

カラー画像への可変表示型電子透かしの提案

ウイセツスト ピヤピスト[†] 松井 甲子雄[†]

積極的な著作権保護対策の1つとして画像に固定のロゴマークなどを表示する方法がすでに利用されている。この論文では、色相などの変化に着目して、ロゴマークを可変表示できるカラー画像への電子透かしの1方法を提案する。その原理は、著作権情報の挿入対象となる各画素に対し、RGB信号から $YCbCr$ 色信号への変換に際して、色相、彩度、明度を微妙に変更し、ロゴマーク信号を埋め込む。その変調の程度により透かし信号を可視から不可視まで制御可能となる。この方法によると挿入する領域のカラー特性により色彩の変化を制御でき、また透かしマスクの色を変更することも可能である。透かし行列を所有する者のみが表示されたロゴマークを不可視化できる利点がある。最後に、埋め込まれた透かしが改ざんにも強くかつStirMark攻撃に耐性を持つことを示す。

A Proposal of Variable Displaying Watermark to Color Image

WISETSUIT PIYAPISUIT[†] and KINEO MATSUI[†]

A logo or trade mark is often displayed on image as one of the positive copyright protection tools, but it might be easily removed in the digital media. In this paper, we propose a digital visible watermarking scheme to color image which controls the color transformation between the RGB and $YCbCr$ color systems for each pixel. The logo mark is displayed in a visible to invisible style on color image according to a transform matrix that consists of the prescribed entries and watermarking variables. The displayed mark is changeable to invisible or half-visible state when it is requested. Then, the original image is recovered smoothly but the watermark remains in the invisible state. Moreover, the mark color may be altered with another transform matrix and be expressed with multiple watermarking. Finally, we show that the displayed mark becomes more tamper-resist watermarking and robust against StirMark attack.

1. はじめに

最近、マルチメディアの品質を劣化させることなくコンテンツを容易に複製できる技術が普及し、その著作権の管理が緊急の課題となっている。このような著作権保護対策の1つとして電子透かしが提案され、デジタル画像データに著作者の情報を埋め込み、不正利用に対する検証道具として利用しようと試みられている^{1),2)}。

ところで、すでに提案された電子透かし法では、画像に透かしの密かに埋め込むため、肉眼では観察できない。したがって、追跡調査や著作権侵害に抵触する際に、埋め込まれた透かしの復号して、問題解決の一助に利用するだけであり、電子透かしは著作権保護の立場から見ると消極的な手段である。一方、著作権を積極的に主張したい者は、画像にロゴマークなどを表

示する方法を用いている。この方法では、画像上にその存在が明らかとなるため、不正利用者に心理的な圧力を与えることができる。さらに、電子透かしと合体させて利用すれば、その効果が向上すると思われる。しかし、このような可視型の透かしは、透かし対象となる画素の情報を失うため、多くの場合に元の画像に復元することができなくなる欠点を持っている。

このような背景のもとで可視透かしの研究は、すでに文献3)~6)などで取り上げられ、いくつかの成果が得られている。文献3), 4)では、濃淡画像において署名を表示かつ除去可能な透かし方式を提案した。文献5)では、DCT係数を用いて動画MPEG-1およびMPEG2のビデオ信号に適應する方法を示している。また、文献6)では、カラー画像に適用する方法を提案しているが、上下位ビットの置き換えおよびビットシフトのような局所処理を用いるため、セキュリティ強度に欠ける問題がある。

そこで、この論文ではカラー画像固有の性質を利用した可変表示型の透かし方式を提案する。その方法は、

[†] 防衛大学校情報工学科
Department of Computer Science, National Defense Academy

まず, RGB 表色系から YC_bC_r 表色系への変換行列に透かしパラメータを付加し, 得られた改訂変換行列で署名挿入対象となる画素のみを YC_bC_r 色信号に変換する. 次に, 公知の逆変換行列で RGB 信号にもどす. 得られた署名済画像には付加した透かしパラメータの値 (以後, 透かし値とよぶ) によって画素の色相, 彩度, 明度が変化する. 透かし値および署名挿入領域の色の 3 属性に従い, 署名マークが透明的に視覚できるようにする. また, 透かし値を制御することにより半可視, 不可視の透かしに変更することができる. 明示された可視署名を不可視にするには, 透かし値を知る者のみが変換行列を作成して透かし画素ごとに不可視状態にもどすことが可能である.

以下, 2 章では, 色信号変換による透かしの埋込みの概要を述べ, 3 章において, 可視, 不可視, 半可視の可変透かしへの変換条件, これらの変色方法, 不可視化方法などについて具体的に示す. 4 章では, 自然画像と人工画像の 2 つのカラー画像を用いて実験した結果を示し, StirMark 攻撃に対する耐性, セキュリティの強化を検討する.

2. カラー透かし方式の原理

カラー画像の持つ固有の性質に注目して, 筆者らはすでにその特徴を利用した色信号変換行列による電子透かし法を提案した⁷⁾. この方法は RGB 信号から YC_bC_r 信号に変換する際に, 式 (1) の係数行列を式 (2) で置き換える方式である.

$$\begin{bmatrix} y \\ c_b \\ c_r \end{bmatrix} = \begin{bmatrix} 0.299 & 0.587 & 0.114 \\ -0.169 & -0.331 & 0.500 \\ 0.500 & -0.419 & -0.081 \end{bmatrix} \begin{bmatrix} r \\ g \\ b \end{bmatrix} \quad (1)$$

$$\begin{bmatrix} 0.299 & 0.587 & 0.114 \\ -0.169 & -0.331 & 0.500 \\ 0.500 & -0.419 & -0.081 \end{bmatrix} + \begin{bmatrix} 0 & -x & x \\ x & 0 & -x \\ -x & x & 0 \end{bmatrix} \quad (2)$$

この方法は, 1 画素単位で透かし信号を埋め込むので, ログマークなどを画像の任意の位置に設定できる. すなわち, 原画像上における署名マーク挿入対象となる画素ごとに式 (2) の変換をすれば, そのマーク領域内に透かし情報が埋め込まれることになる. ここで, 変換過程を簡潔に記述するために, 次の記号を導入する. $P(i, j) = [r_{ij}, g_{ij}, b_{ij}]^t$, $F(i, j) = [y_{ij}, cb_{ij}, cr_{ij}]^t$ を RGB および YC_bC_r 信号の任意画素 (i, j) の信号ベクトルとし, A : RGB- YC_bC_r 信号変換行列, A^{-1} : その逆変換行列, X : 透かし行列と定義する. ただし, 添字 t は転置を表す. 以下, 式 (2) の行列を

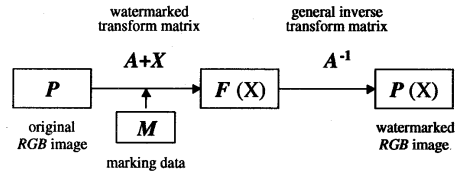


図 1 署名マークの埋込み過程
Fig. 1 Embedding process of watermark.

$A + X$ と表現する.

原画像にログマーク M を挿入する際には, 挿入対象となる画素に対して図 1 に示す処理を実施する. まず, カラー画像 P と署名するログマークを 2 値画像データ M として準備する. ここでは P も M も 256×256 画素からなるものと仮定する. 今, M の任意画素 $m(i, j)$ ($i, j = 1, 2, \dots, 256$) に対して $m(i, j) = 1$ をマーク領域, $m(i, j) = 0$ を他の領域とする. $m(i, j) = 1$ ならば, $P(i, j)$ の RGB 信号を式 (2) で YC_bC_r 信号に変換する. もし, $m(i, j) = 0$ ならば, $P(i, j)$ に対して式 (1) を適用する. すなわち,

$$\begin{aligned} F_X(i, j) &= (A + X)P(i, j) & m(i, j) = 1 \\ F_0(i, j) &= AP(i, j) & m(i, j) = 0 \end{aligned} \quad (3)$$

次に, 公知の逆変換行列で変換すると $m(i, j) = 1$ の画素については

$$\begin{aligned} P_X(i, j) &= A^{-1}F_X(i, j) \\ &= A^{-1}(AP(i, j) + XP(i, j)) \\ &= P(i, j) + A^{-1}XP(i, j) \end{aligned} \quad (4)$$

を得る. ただし, これらの操作時に, オーバフローまたはアンダフローが発生すれば, それらを上限または下限に補正する. この画素 $P_X(i, j)$ は, 透かし値 x が埋め込まれた RGB 色信号であり, 式 (4) により, 元の信号 $P(i, j)$ に対して $A^{-1}XP(i, j)$ からなるノイズが重畳されることが分かる. したがって, 署名マーク M 領域内のすべての画素がこの方法で変換されれば, マークの部分の色彩が近傍から変化して, 透かし信号の役割を果たすことになる. 一方, 色信号変換行列に付加する透かし行列を式 (2) の標準形 (以後, 標準透かし行列とよぶ) のみに限定すると, ログマークが同色系に偏る恐れがあるので, この標準形の行と行または列と列を入れ替えることによってマーク部分を異なる色に発色することができる. たとえば, 標準透かし行列の第 1 行目と第 2 行目を入れ替えた行列を

$$X_2^1 = \begin{bmatrix} x & 0 & -x \\ 0 & -x & x \\ -x & x & 0 \end{bmatrix} \quad (5)$$

とする。または、第1列目と第3列目を入れ替えた場合には、

$$X_{1,3} = \begin{bmatrix} x & -x & 0 \\ -x & 0 & x \\ 0 & x & -x \end{bmatrix} \quad (6)$$

で示すことにする。行または列を入れ替えることによって付加する要素の値も変わるため、透かしを変色して表示できる。

また、本手法では、可視状態にある透かしを不可視に変換することも容易にできる。これは、不可視化行列を作成して、透かし部分に適用する。こうすると、式(4)から $A^{-1}XP$ のノイズ成分を低減し、色彩の変化を元の値の近くに復号できるからである。

3. 可変透かし方式

色信号変換によるカラー透かし法は、透かし行列 X を用いてロゴマークの埋込みを行い、 x の値を変えることによって色彩が段階的に変化するので、可視、不可視、または半可視の可変透かしを作成することができる。以下、各可変透かしの特徴を示す。

3.1 可視透かしの条件

可視透かしを作成するには、埋込み処理の際に比較的に大きな透かし値 x を用いなければならない。これは、挿入対象となる領域の色彩の特性値に比較し、透かし値が大きければ、色彩が著しく変化するので、マークの部分が十分に視覚できるようになる。しかし、透かし値 x が大きすぎると視覚の面では有利であるが、画素値に対するオーバーフローまたはアンダフローが発生しやすくなる。この現象が多くの画素に発生すると透かしを完全に不可視状態にもどせなくなる。したがって、適切な透かし値を事前に調整しておくことが重要である。

3.2 不可視透かしの条件

不可視透かしは可視化の逆の方法で作成できる。すなわち、人間が視覚できない程度に透かし値 x を制御する。さらに、対象画素周辺の領域の色彩特徴によって人間の視覚特性では、ロゴマークを知覚できないレベルが異なるので、一般に、明度が低く、または、各 R , G , B の彩度がほぼ均等（濃淡に見える）の領域にマークを挿入することにより、不可視的な透かしを作成することが容易になる。この不可視状態にある透かし M を確認する際には、一般にロゴマークのない原画像を鍵として用いるものとする。

3.3 半可視透かしの条件

可視透かしのもう1つの拡張版として背景との半

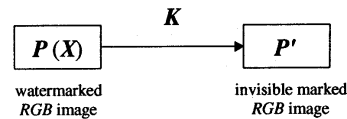


図2 可視透かしの不可視化過程
Fig. 2 Invisibilizing process of visible mark.

透明的な透かしがある。これは可視および不可視透かしの中間の透かしで、本論文では、半可視透かしとよぶことにする。半可視透かしは、可視透かしと同様にマークの挿入対象となる領域特性に従い、適切な x の値を用いればよい。

3.4 透かしの不可視化方法

可視状態にある透かしの部分を不可視化するために、式(4)に示した透かし画素における $A^{-1}XP(i,j)$ ノイズを低減すれば、信号 $P(i,j)$ の近くの値に復元することができる。ここで、不可視化行列 K を以下に定義する。ただし、 I は 3×3 の単位行列である。

$$K = (I + A^{-1}X)^{-1} \quad (7)$$

ロゴマーク M の画素値 $m(i,j)$ が1の画素に対してこの行列を適用する。その積算結果は

$$KPx(i,j) = (I + A^{-1}X)^{-1}(I + A^{-1}X)P(i,j) = P'(i,j) \cong P(i,j) \quad (8)$$

となる。すなわち、マーク領域の各画素に対して画素値を復元し、原画像に近い状態にもどすことができる。その処理過程を図2に示す。

YC_bCr 信号から RGB 信号にもどすときの埋込み処理において、四捨五入則で整数化する。したがって、正しい実数値としての画素データを失うことになり、不可視化後の画素 $P'(i,j)$ が元の画素 $P(i,j)$ と同じ値を得ることはできないが、その誤差が小数点の小さな量なので、人間の視覚では、その画質が元の画像と変わらない状態に見える ($P'(i,j) \cong P(i,j)$)。このとき、マークの部分がまだ残っているため、不可視化後の画像からでもロゴマーク M を確認できる。しかし、整数化と同時にオーバーフローまたはアンダフローを補正する場合、誤差が大きな整数値の量になるため、不可視化の際に、色彩を元にもどせなくなり、形跡が残ることもある。したがって、完全に不可視化できるためには、埋込み時に、多くのオーバーフローまたはアンダフローを発生させない程度の透かし値 x を用いる必要がある。

3.5 セキュリティ強化策

今まで述べた方式はマーク領域全体に1つの透かし値 x を用いた。このシステムでは、透かし値を密かに保管しなければならないが、もし第三者に知られた

場合、偽の透かしが作成されたり、ロゴマークを容易に制御されることになる。そこで、セキュリティを強化する1つの方法は、ロゴマーク全体を複数の透かし値で第三者に気付かれないように可視から不可視へと制御することである。このために、ロゴマークを部分的に分割して、部分ごとに異なる透かし値を適用する多重透かしを考える。たとえば、ロゴマークが文字列ならば、1つの文字に1つの透かし値を用いる。または、1つの文字内の領域を分割し、複数の透かし値を繰り返して適用することなどがある。この多重透かし法では、どの領域にどの透かし値が用いられるかを秘匿できるため、不正利用を試みようとする第三者に対し、さらに強い耐久性をもたらすことが期待できる。

4. 実験結果

この章では、可変透かしの実験結果を示す。この実験には、色彩の変化が激しいカラー画像 *girl* および色彩の変化が少ない人工画像 *graphic* (各画像 256×256 画素, *RGB* 各 256 階調) を用いる。また、埋込みの際の透かし行列は標準形式 (2) を利用する。

最初に、*girl* および *graphic* に対して透かし値 x の最適な範囲を求める実験を行った。透かし埋込み処理の際に、さまざまな x の値を用いて各要素 r , g , b におけるオーバーフローおよびアンダフローの発生率を求めた。その結果を表 1, 表 2 に示す。形跡が残らないようにロゴマークを不可視化するには、オーバーフローやアンダフローの補正が少ない方が好ましいので、表 1 および表 2 の結果により、各原画像に対して 0.1 ~ 0.7 の範囲の透かし値 x を利用すれば十分である。

次に、その範囲の値 x を用いて可変型透かしを作成した。参考までに署名情報として 5 種類のロゴマーク (TEST1~5) を準備する。これは、埋込み対象となる領域の特徴が可変透かしに対してどのような影響を与えるかを調べるために、それぞれの署名情報を原画像の異なる位置に図 3 のように埋め込むこととする。

4.1 可視透かし

可視透かしの実験においては、*girl* および *graphic* ともに 0.7 の x 値を用いて署名情報を埋め込んだ結果を図 4 (a) に示す。署名部分の色相などが著しく変化したため、透かしの十分に知覚できる。特に、人工画像 *graphic* では、色彩の変化が少ないので、透かしマークが自然画像よりはっきりと浮き上がることになる。

また、明度が低く、各 R , G , B の彩度がほぼ均等 (濃淡に見える) のような場合、たとえば、*girl* では、TEST1, 5 の領域に挿入した透かしは知覚しにくいことが分かる。

表 1 x による *girl* の各要素におけるオーバーフローおよびアンダフロー発生率

Table 1 Overflow and underflow occurrence rate for x in each element of *girl*.

透かし値 x	r	g	b
0.9	13.02%	0.31%	0.79%
0.7	0%	0%	0.31%
0.5	0%	0%	0.08%
0.3	0%	0%	0%
0.1	0%	0%	0%
-0.1	0.01%	1.67%	11.94%
-0.3	0.79%	10.44%	20.47%

表 2 x による *graphic* の各要素におけるオーバーフローおよびアンダフロー発生率

Table 2 Overflow and underflow occurrence rate for x in each element of *graphic*.

透かし値 x	r	g	b
0.9	30.60%	18.83%	17.43%
0.7	0%	0.42%	14.38%
0.5	0%	0%	12.00%
0.3	0%	0%	4.90%
0.1	0%	0%	0.04%
-0.1	6.43%	1.73%	30.34%
-0.3	24.55%	14.05%	33.78%

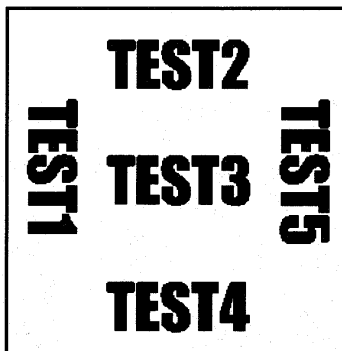


図 3 署名情報
Fig. 3 Marking data.

4.2 不可視透かし

可視透かし実験で述べたように人間が知覚しにくい領域に透かしの挿入し、または、小さい透かし値 x で色彩を変化させることが不可視透かしへの作成要領である。図 4 (b) に示した画像は、 $x = 0.05$ で *girl* に、 $x = 0.03$ で *graphic* に図 3 の署名を埋め込んだ結果である。透かしの部分の色相が変化した、人間の目では、ほぼ知覚できないであろう。しかし、色彩が滑らかな人工画像では色彩の変化が目立ちやすい。したがって、知覚されないためには、十分に小さい x 値

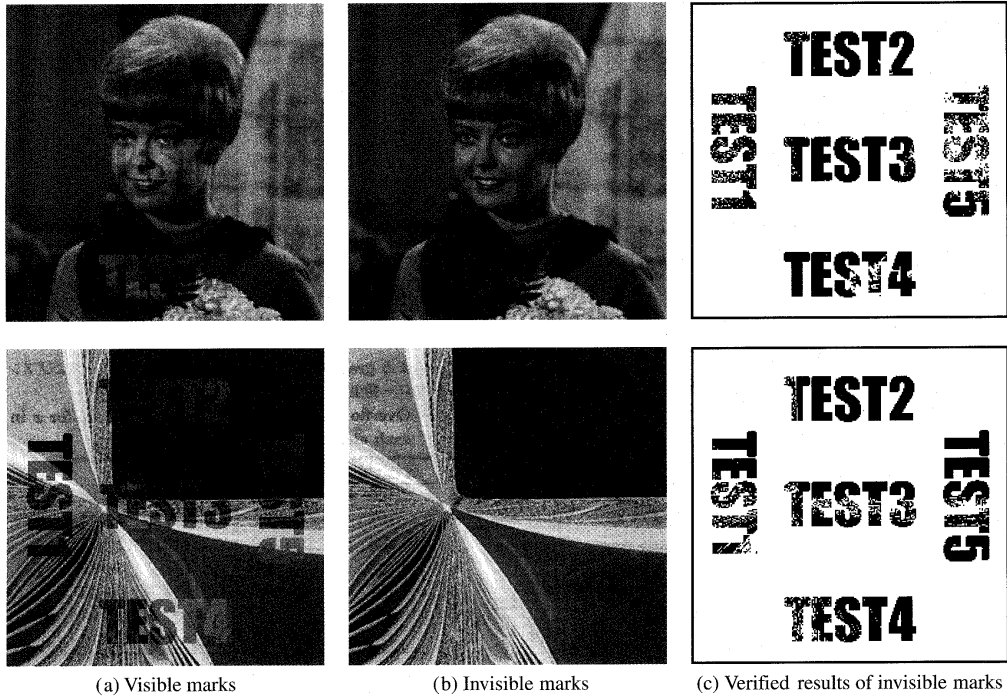


図4 署名済画像と検証結果
Fig. 4 Marked images and verified results.

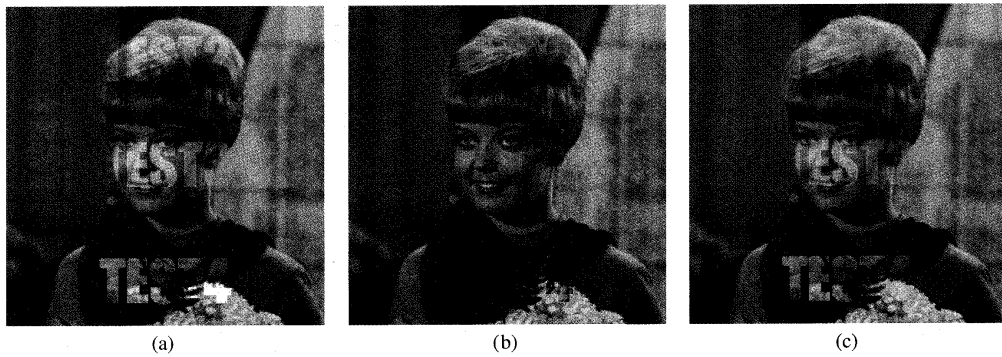


図5 他の透かし行列による署名の色彩変更
Fig. 5 Color alterations of mark by other transform matrixes.

を用いなければならない。不可視透かしを検証するときには、透かし部分と周辺領域の色彩値を極端に最大値の近くまで増加すれば、透かしの部分が確認できるようになる。この方法でも可視化できない場合には、ロゴマークのない原画像との差分情報から透かしを求めることができることに注意する。その差分情報の結果を図4(c)に示す。可視透かしおよび不可視透かし

で用いられる透かし値 x の中間の値で半可視透かしを容易に作成できる。

4.3 透かしマスクの変色

透かしマスクの色の変化を調べた。標準透かし行列とは異なる3つの透かし行列を用いて girl 画像に $x = 0.7$ で署名を埋め込んだ。それらの署名済画像を図5に示す。同図(a)は標準透かし行列の第1行目



図 6 StirMark 攻撃による不可視化結果の影響
Fig. 6 Effect on invisualized marks by StirMark attack.

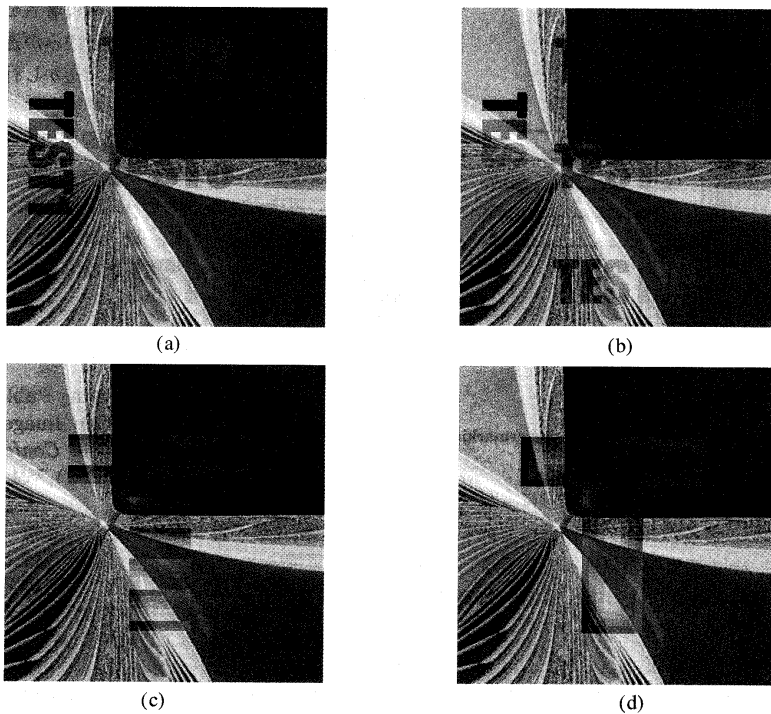


図 7 多重透かしによるセキュリティ対策
Fig. 7 Security scheme with multiple watermarking.

と第 2 行目を入れ替えた X_2^1 , 同図 (b) は第 2 行目と第 3 行目を入れ替えた X_3^2 , 同図 (c) は第 1 列目と第 3 列目を入れ替えた $X_{1,3}$ の透かし行列を用いた. 図 4 (a) と比べ, マスク部分の色彩が変化していることが分かる.

4.4 StirMark 攻撃に対する不可視化の耐性
強力な攻撃ツール StirMark[®] に対する本手法の耐

性を評価した. StirMark 攻撃は, 視覚特性を考慮して, スケーリング, ぼかし, RGB 変更, メディアンフィルタリング, 微小回転, JPEG 圧縮などの処理を複合的に行うツールである. 可視, 半可視, 不可視のそれぞれの透かし画像ヘデフォルトのパラメータで攻撃し, その不可視化した結果を図 6 に示す. この結果から署名済画像が攻撃されてもマークの主な部分は人

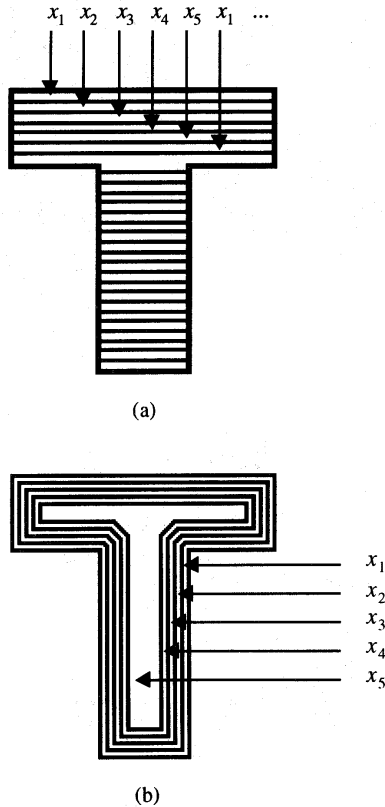


図8 多重透かしの構成例

Fig. 8 Schematic examples of multiple watermarking.

間の視覚で分からない程度まで元の色彩にもどすことができた。しかし、署名のエッジの部分においては目立った形跡が約2~3画素の幅で残ってしまう。これは、StirMarkの回転攻撃によって、署名が元の位置からずれてしまったからである。

4.5 セキュリティの強化

最後に、本手法のセキュリティを強化するために、1つのロゴマークに対して複数の透かし値を用いる場合の実験を行った。ここで、 $x_1 = 0.7$, $x_2 = 0.5$, $x_3 = 0.3$, $x_4 = 0.1$, $x_5 = 0.05$ の可視から不可視レベルまでの値を設定し、次の埋込み方法を試みた。最初に、図3の署名情報に対して、TEST1を x_1 、TEST2を x_2 、TEST5までの順で埋め込んだ。その結果を図7(a)に示す。次に、署名情報各文字にそれぞれ $x_1 \sim x_5$ を対応させると、署名済画像は図7(b)となった。さらに、1つの文字に対して複数の x を適用することもできる。例として、文字内の領域を図8(a)

のような横および図8(b)のように文字の周囲を分割し、各領域に $x_1 \sim x_5$ を埋め込む。ただし、簡単に視覚できるように署名を大きなT文字形に変更して、埋め込んだ結果を図7(c), (d)に示す。これらの方法で可視から不可視へと表示レベルを制御すれば、透かしマスクを消去するには秘匿した複数の x が必要になるので、第三者による不正利用に対してより強化した結果となっている。

5. まとめ

この論文では、色信号変換行列を用いて積極的な著作権表示手段としてのカラー画像への変型透かし方式を提案した。本手法を用いれば、透かし行列内の透かし値の調整および背景のカラー特性を利用することによって可視、半可視、不可視に署名を埋め込むことができ、かつ透かし値の所有者のみが透かしを制御することが可能である。さらに、透かし行列の形を変更して埋め込めば、署名マークを変色することもできることを示した。また、署名済画像にStirMark攻撃を行っても、透かしを保持することができる。

この可変表示型透かし方式を用いると著作権の所在が明示されるとともに、鍵の購入者には可視透かしを除去できるが、不可視透かしは除去できないという長所が得られる。

参考文献

- 1) Braudaway, G.: Protecting Publicly-Available Images with an Invisible Image Watermark, *Proc. IEEE International Conference on Image Processing '97 (ICIP97)*, Vol.1, pp.524-527 (1997).
- 2) 松井甲子雄: 電子透かしの基礎—マルチメディアのニュープロテクト技術, 森北出版 (1998).
- 3) 松井甲子雄, 阪口康弘: FSR 系列による画像へのデジタル透かしとマスク, 1996年画像メディア処理シンポジウム (*IMPS 96*), I-6.16, pp.35-36 (1996).
- 4) 中里隆博, 松井甲子雄: 積極的に著作権を表示する署名透かし方式の提案, 画像電子学会誌, Vol.27, No.5, pp.507-512 (1998).
- 5) Meng, J. and Chang, S.F.: Embedding Visible Video Watermarks in the Compressed Domain, *Proc. IEEE International Conference on Image Processing '98 (ICIP98)*, pp.474-477 (1998).
- 6) 岩本圭司, 新堀英二: 原画像の色調を損なわない除去可能な可視電子透かし, 1999年暗号と情報セキュリティシンポジウム (*SCIS '99*), Vol.1, pp.719-724 (1999).
- 7) ウィセスト・ピヤピスト, 松井甲子雄: 等価

信号変換によるカラー画像への電子透かし, 情報処理学会論文誌, Vol.40, No.4, pp.1801-1807 (1999).

- 8) Kuhn, M.G.: *StirMark*. <http://www.cl.cam.ac.uk/~fapp2/watermarking/image_watermarking/stirmark> (1997).

(平成 11 年 4 月 30 日受付)

(平成 11 年 9 月 2 日採録)



ウィセスト・ピヤピスト

昭和 48 年タイ王国生. 平成 10 年防衛大学校情報工学科卒業. 現在防衛大学校理工学研究科情報数理専攻在学中. 情報セキュリティと画像への電子透かしに関する研究に従事.

電子情報通信学会会員.



松井甲子雄 (正会員)

昭和 14 年生. 昭和 36 年防衛大学校電気工学科卒業. 昭和 40 年九州大学大学院工学研究科電子専攻修了. 昭和 56 年防衛大学校電気工学科教授. 平成元年同大学校情報工学科教授.

この間暗号学, 情報セキュリティ, 電子透かし, 音声・画像データの符号化に関する研究に従事. 著書「電子透かしの基礎」(森北出版). 工学博士. 電子情報通信学会, 画像電子学会, 映像情報メディア学会各会員.