数論変換を用いた可逆電子透かしの埋め込み容量改善

森田 洋平† 與本 亮太† 岩村 恵市† 越前 功‡
†東京理科大学 〒102-0073 東京都千代田区九段北1-14-6
yomoto@sec.ee.kagu.tus.ac.jp
‡国立情報学研究所 〒101-8430 東京都千代田区一ツ橋 2-1-2

あらまし：可逆電子透かしは、品質や耐性の評価に比重が置かれる非可逆電子透かしとは用途が異なるということもあり、品質、耐性、容量のうちで容量の評価に比重が置かれることが多い。著者らの知る限り従来方式の中では、D.Coltuc らによる方法が 1 度の埋め込みで最大の埋め込み容量を実現する（Lena に対して 8 ビット構成の 1 ピクセル当たり、1.690 ビット埋め込み）。本研究では、この従来方式が情報埋め込みできなかった部分に着目し、その部分に新しく処理を加えることで、より多くの埋め込み容量を実現した。その結果 1 ピクセル当たり 1.694 ビットの埋め込みを実現し、現時点での最大埋め込みを実現した。

The embedding capacity improvement of reversible digital watermarking using number-theoretic transform

Yohei Morita† Ryota Yomoto† Keiichi Iwamura† Isao Echizen‡
† Tokyo University of Science 1-14-6 Kundankita, Chiyoda-ku, Tokyo 102-0073, Japan
yomoto@sec.ee.kagu.tus.ac.jp
‡ National Institute of Informatics2-1-2 Hitotsubashi, Chiyoda-ku, Tokyo 101-8430, Japan

Abstract Since it says that reversible digital watermarking differs in a use from irreversible digital watermarking in which specific gravity is placed on evaluation of quality or tolerance, specific gravity is placed on evaluation of capacity among quality, tolerance, and capacity in many cases. As far as authors get to know, in the conventional system, the method by D.Coltuc and others realizes the embedding capacity maximum by the embedding which is 1 time (it is the 1.690-bit embedding per pixel of 8 bit configurations to Lena). In this research, adding processing to that portion newly realized more embedding capacity paying attention to the portion which was not able to carry out information embedding of this conventional system. As a result, 1.694 bits per pixel embedding was realized, and the maximum embedding in this time was realized.

１．はじめに

電子透かしとは画像や動画、音声などのデジタルコンテンツに、画質や音質にはほとんど影響を与えずに特定の情報を埋め込む技術

のことをいう。一般に、情報を埋め込みにより原コンテンツの不可逆な劣化が起こるが、この劣化が受け入れられない用途がある。そのような用途のために、可逆型の電子透かし(以降、可逆透かしと呼ぶ）が提案されている[1][2][3]。

可逆透かしとは、秘密情報と復元情報で構成される透かし情報をデジタルコンテンツに埋め込み、そのコンテンツから透かし情報を抽出した後、復元情報を用いて原コンテンツを復元する技術である。また、通常の電子透かしが画質と耐性と容量をその評価尺度とするのに比べ、可逆透かしは容量のみを評価尺度とする場合が多い。

一般に可逆透かしは、原画像を復元するための副情報が必要な方法とそうでない方法がある。副情報が必要でない方法は、埋めたい情報のみを埋め込めばよいが、副情報が必要な方法は、埋めたい情報の他に、その副情報も一緒に埋め込まなくてはならない。

可逆透かしは、品質や耐性の評価に比重が置かれる非可逆電子透かしとは用途が異なるということもあり、品質、耐性、容量のうちで容量の評価に比重が置かれることが多い。特に、1 度の埋め込み容量に対しての評価がなされることが多く、著者らが知る限り、1 度の埋め込みに対して 1 番多くの情報を埋め込める方法[1]が存在する。

この方法のポイントとしては、埋める情報の要素の個数 n=8 の場合、埋め込みができない画素が 1 画素存在すると、それを復元するための副情報が平均 1.1 画素必要になる。これは、情報の埋め込みができない画素が 1 画素存在すると、その埋め込めない画素も含め、冗長な画素が平均 2.1 画素発生することを意味する。また、ICIP (International Conference on Information Processing)で発表された可逆透かしについての論文を調査したところ、これ以上の埋め込み容量は実現できていない。

そこで、本研究では、誤り訂正符号を用いることで、従来方式の冗長度を減らし、情報の埋め込みができなかった部分に着目し、その部分に新しく処理を加えることで、より多くの埋め込み容量が実現できるのではないかと考え、誤り訂正符号を用いた情報の埋め込み・抽出のアルゴリズムと埋め込みの容量について検討した。

２．従来方式

２．１　埋め込み方法

図 1 のように画素を横一列に見たとき、画素 $x_i,(i=0,\ldots,N)$ に番号を付ける。また、画素値は 0 から L の範囲にあるとする。埋める情報は n 個の要素からなる $w_i \in \{1,\ldots,n\}$ である。この埋める情報に復元情報も含まれる。次に埋め込み手順を示す

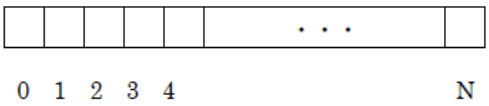

図 1 ：画素のイメージ

[手順 1]　$i := 0$

[手順 2]　式(1)、式(2)を同時に満たす場合は(a)、それ以外は(b)に分ける。

$$0 \le (n+1)x_i - nx_{i+1} \le L \quad \cdots (1)$$

$$(n+1)x_i - nx_{i+1} + n \le L \quad \cdots (2)$$

(a)　式(3)によって x_i の画素値を y_i とする。

$$y_i = (n+1)x_i - nx_{i+1} \quad \cdots (3)$$

(b)　式(4)により c_i を求め、式(5)によって x_i の画素値を y_i' とする。また、c_i は復元するために必要なので記憶しておく。

$$c_i \equiv x_i + nx_{i+1} \bmod (n+1) \quad \cdots (4)$$

$$y_i' = x_i - c_i \quad \cdots (5)$$

[手順 3]　$i := i+1$.　$i < N-1$であれば、手順 2 へ。

[手順 4]　$i = N-1$から$i = 0$に向けて、式(3)

によって y_i に変換した画素にのみ情報を埋める。このとき、まず復元情報 c_i を、i が大きい順に埋めていく。復元情報を埋め終えた後、本来埋め込みたい情報を埋めていく。

$y_i' = y_i + w_i$ ・・・(6)

ここで、式(4)より復元情報 c_i は $c_i \in \{0,1,\ldots,n\}$ の n+1 要素であるが、実際に埋めていく情報 w_i は $w_i \in \{1,\ldots,n\}$ で n 要素である。そのため、w_i の n 要素で c_i の n+1 要素を表さなければならない。つまり、以下の表 1 のように w_i と w_{i+1} の 2 つの情報を用いて c_i を表している。

表 1　n=3 のときの w_i と c_i の関係

c_i	w_i	w_{i+1}
0	1	1
1	1	2
2	2	
3	3	

２．２　抽出方法

抽出は、復元情報と秘密情報を同時に抽出していく。

[手順 1]　$i := N-1$

[手順 2]　式(7)を満さない場合は(a)へ、満たす場合は(b)に。

$$y_i + nx_{i+1} \equiv 0 \bmod (n+1) \quad \text{・・・(7)}$$

(a)　式(8)により、情報 w_i を抽出し、式(9)から y_i を求める。また、式(10)から原画像の画素値 x_i を求める。

$$w_i + y_i + nx_{i+1} \bmod (n+1) = w_i \quad \text{・・・(8)}$$

$$y_i = y_i' - w_i \quad \text{・・・(9)}$$

$$x_i = \frac{y_i + nx_{i+1}}{n+1} \quad \text{・・・(10)}$$

(b)　抽出した復元情報 c_i (w_i)から式(11)を用い、x_i を求める。

$x_i = y_i' + c_i$ ・・・(11)

[手順 3]　$i := i-1$.　$i<0$ でなければ手順 2 へ。

３．提案方式

３．１　埋め込み不可画素の取り扱い

埋め込みが可能な画素には従来通りに情報を埋めていく。従来方式では、埋め込み不可能画素には復元情報を用いていたが、提案方式では、誤り訂正符号を用いる。埋め込み不可能画素の最下位 bit に図 2 のように EXOR 演算で”1”を付加することで誤りとして捉える。

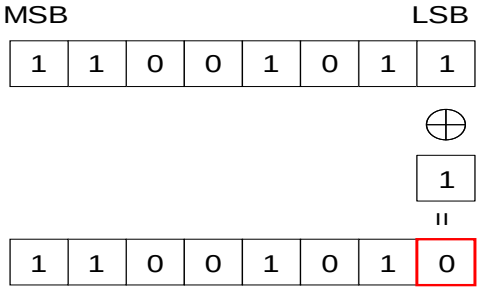

図 2：誤りを発生させるイメージ

符号化率を予め定め、以下に示す図 3 のように情報部分とパリティ部分を決める。

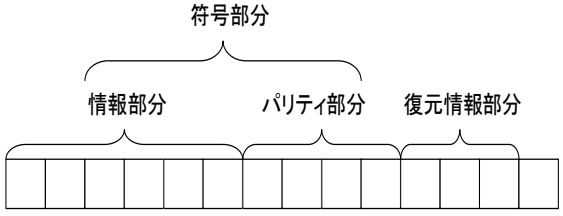

図 3：符号の構成イメージ

抽出方法は情報の抽出と原画素への復元を行いながら、パリティを抽出していき、抽出したパリティと情報部分の最下位 bit とで復号を行い、埋め込み不可能画素を特定する。

３．２　提案方式の埋め込み

提案方式は、従来方式の埋め込み不可能画素について着目し、新たな処理を加えることで、埋め込み可能画素を増やす。その画素と埋め

込み不可能画素に対して、従来方式の復元情報の方式を用いることで、埋め込み可能画素の増加と、誤り率の低減を実現し、冗長度を少なくする方式である。埋め込みが可能と判定される場合は、式(1),(2)を同時に満たす式(12)であり、それ以外の式(13)は埋め込みが不可能な画素である。

$$0 \le (n+1)x_i - nx_{i+1} \le L - n \quad \cdots (12)$$

$$x_i < \frac{n}{n+1} x_{i+1} \quad , \frac{L-n+nx_{i+1}}{n+1} < x_i \quad \cdots (13)$$

画素値 x_i, x_{i+1} は 0 から L までの変数であるが、図 4 のように埋め込み不可能な画素の画素値を±A することで、情報の埋め込みが不可能だった画素が埋め込み可能になるのではないかと考えた。

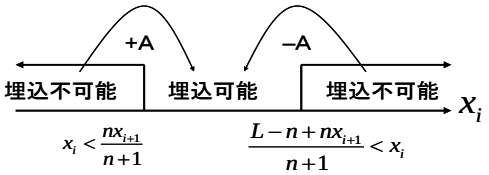

図 4 ：埋込可能画素への数論変換のイメージ

情報の埋め込み・抽出の手順は従来方式と同様であるが、変更点も含め、説明していく。

[手順 1]　$i := 0$

[手順 2]　式(1)、式(2)を同時に満たす場合は(a)、満たさない場合は(b)の処理へ。

$$0 \le (n+1)x_i - nx_{i+1} \le L - n \quad \cdots (14)$$

(a) 式(15)によって x_i の画素値を y_i とする。

$$y_i = (n+1)x_i - nx_{i+1} \quad \cdots (15)$$

(b) ここで、情報の埋め込みが不可能と判定された画素を式(16),(17)のように埋め込みが可能なるための処理を行う。さらに情報を抽出する際に以下の①と②のどちらの処理かがわかるようにあらかじめ変換する画素値 x_i の範囲を決めておき、設定値 t で判断する。

① $y_i > L - n$ かつ $(n+1)(x_i - A) - nx_{i+1} \ge t$ であり、$0 \le (n+1)(x_i - A) - nx_{i+1} \le L - n$ ならば、式(16)のように変換を行う。

$$y_i = (n+1)(x_i - A) - nx_{i+1} \quad \cdots (16)$$

② $y_i < 0$ かつ $(n+1)(x_i + A) - nx_{i+1} < t$ であり、$0 \le (n+1)(x_i + A) - nx_{i+1} \le L - n$ ならば、式(17)のように変換を行う。

$$y_i = (n+1)(x_i + A) - nx_{i+1} \quad \cdots (17)$$

①、②の処理でそれでも埋め込みが不可能である場合(c)の処理へ。

(c)原画素のまま保持する。

$$y_i = x_i \quad \cdots (18)$$

[手順 3]　それぞれの画素を分類し終えたら、(a)と(b)の変換した画素に式(19)のように情報を埋めていく。

$$y_i' = y_i + w_i \quad \cdots (19)$$

ここで、(a),(b)の処理を区別するために(b)の処理をした画素は式(20)のように情報を埋め終えた後に、従来方式のように復元情報を用いることで(a)の処理と区別する。式(21)のように情報を埋め終えた画素から復元情報を生成し、式(22)のように変換する。

$$y_i' = (n+1)(x_i \pm A) - nx_{i+1} + w_i \quad \cdots (20)$$

$$c_i = y_i' + nx_{i+1} \bmod (n+1) \quad \cdots (21)$$

$$y_i'' = y_i' - c_i \quad \cdots (22)$$

このような処理をする理由として、(a)の処理と区別する以外に冗長度的な観点から考えると、情報の埋め込みができない画素が 1 画素存在すると、その埋め込めない画素も含め、冗長な画素が平均 2.1 画素発生していた従来方式に対して、提案方式は情報の埋め込みができない画素が埋め込みが可能になっている上、それを表すために平均 1.1 画素でよいので、より冗長度が少なくなるからである。

[手順 4]　(c)の画素については、３．１のように誤り訂正符号を用いる。

３．３　抽出方法

抽出方法も従来方式と同様であるが、変更点も含め、説明していく。

[手順 1]　$i := N-1$

[手順 2]　式(23)を満たす場合、処理(b)の画素であり、満たさない場合は処理(a)の画素である。

$$y_i + nx_{i+1} \equiv 0 \bmod (n+1) \quad \cdots (23)$$

式(24)のように情報 w_i を抽出していき、式(25)から y_i を求める。式(23)を満たさない場合は、(i)へ、満たす場合は(ii)のように原画像の画素値 x_i を求めていく。

$$w_i + y_i + nx_{i+1} \bmod (n+1) = w_i \quad \cdots (24)$$

$$y_i = y_i' - w_i \quad \cdots (25)$$

(i)　$y_i + nx_{i+1} \neq 0 \bmod (n+1)$ の場合

$$x_i = \frac{y_i + nx_{i+1}}{n+1} \quad \cdots (26)$$

(ii)　$y_i + nx_{i+1} \equiv 0 \bmod (n+1)$ の場合

y_i と t の大小関係から以下の①、②の処理を行ない、原画像の画素値 x_i を求める。

① $y_i \geq t$ の場合は $y_i = (n+1)(x_i - A) - nx_{i+1}$ より同様に式(24),(25)で情報の抽出、y_i への変換を行い、式(27)のように原画素に復元する。

$$x_i = \frac{y_i + nx_{i+1}}{n+1} + A \quad \cdots (27)$$

② $y_i < t$ の場合は $y_i = (n+1)(x_i + A) - nx_{i+1}$ より①と同様に情報を抽出し、式(28)のように原画素に復元する。

$$x_i = \frac{y_i + nx_{i+1}}{n+1} - A \quad \cdots (28)$$

ここで、従来方式は、埋め込んだ情報の抽出と原画素への復元を同時に行っていくが、提案方式はパリティ部分まで抽出を行い、情報部分の下位 1bit と抽出したパリティとで復号を行う。復号を行う際、埋め込みができない画素には誤りが発生するので、訂正することでそれを特定し、原画素へ復元する。

４．評価

４．１評価方法

実験には、図 5、図 6、図 7 に示す 256×256 画素の 8bit/画素の濃淡画像の画像を用いた。秘密情報として、擬似乱数を用いた。この擬似乱数は rand()関数によって生成したものである。本研究は、可逆性を保つため、符号を構成するにあたり、発生させた誤りを完全に訂正できるよう、パリティを確保した上で、情報の埋め込み容量について検討した。また、埋め込み容量や各パラメータの算出方法を式(29)~式(31)として以下に示す。さらに、以降に式で使う文字を次のように定義する。

(N：全画素数、 s ：画像の縦の画素数、X：埋め込み可能画素数、Y：埋め込み不可画素数、Z：埋め込みが不可能から可能になった画素に対して、使用した復元情報の画素数、A：パリティ部分の画素数、K：情報部分の画素数、n : n 個の要素からなる埋め込む情報)

図 5　lena

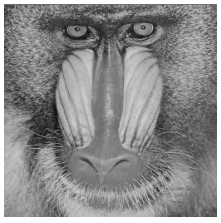

図 6 mandrill

図 7　girl

$$\text{符号化率} = \frac{K \times 1bit}{K \times 1bit + A \times 3bit} \quad \cdots (29)$$

$$\text{誤り率} = \frac{Y}{K \times 1bit + A \times 3bit} \quad \cdots (30)$$

$$\text{埋め込み容量[bpp]} = \frac{(X - Y - Z - A - s)}{N} \times \log_2 n \quad \cdots (31)$$

４．２　評価結果

提案方式の結果を示す前に設定値Aに対する結果及び考察を行う。各対象画像における提案方式2の設定値Aに対する情報の埋め込みができない画素から可能になった画素数についてのグラフを図 9 として以下に示す。t の値は最大画素値の半分である t=127 と固定した。

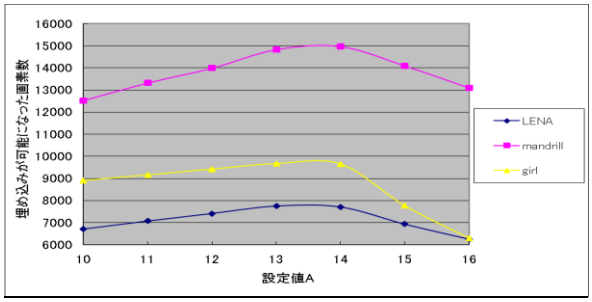

図 9：設定値 A と埋め込み可能画素の関係

図 9 の結果で最も埋め込み可能な画素が増加した A の値を評価に用いる。また、評価に用いる符号は LDPC 符号を用いた。理由としては符号長が長い場合にシャノン限界に迫る性能を持ち、様々な符号長、符号化率の符号を容易に構成することできるという特徴があるからである。シミュレーション結果を表３に各画像の 8bit/画素の濃淡画像に対する従来方式の最大の埋め込み容量[bpp]と n=8 のときの埋め込み容量[bpp]、また、表３のシミュレーションを行った符号化率から式(31)より算出した提案方式の埋め込み容量[bpp]の結果を表４に示す。

表３　LDPC 符号のシミュレーション結果

対象画像	lena	mandrill	girl
誤り率	0.0206	0.0221	0.0131
シミュレーション符号長	12000	12000	12000
シミュレーション符号化率	0.700	0.750	0.700
ブロック誤り率	0/1000000	0/1000000	0/1000000

表４　埋め込み容量の結果

対象画像	従来方式の最大の埋込容量[bpp]	従来方式(n=8)[bpp]	提案方式(n=8)[bpp]
lena	1.724(n=6)	1.690	1.694
girl	1.894(n=6)	1.816	1.888
mandrill	1.096 (n=3)	0.360	0.368

上記の結果より、提案方式(n=8)については、従来方式(n=8)の埋め込み容量より上回る結果が得られた。

５．まとめ

従来方式の情報の埋め込みができていないところに着目し、情報を埋め込む前の変換の時点で画素値自体に微量な変化を加えることでより、情報の埋め込みが可能な画素を増加させ、増加した分の処理は従来方式の復元情報の処理を用いた。その結果、全体的に埋め込みができない画素が減るので、その埋め込みができない画素を誤りと捉えることで、より低い誤り率にすることができ、それに用いるパリティも少なくなると考え、この方式を提案した。しかし、画像の画素値に依存することもあり、埋め込みができない画素が多すぎると、誤り率も高くなり結果的に従来方式より冗長な画素が増える結果となった。

参考文献

[1] D.Coltuc, “IMPROVED CAPACITY REVERSIBLE WATERMARKING”

[2]Masaaki FUJIYOSHI, Shuji SATO, Hong Lin JIN, and Hitoshi KIYA, “A LOCATION-MAP FREE REVERSIBLE DATA HIDING METHOD USING BLOCK-BASED SINGLE PARAMETER”

[3]Shaowei Weng, Yao Zhao, Jeng-Shyang Pan, and Rongrong Ni, “A NOVEL REVERSIBLE WATERMARKING BASED ON AN INTEGER TRANSFORM