

## 確率論的観点からの画像割符の定式化

樋口 政和\*1 會森 彩\*2 川崎 秀二\*3 ガンバ ジョナ\*4 小池 淳\*5 村上 仁己\*6

A formulation of Visual Cryptography from Stochastic Viewpoint

Masakazu HIGUCHI\*1 Aya EMORI\*2 Shuji KAWASAKI\*3 Jonah GAMBA\*4  
Atsushi KOIKE\*5 Hitomi MURAKAMI\*6

**ABSTRACT:** In a kind of visual cryptography, a secret image is encrypted to plural share images. Then, we can reconstruct the secret image by using share images produced in secret image encoding scheme. In the case of two binary share images, the secret image is reconstructed by printing the two share images onto transparencies and stacking them together without any special electronic calculation. The conventional method based on error diffusion, which has been proposed by Fu and Au, can produce two high quality binary halftone share images from three gray-scale images and restore the secret image with rather high quality by decoding their share images. In this paper, we propose a formulation of the method in the view of a stochastic analysis.

**Keywords:** Visual cryptography, Halftone image, Error diffusion, Probability theory

(Received April 4, 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、暗号化された秘匿画像は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。本稿では、視覚復号型暗号技術として、画像割符と呼ばれる技術について議論する。これは、一般には、1枚の秘匿画像を割符画像と呼ばれる  $n$  枚の画像に暗号化する技術であり、その  $n$  枚のうちの任意の  $k$  枚の割符画像を重ね合わせる、すなわち重畳することによって元の秘匿画像を光学的に復号することができるという特徴をもつ。

先行研究として、Noar と Shamir は白黒 2 値のテキストのような簡単な画像を、白黒 2 値のランダムドットパターンを持つ  $n$  枚の画像に暗号化する手法を提案した<sup>3)</sup>。また、割符画像として自然画像のような意味のある白黒 2 値疑似濃淡画像を出力する手法の研究<sup>4)-9)</sup>も多数報告されている。

それらでは、割符画像を生成する際にハーフトーン技術<sup>1)</sup>が利用されている。ハーフトーン技術で代表的なものは、誤差拡散法であり、その基本原理は 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につきにくい形で処理でき、自然な白黒 2 値疑似濃淡画像を生成することができる。秘匿画像として、Fu と Au は 2 値、3 値の簡単な文字画像のような画像を取り扱っている<sup>6)</sup>が、現在はグレイスケール値の画像を取り扱う研究<sup>5), 7)-9)</sup>が主流である。また、カラー画像を秘匿画像として取り扱っている研究<sup>4)</sup>もある。明堂らは、自然画像のような 3 枚のグレイスケール値の画像から 2 枚の高品質な白黒 2 値の割符画像の高速生成を実現している<sup>7)</sup>。また、同手法では、3 枚の入力画像のうちの 1 枚は秘匿画像であり、生成される割符画像から比較的高品質にそれを再現することができる。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、主観評価で割符画像の品質は明堂法のそれと同程度だが、秘匿画像は明堂法よりも高品質に再現することができる手法を提案した<sup>8)-12)</sup>。

画像割符において、生成される割符画像とそれらから再現される秘匿画像の品質、入力画像による秘匿画像の再現性

\*1: 情報科学科博士研究員  
\*2: 理工学研究科理工学専攻修士学生  
\*3: 情報科学科ユビキタス工学研究室客員研究員  
\*4: 情報科学科ユビキタス工学研究室客員研究員  
\*5: 情報科学科教授  
\*6: 情報科学科教授 (hi-murakami@st.seikei.ac.jp)

の傾向, 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, 画像割符の処理には, 確率的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。通常の画像変換, 例えばフィルタ処理やリサイズなどは, 所望の条件から変換作用素を構成することで, 比較的容易に定式化が可能である。一方, 2値への変換などが絡む画像変換では, 通常の画像変換のような確定的な定式化は困難である。例えば, 画像の2値変換法である誤差拡散法では, 画像の各画素を2階調の値へ変換し, それによって生じた誤差を他の画素へ拡散させていくといった処理が行われる。このとき, 画像の画素値は処理が進むにつれ刻一刻と動的に変化していく。更に, 画素値の2値変換の際に生じる誤差は確定的には求まらない。それは, 各画素値の条件によって決まる。また, 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, 割符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。このときも, 割符画像の画素は至る所で動的に変化する。加えて, 画像の明るい個所, 暗い個所といった条件は確定的に定式化することは困難である。このように, 条件に応じて動的に変化する状況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。

本稿では,  $F_u$  と  $A_u$  によって提案された手法に基づき, 画像割符の確率論的観点からの定式化を試みる。 $F_u$  と  $A_u$  の手法は明堂らの手法の基礎となっており, 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。

本稿の構成は以下の通りである。第2節では, 明堂法の根幹を構成する  $F_u$  と  $A_u$  の手法について述べる。第3節においては,  $F_u$  と  $A_u$  の手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. 従来手法の概要

$F_u$  と  $A_u$  の手法の流れを図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。 $F_u$  と  $A_u$  は文献<sup>6)</sup>において, 秘匿画像として2値あるいは3値の文字などの簡単な画像を提案手法に適用しているが, グレースケール濃淡画像でも同手法は比較的高いパフォーマンスを発揮する。割符画像元の2枚のグレースケール濃淡画像をそれぞれ  $G_1$ ,  $G_2$  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。 $F_u$  と  $A_u$  の手法では, 前処理として  $G_1$  と  $G_2$  および  $S$  に輝度変換を施し, 得られた変換後画像  $G_1'$  と  $G_2'$  および  $S'$

に割符処理を行う。まず,  $G_1'$  を誤差拡散法により単なる白黒2値疑似濃淡画像に変換する。それを一枚目の割符画像  $W_1$  とする。次に,  $W_1$  と  $S'$  の情報を考慮しながら  $G_2'$  を誤差拡散法により白黒2値疑似濃淡画像に変換し, 得られた画像を二枚目の割符画像  $W_2$  とする。手法の評価は  $W_1$  と  $W_2$  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。

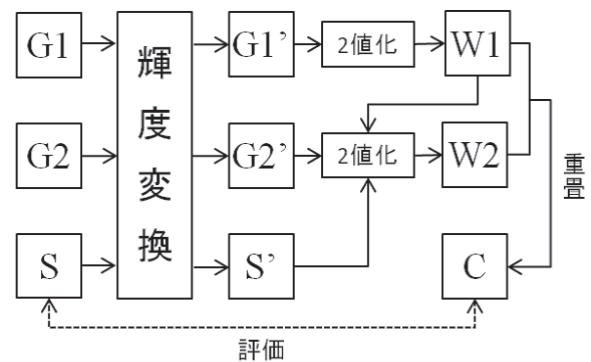


図1 従来法のフローチャート

なお, 以後,  $G_1$  と  $G_2$  および  $S$  の任意の画素における輝度値をそれぞれ  $g_{1k}$ ,  $g_{2k}$ ,  $s_k$  で表す。また, それぞれの輝度値は  $0 \sim 1$  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。

### 2.1 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。

量子化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。ラスタ走査において, 処理中の画素の輝度値を  $g_k$  とする。これに, 処理中の画素に到達するまでの各画素で生じた量子化誤差に誤差拡散フィルタの重みを乗じて蓄積したもの (蓄積誤差  $ER_k$ ) を加え, 得られた値  $u_k = g_k + ER_k$  を量子化閾値  $T$  の量子化器で量子化し, 2階調の輝度値  $w_k$  を得る。そして, 処理中の画素における量子化誤差  $e_k = u_k - w_k$  を求め, それを保持し次の画素に処理が移る。蓄積誤差  $ER_k$  は具体的には以下の

式で計算される.

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

ただし,  $J_k$  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.

## 2.2 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

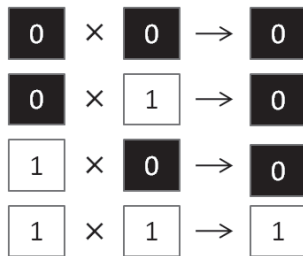


図2 白黒2値画素同士の重畳規則

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.

Fu と Au の手法では秘匿画像の情報埋め込みは画像 G2' の2値化の際に行われる. G2' のラスタ走査において, 処理中の画素の輝度値  $g2'_k$  に蓄積誤差を加えた値  $u_k$  が,

$$T - \Delta u < u_k < T + \Delta u \quad (2)$$

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  $\Delta u$  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, 輝度変換後の秘匿画像 S' の画素における輝度値  $s'_k$  を3階調の値に量子化する. そして, その値  $(s'_k)_{v3}$  を参照し,

- $(s'_k)_{v3} = 0$  (黒色) であれば,  $w2_k = \overline{w1_k}$  とする.
- $(s'_k)_{v3} = 0.5$  (灰色) であれば,  $w2_k$  は誤差拡散法の量子化によって得られた値とする.
- $(s'_k)_{v3} = 1$  (白色) であれば,  $w2_k = w1_k$  とする.

この埋め込み規則により,  $(s'_k)_{v3} = 0$  の場所, すなわち元の S' において暗い場所は, 重畳後は必ず黒となる.  $(s'_k)_{v3} = 1$  の場所, すなわち元の S' において明るい場所は, 重畳後は確率 1/2 で白となる.  $(s'_k)_{v3} = 0.5$  の場所, すなわち元の S' において中間的な明るさの場所は, 重畳後は確率 3/4 で黒となる. よって, 重畳画像 C は見た目では低階調のような画像になりやすい.

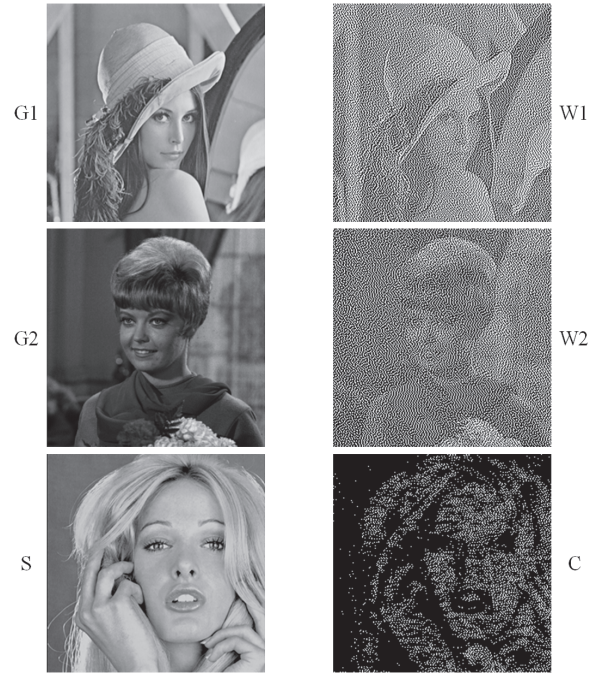


図3 従来法の適用例

## 2.3 適用例

Fu と Au の手法の適用例を図3に示す. 図3より, 割符画像 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 も概ね良好に秘匿画像 S を復号出来ている. 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.  $x$  と  $x'$  はそれぞれ画像のある画素における輝度値と変換後の輝度値を表す. S' の3値化に対する量子化閾値  $q_1, q_2$  はそれぞれ 0.25, 0.75 に設定している. 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それぞれ  $T = 0.5, \Delta u = 0.067$  としている.

## 3. 従来手法の定式化

本節では, 統計確率的な解析<sup>2)</sup>を用いることにより, Fu と Au の手法を定式化する. 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

$$x' = T(x)$$

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  $T$  は適当な画像変換を表す.

### 3.1 前準備

Fu と Au の手法の流れは以下の通りであった。まず入力画像 G1 を誤差拡散法によってあらかじめ 2 値画像 W1 に変換しておき、次の入力画像 G2 を同じく誤差拡散法によって 2 値化し W2 を生成する際に、処理中の画素において式 (2) が満たされれば、埋め込み規則を適用し、W2 の画素の輝度値を決定する。入力画像において、各画像が別の画像に変更されれば、当然その輝度分布も変化する。従って、各画像の輝度値はその輝度分布に従う確率的な変数と見なすことができる。画像 G2, S, W1, W2 の画素の輝度値をそれぞれ確率変数  $G2, S, W1, W2$  と表すこととし、 $G2$  と  $S$  はそれぞれ輝度分布密度関数  $f_{G2}(x)$  と  $f_S(x)$  に従うものとする。

また、画像に対する誤差拡散法の  $k$  番目の画素における処理の流れは以下の通りであった。

$$u_k = x_k + ER_k, \quad ER_k = \sum_{i \in J_k} j_i e_i, \quad (3)$$

$$u_k \rightarrow w_k = \begin{cases} 0 & (u_k < T) \\ 1 & (u_k \geq T) \end{cases}, \quad (4)$$

$$e_k = u_k - w_k, \quad (5)$$

ここで、 $x_k$  は画像の  $k$  番目の画素における画素値を表す。なお、 $k=1$  のときの蓄積誤差  $ER_1$  は 0 である。このとき、 $u_k, w_k, e_k$  も確率的に変動する値なので、それらを確率変数としてそれぞれ  $U_k, W_k, E_k$  と表すことにする。式 (4) より、 $W_k$  は  $U_k$  に依存するので

$$W_k = h(U_k)$$

と表現することが出来る。  $h$  は 2 値への量子化関数である。 $U_k, E_k$  が従う分布密度関数をそれぞれ  $f_{U_k}(u), f_{E_k}(e)$  とする。

これらの記号を用いれば、例えば、式 (2) が満たされる確率は

$$P(T - \Delta u < U_k < T + \Delta u) = \int_{T - \Delta u}^{T + \Delta u} f_{U_k}(u) du$$

と表すことが出来る。また、画像 S の画素が 3 値化によって黒、灰色、白となる確率はそれぞれ

$$P_0^S = P((S)_{v3} = 0) = P(0 \leq S < q_1) = \int_0^{q_1} f_S(x) dx,$$

$$P_{0.5}^S = P((S)_{v3} = 0.5) = P(q_1 \leq S < q_2) = \int_{q_1}^{q_2} f_S(x) dx,$$

$$P_1^S = P((S)_{v3} = 1) = P(q_2 \leq S \leq 1) = \int_{q_2}^1 f_S(x) dx$$

となり、画像 W1 の画素が白となる確率は

$$P_1^{W1} = P(W1 = 1) = \frac{(\text{画像 W1 中の白画素の総数})}{(\text{画像 W1 中の全画素数})}$$

と求めることが出来る。ただし、 $q_1$  と  $q_2$  は 3 値化への量子化閾値であり  $q_1 < q_2$  とする。

### 3.2 割符画像の統計確率的解析

この小節では、割符画像の白黒画素の分布について考察する。割符画像は入力画像 G1 と G2 に誤差拡散法を適用することで生成される。割符画像 W1 は誤差拡散法をそのまま G1 に適用して得られるため、その白黒分布は前小節のように容易に求めることが出来る。しかし、割符画像 W2 は情報埋め込み規則を考慮しながら誤差拡散法を適用し生成されるため、そのまま誤差拡散法を適用したときに得られる白黒分布とは異なる分布となり、それは秘匿画像 S と W1 に依存する。そこで、誤差拡散法により W2 を生成する際に生じる誤差を確率的に記述し、W2 の白黒分布の挙動を明らかにする。

前小節で定義した記号を用いると、誤差拡散法によって W2 の  $k$  番目の画素で生じる誤差は式 (5) より

$$E_k = U_k - W2_k = U_k - h(U_k) \quad (6)$$

と表すことが出来る。 $U_k$  の値としては以下の 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

$W2_k$  は必ず 0 となり、式 (6) 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、 $-\infty < E_k \leq T - \Delta u$  を満たす  $E_k$  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

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

である。

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

$W2_k$  は必ず 1 となり、式 (6) 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

$$T + \Delta u \leq E_k + 1 < \infty$$

$$T + \Delta u - 1 \leq E_k < \infty$$

となり、これを満たす  $E_k$  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

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

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  $W2_k = 0$  となるが、情報埋め込みの規則によっては  $W2_k = 1$  となる場合もあり得る。従って、 $W2_k$  の値として期待値を用いること

にする。  $W2_k$  の期待値は

$$\langle W2_k \rangle = \left( P_0^S P_1^{W1} + P_{0.5}^S + P_1^S P_0^{W1} \right) \cdot 0 \\ + \left( P_0^S P_0^{W1} + P_1^S P_1^{W1} \right) \cdot 1$$

と求めることが出来るので、式 (6) の  $W2_k$  をこれで置き換え、上記の  $U_k$  の範囲を  $E_k$  で記述し直せば

$$T - \Delta u < E_k + \langle W2_k \rangle < T \\ T - \Delta u - \langle W2_k \rangle < E_k < T - \langle W2_k \rangle$$

となり、これを満たす  $E_k$  の分布は  $U_k - \langle W2_k \rangle$  の分布と等しくなるということである。すなわち

$$f_{E_k}^{(3)}(e) = f_{U_k - \langle W2_k \rangle}(e) \\ = f_{U_k}(e + \langle W2_k \rangle), \\ T - \Delta u - \langle W2_k \rangle < e < T - \langle W2_k \rangle$$

である。

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

Case 3 と同様に  $W2_k$  の期待値を考えると、それは

$$\langle W2_k \rangle = \left( P_0^S P_1^{W1} + P_1^S P_0^{W1} \right) \cdot 0 \\ + \left( P_0^S P_0^{W1} + P_{0.5}^S + P_1^S P_1^{W1} \right) \cdot 1$$

と求めることが出来るので、式 (6) の  $W2_k$  をこれで置き換え、上記の  $U_k$  の範囲を  $E_k$  で記述し直せば

$$T \leq E_k + \langle W2_k \rangle < T + \Delta u \\ T - \langle W2_k \rangle \leq E_k < T + \Delta u - \langle W2_k \rangle$$

となり、これを満たす  $E_k$  の分布は  $U_k - \langle W2_k \rangle$  の分布と等しくなるということである。すなわち

$$f_{E_k}^{(4)}(e) = f_{U_k - \langle W2_k \rangle}(e) \\ = f_{U_k}(e + \langle W2_k \rangle), \\ T - \langle W2_k \rangle \leq e < T + \Delta u - \langle W2_k \rangle$$

である。

以上より、 $E_k$  の分布密度関数は

$$f_{E_k}(e) = f_{E_k}^{(1)}(e) + f_{E_k}^{(2)}(e) + f_{E_k}^{(3)}(e) + f_{E_k}^{(4)}(e)$$

と求めることが出来る。

次に、誤差拡散法において、輝度値を 2 値化する際の際になる値の分布について調べる。式 (3) より  $k+1$  番目の画素におけるその値は前小節の記号を用いれば

$$U_{k+1} = G2 + ER_{k+1}, \quad ER_{k+1} = \sum_{i \in J_{k+1}} j_i E_i$$

と表現出来る。この式の誤差項において、任意の  $i \in J_{k+1}$  に対する  $j_i E_i$  の分布密度関数は

$$f_{j_i E_i}(e) = f_{E_i}\left(\frac{1}{j_i}e\right)$$

と表すことが出来る。また、任意の  $m, n \in J_{k+1}$  に対する  $j_m E_m, j_n E_n$  について、それらの和の分布密度関数は、各  $j_n E_n$  を  $j_m E_m$  に加えて出来る分布に  $j_n E_n$  の出現割合を掛けて、各  $j_n E_n$  について足し合わせるにより得られる。すなわち、 $\Delta y$  を正のある微小量とすると

$$f_{j_m E_m + j_n E_n}(e) \\ = \sum_{t=-\infty}^{\infty} f_{j_m E_m + t \Delta y}(e) f_{j_n E_n}(t \Delta y) \Delta y \\ = \sum_{t=-\infty}^{\infty} f_{j_m E_m}(e - t \Delta y) f_{j_n E_n}(t \Delta y) \Delta y \\ = \int_{-\infty}^{\infty} f_{j_m E_m}(e - y) f_{j_n E_n}(y) dy, \quad \Delta y \rightarrow 0 \\ = \int_{-\infty}^{\infty} f_{E_m}\left(\frac{1}{j_m}(e - y)\right) f_{E_n}\left(\frac{1}{j_n}y\right) dy$$

となる。これを繰り返し適用することにより、蓄積誤差の分布密度関数は

$$f_{ER_{k+1}}(e) \\ = \iiint \dots \int f_{E_{i'}}\left(\frac{1}{j_{i'}}(e - \sum_{\substack{i \in J_{k+1} \\ i \neq i'}} y_i)\right) \prod_{\substack{i \in J_{k+1} \\ i \neq i'}} f_{E_i}\left(\frac{1}{j_i}y_i\right) dy_i$$

により求まる。ここで多重積分は誤差フィルタ  $J_{k+1}$  に含まれる画素数から 1 を引いた回数分の積分であり、積分範囲は各積分で  $-\infty \sim \infty$  である。同様にすれば、 $U_{k+1}$  の分布密度関数は

$$f_{U_{k+1}}(u) = \int_{-\infty}^{\infty} f_{G2}(u - x) f_{ER_{k+1}}(x) dx$$

となる。

以上により、 $W2$  の  $k+1$  番目の画素が白になる確率は

$$P_1^{W2_{k+1}} = P(W2_{k+1} = 1) \\ = P(T - \Delta u < U_{k+1} < T + \Delta u) P_0^S P_0^{W1} \\ + P(T - \Delta u < U_{k+1} < T + \Delta u) P_1^S P_1^{W1} \\ + P(T \leq U_{k+1} < T + \Delta u) P_{0.5}^S \\ + P(U_{k+1} \geq T + \Delta u) \\ = \left\{ P_0^S P_0^{W1} + P_1^S P_1^{W1} \right\} \int_{T - \Delta u}^{T + \Delta u} f_{U_{k+1}}(u) du \\ + P_{0.5}^S \int_T^{T + \Delta u} f_{U_{k+1}}(u) du \\ + \int_{T + \Delta u}^{\infty} f_{U_{k+1}}(u) du$$

のように求めることが出来る。

### 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。重畳画像  $C$  は割符画像  $W1$  と  $W2$  を光学的に重ね合わせることにより得られる。よって、 $C$  の各画素が白か黒になるかは  $W1$  と  $W2$  の画素に依存する。 $C$  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  $k$  番目の画素が白になる確率は、前小節の記号を用いれば

$$\begin{aligned} P_1^{C_k} &= P(C_k = 1) \\ &= P(T - \Delta u < U_k < T + \Delta u) P_1^S P_1^{W1} \\ &\quad + P(T \leq U_k < T + \Delta u) P_{0.5}^S P_1^{W1} \\ &\quad + P(U_k \geq T + \Delta u) P_1^{W1} \\ &= P_1^{W1} \left\{ P_1^S \int_{T-\Delta u}^{T+\Delta u} f_{U_k}(u) du \right. \\ &\quad \left. + P_{0.5}^S \int_T^{T+\Delta u} f_{U_k}(u) du \right. \\ &\quad \left. + \int_{T+\Delta u}^{\infty} f_{U_k}(u) du \right\} \end{aligned}$$

となる。

### 4. まとめ

本稿では、従来法として  $F_u$  と  $A_u$  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。同手法は、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。定式化の結果、割符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出来た。これにより、例えば、割符画像とそれらから再現される秘匿画像を高品質に得るための入力画像セットに対する輝度分布の傾向を推定したり、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、極めて初歩的な方法を用いており、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、実験的シミュレーションによる検証により明らかになるであろうモデルの不備を補強し、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、本稿を画像割符の定式化に関する第一報とする。

### 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) 会森 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, 会森 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.