通信学会，人工知能学会各会員．