

確率論的観点からの画像割符の定式化 (第2報)

樋口 政和*1 川崎 秀二*2 ガンバ ジョナ*2 小池 淳*3 村上 仁己*4

A Formulation of Visual Cryptography from Stochastic Viewpoint (Part II)

Masakazu HIGUCHI*1 Shuji KAWASAKI*2 Jonah GAMBA*2
Atsushi KOIKE*3 Hitomi MURAKAMI*4

ABSTRACT: In this paper, we consider to formulate an image data hiding scheme based on error diffusion. By using the scheme, visual patterns are embedded in a halftone image without affecting its perceptual quality depending on a halftone key image. The scheme has the feature of visual cryptography with respect to extracting of the embedded patterns, i.e., when we print the two halftone images onto transparencies and stack them together, the embedded patterns are visible by human visual system without any special electronic calculation. We propose a formulation for the scheme in the view of a stochastic analysis. The idea is basic, but theoretical studies by formulating is important trial in this field.

Keywords: Data hiding, Visual cryptography, Halftone image, Error diffusion, Probability theory

(Received October 17, 2011)

1. はじめに

視覚復号型暗号技術は、人間の視覚特性を利用した画像暗号化の技術である。その方式では、秘匿画像を複数の画像に分割し、それらを暗号化する。秘匿画像は暗号化された画像から電子的な計算なしで視覚的に復号することが可能となる。近年、その技術を画像情報埋め込み技術に応用した研究が盛んに行なわれている。画像情報埋め込み技術は、一般に1枚の秘匿画像の情報を n 枚の別の画像の中に埋め込む技術であるが、この「情報の埋め込み」を視覚復号型暗号技術の考えを利用して行い、秘匿画像が n 枚の画像に「暗号化」されたと考えるのである。秘匿画像は、その「暗号化」された n 枚の画像のうちの任意の k 枚の画像を重ね合わせる、すなわち重畳することによって光学的に再現することができる。本稿では、この技術を画像割符と呼ぶ。

先行研究は以下の通りである。視覚復号型暗号技術は Noar と Shamir によって初めて提案された³⁾。また、画像

割符に関しては、複数の疑似濃淡画像に秘匿画像の情報を埋め込む研究が主流であり、秘匿画像として、 F_u と A_u は2値、3値の簡単な文字画像を、古賀と山本はカラー画像を取り扱っている^{4),6)}が、大部分の研究者はグレイスケール値の画像を取り扱っている^{5),7)-12)}。疑似濃淡画像の生成には主に誤差拡散法¹⁾が利用されている。誤差拡散法の基本原理は2次元デルタ-シグマ変調により量子化誤差を高域側に変調することである。その結果、量子化の影響を比較的目的に付きにくい形で処理でき、自然な疑似濃淡画像を生成することができる。KDDI 研究所の明堂らは、2枚の白黒2値疑似濃淡画像から秘匿画像を高品質に再現する手法を開発した⁷⁾。著者らは、明堂らの手法にヒストグラム修正型の輝度変換と入力画像に応じた輝度変換パラメータの自動調整を取り入れることで、明堂法よりも秘匿画像を主観的に高品質に再現することが可能な手法を提案した⁸⁾⁻¹²⁾。

画像割符において、生成される疑似濃淡画像とそれらから再現される秘匿画像の品質、入力画像の特徴と秘匿画像の再現性の関係、などを理論的に検証するためには、提案された手法が理論的に定式化されていることが望ましい。しかしながら、先行研究では手法の理論的な定式化は行われておらず、実験的観点からの評価のみであった。これは、画像

*1: 情報科学科博士研究員

*2: 情報科学科ユビキタス工学研究室客員研究員

*3: 情報科学科教授

*4: 情報科学科教授 (hi-murakami@st.seikei.ac.jp)

割符の処理には、不確定な要素が含まれており、確定的な定式化は困難であるためと考えられる。画像割符では、例えば秘匿画像の明るい個所はその再現画像においても明るくなるように疑似濃淡画像上の対応する個所付近の白と黒の画素の割合を調整するといった処理が行われる。すなわち、画素の明暗に応じて処理が異なるということであり、具体的に画像が与えられれば処理後の結果が確定するが、定式化の段階ではそれは不確定である。また、誤差拡散法は前段の画素での処理結果が後段の画素での処理結果に影響を及ぼす動的なシステムであり、これもまた不確定な要素を含んでいる。このような状況に対して確定的な定式化を行おうとすると非常に複雑なものになってしまう。このように、条件に応じて異なる状況や動的な振る舞いを理論モデルに組み込むためには、確率的な記述が有効であると考えられる。

筆者らは、これまでの研究において、Fu と Au によって提案された画像割符の手法に対して確率論的観点からの定式化を与えた^{13),14)}。Fu と Au の手法は比較的簡単な着想の下で構成されているにも関わらず、高いパフォーマンスが得られる手法であるため、画像割符の定式化の足掛かりとしてこれを選んだ。

本稿では、Fu と Au の手法に基づいて構成されている明堂法に対して確率論的観点からの定式化を試みる。

本稿の構成は以下の通りである。第 2 節では、明堂法について述べる。第 3 節においては、明堂法に対する確率論的観点からの定式化を提案する。最後に第 4 節にて、本稿を纏める。

2. 対象手法の概要

2.1 処理フローチャート

明堂法の流れを図 1 に示す。入力画像は 3 枚のグレースケール濃淡画像である。疑似濃淡画像元の 2 枚のグレースケール濃淡画像をそれぞれ G1, G2 とし、同じくグレースケール濃淡を持つ秘匿画像を S とする。明堂法では、前処理として G1 と G2 および S に輝度変換を施し、得られた変換後画像 G1' と G2' および S' に割符処理を行う。まず、G1' を誤差拡散法により疑似濃淡画像に変換する。それを一枚目の疑似濃淡画像 W1 とする。次に、W1 と S' の情報を考慮しながら G2' を誤差拡散法により疑似濃淡画像に変換し、得られた画像を二枚目の疑似濃淡画像 W2 とする。手法の評価は W1 と W2 を重畳して得られる白黒 2 値の画像 C に対して行う。評価方法としては S と C の PSNR (Peak Signal-to-Noise Ratio) などが用いられる。なお、以後、画像 X の k 番目の画素における輝度値を x_k で表す。また、輝

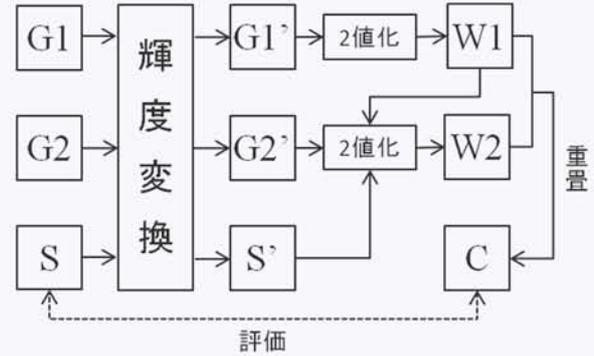


図 1 明堂法のフローチャート

度値は 0 から 1 までの連続階調値をとるものとする。0 は黒を表し、1 は白を表す。

2.2 誤差拡散法

多階調の画像を 2 階調の画像に変換するには、量子化を行う必要があるが、それには必ず量子化誤差が伴う。したがって、高品位な疑似濃淡画像を生成するには、量子化誤差を視覚的に目障りにならないように制御する必要がある。誤差拡散法の基本原理は人間の視覚特性を考慮して、量子化誤差を高域に変調することである。誤差拡散法の構成は 2 次元デルタ-シグマ変調とみなせるので、この処理により、量子化誤差を高域側に変調することができる。その結果、量子化の影響を比較的目につきにくい形で処理できる。

誤差拡散法に対する入力画像 X と出力画像 W の k 番目の画素の輝度値の関係は以下の通りである。

$$u_k = x_k + ER_k, \quad ER_k = \sum_{i \in J_k} j_i e_i, \quad (1)$$

$$u_k \rightarrow w_k = \begin{cases} 0 & (u_k < T) \\ 1 & (u_k \geq T) \end{cases}, \quad (2)$$

$$e_k = u_k - w_k. \quad (3)$$

ここで、 ER_k は蓄積誤差であり、 J_k は誤差拡散フィルタが適用される画像上の領域、 j_i は誤差拡散フィルタの重みを表す。なお、 $k=1$ のときの蓄積誤差は 0 である。T は量子化閾値である。処理は画像の左上のピクセルから右下のピクセルへ向けてラスタ走査により順次行われる。

2.3 秘匿画像の埋め込み処理

まず、白黒 2 値の重畳規則を図 2 に示す。一般に画素同士の重畳は各画素の輝度積で表され、白黒 2 値の場合は 0, 1 の論理積に対応する。

明堂法では秘匿画像の情報埋め込みは G2' の 2 値化の際に行われる。G2' に対する 2 値化において、処理中の画素の

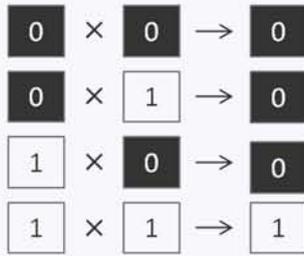


図2 白黒2値画素同士の重畳規則

輝度値 $g2'_k$ に蓄積誤差を加えた値 u_k が,

$$T - \Delta u < u_k < T + \Delta u \quad (4)$$

を満たしているときに、この画素の位置に秘匿画像の情報を埋め込む。ここで Δu は任意の正定数である。情報の埋め込み規則は以下の通りである。

まず、現在の処理位置の付近に対応する $W1$ と $W2$ の領域（輝度値が既知の領域）を重畳し得られる白黒領域にガウシアンフィルタの一部を適用することにより、その領域が仮にグレイスケール濃淡を持っていた場合の輝度値を推定する。その推定輝度値を d_k とすると、 d_k は以下で与えられる。

$$d_k = \sum_{i \in A_k} \alpha_i w1_i w2_i. \quad (5)$$

ここで、 A_k はガウシアンフィルタが適用される画像上の領域、 α_i はガウシアンフィルタの重みを表す。そして、 d_k と実際の S' の k 番目の輝度値 s'_k を参照し、以下のいずれかの処理を $w2_k$ に対して行う。

1. $d_k > s'_k$ のときは、推定輝度値を暗くするために、 $W1$ と $W2$ の k 番目の画素を重畳したときに必ず0となるように $W2$ の輝度値を調整する。具体的には、
 - (a) $d_k - s'_k > tb$ のとき、 $w1_k = 1$ かつ $w2_k = 1$ であれば、 $w2_k = \overline{w1_k}$ とする。
 - (b) $d_k - s'_k > tbu$ のとき、 $w1_k = 0$ かつ $w2_k = 0$ であれば、 $w2_k = \overline{w1_k}$ とする。
2. $d_k < s'_k$ のときは、推定輝度値を明るくするために、 $W1$ と $W2$ の k 番目の画素を重畳したときに確率 $1/2$ で1となるように $W2$ の輝度値を調整する。具体的には、
 - (a) $s'_k - d_k > td$ のとき、 $w1_k = 1$ かつ $w2_k = 0$ であれば、 $w2_k = w1_k$ とする。
 - (b) $s'_k - d_k > tdu$ のとき、 $w1_k = 0$ かつ $w2_k = 1$ であれば、 $w2_k = w1_k$ とする。
3. 1(a), 1(b), 2(a), 2(b) 以外のときは、 $w2_k$ は誤差拡散法の量子化によって得られた値とする。

パラメータ tb, tbu, td, tdu は任意の正定数であり、 d_k と s'_k が異なると判断される閾値である。 d_k と s'_k の差の絶対値が各パラメータ以下のときは、 d_k と s'_k は等しいと見なされ、 $w2_k$ に対しては何も処理は行われない。 d_k と各パラメータの関係は例えば図3のようになる。この埋め込み規則によ

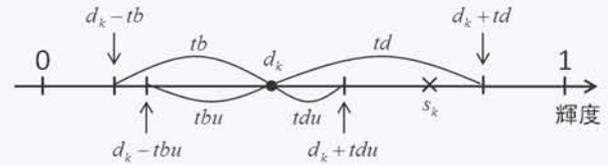


図3 推定輝度値とパラメータの関係の一例

り、重畳画像 C における微小領域の擬似輝度値が S' の対応する領域の平均輝度値に近づき、その結果、 S に近い画像を C によって再現することが可能となる。

2.4 適用例

明堂法の適用例を図4に示す。図4より、擬似濃淡画像

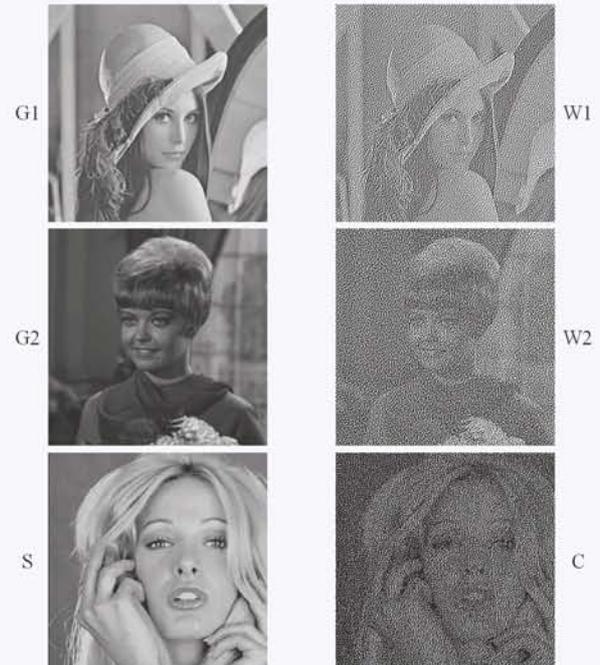


図4 明堂法の適用例

$W1$ と $W2$ は高品質に生成出来ていることが分かる。また、重畳画像 C も良好に秘匿画像 S を再現出来ている。この例では、 $G1$ と $G2$ および S に施す輝度変換として、アフィン型の変換を用いている。 $G1$ と $G2$ には $x' = 0.45x + 0.275$ なる変換を、 S には $x' = 0.45x$ なる変換を施している。 x は処理画像のある画素における輝度値を表す。また、 $G1'$ と $G2'$ の2値化と情報埋め込みに関するパラメータは $T = 0.5$, $\Delta u = 0.067$, $tb = td = \alpha_1/2$, $tbu = tdu = \alpha_1/4$ による。

設定している。ただし、 α_1 は着目画素に対するガウシアンフィルタの係数を表す。

3. 対象手法の定式化

3.1 前準備

本節では、統計確率的な解析²⁾を用いることにより、明堂法を定式化する。同手法において、入力画像に前処理として輝度変換が施されているが、これは定式化の本質には関係しないので、ここでは省略することにする。もし前処理も含めた解析が必要であれば、定式化の際に現れる各種入力画像の画素の輝度値 x を

$$x' = Tr(x) \quad (6)$$

によって変換して得られた値 x' に置き換えれば良い。ここで Tr は適当な画像変換を表す。

本稿では、画像の各画素の輝度値を確率変数と見なす。すると、割符処理の際に現れる各種変数は、画像の画素の輝度値に依存するので、それらもまた確率変数と見なすことができる。画像は画素の輝度相対度数分布により特徴付けられ、画像の画素の輝度値に対応する確率変数はそれから得られる確率密度関数に従う。理論的には、その確率密度関数と輝度相対度数分布は同じものとなる。なぜなら、輝度値は区間 $[0, 1]$ 上の連続値を取るからである。従って、割符処理中の各種変数に対応する確率変数もまた確率密度関数を持つ。なお、以後、確率変数 \mathcal{X} が持つ確率密度関数を $f_{\mathcal{X}}$ と表す。

3.2 擬似濃淡画像の統計確率的解析

この小節では、擬似濃淡画像の白黒画素の分布について考察する。擬似濃淡画像は G1 と G2 に誤差拡散法を適用することで生成される。そこで、誤差拡散法の際に生じる誤差を確率的に記述し、W1 と W2 の白黒分布の挙動を明らかにする。

誤差拡散法に現れる各種変種 u_k , ER_k , e_k に対応する確率変数をそれぞれ U_k , \mathcal{ER}_k , \mathcal{E}_k とすると、式 (1) より、

$$U_k = \mathcal{X} + \mathcal{ER}_k, \quad \mathcal{ER}_k = \sum_{i \in J_k} j_i \mathcal{E}_i \quad (7)$$

の関係をj得る。ここで、 \mathcal{X} は処理画像の画素の輝度値に対応する確率変数を表す。2つの確率変数の和に対する確率密度関数はそれぞれの確率変数に対する確率密度関数の畳み込みで与えられることから、 U_k に対する確率密度関数は、

$$f_{U_k}(u) = \int_{-\infty}^{\infty} f_{\mathcal{X}}(u-y) f_{\mathcal{ER}_k}(y) dy \quad (8)$$

となる。また、式 (7) の誤差項において、任意の $i \in J_k$ に対する $j_i \mathcal{E}_i$ の確率密度関数は、

$$f_{j_i \mathcal{E}_i}(e) = f_{\mathcal{E}_i}(\frac{1}{j_i} e) \quad (9)$$

で与えられるので、これと確率変数の和と畳み込みの関係を用いれば、 \mathcal{ER}_k に対する確率密度関数は、

$$\begin{aligned} f_{\mathcal{ER}_k}(e) &= \int_R \int_R \cdots \int_R f_{\mathcal{E}_{i'}}(\frac{1}{j_{i'}}(e - \sum_{\substack{i \in J_k \\ i \neq i'}} y_i)) \prod_{\substack{i \in J_k \\ i \neq i'}} f_{\mathcal{E}_i}(\frac{1}{j_i} y_i) dy_i \\ & \quad (10) \end{aligned}$$

となる。ここで、多重積分は $|J_k| - 1$ 回の積分である。 \mathcal{E}_k に対する確率密度関数に関しては、G1 と G2 とで導出方法が異なる。それは、G1 には通常の誤差拡散法を適用するのに対し、G2 は情報埋め込み処理を含めた誤差拡散法を適用するからである。導出方法はそれぞれ以下の通りとなる。なお、 s_k , w_{1k} , w_{2k} に対応する確率変数をそれぞれ \mathcal{S} , \mathcal{W}_{1k} , \mathcal{W}_{2k} とする、

G1 の場合については、 u_k の値は以下の2通りの場合が考えられるので、それぞれの場合について誤差の分布を調べると、

Case 1. $-\infty < u_k < T$ のとき

w_{1k} は必ず0となり、式 (3) より $e_k = u_k$ となる。よって、上記の u_k の範囲を e_k で記述し直せば、 $-\infty < e_k < T$ となり、これを満たす e_k に対応する確率変数 $\mathcal{E}_k^{(1)}$ の分布は U_k の分布と等しくなるということである。すなわち、

$$f_{\mathcal{E}_k^{(1)}}(e) = f_{U_k}(e), \quad -\infty < e < T \quad (11)$$

である。

Case 2. $T \leq u_k < \infty$ のとき

w_{1k} は必ず1となり、式 (3) より $e_k = u_k - 1$ となる。よって、上記の u_k の範囲を e_k で記述し直せば、 $T - 1 \leq e_k < \infty$ となり、これを満たす e_k に対応する確率変数 $\mathcal{E}_k^{(2)}$ の分布は $U_k - 1$ の分布と等しくなるということである。すなわち、

$$\begin{aligned} f_{\mathcal{E}_k^{(2)}}(e) &= f_{U_k-1}(e) \\ &= f_{U_k}(e+1), \quad T-1 \leq e < \infty \end{aligned} \quad (12)$$

である。

よって、式 (11) と (12) より、 \mathcal{E}_k の確率密度関数は、

$$f_{\mathcal{E}_k}(e) = f_{\mathcal{E}_k^{(1)}}(e) + f_{\mathcal{E}_k^{(2)}}(e) \quad (13)$$

と求めることができる。

G2 の場合については、 u_k の値は以下の4通りの場合が考えられるので、それぞれの場合について誤差の分布を調べると、

Case 1. $-\infty < u_k \leq T - \Delta u$ のとき

w_{2k} は必ず 0 となり、式 (3) より $e_k = u_k$ となる。よって、上記の u_k の範囲を e_k で記述し直せば、 $-\infty < e_k \leq T - \Delta u$ となり、これを満たす e_k に対応する確率変数 $\mathcal{E}_k^{(1)}$ の分布は U_k の分布と等しくなるということである。すなわち、

$$f_{\mathcal{E}_k^{(1)}}(e) = f_{U_k}(e), \quad -\infty < e \leq T - \Delta u \quad (14)$$

である。

Case 2. $T + \Delta u \leq u_k < \infty$ のとき

w_{2k} は必ず 1 となり、式 (3) より $e_k = u_k - 1$ となる。よって、上記の u_k の範囲を e_k で記述し直せば、 $T + \Delta u - 1 \leq e_k < \infty$ となり、これを満たす e_k に対応する確率変数 $\mathcal{E}_k^{(2)}$ の分布は $U_k - 1$ の分布と等しくなるということである。すなわち、

$$\begin{aligned} f_{\mathcal{E}_k^{(2)}}(e) &= f_{U_k-1}(e) \\ &= f_{U_k}(e+1), \\ T + \Delta u - 1 &\leq e < \infty \end{aligned} \quad (15)$$

である。

Case 3. $T - \Delta u < u_k < T$ のとき

通常の誤差拡散法であれば $w_{2k} = 0$ となるが、情報埋め込みの規則によっては $w_{2k} = 1$ となる場合もあり得る。従って、 w_{2k} の値として期待値を用いることにする。ここで、

$$P_x^{S<} = P(S < x) = \int_0^x f_S(s) ds \quad (16)$$

$$P_x^{S>} = P(S > x) = \int_x^1 f_S(s) ds \quad (17)$$

$$P_b^{Wt_k} = P(Wt_k = 0), \quad t = 1, 2 \quad (18)$$

$$P_w^{Wt_k} = P(Wt_k = 1), \quad t = 1, 2 \quad (19)$$

とおく。ただし、 $P(A)$ は事象 A が起こる確率を表す。 w_{2k} の期待値は、

$$\langle w_{2k} \rangle = P_b^{W2k} \cdot 0 + P_w^{W2k} \cdot 1 \quad (20)$$

で与えられる。情報埋め込み規則より、式 (20) 中の P_w^{W2k} は、

$$P_w^{W2k} = P_{(d_k)-tbu}^{S<} P_b^{W1k} + P_{(d_k)+td}^{S>} P_w^{W1k} \quad (21)$$

となり、 P_b^{W2k} は、

$$\begin{aligned} P_b^{W2k} &= P_{(d_k)-tbu}^{S<} P_w^{W1k} + P_{(d_k)+td}^{S>} P_b^{W1k} \\ &\quad + P_{(d_k)+td}^{S<} - P_{(d_k)-tbu}^{S<} \end{aligned} \quad (22)$$

となる。ただし、推定輝度値は、その期待値を用い、

$$\langle d_k \rangle = \sum_{i \in A_k} \alpha_i \langle w_i \rangle, \quad (23)$$

$$\begin{aligned} \langle w_i \rangle &= (1 - P_w^{W1i} P_w^{W2i}) \cdot 0 \\ &\quad + (P_w^{W1i} P_w^{W2i}) \cdot 1 \end{aligned} \quad (24)$$

で与えられる。式 (3) の w_k を式 (20) で置き換え、上記の u_k の範囲を e_k で記述し直せば、 $T - \Delta u - \langle w_{2k} \rangle < e_k < T - \langle w_{2k} \rangle$ となり、これを満たす e_k に対応する確率変数 $\mathcal{E}_k^{(3)}$ の分布は $U_k - \langle w_{2k} \rangle$ の分布と等しくなるということである。すなわち、

$$\begin{aligned} f_{\mathcal{E}_k^{(3)}}(e) &= f_{U_k - \langle w_{2k} \rangle}(e) \\ &= f_{U_k}(e + \langle w_{2k} \rangle), \\ T - \Delta u - \langle w_{2k} \rangle &< e < T - \langle w_{2k} \rangle \end{aligned} \quad (25)$$

である。

Case 4. $T \leq u_k < T + \Delta u$ のとき

通常の誤差拡散法であれば $w_{2k} = 1$ となるが、情報埋め込みの規則によっては $w_{2k} = 0$ となる場合もあり得る。Case 3 と同様に w_{2k} の期待値を考えると、それは式 (20) で与えられる。情報埋め込み規則より、式 (20) 中の P_b^{W2k} は、

$$P_b^{W2k} = P_{(d_k)-tb}^{S<} P_w^{W1k} + P_{(d_k)+tdu}^{S>} P_b^{W1k} \quad (26)$$

となり、 P_w^{W2k} は、

$$\begin{aligned} P_w^{W2k} &= P_{(d_k)-tb}^{S<} P_b^{W1k} + P_{(d_k)+tdu}^{S>} P_w^{W1k} \\ &\quad + P_{(d_k)+tdu}^{S<} - P_{(d_k)-tb}^{S<} \end{aligned} \quad (27)$$

となる。式 (3) の w_k を式 (20) で置き換え、上記の u_k の範囲を e_k で記述し直せば、 $T - \langle w_{2k} \rangle \leq e_k < T + \Delta u - \langle w_{2k} \rangle$ となり、これを満たす e_k に対する確率変数 $\mathcal{E}_k^{(4)}$ の分布は $U_k - \langle w_{2k} \rangle$ の分布と等しくなるということである。すなわち、

$$\begin{aligned} f_{\mathcal{E}_k^{(4)}}(e) &= f_{U_k - \langle w_{2k} \rangle}(e) \\ &= f_{U_k}(e + \langle w_{2k} \rangle), \\ T - \langle w_{2k} \rangle &\leq e < T + \Delta u - \langle w_{2k} \rangle \end{aligned} \quad (28)$$

である。

よって、式 (14), (15), (25), (28) より、 \mathcal{E}_k の確率密度関数は、

$$f_{\mathcal{E}_k}(e) = f_{\mathcal{E}_k^{(1)}}(e) + f_{\mathcal{E}_k^{(2)}}(e) + f_{\mathcal{E}_k^{(3)}}(e) + f_{\mathcal{E}_k^{(4)}}(e) \quad (29)$$

と求めることができる。

以上により、誤差拡散法において k 番目以前の処理で発生した誤差分布と処理画像の画素の輝度分布から U_k の確

率密度関数を計算することができ、それを用いれば、W1の k 番目の画素が白になる確率は、

$$P_w^{W1k} = \int_T^\infty f_{U_k}(u) du \quad (30)$$

で求めることができる。また、W2の k 番目の画素が白になる確率は、

$$\begin{aligned} P_w^{W2k} &= P(T - \Delta u < U_k < T) P_{(d_k)-tb}^{S<} P_b^{W1k} \\ &\quad + P(T - \Delta u < U_k < T) P_{(d_k)+td}^{S>} P_w^{W1k} \\ &\quad + P(T \leq U_k < T + \Delta u) \cdot \\ &\quad \left(P_{(d_k)-tb}^{S<} P_b^{W1k} + P_{(d_k)+td}^{S>} P_w^{W1k} \right. \\ &\quad \left. + P_{(d_k)+td}^{S<} - P_{(d_k)-tb}^{S<} \right) \\ &\quad + P(U_k \geq T + \Delta u) \\ &= P_1 \int_{T-\Delta u}^T f_{U_k}(u) du \\ &\quad + P_2 \int_T^{T+\Delta u} f_{U_k}(u) du + \int_{T+\Delta u}^\infty f_{U_k}(u) du \end{aligned} \quad (31)$$

で求めることができる。ただし、

$$P_1 = P_{(d_k)-tb}^{S<} P_b^{W1k} + P_{(d_k)+td}^{S>} P_w^{W1k} \quad (32)$$

$$\begin{aligned} P_2 &= P_{(d_k)-tb}^{S<} P_b^{W1k} + P_{(d_k)+td}^{S>} P_w^{W1k} \\ &\quad + P_{(d_k)+td}^{S<} - P_{(d_k)-tb}^{S<} \end{aligned} \quad (33)$$

である。

3.3 重畳画像の統計確率的解析

この小節では、重畳画像の白黒画素の分布について考察する。CはW1とW2を光学的に重ね合わせるにより得られる。Cの画素が白になるのは、W1とW2の画素が共に白になる場合のみである。従って、Cの k 番目の画素の輝度値に対応する確率変数を C_k とすると、それが白になる確率は、

$$\begin{aligned} P_w^{Ck} &= P(C_k = 1) \\ &= P(T - \Delta u < U_k < T) P_{(d_k)+td}^{S>} P_w^{W1k} \\ &\quad + P(T \leq U_k < T + \Delta u) \cdot \\ &\quad P_{(d_k)-\min\{tb, tbu\}}^{S>} P_w^{W1k} \\ &\quad + P(U_k \geq T + \Delta u) P_w^{W1k} \\ &= P_w^{W1k} \left\{ P_{(d_k)+td}^{S>} \int_{T-\Delta u}^T f_{U_k}(u) du \right. \\ &\quad + P_{(d_k)-\min\{tb, tbu\}}^{S>} \int_T^{T+\Delta u} f_{U_k}(u) du \\ &\quad \left. + \int_{T+\Delta u}^\infty f_{U_k}(u) du \right\} \end{aligned} \quad (34)$$

で求めることができる。

4. まとめ

本稿では、明堂らにより提案された画像割符の手法について確率論的観点からの定式化を試みた。定式化の結果、疑似濃淡画像と重畳画像の輝度分布に関して、それらの確率的な挙動を理論的に記述することができた。これにより、例えば、疑似濃淡画像から高品質な重畳画像が得られるような入力画像セットの推定や画像割符のパフォーマンスに影響を及ぼす各種パラメータの最適化などが理論的に可能となる。

今回の定式化では、統計確率論における初歩的な手法を用いており、得られたモデルが実際の結果に即しているかをシミュレーションを行い検証する必要がある。そして、より洗練された着想に基づく定式化を行い、より高度な理論モデルとして昇華させていく。以上のことを今後の課題とし、本稿のまとめとする。

謝辞

本研究の一部は、戦略的研究基盤形成支援事業の援助を受けていることをここに記し、謝意を表します。

参考文献

- 1) R. A. Ulichney, "Digital halftoning", MIT Press, Cambridge, 1987.
- 2) C. W. Helstrom, "Probability and Stochastic Processes for Engineers 2 Sub edition", Macmillan Coll Div, 1991.
- 3) M. Noar, A. Shamir, "Visual Cryptography", Proc. Eurocrypt'94, pp.1-12, 1994.
- 4) H. Koga and H. Yamamoto, "Proposal of a lattice-based visual secret sharing scheme for color and gray-scale images", IEICE Transaction on Fundamentals, Vol.E81-A, No.6, pp.1262-1269, 1998.
- 5) M. Nakajima and Y. Yamaguchi, "Extended visual cryptography for natural images", Journal of WSCG, Vol.2, pp.303-310, 2002.
- 6) M. S. Fu, O. C. Au, "A novel method to embed watermark in different halftone images: data hiding by conjugate error diffusion (OHCED)", Proc. IEEE Int. Conf. on Multimedia and Expo, Vol.1, pp.609-612, 2003.
- 7) 明堂 絵美, 高木 幸一, 酒澤 茂之, 滝嶋 康弘, 「誤差拡散法を用いた自然画像埋め込み可能な割符生成方式」, IEICE Technical Report, SIP2006-2, IE2006-2, pp.7-12, 2006.
- 8) 會森 彩, 樋口 政和, 明堂 絵美, 川崎 秀二, 小池 淳, 村上 仁己, 「画像割符における埋め込み画像を高品質に復号するための輝度変換に関する検討」, 成蹊大学理工学研究報告, Vol.47, No.1, pp.67-73, 2010.

- 9) 会森 彩, 樋口 政和, 川崎 秀二, 小池 淳, 村上 仁己, 「画像割符における高品質復号画像生成のための輝度変換に関する考察」, ITE Technical Report, Vol.34, No.31, AIT2010-106, pp.53-56, 2010.
- 10) 樋口 政和, 會森 彩, 川崎 秀二, ガンバ ジョナ, 小池 淳, 村上 仁己, 「画像割符における輝度変換のパラメータ調整による秘匿画像高品質再現」, 成蹊大学理工学研究報告, Vol.47, No.2, pp.7-14, 2010.
- 11) M. Higuchi, A. Emori, S. Kawasaki, J. Gamba, A. Koike, H. Murakami, "Performance Evaluation of Visual Cryptography Schemes with Intensity Transformations for Gray-Scale Images", Proceedings of the 3rd WSEAS International Conference on Visualization, Imaging and Simulation: Advances in Visualization, Imaging and Simulation, pp.111-117, 2010.
- 12) M. Higuchi, A. Emori, S. Kawasaki, J. Gamba, A. Koike and H. Murakami, "Image Encryption Methods Using Intensity Transformations in Visual Cryptography", International Journal of Mathematics and Computers in Simulation, Issue 1, Vol.5, pp.61-68, 2011.
- 13) 樋口 政和, 會森 彩, 川崎 秀二, ガンバ ジョナ, 小池 淳, 村上 仁己, 「確率論的観点からの画像割符の定式化」, 成蹊大学理工学研究報告書, Vol.48, No.1, pp.63-68, 2011.
- 14) M. Higuchi, S. Kawasaki, J. Gamba, A. Koike and H. Murakami, "A Fundamental Conception to Formulate Image Data Hiding Scheme Based on Error Diffusion", Proceedings of the 2nd IEEEAM International conference on Applied Informatics and Computing Theory: Recent Researches in Applied Informatics, pp.162-166, 2011.