(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号

特許第4240614号
(P4240614)

(45)発行日　平成21年3月18日(2009.3.18)　(24)登録日　平成21年1月9日(2009.1.9)

(51)Int.Cl.		F I	
H03M 7/00	(2006.01)	H03M	7/00
G09C 5/00	(2006.01)	G09C	5/00
H03M 13/23	(2006.01)	H03M	13/23
H03M 13/29	(2006.01)	H03M	13/29
H04N 1/387	(2006.01)	H04N	1/387

請求項の数 16　(全 23 頁)　最終頁に続く

(21)出願番号　特願平10-345452
(22)出願日　平成10年12月4日(1998.12.4)
(65)公開番号　特開2000-174628(P2000-174628A)
(43)公開日　平成12年6月23日(2000.6.23)
審査請求日　平成17年12月2日(2005.12.2)

(73)特許権者　000001007
キヤノン株式会社
東京都大田区下丸子３丁目３０番２号
(74)代理人　100090538
弁理士　西山　恵三
(74)代理人　100096965
弁理士　内尾　裕一
(72)発明者　吉田　淳
東京都大田区下丸子３丁目３０番２号キヤノン株式会社内

審査官　矢頭　尚之

最終頁に続く

(54)【発明の名称】埋め込み装置及びコンピュータ読み取り可能な記憶媒体

(57)【特許請求の範囲】

【請求項１】

電子透かし情報を暗号化する暗号化手段と、

前記暗号化手段によって暗号化された前記電子透かし情報を、畳み込み符号化方式を用いて符号化する符号化手段と、

前記符号化手段によって符号化された前記電子透かし情報を複数個前記デジタル画像データに埋め込む埋め込み手段と

を有することを特徴とする埋め込み装置。

【請求項２】

前記電子透かし情報は、著作権に関する情報、ユーザに関する情報、前記埋め込み装置に関する情報、前記デジタル画像データのコピー回数または世代を制限するための情報、前記デジタル画像データの流通経路に関する情報の少なくとも一つを含むことを特徴とする請求項１に記載の埋め込み装置。

【請求項３】

前記デジタル画像データに対してウェーブレット変換を行う変換手段をさらに有し、

前記埋め込み手段は、前記符号化手段によって符号化された前記電子透かし情報を、ウェーブレット変換後の前記デジタル画像データに埋め込むことを特徴とする請求項１または２に記載の埋め込み装置。

【請求項４】

前記埋め込み装置は、デジタルカメラ、デジタルカメラ付き情報端末、スキャナのいず

れかであることを特徴とする請求項１から３のいずれか１項に記載の埋め込み装置。
【請求項５】
電子透かし情報を暗号化する暗号化手段と、
前記暗号化手段によって暗号化された前記電子透かし情報を、ターボ符号化方式を用いて符号化する符号化手段と、
前記符号化手段によって符号化された前記電子透かし情報を複数個前記デジタル画像データに埋め込む埋め込み手段と
を有することを特徴とする埋め込み装置。
【請求項６】
前記電子透かし情報は、著作権に関する情報、ユーザに関する情報、前記埋め込み装置に関する情報、前記デジタル画像データのコピー回数または世代を制限するための情報、前記デジタル画像データの流通経路に関する情報の少なくとも一つを含むことを特徴とする請求項５に記載の埋め込み装置。
【請求項７】
前記デジタル画像データに対してウェーブレット変換を行う変換手段をさらに有し、
前記埋め込み手段は、前記符号化手段によって符号化された前記電子透かし情報を、ウェーブレット変換後の前記デジタル画像データに埋め込むことを特徴とする請求項５または６に記載の埋め込み装置。
【請求項８】
前記埋め込み装置は、デジタルカメラ、デジタルカメラ付き情報端末、スキャナのいずれかであることを特徴とする請求項５から７のいずれか１項に記載の埋め込み装置。
【請求項９】
電子透かし情報を暗号化する暗号化ステップと、
前記暗号化ステップで暗号化された前記電子透かし情報を、畳み込み符号化方式を用いて符号化する符号化ステップと、
前記符号化ステップで符号化された前記電子透かし情報を複数個前記デジタル画像データに埋め込む埋め込みステップと
を有する埋め込み方法を埋め込み装置に実行させるためのプログラムを記憶したことを特徴とするコンピュータ読み取り可能な記憶媒体。
【請求項１０】
前記電子透かし情報は、著作権に関する情報、ユーザに関する情報、前記埋め込み装置に関する情報、前記デジタル画像データのコピー回数または世代を制限するための情報、前記デジタル画像データの流通経路に関する情報の少なくとも一つを含むことを特徴とする請求項９に記載のコンピュータ読み取り可能な記憶媒体。
【請求項１１】
前記デジタル画像データに対してウェーブレット変換を行う変換ステップをさらに有し、
前記埋め込みステップは、前記符号化ステップで符号化された前記電子透かし情報を、ウェーブレット変換後の前記デジタル画像データに埋め込むことを特徴とする請求項９または１０に記載のコンピュータ読み取り可能な記憶媒体。
【請求項１２】
前記埋め込み装置は、デジタルカメラ、デジタルカメラ付き情報端末、スキャナのいずれかであることを特徴とする請求項９から１１のいずれか１項に記載のコンピュータ読み取り可能な記憶媒体。
【請求項１３】
電子透かし情報を暗号化する暗号化ステップと、
前記暗号化ステップで暗号化された前記電子透かし情報を、ターボ符号化方式を用いて符号化する符号化ステップと、
前記符号化ステップで符号化された前記電子透かし情報を複数個前記デジタル画像データに埋め込む埋め込みステップと

を有する埋め込み方法を埋め込み装置に実行させるためのプログラムを記憶したことを特徴とするコンピュータ読み取り可能な記憶媒体。
【請求項１４】
前記電子透かし情報は、著作権に関する情報、ユーザに関する情報、前記埋め込み装置に関する情報、前記デジタル画像データのコピー回数または世代を制限するための情報、前記デジタル画像データの流通経路に関する情報の少なくとも一つを含むことを特徴とする請求項１３に記載のコンピュータ読み取り可能な記憶媒体。
【請求項１５】
前記デジタル画像データに対してウェーブレット変換を行う変換ステップをさらに有し、
前記埋め込みステップは、前記符号化ステップで符号化された前記電子透かし情報を、ウェーブレット変換後の前記デジタル画像データに埋め込むことを特徴とする請求項１３または１４に記載のコンピュータ読み取り可能な記憶媒体。
【請求項１６】
前記埋め込み装置は、デジタルカメラ、デジタルカメラ付き情報端末、スキャナのいずれかであることを特徴とする請求項１３から１５のいずれか１項に記載のコンピュータ読み取り可能な記憶媒体。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】
本発明は、デジタルコンテンツの著作権の保護、改竄の防止等を実現する埋め込み装置及びコンピュータ読み取り可能な記憶媒体に関する。
【０００２】
【従来の技術】
デジタル情報には、従来のアナログ情報と比較して次のような特徴がある。
【０００３】
一つ目は、パーソナルコンピュータ（以下、ＰＣ）等によって、簡単に劣化することなくオリジナルと同程度の品質の複製データを作ることができる。二つ目は、ＰＣ等によって、オリジナルデータを容易に改竄することができる。三つ目は、不正にコピーした複製データや不正に改竄を行った改竄データを通信回線を通じて他のユーザに簡単に転送することができる。このような特徴により、デジタル情報には、容易にコピーされ、不正に再配布される危険性があった。
【０００４】
このような危険性を防止する手法の一つに、電子透かし技術がある。電子透かし技術とは、デジタル情報からなるデジタルコンテンツに対して目に見える又は目に見えない形で何らかの情報（例えば、著作権情報）を埋め込む技術である。
【０００５】
【発明が解決しようとする課題】
通常、電子透かし情報を埋め込んだデジタルコンテンツに対して圧縮、切り取り、回転、拡大、縮小、色変換等の信号処理を加えた場合、或いは埋め込まれた電子透かし情報を故意に消去又は破壊しようとする信号処理（以下、このような信号処理を単に「攻撃」と称する）を加えた場合、そのデジタルコンテンツから抽出される電子透かし情報が埋め込み前の電子透かし情報とは異なってしまう問題があった。
【０００６】
各種の信号処理或いは攻撃の強弱に関わらずデジタルコンテンツに埋め込まれた電子透かし情報を正しく抽出するためには、埋め込み強度を強くして電子透かし情報の耐性を高める必要があった。例えば、量子化によって電子透かし情報を埋め込む場合には、量子化ステップを大きくすることによって、埋め込み強度が強くなるようにしていた。
【０００７】
しかしながら、デジタルコンテンツに対して強い強度で電子透かし情報を埋め込む場合、

抽出情報の誤り率を小さくすることはできるが、そのデジタルコンテンツの品質を大きく劣化させてしまう問題があった。

【０００８】

そこで、本発明は、デジタルコンテンツに埋め込まれた電子透かし情報の耐性を高めることができるようにすることを目的とする。

【００１０】

【課題を解決するための手段】

本発明に係る埋め込み装置は、例えば、電子透かし情報を暗号化する暗号化手段と、前記暗号化手段によって暗号化された前記電子透かし情報を、畳み込み符号化方式を用いて符号化する符号化手段と、前記符号化手段によって符号化された前記電子透かし情報を複数個前記デジタル画像データに埋め込む埋め込み手段とを有することを特徴とする。

【００１１】

本発明に係る他の埋め込み装置は、例えば、電子透かし情報を暗号化する暗号化手段と、前記暗号化手段によって暗号化された前記電子透かし情報を、ターボ符号化方式を用いて符号化する符号化手段と、前記符号化手段によって符号化された前記電子透かし情報を複数個前記デジタル画像データに埋め込む埋め込み手段とを有することを特徴とする。

【００１２】

本発明に係るコンピュータ読み取り可能な記憶媒体は、例えば、電子透かし情報を暗号化する暗号化ステップと、前記暗号化ステップで暗号化された前記電子透かし情報を、畳み込み符号化方式を用いて符号化する符号化ステップと、前記符号化ステップで符号化された前記電子透かし情報を複数個前記デジタル画像データに埋め込む埋め込みステップとを有する埋め込み方法を埋め込み装置に実行させるためのプログラムを記憶したことを特徴とする。

【００１３】

本発明に係る他のコンピュータ読み取り可能な記憶媒体は、例えば、電子透かし情報を暗号化する暗号化ステップと、前記暗号化ステップで暗号化された前記電子透かし情報を、ターボ符号化方式を用いて符号化する符号化ステップと、前記符号化ステップで符号化された前記電子透かし情報を複数個前記デジタル画像データに埋め込む埋め込みステップとを有する埋め込み方法を埋め込み装置に実行させるためのプログラムを記憶したことを特徴とする。

【００２５】

【発明の実施の形態】

以下、本発明に係る埋め込み装置、埋め込み方法、抽出装置、抽出方法及びコンピュータ読み取り可能な記憶媒体について図面を用いて詳細に説明する。

【００２６】

以下では、まず、後述の各実施例に適用可能なビタビ復号アルゴリズムの基本的な処理手順について説明する。次に、埋め込み情報（例えば、畳み込み符号化された電子透かし情報）を表すビット列を複数回デジタルコンテンツに対して埋め込む埋め込み装置について説明する。続いて、各実施例において、そのデジタルコンテンツに埋め込まれた複数個の同じ埋め込み情報を抽出し、各埋め込み情報の同じビット位置に対応する複数１ビットの抽出情報の集合を入力系列の一つとして軟判定復号を行う抽出装置について説明する。

【００２７】

（ビタビ復号アルゴリズム）

図１は、ビタビ復号部の内部状態を各時刻毎に示したトレリス線図である。以下、図１に示すトレリス線図を用いて各実施例に適用可能なビタビ復号アルゴリズムの基本的な処理手順について説明する。

【００２８】

図１では、生成行列Ｇ（Ｄ）を、

$G(D) = [1 + D^2, \ 1 + D + D^2]$

とする場合の例を示す。ここでＤは、遅延演算子を表している。

【００２９】
図１において、各時刻ｔにおける内部状態を黒点で示す。時刻ｋにおいて、新しい入力系列が入力されると、ビタビ復号部はそれに応じて２個のコードシンボルを出力し、時刻ｋ＋１の状態に遷移する。図１において、実線は入力系列に含まれる情報系列が「０」、点線は入力系列に含まれる情報系列が「１」となる場合の遷移を示している。ここで、状態の遷移を示す各線を「ブランチ」と呼び、各ブランチに対応したシンボルを「ブランチシンボル」と呼ぶ。
【００３０】
今、あるブランチに着目した場合、そのブランチのブランチシンボルと入力系列との相関の強さを「ブランチメトリック」と呼ぶ。又、時刻ｋの状態Ｓ（ｋ）から時刻ｋ'の状態Ｓ'（ｋ'）に至るルート、即ち複数のブランチをつなぐルートを「パス」と呼び、あるパスに含まれるブランチのブランチメトリックの総和を「パスメトリック」と呼ぶ。更に、ある時刻ｋにおいて状態Ｓ（ｋ）に至るパスのうち、入力系列と相関の最も強くなるパスを「生き残りパス」と呼ぶ。
【００３１】
図１において、各ブランチのブランチメトリックは、入力系列とブランチシンボルとのハミング距離により求められる。従って、ある状態Ｓ（ｋ）に至るパスのうち、パスメトリックの値が最小となるパスが生き残りパスとなる。ここで、各状態Ｓ（ｋ）における生き残りパスのパスメトリックの値を図１の黒点付近に十進数で表す。又、図１において、生き残りパスとして選択されなかったパスを三角形（△）によって消去する。
【００３２】
例えば、図１において、時刻４の状態Ｓ００（４）に至るパスには、時刻３の状態S_{00}（３）において情報系列「０」が入力された場合（第１のパス）と時刻３の状態S_{01}（３）において情報系列「０」が入力された場合（第２のパス）とがある。第１のパスにおいて、状態S_{00}（３）から状態S_{00}（４）に遷移するブランチのブランチメトリックは「１」であり、状態S_{00}（３）における生き残りパスのパスメトリックは「１」であるので、このパスのパスメトリックは「２」となる。又、第２のパスにおいて、状態S_{01}（３）から状態S_{00}（４）に遷移するブランチのブランチメトリックは「１」であり、状態S_{00}（３）における生き残りパスのパスメトリックは「２」であるので、このパスのパスメトリックは「３」となる。従って、第１のパスが、状態S_{00}（４）に至る生き残りパスとなる。
【００３３】
このように、ビタビ復号アルゴリズムでは、各時刻において各状態の生き残りパスとそのパスのパスメトリックとを順次定めていく。ビタビ復号アルゴリズムの終了方法には数通りの方法があるが、代表的なものとして次の二つ方法がある。
【００３４】
第１の方法では、畳み込み符号化される情報系列のビット長を予め定めておく。ビタビ復号部では、そのビット長に対応する生き残りパスを求めたら、その時刻において最も入力系列と相関の高いパスに対応する情報系列を復号結果とする。第２の方法では、符号化される情報系列のビット長を予め定めておき、その情報系列の最後に遅延演算子（即ち、生成行列中のＤ）を全て初期状態に戻すだけの「０」を加えて符号化する。ビタビ復号部では、最終的に初期状態に達した後、その時点の生き残りパスに対応する情報系列を復号結果とする。
【００３５】
例えば、図１を用いて、第２の方法（即ち、遅延演算子を初期状態に戻す方法）を用いたビタビ復号アルゴリズムについて説明する。送信側では、情報系列のビット長が５ビット、遅延演算子を初期状態〔０，０〕に戻すためのビットが２ビットとなる情報を畳み込み符号化し、外部に出力する。この出力は、伝送路を介してビタビ復号部に入力される。このときビタビ復号部に入力された入力系列が〔００　１０　００　１０　００　１１　１１〕となった場合、図１の太線で示したパスがただ一つの生き残りパスとなり、その結果、情報系列〔０　１　１　０　１　０　０〕が復号される。この情報系列のうち、最後の２ビットは遅

延演算子を初期状態に戻すためのビットである。従って、畳み込み符号化される前の情報系列は〔０　１　１　０　１〕と推定される。

【００３６】

このように、上述のビタビ復号アルゴリズムでは、入力系列とブランチシンボルとのハミング距離を用いてブランチメトリックを求める方法について説明したが、より訂正能力を高めるためには、上述のビタビ復号アルゴリズムに軟判定方式を導入することができる。

【００３７】

軟判定方式とは、入力情報がある値となる確からしさを使用する方法であり、例えば入力情報を複数個の閾値で判定し、その判定結果を用いて入力系列を復号する方法である。この場合、上述のブランチメトリックは、入力情報とブランチシンボルとのユークリッド距離、ユークリッド距離の二乗、確率Ｐ（ｕ｜ｙ）等を用いて求められる。ここで、ｕはブランチシンボルを示し、ｙは入力情報を示す。従って、ユークリッド距離或いはユークリッド距離の二乗を用いた場合、ある状態に至るパスの中でパスメトリックの値が最小となるパスが生き残りパスとなる。又、確率を用いた場合は、パスメトリックの値が最大となるパスが生き残りパスとなる。

【００３８】

このような軟判定方式に基づくビタビ復号アルゴリズムを本実施例では、「軟判定ビタビ復号アルゴリズム」と呼ぶ。

【００３９】

（埋め込み装置）

図２は、本実施例の埋め込み装置２０１の構成を説明するブロック図である。尚、埋め込み装置２０１は、例えば、撮像部２０４を具備するデジタルカメラ、カメラ一体型デジタルカメラ、スキャナ、デジタルカメラ付き情報端末等の情報処理装置である。

【００４０】

図２において、２０２は埋め込み装置２０１を構成する各部を協調させて制御するＣＰＵ、２０３は各種の演算処理に用いられるメモリ、２０４は被写体の光学像を電気信号に変換し、その電気信号を所定のフォーマットのデジタル画像データを生成する撮像部である。

【００４１】

２０５は外部の電子機器にて生成されたデジタル画像データを入力し、電子透かし情報を埋め込んだデジタル画像データとそのデジタル画像データから電子透かし情報を抽出する際に必要となる付加情報とを出力する入出力部、２０６は撮像部２０４より出力されたデジタル画像データに対してウェーブレット変換を行うウェーブレット変換部、２０７はウェーブレット変換部２０６にて生成される複数のツリーの内、所定の規則により選択されたツリーを埋め込み対象として１つ以上の同じ電子透かし情報を埋め込む電子透かし埋め込み部である。

【００４２】

２０８はリードソロモン方式を用いて電子透かし情報を誤り訂正符号化する誤り訂正符号化部、２０９は共通鍵暗号方式の一つであるＤＥＳ（Ｄａｔａ　Ｅｎｃｒｙｐｔｉｏｎ　Ｓｙｓｔｅｍ）方式を用いて電子透かし情報を暗号化するＤＥＳ暗号化部、２１０はデジタル画像データに埋め込む埋め込み情報を畳み込み符号化する畳み込み符号化部である。

【００４３】

２１１は各部の間のデータの送受信を行う内部バス、２１２は図３にて説明する電子透かし埋め込みアルゴリズムを実現するＣＰＵ２０２の読み出し可能なプログラムが格納されたＲＯＭ、２１３はデジタル画像データに埋め込む電子透かし情報を生成する電子透かし生成部、２１４はターボ符号化方式を用いて電子透かし情報を符号化するターボ符号化部である。

【００４４】

尚、入出力部２０５は、ＩｒＤＡ規格に準拠した赤外線通信用インタフェース回路、或い

はＵＳＢ規格やＩＥＥＥ１３９４規格に準拠したデジタルインタフェース回路等からなり、デジタル画像データを通信するのに適した通信プロトコルを用いて外部の情報処理装置とデジタル画像データの送受信を行う。

【００４５】

又、電子透かし生成部２１３は、著作権情報、ユーザの個人情報（例えば、氏名、ユーザコード、e-mailのアドレス等）、埋め込み装置２０１に関する情報（例えば、メーカコード、機種コード等）、２次元的な模様を示すデータ、デジタル画像データのコピー回数やコピー世代を制限する管理情報、デジタル画像データの流通経路を示すデータの少なくとも一つから電子透かし情報を生成する。ここで、これらの情報は、電子透かし生成部２１３に予め保持されているか、電子透かし生成部２１２を用いてユーザ自身が設定したものである。

【００４６】

又、ターボ符号化部２１４の構成の一例を図１４（Ａ）に示す。ターボ符号化部２１４は、インタリーバ１４０１を介して複数個の誤り訂正符号化回路１４０２、１４０３を組み合わせるように構成されている。ここで、インタリーバ１４０１は、電子透かし情報ｘを一時的にメモリに書き込んだ後、不規則な順序で読み出していく非一様インタリーバである。又、誤り訂正符号化回路１４０２、１４０３の夫々は、軟判定復号可能な符号化方式でよく、畳み込み符号化方式或いはブロック符号化方式に基づいて誤り訂正符号化を行う。これにより、誤り訂正符号化回路１４０２、１４０３の各出力ｙ１、ｙ２と電子透かし情報ｘとの一組がターボ符号化データとしてターボ符号化部２１４から出力され、デジタル画像データに埋め込まれる。

【００４７】

図３は、埋め込み装置２０１における電子透かし埋め込みアルゴリズムの一例を示すＮＳチャートである。以下、図３を用いて本実施例のおける電子透かし埋め込みアルゴリズムを説明する。

【００４８】

処理３１は、入力処理である。処理３１において、撮像部２０４は、被写体の光学像を電気信号に変換し、その電気信号から所定のフォーマットのデジタル画像データを生成する。このデジタル画像データは、ウェーブレット変換部２０６に入力される。又、処理３１では、入出力部２０５を介して、外部の情報処理装置からデジタル画像データを入力し、そのデータをウェーブレット変換部２０６に入力してもよい。

【００４９】

処理３２は、埋め込み情報生成処理である。処理３２において、電子透かし生成部２１３は、上述の情報からなる電子透かし情報を生成する。畳み込み符号化部２１０は、これらの電子透かし情報を畳み込み符号化し、それを埋め込み情報として電子透かし埋め込み部２０７に供給する。

【００５０】

ここで、電子透かし生成部２１３は、電子透かし情報を畳み込み符号化部２１０に供給する前に、必要に応じて誤り訂正符号化部２０８或いはＤＥＳ暗号化部２０９に供給してもよい。

【００５１】

誤り訂正符号化部２０８に供給された場合、誤り訂正符号化部２０８は、電子透かし情報を、例えばリードソロモン符号化方式を用いて誤り訂正符号化し、その結果を畳み込み符号化部２１０に供給する。尚、この場合、電子透かし情報は、訂正能力の異なる複数の誤り訂正符号化方式により連接符号化されることとなる。より具体的に説明すると、図９（Ａ）に示すように、電子透かし情報は、リードソロモン符号化方式を用いて外符号化され、畳み込み符号化方式により内符号化される。

【００５２】

又、ＤＥＳ暗号化部２０９に供給された場合、ＤＥＳ暗号化部２０９は、電子透かし情報を、例えば共通鍵暗号化方式の一つであるＤＥＳ暗号化方式を用いて暗号化し、その結果

を畳み込み符号化部２１０に供給する。

【００５３】

処理３３は、ブロック分割処理である。処理３３において、ウェーブレット変換部２０６は、処理３１で入力されたデジタル画像データを複数の画素からなるブロック（縦Ｈｂ画素×横Ｗｂ画素）に分割する。

【００５４】

処理３４は、繰り返し処理である。処理３４において、処理３３にて生成された各ブロックはウェーブレット変換され、埋め込み処理される。処理３４は、処理３５～処理３９の処理を各ブロックについて繰り返し行う。

【００５５】

処理３５は、ウェーブレット変換処理である。処理３５において、ウェーブレット変換部２０６は、処理３３で生成された１つのブロックをウェーブレット変換する。そのブロックに含まれる複数のツリーは、順次電子透かし埋め込み部２０７に供給される。ここで、ツリーとは、ウェーブレット変換領域において、複数の周波数帯域（サブバンド：ＬＬ，ＬＨ３，ＨＬ３，ＨＨ３，ＬＨ２，ＨＬ２，ＨＨ２，ＬＨ１，ＨＬ１，ＨＨ１）の夫々に含まれる係数の内、同じ空間位置に対応する係数の集合のことである。あるブロックに含まれる１つのツリーの構成を図４に示す。図４において、各サブバンドの左上に示された１つ以上のウェーブレット係数がツリー４０１を構成する係数である。

【００５６】

処理３６は、繰り返し処理である。処理３６において、埋め込み部２０７は、処理３２にて生成された埋め込み情報の一部を１つのブロックに埋め込む。具体的に、埋め込み部２０７は、埋め込み情報のあるビット位置に対応する１ビットの情報を１つのブロックに対して複数個埋め込む。処理３６は、処理３７～処理３８を１ブロックに含まれる複数個のツリーに対して繰り返し行う。

【００５７】

処理３７は、埋め込み位置を特定する処理である。処理３７において、埋め込み部２０７は、１つのブロックに含まれる複数個のツリーのうち、最低域サブバンド（ＬＬ）に含まれる係数を除く係数で、各係数の絶対値がｎ（ｉ）番目に大きな係数を埋め込み対象とする。ここで、ｎ（ｉ）は乱数発生回路等により決定される自然数で、ｉは各ツリーを識別する番号である。尚、埋め込み対象となるツリーと係数とを特定する情報は、埋め込み位置情報として埋め込み後のデジタル画像データと共に外部へ出力される。

【００５８】

処理３８は、埋め込み処理である。処理３８において、埋め込み部２０７は、例えば量子化による埋め込み操作を用いて、埋め込み情報の一部（即ち、埋め込み情報のあるビット位置に対応する１ビット）を埋め込み対象となる係数の一つに埋め込む。ここで、量子化とは、連続値や離散値を他の離散値或いは異なる幅の離散値に丸める処理のことである。量子化された値を「量子化代表値」と呼び、幅、即ち隣り合う量子化代表値の間隔を「量子化ステップ」と呼ぶ。

【００５９】

具体的に埋め込み部２０７は、次の埋め込み規則により１ビットの埋め込み情報を埋め込む。

【００６０】

（１）埋め込むビットが「０」の場合、最も近い偶数（或いは奇数）インデックスとなる量子化代表値へ量子化する。

【００６１】

（２）埋め込むビットが「１」の場合、最も近い奇数（或いは偶数）インデックスとなる量子化代表値へ量子化する。

【００６２】

ここで、インデックスとは、量子化代表値を量子化ステップで割った時の商である。尚、この量子化ステップは、埋め込み対象となるツリーから埋め込み情報を抽出するために必

要な情報として、埋め込み後のデジタル画像データと共に外部へ出力される。

【００６３】

尚、処理３６～処理３８では、複数ビットからなる埋め込み情報のあるビット位置に対応する１ビットを、１つのブロックに含まれる複数個のツリーに対して埋め込む処理について説明したが、それに限るものでない。複数個の同じ埋め込み情報を埋め込むのであれば、例えば、複数個の同じ埋め込み情報の夫々を各ブロックに対して埋め込みようにしてもよい。

【００６４】

処理３９は、逆ウェーブレット変換処理である。処理３９において、埋め込み情報の一部を埋め込んだブロックは、ウェーブレット変換部２０６に供給され、そこで逆ウェーブレット変換される。これにより、電子透かし情報を不可視的に埋め込んだデジタル画像データが生成される。

【００６５】

処理４０は、出力処理である。処理４０において、入出力部２０５は、複数個の同じ埋め込み情報を埋め込んだデジタル画像データと処理３７で生成された埋め込み位置情報と処理３８で生成された量子化ステップとを一組として外部の電子機器に出力する。

【００６６】

以上のように、上述の電子透かし埋め込みアルゴリズムでは、誤り訂正符号化された複数個の同じ埋め込み情報を、視覚的に影響の少ない周波数領域に対して埋め込むことによりデジタル画像の品質を劣化させることなく、耐性の強い電子透かし情報を埋め込むことができる。

【００６７】

又、上述の電子透かし埋め込みアルゴリズムでは、誤り訂正符号化された埋め込み情報のあるビット位置にある情報を、１ブロックに含まれる複数個のツリーに対して埋め込むように処理している。これにより、各ブロックから抽出された複数ビットの情報を１単位として軟判定復号することができる。これにより、埋め込み強度を強くすることなく（即ち、量子化ステップを大きくすることなく）、デジタル画像データに電子透かし情報を埋め込むことができ、埋め込み後の電子透かし情報の耐性をより向上させることができる。

【００６８】

以下、図３を用いて説明した電子透かし埋め込みアルゴリズムを単に「ＥＣＣ複数ビット法」と呼ぶ。

【００６９】

尚、上述の電子透かし埋め込みアルゴリズムでは、処理３２において、電子透かし生成部２１３にて生成された電子透かし情報を畳み込み符号化部２１０で畳み込み符号化する処理について説明したが、軟判定復号可能な符号化方式であれば図２に示すターボ符号化部２１４を用いてターボ符号化してもよい。この場合、ターボ符号化部２１４の出力（即ち、図１４のｘ、ｙ１、ｙ２）が埋め込み情報としてデジタル画像データに埋め込まれる。ここで、上述のように電子透かし生成部２１３は、電子透かし情報をターボ符号化部２１４に供給する前に、必要に応じて誤り訂正符号化部２０８或いはＤＥＳ暗号化部２０９に供給してもよい。処理３２をこのように処理することによって、デジタル画像データに埋め込む情報の誤り訂正能力をより一層向上させることができる。尚、処理３２を上述のように処理した場合、処理３３以下の処理は、上述の電子透かし埋め込みアルゴリズムと同様に処理される。

【００７０】

又、上述の電子透かし埋め込みアルゴリズムでは、１画面のデジタル画像データを複数個のブロックに分割した後、各ブロックをウェーブレット変換したがそれに限るものではない。例えば、１画面のデジタル画像データに対してウェーブレット変換を行ってもよい。この場合、埋め込みアルゴリズムは、最低域サブバンド（ＬＬ）を複数個のウェーブレット係数を含むブロックに分割し、そのブロック毎に埋め込み情報を埋め込むように処理される。

【００７１】
（第１の実施例）
図５は、第１の実施例の電子透かし抽出装置５０１の一例を示すブロック図である。尚、抽出装置５０１は、パーソナルコンピュータ等の情報処理装置や、それに接続可能な拡張ボード、或いはプリンタ、ディスプレイ等の出力装置、ハードディスク、ＣＤ－ＲＯＭプレーヤ等の記録装置に搭載可能なユニットである。
【００７２】
図５において、５０２は電子透かし抽出装置５０１を構成する各部を協調させて制御するＣＰＵ、５０３は各種の演算に用いられるメモリ、５０４は外部から電子透かし情報の埋め込まれたデジタル画像データ、上述の埋め込み位置、上述の量子化ステップを取り込む入力部である。
【００７３】
５０５は外部の電子機器５１１へデジタル画像データから抽出した抽出情報を出力する出力部、５０６はウェーブレット変換を行うウェーブレット変換部、５０７はデジタル画像データから埋め込み情報を抽出する電子透かし抽出部である。
【００７４】
５０８は上述の軟判定ビタビ復号アルゴリズムを用いて復号処理を行うビタビ復号部、５０９は各部間を接続し、データの送受信を行う内部バス、５１０は図６にて説明する電子透かし抽出アルゴリズムを実現するＣＰＵ５０２の読み出し可能なプログラムが格納されたＲＯＭである。
【００７５】
尚、入力部５０４及び出力部５０５は、ＩｒＤＡ規格に準拠した赤外線通信用インタフェース回路、或いはＵＳＢ規格やＩＥＥＥ１３９４規格に準拠したデジタルインタフェース回路等からなり、デジタル画像データを通信するのに適した通信プロトコルを用いて外部の電子機器とデジタル画像データ等の送受信を行う。
【００７６】
次に図５の各部の動作について詳細に説明する。
【００７７】
入力部５０４には、上述のＥＣＣ複数ビット法を用いて埋め込み情報（畳み込み符号化された電子透かし情報）の各ビットを複数個を埋め込んだデジタル画像データ、埋め込み情報の各ビットがデジタル画像データのどの位置に存在するかを示す埋め込み位置情報、上述の量子化ステップが入力される。
【００７８】
ウェーブレット変換部５０６は、入力部５０４より入力されたデジタル画像データを、埋め込み装置２０１におけるウェーブレット変換と同様の方式でウェーブレット変換する。
【００７９】
抽出部５０７では、埋め込み位置情報を用いてあるブロックに含まれる複数個のツリーから複数個の埋め込み対象係数を特定する。ここで特定された係数は、各係数に対応する量子化ステップで割り算され、その結果、各係数の量子化インデックスが求められる。各量子化インデックスは、埋め込み時と同様の規則を用いて判定され、その結果、１ブロックに埋め込まれた複数個のビットが抽出される。このように、埋め込み対象係数の特定から１ビットの埋め込み情報の判定までの一連の処理を各ブロックに対して行うことにより、抽出部５０７は複数個のビットをデジタル画像データの各ブロックから抽出できる。
【００８０】
ビタビ復号部５０８では、各ブロックから抽出された複数個のビットを１単位の入力系列とし、その入力系列を上述の軟判定ビタビ復号アルゴリズムを用いて復号する。復号の結果、求められた情報系列は、抽出情報として出力部５０５より出力される。
【００８１】
図６は、図５に示した抽出装置５０１における電子透かし抽出アルゴリズムの一例を示すＮＳチャートである。以下、図６を用いて第１の実施例における電子透かし抽出アルゴリ

ズムを説明する。

【００８２】

処理６１は、入力処理である。処理６１において、入力部５０４は、上述のＥＣＣ複数ビット法を用いて埋め込み情報（畳み込み符号化された電子透かし情報）の各ビットが複数個埋め込まれたデジタル画像データ、埋め込み情報の各ビットがデジタル画像データのどの位置に存在するかを示す埋め込み位置情報、上述の量子化ステップを外部から入力する。

【００８３】

処理６２は、ブロック分割処理である。処理６２において、ウェーブレット変換部２０６は、処理６１で入力されたデジタル画像データを埋め込み装置２０１と同様に複数の画素からなるブロック（縦Ｈｂ画素×横Ｗｂ画素）に分割する。

【００８４】

処理６３は、繰り返し処理である。処理６３において、処理６２にて生成された各ブロックはウェーブレット変換され、埋め込み処理される。処理６３は、処理６４～処理６７の処理を各ブロックについて繰り返し行う。

【００８５】

処理６４は、ウェーブレット変換処理である。処理６４において、ウェーブレット変換部５０６は、処理６２にて生成された１つのブロックを埋め込み装置２０１と同様の手順でウェーブレット変換する。

【００８６】

処理６５は、繰り返し処理である。処理６５において、抽出部５０７は、１つのブロックに埋め込まれている埋め込み情報の一部を抽出する。具体的に、抽出部５０７は、埋め込み情報のあるビット位置に対応する１ビットの情報を１つのブロックから複数個抽出する。処理６５は、処理６６～処理６７を１ブロックに含まれる複数個のツリーに対して繰り返し行う。

【００８７】

処理６６は、埋め込み位置を特定する処理である。処理６６において、抽出部５０７は、上述の埋め込み位置情報を用いて各ツリーの埋め込み対象係数を特定する。具体的には、最低域サブバンド（ＬＬ）に含まれる係数を除く係数で、各係数の絶対値がｎ（ｉ）番目に大きな係数が各ツリーの埋め込み対象係数となる。

【００８８】

処理６７は、埋め込み情報を抽出する処理である。処理６７において、抽出部５０７は、上述の量子化ステップを用いて処理６６にて特定された対象係数を割り算し、各係数の量子化インデックスを求める。この量子化インデックスは、埋め込み時と同様の規則を用いて判定され、その結果、対象係数に埋め込まれた１ビットの埋め込み情報が抽出される。

【００８９】

処理６８は、軟判定ビタビ復号処理である。処理６８において、ビタビ復号部５０８は、各ブロックから抽出された複数個のビットを用いて軟判定ビタビ復号する。ここで、１つのブロックから抽出される複数個のビットは、埋め込み情報のあるビット位置に対応する１ビットの情報を示す。ビタビ復号部５０８は、これを用いて軟判定ビタビ復号を行う。具体的に、ビタビ復号部５０８は、１つ又は２つ以上のブロックから抽出された複数個のビットと所定のブランチシンボルとのユークリッド距離或いは確率を相関値として入力系列を軟判定ビタビ復号する。これにより、ビタビ復号方式の誤り訂正能力を十分に引き出すことができ、他の硬判定復号方式に比べてＳＮ比を大きく改善することができ、その結果として埋め込み情報の耐性を高めることができる。

【００９０】

処理６９は、出力処理である。処理６９において、出力部５０５は、ビタビ復号部５０８の復号結果（即ち、デジタル画像データから抽出された抽出情報）を外部の電子機器５１１或いはＣＰＵ５０２に出力する。外部の電子機器５１１或いはＣＰＵ５０２は、上述の抽出情報からデジタル画像データに埋め込まれた電子透かし情報の内容を判断し、その内

容（例えば、著作権情報、デジタル画像データの流通経路等）を表示したり、その内容に応じた制御（例えば、デジタル画像データのコピー回数を制限、デジタル画像データの入出力の制限等）を行ったりすることができる。

【００９１】

以上のように、第１の実施例では、複数個の誤り訂正符号化された電子透かし情報の埋め込まれたデジタル画像データに対して、軟判定による復号を行うことができる。これにより、埋め込み強度を強くすることなく（即ち、量子化ステップを大きくすることなく）、デジタル画像データに電子透かし情報を埋め込むことができ、電子透かし情報の耐性をより向上させることができる。

【００９２】

又、第１の実施例では、デジタル画像データに対して圧縮、切り取り、回転、拡大、縮小、色変換等の信号処理が加えられた場合でも、或いはそのデジタル画像データに攻撃が加えられた場合でも、そのデジタル画像データから正常な電子透かし情報を従来よりも高い確率で抽出することができる。

【００９３】

尚、第１の実施例では、各ブロックから抽出された複数個のビットを１単位として上述の軟判定ビタビ復号アルゴリズムで復号する手順について説明したがそれに限るものではない。軟判定復号方式による復号アルゴリズムであれば、例えばビタビシンドローム方式、ＧＭＤ（Generalized Minimum Distance）復号方式、チェイス復号方式等の他の軟判定復号方式を用いた復号アルゴリズムを実行してもよい。

【００９４】

例えば、ビタビシンドローム方式では、入力系列から誤り系列のみを取り出し、取り出した誤り系列を軟判定ビタビ復号し、受信系列と軟判定ビタビ復号した誤り系列とから送信されたデジタル画像データに埋め込まれた情報系列を判定することができる。

【００９５】

（第２の実施例）

第１の実施例では、デジタル画像データから畳み込み符号化された電子透かし情報を抽出し、その抽出結果から埋め込み前の電子透かし情報を判別する処理について説明した。

【００９６】

第２の実施例では、デジタル画像データからリードソロモン符号化された後に畳み込み符号化された電子透かし情報を抽出し、その抽出結果から埋め込み前の電子透かし情報を判別する処理について説明する。尚、第２の実施例において、デジタル画像データに埋め込まれた電子透かし情報は、埋め込み装置２０１において、訂正能力の異なる複数の誤り訂正符号化方式により連接符号化されている。より具体的に説明すると、図９（Ａ）に示すように、リードソロモン符号化方式を用いて外符号化され、畳み込み符号化方式により内符号化された電子透かし情報である。

【００９７】

図７は、第２の実施例の電子透かし抽出装置７０１の一例を示すブロック図である。尚、抽出装置７０１は、パーソナルコンピュータ等の情報処理装置や、それに接続可能な拡張ボード、或いはプリンタ、ディスプレイ等の出力装置、ハードディスク、ＣＤ－ＲＯＭプレーヤ等の記録装置に搭載可能なユニットである。

【００９８】

図７において、７０２は電子透かし抽出装置７０１を構成する各部を協調させて制御するＣＰＵ、７０３は各種の演算に用いられるメモリ、７０４は外部から電子透かし情報の埋め込まれたデジタル画像データ、上述の埋め込み位置、上述の量子化ステップを取り込む入力部である。

【００９９】

７０５は外部の電子機器７１１へデジタル画像データから抽出した抽出情報を出力する出力部、７０６はウェーブレット変換を行うウェーブレット変換部、７０７はデジタル画像データから埋め込み情報を抽出する電子透かし抽出部である。

【０１００】
７０８は上述の軟判定ビタビ復号アルゴリズムを用いて復号処理を行うビタビ復号部、７０９は各部間を接続し、データの送受信を行う内部バス、７１０は図８にて説明する電子透かし抽出アルゴリズムを実現するＣＰＵ７０２の読み出し可能なプログラムが格納されたＲＯＭである。
【０１０１】
７１２はリードソロモン符号化方式等を用いて誤り訂正符号化方式された電子透かし情報を硬判定により復号する誤り訂正符号復号部である。ここで、誤り訂正符号復号部７１２には、第１の実施例と同様の処理手順によって抽出された抽出情報がビタビ復号部７０８から供給される。誤り訂正符号復号部７１２は、この抽出情報に対して硬判定による復号を行い、その復号結果を出力部７０５から出力する。
【０１０２】
尚、入力部７０４及び出力部７０５は、ＩｒＤＡ規格に準拠した赤外線通信用インタフェース回路、或いはＵＳＢ規格やＩＥＥＥ１３９４規格に準拠したデジタルインタフェース回路等からなり、デジタル画像データを通信するのに適した通信プロトコルを用いて外部の電子機器とデジタル画像データ等の送受信を行う。
【０１０３】
図８は、図７に示した抽出装置７０１における電子透かし抽出アルゴリズムの一例を示すＮＳチャートである。以下、図８を用いて第２の実施例における電子透かし抽出アルゴリズムを説明する。
【０１０４】
図８において、処理８１～処理８８までの処理手順は夫々、図６にて説明した抽出アルゴリズムの処理６１～処理６８と同様の処理を行う。
【０１０５】
処理８９は、誤り訂正符号を復号する処理である。処理８９において、誤り訂正符号復号部７１２では、ビタビ復号部７０８から供給された抽出情報に対して硬判定によるリードソロモン復号を行う。
【０１０６】
処理９０は、出力処理である。処理９０において、出力部７０５は、誤り訂正符号復号部７１２の復号結果（即ち、デジタル画像データから抽出された抽出情報をリードソロモン復号した結果）を外部の電子機器７１１或いはＣＰＵ７０２に出力する。外部の電子機器７１１或いはＣＰＵ７０２は、復号された抽出情報からデジタル画像データに埋め込まれた電子透かし情報の内容を判断し、その内容（例えば、著作権情報、デジタル画像データの流通経路等）を表示したり、その内容に応じた制御（例えば、デジタル画像データのコピー回数を制限、デジタル画像データの入出力の制限等）を行ったりすることができる。
【０１０７】
以上のように、第２の実施例では、訂正能力の異なる複数の誤り訂正符号化方式により連接符号化された電子透かし情報を抽出することができるため、第１の実施例に比べより精度よく電子透かし情報を抽出することができる。
【０１０８】
又、第２の実施例では、埋め込み対象となるデジタルコンテンツの性質、そのデジタルコンテンツが伝送される伝送路の誤り特性、そのデジタルコンテンツに加えられる信号処理や攻撃の特性に対応させた複数の誤り訂正符号化方式を組み合わせて適用することができるため、より無駄なく正確に電子透かし情報を抽出することができる。これにより、例えば誤りがバースト的に発生した場合でもより効果的に誤りを訂正することができる。
【０１０９】
又、第２の実施例では、デジタル画像データに対して圧縮、切り取り、回転、拡大、縮小、色変換等の信号処理が加えられた場合でも、或いはそのデジタル画像データに攻撃が加えられた場合でも、そのデジタル画像データから正常な電子透かし情報を従来よりも高い確率で効果的に抽出することができる。

【０１１０】
尚、第２の実施例では、リードソロモン符号化方式を用いて外符号化し、畳み込み符号化方式を用いて内符号化した電子透かし情報を、デジタル画像データに埋め込む手順とそれに対応する抽出手順について説明したが、それに限るものではない。例えば、デジタル画像データに埋め込まれた電子透かし情報に生じる誤りを効果的に低減できるような誤り訂正符号化方式の組合せならば、硬判定可能な符号化方式を用いて外符号化し、軟判定可能な符号化方式を用いて内符号化する連接符号化方式を用いて誤り訂正符号化してもよい。
【０１１１】
（第３の実施例）
第１の実施例では、デジタル画像データから畳み込み符号化された電子透かし情報を抽出し、その抽出結果から埋め込み前の電子透かし情報を判別する処理について説明した。
【０１１２】
第３の実施例では、デジタル画像データから暗号化された後に畳み込み符号化された電子透かし情報を抽出し、その抽出結果から埋め込み前の電子透かし情報を判別する処理について説明する。
【０１１３】
図１０は、第３の実施例の電子透かし抽出装置１００１の一例を示すブロック図である。尚、抽出装置１００１は、パーソナルコンピュータ等の情報処理装置や、それに接続可能な拡張ボード、或いはプリンタ、ディスプレイ等の出力装置、ハードディスク、ＣＤ－ＲＯＭプレーヤ等の記録装置に搭載可能なユニットである。
【０１１４】
図１０において、１００２は電子透かし抽出装置１００１を構成する各部を協調させて制御するＣＰＵ、１００３は各種の演算に用いられるメモリ、１００４は外部から電子透かし情報の埋め込まれたデジタル画像データ、上述の埋め込み位置、上述の量子化ステップを取り込む入力部である。
【０１１５】
１００５は外部の電子機器１０１１へデジタル画像データから抽出した抽出情報を出力する出力部、１００６はウェーブレット変換を行うウェーブレット変換部、１００７はデジタル画像データから埋め込み情報を抽出する電子透かし抽出部である。
【０１１６】
１００８は上述の軟判定ビタビ復号アルゴリズムを用いて復号処理を行うビタビ復号部、１００９は各部間を接続し、データの送受信を行う内部バス、１０１０は図１１にて説明する電子透かし抽出アルゴリズムを実現するＣＰＵ１００２の読み出し可能なプログラムが格納されたＲＯＭである。
【０１１７】
１０１２はＤＥＳ暗号化方式を用いて暗号化された電子透かし情報を復号するＤＥＳ復号部である。ここで、ＤＥＳ復号部１０１２には、第１の実施例と同様の処理手順によって抽出された抽出情報がビタビ復号部１００８から供給される。ＤＥＳ復号部１０１２は、この抽出情報に施された暗号を特定のユーザの持つ復号鍵を用いて復号し、その復号結果を出力部１００５から出力する。
【０１１８】
尚、入力部１００４及び出力部１００５は、ＩｒＤＡ規格に準拠した赤外線通信用インタフェース回路、或いはＵＳＢ規格やＩＥＥＥ１３９４規格に準拠したデジタルインタフェース回路等からなり、デジタル画像データを通信するのに適した通信プロトコルを用いて外部の電子機器とデジタル画像データ等の送受信を行う。
【０１１９】
又、上述の復号鍵は、入力部１００４を介して外部入力するようにしても、外部からの不正な攻撃に耐えるようにＣＰＵ１００２の具備するレジスタに記憶していても、ＤＥＳ復号部１０１２の具備するメモリに記憶していてもよい。
【０１２０】

図１１は、図１０に示した抽出装置１００１における電子透かし抽出アルゴリズムの一例を示すＮＳチャートである。以下、図１１を用いて第３の実施例における電子透かし抽出アルゴリズムを説明する。

【０１２１】

図１１において、処理１１１～処理１１８までの処理手順は夫々、図６にて説明した抽出アルゴリズムの処理６１～処理６８と同様の処理を行う。

【０１２２】

処理１１９は、抽出情報を復号する処理である。処理１１９において、ＤＥＳ復号部１０１２では、ビタビ復号部１００８から供給された抽出情報に対してＤＥＳ暗号化方式に基づく復号処理を行う。ここで、ＤＥＳ復号部１０１２は、特定のユーザの持つ復号鍵によってのみ正常な復号処理を行う。

【０１２３】

処理１２０は、出力処理である。処理１２０において、出力部１００５は、ＤＥＳ復号部１０１２の復号結果（即ち、デジタル画像データから抽出された抽出情報をＤＥＳ暗号化方式に基づく復号処理を行った結果）を外部の電子機器１０１１或いはＣＰＵ１００２に出力する。外部の電子機器１０１１或いはＣＰＵ１００２は、復号された抽出情報からデジタル画像データに埋め込まれた電子透かし情報の内容を判断し、その内容（例えば、著作権情報、デジタル画像データの流通経路等）を表示したり、その内容に応じた制御（例えば、デジタル画像データのコピー回数を制限、デジタル画像データの入出力の制限等）を行ったりすることができる。

【０１２４】

以上のように、第３の実施例では、暗号化され、且つ誤り訂正符号化された電子透かし情報をデジタル画像データを抽出することができるため、その電子透かし情報の秘匿性を向上させることができる。これにより、その電子透かし情報の内容を復号鍵を持つ限られたユーザのみが確認できるようにすることもできる。

【０１２５】

又、第３の実施例では、デジタル画像データに対して圧縮、切り取り、回転、拡大、縮小、色変換等の信号処理が加えられた場合でも、或いはそのデジタル画像データに攻撃が加えられた場合でも、そのデジタル画像データから正常な暗号化電子透かし情報を従来よりも高い確率で効果的に抽出することができる。これにより、埋め込み後から抽出前までに生じた誤りによる復号不能をより高い確率で回避することができる。

【０１２６】

尚、第３の実施例では、電子透かし情報に対して施す暗号化方式として共通鍵暗号方式の一つであるＤＥＳ暗号方式を用いたが、それに限るものではない。例えば、バーナム暗号方式等の共通鍵暗号方式や、ＲＳＡ（Rivest-Shamir-Adleman）暗号方式等の公開鍵暗号方式を適用することも可能である。

【０１２７】

（第４の実施例）

第１の実施例では、デジタル画像データから畳み込み符号化された電子透かし情報を抽出し、その抽出結果から埋め込み前の電子透かし情報を判別する処理について説明した。

【０１２８】

第４の実施例では、デジタル画像データからターボ符号化された電子透かし情報を抽出し、その抽出結果から埋め込み前の電子透かし情報を判別する処理について説明する。

【０１２９】

図１２は、第４の実施例の電子透かし抽出装置１２０１の一例を示すブロック図である。尚、抽出装置１２０１は、パーソナルコンピュータ等の情報処理装置や、それに接続可能な拡張ボード、或いはプリンタ、ディスプレイ等の出力装置、ハードディスク、ＣＤ－ＲＯＭプレーヤ等の記録装置に搭載可能なユニットである。

【０１３０】

図１２において、１２０２は電子透かし抽出装置１２０１を構成する各部を協調させて制

御するＣＰＵ、１２０３は各種の演算に用いられるメモリ、１２０４は外部から電子透かし情報の埋め込まれたデジタル画像データ、上述の埋め込み位置、上述の量子化ステップを取り込む入力部である。

【０１３１】

１２０５は外部の電子機器１２１１へデジタル画像データから抽出した抽出情報を出力する出力部、１２０６はウェーブレット変換を行うウェーブレット変換部、１２０７はデジタル画像データから埋め込み情報を抽出する電子透かし抽出部。

【０１３２】

１２０８は抽出部１２０７の出力をターボ復号するターボ復号部、１２０９は各部間を接続し、データの送受信を行う内部バス、１２１０は図１３にて説明する電子透かし抽出アルゴリズムを実現するＣＰＵ１２０２の読み出し可能なプログラムが格納されたＲＯＭである。

【０１３３】

尚、入力部１２０４及び出力部１２０５は、ＩｒＤＡ規格に準拠した赤外線通信用インタフェース回路、或いはＵＳＢ規格やＩＥＥＥ１３９４規格に準拠したデジタルインタフェース回路等からなり、デジタル画像データを通信するのに適した通信プロトコルを用いて外部の電子機器とデジタル画像データ等の送受信を行う。

【０１３４】

又、ターボ復号部１２０８の構成の一例を図１４（Ｂ）に示す。ターボ復号部１２０８は、インタリーバ１４０５とデインタリーバ１４０７と複数個の軟出力復号回路１４０４、１４０６とにより構成されている。ターボ復号部１２０８は、デジタル画像データから抽出された２つの誤り訂正符号Ｙ１、Ｙ２（Ｙ１、Ｙ２は、埋め込み時のｙ１、ｙ２である。）と電子透かし情報Ｘ（Ｘは、埋め込み時のｘである。）とを軟出力復号回路１４０４、１４０６に入力し、電子透かし情報ｘを推定する。ここで、軟出力復号回路１４０６の出力は、デインタリーバ１４０７を介して軟出力復号回路１４０４にフィードバックされ、繰り返し復号される。

【０１３５】

図１３は、図１２に示した抽出装置１２０１における電子透かし抽出アルゴリズムの一例を示すＮＳチャートである。以下、図１３を用いて第４の実施例における電子透かし抽出アルゴリズムを説明する。

【０１３６】

図１３において、処理１３１～処理１３７までの処理手順は夫々、図６にて説明した抽出アルゴリズムの処理６１～処理６７と同様の処理を行う。

【０１３７】

処理１３８は、ターボ復号処理である。処理１３８において、ターボ復号部１２０８は、各ブロックから抽出された複数個のビットを用いてターボ復号する。各ブロックから抽出される複数個のビットは、誤り訂正符号ｙ１、ｙ２と電子透かし情報ｘとからなる埋め込み情報のあるビット位置に対応する１ビットの情報を示す。軟出力復号回路１４０４、１４０６は、これを用いて軟判定復号を行う。これにより、上述の軟判定ビタビ復号よりも高い誤り訂正能力により埋め込み情報に生じた誤りを訂正することができる。

【０１３８】

処理１３９は、出力処理である。処理１３９において、出力部１２０５は、ターボ復号部１２０８の復号結果を外部の電子機器１２１１或いはＣＰＵ１２０２に出力する。外部の電子機器１２１１或いはＣＰＵ１２０２は、復号された抽出情報からデジタル画像データに埋め込まれた電子透かし情報の内容を判断し、その内容（例えば、著作権情報、デジタル画像データの流通経路等）を表示したり、その内容に応じた制御（例えば、デジタル画像データのコピー回数を制限、デジタル画像データの入出力の制限等）を行ったりすることができる。

【０１３９】

以上のように、第４の実施例では、軟判定による誤り訂正の可能な符号化方式により符号

化された電子透かし情報を抽出することができるため、従来に比べより精度よく電子透かし情報を抽出することができる。

【０１４０】

又、第４の実施例では、デジタル画像データに対して圧縮、切り取り、回転、拡大、縮小、色変換等の信号処理が加えられた場合でも、或いはそのデジタル画像データに攻撃が加えられた場合でも、そのデジタル画像データから正常な電子透かし情報を従来よりも高い確率で効果的に抽出することができる。

【０１４１】

尚、第４の実施例では、単にターボ符号化された電子透かし情報をデジタル画像データから抽出するアルゴリズムについて説明したが、それに限るものではなく。第２の実施例のように、リードソロモン符号化後にターボ符号化した電子透かし情報を抽出するように構成してもよい。又、第３の実施例のように、暗号化後にターボ符号化した電子透かし情報を抽出するように構成してもよい。更に、畳み込み符号化後にターボ符号化した電子透かし情報を抽出するように構成してもよい。

【０１４２】

（他の実施例）

上述の実施例は、以下のように実現することも可能である。

【０１４３】

例えば、図３にて説明した電子透かし埋め込みアルゴリズムを実現するプログラムコードを記憶したＲＯＭ２１２を、埋め込み装置２０１のＣＰＵ２０２に供給することもできる。そして、ＣＰＵ２０２が、ＲＯＭ２１２に格納されたプログラムコードを読み出し、上述の埋め込みアルゴリズムの機能を実現するように、図２に示す埋め込み装置２０１の各処理部を動作させるようにしてもよい。

【０１４４】

この場合、ＲＯＭ２１２から読み出されたプログラムコード自体が上述した実施例の機能を実現することになり、そのプログラムコードを記憶したＲＯＭ２１２は、本発明の一部の構成要件になる。

【０１４５】

同様に、図６、８、１１、１３に示した電子透かし抽出アルゴリズムを実現するプログラムコードを記録したＲＯＭ５１０、７１０、１０１０、１２１０を、抽出装置５０１、７０１、１００１、１２０１のＣＰＵ５０２、７０２、１００２、１２０２に供給することもできる。

【０１４６】

上述のプログラムコードを供給するための記録媒体としてはＲＯＭ以外にも、例えば、フロッピディスク、ハードディスク、光ディスク、光磁気ディスク、ＣＤ－ＲＯＭ、ＣＤ－Ｒ、磁気テープ、不揮発性のメモリカード等を用いることができる。

【０１４７】

又、上述の実施例の機能を実現するソフトウェアのプログラムコードは、ＲＯＭ２１２、５１０、７１０、１０１０、１２１０に予め記録されているものでも、入出力部２０５、入力部５０４、７０４、１００４、１２０４を介して外部から供給された後、ＲＯＭ２１２、５１０、７１０、１０１０、１２１０に記録したものでもよい。

【０１４８】

又、ＣＰＵ２０２、５０２、７０２、１００２、１２０２上で稼動しているＯＳ（オペレーティングシステム）或いはアプリケーションソフト等が、ＲＯＭ２１２、５１０、７１０、１０１０、１２１０より読み出されたプログラムコードの指示に基づき、上述の実施例の処理動作と機能とを実現する場合も本発明に含まれることは言うまでもない。

【０１４９】

尚、本発明はその精神、又はその主要な特徴から逸脱することなく、様々な形で実施することができる。

【０１５０】

例えば、上述の実施例では、埋め込み装置２０１と抽出装置５０１、７０１、１００１、１２０１の夫々を別々の装置として説明したが、それらを一つの装置としてもよい。その場合、抽出装置側が抽出された電子透かし情報の内容の一部を変更し、その変更された電子透かし情報を再度埋め込み装置側で埋め込むように制御してもよい。

【０１５１】

又、上述の実施例では、デジタル画像データに埋め込む処理について説明したが、デジタル音声データ、テキストデータ、グラフィックデータ等のデジタルコンテンツに対して適用し、各デジタルコンテンツの性質に合わせて電子透かし情報の情報量と埋め込み位置と設定するようにしてもよい。

【０１５２】

従って、前述の実施例はあらゆる点おいて単なる例示に過ぎず、限定的に解釈してはならない。

【０１５３】

【発明の効果】

以上のように、本発明によれば、デジタルコンテンツに埋め込まれた電子透かし情報の耐性を高めることができる。

【図面の簡単な説明】

【図１】本実施例のビタビ復号アルゴリズムを説明する図。

【図２】本実施例の埋め込み装置の構成の一例を示すブロック図。

【図３】本実施例の電子透かし埋め込みアルゴリズムの一例を示すＮＳチャート。

【図４】１つのツリーの構成を説明する図。

【図５】第１の実施例の抽出装置の構成の一例を示すブロック図。

【図６】第１の実施例の電子透かし抽出アルゴリズムの一例を示すＮＳチャート。

【図７】第２の実施例の抽出装置の構成の一例を示すブロック図。

【図８】第２の実施例の電子透かし抽出アルゴリズムの一例を示すＮＳチャート。

【図９】第２の実施例の埋め込み手順及び抽出手順を説明する図。

【図１０】第３の実施例の抽出装置の構成の一例を示すブロック図。

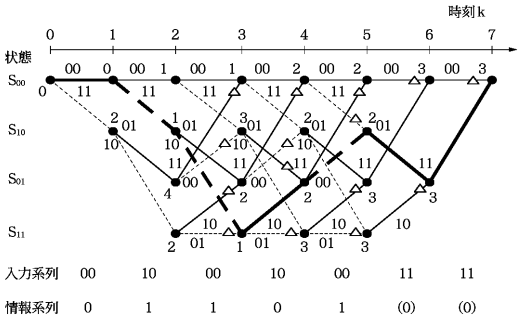
【図１１】第３の実施例の電子透かし抽出アルゴリズムの一例を示すＮＳチャート。

【図１２】第４の実施例の抽出装置の構成の一例を示すブロック図。

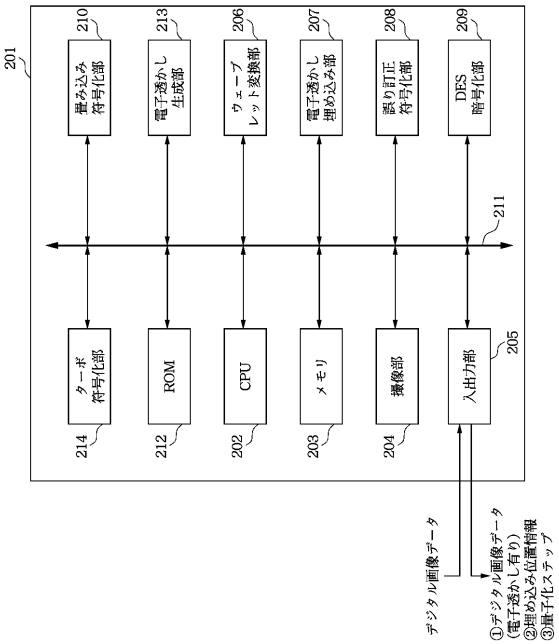
【図１３】第４の実施例の電子透かし抽出アルゴリズムの一例を示すＮＳチャート。

【図１４】ターボ符号化回路及びターボ復号回路の構成の一例を示すブロック図。

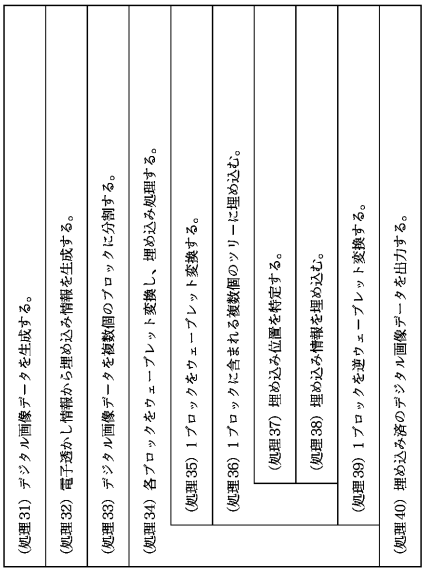
【図１】



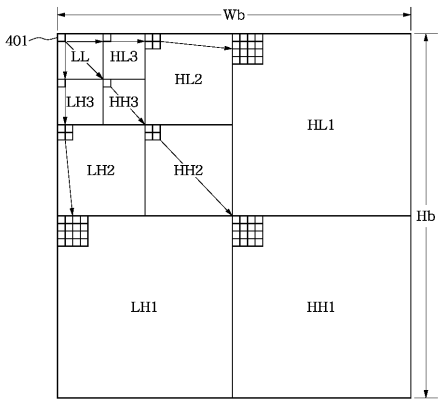
【図２】



【図３】

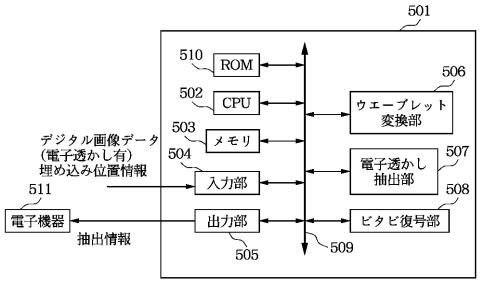


【図４】

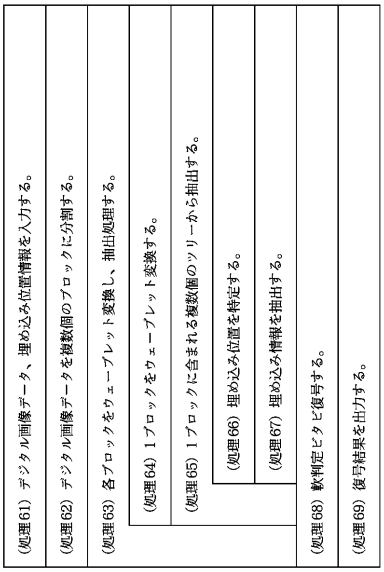


1つのツリーの構成を説明する図

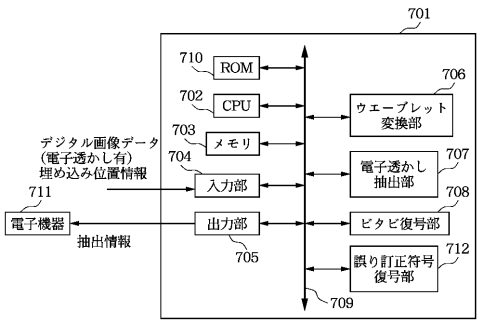
【図５】


501
510
ROM
502
CPU
503
メモリ
504
入力部
505
出力部
506
ウェーブレット
変換部
507
電子透かし
抽出部
508
ビタビ復号部
509
デジタル画像データ
(電子透かし有)
埋め込み位置情報
511
電子機器
抽出情報

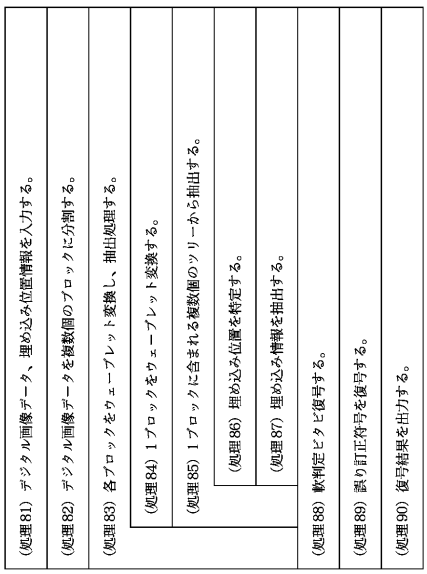
【図６】


(処理61) デジタル画像データ、埋め込み位置情報を入力する。
(処理62) デジタル画像データを複数個のブロックに分割する。
(処理63) 各ブロックをウェーブレット変換し、抽出処理する。
(処理64) 1ブロックをウェーブレット変換する。
(処理65) 1ブロックに含まれる複数個のツリーから抽出する。
(処理66) 埋め込み位置を特定する。
(処理67) 埋め込み情報を抽出する。
(処理68) 軟判定ビタビ復号する。
(処理69) 復号結果を出力する。

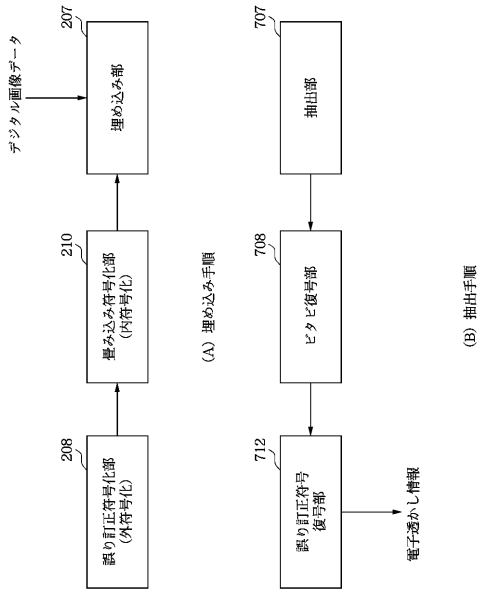
【図７】


701
710
ROM
702
CPU
703
メモリ
704
入力部
705
出力部
706
ウェーブレット
変換部
707
電子透かし
抽出部
708
ビタビ復号部
709
712
誤り訂正符号
復号部
デジタル画像データ
(電子透かし有)
埋め込み位置情報
711
電子機器
抽出情報

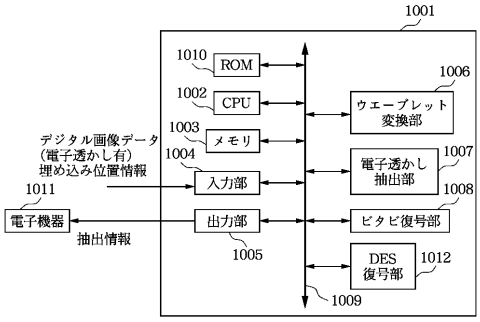
【図８】


(処理81) デジタル画像データ、埋め込み位置情報を入力する。
(処理82) デジタル画像データを複数個のブロックに分割する。
(処理83) 各ブロックをウェーブレット変換し、抽出処理する。
(処理84) 1ブロックをウェーブレット変換する。
(処理85) 1ブロックに含まれる複数個のツリーから抽出する。
(処理86) 埋め込み位置を特定する。
(処理87) 埋め込み情報を抽出する。
(処理88) 軟判定ビタビ復号する。
(処理89) 誤り訂正符号を復号する。
(処理90) 復号結果を出力する。

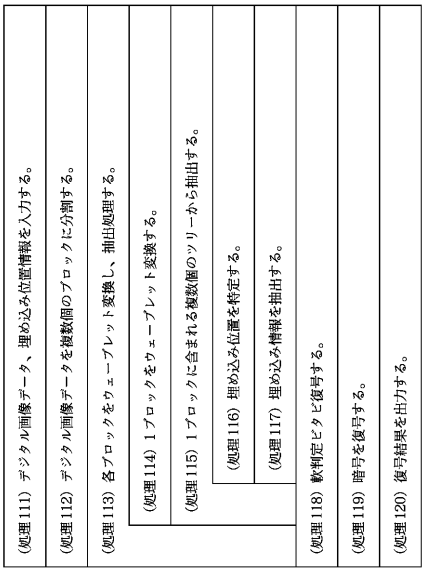
【図９】



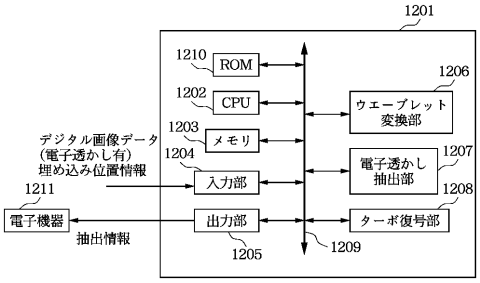
【図１０】



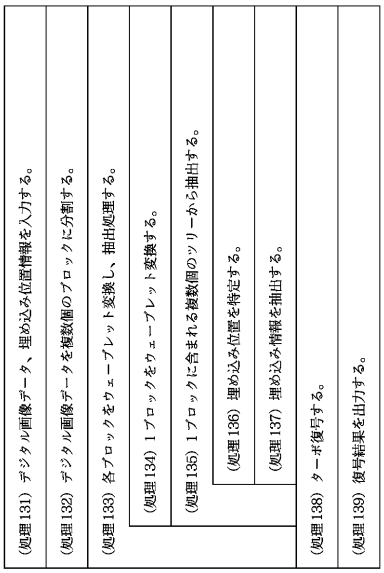
【図１１】



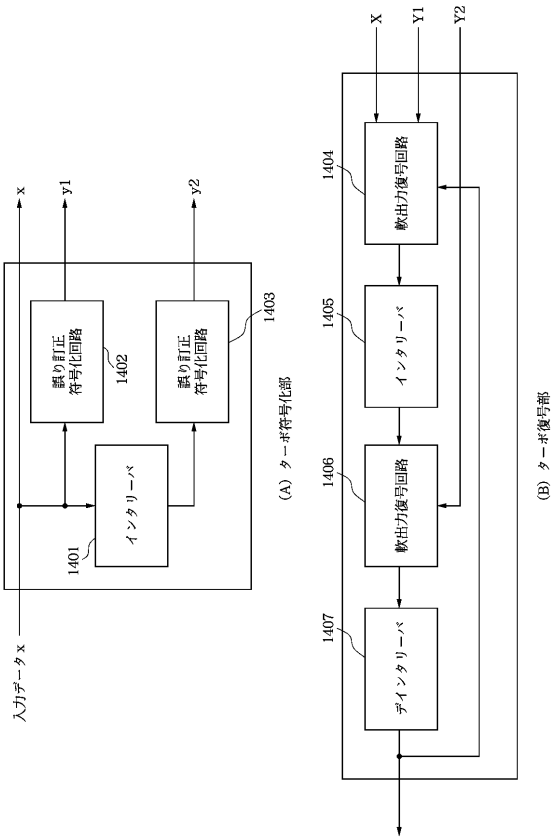
【図１２】



【図１３】


(処理131) デジタル画像データ、埋め込み位置情報を入力する。
(処理132) デジタル画像データを複数個のブロックに分割する。
(処理133) 各ブロックをウェーブレット変換し、抽出処理する。
(処理134) 1ブロックをウェーブレット変換する。
(処理135) 1ブロックに含まれる複数個のツリーから抽出する。
(処理136) 埋め込み位置を特定する。
(処理137) 埋め込み情報を抽出する。
(処理138) ターボ復号する。
(処理139) 復号結果を出力する。

【図１４】


x
y1
y2
誤り訂正符号化回路
1402
インタリーバ
1401
誤り訂正符号化回路
1403
入力データx
(A) ターボ符号化部
X
Y1
Y2
1404
軟出力復号回路
1405
インタリーバ
1406
軟出力復号回路
1407
デインタリーバ
(B) ターボ復号部

フロントページの続き

(51)Int.Cl. ＦＩ
Ｈ０４Ｎ 1/41 (2006.01) Ｈ０４Ｎ 1/41 Ｚ

(56)参考文献 特開平１０－２９０２０４（ＪＰ，Ａ）
特開平１０－３０８８６７（ＪＰ，Ａ）
特開平０８－０７９４９６（ＪＰ，Ａ）
特開平１０－２７６３２１（ＪＰ，Ａ）
特開平１０－１４５７５７（ＪＰ，Ａ）
特開２０００－１８７４４１（ＪＰ，Ａ）
特開２０００－１５１９６８（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
H03M 7/00
G09C 5/00
H03M 13/23
H03M 13/29
H04N 1/387
H04N 1/41