

(19) 日本国特許庁(JP)

(12) 特 許 公 報(B2)

(11) 特許番号

特許第4006141号

(P4006141)

(45) 発行日 平成19年11月14日(2007.11.14)

(24) 登録日 平成19年8月31日(2007.8.31)

(51) Int. Cl.		F I	
HO4N 1/387 (2006.01)		HO4N 1/387	
GO6T 1/00 (2006.01)		GO6T 1/00	500B
GO9C 5/00 (2006.01)		GO9C 5/00	
HO4N 7/26 (2006.01)		HO4N 7/13	Z

請求項の数 5 (全 33 頁)

(21) 出願番号	特願平11-224120	(73) 特許権者	000001007
(22) 出願日	平成11年8月6日(1999.8.6)		キヤノン株式会社
(65) 公開番号	特開2000-101828 (P2000-101828A)		東京都大田区下丸子3丁目30番2号
(43) 公開日	平成12年4月7日(2000.4.7)	(74) 代理人	100076428
審査請求日	平成17年6月9日(2005.6.9)		弁理士 大塚 康德
(31) 優先権主張番号	98-10148	(74) 代理人	100112508
(32) 優先日	平成10年8月6日(1998.8.6)		弁理士 高柳 司郎
(33) 優先権主張国	フランス (FR)	(74) 代理人	100115071
(31) 優先権主張番号	98-10149		弁理士 大塚 康弘
(32) 優先日	平成10年8月6日(1998.8.6)	(74) 代理人	100116894
(33) 優先権主張国	フランス (FR)		弁理士 木村 秀二
		(74) 代理人	100093908
			弁理士 松本 研一
		(74) 代理人	100101306
			弁理士 丸山 幸雄

最終頁に続く

(54) 【発明の名称】 デジタルデータの透かしの挿入及び復号する方法及び装置

(57) 【特許請求の範囲】

【請求項1】

補助情報項目を画像データに秘密透かしとして挿入する方法であって、

最低周波数の成分の数が 8×8 乃至 32×32 の間となるまで、前記画像データのサイズに依存した回数分、離散的ウェーブレット変換による多重分解能スペクトル分解する工程と、

最低周波数の成分の部分集合を選択する工程と、

前記選択した最低周波数の成分の部分集合をスキャンする過程で、擬似乱数を発生し、発生した擬似乱数が予め設定された閾値以下の値であるとき、該当する成分を補助情報項目を挿入する成分として決定し、変調する工程と、

変調後の最低周波数の部分集合と、前記多重分解能スペクトル分解の工程で得られた他の周波数成分の部分集合を再組成することで、画像データを生成する工程と

を備えることを特徴とする挿入方法。

【請求項2】

変調する工程で、挿入すべき補助情報を表現するデジタル信号により初期設定される前記擬似乱数により生成される変調値を加算することにより、前記部分集合の成分を変調することを特徴とする請求項1に記載の挿入方法。

【請求項3】

補助情報項目を画像データに秘密透かしとして挿入する装置であって、

最低周波数の成分の数が 8×8 乃至 32×32 の間となるまで、前記画像データのサイ

ズに依存した回数分、離散的ウェーブレット変換による多重分解能スペクトル分解するスペクトル分解手段と、

最低周波数の成分の部分集合を選択する選択手段と、

前記選択した最低周波数の成分の部分集合をスキャンする過程で、擬似乱数を発生し、発生した擬似乱数が予め設定された閾値以下の値であるとき、該当する成分を補助情報項目を挿入する成分として決定し、変調する変調手段と、

変調後の最低周波数の部分集合と、前記多重分解能スペクトル分解の工程で得られた他の周波数成分の部分集合を再組成することで、画像データを生成する手段とを備えることを特徴とする挿入装置。

【請求項 4】

請求項 1 又は 2 に記載の挿入方法に従って補助情報項目が秘密透かしとして挿入された画像データを復号する方法であって、

透かし挿入前の画像データを画像データ I、透かし挿入後の画像データを画像データ I*としたとき、それぞれの画像データ I、I*の最低周波数の成分の数が 8×8 乃至 32×32 の間となるまで、それぞれの画像データ I、I*のサイズに依存した回数分、離散的ウェーブレット変換による多重分解能スペクトル分解する工程と、

画像データ I、I*それぞれの最低周波数の成分の部分集合を選択する工程と、

前記画像データ I の最低周波数の成分から、前記画像データ I*の最低周波数の成分を減算することで、変調値の推定シーケンス W*を得る工程と、

請求項 1 又は 2 に記載の擬似乱数と同一の擬似乱数に基づき、変調値のシーケンス W を生成する工程と、

前記推定シーケンス W*と前記シーケンス W との相関値を計算する工程と、

前記推定シーケンス W*と前記シーケンス W とが類似しているか否かを前記相関値に従って決定する工程と

を備えることを特徴とする復号方法。

【請求項 5】

請求項 3 に記載の挿入装置に従って補助情報項目が秘密透かしとして挿入された画像データを復号する装置であって、

透かし挿入前の画像データを画像データ I、透かし挿入後の画像データを画像データ I*としたとき、それぞれの画像データ I、I*の最低周波数の成分の数が 8×8 乃至 32×32 の間となるまで、それぞれの画像データ I、I*のサイズに依存した回数分、離散的ウェーブレット変換による多重分解能スペクトル分解する手段と、

画像データ I、I*それぞれの最低周波数の成分の部分集合を選択する手段と、

前記画像データ I の最低周波数の成分から、前記画像データ I*の最低周波数の成分を減算することで、変調値の推定シーケンス W*を得る手段と、

請求項 3 に記載の擬似乱数と同一の擬似乱数に基づき、変調値のシーケンス W を生成する手段と、

前記推定シーケンス W*と前記シーケンス W との相関値を計算する手段と、

前記推定シーケンス W*と前記シーケンス W とが類似しているか否かを前記相関値に従って決定する手段と

を備えることを特徴とする復号装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、秘密透かしなどの補助情報項目をデジタルデータに挿入する方法及び装置に関する。

【0002】

また、本発明は、本発明による挿入方法により挿入されたそのような補助情報項目を復号する方法及び装置に関する。

【0003】

10

20

30

40

50

一般的にいえば、本発明は、デジタルデータに透かしを追加する技術の分野に含まれる。

【0004】

【従来の技術】

コンピュータによりデジタル化マルチメディアを交換する機会が急増した結果、不正なコピーの作成や配布、一般的な言葉で言えば、データの不法操作が助長されている。

【0005】

デジタルデータの透かし付けは、デジタル化データに透かしを直接挿入することから成る。この透かしの挿入は、デジタルデータにおける補助データ項目の符号化のようなものである。

【0006】

従来の透かし付けは、デジタルデータが画像である場合、目に見えるロゴを挿入することにより行われていた。それでも、この画像を不法に操作しようとするユーザにとって、この透かしを除去することは容易である。

【0007】

そこで、いわゆる目に見えない透かしが頻繁に利用されているが、この種の透かしは品質に関して次のような性質を有していなければならない。

【0008】

このような透かしは気づかれないものでなければならない。すなわち、このような透かしを挿入しても、デジタルデータの知覚的品質、例えば、画像の視覚的品質又は音声データの聴覚的品質は維持されなければならない。また、透かしが気づかれなければ、その侵害をより困難にもできる。

【0009】

更に、この透かしは消えないものでなければならない。すなわち、透かしを意図的に破壊しようとする攻撃に対抗するために、透かし挿入デジタルデータの中で透かしを統計的に検出できてはならない。

【0010】

また、この透かしは、圧縮及び伸張、デジタル／アナログ変換、フィルタリングなどの、従来、デジタルデータに適用されていた処理に対して、強固でなければならない。

【0011】

最後に、この透かしは高い信頼性を有していなければならない。すなわち、与えられたデジタルデータの所定の透かしが存在しているか否かについて確実に決定できるものでなければならない。

【0012】

【発明が解決しようとする課題】

既存の挿入方法、特に、デジタルデータが画像を表現している場合には、デジタルデータに含まれる高周波数又は中間周波数を変形することにより使用されている。高周波数のみを変形すると、挿入透かしの不可視度を確保することはできるが、そのような透かしはひずみに対してごくわずかな強固さしか示さず、特に、中間周波数又は高周波数のスペクトル成分を広く量子化する従来の圧縮には絶えられない。

【0013】

NEC Corporationの名で欧州特許出願第0766468号に記載されている透かしを挿入する方法が知られており、この方法においては、知覚的に重大な成分に補助情報を挿入する前に、デジタルデータの周波数変換を実行する。逆周波数変換により、透かし挿入デジタルデータが得られる。全てのデジタルデータ、例えば、画像に、離散的コサイン変換、又は離散的ウェーブレット変換による部分帯域への分解を適用することができる。その後、補助情報を挿入するために、変換のN個の最大周波数成分を変調する。しかし、知覚的に重大な成分の選択を実現するのは困難である。

本発明の目的は、主に、既存の挿入方法を改善し且つ特に不可視度及び強固さに関して、挿入される透かしの品質を向上させることである。

【0014】

10

20

30

40

50

【課題を解決するための手段】

本発明の第1の態様によれば、秘密透かしなどの補助情報項目（S）をデジタルデータ（I）に挿入する方法は、
デジタルデータを多重分解能スペクトル分解する工程（E1）と、
最低周波数の成分を抽出する工程（E2）と、
最低周波数の成分の部分集合を選択する工程（E3）と、
補助情報項目（S）を挿入するために、前記部分集合の成分を変調する工程（E4）と、
透かし挿入デジタルデータ（I'）を逆多重分解能スペクトル再組成する工程（E5）とを含む。

【0015】

10

これに関連する、秘密透かしなどの補助情報項目（S）をデジタルデータ（I）に挿入する装置は、
デジタルデータ（I）を多重分解能スペクトル分解するスペクトル分解手段（11）と、
最低周波数の成分を抽出する抽出手段（12）と、
最低周波数の成分の部分集合を選択する選択手段（13）と、
補助情報項目（S）を挿入するために、前記部分集合の成分を変調する変調手段（14）と、
透かし挿入デジタルデータ（I'）を逆多重分解能スペクトル再組成する手段（15）とを含む。

【0016】

20

本発明の第1の態様によれば、多重分解能スペクトル分解及び最低周波数の成分の抽出により、事前の選択が成される。その結果、スペクトルドメイン全体ではなく、スペクトルの1つの領域で、自動的に変調可能性分の場所を確定することができる。これは、例えば、デジタル化画像における著作権を検証する場合などに、挿入されている透かしを検証するのに非常に適している。

【0017】

更に、いくつかの成分が補助情報を導入するために変調されているような、最低周波数のスペクトル部分帯域を事前を選択しておく、様々なデジタルデータ圧縮アルゴリズムに対して、特に、デジタル画像に従来より使用されてきた圧縮及び伸張の処理に対して強固である周波数成分を系統的に選択することが可能になる。

30

【0018】

出願人は、低周波数成分を利用した場合、再構成画像に目に見える重大なひずみを生じさせずにごく小さな変調しか可能にしないことが現時点では容認されているが、多重分解能スペクトル分解の間に十分に低い分解能レベルが達成されるならば、それらの成分に大きなパワー信号を挿入することにより、気づかれないような方式で補助情報項目を追加することが可能であることを示した。

【0019】

本発明の好ましい態様によれば、多重分解能スペクトル分解レベル（d）は、最低周波数の成分の数（n）が8 x 8から32 x 32の間であるようにあらかじめ定められる。

【0020】

40

出願人は、この大きさの部分帯域が、補助情報項目の不可視度を保証しつつこの補助情報項目を挿入するのに特に適していること実験により示した。

【0021】

更に、厳密に言えば、補助情報を表現する信号を挿入し且つこの信号を検出する方法は、初期デジタルデータの大きさに対して、変調できるスペースが大幅に縮小されるという点で、特に有効である。

【0022】

デジタル画像への透かしの挿入に特に適する本発明の有利な態様によれば、スペクトル分解する工程（E1）で、離散的ウェーブレット変換によりスペクトル分解を実行し、抽出する工程（E2）では、近似部分帯域（LL）の成分を選択する。

50

【0023】

本発明の、上記の態様に代わる別の有利な態様によれば、スペクトル分解する工程（E1）で、デジタルデータ（I）を、デジタルデータ又は先行する近似バージョンの低域フィルタリング及びサブサンプリングに相当する近似バージョンと、デジタルデータから又は先行する近似バージョンからの近似バージョンの減算に相当する詳細バージョンとに繰り返し分解し、抽出する工程（E2）では、近似バージョンの成分を選択する。

【0024】

このピラミッド方式による分解は、画像を連続する近似部分帯域に分解する場合にも特に適しており、補助情報を表現する信号を挿入した後も、画像を完璧に再構成することができる。

10

【0025】

本発明の好ましい態様によれば、変調する工程（E4）で、挿入すべき補助情報を表現するデジタル信号（S）により初期設定される擬似ランダム関数により生成される変調値（ W_k ）を加算することにより、前記部分集合の成分を変調する。

【0026】

擬似ランダム関数により生成される変調値によって補助情報を追加すれば、この情報をマスキングできると共に、この情報の侵害をより困難にするために、情報の不可視度を更に強化することができる。

【0027】

本発明の有利な態様によれば、選択する工程（E3）で、挿入すべき補助情報（S）と関連する機密鍵を表現するデジタル信号（K）により初期設定される擬似ランダム関数に従って、成分の部分集合を選択する。

20

【0028】

この機密鍵は、擬似ランダム方式で変調可能な成分を選択することを可能にし、それにより意図的な攻撃に対する挿入情報の強固さをより向上させ、周波数スペクトルにおける挿入情報の位置を更に識別しにくくする。秘密鍵を使用すると、デジタルデータに挿入された信号の保護を強化することができる。

【0029】

本発明は、第1の態様による挿入方法に従って初期デジタルデータ（I）に挿入された、秘密透かしなどの補助情報項目（S）を透かし挿入デジタルデータ（ I^* ）の中で復号する方法であって

30

透かし挿入デジタルデータ（ I^* ）及び初期デジタルデータ（I）を多重分解能スペクトル分解する工程（E6）と、

透かし挿入デジタルデータ（ I^* ）及び初期デジタルデータ（I）における最低周波数の成分を抽出する工程（E7）と、

透かし挿入デジタルデータ（ I^* ）及び初期デジタルデータ（I）から前記挿入方法の選択する工程（E3）で選択された成分の部分集合を選択する工程（E8）と、

初期デジタルデータ（I）の前記部分集合の成分から透かし挿入デジタルデータ（ I^* ）の前記部分集合の成分をそれぞれ減算することにより、変調値（ W^* ）の推定シーケンスを推定する工程（E9）と、

40

前記挿入方法の変調する工程（E4）で挿入された変調値の前提シーケンス（W）を生成する工程（E10）と、

推定シーケンス（ W^* ）と前提シーケンス（W）と相関値を計算する工程（E11）と、

推定シーケンス（ W^* ）と前提シーケンス（W）とが類似しているか否かを前記相関値の関数として決定する工程（E12）とを含む復号方法にも関する。

【0030】

従って、この復号方法により、デジタルデータに補助情報を挿入するために変調されていた最低周波数の成分を容易に見出すことができるようになると共に、挿入情報を前提変調と比較するために挿入情報を推定することが可能になる。そのような復号方法は、送信中又は格納中に雑音を含んでいる可能性のあるデジタルデータにおける著作権の認知に特に

50

適している。

【0031】

これに関連して、本発明の第1の態様による挿入方法に従って初期デジタルデータ (I) に挿入された、秘密透かしなどの補助情報項目 (S) を透かし挿入デジタルデータ (I^*) の中で復号する装置は、

透かし挿入デジタルデータ (I^*) 及び初期デジタルデータ (I) を多重分解能スペクトル分解するスペクトル分解手段 (61) と、

透かし挿入デジタルデータ (I^*) 及び初期デジタルデータ (I) における最低周波数の成分を抽出する抽出手段 (62) と、

透かし挿入デジタルデータ (I^*) 及び初期デジタルデータ (I) から前記挿入方法の選択する工程 (E3) で選択された成分の部分集合を選択する選択手段 (63) と、

初期デジタルデータ (I) の前記部分集合の成分から透かし挿入デジタルデータ (I^*) の前記部分集合の成分をそれぞれ減算することにより、変調値の推定シーケンス (W^*) を推定する推定手段 (64) と、

前記挿入方法の変調する工程 (E4) で挿入された変調値の前提シーケンス (W) を生成する生成手段 (65) と、

推定シーケンス (W^*) と前提シーケンス (W) との相関値を計算する計算手段 (67) と、

推定シーケンス (W^*) と前提シーケンス (W) とが類似しているか否かを前記相関値の関数として決定する決定手段 (68) とを具備する。

【0032】

この復号装置は本発明の第1の態様による復号方法の利点に類似する利点を有し、例えば、デジタル画像などのデジタルデータの著作権の認知に特に適している。

【0033】

本発明の挿入方法の実用的で、好都合な実施形態を提供する本発明の第1の態様の好ましい態様によれば、挿入装置のスペクトル分解手段 (11)、抽出手段 (12)、選択手段 (13)、変調手段 (14) 及びスペクトル再組成手段 (15) は、

マイクロプロセッサ (10) と、

補助情報項目 (S) を挿入するためのプログラムを格納する読み取り専用メモリ (102) と、

プログラムの実行中に修正される変数を記録するための複数のレジスタを含むランダムアクセスメモリ (103) とに組み込まれている。

【0034】

同様に、本発明の第1の態様による復号方法の実用的で、好都合な実施形態を提供する好ましい態様によれば、復号装置のスペクトル分解手段 (61)、抽出手段 (62)、選択手段 (63)、推定手段 (64)、生成手段 (65)、計算手段 (67) 及び決定手段 (68) は、

マイクロプロセッサ (10) と、

補助情報項目 (S) を復号するためのプログラムを格納する読み取り専用メモリ (102) と、

プログラムの実行中に修正される変数を記録するための複数のレジスタ (103) を含むランダムアクセスメモリとに組み込まれている。

【0035】

本発明の第2の態様によれば、秘密透かしなどの補助情報項目 (S) をデジタルデータ (I) に挿入する方法は、

デジタルデータ (I) を多重分解能スペクトル分解する工程 (E101) と、

1つの周波数部分帯域 (LL) の成分を抽出する工程 (E102) と、

前記周波数部分帯域 (LL) の成分をスペクトル変換する工程 (E103) と、

前記スペクトル変換の係数 (X_k) の部分集合を選択する工程 (E104) と、

補助情報 (S) を挿入するために、前記部分集合の係数 (X_k) を変調する工程 (E10

5) と、
変調された係数の部分集合を含む係数 (X'_k) を逆スペクトル変換する工程 (E106)
と、
透かし挿入デジタルデータ (I') を逆多重分解能スペクトル再組成する工程 (E107)
) とから成る。

【0036】

これに関連する、秘密透かしなどの補助情報項目 (S) をデジタルデータ (I) に挿入する装置は、

デジタルデータ (I) を多重分解能スペクトル分解するスペクトル分解手段 (31) と、
1つの周波数部分帯域 (LL) の成分を抽出する抽出手段 (32) と、

10

前記周波数部分帯域 (LL) の成分をスペクトル変換するスペクトル変換手段 (33) と、

前記スペクトル変換の係数 (X_k) の部分集合を選択する選択手段 (34) と、

補助情報 (S) を挿入するために、前記部分集合の係数 (X_k) を変調する変調手段 (35) と、

変調された係数 (X'_k) の部分集合を含む係数を逆スペクトル変換する逆スペクトル変換手段 (36) と、

透かし挿入デジタルデータ (I') を逆多重分解能スペクトル再組成するスペクトル再組成手段 (37) とを具備する。

【0037】

20

このようなデジタルデータの二重変換によって、変調すべき係数のシークは限られた範囲の周波数について実行される。これは、多重分解能スペクトル分解を経て事前の選択が行われるために、スペクトル範囲全体ではなく、スペクトルの1つの領域で自動的に変調可能な成分の場所を確定できるからである。これは、例えば、デジタル化画像の著作権を検証する場合のように、挿入透かしを検証するのに特に適している。

【0038】

更に、1つの変調可能周波数帯域を事前を選択しておく、様々なデジタルデータ圧縮アルゴリズムに対して強固である周波数成分を系統的に選択することができるようになる。

【0039】

最後に、選択された部分帯域の成分にスペクトル変換を適用しても、後にデジタルデータの空間ドメイン全体に挿入される補助情報は確実に分散される。加えて、このスペクトル変換は、より小さな、初期デジタルデータの1つの部分帯域について実行される。従って、このスペクトル変換は、全ての初期デジタルデータについてスペクトル変換を実行する周知の方法と比べて、はるかに迅速である。

30

【0040】

本発明の好ましい態様によれば、抽出する工程で、最低周波数の部分帯域の成分を選択する。

【0041】

この選択は、後に従来の圧縮方法及び伸張方法に対して強固であるスペクトル範囲の補助情報を挿入するためにデジタル化された画像の場合に特に賢明である。

40

【0042】

デジタル画像への透かしの挿入に特に適している有利な態様によれば、スペクトル分解する工程 (31) で、離散的ウェーブレット変換によりスペクトル分解を実行し、抽出する工程 (32) では、近似部分帯域の成分を選択する。

【0043】

出願人は、最低周波数に対応する近似部分帯域が再構成画像に目に見える重大なひずみを生じさせずにごくわずかな修正しか与えないことは現時点では容認されているが、多重分解能スペクトル分解の間に十分に低い分解能レベルに到達すれば、近似部分帯域の成分に気づかれないように補助情報項目を追加することは可能であることを示した。

【0044】

50

ウェーブレット変換分解レベルは、近似部分帯域（ LL ）の成分の数（ n ）が 8×8 から 32×32 の間にあるようにあらかじめ定められるのが好ましい。

【0045】

出願人は、この大きさの部分帯域が補助情報項目の不可視度を保証しつつ、その補助情報項目を挿入するのに特に適していることを実験により示した。

【0046】

本発明の好ましい態様によれば、スペクトル変換（33）は離散的コサイン変換である。

【0047】

このようなスペクトル変換の使用は、画像に透かしを挿入するのに特に適しており、挿入透かしが空間ドメイン全体に適切に分布することを保証する。

本発明の好ましい態様によれば、変調する工程で、挿入すべき補助情報を表現するデジタル信号により初期設定される擬似ランダム関数により生成される変調値を加算することにより、部分集合の成分を変調する。

【0048】

擬似ランダム関数により生成される変調値による補助情報を追加することによって、この情報をマスキングできると共に、この情報の侵害をより困難にするために、情報の不可視度を更に強化することができる。

【0049】

本発明の有利な態様によれば、選択する工程で、挿入すべき補助情報と関連する機密鍵を表現するデジタル信号により初期設定される擬似ランダム関数に従って、係数の部分集合を選択する。

【0050】

この機密鍵により、擬似ランダム方式で変調可能係数を選択することができ、従って、周波数スペクトルにおける挿入情報の場所を見出すことをより困難にすることによって、挿入情報を意図的な攻撃に対し、より強固なものにすることができる。

【0051】

本発明の挿入方法の実用的で、好都合な実施形態を提供する本発明のこの第2の態様の好ましい態様によれば、挿入装置のスペクトル分解手段（31）、抽出手段（32）、スペクトル変換手段（32）、選択手段（34）、変調手段（35）、逆スペクトル変換手段（36）及びスペクトル再組成手段（37）は、

マイクロプロセッサ（10）と、
補助情報項目（S）を挿入するためのプログラムを格納する読み取り専用メモリ（102）と、

プログラムの実行中に修正される変数を記録するための複数のレジスタを含むランダムアクセスメモリ（103）とに組み込まれている。

【0052】

この挿入方法と関連して、第2の態様によれば、本発明は、前記挿入方法による挿入方法に従って初期デジタルデータ（I）に挿入された、秘密透かしなどの補助情報項目（S）を透かし挿入デジタルデータ（ I^* ）の中で復号する方法であって、

透かし挿入デジタルデータ（ I^* ）及び初期デジタルデータ（I）を多重分解能スペクトル分解する工程（E110）と、

透かし挿入デジタルデータ（ I^* ）及び初期デジタルデータ（I）それぞれにおける周波数の部分帯域（ LL ）の成分を抽出する工程（E111）と、

透かし挿入デジタルデータ（ I^* ）及び初期デジタルデータ（I）の周波数部分帯域（ LL ）の成分をスペクトル変換する工程（E112）と、

透かし挿入デジタルデータ（ I^* ）及び初期デジタルデータ（I）から前記挿入方法の選択する工程（E104）で選択された係数の部分集合を選択する工程（E113）と、

初期デジタルデータ（I）の前記部分集合の係数から透かし挿入デジタルデータ（ I^* ）の前記部分集合の係数をそれぞれ減算することにより、変調値の推定シーケンス（ W^* ）を推定する工程（E114）と、

10

20

30

40

50

前記挿入方法の変調する工程 (E 1 0 5) で挿入された変調値の前提シーケンス (W) を生成する工程 (E 1 1 5) と、
推定シーケンス (W^*) と前提シーケンス (W) との相関値を計算する工程 (E 1 1 6) と、
推定シーケンス (W^*) と前提シーケンス (W) とが類似しているか否かを前記相関値の関数として決定する工程 (E 1 1 7) とを含む復号方法にも関する。

【0053】

これに関連して、本発明の第2の態様による挿入方法に従って初期デジタルデータ (I) に挿入された、秘密透かしなどの補助情報項目 (S) を透かし挿入デジタルデータ (I^*) の中で復号する装置は、
透かし挿入デジタルデータ (I^*) 及び初期デジタルデータ (I) を多重分解能スペクトル分解するスペクトル分解手段 (21) と、
透かし挿入デジタルデータ (I^*) 及び初期デジタルデータ (I) それぞれにおける周波数の部分帯域 (LL) の成分を抽出する抽出手段 (22) と、
透かし挿入デジタルデータ (I^*) 及び初期デジタルデータ (I) の周波数部分帯域 (LL) の成分をスペクトル変換するスペクトル変換手段 (23) と、
透かし挿入デジタルデータ (I^*) 及び初期デジタルデータ (I) から前記挿入方法の選択する工程 (E 1 0 4) で選択された係数の部分集合を選択する選択手段 (24) と、
初期デジタルデータ (I) の前記部分集合の係数から透かし挿入デジタルデータ (I^*) の前記部分集合の係数をそれぞれ減算することにより、変調値の推定シーケンス (W^*) を推定する推定手段 (25) と、
前記挿入方法の変調する工程 (E 1 0 5) で挿入された変調値の前提シーケンス (W) を生成する生成手段 (26) と、
推定シーケンス (W^*) と前提シーケンス (W) との相関値を計算する計算手段 (28) と、
推定シーケンス (W^*) と前提シーケンス (W) とが類似しているか否かを前記相関値の関数として決定する決定手段 (29) とを具備する。

【0054】

このようなデジタルデータの二重変換によって、変調された係数は限られた範囲の周波数について探索される。これは、多重分解能スペクトル分解を経て事前の選択が行われるために、スペクトルの1つの領域で自動的に変調可能な成分の場所を確定できるからである。

【0055】

この復号方法及び装置は、例えば、デジタル化画像の著作権を検証する場合のように、挿入透かしを検証するのに特に適している。

【0056】

本発明の復号方法の実用的で、好都合な実施形態を提供する本発明のこの第2の態様の好ましい態様によれば、復号装置のスペクトル分解手段 (21)、抽出手段 (25)、スペクトル変換手段 (23)、選択手段 (24)、推定手段 (25)、生成手段 (26)、計算手段 (28) 及び決定手段 (29) は、
マイクロプロセッサ (10) と、
補助情報項目を復号するためのプログラムを格納する読み取り専用メモリ (102) と、
プログラムの実行中に修正される変数を記録するための複数のレジスタを含むランダムアクセスメモリ (103) とに組み込まれている。

【0057】

挿入装置又は復号装置に一体化されているか、又は一体化されておらず、オプションとして着脱自在であり、コンピュータ又はマイクロプロセッサにより読み取り可能である情報格納手段は、本発明の第1及び／又は第2の態様に従って補助情報項目を挿入又は復号する方法を実現するプログラムを格納する。

【0058】

本発明は、本発明の第1及び／第2の態様による挿入又は復号方法を実現するための手段を有するか、又は本発明の第2及び／又は第2の態様による挿入又は復号装置を有するデジタル信号処理装置にも関する。

【0059】

この処理装置の利点は、本発明の第1及び／又は第2の態様による挿入方法及び装置並びに復号方法及び装置に関連して先に開示した利点と同一である。

【0060】

挿入方法及び復号方法は、特に、デジタル写真装置、デジタルカメラ、データベース管理システム、コンピュータ、スキャナ、又は医療用画像撮影装置、とりわけ、X線撮影装置において実現できる。

10

【0061】

これに関連して、デジタル写真装置、デジタルカメラ、データベース管理システム、コンピュータ、スキャナ、又は医療用画像撮影装置、とりわけ、X線撮影装置は、本発明による挿入装置及び／又は復号装置を有する。

【0062】

上記のデジタル写真装置、デジタルカメラ、データベース管理システム、コンピュータ、スキャナ、又はX線撮影装置などの医療用画像撮影装置は、本発明による挿入方法及び装置並びに復号方法及び装置の利点に類似する利点を有する。

【0063】

本発明のその他の特異性及び利点は、以下の説明から明白になるであろう。

20

【0064】

【発明の実施の形態】

まず、デジタルデータに補助情報項目を挿入する装置について説明する。

【0065】

以下の、限定的な意味をもたない例においては、デジタルデータは画像Iを表現する一連のデジタルサンプルから構成されている。画像Iは、例えば、一連のバイトにより表現されており、各バイト値は256のグレイレベルを有する白黒画像などの画像Iの1つの画素を表現する。

【0066】

補助情報は、画像I中に認知不可能な、強固な方式で挿入することが望まれる秘密透かしである。この秘密透かしは、例えば、画像Iの原作者又は所有者を識別できるようにするものであっても良い。この例においては、補助情報はあるビット数、例えば、32ビットの識別番号Sから構成され、識別番号Sは同様にあるビット数で定義される機密鍵(confidential key)Kと関連している。この識別番号Sと機密鍵Kにより、以下に説明するように、画像Iに有効に挿入される変調信号を発生させることができる。機密鍵Kは任意の方式で識別番号Sと関連させることができる。

30

【0067】

一般的に言えば、図1に示すように、挿入装置は全体としてエンコーダ1に類似しており、画像IにおいてS及びKから定義される透かしを符号化する。透かしが挿入された画像I'はエンコーダ1の出力端子に供給される。

40

【0068】

この画像I'を送信又は格納するために、画像I'は圧縮及び伸張などの、非線形雑音の追加に類似するいくつかの処理を受ける。また、画像を表示するときには、画像をデジタル／アナログ変換し、あるいは、フィルタリングを実行する場合もある。

【0069】

処理後に、透かし挿入画像I'の雑音を含むバージョンに相当する画像I^{*}を、エンコーダ1と関連するデコーダ2へ送信することができる。このデコーダ2は、従来通り、初期画像I及び挿入されている補助情報S、Kから、雑音を含む画像I^{*}の中の挿入変調信号W^{*}を推定する。雑音を含む画像I^{*}の中のこの変調信号W^{*}は、画像Iに挿入された変調信号Wと共に、検出器3に供給され、そこで、これら2つの信号W及びW^{*}の類似度を評価し

50

、それにより、例えば、挿入されている著作権情報を検査する。この相関測定については、後に、復号装置及び方法に関連して詳細に説明する。

【0070】

本発明の第1の態様によれば、図2に示すように、挿入装置1は、この例では画像Iを表現するデジタルデータを多重分解能スペクトル分解する手段11と、最低周波数の成分を抽出する抽出手段12と、最低周波数の成分の部分集合を選択する選択手段13と、補助情報を挿入するために、この部分集合の成分を変調する手段14と、透かし挿入画像I'を再構成するために、デジタル信号を逆多重分解能スペクトル再組成(reverse multi-resolution spectral recomposition)する手段15とを有する。 10

【0071】

本発明の第2の態様によれば、図3に示すように、挿入装置1はこの例では画像Iを表現するデジタルデータを多重分解能スペクトル分解する手段31と、1つの周波数部分帯域の成分を抽出する抽出手段32と、この周波数部分帯域の成分をスペクトル変換する手段33と、スペクトル変換の係数の部分集合を選択する選択手段34と、補助情報を挿入するために、この部分集合の係数を変調する手段35と、変調された係数の部分集合を含む係数を逆スペクトル変換する手段36と、透かし挿入画像I'を再構成するために、デジタルデータを逆多重分解能スペクトル再組成する手段37とを有する。 20

【0072】

多重分解能スペクトル分解手段11、31は、離散的ウェーブレット変換を実行するものであり、複数の部分帯域への分解を実行する回路、又は、それぞれがx2デシメータと関連する一組の解析フィルタにより形成される解析回路から構成されるのが好ましい。この分解回路は、画像Iの信号を2方向にフィルタリングして、高い空間周波数と、低い空間周波数の複数の部分帯域を得る。この回路は、いくつかの分解能レベルに従って画像Iを部分帯域に分解するいくつかの連続する解析ユニットを有する。

【0073】

従来より、信号の分解能は、その信号を表現するために使用される単位長さ当たりのサンプル数である。画像信号Iの場合、部分帯域の分解能は、この部分帯域を水平方向及び垂直方向に表現するために使用される単位長さ当たりのサンプル数と関連している。分解能は、実行されるデシメーションの回数、デシメーション係数及び初期画像の分解能によって決まる。 30

【0074】

この部分帯域への分解は良く知られている。次に、画像Iを3に等しい分解レベルdで部分帯域に分解する場合に使用される様々な解析工程を図5を参照して簡単に説明する。

【0075】

第1の解析ユニットは画像信号Iを受信し、それぞれ、低域フィルタと高域フィルタである2つのデジタルフィルタを介して、この信号を第1の方向、例えば、水平方向にフィルタリングする。2対1デシメータを通過した後、得られたフィルタリング済み信号は、それぞれ、低域フィルタと高域フィルタである2つのフィルタにより、第2の方向、例えば、垂直方向に再びフィルタリングされる。各信号は2対1デシメータを再度通過する。そこで、この第1の解析ユニットの出力端子では、分解の最高の分解能で4つの部分帯域 L_1 、 LH_1 、 HL_1 及び HH_1 が得られる。 40

【0076】

部分帯域 LH_1 は、画像信号Iの両方向の低周波数の成分を含む。部分帯域 LH_1 は画像信号Iの第1の方向の低周波数の成分と、第2の方向の高周波数の成分とを含む。部分帯域 HL_1 は、第1の方向の高周波数の成分と、第2の方向の低周波数の成分とを含む。最後 50

に、部分帯域 HH_1 は両方向の高周波数の成分を含む。

【0077】

第2の解析ユニットは、部分帯域 LL_1 をフィルタリングして、先行するユニットと同様に、分解の中間分解能レベルの4つの部分帯域 LL_2 、 LH_2 、 HL_2 及び HH_2 を供給する。最後に、この例では、部分帯域 LL_2 を更に第3の解析ユニットにより解析して、この分解の最低の分解能の4つの部分帯域 LL_3 、 LH_3 、 HL_3 及び HH_3 を得る。

【0078】

このようにして、10の部分帯域と3つの分解能レベルが得られる。最低周波数の部分帯域 LL_3 を近似部分帯域と呼び、その他の部分帯域を詳細部分帯域と呼ぶ。

【0079】

言うまでもなく、分解能レベルの数、従って、部分帯域の数は上記の数とは異なっているも良く、例えば、分解能レベルを4つとし、部分帯域の数を13とすることもできる。

【0080】

次に、抽出手段12、32は、画像Iの分解における最低周波数を有する部分帯域、すなわち、この例においては近似部分帯域 LL_3 の成分を選択する。

【0081】

従って、透かしSの挿入は、概して、画像の圧縮処理及び伸張処理ではほとんど量子化されない低周波数部分帯域で実行されるので、画像が受ける歪みに対する挿入透かしの強固さは強化される。

【0082】

出願人は、十分に低い分解能レベルに到達すれば、近似部分帯域に認知不可能なように情報を追加することが可能であると気づいた。

【0083】

そこで、画像Iの大きさに従って分解レベルの数dを調整することが必要である。これは、 $N \times N$ サイズの画像Iの場合、この例における非常に低い周波数の部分帯域の大きさが $N/2^d \times N/2^d$ になるためである。

【0084】

近似部分帯域 LL_d の成分の数nが 8×8 から 32×32 の間にあるように、ウェーブレットへの変換による分解のレベルの数dはあらかじめ定められるのが好ましい。

【0085】

試験によれば、 $n = 16 \times 16$ であるのが好ましいことがわかっている。これは、画像Iが $N \times N = 512 \times 512$ の大きさを有するときの5つの分解レベルに相当する。

【0086】

そこで、近似部分帯域 LL_5 の $0 \leq i \leq N/2^{d-1}$ 及び $0 \leq j \leq N/2^{d-1}$ である成分 I_{ij} を抽出する。

【0087】

変形例として、図6に示す本発明の別の実施形態によれば、デジタルデータIをデジタルデータI又は先行する近似バージョンの低域フィルタリング及びサブサンプリングに相当する近似バージョンと、デジタルデータから又は先行する近似バージョンからの近似バージョンの減算に相当する詳細バージョンとに繰り返し分解する。このような連続ピラミッド型近似の方式は、Burt及びAdelsonの「The Laplacian pyramid as a compact image code」(IEEE, Trans. on Communications, 31(4): 532-540ページ、1983年)により提案されている。この方式は、水平と垂直の各方向に2に等しい係数による低域フィルタリング及びサブサンプリングを実行することにより、考慮すべき画像Iの低分解能バージョンを抽出することからなる。このようにレベル1近似を得る。初期画像Iと同じ大きさのレベル0詳細画像は、初期画像Iからレベル1近似を減算することにより生成される。この減算を実行するために、まず、低分解能バージョンの補間により、初期画像と同一の大きさの画像を予測し、次に、この予測画像を初期画像から減算して、詳細画像を求める。画像の十分に簡略化された近似を獲得し、補助情報を近似バージョンに見えないように挿入できるようにするために、低分解能画像に対して、この方式を必要な回数

10

20

30

40

50

だけ繰り返し実行することができる。この場合には、レベル1近似バージョンに対して分解を繰り返すと、近似バージョンはレベル2近似バージョンと、レベル1詳細バージョンとに分解されることになる。次に、抽出する工程においては、最低の分解能を有するバージョン、ここでは、同様に i 及び j がそれぞれ第1及び第2の方向でレベル2近似バージョンの長さに沿ってそれぞれ変化するような成分 I_{ij} の集合により形成されるレベル2近似バージョンを選択する。

【0088】

本発明の第1の態様では、成分 I_{ij} の部分集合を選択する手段13は、挿入すべき補助情報 S と関連する機密鍵を表現するデジタル信号 K により初期設定される擬似ランダム関数で数発生器16と協働する。

10

【0089】

擬似ランダム関数に従って数を取り出すと、擬似ランダム方式で変調すべき成分を選択することにより、挿入される透かしの強固さを強化することができる。使用される機密鍵と擬似ランダム関数の知識があるだけで、変調されていた非常に低い周波数の成分を見つけ出すことができる。

【0090】

同様に、変調手段14は、挿入すべき追加情報を表現するデジタル信号 S により初期設定される擬似ランダム関数により生成される変調値の発生器16と協働し、それらの変調値を先に選択された部分集合の成分に追加する手段15を有する。

【0091】

20

スペクトル再組成手段15は、2の乗算器と関連する一連の合成フィルタを具備する従来通りの再組成回路を有し、そこで、いくつかの、この例では3に等しい数の再組成レベルの後、透かし挿入画像 I' はコーダ1の出力端子に供給される。

【0092】

本発明の第2の態様においては、スペクトル変換手段33は離散的コサイン変換、すなわち、DCTを実行する。

【0093】

従来より画像処理で使用されているこのDCT変換は、画像 I の1つの小さな部分帯域に限定されているために、ここでは有効に利用されている。このDCT変換により、後に、画像 I の空間ドメイン全体にわたる挿入透かし S の分布を得ることができる。

30

【0094】

係数の部分集合を選択する手段34は、挿入すべき補助情報 S と関連する機密鍵を表現するデジタル信号 K により初期設定される擬似ランダム関数で数発生器38と協働する。

【0095】

擬似ランダム数を取り出すと、変調すべきDCTの係数を無作為に選択することにより、挿入透かしの強固さを強化することができる。使用される機密鍵と擬似ランダム関数の知識があるだけで、変調されているDCTの係数を見出すことができる。

【0096】

同様に、変調手段35は、挿入すべき追加情報を表現するデジタル信号 S により初期設定される擬似ランダム関数により生成される変調値の発生器38と協働し、それらの変調値を先に選択された部分集合の係数に追加する手段35を有する。

40

【0097】

逆スペクトル変換手段36は、この例では、画像処理において通常使用される逆離散的コサイン変換である。

【0098】

同様に、スペクトル再組成手段37は、2の乗算器と関連する一連の合成フィルタを具備する従来通りの再組成回路を含み、そこで、いくつかの、この例では3に等しい数の再組成レベルの後に、透かし挿入画像 I' はコーダ1の出力端子に供給される。

【0099】

図4に示すように、スペクトル分解手段11と、抽出手段12と、選択手段13と、変調

50

手段14と、スペクトル再組成手段15と、擬似ランダム数発生器16は、マイクロプロセッサ又はコンピュータ10、補助情報項目Sを挿入するためのプログラムを格納する読み取り専用メモリ102（ROM）、及びプログラムの実行中に修正される変数を記録するための複数のレジスタを含むランダムアクセスメモリ103（RAM）に組み込まれているのが好ましい。

【0100】

同様に、スペクトル分解手段31と、抽出手段32と、スペクトル変換手段33と、選択手段34と、変調手段35と、逆スペクトル変換手段36と、スペクトル再組成手段37と、擬似ランダム数発生器38とは、マイクロプロセッサ又はコンピュータ10、補助情報項目Sを挿入するためのプログラムを格納する読み取り専用メモリ102（ROM）、及びプログラムの実行中に修正される変数を記録するための複数のレジスタを含むランダムアクセスメモリ103（RAM）に組み込まれているのが好ましい。

10

【0101】

言うまでもなく、補助情報項目を挿入するためのプログラムをコンピュータ10のハードディスク108に格納することも可能である。

【0102】

この挿入プログラム全体または一部を、着脱自在ではあるが、コンピュータプロパーには一体化されていない格納手段に格納することも可能である。すなわち、通信インタフェース112によってコンピュータに接続された通信ネットワーク113により読み取り専用メモリ102又はハードディスク108から受信したり、読み取り専用メモリ102又はハードディスク108にロードしたりすることができる。又、先にディスク110に格納されているプログラム命令を読み取るディスクドライブ109によってプログラムをロードすることも考えられる。言うまでもなく、ディスクの代わりに、固定メモリコンパクトディスク（CD-ROM）、磁気テープ又はメモリカードなどの情報媒体を使用することも可能である。

20

【0103】

中央装置100（CPU）により、挿入プログラムの命令を実行できる。すなわち、パワーアップ時、不揮発性メモリの1つ、例えば、読み取り専用メモリ102に格納されているプログラムをランダムアクセスメモリ（RAM）103へ転送する。ランダムアクセスメモリ103は、本発明の第1及び第2の態様に従った挿入方法を実現するために必要な変数も格納している。

30

【0104】

ランダムアクセスメモリ103は、特に、プログラムの実行中に修正される変数を格納するためのいくつかのレジスタを含むことができる。すなわち、ランダムアクセスメモリ103は、例えば、各分解レベルにおける近似部分帯域の大きさを格納するレジスタと、変調すべき成分を確定するために引き出される擬似ランダム数を格納するレジスタと、選択された成分の部分集合を格納するレジスタと、変調値を格納するレジスタと、変調成分を格納するレジスタとを有する。

【0105】

通信バス101は従来のようにコンピュータの様々な部分要素の間で通信を実行する。

40

【0106】

コンピュータ10は、例えば、透かしを挿入すべき画像Iを表示すると共に、ユーザが、例えば、キーボード114を使用して、挿入方法を実現するためのいくつかのデータをパラメータ化することができるように、ユーザとの間のインタフェースとして機能する画面104を更に有する。

【0107】

例えば、データの原作者を識別するために、秘密透かしを挿入したいデータのコンピュータ10への供給は、様々な周辺装置、特に、グラフィックスカードに接続するデジタルカメラ107、又はスキャナ、X線撮影装置、あるいはその他の画像収集手段又は画像格納手段により実行できる。

50

【0108】

通信ネットワーク113も、透かしを挿入すべきデジタル画像を供給することができる。
ディスク110も、同様に、デジタルデータを格納することができる。

【0109】

変形例として、マイクロホン111が入出力カード106によりコンピュータ10に接続している。この変形例における透かしを挿入すべきデジタルデータは、音声信号である。

【0110】

格納または処理されたデジタルデータに透かしを形成する為に、本挿入装置は各種のデジタル処理装置または直接デジタル写真装置やデジタルカメラに内蔵されてもよく、データベース管理システムと一体化されてもよい。

10

【0111】

次に、本発明の第1の態様による挿入方法を、特に図7及び図8を参照して説明する。

【0112】

本発明によれば、デジタルデータ、ここでは画像Iに秘密透かしなどの補助情報項目Sを挿入する方法は、次のような工程を含む。

【0113】

- a) デジタルデータIを多重分解能スペクトル分解する工程E1,
- b) 最低周波数の成分を抽出する工程E2.

この場合、挿入方法は、 $N = 512$ バイトである $N \times N$ の大きさの画像Iに適用される。

【0114】

スペクトル分解する工程E1は、図7の実施形態においては、不連続のウェーブレットへの変換によって実行される。離散的ウェーブレット変換による分解のレベルの数dは、近似部分帯域LLの成分の数nが 8×8 から 32×32 の間であるようにあらかじめ定められる。

20

【0115】

このようにして、閾値Tを、例えば、 32×32 に固定し、試験する工程E2.1中に、各分解能レベルで、近似部分帯域LLの成分の数nをこの閾値Tと比較する。

【0116】

試験が否定であれば、すなわち、nが閾値Tより大きい場合には、部分帯域をより高い分解レベルで分解する。

30

【0117】

この例では、画像Iが正方形であり且つ大きさが 512×512 バイトに等しいとき、2対1デシメータによる部分帯域への分解を採用する。同様に正方形である部分帯域LLの大きさは、各分解レベルdで、 $N/2^d \times N/2^d$ に等しい。

【0118】

閾値Tを 32×32 に固定することにより、4に等しい分解レベルdに適する大きさの部分帯域LLが得られる。

【0119】

工程E2では、その結果として、 $0 \leq i \leq N/2^d - 1$ 及び $0 \leq j \leq N/2^d - 1$ として、成分 I_{ij} により形成される最低周波数の近似部分帯域 LL_4 を選択する。

40

【0120】

図8に示す別の実施形態においては、画像信号Iを先に図6を参照して説明したピラミッド型の分解により分解する。各分解レベルにおいて、工程E2.1では、得られた近似の成分の数nを、例えば、 32×32 に固定された閾値Tと比較して、離散的ウェーブレット変換の場合と同じように、近似の大きさが十分に小さいか否か又はより高いレベルで分解を繰り返さなければならないか否かを判定する。

【0121】

本発明によれば、工程E3では、抽出された非常に低い周波数の部分帯域の成分 I_{ij} の部分集合を選択する。従って、変調すべき成分を限定されたスペクトル領域内で選択することになる。

50

【0122】

以上の実施形態では、変調の際に、抽出される非常に低い周波数の部分帯域のカバレッジの程度 $x\%$ を固定する。例えば、 $x = 80$ を選択する。

【0123】

この例においては、挿入すべき補助情報 S と関連する機密鍵を表現するデジタル信号 K により初期設定される擬似ランダム関数に従って、成分の部分集合を選択する。

【0124】

成分 I_{ij} を走査する順序は定義されている。これらの成分が $N/2^d \times N/2^d$ の大きさの行列の中にあるとき、映像走査の順序は、例えば、左上角から右下角に向かうジグザグの形態で設定される。

10

【0125】

成分 I_{ij} ごとに、工程 E 3 1 では、0 と 1 との間の擬似乱数 $b_k = U(K)$ が得られるように、 K により初期設定される、間隔 $[0, 1]$ に関する均一法則 U などの所定の均一法則 U に従って取り出しを実行する。

【0126】

周知のように、この間隔に関する均一法則 U は、間隔 $[0, 1]$ にわたって均一に分布する一連の実数からなり、各間隔数は同じ出現確率を有する。そこでは、各初期設定値 K に、所定の一連の実数が対応している。この初期設定値 K は秘密鍵になぞらえることができ、これを知っていれば、その一連の実数を全く同じように再構成することが可能である。

【0127】

b_k を取り出すたびに、すなわち、均一法則 U により定義される一連の実数の連続する値ごとに、試験する工程 E 3 2 で、この数 b_k をカバレッジ度 $x/100$ と比較する。 b_k がここでは 0.8 に等しい $x/100$ より小さければ、変調するために、関連する成分 I_{ij} を採用する。これに対し、数 b_k が 0.8 より大きい場合には、関連する成分 I_{ij} を変化させず、工程 E 3 3 で、この成分を非常に低い周波数の部分帯域に再び挿入する。

20

【0128】

この特定の例においては、変調される成分 I_{ij} の割合は、統計的には、工程 E 2 で抽出される非常に低い周波数の成分の五分の四に等しい。

【0129】

言うまでもなく、機密鍵 K がいないときには、変調すべき成分の選択は、例えば、5つの係数の中から続けて4つを選択することにより、系統的に実行できる。また、最も大きい係数を選択するか、又は非常に低い周波数の部分帯域のジグザグに進む順で最初の係数を選択することも可能である。

30

【0130】

更に、本発明によれば、選択された部分集合の成分 I_{ij} を、工程 E 4 で、挿入すべき追加情報を表現するデジタル信号 S により工程 E 4 1 で初期設定される擬似ランダム関数により生成される変調値を加算することにより変調する。

【0131】

例えば、ガウスの法則 $G(0, 1)$ を使用し、挿入すべき信号 S により擬似乱数発生器 16 で初期設定する。

40

【0132】

工程 E 4 1 では、変調すべき成分 I_{ij} ごとに、変調値 $w_k = G(S)$ を取り出す。指標 k は、事前に定義された走査の順序で k 番目の成分 I_{ij} に相当する。各初期設定信号 S に、平均が 0 に等しく且つ標準偏差が 1 に等しい独自の、あらかじめ定められた一連の変調値 w_k が対応している。

【0133】

工程 E 4 2 で、修正係数 α を計算する。この係数 α は変調すべき全ての成分 I_{ij} に対して一定であることができ、典型的には、1 に等しい。これは、挿入情報 S が確実に見えないように保証するものである。

【0134】

50

各成分 I の変調は、工程 E 4 で、変調値：

$$I'_{ij} = I_{ij} + \alpha w_k$$

を加算することにより得られる。

【0135】

ウェーブレットへの分解又はピラミッド型の分解を利用するこれらの実施形態においては、成分 I_{ij} が同等の大きさの順序を有しているならば、一定の修正係数 α を選択すれば十分である。

【0136】

工程 E 4 で、変調値：

$$I'_{ij} = I_{ij} + \alpha_{ij} w_k$$

を加算することにより各成分 I_{ij} の変調が得られるように、係数 I_{ij} に従って修正係数 α を決定することもできるであろう。

【0137】

$\alpha_{ij} = 0.1 \times I_{ij}$ となるように、変調された成分の値に従って係数 α_{ij} に重み付けすることができる。

【0138】

また、変調された成分にごく近い値 I_{ij} の平均に係数 α_{ij} を対応させることもできる。

【0139】

更に、秘密透かしを挿入するための成分の変調が視覚的に許容される最大ひずみを越えないように心理視覚マスキングを行うために、局所可視限界を考慮に入れることも可能である。

【0140】

次に、工程 E 3 3 では、初期成分 I_{ij} の代わりに、変調成分 I'_{ij} を非常に低い周波数の成分に挿入する。

【0141】

工程 E 3 4 では、非常に低い周波数の全ての成分 I_{ij} を走査し終わったか否かを判定するために、試験を実行する。

【0142】

その答えが否定であれば、走査順で次の成分 I_{ij} を考慮し、工程 E 3 から、この成分 I_{ij} を変調すべきか否かを判定するために次の擬似乱数 b_k を取り出すことにより、プロセスを繰り返す。

【0143】

走査が終了すると、最終逆多重分解能スペクトル再組成する工程 E 5 で、透かし挿入画像 I' を再構成する。

【0144】

図 7 に示す実施形態では、逆ウェーブレット返還を実現するために、合成フィルタを使用している。

【0145】

図 8 の例では、連続する近似バージョンと詳細バージョンから透かし挿入画像 I' を再構成している。

【0146】

本発明の第 1 の態様に従った挿入方法により、画像 I' 中の挿入透かし S は、後続する画像 I' の処理に対してはるかに強固なものになっている。加えて、挿入される変調は周波数の一帯域に限定されており、挿入透かしの検査をはるかに迅速に実行できる。

【0147】

次に、本発明のこの第 1 の態様における挿入透かしの復号について、特に図 9 から図 11 を参照して説明する。

【0148】

デコーダ 2（図 1 を参照）は雑音を含む画像 I^* を受信し、初期画像 I 並びに機密鍵 K と関連する情報 S も利用する。

10

20

30

40

50

【0149】

図9に示すように、本発明の第1の態様による復号装置は、透かし挿入デジタルデータ I^* 及び初期デジタルデータ I を多重分解能スペクトル分解するスペクトル分解手段61と、透かし挿入デジタルデータ I^* 及び初期デジタルデータにおける最低周波数の成分を抽出する抽出手段62と、透かし挿入デジタルデータ I^* 及び初期デジタルデータから、先に説明した挿入方法の選択する工程E3で選択された成分の部分集合を選択する選択手段63と、初期デジタルデータ I の前記部分集合の成分 I_{ij} から透かし挿入デジタルデータ I^* の前記部分集合の成分 I'_{ij} をそれぞれ減算することにより、変調値 w_k の推定シーケンス W^* を推定する推定手段64と、前記挿入方法の変調する工程E4で挿入された変調値 w_k の前提シーケンス W を生成する生成手段65と、推定シーケンス W^* と前提シーケンス W との相関値を計算する計算手段と、推定シーケンス W^* と前提シーケンス W とが類似しているか否かを前記相関値に従って決定する決定手段68とを有する。

10

【0150】

挿入装置と同様に、スペクトル分解手段61は離散的ウェーブレット変換を実行し、抽出手段62は近似部分帯域 LL の成分を選択する。このスペクトル分解に関しては先に詳細に説明した。

20

【0151】

本発明の第2の実施形態においては、スペクトル分解手段61は初期デジタルデータ I 及び透かし挿入デジタルデータ I^* を、デジタルデータ又は先行する近似バージョンの低域フィルタリング及びサブサンプリングに相当する近似バージョンと、デジタルデータから又は先行する近似バージョンからの近似バージョンの減算に相当する詳細バージョンとに繰り返し分解し、抽出手段62は近似バージョンの成分を選択する。

【0152】

これらのスペクトル分解手段の選択が秘密情報 S の挿入中に使用された分解の種類によって決まることは容易に理解されるであろう。

【0153】

変調値の前提シーケンス W を生成する生成手段65は、復号すべき補助情報を表現するデジタル信号 S により初期設定される擬似ランダム関数によって生成される変調値を生成する発生器66と協働する。

30

【0154】

この発生器66は挿入装置で使用される発生器16と同一であり、復号することが望まれている補助情報を表現するデジタル信号 S により初期設定される同じガウスの法則 G を使用する変調値 w_k を再計算することが可能になる。

【0155】

同様に、選択手段63は、復号すべき補助情報 S と関連する機密鍵を表現するデジタル信号 K により初期設定される擬似ランダム関数に従って数 b_k を生成する発生器66と協働する。

40

【0156】

図4に示すように、スペクトル分解手段61、抽出手段62、選択手段63、推定手段64、生成手段65、計算手段67及び決定手段68は、マイクロプロセッサ10と、補助情報項目 S を復号するためのプログラムを格納する読み取り専用メモリ102と、プログラムの実行中に修正される変数を記録するためのレジスタを含むランダムアクセスメモリ103とに組み込まれている。

【0157】

マイクロプロセッサ10自体及びその機能は、先に本発明の第1の態様による挿入装置及び方法について説明したのと全く同じである。

50

【0158】

補助情報項目を復号するためのプログラムは、コンピュータ10のハードディスク108に格納するか、あるいはその全体又は一部を着脱自在ではあるが、コンピュータプロパーに一体化されていない格納手段に格納することが可能であろう。

【0159】

中央装置100（CPU）により、復号プログラムの命令を実行できる。すなわち、パワーアップ時、不揮発性メモリの1つ、例えば、読み取り専用メモリ102に格納されているプログラムをランダムアクセスメモリ（RAM）103に格納する。ランダムアクセスメモリ103は、本発明による復号方法を実現するのに必要な変数も格納している。

【0160】

ランダムアクセスメモリ103は、特に、プログラムの実行中に修正される変数を格納するためのいくつかのレジスタを含むことができる。すなわち、ランダムアクセスメモリ103は、例えば、分解レベルごとの近似部分帯域の大きさを格納するレジスタ、変調すべき成分を確定するために取り出される擬似乱数を格納するレジスタ、選択された成分の部分集合を格納するレジスタ、変調値の推定シーケンスを格納するレジスタ、変調値の前提シーケンスを格納するレジスタ及び相関値の計算を格納するレジスタを有する。

【0161】

例えば、原作者を識別するために、秘密透かしを復号することが望まれるデータのコンピュータ10への供給は、様々な周辺装置、特に、グラフィックスカードに接続するデジタルカメラ107、又はスキャナ、あるいはX線撮影装置、その他の画像収集手段又は画像格納手段により実行できる。

【0162】

通信ネットワーク113も復号すべきデジタル画像を供給できる。同様に、ディスク110もデジタルデータを格納することができる。

【0163】

この復号装置はどのような種類のデジタル処理装置にも組み込むことができ、デジタル写真装置又はデジタルカメラに直接に組み込んだり、格納又は処理されるデジタルデータを復号するためにデータベース管理システムに一体化することが可能である。

【0164】

次に、本発明の第1の態様による挿入方法に従ってデジタルデータIに挿入された補助情報項目Sを復号する本発明による復号方法を更に詳細に説明する。

【0165】

図10及び図11を参照すると、この復号方法は、透かし挿入デジタルデータ I^* 及び初期デジタルデータIを多重分解能スペクトル分解する工程E6と、

透かし挿入デジタルデータ I^* 及び初期デジタルデータIから最低周波数の成分を抽出する工程E7と、

透かし挿入デジタルデータ I^* 及び初期デジタルデータIから前記挿入方法の選択する工程E3で選択された成分の部分集合を選択する工程E8と、

初期デジタルデータIの前記部分集合の成分から透かし挿入デジタルデータ I^* の前記部分集合の成分をそれぞれ減算することにより、変調値の推定シーケンス W^* を推定する工程E9と、

前記挿入方法の変調工程E4で挿入された変調値の前提シーケンスWを生成する工程E10と、

推定シーケンス W^* と前提シーケンスWとの相関値を計算する工程E11と、推定シーケンス W^* が前提シーケンスWと類似するか否かを前記相関値に従って決定する工程E12とを含む。

【0166】

図10及び図11は分解する工程E6及び抽出する工程E7以外は同じ復号方法を示す。

【0167】

10

20

30

40

50

図10に示す第1の実施形態では、離散的ウェーブレット変換によりスペクトル分解を実行し、抽出する工程E7では、近似部分帯域LLの成分を選択する。

【0168】

このような復号方法は、補助情報Sが図7を参照して説明した本発明の第1の実施形態による挿入方法を使用して挿入されている場合に使用される。

【0169】

図11に示す復号方法の第2の実施形態においては、スペクトル分解の工程E6中に、初期デジタルデータI及び透かし挿入デジタルデータ I^* を、デジタルデータ又は先行する近似バージョンの低域フィルタリング及びサブサンプリングに相当する近似バージョンと、デジタルデータから又は先行する近似バージョンからの近似バージョンの減算に相当する詳細バージョンとに繰り返し分解し、抽出する工程E7では、近似バージョンの成分を選択する。

10

【0170】

このような復号方法は、補助情報Sが図8を参照して説明した挿入方法の第2の実施形態による挿入方法を使用して挿入されている場合に使用される。

【0171】

いずれの場合にも、多重分解能スペクトル分解方法は、関連する挿入方法において使用されている方法と同一である。

【0172】

各分解レベルで、試験する工程E71において、近似部分帯域の大きさが閾値Tより小さいか否かを検査し、その答えが否定であれば、より高い分解レベルでスペクトル分解を繰り返す。使用される閾値Tは、先に説明した挿入方法で使した閾値と同一である。

20

【0173】

選択する工程E8では、復号すべき補助情報Sと関連する機密鍵を表現するデジタル信号Kにより初期設定される擬似ランダム関数に従って成分の部分集合を選択する。

【0174】

挿入方法の間に使用した法則と同一であり、機密鍵Kにより初期設定される均一法則Uを使用して、同じ一連の擬似実乱数を見出す。従って、雑音を含む画像Iで変調された全ての成分 I'_{ij} と、変調されている初期成分 I_{ij} とを見出すことが可能である。

【0175】

30

初期デジタルデータI及び透かし挿入デジタルデータ I^* の近似部分帯域LLの所定の走査順序で取り出される成分 I_{ij} 及び I'_{ij} ごとに、工程E81で、 $b_k = U(K)$ の取り出しを実行する。工程E82では、この数 b_k をここでは0.8に等しいカバレッジ比 $x/100$ と比較する。

【0176】

b_k が0.8より大きければ、あらかじめ定義された走査順序の次の成分を直接に送り出す。

【0177】

そうでなければ、工程E9で、変調成分ごとに、挿入される変調値 w_k の推定シーケンス W_k^* を得るために、成分 I_{ij} と I'_{ij} との差を生成する。

40

【0178】

$$W_k^* = (I'_{ij} - I_{ij}) / \alpha$$

工程E83では、部分帯域LLの走査が終了したか否かを試験する。その答えが否定であれば、走査順序で次に続く成分に対して工程E8以降を繰り返す。

【0179】

このようにして、一連の推定値 w_k^* に対応するシーケンス W^* を獲得する。

【0180】

デコーダは更に情報Sを有し、生成する工程E10において、変調値 w_k の前提シーケンスW、すなわち、全ての w_k 値を挿入方法の変調工程E4中に使用されたガウスの法則G(S)に従って計算することができる。

50

【0181】

次に、計算する工程E11で、例えば、標準化相関測定を利用して、WとW^{*}との相関の測定を実行する。

【0182】

【数1】

$$\text{corr}(W, W^*) = \frac{(W, W^*)}{\|W\| \times \|W^*\|}$$

10

$$\text{式中、}(W, W^*) = \sum_k w_k w_k^* \text{ 及び } \|W\| = \sqrt{(W, W^*)}$$

【0183】

100 × corr(W, W^{*}) による類似度の計算によって、決定する工程E12において、2つのシーケンスW及びW^{*}が類似しているか否かを決定できるようになる。

【0184】

50%を越えると、相関はデコーダ3の出力端子で肯定の応答を与えるのに十分であると 20
考えられる。言うまでもなく、相関が100%に近いほど、検出の信頼性は高く、従って、挿入されている情報項目Sの認知も高まる。

【0185】

ここで、本発明の第1の態様による挿入方法は、復号の時点で、非常に劣化した画像に相当する品質係数5まで、JPE G (Joint Photographic Expert Group) などの様々な圧縮アルゴリズムに対して75%を越える類似度をもたらすことに注意すべきである。

【0186】

次に、特に図12を参照して本発明の第2の態様による挿入方法を説明する。

【0187】

本発明によれば、秘密透かしなどの補助情報項目Sをデジタルデータ、ここでは画像Iに 30
挿入する方法は、

- a) デジタルデータIを多重分解能スペクトル分解する工程E101と、
- b) 1つの周波数部分帯域の成分を抽出する工程E102とを含む。

【0188】

この場合、挿入方法は、例えば、N=512バイトであるN×Nサイズの画像Iに適用される。

【0189】

スペクトル分解する工程E101は、例えば、離散的ウェーブレット変換によって実行される。ウェーブレット変換による分解のレベルの数dは、近似部分帯域LLの成分の数nが8×8から32×32の間にあるようにあらかじめ定められる。 40

【0190】

このようにして、閾値Tを、例えば、32×32に固定し、分解レベルごとに、試験する工程E121中に、近似部分帯域LLの成分の数nを閾値Tと比較する。

【0191】

試験が否定であれば、すなわち、nが閾値Tより大きい場合には、部分帯域をより高い分解レベルで分解する。

【0192】

この例では、画像Iが正方形であり且つ512×512バイトに等しい大きさであるとき、2対1デシメータによる部分帯域への分解を採用する。同様に正方形である部分帯域LLの大きさは、各分解レベルdにおいて、N/2^d×N/2^dに等しい。 50

【0193】

閾値 T を 32×32 バイトに固定することにより、4 に等しい分解レベル d に適する大きさの部分帯域 LL が得られる。

【0194】

工程 E102 では、低周波数の近似部分帯域 $LL4$ を結果として選択することになる。

【0195】

本発明の第2の態様の方法によれば、工程 E103 で、周波数部分帯域 $LL4$ の成分のスペクトル変換を実行する。このスペクトル変換は、ここでは、離散的コサイン変換、すなわち、DCT である。

【0196】

この DCT 変換は、初期画像 I よりはるかに小さい、ここでは画像 I の $1/6$ の大きさである行列 LL_4 について実行される。従って、変換の速度ははるかに速くなる。

【0197】

その代わりに、高速フーリエ変換、すなわち、FFT を実行することも可能であろう。

【0198】

本発明によれば、工程 E104 で、部分帯域 $LL4$ に限定された DCT スペクトル変換の係数 X_k の部分集合の選択を実行する。従って、変調すべき係数 X_k は限定された一組のスペクトル係数から選択されることになる。

【0199】

変調すべき係数の数 P を確定する。例えば、 P は $(N/2^d \times N/2^d) / 2$ に等しい。

【0200】

変調すべき係数の組から、連続成分 (DC 係数) を除外する。

【0201】

この例では、挿入すべき補助情報 S と関連する機密鍵を表現するデジタル信号 K により初期設定される擬似ランダム関数に従って、係数の部分集合を選択する。

【0202】

例えば、所定の初期設定値 K に対して、間隔 $[0, 1]$ にわたって均一に分布する一連の擬似乱数を関連付ける均一法則 $U(0, 1)$ を使用する。実際には、値 1 も除外する。

【0203】

工程 E181 では、 K により初期設定されるこの所定の均一 U 法則に従って取り出しを実行し、それにより、1 から P の間の k に対して $b_k = U(K)$ を得る。 b_k は厳密に 0 から 1 までの値である。

【0204】

工程 E181 の取り出しごとに、 $b_k \times P$ の整数部を計算する。これは、0 と $P-1$ の間の整数 $n_k = \text{Ent}(b_k P)$ を表す。これは、たとえば、変換後の部分帯域 LL_4 の左上角から右下角に向かうジグザグ走査順序で読み取られる DCT の変調可能係数の中の n_k 番目の係数を変調するために選択される。このようにして、 k が 1 から P まで変化する係数 X_k の部分集合を得る。

【0205】

当然のことながら、機密鍵 K がなければ、最大の大きさの P 個の係数、又はジグザグ走査順序で初めの P 個の係数を常に DC 係数を除外して選択することが可能である。

【0206】

更に、本発明によれば、工程 E105 で、挿入すべき補助情報を表現するデジタル信号 S により初期設定される工程 E182 の擬似ランダム関数により生成される変調値を加算することにより、選択された部分集合の係数 X_k を変調する。

【0207】

例えば、挿入すべき信号 S により初期設定されるガウスの法則 $G(0, 1)$ を利用する。

【0208】

工程 E182 では、 k が 1 から P まで変化するような係数 X_k ごとに、変調値 $w_k = G(S)$ の取り出しを実行する。

10

20

30

40

50

【0209】

工程E183では、修正係数 α を計算する。この係数 α は変調すべきあらゆる係数 X_k に対して一定であることができ、典型的には0.1に等しい。これは、挿入情報Sが確実に見えなくなるように保証する。

【0210】

係数 X_k の変調は、工程E105で変調値：

$$X'_k = X_k (1 + \alpha w_k)$$

を加算することにより得られる。

【0211】

工程E152では、選択された部分集合の全ての係数 X_k を変調したか否かを検査するために試験を実行する。 10

【0212】

全ての変調が終了していなければ、次の係数 X_{k+1} を考慮し、新たな変調値 w_{k+1} を取り出すことにより、工程E182からのプロセスを繰り返す。

【0213】

走査が終了すると、工程E106で、変調済み係数 X'_k の部分集合を含む部分帯域 LL_4 の係数の逆スペクトル変換、ここでは逆DCTを実行する。

【0214】

次に、最終逆多重分解能スペクトル再組成する工程E107で、この場合のように逆ウェーブレット変換の場合には合成フィルタを使用して、透かし挿入画像 I' を得る。 20

【0215】

本発明の第2の態様に従った挿入方法により、画像 I' 中に挿入される透かしSは、画像 I' のその後の処理に対してはるかに強固なものになる。透かしは画像 I' の空間ドメイン全体に分布しているが、挿入される変調は1つの周波数帯域に限定されている。

【0216】

次に、特に図13及び図14を参照して、本発明のこの第2の態様による挿入透かしの復号を説明する。

【0217】

デコーダ2（図1を参照）は雑音を含む画像 I^* を受信し、また、初期画像 I 並びに機密鍵 K と関連する情報 S を利用できる。 30

【0218】

図13に示すように、本発明の第2の態様による復号装置は、透かし挿入デジタルデータ I^* 及び初期デジタルデータ I を多重分解能スペクトル分解するスペクトル分解手段21と、

透かし挿入デジタルデータ I^* 及び初期デジタルデータ I から1つの周波数部分帯域 LL の成分をそれぞれ抽出する抽出手段22と、

透かし挿入デジタルデータ I^* 及び初期デジタルデータ I の周波数部分帯域 LL の成分をスペクトル変換するスペクトル変換手段23と、

透かし挿入デジタルデータ I^* 及び初期デジタルデータ I から前記挿入方法の選択する工程E104で選択された成分の部分集合を選択する選択手段24と、 40

初期デジタルデータ I の前記部分集合の係数から透かし挿入デジタルデータ I^* の前記部分集合の係数をそれぞれ減算することにより、変調値の推定シーケンス W^* を推定する推定手段25と、

前記挿入方法の変調する工程E105で挿入された変調値の前提シーケンス W を生成する生成手段26と、

推定シーケンス W^* と前提シーケンス W との相関の値を計算する計算手段28と、

推定シーケンス W^* と前提シーケンス W とが類似しているか否かを前記相関値に従って決定する決定手段29とを有する。

挿入装置と同様に、抽出手段22は最低周波数を有する部分帯域 LL の成分を選択する。

【0219】

この例では、多重分解能スペクトル分解手段 2 1 は離散的ウェーブレット変換を実行し、抽出手段 2 2 は近似部分帯域 LL の成分を選択する。このスペクトル分解については先に詳細に説明してあり、復号装置により先に図 3 に関連して説明した挿入装置と同様にして実現される。

【0220】

言うまでもなく、挿入装置によりピラミッド型のスペクトル分解が実行された場合には、関連する復号装置も同じピラミッド型の分解を使用して、挿入された補助情報を復号する。

【0221】

同様に、スペクトル変換手段 2 3 は離散的コサイン変換を実行する。

10

【0222】

一般的に、スペクトル分解手段 2 1、抽出手段 2 2 及びスペクトル変換手段 2 3 が、復号することが望まれる補助情報 S を挿入するために挿入装置で使用されたスペクトル分解手段 3 1、抽出手段 3 2 及びスペクトル変換手段 3 3 と同一であることは容易に理解されるであろう。

【0223】

変調値の前提シーケンス W を生成する生成手段 2 6 は、復号すべき補助情報を表現するデジタル信号 S により初期設定される擬似ランダム関数によって生成される変調値を生成する発生器 2 7 と協働する。

【0224】

20

発生器 2 7 は挿入装置で使用される発生器と同一であり、これにより、同じ擬似ランダム関数を使用して変調値 w_k を再計算することができる。

【0225】

同様に、選択手段 2 4 は、復号すべき補助情報 S と関連する機密鍵を表現するデジタル信号 K により初期設定される擬似ランダム関数に従って数 b_k を生成する発生器 2 7 と協働する。

【0226】

スペクトル分解手段 2 1、抽出手段 2 2、スペクトル変換手段 2 3、選択手段 2 4、推定手段 2 5、生成手段 2 6、計算手段 2 8 及び決定手段 2 9 は、図 4 に示すようなマイクロプロセッサ 1 0 に組み込むことができる。このマイクロプロセッサ 1 0 は、先に説明した本発明の第 2 の態様による挿入装置を組み込むためのマイクロプロセッサと構造の点で同じである。

30

【0227】

読み取り専用メモリ 1 0 2 は補助情報項目 S を復号するためのプログラムを格納し、ランダムアクセスメモリ 1 0 3 は、プログラムの実行中に修正される変数を記録するための複数のレジスタを含む。

【0228】

補助情報項目を復号するためのプログラムはコンピュータ 1 0 のハードディスク 1 0 8 に格納するか、あるいはその全体又は一部を着脱自在ではあるが、コンピュータプロパーに一体化されていない格納手段に格納することができるであろう。

40

【0229】

中央装置 1 0 0 (CPU) により、復号プログラムの命令を実行できる。

【0230】

ランダムアクセスメモリ 1 0 3 は、特に、プログラムの実行中に修正される変数を格納するためのいくつかのレジスタを含むことができる。すなわち、ランダムアクセスメモリは、例えば、各分解レベルにおける近似部分帯域の大きさを格納するレジスタ、所定の走査順序の DCT 変換の係数を格納するレジスタ、変調すべき成分を確定するために取り出される擬似乱数を格納するレジスタ、選択された成分部分集合を格納するレジスタ、変調値の推定シーケンスを格納するレジスタ、変調値の前提シーケンスを格納するレジスタ及び修正値の計算を格納するレジスタを有する。

50

【0231】

例えば、原作者を識別するために、秘密透かしを復号することが望まれるデータのコンピュータ10への供給は、様々な周辺装置、特に、グラフィックスカードに接続するデジタルカメラ107、又はスキャナ、X線撮影装置、あるいはその他の画像獲得手段又は画像格納手段により実行できる。

【0232】

この復号装置はどのような種類のデジタル処理装置にも組み込むことができ、デジタル写真装置又はデジタルカメラに直接組み込むか、あるいは格納又は処理されるデジタルデータを復号するためにデータベース管理システムに一体化することも可能である。

【0233】

次に、本発明の第2の態様による挿入方法に従ってデジタルデータIに挿入された補助情報項目Sを復号する本発明による復号方法を更に詳細に説明する。

【0234】

図14を参照すると、この復号方法は、

透かし挿入デジタルデータ I^* 及び初期デジタルデータを多重分解能スペクトル分解する工程E110と、

透かし挿入デジタルデータ I^* 及び初期デジタルデータIから1つの周波数部分帯域LLの成分をそれぞれ抽出する工程E111と、

透かし挿入デジタルデータ I^* 及び初期デジタルデータIの周波数部分帯域LLの成分をスペクトル変換する工程E112と、

透かし挿入デジタルデータ I^* 及び初期デジタルデータIから前記挿入方法の選択する工程E104で選択された成分の部分集合を選択する工程E113と、

初期デジタルデータIの前記部分集合の係数から透かし挿入デジタルデータ I^* の前記部分集合の係数をそれぞれ減算することにより、変調値の推定シーケンス W^* を推定する工程E114と、

前記挿入方法の変調する工程E105で挿入された変調値の前提シーケンスWを生成する工程E115と、

推定シーケンス W^* と前提シーケンスWとの相関の値を計算する工程E116と、

推定シーケンス W^* と前提シーケンスWとが類似しているか否かを前記相関値に従って決定する工程E117とを含む。

【0235】

関連する挿入方法の場合と同様に、スペクトル分解する工程E110では、離散的ウェーブレット変換によってスペクトル分解を実行し、抽出する工程E111では、最低周波数を有する近似部分帯域LLの成分を選択する。

【0236】

試験する工程E1111では、各分解レベルで、近似部分帯域の大きさが閾値Tより小さいか否かを検査し、その答えが否定であれば、より高い分解レベルでスペクトル分解を繰り返す。使用する閾値Tは、先に図12を参照して説明した挿入方法で使用した閾値と同一である。

【0237】

スペクトル変換も同様に離散的コサイン変換DCTである。

【0238】

選択する工程E113では、復号すべき補助情報Sと関連する機密鍵を表現するデジタル信号Kにより初期設定される擬似ランダム関数に従って係数の部分集合を選択する。

【0239】

挿入方法の間に使用された法則と同一であり、機密鍵Kにより初期設定される均一法則Uを使用して、同じ一連の実擬似乱数を見出す。従って、雑音を含む画像 I^* で変調された全ての係数 X'_k と、初期画像Iで変調されている初期係数 X_k とを見出すことができる。

【0240】

更に厳密に言えば、挿入方法において詳細に説明したように、工程E1131で、数 b_k

10

20

30

40

50

= U (K) の取り出しを実行し、 $b_k \times P$ の整数部を計算する。なお、P は変調される係数の数である。 $n_k = \text{Ent} (b_k \times P)$ を求め、雑音を含む画像 I^* と初期画像 I の双方について、DCT の係数のあらかじめ定義された走査の順序で n_k 番目の係数を選択する。

【0241】

選択された係数の部分集合に関して、推定する工程 E 1 1 4 では、次の復調式に従って、 k が 1 から P まで変化するような変調値 w_k の推定 w_k^* を得るために、これらの係数 X'_k と X_k との差を生成する。

【0242】

【数2】

10

$$w_k^* = \frac{1}{\alpha} \left(\frac{X'_k - X_k}{X_k} \right)$$

【0243】

画像 I' が重大なひずみを受けており、変調された係数 X_k が低振幅である場合、推定値 w_k^* は非常に大きくなる可能性があり、従って、異常な値になるおそれがある。実際には、この値 w_k^* を制限する必要がある。例えば、 w_k^* が 5 に固定された閾値より大きい場合には、値 1 が w_k^* に割り当てられる。

20

【0244】

このようにして、 k が 1 から P まで変化する推定値 w_k^* の連続に相当するシーケンス W^* を獲得する。

【0245】

生成する工程 E 1 1 5 では、復号すべき補助情報を表現するデジタル信号 S により初期設定される擬似ランダム関数により、変調値の前提シーケンス W を生成する。

【0246】

30

同様に情報 S を利用できるデコーダは、実際には、生成する工程 E 1 1 5 で、前提シーケンス W、すなわち、 k が 1 から P まで変化する全ての w_k 値を、挿入方法の変調する工程 E 1 0 5 中に使用されたガウスの法則 G (S) に従って計算することができる。

【0247】

そこで、計算する工程 E 1 1 6 では、例えば、標準相関測定を使用して、W と W^* との相関の測定を実行する。

【0248】

【数3】

40

$$\text{corr}(W, W^*) = \frac{(W, W^*)}{\|W\| \times \|W^*\|}$$

$$\text{式中、}(W, W^*) = \sum_k w_k w_k^* \text{ 及び } \|W\| = \sqrt{(W, W^*)}$$

【0249】

$100 \times \text{corr}(W, W^*)$ による類似度の計算によって、決定する工程 E 1 1 7 で、2 つのシーケンス W 及び W^* が類似しているか否かを決定することができる。

50

【0250】

50%を越えると、相関は検出器3の出力端子で肯定の応答を与えるのに十分であると考えられる。当然のことながら、相関が100%に近づくほど、検出の信頼性は高くなり、従って、挿入情報項目Sの認知の信頼性も高まる。

【0251】

図15は、本発明の第2の態様による挿入方法に従って挿入された情報の強固さと、画像I全体に適用されるDCT変換を使用して補助情報を挿入する従来の方法における挿入情報の強固さとを比較した図である。

【0252】

この強固さは、挿入された透かしと、画像I'の処理後に抽出された透かしとの類似度により、使用される処理の品質係数に従って表される。 10

【0253】

この例では、画像I'は、離散的コサイン変換DCTに基づくJPEG (Joint Photographic Expert Group) 規格に従って圧縮及び伸張の処理を受けている。

【0254】

本発明による方法においては、分解レベルは5に等しく、双方の場合で、変調される係数の数は128に等しい。

【0255】

ここでは、本発明の方法は非常に劣化した画像に相当する品質係数5まで90%の類似度を示し、これに対し、従来の方法は品質係数60までと、明らかに低いことがわかってい 20

【0256】

本発明による挿入方法及び関連する装置によって、デジタルデータに挿入される情報の強固さを気づかれないような方式で大幅に向上させることができる。

【0257】

言うまでもなく、本発明は先に説明した例にのみ限定されるのではなく、本発明の範囲から逸脱せずに、数多くの変形を実施することができる。

【0258】

すなわち、透かしを挿入されるデジタルデータは音声データであっても良いであろう。

【0259】

更に、本発明の第2の態様における多重分解能スペクトル分解の近似部分帯域にではなく、詳細部分帯域にスペクトル変換を適用することも可能であろう。 30

【0260】

【発明の効果】

以上説明したように本発明によれば、既存の挿入方法を改善し且つ特に不可視度及び強固さに関して、挿入される透かしの品質を向上させることが可能になる。

【図面の簡単な説明】

【図1】 デジタル信号への補助情報項目の挿入を示す概略図である。

【図2】 第1の態様による本発明の一実施形態の挿入装置を示すブロック線図である。

【図3】 第2の態様による本発明の一実施形態の挿入装置の処理の流れを示す図である。 40

【図4】 本発明による方法を実現するためのデジタル信号処理装置のブロック図である。

【図5】 画像を複数の部分帯域に分解する第1の方法を概略的に示す図である。

【図6】 画像を複数の部分帯域に分解する第2の方法を概略的に示す図である。

【図7】 本発明の第1の態様の第1の実施形態に従って補助情報項目を画像に挿入するためのアルゴリズムを示す図である。

【図8】 本発明の第1の態様の第2の実施形態に従って補助情報項目を画像に挿入するためのアルゴリズムを示す図である。

【図9】 本発明の第1の態様の一実施形態による復号装置の処理の流れを示す図である。

【図10】 本発明の第1の態様の第1の実施形態に従って画像中の補助情報項目を復号するためのアルゴリズムを示す図である。 50

【図 1 1】 本発明の第 1 の態様の第 2 の実施形態に従って画像中の補助情報項目を復号するためのアルゴリズムを示す図である。

【図 1 2】 本発明の第 2 の態様の一実施形態に従って補助情報項目を画像に挿入するためのアルゴリズムを示す図である。

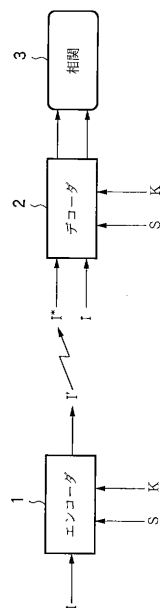
【図 1 3】 本発明の第 2 の態様の一実施形態による復号装置の処理の流れを示す図である。

【図 1 4】 本発明の第 2 の態様の一実施形態に従って画像中の補助情報項目を復号するためのアルゴリズムを示す図である。

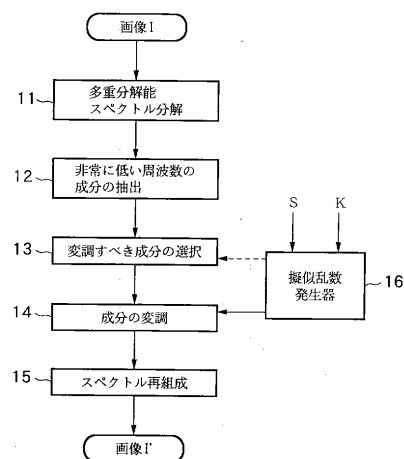
【図 1 5】 本発明の第 2 の態様による挿入方法により挿入された透かしと、従来の方法により挿入された透かしの、J P E G 規格に従った圧縮に対する強固さを比較した曲線を示す図である。

10

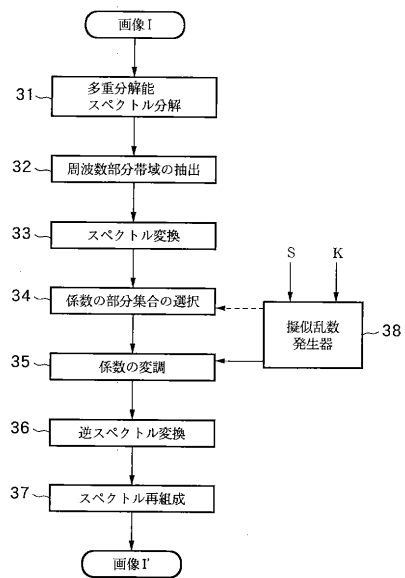
【図 1】



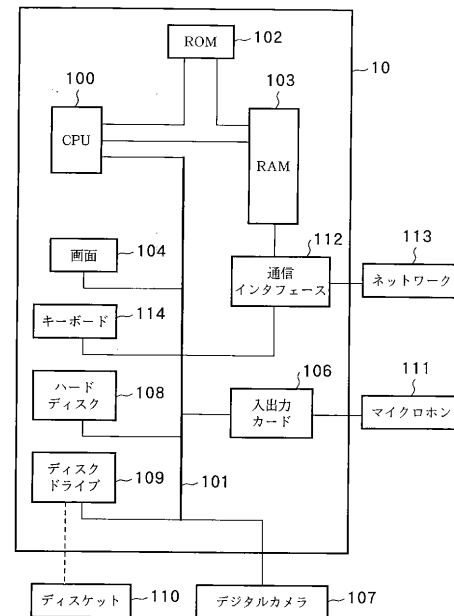
【図 2】



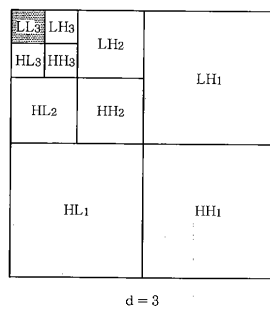
【図 3】



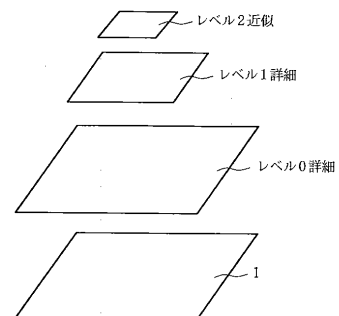
【図 4】



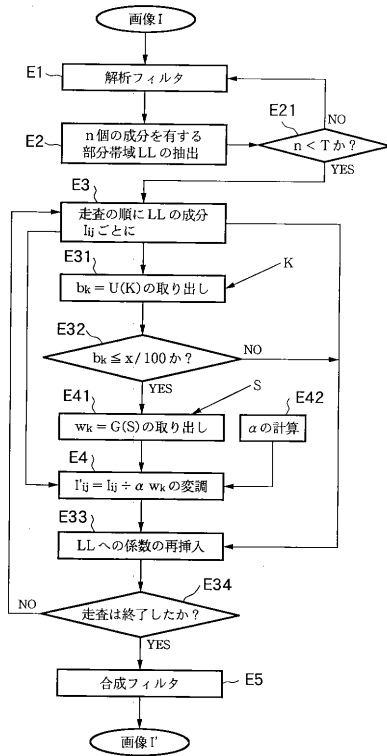
【図 5】



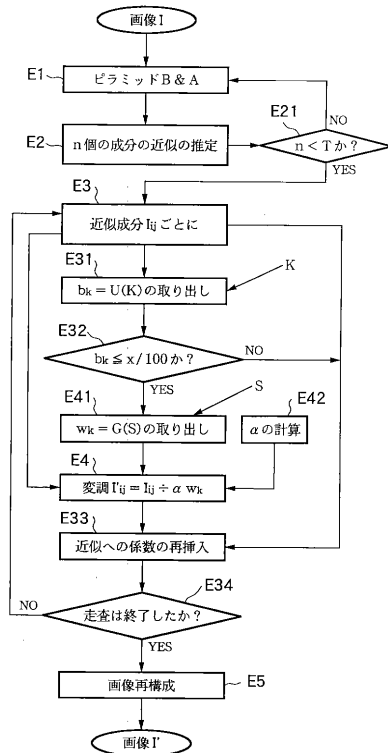
【図 6】



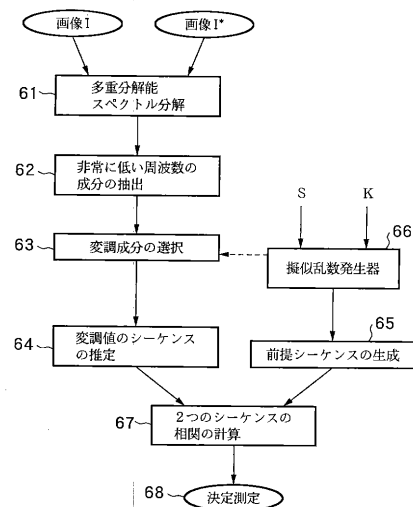
【図 7】



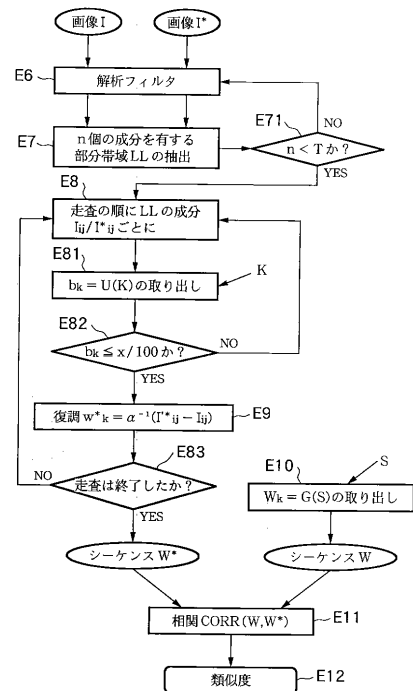
【図 8】



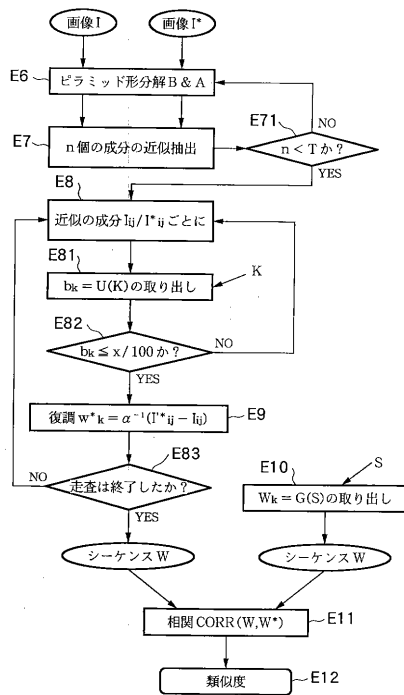
【図 9】



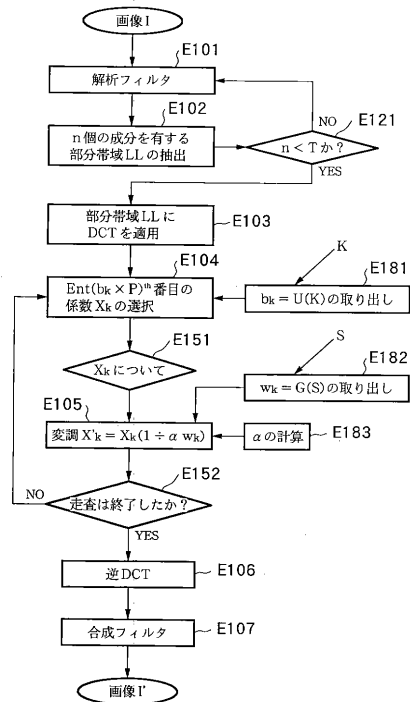
【図 10】



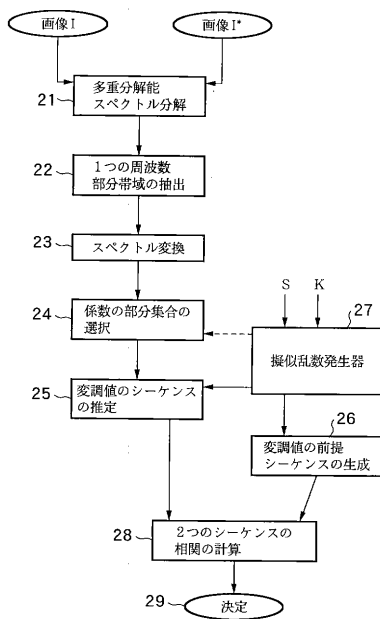
【図 1 1】



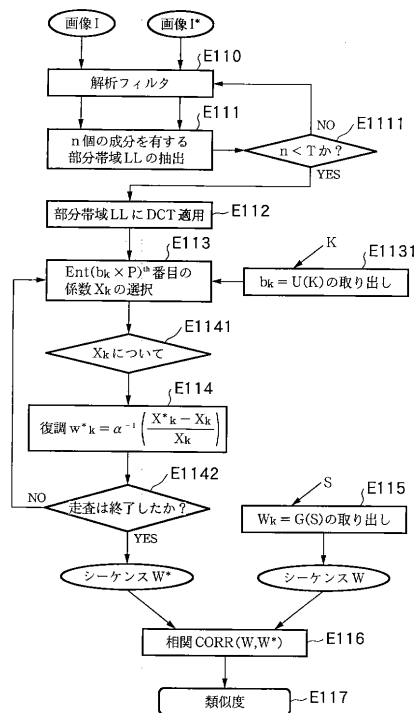
【図 1 2】



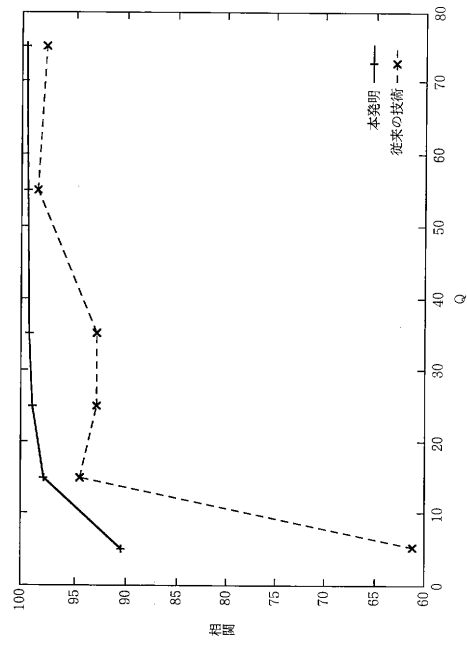
【図 1 3】



【図 1 4】



【図 15】



フロントページの続き

(72)発明者 イオアナ ドネスワ

フランス国 レンヌーアタラント, セデックス セッソニーセヴィニエ 35517, リュ
ドゥ ラ トゥッシューランベール キヤノン リサーチ センター フランス エス. エー.
内

審査官 曾我 亮司

(56)参考文献 米国特許第06332030 (US, B1)

特開平09-191394 (JP, A)

米国特許第06359998 (US, B1)

(58)調査した分野(Int.Cl., DB名)

H04N 1/387

G06T 1/00

G09C 5/00

H04N 7/26