グラフの同型判定の零知識相互証明を用いたオンライン検証型電子透かしシステム

木下宏揚[†] 小林輝伸[†]

電子透かしの情報を検証者に再利用されることのない新しい画像に対する電子透かしの構成法を提案する．通常の電子透かしは，透かしの情報を検証者に明らかにしてしまうため，検証者がその透かし情報を別の画像に組み込んでしまう可能性がある．本稿では，この問題を解決するために，電子透かしシステムを透かし情報の生成法と埋め込み法に分割して扱い，それぞれに必要な条件を考察する．そして，透かし情報の生成法としてグラフ同型問題の零知識相互証明を応用した電子透かし情報の生成法を提案する．また，これに適した周波数領域における電子透かし情報の埋め込み法を用いる．本方式は透かしの検査にオンライン検証システムを用いている．本手法を用いることにより，原画像の著作権保有者またはディジタル署名者はグラフ同型問題の置換を秘密にしておくことで透しが埋め込まれていることを証明でき，また，透かし情報を悪用されることがない．

An Online Verification Watermark System with Zero Knowledge Interactive Proof for the Graph Isomorphism

Hirotsugu Kinoshita[†] and Terunobu Kobayashi[†]

We propose digital signature method for the image which there is not of it being recycled information of digital watermark by a verifier. On conventional watermarking techniques, secret information, which is utilized for authentication, is disclosed to the verifier. We divide the watermarking system into two parts. One is the watermark generating method. Another is the watermark embedding method. We use zero knowledge interactive proof for graph isomorphism as the generating method to realize above condition. Furthermore, a embedding method in frequency domain suited for this method are applied. An online verification system is applied in this system. Consequently the secret information is not disclosed during the authentication process.

1. はじめに

マルチメディアシステムの発展にともなって，画像データに関係したセキュリティの問題が起きている．インターネットなどを利用して多くの画像データが入手可能であるが，これらの画像の大半は版権などの情報を含まず，コピーおよび配布に関して著作権上の問題点が発生している．

これに対応するため，スクランブル技術を含む画像暗号化[1),2)]や画像情報に対するディジタル署名，著作権を明らかにする電子透かし[3)~8)]などが研究されている．対象となる画像は，ディジタル化された画像データだけでなく，物理的な紙に描かれた画像を対象としたものもある[13)]．

† 神奈川大学工学部
Faculty of Engineering, Kanagawa University

特に，ディジタルデータは簡単に複製可能なので，不正なコピー使用は重大な問題となる．

電子透かしシステムは透かし情報の生成法とその埋め込み法に分けて考えることができる．

電子透かしのデータの生成法について検討してみると，通常の電子透かしは，透かしの情報を検証者に明らかにしてしまうため，検証者がその透かし情報を別の画像に組み込んでしまう可能性がある．したがって，システムの運用方法によっては，透かしが他の画像に転用され，なりすましを許してしまう可能性がある．これは，現代のセキュリティシステムとしては望ましくない．また，透かし情報を人間が視覚的に検出する手法では，機械による自動的な認証が可能でないため不便である．

一方，従来の電子透かしの埋め込み法のうち，画像に埋め込んだ透かし情報を取り出すために原画像と透かし情報の差分で透かし情報を取り出すために原画像

を必要としている方式は，次のような問題がある．これは透かし情報を取り出すときに検証者に対し原画像を見せることを意味しており，もし検証者が信用のおけない者であるならば原画像の違法コピー，2 次利用などの危険性がある．

本稿では，透かし情報の不正な 2 次利用の防止を考慮した，ディジタル化された静止画像の画像データの著作権を管理するのに適している新しい電子透かしシステムを提案する．電子透かしやディジタル署名の検査法としてはデータ本体と署名情報のみから確認が可能なオフラインの方式と検査時に確認を行うエンティティと他のエンティティの間で通信が必要なオンラインの方式がある．本方式は透かしの検査にオンライン検証システムを用いている．既存のオンライン検証システムとしては，Chaum らの Undeniable signatures [9] などがある．通常の電子署名と電子透かしとのオンライン検証法システムの類似点は，検証を行う際に，署名（透かし）作成者と検証者との間で通信が必要となり，作成者の協力が必要となる点である．相違点には次のものがある．本方式は ZKIP を利用して署名者が秘密情報を所有していることで画像に対して透かしを作成したことを示している．また，原画像固有の情報と署名者の秘密情報に依存して透かし情報を作成している．一般に電子透かしでは，原画像と透かし情報が不可分であるという性質によって，署名の機能と著作権管理の方法を実現している．一方，Undeniable signature では，離散対数問題に基づいて署名を行っており，ディジタル署名した事実を後に否定できない機能を実現している．また，一般のディジタル署名では，被署名情報と署名情報が分離可能なため著作権管理には向いていない．

このシステムでは，電子透かしを埋め込もうとしている画像からグラフを生成し，これと同型なグラフを電子透かし情報として一方向性ハッシュ関数をかけた後，この画像に埋め込みを行う．そして，グラフ同型判定のゼロ知識相互証明（ZKIP: zero knowledge interactive proof）[14] を電子透かしの確認に用いる．この方式では，原画像を必要としない透かし検出法が必要となるが，従来提案されている方式では，本方式に要求される電子透かし埋め込みの条件を満たさないため，これに適した透かし埋め込み法を示す．この方法では，原画像を DCT で周波数領域に変換後，画質への影響と透かし情報の耐性を考慮して，DCT 係数のレベルに適応した透かし情報の埋め込みを行う．

このシステムでは，電子透かしを埋め込もうとしている画像から固有の情報を取り出し，これをもとにグラフを生成し，グラフ同型判定の ZKIP を電子透かしの確認に用いる．このため，秘密情報は電子透かしの検証手続き中に洩れることはない．したがって，なりすましなどの悪用を防止することが可能となる．

2. グラフの同型判定問題

2.1 グラフ同型判定の ZKIP

グラフの同型判定はクラス NP に属するので，2 つの同型グラフ間の置換行列の情報は，秘密の情報となりうる．したがって，2 つの同型グラフがあるデータと密に結合していれば，置換情報を示すことは，著作権の主張に利用可能である．

Prover P がグラフ G_1，G_2 の同型写像を Verifier V に対して示すための ZKIP のプロトコルを以下に示す．

step 1：P はランダムな置換 ϕ を生成し，ランダムなグラフ G_2 $(= \phi(G_1))$ を V へ送る．

step 2：V は $b \in \{1, 2\}$ を選択し，b を P へ送る．

step 3：P は写像 g を送る．

ここで，$g = \phi$ if $b = 1$, otherwise $g = \phi\pi$ if $b = 2$.

step 4：V は $G_2 = g(G_b)$ が成立することを確認する．

P がこのプロトコルを 1 回実行したとき，V をだませる確率は 0.5 なので，プロトコルは n 回繰り返して行う．この場合，だませる確率は $1/2^n$ に減少する．

2.2 グラフの性質による同型問題の難しさについて

グラフ G において，ある頂点 ν に接続している枝の数を次数といい，$deg(\nu)$ と表す．また，各頂点の次数を大きい順に並べたものを次数列という．頂点数が同じである 2 つのグラフ G_1，G_2 の間の同型判定はたかだか $n!$ 通りの同型写像を調べればよいから，グラフ同型問題は *NP*に属する問題である．しかし，同型変換によって頂点の次数は変化しないから，2 つのグラフにおいて同じ次数の頂点が対応することになり実際には可能な同型写像の数がかなり限定される．したがって次数列を調べることにより G_1 と G_2 の各頂点の対応関係，すなわち同型写像が簡単に分かってしまう可能性がある．このことから，G_1（G_2）は各頂点の次数が等しくなる正則グラフの同型問題がいちばん難しい問題である．したがって，グラフは正則グラフとする必要がある [10]．

グラフ同型問題は一般のグラフについては *NP*であるが，特別な性質を持つグラフに対しては多項式時間で解くことができる [11]．たとえば，平面グラフ（planar graph）は $O(n)$，木（tree）は $O(n^2)$ で同型判定で

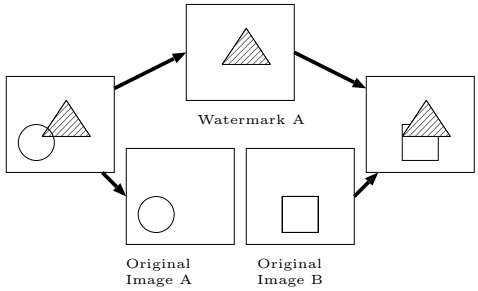

図 1 電子透かしの再利用
Fig. 1 Reuse of watermark.

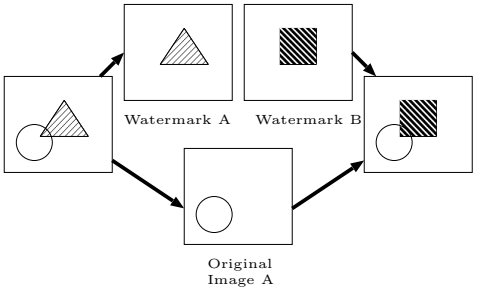

図 2 原画像の詐取
Fig. 2 Fraud of original image.

きる．正則グラフの同型問題が多項式時間で解けるかどうかは分からないが，次数 d と頂点の数 n の間の関係から以下のようなことが分かる．

(1) 次数について，$0 \leq d \leq n-1$

(2) $d \leq 3$ のとき，多項式時間 $(O(n^3 \log n))$ で同型判定ができる[12]．

(3) $d = n-1$ のとき，グラフは完全グラフ（complete graph）であり，同型写像は 1 つしかない．

(4) $d \geq n-4$ のとき，補グラフ（complementary graph）の次数は 3 以下であり，補グラフが同型なら元のグラフも同型であるから (2) と同様に多項式時間で同型判定ができる．

(5) 同型グラフの安全性は，$n^{cd/\log d}$ を用いて数値的に表すことができる．

したがって，d の範囲は $4 \leq d \leq n-5$ とする必要がある．しかし次数が小さくても，また大きくても同型問題は簡単に解けてしまう可能性はある[10]．

以上のことを考慮して本方式では次数が $d = \frac{n}{2}$ の正則グラフを用いることにする．

3. 本方式の概略

3.1 従来の電子透かしの問題点

従来の電子透かしシステムには次のような問題点がある．

透かし情報生成の問題点 通常の電子透かしシステムでは，透かし情報を抽出することにより検査を行う．したがって，電子透かしにディジタル署名の機能を持たせる場合，**図 1** に示すように確認者が証明者の透かしを入れ，第三者に流す可能性がある．すなわち，なりすましが可能となる．また，著作権の制御に用いる場合でも，本来の著作者の意図しない情報に対して透かしを入れられてしまう可能性がある．

透かし確認法の問題点 電子透かし確認時に原画像を必要とする電子透かしの埋め込み方を用いた場合，電子透かしの検証者が原画像を手にいれてしまうことになる．したがって，透かしを埋め込んだ画像から透かし情報を除去したのと等価となるため，**図 2** に示すように，検証者が入手した原画像に，自らの透かし情報を埋め込んで流通させてしまう危険性がある．

3.2 電子透かしシステムに要求される条件

署名機能を考慮した電子透かしシステムを実現するためには，以下の条件が必要となる．

- 公開情報となる透かし情報は，原画像と署名された画像から，一意に生成されなければならない．
- 公開情報となる透かし情報は，画質の大きな劣化なしに取り除くことができない．
- 透かし生成者の秘密情報は，電子透かしを埋め込んだ画像だけから引き出すことはできない．

さらに，信用できるセンターを仮定せずに著作権の主張のためには，

- 原画像データと透かしデータは分離不能でなければならない．

透かしの検証者が検査した画像に自分の署名をしてあたかも自分に著作権があるように主張することを防止するためには，

- 透かしの検証が原画像なしで行えなければならない．

3.3 電子透かしシステムの階層構造

本稿では，画像に対する電子透かしを作成し，著作権を所有するエンティティを証明者（Prover），画像に埋め込まれた電子透かしを確認するエンティティを検証者（Verifier）と呼ぶ．本システムは，**図 3** に示すように 3 つのレイヤに分けることができる．

一番上にレイヤは電子透かし生成レイヤ（**4.2 節参照**）と電子透かし検査レイヤ（**4.4 節参照**）が位置する．

上述の問題点を解決するために，従来の電子透かし情報の代わりに画像から一意に決定される情報を生成

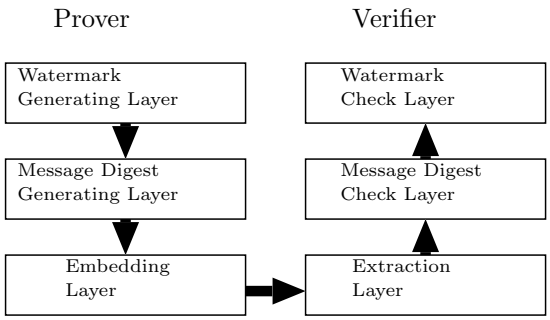

図 3 システムの階層構造
Fig. 3 Hierarchy of this system.

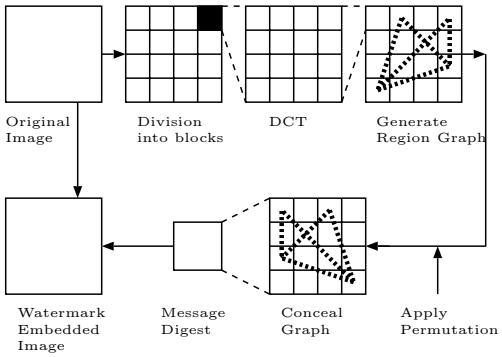

図 4 透かし生成のアルゴリズム
Fig. 4 Algorithm of watermark generation.

する．

単純な RSA などの公開鍵暗号に基づいたディジタル署名を画像情報に適用しても画像の符号化や処理の過程で元の情報が失われるためうまくいかない．

中間のレイヤはメッセージダイジェスト生成レイヤとメッセージダイジェスト検査レイヤからなる（**4.3 節参照**）．一般に耐性と安全性を高めるために，電子透かしのデータサイズは，可能な限り小さく，また，できるだけ多くの重複度を持って埋め込む必要がある．このレイヤにより，電子透かしのデータサイズを減少させることができる．

最下層のレイヤは埋め込みレイヤと取り出しレイヤである（**5.2 節参照**）．この層で，電子透かしは原画像に埋め込まれ，また取り出すことができる．

3.4 透かし情報の生成と埋め込み法の概要

図 4 に透かし情報生成と埋め込みの概略を示す．本方式では，透かし情報を原画像と証明者の秘密情報に基づいて生成する．このため，2 つの同型グラフと 1 つのグラフ間の置換は上記の条件を達成するために利用される．領域グラフ G_{block} は，原画像から一意に生成される．埋め込みグラフ $G_{conceal}$ は，領域グラフ G_{block} と同型なグラフである．$G_{conceal}$ は，原画像の権利者である証明者が保持する秘密情報であるランダムな置換により G_{block} から生成される．$G_{conceal}$ と G_{block} は，電子透かしを埋め込んだ画像から誰でも得ることが可能な公開情報である．

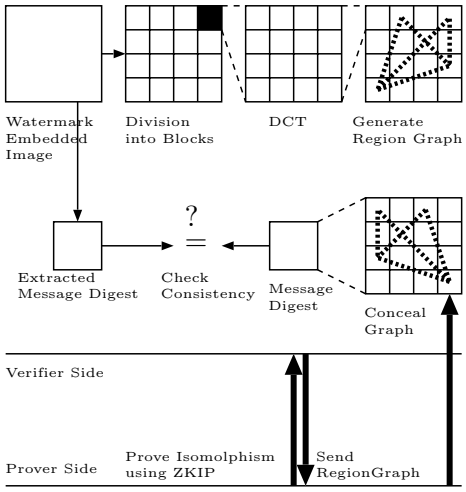

図 5 検証のアルゴリズム
Fig. 5 Algorithm of verification.

本方式のアルゴリズムを以下に示す．

(1) 原画像をブロックに分解する．各ブロックがグラフの節点となる．
(2) 各ブロックの輝度値を離散コサイン変換（DCT）する．
(3) 各ブロックの DCT 係数の平均値に依存して，グラフの枝を生成する（ブロックグラフ G_{block}）．
(4) 署名者の秘密情報として，ランダムな置換 π_s を生成する．
(5) 同型なグラフを生成する（埋め込みグラフ $G_{conceal}$）．
(6) 一方向性ハッシュ関数で圧縮した後，誤り訂正符号を付加し，これを透かし情報とする．
(7) 原画像に生成した透かし情報を埋め込む．

埋め込みグラフ $G_{conceal}$ は画像データと別に添付しておくか添付せずに署名検査時に別途送付する．

3.5 透かし情報検証法の概要

図 5 に透かし情報検証法の概略を示す．

(1) 署名された画像より署名情報を取り出す．また，署名画像より領域グラフ G'_{block} を生成する．
(2) 画像に添付された埋め込みグラフ $G_{conceal}$ と G'_{block} が同型であることを ZKIP で示す．
(3) $G_{conceal}$ が本物であることを確認する．

4. 署名情報の生成と検査

4.1 計算量的安全性とデータ量に関する考察

一般的に，今から近い将来の計算機の能力で安全と思われる解読に必要なステップ数が $10^{150\sim200}$ 以上となる．これより，グラフの同型問題で安全な節点の数 n と枝の数 d は，次式を満たす必要がある．

$$10^{150\sim200} < n^{cd/\log_2 d} \qquad (1)$$

n : 節点数，　d : 1 つの節点から出る枝の数

c : 定数，　　$d = n/2$

この式から，安全と考えられる n の値は 1000 から 1200 ぐらいの範囲となり，2 の n 冪乗の中から選択し，$n = 1024$，$d = 512$ とする．1 つの節点のラベルを表すのに 10 bit，$d = 512$ であるから，1 つの節点につながっている枝のデータ量は 512×10 bit となる．方向を考慮しないグラフの節点接続行列は対称行列となり，節点が自分自身への枝を持たないと考えれば，節点接続行列を表現するために必要なデータのサイズは $(1024^2 - 1024)/2$ bit となる．

4.2 原画像からのブロックグラフ生成アルゴリズム

4.2.1 ブロックグラフ生成における前処理

原画像からブロックグラフの節点と枝を一意に生成するために，以下のアルゴリズムを用いる．まず記号の定義を行う．

N_i ：節点のラベル

$N_i.h$: 節点 N_i より輝度値の高い節点に伸びている枝の数

$N_i.l$: N_i の輝度値以下の節点に伸びている枝の数

$N_i.c$: N_i より伸びている枝の総数

(1) **図 6** に示すように，原画像を 8×8 のブロックに分割する．この際，原画像のサイズが $(x_{\text{size}} \times y_{\text{size}})$ であるとすると，縦のブロック数は $y_{\text{size}}/8$，横のブロック数は $x_{\text{size}}/8$ となる．ラベル付けに際しては，左上を始点，右下を終点として，番号を割り当てていく．なお，このブロックが，生成されるグラフにおける節点となり，それぞれの節点は以下のパラメータを持つ．各ブロックがグラフの節点となる．

(2) **図 7** に示すように，DCT 係数の平均値（(0,1),(1,0),(1,1) の位置にある係数の平均値）を用いて，大きい順に並べ替え，ラベル付けを行う．なお，このブロックが，生成されるグラフにおける節点となり，それぞれの節はパラメータとして，枝の総数を表す $N_i.c$ を持つ．また，

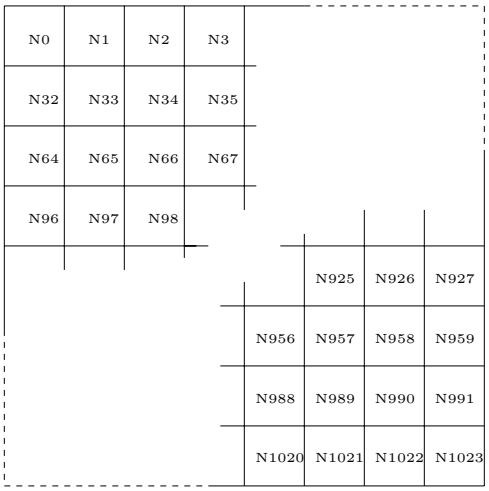

図 6 ブロック（節点）への分割とラベル付け
Fig. 6 Division in blocks and labeling.

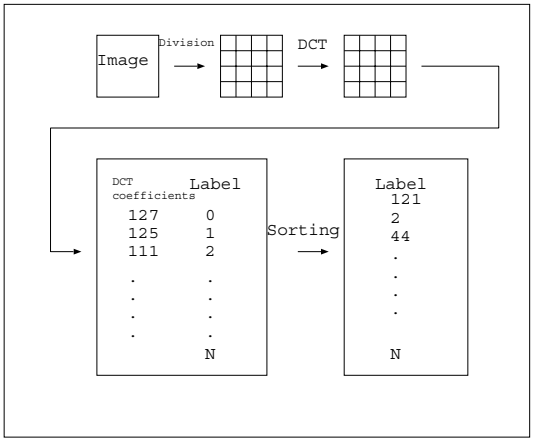

図 7 ブロックの順序付け
Fig. 7 Ordering of blocks.

1 つの節点から伸びる枝の本数を $N/2$ とする．(1,0),(0,1),(1,1) 成分を選択する理由は，低周波数成分は加工処理後にも残存する可能性が大きいため，検証時のブロックグラフの再現性を高めるためである．

(3) 実際のブロックグラフのデータは節点接続行列で表されるため，枝の存在を次のように定義する．

枝の元の節点を N_i，伸び先の節点を N_j としたとき，マトリックスの要素 M_{ij} は次の値をとる．

$$\begin{cases} M_{ij} = 0 \rightarrow N_i, N_j \text{ 間に枝がない場合} \\ M_{ij} = 1 \rightarrow N_i, N_j \text{ 間に枝がある場合} \end{cases}$$

ブロックグラフの生成は以下のプロセスで行われる．

4.2.2 N_i から N_j の節点への N/2 本の枝の生成

(1) N_i を $0 \leq i \leq$（節点のラベル番号最大値）とする（はじめは $i = 1$ とする）．

(2) N_j を $0 \leq j \leq$（節点のラベル番号最大値）とする（はじめは $j = 1$ とする）．

(3) N_i に対する N_j を順に次の条件を満たしているか調べる．

$$N_i.c < N/2$$
$$N_j.c < N/2$$

(4) (3) の条件を満たしていれば，次の操作を行う．

$$M_{ij} = 1$$
$$M_{ji} = 1$$
$$N_i.c = N_i.c + 1$$
$$N_j.c = N_j.c + 1$$

(5) $N_i.l = \frac{N}{2}$ であれば (7) へ

(6) (2)〜(5) の操作を j の最大値になるまで繰り返したら，次の操作を行って再び (2)〜(5) を繰り返す．

(7) $i = i + 1$ として (1)〜(6) を繰り返す．

以上までが基本的な生成プロセスである．このプロセスだけでは枝が足りない節点がでてくるが，無視することにする．以上により，ブロックグラフ G_b は生成される．

4.3 埋め込みグラフの生成

ブロックグラフ G_b から，実際の署名情報となる，G_b と同型なグラフである埋め込みグラフ G_c を生成する．まず，置換行列 π_s を生成する．

$$\pi_s = \begin{pmatrix} 0, & 1, & 2, & \cdots, & 1023 \\ 448, & 967, & 639, & \cdots, & 426 \end{pmatrix}$$

注：上の π_s は参考例（原画像が 256×256 の場合）

前に述べたが，これは，G_b と，そこから置換されて生成される G_c との節点のラベル番号の対応関係を示している．この π_s はランダムなものでよい．証明者は置換 π_s を秘密情報として保管する．

次に，G_b から π_s により G_c を生成する．すなわち

$$G_c = \pi_s(G_b)$$

以上により，埋め込みグラフ G_c は生成される．さらに，一方向性ハッシュ関数として MD5 をかけ，データ圧縮を行い，誤り訂正符号を付加したものを透かし情報とする．

4.4 透かし情報の検査

透かし情報の正当性の検証のプロセスは，証明者 P と画像上の署名を確認しようとする検証者 V との間で実行される．

(1) V は埋め込み画像から署名を取り出す．

(2) P は V に $G_{conceal}$ をおくり，V は一方向性ハッシュ関数をかけて署名と確認をとる．

(3) V は署名時と同様の方法で，ブロックグラフ G'_{block} を生成する．

(4) P は V に対して 2 グラフ間の同型性を ZKIP により証明する．

5. 透かし情報の埋め込み法

5.1 埋め込みの前処理

透かし情報を可能な限り小さくし，多重度を増加させるために，埋め込む署名情報 W の作成には署名情報にハッシュ関数（MD5）をかけて得られた 128 bit のデータと，エラー訂正コード 128 bit をあわせた 256 bit を作成し，埋め込む署名情報として作成した．

MD5 は不可逆圧縮であるが，図 5 に示したように検証時に圧縮前の情報を入手することで解決可能である．

5.2 透かし情報の埋め込み方法

画像処理や透かし情報除去に対する耐性を向上させるため，本方式では以下のような手法を採用する．

ブロックグラフの生成と同様に DCT 変換後の周波数領域において，透かし情報の埋め込みを行う．ブロックグラフは (0,1)(1,0)(1,1) の位置にある DCT の係数に依存して生成されている．透かし情報を埋め込んだあとにこの画像から，ブロックグラフを再構成する必要があるため，埋め込みにはこれ以外の周波数成分を利用する．

(1) 原画像を 8×8 のブロックに分解し，各ブロックの輝度値を DCT で周波数領域に変換する．

(2) 情報を埋め込む係数として以下のものを選択する．

$$\{(x, y) | 2 \leq x \leq 3, 2 \leq y \leq 3\}$$

a_{ij} を DCT の係数とする．$(a_{2,0}, a_{0,2})$, $(a_{3,0}, a_{0,3})$, $(a_{2,2}, a_{3,3})$ を埋め込を行う係数のペアとする．それぞれのペアの値を (s, t) $(s \geq t)$ とするとき，

$$m = \frac{|s| + |t|}{2}, \quad d = |s| - |t|$$

を計算する．

図 8 に示すように，ブロック中の DCT 係数 s と t の差の大きさに応じて埋め込むビットを 0

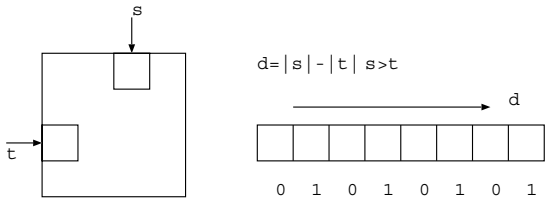

図 8 透かし埋め込みのアルゴリズム
Fig. 8 Algorithm fo embedding.

と 1 を表現する．埋め込むビットを識別するための窓の幅を q，段階を n とすると $q = \frac{m}{n}$ とする．

0 を埋め込む場合

$i = 0$ から $2n + 2$ まで以下の繰返し
if $2iq \leq d < (2i + 1)q$
then $s = m + q(i + \frac{1}{4}), t = m - q(i + \frac{1}{4})$
if $(2i + 1)q \leq d < (2i + 2)q$
then $s = m + q(i + \frac{3}{4}), t = m - q(i + \frac{3}{4})$

1 を埋め込む場合

$i = 0$ から $2n + 2$ まで以下の繰返し
if $2iq \leq d < (2i + 1)q$
then $s = m + q(i + \frac{5}{4}), t = m - q(i + \frac{5}{4})$
if $(2i + 1)q \leq d < (2i + 2)q$
then $s = m + q(i + \frac{3}{4}), t = m - q(i + \frac{3}{4})$

透かし情報の取り出し
取り出すビット b は以下の条件で求める．

$i = 0$ から $2n + 2$ まで以下の繰返し
if $2iq \leq d < (2i + 1)q$
then $b = 0$
if $(2i + 1)q \leq d < (2i + 2)q$
then $b = 1$

本方式では，256×256 画素の画像に対して，9216 bit の情報を埋め込むことが可能である．多重度を増加するために 36 セットの透かし情報を埋め込む．

6. 実験結果

原画像として**図 9** の 256 × 256 画素の画像を用いた．原画像より生成したグラフを**図 10** に示す．これを元に生成した透し情報は 16 進数で表現すると

$c518ab79a657c330ad630f84a3613abd$

のような 128 bit の情報となる．

図 11 に本方式で電子透かしを生成し埋め込みを行った画像を示す．また，図 11 の電子透かしを埋め込ん

図 9 原画像
Fig. 9 Original image.

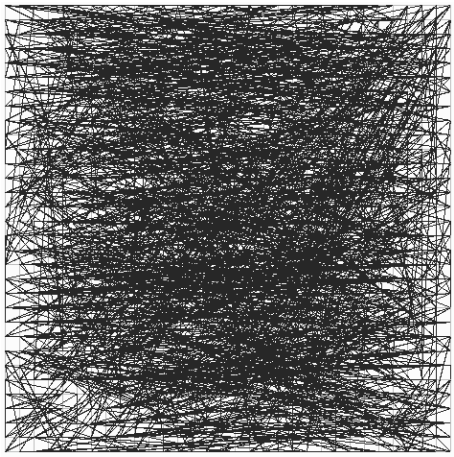

図 10 Region graph の例
Fig. 10 An example of region graph.

図 11 透かしを埋め込んだ画像
Fig. 11 An image including watermark.

だ画像に対して，5.2 節で述べた方法で復号した結果，透かし情報を復号し，4 章で述べた方法により，これが正当なものであることを検証することができた．

7. 考　　察

7.1 ZKIP の利用について

ここで，本方式の有効性について考察する．

本稿の大きな目的の 1 つは，画像の特徴をパラメータとして ZKIP を直接適用することにある．

ZKIP を電子透かしとリンクする利点としては，ZKIP は通常のディジタル署名や認証システムと比較して，証明者の秘密情報漏洩の危険性がないという特徴があげられる．したがって，電子透かしに ZKIP を導入することはセキュリティ上意味がある．また，公開鍵暗号によるディジタル署名を応用した方式とは異なる存在意義がある．

7.2 検証時の原画像の必要性について

電子透かしの構成法には検証時に原画像が必要な方式と必要としない方式がある．原画像が必要な方式は，透かしの検証者に著作権の設定されていない画像を与えてしまうことと等価なため，検証者が画像を詐取して，検証者自信が新たな透かしを埋め込み流通させてしまうことを防ぐための条件として，原画像を必要としないで検証する方式が要求される．

7.3 本方式の有用性について

本方式は電子透かしの情報の正当性の確認に ZKIP を用いており，透かしの作成者と検証者の間で複数回の通信を必要とする．また，透かし情報の耐性向上と透かし情報の情報量削減のため，メッセージダイジェストを用いているため，検証時にこれを圧縮前の情報と確認する作業が必要となる．以上のように通信量やアルゴリズムの複雑など効率の観点から，現状では必ずしも優れているとはいえない．しかし，従来提案されている電子透かしシステムは，透かし情報として，文字や図形の画像パターンやバイナリにエンコードされた文字情報が用いられている．これらの方式は認証におけるパスワード方式と同様に検証者に対して透かし情報のすべてを暴露してしまうことになる．すなわち，検証者が信頼できることを前提としている．したがって，透かし情報を詐取され悪用される可能性が存在する．これを防止するためには，透かし情報が埋め込まれる画像に依存して作成されていないこと，透かし情報が透かし作成者の秘密に依存して作成されていないこと，が求められる．これは，従来の方式では検討されていない概念であり，本方式の従来の電子透かしシステムにはない特徴である．

7.4 耐性について

名画像から G_{block} を生成する際には，攻撃により低域成分の平均値が変化した場合には誤った生成が起こる可能性がある．解決法としては次のようなことが考えられる．同型性の証明時に，前もって証明者と検証者で誤りを確認することができる．ラベルの順序の組合せはブロック数を n とすれば，$n!$ 通りとなるが，異なる画像で同じグラフになる確率も小さいながら存在する．部分的に，この順序が異なる場合でも確率は低下するが画像の同一性は判定可能である．

透かし情報に誤りが生じた場合，3.5 節の透かし情報検証法の (2) の段階で失敗する．領域グラフ生成に誤りを生じた場合，2.1 節のグラフの同型の ZKIP のプロトコル中の step 4 で失敗する．透かし情報と領域グラフのどちらが誤っていたかは以上のように判別可能となる．

透かし情報を不当に他の画像に再利用されることを防ぐためにはどうしたらよいかという点について議論するためには，透かし情報の生成法と透かし情報の埋め込み手法は，ある程度分離して議論した方がよいと考えられる．本稿では透かし情報の生成法について，その問題点と解決法を提案したが，埋め込み手法自体は耐性や効率など今後検討しなければならない課題が多いと考えられる．

8. む　す　び

グラフの同型問題に対する ZKIP を用いた画像に対する新しい電子透かしシステムを提案した．この方法は，著作権の主張などに応用可能である．ZKIP は通常のディジタル署名や認証システムと比較して，証明者の秘密情報漏洩の危険性がないという特徴があげられる．本方式の最大の目的は証明者の秘密情報が漏れることを防ぐことにある．一般に ZKIP を利用するうえではこのような用途ではオンラインの検証システムが必須となる．本方式の想定するアプリケーションとしては，著作権が問題となり裁判で係争するような場合，裁判所などの調停機関と著作権保有者との間で確かに当該画像データが著作見者のものであることを証明する場合などに有効となる．従来の一般的な電子透かしシステムであるオフライン検証システムと本方式のオンライン検証システムを比較すると，前者は透かし検証時に通信を必要としない．一方，本方式は，検証時に透かし生成者との間で通信を必要とするが，より安全性の高い電子透かしシステムを提供可能である．本手法の特徴としては，画像データの 2 次元的特徴をグラフに結び付け，ZKIP を利用したことにより，署

名情報を搾取し，なりすましを行うことを不可能にしたことがあげられる．

ブロックごとの周波数領域のスペクトルに依存して透かし情報が生成されるため，透かし情報は一意に生成される．埋め込みが輝度値に対して適応的に行われ，多重的に情報が埋め込まれているため，透かし情報の除去の耐性が高い．秘密情報となる同型写像の置換は，透かしが埋め込まれた画像および検証過程において，暴露されない．埋め込み法が DCT 係数間の差分情報に基づいているため，透かし情報を分離し，原画像のみを取り出すことは困難である．

今後の課題としては，本方式では電子透かしの確認時に，署名者との間での通信が必要となるが，運用上これをいかにして効率的に行うかという問題がある．また，画像の透かし情報を盗用させないという目的に限定すれば，ZKIP を用いないデジタル署名を適用しても実用上十分機能する場合もあるので，ZKIP の特徴と安全性を生かした電子透かしに対する応用についても検討していく必要がある．

謝辞 本研究は平成 11 年度科研費奨励研究（A）により行われた．

参 考 文 献

1) 木下，塩入，酒井：DCT 符号化に適した画像暗号化方式の提案，信学論，Vol.J75-D-I, No.5, pp.314–321 (1992).
2) Matias, Y. and Shamir, A.: A Video Scrambling Technique Based on Space Filling Curves, *Proc. ICASSP'80*, pp.291–294 (1980).
3) Brassil, J., Low, S., Maxemchuk, N. and Gorman, O.: Electronic Marking and Identification Techniquies to Discourage Document Copying, *Proc. IEEE INFOCOM'94*, Vol.3, pp.1278–1287 (1994).
4) 松井甲子雄，田中 清，中村康弘：再起型 MH 符号によるファクシミリ文書への署名，暗号と情報セキュリティシンポジウム，CIS89 (1989).
5) 小松尚久，山田道夫，富永英義：文書画像通信におけるディジタル透かしの提案，暗号と情報セキュリティシンポジウム，CIS89 (1989).
6) 松谷秀久，稲葉宏幸，若杉耕一朗，笠原正雄：著作権保護機能を有する文書画像データの構成法，信学技法，ISEC94-58, pp.59–67 (1995).
7) 西村純則，若杉耕一朗，笠原正雄：多値画像情報の不正複製防止に関する考察，信学技法，ISEC94-58, pp.33–39 (1994).
8) Kutter, M., Bhattacharjee, S.K. and Ebrahimi, T.: Towards second generation watermarking schemes, *IEEE International Conference on Image Processing*, ICIP99, 25PO2.8 (1999).
9) Chaum, D. and van Antwerpen, H.: Undeniable signatures, *Proc. CRYPTO'89*, SpringerLNCS#445 (1989).
10) 松田洋一，中野秀男：グラフ問題を使ったゼロ知識証明プロトコルの効率，暗号と情報セキュリティシンポジウム，CIS89, 4B (1989).
11) Jhonson, D.: The NP-Completeness Column: An Ongoing Guide, *J. Algorithms*, Vol.6, No.3, pp.434–451 (1985).
12) Galil, Z., Hoffmann, C., Luks, E., Schnorr, C. and Weber, A.: An $O(n^3 \log n)$ Deterministic and an $O(n^3)$ Las Vegas Isomorphism Test for Trivalent Graphs, *J. ACM*, Vol.34, No.3, pp.513–531 (1987).
13) 中村康宏，松井甲子雄：著作権保護のための和文書へのシール画像の埋込み，情報処理学会論文誌，Vol.38, No.11, pp.2356–2361 (1997).
14) Goldwasser, S., Micali, S. and Rackoff, C.: The Knowledge Complexity of Interactive Proof Systems, *Proc. STOC*, pp.291–304 (1985).

(平成 12 年 5 月 1 日受付)
(平成 13 年 2 月 1 日採録)

木下 宏揚（正会員）

1962 年生．1985 年電気通信大学電気通信学部電子情報学科卒業．1990 年東京工業大学大学院工学研究科電気・電子工学専攻博士後期課程修了．1990 年東京工業大学助手．1994 年玉川大学講師．1999 年より神奈川大学工学部助教授．情報セキュリティの研究開発に従事．工学博士．

小林 輝伸

1974 年生．1999 年神奈川大学工学部電気工学科卒業．1999 年神奈川大学大学院入学．電子透かしの研究開発に従事．