Vol.2011-CG-144 No.6
2011/9/5

自然画像のための視覚復号型暗号の一手法

山　口　　泰[†1,†2]

計算を必要とせず視覚のみによって復号可能な暗号として視覚復号型暗号がある．視覚復号型暗号は，その原理上，暗号化に伴って画質の劣化が避けられない．本稿では，ピクセル拡大とコントラスト低下という画質劣化の要因について検討し，これらの問題を解決する自然画像のための新たな暗号化手法として，並列誤差拡散法と最適化階調変換を提案する．

A New Scheme of Visual Cryptography for Natural Images

Yasushi Yamaguchi[†1,†2]

Visual cryptography is a kind of cryptography that can be decoded directly by the human visual system when transparencies are stacked. It suffers from deterioration of the resulting images because of pixel expansion and contrast decline. This report proposes a new method for visual cryptography for natural images which allows no pixel expansion and high contrast.

1. はじめに

視覚復号型暗号とは，一切の計算を必要とせず，視覚のみで復号可能な暗号である．実際には画像を複数の透明シートに印刷し，それらを重ね合わせることで秘密情報を復元できる，という形式をとるものである．復元される秘密情報だけでなく，各透明シートにも意味のある画像が存在する場合には，特に**拡張視覚復号型暗号**と呼ばれる．これまでに拡張視覚復号型暗号について，様々な研究が行われてきたが，写真などの自然画像を扱うものはそれほど多くはなかった．それは，視覚復号型暗号の原理上，ピクセル拡大とコントラスト低下という問題が避けられず，画質が大幅に劣化してしまい，画像としての魅力に乏しいものとならざるを得なかったためである．本稿では，これらの問題を解決する拡張視覚復号型暗号の新たな手法について提案する．

†1 東京大学 大学院総合文化研究科
The University of Tokyo, Graduate School of Arts and Sciences
†2 独立行政法人科学技術振興機構 CREST
JST, CREST

2. 拡張視覚復号型暗号

視覚復号型暗号は Noar と Shamir によって，(k,n) **視覚復号秘密分散**として提案された[1)]．ここでは，秘密画像の復元に n 枚の透明シートを用い，このうちの k 枚（$k \leq n$）以上の透明シートが重ねられたときのみに，秘密画像を取得できるというものである．秘密分散とは暗号の一種であるが，より強固な性質を持っている．一般の暗号では，暗号解読によって鍵を推測されるという危険性があり，完全な安全性を保証することはできない．これに対して秘密分散は，分散された暗号文が揃わない限りは，原理的に復号が不可能という性質を持っている．なお，このときに提案された手法では，各透明シートは砂の嵐様のランダムドットで構成されていた．

拡張視覚復号型暗号については Naor と Shamir も指摘していたが，より詳細な議論を行ったのは Ateniese らである[2)]．ここでは紙面の都合もあるので，彼らの提案した手法についての概略を説明する．彼らの手法は，明暗 2 値のピクセル値を持つ n 枚の透明シート画像と 1 枚の秘密画像を入力とし，ピクセル単位での処理を行う．各ピクセルは，入力された $n+1$ 個のピクセル値から，n 枚の透明シートに対応する n 個のサブピクセルパターンに変換される．サブピクセルパターンは**シェア**と呼ばれ，それぞれ m 個の黒または白のサブピクセルから構成される．この黒と白のサブピクセルの割合によって，ピクセルの明暗が実現される．このときのサブピクセルの個数 m を**ピクセル拡大**と呼ぶ．

n 個のシェアにおける m 個のサブピクセル値を $n \times m$ のブール行列 $M = [m_{ij}]$ で表すこととする．ただし，m_{ij} はサブピクセルが黒の場合に 0，白の場合には 1 とする[⋆1]．n 枚の透明シートのうち，r 枚の透明シートを重ねる操作は，ブール行列 M から対応する r 行の m 次元ベクトルを取り出して，要素ごとに論理積をとって得られる m 次元ベクトル M_r を求めることに等しく，そのときの明るさはハミング重み $H(M_r)$ によって与えられる．$H(M_r) \geq t$ の場合には明るいピクセル，$H(M_r) < t - \alpha m$ の場合には暗いピクセルと判断される．ここで，$t \in \{1, \cdots, m\}$ は閾値，$\alpha > 0$ は相対コントラスト，$\alpha m \geq 1$ はコントラストと呼ばれる．

拡張視覚復号型暗号では，n 個の透明シート画像と秘密画像のピクセルの色（明暗）の組合せによって，サブピクセルのパターンを定めることになる．言い換えると，2^n 通りの $n \times m$ ブール行列集合の組 $(\mathcal{C}_b^{c_1 \cdots c_n}, \mathcal{C}_w^{c_1 \cdots c_n})$ があれば良い．ここで，上付の添字 $c_1 \cdots c_n \in \{b, w\}$ は n 個の透明シートピクセルの色の組合せ，下付の添字 b と w は重ねて得られるピクセルの色を表しており，b と w はそれぞれ黒（暗）と白（明）に対応するものとする．(k,n) 拡張

⋆1 多くの視覚復号型暗号の論文では，白に 0，黒に 1 を対応させることが多いが，本稿では一般的な画像の表現と対応させるために，黒を 0，白を 1 としている．

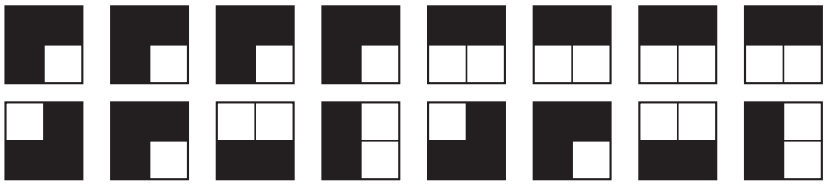

図 1 $(2,2)$ 拡張視覚復号型暗号の基底行列に対応するサブピクセルパターンの組：左から $S_b^{bb}, S_w^{bb}, S_b^{bw}, S_w^{bw}$, $S_b^{wb}, S_w^{wb}, S_b^{ww}, S_w^{ww}$ で，上段がシェア 1，下段がシェア 2 に対応する

視覚復号型暗号を実現するには，以下の条件を満たす $(\mathcal{C}_b^{c_1\cdots c_n}, \mathcal{C}_w^{c_1\cdots c_n})$ があれば良く，透明シート画像と秘密画像のピクセルの色から n 個のシェアを定めることが可能となる．

(1) いかなる $c_1,\cdots,c_n$ についても，$n\times m$ ブール行列 M から k 行を抜き出して論理積をとったベクトル M_k は，$M\in\mathcal{C}_w^{c_1\cdots c_n}$ の場合には $H(M_k)\geq t$，$M\in\mathcal{C}_b^{c_1\cdots c_n}$ の場合には $H(M_k)<t-\alpha_R m$ となる．

(2) いかなる $c_1,\cdots,c_n$ でかつ，$\{1,\cdots,n\}$ のいかなる部分集合 $\{i_1,i_2,\cdots,i_q\}$（ただし，$q<k$）についても，$n\times m$ ブール行列 M から行 $i_1,i_2,\cdots,i_q$ を抜き出して作られる $q\times m$ ブール行列の集合 $\mathcal{D}_b^{c_1\cdots c_n}$ と $\mathcal{D}_w^{c_1\cdots c_n}$ には差が見られない，すなわち，どちらの集合にも同じ行列が同じ個数だけ含まれている．

(3) いかなる $i\in\{1,\cdots,n\}$ でかつ，いかなる $c_1,\cdots,c_{i-1},c_{i+1},\cdots,c_n\in\{b,w\}$ についても，$n\times m$ ブール行列 M の第 i 行ベクトル M_i のハミング重み $H(M_i)$ は，以下の関係を満たす．

$$\min_{M\in\mathcal{M}_w} H(M_i)-\max_{M\in\mathcal{M}_b} H(M_i)\geq\alpha_S m,$$

ただし，ブール行列集合 $\mathcal{M}_b$ と $\mathcal{M}_w$ は，次のように定義される．

$$\mathcal{M}_b=\mathcal{C}_b^{c_1\cdots c_{i-1}bc_{i+1}\cdots c_n}\cup\mathcal{C}_w^{c_1\cdots c_{i-1}bc_{i+1}\cdots c_n},$$
$$\mathcal{M}_w=\mathcal{C}_b^{c_1\cdots c_{i-1}wc_{i+1}\cdots c_n}\cup\mathcal{C}_w^{c_1\cdots c_{i-1}wc_{i+1}\cdots c_n},$$

(1) は復号される秘密画像のコントラスト $\alpha_R m$ に関わる条件で，k 枚の透明シートを重ねて得られる画像のコントラストを示している．(2) は秘密画像のセキュリティで，k 枚未満の透明シートからは秘密情報が得られないことを保証している．(3) はシェアのコントラスト $\alpha_S m$ に関する条件で，各透明シートにおける画像のコントラストを示している．

具体例として，$(2,2)$ 拡張視覚復号型暗号について考えてみる．サブピクセルの個数を $m=4$ として，4 組の 2×4 ブール行列の集合 $(\mathcal{C}_b^{c_1c_2}, \mathcal{C}_w^{c_1c_2})$（ただし $c_1,c_2\in\{b,w\}$）が必要となる，このとき，各集合 $\mathcal{C}_c^{c_1c_2}$ は，それぞれ以下の基底行列 $S_c^{c_1c_2}$ の列の順序を入れ替えることで得られる．

図 2 拡張視覚復号型暗号の例：左と中央が透明シート上の画像，右が復元された秘密画像

$$S_b^{bb}=\begin{bmatrix}0&0&0&1\\1&0&0&0\end{bmatrix},\ S_w^{bb}=\begin{bmatrix}0&0&0&1\\0&0&0&1\end{bmatrix},\ S_b^{bw}=\begin{bmatrix}0&0&0&1\\1&1&0&0\end{bmatrix},\ S_w^{bw}=\begin{bmatrix}0&0&0&1\\0&1&0&1\end{bmatrix},$$
$$S_b^{wb}=\begin{bmatrix}0&0&1&1\\1&0&0&0\end{bmatrix},\ S_w^{wb}=\begin{bmatrix}0&0&1&1\\0&0&0&1\end{bmatrix},\ S_b^{ww}=\begin{bmatrix}0&0&1&1\\1&1&0&0\end{bmatrix},\ S_w^{ww}=\begin{bmatrix}0&0&1&1\\0&1&0&1\end{bmatrix}.$$

図 1 は，上記の基底行列に対応するサブピクセルパターンの組である．たとえば，左端の S_b^{bb} は上下ともに暗い（明るさが 1/4）のピクセルパターンで，これらを重ねるとさらに暗い（明るさが 0）結果が得られる．その次の S_w^{bb} は上下ともに暗い（明るさが 1/4）が，重ねると元と同じ明るさ 1/4 の結果が得られる．

これを用いて作られる拡張視覚復号型暗号の例を図 2 に示す．透明シート上には明暗 2 種類の領域，重ねて得られる画像にも明暗 2 種類の領域がある．ただし，前者の場合には，各領域の明るさは 1/2 と 1/4 であるのに対して，後者の場合には 1/4 と 0 になっている．この例で与えられた原画像は，それぞれ 64×64 ピクセルであり，結果の画像は縦横 2 倍ずつの 128×128 ピクセルになっている．また，相対コントラストは $\alpha_R=\alpha_S=0.25$ である．

Ateniese らは，相対コントラスト α_R,α_S やピクセル拡大 m について考察し，(k,k) 拡張視覚復号型暗号には，以下の制約があることを示した．

$$2^{k-1}\alpha_R+\frac{k}{k-1}\alpha_S\leq1,\qquad m\geq2^{k-1}+2.$$

すなわち，相対コントラストには上限があり，α_R,α_S との間にはトレードオフが存在する．また，拡張視覚復号型暗号を実現する際には，必ずピクセル拡大が生じることになる．

3. 自然画像の拡張視覚復号型暗号化

3.1 ハーフトーニングを用いた直接的な方法

Ateniese らの提案した拡張視覚復号型暗号では，与えられる画像のピクセル値が 2 値であることが前提となっている．近年，デジタルカメラやデジタルビデオは一般化して，容易に

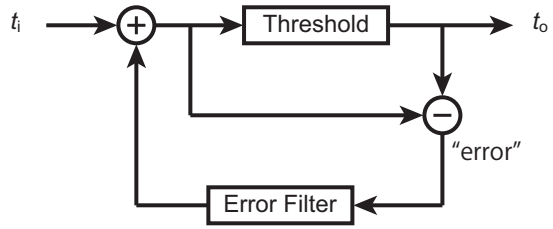

図 3 誤差拡散法の処理ダイアグラム

		X	7/48	5/48
3/48	5/48	7/48	5/48	3/48
1/48	3/48	5/48	3/48	1/48

図 4 エラーフィルタの例

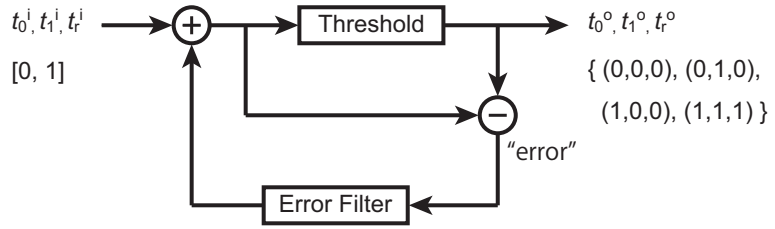

図 5 並列誤差拡散法の処理ダイアグラム

デジタルの自然画像を入手できる．また多くの場合，ピクセル値は 1 チャネルあたり 8 ビットの 256 階調となっている．このような画像を拡張視覚復号型暗号化するには，まず画像を 2 値化する**ハーフトーニング**を施す必要がある．

誤差拡散法は比較的良く利用されるハーフトーニング手法であり，Floyd と Steinberg によって提案された[3]．この手法は画像の端からピクセルごとに処理を進める 1 パスの処理となっている．各ピクセルの処理は，図 3 に示すように 2 値化と誤差拡散の 2 つのステップによって構成される．ここで誤差とは 2 値化の際のピクセル値の変化量であり，誤差は未処理の近傍ピクセルに対してエラーフィルタに応じた量が分配される．図 4 は Jarvis らによって提案された[4] エラーフィルタの例である．左上からスキャンライン方向を優先して，1 行ずつ処理が進むことを仮定しており，X が現在のピクセルに対応している．このエラーフィルタに従って誤差を拡散することで，近傍ピクセル群によって局所領域の階調を実現できるようになっている．

ハーフトーニングを利用すれば，以下の手順で自然画像を拡張視覚復号型暗号化できる．

(1) 連続階調の自然画像をハーフトーニングを用いて 2 値化する．
(2) 前に述べたブール行列集合の組 $(\mathcal{C}_b^{c_1\cdots c_n}, \mathcal{C}_w^{c_1\cdots c_n})$ を用いて拡張視覚復号型暗号にする．

しかし，結果画像はハーフトーニングだけでなく暗号化によっても画質が劣化してしまう．後者の場合，ピクセル拡大とコントラスト低下が画質劣化に関与する．すなわち，暗号化に伴うピクセル拡大があるために，ピクセル数を維持する（増やさない）ためには，ハーフトーニングに先駆けてダウンサンプリングが必要となる．また，暗号化によって相対コントラストは下がらざるをえない．$(2,2)$ 拡張視覚復号型暗号化の場合には，$\alpha_R = \alpha_S = 0.25$ が最大値となる．これらの問題に対処するために，本稿ではピクセル拡大のない暗号化手法である**並列誤差拡散法**と，相対コントラストの向上を図る**最適階調変換**を提案する．

3.2 並列誤差拡散法

並列誤差拡散法はピクセル拡大のない拡張視覚復号型暗号を実現する手法である．透明シート 0, 1 上の画像と復元される秘密画像に対応する 3 枚のグレースケール自然画像を入力として，暗号化された 2 枚の透明シート画像を出力する．この際，3 枚の画像の間で対応するピクセルを同時に処理していく．入力された 3 ピクセルの値を $t_0^i, t_1^i, t_r^i \in [0,1]$ とし，結果のピクセル値を $t_0^o, t_1^o, t_r^o \in \{0,1\}$ とする．t_0^o と t_1^o は透明シート画像のピクセル値であり，t_r^o は復元される秘密画像のピクセル値であるが，必ず次式を満たさなくてはならない．

$$t_r^o = t_0^o \cdot t_1^o \qquad t_0^o, t_1^o, t_r^o \in \{0,1\}.$$

したがって，取りうる結果のピクセル値 (t_0^o, t_1^o, t_r^o) は，$(0,0,0)$, $(0,1,0)$, $(1,0,0)$, $(1,1,1)$ の 4 通りとなる．図 5 は並列誤差拡散法の処理を示したものである．3 つのピクセル値は暗号化の制約を満たすように 2 値化されるとともに，そのための余分の誤差も近隣に拡散することで，全体としての階調を実現する．

残念ながら並列誤差拡散法によって作られる暗号画像は，厳密な意味での秘密分散にはなっていない．それは透明シート上のピクセル値を 2 値化するにあたって，秘密画像のピクセル値も考慮しているためである．しかし，写真などの自然画像を暗号化する際には，この問題は無視できると考えられる．なぜならば，透明シート上の画像に対する秘密画像の影響は微小であるとともに，そこには秘密画像だけでなく，他の透明シート画像も関与している．さらに複数画像が重畳された際の画像信号分離は非常に難しい問題であり，微小な秘密画像信号を分離することは現実的には不可能と考えて良いからである．

3.3 最適階調変換

並列誤差拡散法を実現するためには，入力される 3 つのピクセル値 t_0^i, t_1^i, t_r^i の間にも，一定の条件が成り立つ必要がある．たとえば，透明シート画像ピクセルの一方が完全に黒の場合には，秘密画像ピクセルが白くなることはない．また，透明シート画像ピクセルが両方とも完全に白だったとすると，秘密画像ピクセルは黒くなりえない．図 6 は，3 ピクセル値 t_0, t_1, t_r の取りうる領域を示したものである．白丸で示された 4 点 $(0,0,0)$, $(0,1,0)$, $(1,0,0)$, $(1,1,1)$ だけが，暗号化後に許容されるピクセル値であり，この 4 点が張る四面体の内部領域が表現可能ということになる．したがって，入力されたグレースケール画像は，すべての 3 ピクセルの組が四面体内部に収まるように階調変換される必要がある．

いかなる画像の組合せについても，必ず四面体内部に収まるような階調変換は，次式で与えられる．

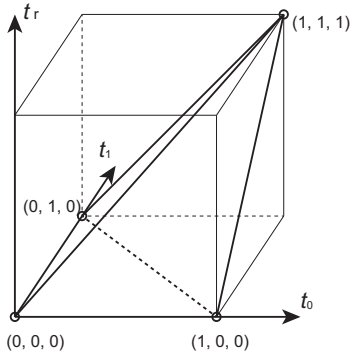

図 6 暗号化可能なピクセル値の領域

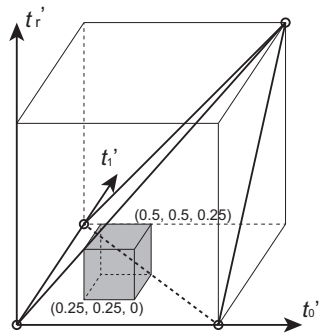

図 7 必ず暗号化可能となる階調変換の結果領域

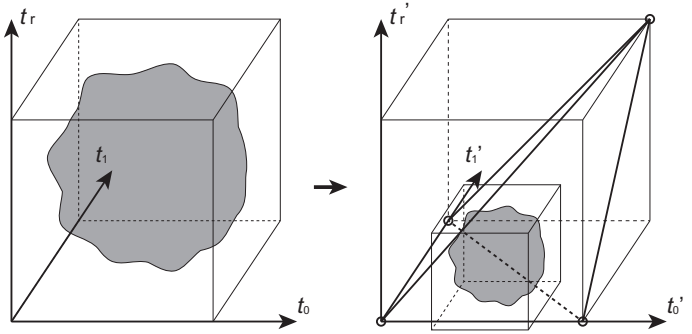

図 8 実際のピクセル値を考慮した階調変換

$t_0' = 0.25t_0 + 0.25, \quad t_1' = 0.25t_1 + 0.25, \quad t_r' = 0.25t_r.$

ここで，t_0, t_1, t_r は入力されたピクセル値，t_0', t_1', t_r' は階調変換後のピクセル値を表している．この結果，単位立方体で表される元画像のダイナミックレンジは，図 7 のように四面体に内接する小立方体に写される．このダイナミックレンジは，第 2 節で説明した従来の拡張視覚復号型暗号の相対コントラストに対応している．

実際の画像中には，完全に黒や完全に白のピクセルはそれほど多くは含まれておらず，3 枚の画像の間でちょうどそのようなピクセルが同じ位置に重なることは稀である．つまり，与えられた画像の組に応じて階調変換を調整すれば，より高いコントラストを得られる可能性がある．これを示したものが，図 8 である．左図の網掛け領域が実際のピクセル値の組を示すとすれば，この網掛け領域が右図のように四面体に内接する変換を施してやれば良い．そのような階調変換として，次のようなアフィン変換を考える．

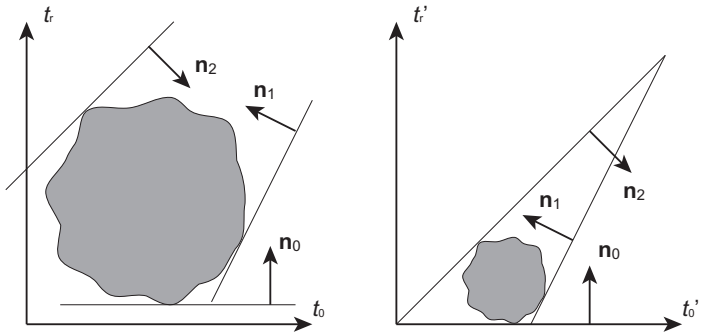

図 9 実領域を四面体に内接させるアフィン変換

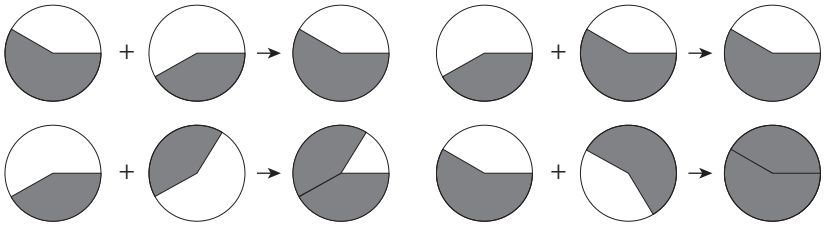

図 10 3 つのピクセル値に対する制約

$t_0' = at_0 + b_0, \quad t_1' = at_1 + b_1, \quad t_r' = at_r + b_r,$

結果として，3 枚の画像はいずれも同じ相対コントラスト a を持つようになる．アフィン変換のパラメータは，a, b_0, b_1, b_r の 4 自由度であるのに対して，四面体による制約も 4 つ（4 平面）であり，一意に定めることが可能である．ところで，このアフィン変換は等方的なスケーリングと平行移動からなる変換である．この際，4 つの制約平面に接する点は事前に求められる．すなわち四面体の面に平行な平面群を仮定すると，図 9 に示すように，いずれかの平面が当該領域にちょうど接するときの接点が，アフィン変換後において四面体に内接する．したがって，最初に 4 つの接点を見つけてから，それぞれが四面体に内接するようにアフィン変換のパラメータを定めれば良い．

ここで四面体によって表現される制約を改めて考えてみると，以下のようになる．

$$t_r' \le t_0', \quad t_r' \le t_1', \quad t_r' \ge t_0' + t_1' - 1, \quad t_r' \ge 0. \tag{1}$$

前の 2 つの不等式は，復元されるピクセル値の上限に関する制約である．復元されるピクセル値 t_r' は，図 10 の上段に示すように，透明シートのピクセル値 t_0', t_1' よりも大きく（明るく）なることはありえない．後の 2 つの不等式は，復元されるピクセル値の下限に関する制約である．復元されるピクセル値 t_r' は，透明シートのピクセルが明るい場合には，図 10

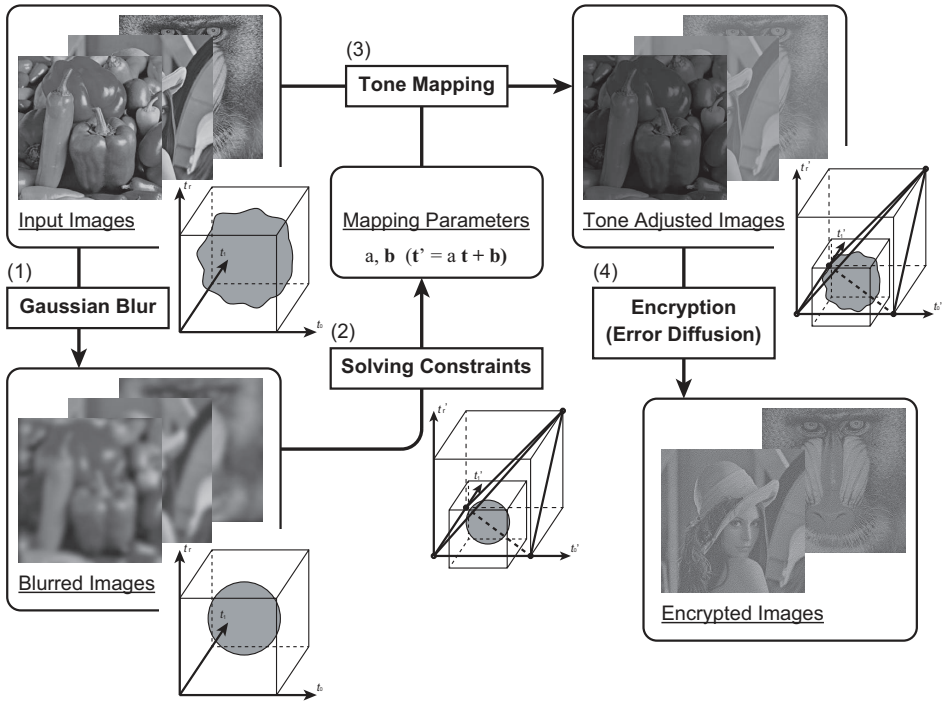

図 11 提案手法全体の処理の流れ

の左下に示すように一定以上に暗くなることはできない，また，いかなるピクセル値も，図 10 の右下に示すように，負にはなりえない．これらの制約は，黒領域と白領域の面積比に関する制約であるが，ハーフトーニング後のピクセルは完全な黒か白のいずれかにしかならない．すなわち，四面体の内部で表される制約は，個々のピクセルに対する制約ではなく，複数ピクセルからなる局所領域に対する制約と考えるべきである．このような性質は周辺ピクセルとの平滑化によって判断することが可能となる．言い換えるならば，与えられた画像そのものを階調変換した際に制約を満たすのではなく，与えられた画像に平滑化フィルタを施した後の画像が階調変換された際に満たすべき制約となる．

以上をまとめると，新たな拡張視覚復号型暗号化処理は，図 11 に示すような手順となる．

(1) 入力画像にガウスフィルタを適用したぼかし画像を生成する．
(2) ぼかし画像が (1) 式の制約を満たすアフィン変換パラメータを求める．
(3) 入力画像に対してアフィン変換の階調変換を施す．
(4) 階調変換後の画像に対して並列誤差拡散法を適用して暗号化する．

4. 実　　験

拡張視覚復号型暗号化による画質を評価するために実験を行った．実験に利用した画像は，図 12 に示す「パプリカ」「レナ」「ヒヒ」「飛行機」「ボート」「湖」の 6 枚であり，いずれも 512×512 ピクセルである．

最初に拡張視覚復号型暗号による結果画像の比較を行った．図 12 のパプリカを秘密画像として，透明シート画像にはレナとヒヒを用いた．図 13 が結果である．紙面の都合上，透明シート画像の一方（レナ）と復元された秘密画像（パプリカ）のみを示してある．左は従来方式を用いた直接的な暗号化による結果，中央と右は並列誤差拡散法を用いた結果である．従来方式の場合は，ピクセル拡大（$m = 4$）があるために，まず画像を 256×256 ピクセルにダウンサンプリングした後に，ハーフトーニングを施し，最後に暗号化を行っている．並列誤差拡散法の場合には，暗号化の前に階調変換が必要となる．中央はいかなる場合にも必ず暗号化可能となる保守的な階調変換，左は最適階調変換を，それぞれ施した結果である．最適階調変換にあたっては，カーネルサイズ $k = 21$（ピクセル），標準偏差 $\sigma = 10$（ピクセル）のガウスフィルタを用いた．相対コントラストは，左と中央の場合には $\alpha = 0.25$ であり，右の場合には $\alpha = 0.44$ になっている．

図 12 実験に用いた画像：「パプリカ」（左上），「レナ」（中央上），「ヒヒ」（右上），「飛行機」（左下），「ボート」（中央下），「湖」（右下）

図 13 暗号化の結果（上段は透明シート画像の 1 枚，下段は復元された秘密画像）：直接的な方法 （左），並列誤差拡散法のみ （中央），並列誤差拡散法と最適階調変換 （右）

Vol.2011-CG-144 No.6
2011/9/5

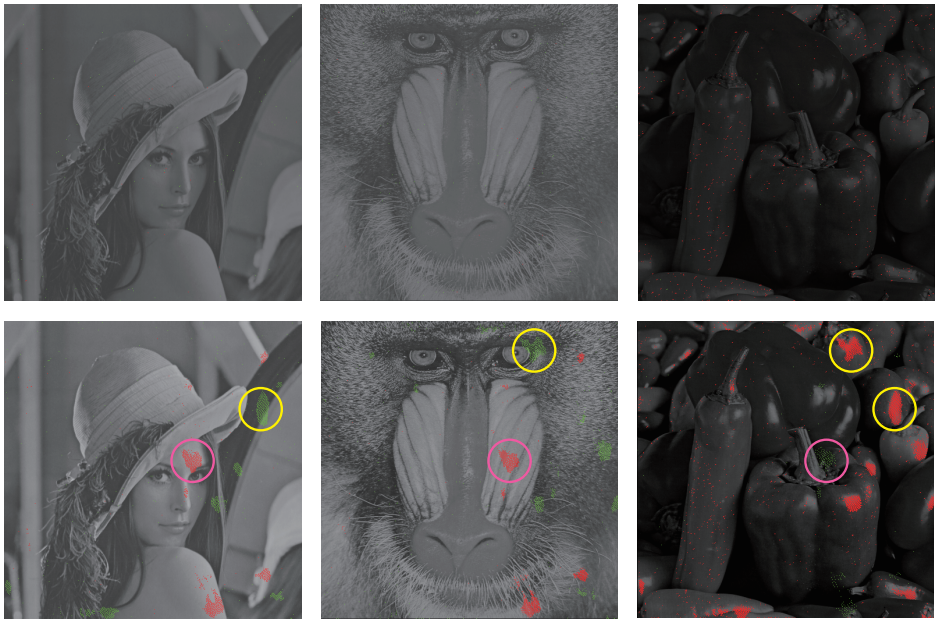

図 14 並列誤差拡散時に比較的大きな誤差が生じた場所：上は $\sigma = 0$ の場合，下は $\sigma = 20$ の場合

並列誤差拡散法によって暗号化を行うと，通常の誤差拡散法よりも大きな誤差が生じる可能性がある．言い換えるならば，従来型の誤差拡散法で白になるべきピクセルが黒になったり，黒くなるべきピクセルが白になったりすることがある．なぜなら，個々の画像のピクセル値だけではなく，他の画像の誤差も考慮して 2 値化するために，1 枚の画像にしわ寄せが生じる可能性があるためである．さらに，各画像のコントラストを大きくしようとすると，画像同士が相互干渉することで，より大きな誤差を生じる場合もある．

図 14 は，並列誤差拡散法の処理時に，比較的大きな誤差の生じたピクセルを示したものである．図の中で，緑色で示したピクセルは本来黒となるべきところが白になったピクセル，赤で示したピクセルは本来白になるべきところが黒となったピクセルである．上段は相対コントラスト $\alpha = 0.25$ という保守的な階調変換を用いた際の結果である．本来は図 7 のように暗号化可能な四面体の内部に全ピクセルが収まるはずであるが，近隣ピクセルの誤差と他の 2 枚の画像の誤差との関連で，誤差が大きくなるピクセルが散発的に発生している．しかし，画像中に占める割合は非常に小さいうえ，近隣のピクセル群によって局所的には適切な階調が実現されており，画質を大きく劣化させるものではない．図 14 の下段は，最適階調変換の際に，ガウスフィルタの範囲を $\sigma = 20$ と大きくし，相対コントラストを $\alpha = 0.56$ まで上げた画像に対して，並列誤差拡散法を施した際の結果である．黄色の丸印で示した箇所は透明シート画像の一方が暗いにも拘らず，秘密画像が明るいために，暗号化の際に無理が生じたものである．これに対して，ピンク色の丸印で示した箇所は 2 枚の透明シート画像が共に明るいにも拘らず，秘密画像が暗いために，暗号化にあたって無理があった部分である．これらの大きな 2 値化誤差は，一定領域に渡って広がっており，結果画像の画質を劣化させる要因となっている．

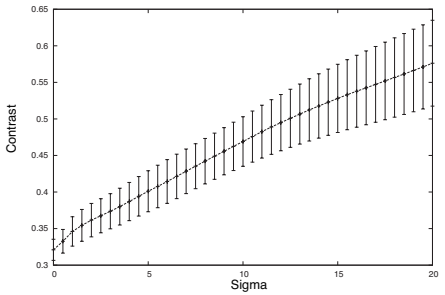

図 15 ガウスフィルタの標準偏差 σ と相対コントラストの関係

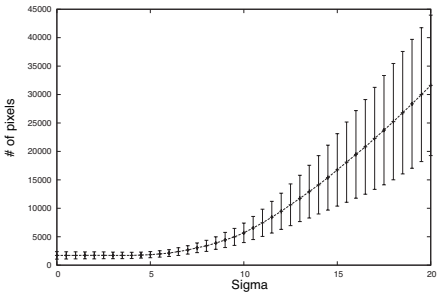

図 16 ガウスフィルタの標準偏差 σ と誤差ピクセル数の関係

そこで，ガウスフィルタの大きさが相対コントラストと誤差に与える影響を測ることにした．つまり，ガウスフィルタの標準偏差 σ を変化させた際の，相対コントラストと大きな誤差を生じたピクセル数を調べた．最適階調変換の相対コントラストは暗号化される画像の組合せに依存することから，図 12 の 6 枚の画像から 3 枚を選び，そのうちの 1 枚を秘密画像，残りの 2 枚を透明シート画像とする，${}_6C_3 \times {}_3C_1 = 30$ 通りの組合せについて計算を行った．図 15 と図 16 は，それぞれガウスフィルタの標準偏差に対する相対コントラストと誤差ピクセル数の関係を示したグラフである．30 通りの組合せから得られた平均値と標準偏差をプロットしている．図 15 からわかることは，ガウスフィルタをかけない場合でも相対コントラストの平均値は 0.32 であり，いかなる画像の組に対しても有効な保守的階調変換の相対コントラスト 0.25 よりも，かなり高い値になっている．またガウスフィルタの標準偏差を大きくすると，相対コントラストが上がっていくことがわかる．ただし，標準偏差がある程度大きくなると，相対コントラストの向上率は徐々に減少する傾向にある．一方，図 16 を見ると，標準偏差の増大にともなって，誤差の大きなピクセル数も増加する傾向にある．ただし，標準偏差 $\sigma < 5$ の間は，ピクセル数はほとんど増加しないが，それ以降 $5 \leq \sigma \leq 10$ の間に徐々にピクセル数が増加し始め，$\sigma > 10$ では急速にピクセル数が増加する．実験の結果からみると $\sigma \leq 10$ の範囲では画像上に目立った劣化は観察されなかった．したがって，この範囲内であればコントラストの向上に寄与するだけで，画質は損なわれないと考えても良いと思われる．

5. 考　　察

並列誤差拡散法は，暗号化のための制約を 2 値化誤差の一種として，近傍ピクセル群に拡散して局所的な階調を実現する手法である．このようにハーフトーニング（2 値化）と暗号化を組み合わせた手法として，Fu らの研究がある[5]．彼らの処理アルゴリズムは，以下のようなものである．

(1) 1 枚目の透明シート画像に通常の誤差拡散法を用いてハーフトーニングする．
(2) 2 枚目の透明シート画像は共役誤差拡散法でハーフトーニングする．共役誤差拡散法では，1 枚目の透明シートのハーフトーン画像ならびに秘密画像のピクセル値を考慮したノイズが加えられる．このノイズは 2 枚目の透明シート画像の画質に影響を与えるため，閾値を設定してノイズの量を制御する．

この手法はピクセル拡大を伴わないが，ロゴや文字などの元々2 値の画像を秘密情報として扱うことを目的としていた．また，2 枚の透明シートを重ねた際に得られる復元画像は，2 枚の透明シート画像と微かなロゴ画像の合計 3 つの画像が重なって見えるというものだった．明堂らは，Fu らの手法をもとに，秘密画像として自然画像も利用できる手法を提案した[6]．Wu らは暗号化の制約を考慮に入れて，すべての透明シート画像と秘密画像を同時にハーフトーニングすることを提案している[7]．彼らはベクトル誤差拡散法の利用についても触れているものの，実際には反復探索によるハーフトーニング手法を利用しており，処理には相当の時間を要するものと想像される．

最終的な透明シート画像や復号される秘密画像のコントラストはできる限り高くしたいものの，拡張視覚復号型暗号の性格上，コントラストの低下は避けられない．中嶋らは $(2,2)$ 拡張視覚復号型暗号におけるピクセル値の関係について検討し，本稿の（1）式と等価な制約を示した[8]．暗号化を伴うハーフトーニング処理の前には，入力画像に適切な階調変換を施す必要がある．階調変換としてよく用いられる方法は，アフィン変換や区分線形変換である[6)–9)]．Wu らは最適パラメータの計算法を提案しているが，凸包の利用を示唆するのみにとどまっており，手法の詳細は不明である[7]．明堂らは，本稿で述べた手法と同様なパラメータの計算法を提案している[9]．彼らの実験では相対コントラストは平均して 0.28 程度まで上げられるとしている．しかし，第 4 節で述べたように，我々の実験ではガウスフィルタをかけない場合でも，平均 0.32 程度まで上げることが可能であった．ただし，これは実験に用いた画像セットの性質に由来するものという可能性もある．

6. おわりに

本稿では自然画像を対象とした新たな拡張視覚復号型暗号の生成法を提案した．この手法は並列誤差拡散法と最適階調変換とによって構成される．並列誤差拡散法は自然画像を 1 パスで拡張視覚復号型暗号化できる手法であり，ピクセル拡大がないため，結果の画像は入力画像と同じピクセル数となる．最適階調変換では，連立 1 次方程式を解くことで，与えられた画像組の相対コントラストを最大化する階調変換のパラメータを求められる．また，最適階調変換の計算にあたって，ガウスフィルタを施すことで，制約を緩和して相対コントラストをさらに上げられる．これらの手法の有効性や限界について，実験を行って確認した．

残念ながら並列誤差拡散法によって作られる暗号画像は，厳密な意味での秘密分散にはなっていない．それは結果の透明シート上のピクセル値を定める際に，秘密画像のピクセル値も考慮しているためである．しかし，透明シート上の画像に対しては，秘密画像だけでなく，他の透明シート画像も影響を与えている．また，それらの影響は非常に小さいために，写真などの自然画像を対象とした拡張視覚復号型暗号から，秘密画像信号を分離することは現実的には不可能と考えて良い．

謝辞　本研究の一部は．科研費基盤研究（B）（22300030）の助成を受けたものである．

参　考　文　献

1) Naor, M., and Shamir, A.: Visual cryptography, *Lecture Notes in Computer Science (Advances in Cryptology- EUROCRYPT'94)*, Vol.950, Elsevier, pp. 1–12 (1990).
2) Ateniese, G., Blundo, C., De Santis, A., and Stinson, D.R.: Extended capabilities for visual cryptography, *Theoretical Computer Science*, Vol.250, pp.143-161 (2001).
3) Floyd, R.W. and Steinberg, L.: An adaptive algorithm for spatial grayscale, *Proceedings of Society for Information Display*, Vol.17, Society for Information Display, pp. 75–77 (1976).
4) Jarvis, J.F., Judice, C.N., and Ninke, W.H.: A survey of techniques for the display of continuous tone pictures on bilevel displays, *Computer Graphics and Image Processing*, Vol.5, No.1, pp. 13–40 (1976).
5) Fu, M.S. and Au, O.C.: A novel method to embed watermark in different halftone images: data hiding by conjugate error diffusion (DHCED), *Intl Conference on Acoustics, Speech, and Signal Processing*, Vol.III, pp. 529–532 (2003).
6) Myodo, E., Takagi, K., Miyaji, S., and Takishima, Y.: Halftone Visual Cryptography Embedding a Natural Grayscale Image Based on Error Diffusion Technique, *Intl Conference on Multimedia and Expo*, pp. 2114–2117 (2007).
7) Wu, C.W., Thompson, G., and Stanich, M.: Digital watermarking and steganography via overlays of halftone images, Electrical Engineering IBM Research Report, RC23267 (W0407-013), IBM, pp. 1–12 (2004).
8) Nakajima, M. and Yamaguchi, Y.: Extended visual cryptography for natural images, *Journal of WSCG*, Vol.10, No.2, pp. 303–310 (2002).
9) 明堂絵美, 高木幸一, 米山暁夫: 画像割符のための濃淡再現域への一意な階調変換法, 電子情報通信学会論文誌 A, Vol.J93-A, No.-12, pp. 805–810 (2010).