

(19)日本国特許庁(JP)

(12)特許公報(B2)

(11)特許番号
特許第7207627号
(P7207627)

(45)発行日 令和5年1月18日(2023.1.18)

(24)登録日 令和5年1月10日(2023.1.10)

(51)国際特許分類 F I
 H 0 4 N 1/32 (2006.01) H 0 4 N 1/32 1 4 4
 G 0 6 T 1/00 (2006.01) G 0 6 T 1/00 5 0 0 B

請求項の数 1 (全16頁)

(21)出願番号	特願2019-87181(P2019-87181)	(73)特許権者	711001893
(22)出願日	令和1年5月3日(2019.5.3)		河村 尚登
(65)公開番号	特開2020-184663(P2020-184663 A)		神奈川県川崎市多摩区菅北浦5丁目7番 50号
(43)公開日	令和2年11月12日(2020.11.12)	(72)発明者	河村尚登
審査請求日	令和4年4月15日(2022.4.15)		神奈川県川崎市多摩区菅北浦5-7-5 0
		審査官	花田 尚樹

最終頁に続く

(54)【発明の名称】 高耐性電子透かし法

(57)【特許請求の範囲】

【請求項1】

画像データ $l(x,y)$ を $R \times R$ のブロックに分割し、ブロック毎に透かし情報ビットに対応した異なるパターンを埋め込む電子透かし法において、

埋め込みパターンはグリーンノイズ特性を示す複数の異なる基本パターン $P_i(x,y)$ を、ブロック毎に異なる位相シフト量 (x_0,y_0) (ただし、 $0 \leq x_0,y_0 < R$)を用いて、 x 方向に x_0 、 y 方向に y_0 だけシフトさせたもので、

$$P'_i(x,y) = P_i((x+x_0) \bmod R, (y+y_0) \bmod R)$$

(ここで、 $P'_i(x,y)$ はシフト後のパターン、 $\bmod R$ は R を法とする剰余)

なる演算式で求められ、

透かしの埋め込みは、かかるパターン $P'_i(x,y)$ を用いて、

$$W(x,y) = l(x,y) + \text{gain} \cdot P'_i(x,y)$$

(ここで、 gain は埋め込み強度)

なる演算にて行い、

前記位相シフト量 (x_0,y_0) は、乱数発生器で発生し位相シフトリスト $L(n)$ (n はブロック番号)に記憶し、

鍵として、基本パターン $P_i(x,y)$ 、埋め込み強度(gain)及び位相シフトリスト $L(n)$ を保管し、

透かし情報の抽出は、透かしの埋め込まれた画像データをブロックに分割し、ブロックのフーリエスペクトルパターンの形状から、埋め込みビット情報を抽出するもので、位相シフト量によらず同じ抽出ソフトウェアで実行可能であり、

透かしの除去は、透かしの埋め込まれた画像 $W(x,y)$ に、鍵を用いて、

$$l(x,y)=W(x,y)-gain \cdot P'i(x,y)$$

なる演算にて除去を行い原画に戻すことや新たな情報を埋め込むことが可能な可逆型電子透かし方法。

【発明の詳細な説明】

【技術分野】

【0001】

本発明は、デジタル画像データに著作権情報などの透かし情報を埋め込む電子透かし法で、特に、特にアルゴリズムを公開しても第三者からの攻撃に対して高耐性を示す不可視型で可逆の電子透かし方法に関するものである。

10

【背景技術】

【0002】

現在のデジタル情報社会において、情報を手軽に複製でき、多くの人が情報を共有することが可能となり、社会が大きく発展してきた。しかし、その利便性が、他人の著作物を違法に複製し流通させることにより、著作権侵害などの事件を引き起こすことにもなった。画像においては、近年のデジタルカメラやプリンタの高画質化により、原画と寸分も違わぬ複製が容易に得られるようになり、著作権を侵害した違反コピーだけでなく、紙幣や有価証券等の偽造行為という悪質な犯罪行為を助長させる結果となっている。

【0003】

そのような状況の中で、画像情報の中に別の情報、例えば、著作者情報等を埋め込み、著作権を保護したり、違法複製に警告を与えたりする不可視の電子透かし (Digital Water mark) 技術が発展してきた。この電子透かし技術は、例えば、著作権保護の目的には、文書や画像の著作物の中に著作権者やURL、連絡先、利用条件などを埋め込み、利用者に注意を喚起するのみならず、不正利用された場合には、その追跡を可能とする。このように、著作権の管理・保護、ならびに不正複製の監視など、セキュリティ対策として電子透かしが広く使われ始めている。

20

【0004】

このセキュリティ対策としての電子透かしは、頑強で簡単に消失あるいは除去できない高耐性のものでなければならない。画像の編集加工や簡単な操作で透かし情報を除去や消去ができるならば、不正使用して追跡や監視の目から逃れることができるからである。

30

【0005】

通常、耐性を強化するためには、電子透かしを画像データの深層に埋め込む必要がある。このため、埋め込みの強度 (gain) を大きくして埋め込む。これは、原画像に対してダメージが増大し、画質が劣化するという弊害をもたらす。つまり、画質と耐性とはお互いにトレードオフの関係にあり、両方を満たすことは通常困難である。

【0006】

画質と耐性を同時に満たす電子透かし法として、特許文献1から6および非特許文献1から2に示されるグリーンノイズパターンを画像データに埋め込む手法 (以降、グリーンノイズ拡散法と呼ぶ) をこれまで提案してきた。グリーンノイズパターンは、そのスペクトルが特定の帯域 $f_{max} \sim f_{min}$ に閉じ込められ、その主周波数は、人の視覚特性で認識できにくい周波数帯に設定できる。このため、電子透かしに用いた場合、埋め込み画像を明視の距離で観察した場合、ドットパターンは低い応答性を示しアーティファクトは認識されにくい。また、プリンタやスキャナーでの書き込みや読み取りでは高い応答感度を有するため、印刷しても埋め込み情報は保持できる。信頼度を上げるため、埋め込み強度 (gain) を上げてアーティファクトが視認され難く、高画質性が保たれる特徴がある。

40

【0007】

グリーンノイズ拡散法はスペクトル拡散法と同じ様に編集や加工に強靱であるが、第三者が不正利用のために透かし情報を除去することに対しても、強固でなければならない。第三者が様々な方法、様々な画像、様々な情報で埋め込みアルゴリズムを解析・推定し攻撃する (以降、結託攻撃と呼ぶ) ことにより、埋め込み画像から透かし情報を除去し、原画

50

に戻すことにより、不正利用を可能としてしまう。アルゴリズム公開型の電子透かしでは、アルゴリズムを知ることにより信号処理を逆解析することが容易で、このため攻撃を受けやすい。埋め込みのパラメータは、通常、“鍵”という形で保持される。この鍵は、通常、埋め込む画素の位置情報や、強さ（gain情報）、乱数列、ハッシュ関数のパスワードなど、各種パラメータを用い、鍵情報がなければ透かしの除去はできない。結託攻撃ではこの鍵の情報を推定することである。

【0008】

ステガノグラフィとしての利用形態では、秘密情報をこっそり画像中に埋め込み、鍵なしでは透かし抽出が出来ないようになっている。このため、アルゴリズムは非公開である。しかし、著作権保護を目的とする電子透かし法は、利用者が誰でも著作権情報の有無や条件などを知ることが出来る必要があり、透かし抽出は誰でも簡単にできるようにする必要があり。また、広く普及するためには、業界で統一された手法として標準化が必要で、アルゴリズムが公開できることが望ましい。

10

【0009】

この時、アルゴリズムを公開しても安全性が確保されるためには、通常、非対称型の電子透かし手法が望ましいとされている。対称型は、透かしの埋め込みと逆手順で抽出を行うので、埋め込み位置や方法などが発覚されやすく攻撃を受けやすいからである。

グリーンノイズ拡散法は埋め込みは実空間で、抽出はスペクトル空間で行われる非対称型で、かつ、グリーンノイズパターンはランダムドットが拡散したパターンのためスペクトラム拡散と同じ様に完全に除去することは一般に難しい。アルゴリズムを公開したとしても、埋め込みの各種パラメータは秘密情報として「秘密鍵」の形で受領者に渡される。秘密性はこの鍵に集約され、安全性が担保され、通常は、この鍵がなければ透かしの除去はできないようになっている。

20

【0010】

さらに、画像ごとに埋め込みパターンなどのパラメータを変えるため、鍵情報は画像ごとに異なる。このため、鍵を紛失したり盗難されたりしても、その鍵で他の画像を操作し、透かしを除去することはできない。

【0011】

そのうえで、前述の結託攻撃に対する対策が必要である。結託攻撃では、鍵なしで原画像との差分をとることや、平坦部の多い画像、複数の画像から、埋め込みの特徴、画像の相関などから、埋め込みパラメータやパターンなどを解読し鍵情報を割り出す。このため、このような攻撃に対する対策が必要である。第三者からのこのような結託攻撃は、近年のAI技術を用いた機械学習を用いて種々のパターンを学習することにより、鍵情報を推定することが可能となりつつある。特に、ブロック型の電子透かし法では、ブロック毎に透かし情報を埋め込むため、1枚の画像からブロック数だけの多数の学習データが揃うため、埋め込みパラメータの推定が行いやすい。

30

【0012】

このため、特許文献5では、埋め込むグリーンノイズパターンに反転パターンを用いてその数を増やし、埋め込むビット情報（0, 1）に対して複数のパターンの選択を乱数列として鍵情報に入れる方法を提案した。複数パターンはオリジナルパターンの空間的反転パターンと輝度データの反転パターン（ネガ/ポジのパターン）から成り、一つのグリーンノイズパターンに対して8つの反転パターンを生成した。このため、パターンの種類と数が増え、同じパターンが繰り返して出るというリスクは減少し、安全性は改善される。

40

【0013】

しかし、反転パターンのみではパターンの位相（空間位置情報のシフト量）がなく常に同じ位相であるため、多くのパターン埋め込み情報からパターンの同定が可能であり、まだ、完全に安全であるとは言えない。

【先行技術文献】

【特許文献】

【0014】

50

【文献】特開2018-182471

特開2018-201134

特開2018-207247

特願2017-117460

特願2018-216362

特願2019-000178

【非特許文献】

【0015】

【文献】N.Kawamura; " Digital Halftoning by Clustered Dither Screen Masks Representing Green-noise Characteristics ", Proceeding of the 1st ICAI 2015, T10 9-3, pp.708-711 (2015).

10

N.Kawamura; " Digital Halftoning by Stochastic Dither Screen Mask Representing Green to Blue Noise Characteristics ", Trans. on IEVC, Vol.5, No.1, pp.34-41 (2017).

【発明の概要】

【発明が解決しようとする課題】

【0016】

そこで、高画質と編集・加工に対する耐性を維持し、結託攻撃に対しても十分強固な電子透かし法を得ることが課題である。すなわちアルゴリズム公開型電子透かし法において、第三者が鍵なしに埋め込みパターンの解析により埋め込みパターンを割り出すことが出来ない強い耐性を示す電子透かし法を得ることが課題である。

20

【課題を解決するための手段】

【0017】

前記課題を解決するために、本発明は、画像をブロック分割し、ブロックごとに透かし情報を埋め込む電子透かし法において、グリーンノイズ特性を示す埋め込みパターンを原画像に重畳し埋め込む際、ブロック毎にパターンの位相をシフトあるいは変動させて埋め込む。

【0018】

すなわち、画像データ $l(x,y)$ を $R \times R$ のブロックに分割し、ブロック毎に透かし情報ビットに対応した異なるパターンを埋め込む電子透かし法において、埋め込みパターンはグリーンノイズ特性を示す複数の異なる基本パターン $P_i(x,y)$ を、ブロック毎に異なる位相シフト量 (x_0,y_0) (ただし、 $0 \leq x_0,y_0 < R$) を用いて、 x 方向に x_0 、 y 方向に y_0 だけシフトさせたもので、 $P'_i(x,y) = P_i((x+x_0) \bmod R, (y+y_0) \bmod R)$ (ここで、 $P'_i(x,y)$ はシフト後のパターン、 $\bmod R$ は R を法とする剰余) なる演算式で求められ、透かしの埋め込みは、かかるパターン $P'_i(x,y)$ を用いて、 $W(x,y) = l(x,y) + \text{gain} \cdot P'_i(x,y)$ (ここで gain は埋め込み強度) なる演算にて行い、前記位相シフト量 (x_0,y_0) は、乱数発生器で発生し位相シフトリスト $L(n)$ (n はブロック番号)に記憶し、鍵として、基本パターン $P_i(x,y)$ 、埋め込み強度 (gain) 及び位相シフトリスト $L(n)$ を保管し、透かし情報の抽出は、透かしの埋め込まれた画像データをブロックに分割し、ブロックのフーリエスペクトルパターンの形状から、埋め込みビット情報を抽出するもので、位相シフト量によらず同じ抽出ソフトウェアで実行可能であり、透かしの除去は、透かしの埋め込まれた画像 $W(x,y)$ に、鍵を用いて、 $l(x,y) = W(x,y) - \text{gain} \cdot P'_i(x,y)$ なる演算にて除去を行い原画に戻すことや新たな情報を埋め込むことが可能なことを特徴とする。

30

40

【0019】

かかる位相をシフトさせたパターン $P'_i(x,y)$ は、 $R \times R$ の基本パターン $P_i(x,y)$ をベースに、 (x_0,y_0) (ただし、 $0 \leq x_0,y_0 < R$) だけシフトさせたもので、シフト量 (x_0,y_0) はブロック毎に異なる値をとるが、透かしの埋め込まれたブロックのフーリエスペクトルパターンの形状は、位相シフト量によらず同じスペクトル形状を示すため、透かし情報の抽出は、この位相シフト量の変更に伴う抽出ソフトウェアの変更は不要であり、透かしを除去する時のみ、この鍵を用いて透かしを除去する。このようにすることにより、結託攻撃から

50

パターンの推定を困難にすることが出来る。

【 0 0 2 0 】

かかる埋め込みパターン $P_i(x,y)$ は、画像ごとに異なる初期値から生成されたグリーンノイズパターンであり、シフトリスト $L(n)$ は、画像ごとに異なるシフト列から構成され、これらが組み込まれた鍵で他の画像の透かしを除去できない。

【 発明の効果 】

【 0 0 2 1 】

本発明により、編集加工による高耐性と、第三者からの結託攻撃に対する耐性が備わり、頑強で、鍵なしでは透かしの除去ができない安全な電子透かしを得ることができる。

【 0 0 2 2 】

また、鍵により元の画像に復元可能である。これは画像の購入者が、配信者から直接原画を配信してもらう手間を省くことができるし、原画での配信を行うことがないため、漏洩や盗難などの心配もなく、セキュリティ上も安全性が高い。さらに購入者はその鍵を用いて、編集加工した画像に第二著作者としての著作権情報を埋め込むことができる。

【 0 0 2 3 】

かかる鍵は、基本となるパターン $P_i(x,y)$ と、gain(埋め込み強度)および位相シフトリスト $L(n)$ のみでよく、鍵のサイズを小さくすることが可能で取り扱いが簡単である。

【 0 0 2 4 】

また、鍵に含まれる基本パターン $P_i(x,y)$ は、画像ごとに異なるグリーンノイズパターンを用い、鍵の紛失や盗難時にも、この鍵を用いて他の画像の透かし除去はできない。このため安全性は極めて高い。

【 0 0 2 5 】

埋め込まれた画像は、シフトパターンにより、埋め込み画像から埋め込みパターンを推定する結託攻撃に対しても安全性は確保されている。このため、アルゴリズムを公開してもそのアルゴリズムから埋め込みパターンを推定することはできず、攻撃の助長とはならない。

【 図面の簡単な説明 】

【 0 0 2 6 】

【 図 1 】 本発明の電子透かしの埋め込みおよび抽出の装置の図、

【 図 2 】 透かし入り画像のインターネットでの配信を示した図、

【 図 3 】 埋め込み用ドットパターン生成のフローを示す図、

【 図 4 】 ドットパターンのスペクトルの回転方向と埋め込みビットを表す図、

【 図 5 】 埋め込み用ドットパターン生成時におけるフィルタの形状を示す図

【 図 6 】 生成されたドットパターンとそのスペクトルおよび埋め込み情報を示す図、

【 図 7 】 透かし埋め込みの処理フローを表す図、

【 図 8 】 透かし抽出の処理フローを表す図、

【 図 9 】 パターン識別の処理フローを表す図、

【 図 1 0 】 マスクパターンを示す図、

【 図 1 1 】 位相シフトパターンを示す図、

【 図 1 2 】 乱数発生による位相シフトパターンを示す図、

【 図 1 3 】 基本パターンと位相シフトパターンおよびそれらのスペクトルを表す図で、(a)は $R=64$ 、(b)は $R=32$ の場合を示す。

【 図 1 4 】 256×256 の画像に埋め込みを行ったときの画像で、(a)は原画像、(b)は埋め込み画像、(c)はそのスペクトルを表す画像。

【 発明を実施するための形態 】

【 0 0 2 7 】

図 1 は本発明の情報埋め込みと抽出のための電子透かしシステムの構成図である。著作権保有者のコンピュータ 3 には、著作権を有す画像データが、例えばハードディスクなどのデータメモリ 7 に保管されている。画像データは、プログラムメモリ 6 にある画像処理プログラムにより、CPU 1 1 , ROM 4 , RAM 5 などを用いて画像処理され、モニター

10

20

30

40

50

8に表示される。コンピュータ3にはスキャナ1、プリンタ2が接続され、処理された画像はプリンタから出力し、またスキャナ1から画像読み取りができる。かかる画像処理は大きなサイズの画像を取り扱う場合、演算負荷が増大するため、並列処理を行うことや、GPUなどの高速化を図るための処理ボードが入っている場合もある。

【0028】

画像中に著作権情報を埋め込むためには、キーボード9から、例えば、著作者の名前や日付、URLなどの文字情報を入れるが、埋め込む文字数は、最低16文字は必要となる。これはASCIIコードの文字で埋め込むものとして16バイト(128ビット)が必要となる。

【0029】

図2は、一つの運用形態を示すもので、インターネット配信の処理手順を示すものである。透かし情報を埋め込まれた画像は、配信者あるいは著作権者16のコンピュータやサーバーからインターネット12により配信や展示される(13)。それを見た購入希望者17は、購入希望を配信者に連絡する(14)。所定の手続き後、配信者は透かしの埋め込みと除去のための秘密鍵を配信する(15)。購入者は、配信者との契約に基づき、送付された画像の埋め込まれた電子透かしを除去し、画像の編集加工を行うことができる。

【0030】

購入者は、さらに編集加工された画像データを、2次著作者として自己の著作情報やURLなどの情報をこの秘密鍵を用いて埋め込むことができる。これらの透かし情報を埋め込まれた画像は、公開され市場に流通し様々な利用がされる。

【0031】

その画像を見た第三者は、透かし抽出ソフトにより、この画像に著作権があることを確認できる。透かし抽出ソフトウェアには秘密性はなく、例えば、配信者や著作権者のホームページなどから自由にダウンロードできるようにして広く公開し、だれでも使用できる。第三者はこれにより画像の所有者や著作権情報、連絡先などを知ることができるため、不正使用の防止・警告にもなる。

【0032】

一方、著作権者や二次著作権者は、その透かしにより、著作物としての画像データの追跡と監視を行うことが可能である。もし、第三者が不正に使用した場合、著作権者や二次著作権者は、監視ソフトウェアにより画像から透かし情報を読みだし、自己の著作物であること、さらに第三者が無断で使用している場合には摘発が可能となる。

【0033】

鍵は埋め込む画像ごとに1対1で対応する。このため、著作権者は悪用されないように画像ごとに異なる鍵を用いる。この鍵を用いて他の画像の透かしを除去することはできない。鍵の紛失や第三者による結託攻撃による鍵の取得が起きても、その被害は該当する1枚の画像のみで、他の画像に対しては透かし除去はできない。このとき、透かし読み出しのソフトウェアは、鍵が異なっても共通に使える。また、鍵の発行はほぼ無限に行えるため、同じ鍵となる確率は極めて低い。

【実施例】

【0034】

以下、実施例に沿って詳しく説明する。

ここで、まず本発明に用いられるグリーンノイズ特性を示すドットパターンの生成について図3に沿って説明する。

今、マトリックスサイズをR画素×R画素($R=2^m$ ここで $^{\wedge}$ はべき乗)として、その中に1画素サイズの黒ドットを埋め込むものとする。黒ドットの面積率を g ($0 \leq g \leq 1$: $g=1$ が全黒, $g=0$ が全白)とする。点 (x,y) におけるドットパターンを $p(x,y)$ として、 $g=1/2$ のグリーンノイズ特性を示すドットパターンを以下の様にして求める。

(工程1) まず、疑似乱数発生器により、ランダムドット $p(x,y)$ を生成する(20)。この時、疑似乱数発生器のSEED値を変えることにより初期状態を変更可能である。

(工程2) $p(x,y)$ を二次元フーリエ変換を行いスペクトル $P(u,v)$ を得る(21)。ここで、

10

20

30

40

50

(x, y)は空間座標、(u, v)は空間周波数座標を表す。 $g=0.5$ の場合、 $(R^2)/2$ 個のランダムドット(初期状態はホワイトノイズ)を発生させ、 $p(x, y)$ とする。

(工程3) $P(u, v)$ にフィルタ $D(u, v)$ を掛けて新たな $P'(u, v)$ を得る(22)。すなわち、

$$P'(u, v) = P(u, v) \cdot D(u, v)$$

(工程4) $P'(u, v)$ に逆フーリエ変換を行い、多値の点プロファイル $p'(x, y)$ を得る(23)。

(工程5) 誤差関数 $e(x, y) = p'(x, y) - p(x, y)$ を求め(24)、各画素位置での誤差の大きい順に白, 黒同数反転する(25)。

(工程6) 工程2から工程5までの操作を誤差が許容量以内になるまで繰り返し、最終的に $g=1/2$ のドットパターンを得る。

【0035】

ここで、フィルタ $D(u, v)$ のパターンの設定について説明する。今、 $D(u, v)$ が円形のリングパターンで、その最大ラジアル周波数を f_{max} 、最小ラジアル周波数を f_{min} であるとする。 $g=1/2$ での平均的ドット間隔による周波数 f_0 は、

$$f_0 = g \cdot f_n = (1/2) \cdot f_n$$

与えられ、 f_{max} 及び f_{min} は f_0 を基準として、

$$a = (f_{max} - f_0) / f_n$$

$$b = (f_{min} - f_0) / f_n$$

として、パラメータ(a, b)を定義する。ここで、 f_n はナイキスト周波数を示す。かかる(a, b)を変化させて、視覚特性に合わせてクラスターサイズの異なるドットパターンを得ることができる。

【0036】

透かし埋め込みは4値のパターンで行うものとする。このためには埋め込み2ビット(00, 01, 10, 11)に対応した4種類のパターンが必要である。そのためフィルタ $D(u, v)$ のパターンが楕円リングパターンで、 45° づつ回転した4つのパターンとなるようにする。図4はフィルタパターンを模式的に示すもので、楕円リングの短軸の最小値を f_{min} 、最大値を f_{max} とし、長軸の最小値を $\cdot f_{min}$ 、最大値を $\cdot f_{max}$ とする。ここで、 \cdot は倍率を表す。正立したものを2ビットの(00)に対応するフィルタパターン、それを 45° 回転したものを(01)、 90° 回転したものをビット(10)、 135° 回転したものを(11)にそれぞれ対応するものとする。このようにして得られた4つの透かしパターンを $P_i(x, y)$ ($i=0, \dots, 3$)と表記するものとする。

【0037】

図5に、かかる4つのフィルタ(フィルタ0、フィルタ1、フィルタ2、フィルタ3)の形状を示す。図で黒領域は0、白領域は1を表す。図6に、このフィルタ $D(u, v)$ を用いて、前述の工程を経て作成されたパターンおよびスペクトルを示す。各パターンは $R \times R$ のサイズで、パターン0は2ビットの埋め込み情報(00)に対応し、パターン1は(01)、パターン2は(10)、パターン3は(11)にそれぞれ対応する。

【0038】

続いて、画像データへの透かし埋め込み手法について説明する。透かし情報の埋め込みは、赤(R)、緑(G)、青(B)からなるカラー画像データの青(B)データに埋め込むか、あるいは、輝度、色差信号となる(Y, C_b, C_r)信号に変換し、輝度(Y)データに埋め込むことが考えられる。電子データでのみ透かし情報を取り扱う場合は、青(B)に埋め込むのがもっとも視覚的には認識されにくく理想的である。印刷画像やモニター画像をカメラやスキャナーで読み取るような応用を考えた場合は、青(B)データ(印刷時はイエロー)は精度よく色分離することが難しいため、輝度(Y)データを用いるのが良い。

【0039】

続いて、図7のフローに沿って処理手順を説明する。まず、埋め込み情報をビット列に変換し、 w_m とする(20)。例えば、埋め込みたい情報が“0123456789abcdef”となるASCII16文字をビット列に展開すると、 $w_m = “0011000000110001...”$ となる128ビット列となる。先頭ビットから i 番目のビットを $w_m(i)$ とする。

【0040】

10

20

30

40

50

次に、画像データをR画素×R画素のブロックに分割する(21)。これはドットパターンのサイズと同じサイズにする必要がある。ブロックサイズとしては、64画素×64画素を用いると高精度に抽出できるが、多くの情報を埋め込みたい場合は32画素×32画素をブロックサイズとすると、4倍の情報の埋め込みが可能となる。

【0041】

埋め込み作業はブロック単位で行われる。n番目のブロックに埋め込む(23)として、まず、n=1からスタートする(22)。埋め込み透かし情報を先頭から連続した2ビットを取り出し、これを $b = (wm(i), wm(i+1))$ とする。

【0042】

bの値により埋め込むパターンを選択する(24)。b=(00)の場合はパターン0を用いて埋め込む(25a)。同様に、b=(01)の場合はパターン1を用いて埋め込む(25b)。b=(10)の場合はパターン2を用いて埋め込む(25c)。b=(11)の場合はパターン3を用いて埋め込む(25d)。

10

【0043】

かかる透かし情報の埋め込みは実空間(画素空間)で行う。今、画像データを $l(x,y)$ 、埋め込み強度をgain、透かしの埋め込まれた画像データを $W(x,y)$ とすると、

$$W(x,y) = l(x,y) + \text{gain} \cdot P_i(x,y) \quad (i=0,1,2,3) \quad \text{----- (1)}$$

ただし、

b=(00)の時 $P_i(x,y)$ はパターン0

b=(01)の時 $P_i(x,y)$ はパターン1

b=(10)の時 $P_i(x,y)$ はパターン2

b=(11)の時 $P_i(x,y)$ はパターン3

20

となる。 P_i は(1,0)の二値であるが、平均輝度を保存するため(1/2, -1/2)とする。埋め込んだ結果、画素データがダイナミックレンジを超えてオーバーフローやアンダーフローが生じることがあるため、あらかじめ画像データに以下の線形変換を施した画像 $l'(x,y)$ にて行うこともある。

$$l'(x,y) = (1 - \text{gain}) \cdot l(x,y) + \text{gain}/2 \quad \text{----- (2)}$$

この処理は後述の透かし情報を完全に除去する場合には必須であるが、除去を必要としない場合や、オーバーフローやアンダーフローの頻度が低い場合は省略しても構わない。全ブロックが終了かを判断し(26)、終了でない場合は次のブロックへ移る(27)。

30

【0044】

以上のようにして、埋め込みビット列 $wm(i)$ をすべて埋め込む。埋め込みブロック数が埋め込みビット数より多い場合は、繰り返し埋め込むことで信頼度を高めることができる。この場合は文字列の先頭を示す区切りマーカが必要である。

埋め込まれた画像は、 $P_i(x,y)$ はランダムドットであるため、ブロック境界は目立たない。グリーンノイズ特性を示すドットパターンは、印刷におけるFMスクリーンとしても用いられ、分散性ドットで均一性にすぐれているため視覚的にも一様で粒状性も感じさせない。

【0045】

続いて、透かし情報の抽出について図8の処理フローに沿って説明する。抽出作業は、埋め込み時と同様R×Rのブロックに分割し(30)、ブロック単位で行われる。n番目のブロックから抽出するものとして、n=1からスタートする(31)。n番目のブロックからR×Rの画像を取り出しFFT(高速フーリエ変換)を行い、スペクトル情報 W_n に変換する(32)。続いて、ヒストグラムイコライゼーションによる規格化を行う(33)。これは、ブロック毎に輝度が異なるため、コントラストを向上させて識別精度を向上させることと、後述の信頼度を各ブロックで平等に評価するためである。続いて後述のパターンの識別を行い(40)、識別パターンから埋め込み情報の2ビットデータを抽出する(34)。ブロックがすべて終わったか否かを判断し(35)、終了していない場合はnをn+1として(36)、次のブロックへ移る。終了した場合は全ビットを取り出して、元の文字情報を復元する(37)。

40

【0046】

50

図9はパターン識別処理(40)の処理フローを示す。ブロック内のスペクトル情報 W_n は、用意されたマスクパターンとのマッチングを行い、その出力 Q_i を求める(41)。マスクパターンは図10に示すようにフィルタパターンと同じで、 45° 毎に回転したマスク0(M0)、マスク1(M1)、マスク2(M2)、マスク3(M3)の4つが用意されている。図9に戻って、 i 番目のマスクを M_i として、 W_n とのマッチングの出力 Q_i は、

$$Q_i = (1/Z_i) M_i \cdot W_n \quad (i=0,1,2,3) \quad \text{----- (3)}$$

ただし $Z_i = M_i$

として求められる(42)。ただし、はブロック内の各画素(今の場合は空間周波数に対応)について行われる。その結果、各マスクに対応した出力(Q_0, Q_1, Q_2, Q_3)が得られる。この4つの出力のうち最も大きいものを Q_{max} として、

$$Q_{max} = Q_0 \text{ の時、 } b=00$$

$$Q_{max} = Q_1 \text{ の時、 } b=01$$

$$Q_{max} = Q_2 \text{ の時、 } b=10$$

$$Q_{max} = Q_3 \text{ の時、 } b=11$$

となる2ビットの透かし情報 b を得る(43および44a、44b、44c、44d)。

【0047】

次に、 Q_{max} の次に大きな出力を Q_{next} とすると、信頼度 rel は

$$rel = Q_{max} - Q_{next} \quad \text{----- (4)}$$

で表される。すなわち Q_{next} が Q_{max} に非常に近い値の場合は誤判定の確率が高く、 Q_{max} と Q_{next} との差が大きい程信頼性は高い。この差を信頼度の指標とすることができる。

以上のようにして、2ビットの埋め込み情報 b と信頼度 rel が求まる。

【0048】

透かしの除去は、埋め込みを減算することで可能となる。すなわち、式(1)より、

$$I(x,y) = W(x,y) - gain \cdot P_i(x,y) \quad (i=0,1,2,3) \quad \text{----- (5)}$$

となり、透かし埋め込み画像から埋め込みパターンに $gain$ を乗じて引くことで、完全に原画に戻すことが可能である。ただし、埋め込み時にオーバーフローやアンダーフローを避けるために線形ダイナミックレンジ補正を行った場合は、逆補正をする必要がある。

以上のようにして透かし除去が可能であるが、埋め込みパターン(パターン0、パターン1、パターン2、パターン3)および $gain$ が必要となる。

【0049】

かかる秘密鍵の容量は、例えばブロックサイズが 64×64 の場合、パターン0～パターン3までの4パターン分で16Kビット(2Kバイト)、それに $gain$ と埋め込み情報の容量が加わる。 32×32 の場合はパターン0～パターン3までの4パターン分で4Kビット(512バイト)となる。 $gain$ は、通常、100バイト以下であるので、鍵容量の大半は埋め込みパターン情報が占める。

【0050】

鍵の容量はなるべく小さくした方が取り扱いが容易である。鍵容量を減らすため、パターン2、パターン3は、それぞれ、パターン0、パターン1から生成することができる。すなわち、パターン2はパターン0を 90° 回転したもの、パターン3はパターン1を 90° 回転したものを採用する。ドットパターンの回転はそのままスペクトルの回転となるため、他の処理の変更はない。

【0051】

鍵の紛失や盗難に対しては、画像ごとに異なるドットパターンを用いることにより、同じ鍵で別の画像の透かしを除去することはできなくすることができる。これらは、グリーンノイズパターン生成時の、初期乱数のseed値を変えることによって得られる。スペクトル分布は同一であり、抽出ソフトウェアは共通であるが、ドットプロファイルは異なる。 $R=64$ の場合、1つのドットパターンにつき異なるパターン数は、 4096×2048 個あり、複数のドットパターンを用いる場合は、その積となるため、同じパターンとなる確率は極めて低いため、安全性は高い。ここで、 C はcombinationを表す。著作権者は購入者に対してそれぞれ異なる乱数から求めたドットパターンを秘密鍵として提供する。購入者ごとに

10

20

30

40

50

この鍵は異なるため、他の購入者の画像から透かしを除去することはできない。

【 0 0 5 2 】

次に位相シフトパターンについて説明する。

$P_i(x,y)$ はグリーンノイズパターンであるため、境界がない。このため位相シフトしたパターンも目立たない特徴がある。そこでこのパターンの位相をシフトしたパターン $P'_i(x,y)$ を生成する。

今、 $R \times R$ の基本パターン $P_i(x,y)$ の位相を x 方向に x_0 、 y 方向に y_0 だけシフトしたものを $P'_i(x,y)$ とする。ただし、シフト量は、 $0 \leq x_0, y_0 < R$ であるとする。 $P'_i(x,y)$ は以下の式で表される。

$$P'_i(x,y) = P_i((x+x_0) \bmod R, (y+y_0) \bmod R) \quad \text{----- (6)} \tag{10}$$

ここで、 $\bmod R$ は R を法とした剰余を表す。つまり、 $x+x_0, y+y_0$ の値が R を超えた場合は先頭に戻り、位相シフトしたパターンが得られる。

【 0 0 5 3 】

位相シフトされた埋め込みパターン $P'_i(x,y)$ を用いて、埋め込みは、位相シフトのない場合と同様に以下のように行われる。

$$W(x,y) = I(x,y) + \text{gain} \cdot P'_i(x,y) \quad \text{----- (7)}$$

ただし、 $P'_i(x,y)$ は式(6)で示されたものである

【 0 0 5 4 】

図11は、位相シフトされた埋め込みパターン $P'_i(x,y)$ を示したもので、 $(x_0, y_0) = (0, 0)$ のパターンをベースに x, y 方向に $R/4, R/2$ 位相シフトした時のパターンである。 $R=32$ の時、シフト量 s は、すべての組み合わせで16パターンあるが、そのうちの $(0, 0)$ 、 $(8, 8)$ 、 $(16, 16)$ 、 $(24, 24)$ 、 $(0, 24)$ 、 $(0, 16)$ 、 $(16, 8)$ 、 $(24, 0)$ の8つのパターンを示す。実際の運用時は、シフト量が知られないように、乱数発生器でシフト量 s を決める。図12は乱数で $0 \sim (W-1)$ までの整数値を発生させたもので、シフト量 s は、1024パターンあるが、そのうちの $(22, 25)$ 、 $(23, 17)$ 、 $(6, 17)$ 、 $(28, 13)$ 、 $(30, 8)$ 、 $(9, 14)$ 、 $(19, 14)$ 、 $(30, 0)$ の s_0 から s_7 までの8パターンのみを示す。

20

【 0 0 5 5 】

これらのパターンはすべて同じスペクトル特性を示す。図13に位相シフトある場合とない場合のパターンとそのスペクトル分布を示す。一例として、シフト値 $(x_0, y_0) = (R/2, R/2)$ として、 $R=64$ の場合 $(32, 32)$ 、 $R=32$ の場合 $(16, 16)$ について示す。シフトしてもパターンの境界は分からないし、そのスペクトル形状は変化がない。透かし抽出は位相のシフト量に依存しないため、抽出ソフトは変更や修正は不要である。

30

【 0 0 5 6 】

図14に画像に埋め込んだ時の図を示す。画像1は 256×256 のLENNAの画像に 32×32 のブロック毎に $\text{gain} = 0.1875$ で埋め込んだもので、4値のグリーンノイズパターンに対して乱数の位相シフトパターンを用いて埋め込んだもので有る。全部で64個のブロックがあり、16文字(ASCII)が埋め込まれている。同図(b)は埋め込み画像で、(c)はスペクトル画像で埋め込んだ16文字が正しく抽出出来ている。画像2は輝度値が192の一樣画像に埋め込んだもので、埋め込みパターンが識別できるように $\text{gain} = 0.5$ の大きな値で意図的に埋め込み、パターンを強調している。これらの図から分かるように、パターンの境界が目立たない。これはグリーンノイズパターンがランダムパターンで境界が無いからである。このため、 x_0, y_0 の値をどのように変えても、その境界が目立たない。

40

【 0 0 5 7 】

位相変化量は x, y 両方向に1画素刻みで R 個可能なため全部で R^2 個が可能である。ブロックサイズが 32×32 の場合、1024個のパターンが可能である。 64×64 の場合は4096個のパターンが可能である。しかし、細かなシフト量は攻撃に弱いため、状態数を減らして大きなシフト量で構成することが好ましい。

【 0 0 5 8 】

この $P'_i(x,y)$ の位相シフト量 (x_0, y_0) はブロック毎に変え、位相シフトリスト $L(n)$ (n はブロック番号)として記憶され鍵に格納される。埋め込まれた透かしの除去は、埋め込み

50

パターン $P'i(x,y)$ 、埋め込み強度 $gain$ 、および位相シフトリスト $L(n)$ から、

$$l(x,y)=W(x,y)-gain \cdot P'i(x,y) \quad \text{-----}(8)$$

として、除去が可能である。完全に原画に戻すためには整数型の演算で丸め誤差を考慮した演算が必要である。埋め込みパターン $P'i(x,y)$ は、式(6)に示すように基本パターン $Pi(x,y)$ と位相シフト量から求まるため、鍵には基本パターン $Pi(x,y)$ 、埋め込み強度 $gain$ 、および位相シフトリスト $L(n)$ を格納する。

【0059】

次に、位相シフトの効果について説明する。第三者からの結託攻撃では、ブロック毎の画像を合成することで埋め込みパターンを推定することが考えられる。すなわち、埋め込みの情報に応じた N 個の埋め込みパターンの集合から、 $Pi(x,y)$ に対応するブロック別に埋め込み画像パターン $Ci(x,y)$ を収集する。続いて、埋め込みパターン $Ci(x,y)$ を加算し平均値を求めると、位相シフトを行わない場合は、

$$Ci(x,y)=(1/N) \sum Wi(x,y) = (1/N) \sum li(x,y)+gain \cdot (1/N) \sum Pi(x,y) \quad \text{----}(8)$$

となる。ここで、 N は $Pi(x,y)$ に対応するブロックの数、 $Wi(x,y)$ は透かしの埋め込まれた画像データの加算、 $li(x,y)$ はブロック分割された画像データの加算を示す。ここで N を無限にすると、

$$(1/N) \sum li(x,y) \rightarrow \text{const (画像のDC成分)} \quad \text{-----}(9)$$

$$(1/N) \sum Pi(x,y) \rightarrow Pi(x,y) \quad \text{-----}(10)$$

となり、したがって、 $Ci(x,y)$ は、

$$Ci(x,y)=gain \cdot Pi(x,y) + \text{const} \quad \text{-----}(11)$$

となり、 $Pi(x,y)$ が抽出されてしまう。

一方、位相シフトを行った埋め込み画像においては、 $P'i(x,y)$ は位相がランダムに変わるため、

$$(1/N) \sum P'i(x,y) \rightarrow \text{const} \quad \text{-----}(12)$$

となり、埋め込みパターン $Pi(x,y)$ は抽出できない。

【0060】

式(12)が成立するためには N が大きくなければならない。今、画像サイズが $W \times H$ であるとして $R \times R$ のブロック数は $[W/R] \times [H/R]$ となる。ここで $[\cdot]$ は少数以下の切り捨てを表す。これを埋め込みパターン $Pi(x,y)$ で埋め込むものとする、一つの埋め込みパターン $Pi(x,y)$ の個数は、最大 $[W/R] \times [H/R]$ となる。例えば 256×256 画素の画像を 32×32 サイズのブロックで埋め込むとすると $Pi(x,y)$ は、最大の出現回数は 64 となる。 $Pi(x,y)$ は4値の場合、4つのパターンがあるので、平均出現回数は 16 となる。したがって、位相シフトのパターン $P'i(x,y)$ が1つのパターンにつき 64 個以上あれば、画像の中に同じパターンが出現する確率は極めて低い。

【0061】

様々な画像サイズに対応するため、一つの埋め込みパターンに対して、 256 個の位相シフトパターンを用意する。すなわち、 $x0,y0$ をそれぞれ $W/16, 2W/16, 3W/16, \dots, 15W/16$ の位相シフト量を与えた 256 パターンを生成し、 0 から 255 までの番号をつけ、位相シフトリストに埋め込み順のリストを作る。 512×512 サイズの画像では 32×32 のブロック分割では 256 ブロックあり、位相シフトリストの容量は 256 バイトでよい。さらに大きな画像に対してはこの位相シフトリストのデータを繰り返して用いる。

【0062】

鍵のサイズは、 32×32 のブロックサイズでは、パターン 0 および 1 の容量がそれぞれ 1024 ビット(128 バイト)、位相シフトリストが 256 バイト、それに $gain$ が数バイトの合計 520 バイト程度である。埋め込み文字情報は抽出時に得ることが出来るので鍵に含ませる必要はない。位相シフトリスト L は、パターン数を減らすとさらに小さくできる。さらには、固定された乱数列を用いる場合は位相リストは不要とすることもできる。この場合は固定乱数の先頭位置のみの指定でよい。そのため数バイトでよい。

【0063】

10

20

30

40

50

埋め込み情報量 V は、画像サイズを $W \times H$ とすると、4 値であるので、 $V = 2 \times [W/R] \times [H/R]$ ビット であたえられる。例えば、 540×530 の画像で $R=64$ のブロックで埋め込むとすると、 $V = 128$ ビットとなり、ASCII 文字コードで 16 文字が埋め込み可能である。 32×32 のブロックで埋め込むとすると、64 文字が埋め込み可能である。著作権保護の用途で使用する場合、少なくとも 16 文字以上が必要となるため、 64×64 のブロックサイズで埋め込む場合は 512×512 の画像サイズ以上、 32×32 のブロックの場合は 256×256 の画像サイズ以上が必要となる。

【0064】

以上のように、本手法は、埋め込みパターンに位相シフトを与えることにより、第三者からの結託攻撃に強靱な電子透かしが得られたものである。この手法は、特許文献 5 に紹介された反転パターンと組み合わせて用いることによりさらに強靱なものとなる。

10

また、元々グリーンノイズ拡散法は、各種編集や加工に対する耐性が高いため、本手法による結託攻撃に対する耐性も加わり、あらゆる攻撃に対して強靱であるといえる。

【産業上の利用可能性】

【0065】

以上、本発明の電子透かし法について説明したが、本手法は視認されにくいグリーンノイズ特性を示すドットパターンを埋め込むため、視覚的な画質劣化が少なく、画像の編集や加工などの攻撃に対して強い耐性がある。その理由は、本手法はスペクトル拡散型透かし手法であるからである。通常のスเปクトル拡散ではホワイトノイズを重畳するが、本発明ではグリーンノイズを重畳するため、画像のスペクトルとの分離が容易であるからである。

20

【0066】

そのうえで、位相シフトパターンを用いることにより、埋め込みドットが空間的に拡散され、パターンの解読が極めて困難で、結託攻撃に対しても強い耐性を示す。このため、あらゆる攻撃に対して耐性が強く安全性が高い。このような特徴から、著作権保護の利用形態では、強靱な透かし埋め込みが可能で、様々な環境において、違法使用やコピー、改ざんなどの検出が可能である。

【0067】

透かしの埋め込みは、ブロック単位で実空間にて埋め込むため、大きなサイズの画像など画像サイズに制限がなく、ディザ法並みに高速に処理可能である。このため動画のリアルタイム埋め込みも可能で、ドライブレコーダや監視カメラなどの利用が可能である。

30

【0068】

また本手法は完全可逆型であるので改ざん検知としても利用が可能である。すなわち、画像データのハッシュ値を、署名情報として透かしに埋め込む。改ざん検知を行う場合は、鍵により透かしを除去し完全に原画に戻した後、画像のハッシュ値を求め、両者が一致した時改ざんがなかったことを証明する。

この改ざん検知手法は、電子透かし技術が完全に可逆な手法に限る。埋め込んだ結果、画像データが変わると Hash 値が変化するためである。結託攻撃による鍵の解読は、このようなシステムを根底から覆すもので有り、それを防ぐためにも本手法が有効である。

【符号の説明】

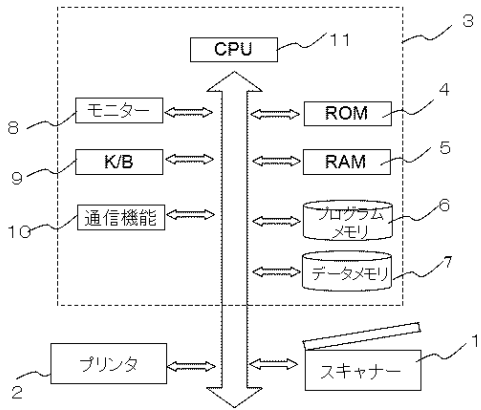
【0069】

1 はスキャナー、2 はプリンタ、3 はコンピュータシステム、4 は ROM、5 は RAM、6 はプログラムメモリ、7 はデータメモリ、8 はモニター、9 はキーボード、10 は通信機能、11 は CPU、12 はインターネット、13 は画像データの配信、14 は購入希望の連絡、15 は秘密鍵の送付、16 は著作権者のコンピュータ、17 は購入者のコンピュータを表す。

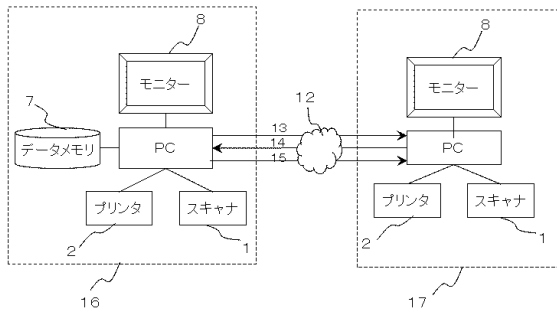
40

【図面】

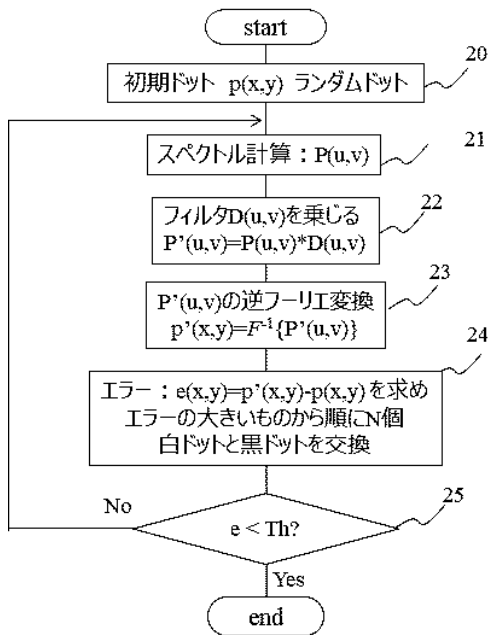
【図 1】



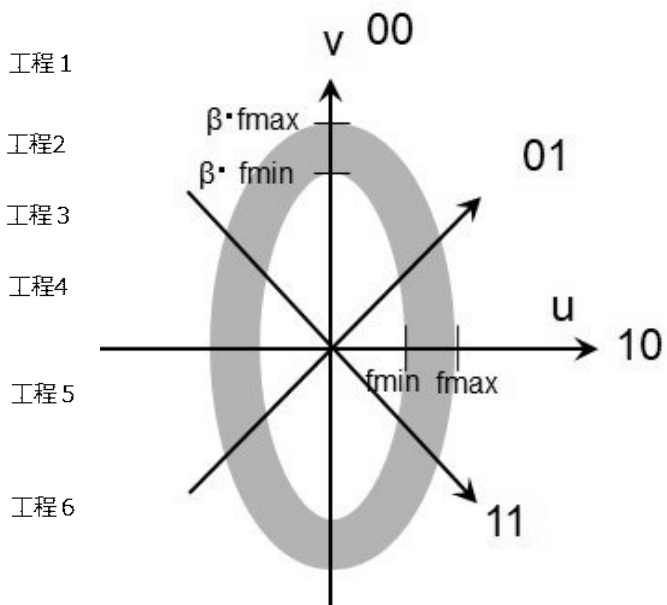
【図 2】



【図 3】



【図 4】



10

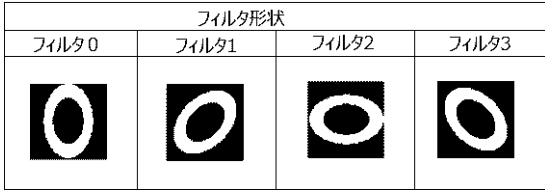
20

30

40

50

【 図 5 】

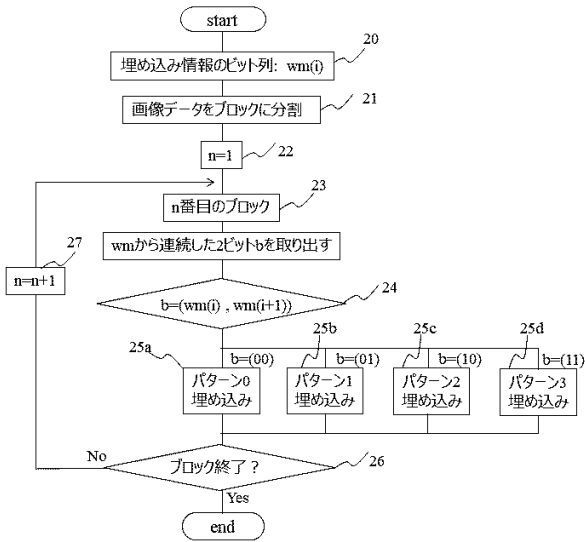


【 図 6 】

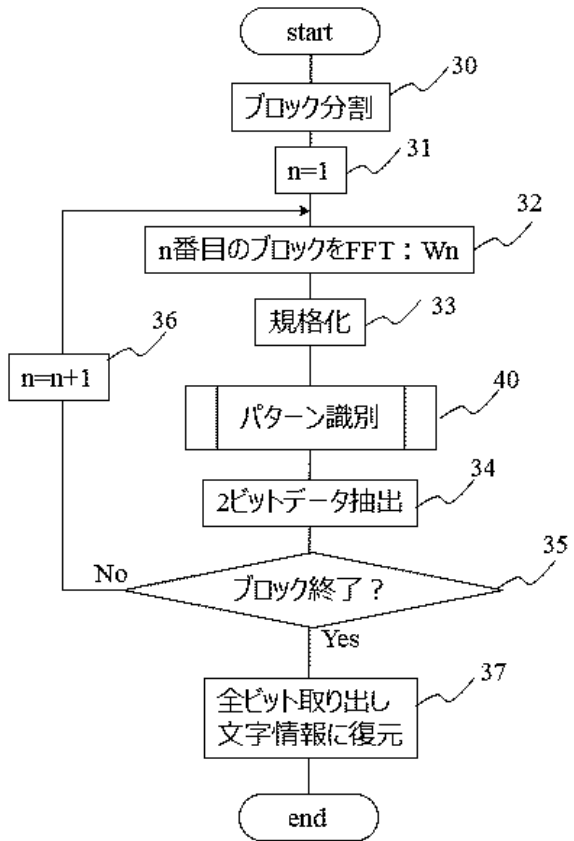
パターン	パターン0	パターン1	パターン2	パターン3
埋め込み情報	(0 0)	(0 1)	(1 0)	(1 1)
ドットパターン				
スペクトル				

10

【 図 7 】



【 図 8 】



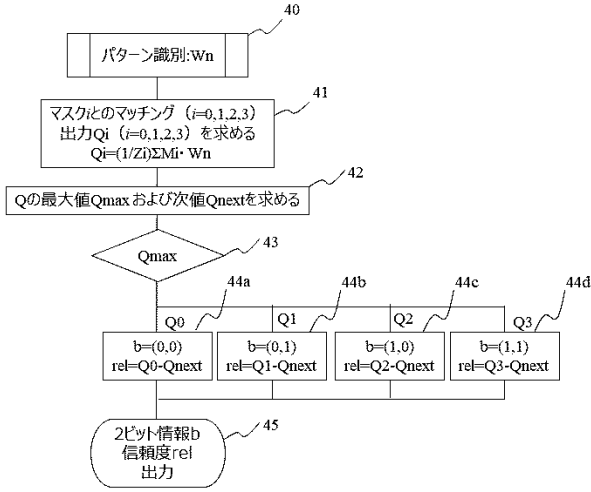
20

30

40

50

【 図 9 】



【 図 10 】

識別器	マスクパターン			
	マスク0:M0	マスク1:M1	マスク2:M2	マスク3:M3

10

【 図 11 】

(x_0, y_0)	(0,0)	(8,8)	(16,16)	(24,24)
パターン				
(x_0, y_0)	(0,24)	(8,16)	(16,8)	(24,0)
パターン				

【 図 12 】

	$s_0: (22,25)$	$s_1: (23,17)$	$s_2: (6,17)$	$s_3: (28,13)$
パターン				
	$s_4: (30,8)$	$s_5: (9,14)$	$s_6: (19,14)$	$s_7: (30,0)$
パターン				

20

【 図 13 】

	$(x_0, y_0)=(0,0)$	$(x_0, y_0)=(32,32)$		$(x_0, y_0)=(0,0)$	$(x_0, y_0)=(16,16)$
パターン					
スペクトル					

(a) R=64 (b) R=32

【 図 14 】

	(a)原画	(b)埋め込み画像	(c)スペクトル画像
画像1			
画像2			

30

40

50

フロントページの続き

- (56)参考文献 特開 2018 - 201134 (JP, A)
特開 2013 - 168789 (JP, A)
特開平 11 - 164134 (JP, A)
- (58)調査した分野 (Int.Cl., DB名)
- H04N 1/32 - 1/36
1/42 - 1/44
G06T 1/00 - 1/40
3/00 - 5/50