

(19) 日本国特許庁(JP)

(12) 特 許 公 報(B2)

(11) 特許番号

特許第4106311号
(P4106311)

(45) 発行日 平成20年6月25日(2008.6.25)

(24) 登録日 平成20年4月4日(2008.4.4)

(51) Int.Cl.

F I

H O 4 N 1/387 (2006.01)

H O 4 N 1/387

G O 6 T 1/00 (2006.01)

G O 6 T 1/00 5 O O B

H O 4 N 1/40 (2006.01)

H O 4 N 1/40 Z

H O 4 N 1/41 (2006.01)

H O 4 N 1/41 B

H O 4 N 7/30 (2006.01)

H O 4 N 7/133 Z

請求項の数 11 (全 19 頁) 最終頁に続く

(21) 出願番号 特願2003-191847 (P2003-191847)
 (22) 出願日 平成15年7月4日(2003.7.4)
 (65) 公開番号 特開2004-135265 (P2004-135265A)
 (43) 公開日 平成16年4月30日(2004.4.30)
 審査請求日 平成18年3月13日(2006.3.13)
 (31) 優先権主張番号 特願2002-232398 (P2002-232398)
 (32) 優先日 平成14年8月9日(2002.8.9)
 (33) 優先権主張国 日本国(JP)

(73) 特許権者 000005821
 松下電器産業株式会社
 大阪府門真市大字門真1006番地
 (74) 代理人 100097179
 弁理士 平野 一幸
 (72) 発明者 井上 尚
 大阪府門真市大字門真1006番地 松下
 電器産業株式会社内

審査官 橋爪 正樹

(56) 参考文献 特開2002-094769(JP, A)
)
 特開2001-203878(JP, A)
)

最終頁に続く

(54) 【発明の名称】 情報埋め込み装置、符号化装置、改ざん検出装置、その方法及び当該方法を実行するためのプログラムを記録した記録媒体

(57) 【特許請求の範囲】

【請求項1】

デジタル画像信号を周波数変換して得られる周波数係数のうち、第1の周波数領域に属する係数に基づいて特徴情報を算出する特徴情報算出部と、

デジタル画像信号を周波数変換して得られる周波数係数のうち、前記第1の周波数領域とは異なる第2の周波数領域に属する周波数係数と

デジタル画像信号を周波数変換して得られる周波数係数のうち、前記第1の周波数領域及び前記第2の周波数領域とは異なる第3の周波数領域に属する周波数係数との両方に、前記特徴情報を埋め込み、埋め込みデータを出力する情報埋め込み部とを備える情報埋め込み装置。

【請求項2】

前記第1の周波数領域は、特定の周波数成分を有する最高周波数領域よりも周波数が低い領域である請求項1記載の情報埋め込み装置。

【請求項3】

前記第2の周波数領域は、特定の周波数成分を有する最高周波数領域よりも周波数が低い領域である請求項1記載の情報埋め込み装置。

【請求項4】

前記第3の周波数領域は、特定の周波数成分を有する最低周波数領域よりも周波数が高い領域であって、前記最低周波数領域は、前記最高周波数領域よりも低い周波数成分を有する請求項2から3のいずれか記載の情報埋め込み装置。

【請求項 5】

デジタル画像信号を周波数変換して得られる周波数係数のうち、第 1 の周波数領域に属する係数に基づいて第 1 の特徴情報を算出する特徴情報算出部と、

デジタル画像信号を周波数変換して得られる周波数係数のうち、前記第 1 の周波数領域とは異なる第 2 の周波数領域に属する周波数係数に基づいて第 2 の特徴情報と

デジタル画像信号を周波数変換して得られる周波数係数のうち、前記第 1 の周波数領域及び前記第 2 の周波数領域とは異なる第 3 の周波数領域に属する周波数係数に基づいて第 3 の特徴情報と

を抽出する特徴情報抽出部と、

前記第 1 の特徴情報と前記第 2 の特徴情報と前記第 3 の特徴情報のうち、いずれか 2 つ以上の特徴情報を比較し、改ざんの有無を判定する改ざん判定部とを備える改ざん検出装置。

10

【請求項 6】

前記改ざん判定部は、前記第 1 の特徴情報と前記第 2 の特徴情報との比較結果と、前記第 1 の特徴情報と前記第 3 の特徴情報との比較結果を用いて、改ざんの有無を判定する請求項 5 記載の改ざん検出装置。

【請求項 7】

前記第 2 の周波数領域は前記第 1 の周波数領域よりも高い周波数を持ち、

前記第 3 の周波数領域は前記第 2 の周波数領域よりも高い周波数を持ち、

前記改ざん判定部は、

前記第 1 の特徴情報と前記第 2 の特徴情報とが一致し、かつ、前記第 1 の特徴情報と前記第 3 の特徴情報とが一致しないとき、改ざんはなく、かつ、画像処理が行われたものと判定する請求項 5 から 6 のいずれか記載の改ざん検出装置。

20

【請求項 8】

特徴情報算出部と、情報埋め込み部とを含む請求項 1 記載の情報埋め込み装置による情報埋め込み方法であって、

前記特徴情報算出部により、デジタル画像信号を周波数変換して得られる周波数係数のうち、第 1 の周波数領域に属する係数に基づいて特徴情報を算出するステップと、

前記情報埋め込み部により、デジタル画像信号を周波数変換して得られる周波数係数のうち、前記第 1 の周波数領域とは異なる第 2 の周波数領域に属する周波数係数と

30

デジタル画像信号を周波数変換して得られる周波数係数のうち、前記第 1 の周波数領域及び前記第 2 の周波数領域とは異なる第 3 の周波数領域に属する周波数係数との両方に、前記特徴情報を埋め込み、埋め込みデータを出力するステップとを含む情報埋め込み方法。

【請求項 9】

特徴情報算出部と、特徴情報抽出部と、改ざん判定部とを含む請求項 5 記載の改ざん検出装置による改ざん検出方法であって、

前記特徴情報算出部により、デジタル画像信号を周波数変換して得られる周波数係数のうち、第 1 の周波数領域に属する係数に基づいて第 1 の特徴情報を算出するステップと、

前記特徴情報抽出部により、デジタル画像信号を周波数変換して得られる周波数係数のうち、前記第 1 の周波数領域とは異なる第 2 の周波数領域に属する周波数係数に基づいて第 2 の特徴情報と

40

デジタル画像信号を周波数変換して得られる周波数係数のうち、前記第 1 の周波数領域及び前記第 2 の周波数領域とは異なる第 3 の周波数領域に属する周波数係数に基づいて第 3 の特徴情報と

を抽出するステップと、

前記改ざん判定部により、前記第 1 の特徴情報と前記第 2 の特徴情報と前記第 3 の特徴情報のうち、いずれか 2 つ以上の特徴情報を比較し、改ざんの有無を判定するステップとを含む改ざん検出方法。

【請求項 10】

50

特徴情報算出部と、情報埋め込み部とを含む請求項 1 記載の情報埋め込み装置における構成要素がコンピュータプログラムとして構築され、前記コンピュータプログラムが記録された記録媒体であって、

前記特徴情報算出部により、デジタル画像信号を周波数変換して得られる周波数係数のうち、第 1 の周波数領域に属する係数に基づいて特徴情報を算出するステップと、

前記情報埋め込み部により、デジタル画像信号を周波数変換して得られる周波数係数のうち、前記第 1 の周波数領域とは異なる第 2 の周波数領域に属する周波数係数と

デジタル画像信号を周波数変換して得られる周波数係数のうち、前記第 1 の周波数領域及び前記第 2 の周波数領域とは異なる第 3 の周波数領域に属する周波数係数との両方に、前記特徴情報を埋め込み、埋め込みデータを出力するステップとを含む情報埋め込みプログラムを記録した記録媒体。

10

【請求項 1 1】

特徴情報算出部と、特徴情報抽出部と、改ざん判定部とを含む請求項 5 記載の改ざん検出装置における構成要素がコンピュータプログラムとして構築され、前記コンピュータプログラムが記録された記録媒体であって、

前記特徴情報算出部により、デジタル画像信号を周波数変換して得られる周波数係数のうち、第 1 の周波数領域に属する係数に基づいて第 1 の特徴情報を算出するステップと、

前記特徴情報抽出部により、デジタル画像信号を周波数変換して得られる周波数係数のうち、前記第 1 の周波数領域とは異なる第 2 の周波数領域に属する周波数係数に基づいて第 2 の特徴情報と

20

デジタル画像信号を周波数変換して得られる周波数係数のうち、前記第 1 の周波数領域及び前記第 2 の周波数領域とは異なる第 3 の周波数領域に属する周波数係数に基づいて第 3 の特徴情報と

を抽出するステップと、

前記改ざん判定部により、前記第 1 の特徴情報と前記第 2 の特徴情報と前記第 3 の特徴情報のうち、いずれか 2 つ以上の特徴情報を比較し、改ざんの有無を判定するステップとを含む改ざん検出プログラムを記録した記録媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

30

本発明は、情報埋め込み装置、改ざん検出装置及びそれらの関連技術に関するものである。特に、本発明は、デジタル画像信号を画像圧縮する場合に、画像圧縮データが改ざんされているか否か判定するための特徴情報を電子透かしとして埋め込み、検出する技術に関する。

【0002】

【従来の技術】

近年、防犯などのセキュリティ上の観点から、監視システムの需要が拡大している。特に、監視用記録装置の分野では、ユーザーは、長時間録画ができること、画質が高いことを強く求めている。

【0003】

40

このため、デジタル化した画像データを画像圧縮し、デジタルのまま記録するデジタルディスクレコーダーが、急速に普及している。

【0004】

デジタルデータを、市販の画像処理ソフトウェアを用いて、改ざん（例えば、編集・加工など）することは、容易である。

【0005】

なお、以上の説明は、監視用記録装置やデジタルディスクレコーダーを例にしているが、本発明は、これらの用途に限定されず、画像処理を実施する技術に広く適用できる。

【0006】

デジタル画像に改ざんが加えられているか否か判定できる改ざん検出技術を確立すること

50

が求められている。従来、その対策の一つとして知られているものに電子認証技術がある。

【 0 0 0 7 】

図 1 3 は、従来の電子認証の手順の概要を示す。図 1 3 において、送信装置は、オリジナルのデジタル画像にハッシュ関数を適用しハッシュ値を得る。また、送信装置は、このハッシュ値に基づいてデジタル画像を圧縮し、ダイジェストを生成する。

【 0 0 0 8 】

次に、送信装置は、このダイジェストを、送り手の秘密鍵で暗号化する。そして、送信装置は、オリジナルのデジタル画像と暗号化されたダイジェストとの両方のデータを、ネットワークを介して、受信装置に送信する。

10

【 0 0 0 9 】

受信装置は、ネットワークを介して、この両方のデータを受信する。受信装置は、受信したデジタル画像を、ハッシュ値により圧縮し、第 1 のダイジェストを作成する。また、受信装置は、受信したダイジェストを、送り手の公開鍵により復号し、第 2 のダイジェストを作成する。

【 0 0 1 0 】

そして、受信装置は、第 1 のダイジェストと第 2 のダイジェストとを比較し、これらが、同一であれば改ざんがないと判定し、同一でなければ改ざんがあると判定する。

【 0 0 1 1 】

ところが、上述の電子認証において、送信装置は、オリジナルのデジタル画像と暗号化されたダイジェストとの、2 種類のデータを、受信装置へ送信しなければならない。

20

【 0 0 1 2 】

デジタル画像が大量に存在するときは、デジタル画像とダイジェストとの対応関係を管理するデータ管理装置が、事実上必要不可欠である。

【 0 0 1 3 】

このようなデータ管理装置に替えて、従来より、電子透かしを用いた手法が知られている。電子透かしとは、デジタル画像データの内部に、人間の目では知覚できないように、デジタル情報を埋め込む技術である。

【 0 0 1 4 】

このような電子透かし技術を用いた改ざん検出方法が提案されている。例えば、特許文献 1 (特開平 1 0 - 1 6 4 5 4 9 号公報) は、画像認証システムを開示する。

30

【 0 0 1 5 】

以下、図 1 4 を参照しながら、このシステムについて簡単に説明する。デジタルカメラなどにおいて撮影された対象の画像データ D (図 1 4 (a) 参照) は、ハッシュ値を生成するための画像領域 D 1 と、生成されたハッシュ値 H を埋め込む画像領域 D 2 とに分割される (図 1 4 (b) 参照) 。

【 0 0 1 6 】

ダイジェスト計算部 (図示せず) は、画像領域 D 1 のデータからハッシュ値 H を計算し、デジタルカメラごとに異なる秘密鍵で暗号化するなどして、画像領域 D 2 にハッシュ値 H を埋め込む。

40

【 0 0 1 7 】

一方、図 1 4 (c) に示すように、検証装置は、画像領域 D 1 のデータから第 1 のハッシュ値 H 1 を生成する。

【 0 0 1 8 】

また、検証装置は、画像領域 D 2 から埋め込まれているハッシュ値 H 2 を抽出し、抽出された第 2 のハッシュ値 H 2 を公開鍵を用いて復号する。

【 0 0 1 9 】

そして、検証装置は、第 1 のハッシュ値 H 1 と第 2 のハッシュ値 H 2 とを比較することにより、画像データ D が改ざんされているか判定する。

【 0 0 2 0 】

50

また、特許文献2（特開平11-341268号公報）の技術は、圧縮デジタル画像を部分的にデコードし、データブロックの係数に基づきハッシュ値を埋め込むか否かを判定しながら、全てのブロックからハッシュ値を計算する。

【0021】

次に、この技術は、再度、圧縮デジタル画像を部分的にデコードし、埋め込むべきブロックの係数とハッシュ値との1ビットを置き換えて透かしビットを埋め込む。

【特許文献1】

特開平10-164549号公報

【特許文献2】

特開平11-341268号公報

10

【0022】

【発明が解決しようとする課題】

しかしながら、特許文献1の技術は、画素空間において処理を行っている。このため、画素空間において、画像データが変化する処理（例えば、画像符号化等）を行うと、その処理の前後で、第1のハッシュ値H1と第2のハッシュ値H2とが、全く異なる値となってしまうから、ハッシュ値の比較による検証が不可能である。したがって、この技術は、画像圧縮されたデジタル画像の改ざん検出に適用できない。

【0023】

また、特許文献2の技術は、ハッシュ値の埋め込みのために、画像圧縮データを二度もデコードすることを前提とする。しかも、この技術では、通常用いられる量子化テーブルの変数値を、少なくとも一係数分変更しなければならない。したがって、改ざん検出のための処理が非常に複雑である。

20

【0024】

さらに、これらの従来技術では、故意の改ざん（例えば、画像の一部をすり替えたりする変更）と、悪意はないが一般的に行われる非可逆的な画像処理による変更とを、区別することができない。

【0025】

本発明は、簡易な手順で画像圧縮データの改ざん検出を可能にする技術を提供することを第1の目的とする。

【0026】

本発明は、画像符号化と親和性がある技術を提供することを第2の目的とする。

30

【0027】

本発明は、画像圧縮データを完全に復号しなくとも、改ざんを検出できる技術を提供することを第3の目的とする。

【0028】

さらに、本発明は、故意の改ざんとは異なる非可逆的な画像処理とを区別できる技術を提供することを第4の目的とする。

【0045】

第5の発明に係る改ざん検出装置は、デジタル画像信号を周波数変換して得られる周波数係数のうち、第1の周波数領域に属する係数に基づいて第1の特徴情報を算出する特徴情報算出部と、デジタル画像信号を周波数変換して得られる周波数係数のうち、第1の周波数領域とは異なる第2の周波数領域に属する周波数係数に基づいて第2の特徴情報とデジタル画像信号を周波数変換して得られる周波数係数のうち、第1の周波数領域及び第2の周波数領域とは異なる第3の周波数領域に属する周波数係数に基づいて第3の特徴情報とを抽出する特徴情報抽出部と、第1の特徴情報と第2の特徴情報と第3の特徴情報のうち、いずれか2つ以上の特徴情報を比較し、改ざんの有無を判定する改ざん判定部とを備える。

40

【0046】

この構成により、画像圧縮データの復号プロセスの途中において、特徴情報の抽出と改ざん判定とを行える。

50

【 0 0 4 7 】

第 7 の発明に係る改ざん検出装置では、第 5 から第 6 のいずれかの発明に加えて、第 2 の周波数領域は第 1 の周波数領域よりも高い周波数を持ち、第 3 の周波数領域は第 2 の周波数領域よりも高い周波数を持ち、改ざん判定部は、第 1 の特徴情報と第 2 の特徴情報とが一致し、かつ、第 1 の特徴情報と第 3 の特徴情報とが一致しないとき、改ざんはなく、かつ、画像処理が行われたものと判定する。

【 0 0 4 8 】

この構成により、第 1 の特徴情報と第 2 の特徴情報とが一致し、かつ、第 1 の特徴情報と第 3 の特徴情報とが一致しない場合があり得るため、故意の改ざんと画像処理による画像の変化とを区別できる。

【 0 0 4 9 】

【発明の実施の形態】

以下、図面を参照しながら、本発明の実施の形態を説明する。

【 0 0 5 0 】

(第 1 の実施の形態)

【 0 0 5 1 】

図 1 は、本発明の第 1 の実施の形態に係る情報埋め込み装置のブロック図である。図 1 に示すように、本形態の情報埋め込み装置は、周波数変換部 1 0 1 と量子化部 1 0 2 と特徴情報算出部 1 0 3 と情報埋め込み部 1 0 4 と画像符号化部 1 0 5 を備える。この情報埋め込み装置は、画像符号化部 1 0 5 を備えるので、符号化装置でもある。

【 0 0 5 2 】

周波数変換部 1 0 1 は、デジタル画像信号を周波数変換して周波数係数 (係数データ) を出力する。

【 0 0 5 3 】

周波数変換部 1 0 1 における周波数変換は、離散ウェーブレット変換、サブバンド分割、離散コサイン変換、またはフーリエ変換のいずれかとすることができる。

【 0 0 5 4 】

量子化部 1 0 2 は、周波数変換部 1 0 1 が出力する係数データを量子化して量子データ (量子化された周波数係数) を出力する。

【 0 0 5 5 】

量子化部 1 0 2 における量子化処理は、周波数係数を一定のビット数のデータに置き換える操作であれば、任意に選択できる。例えば、複数の周波数係数をまとめてベクトル量子化してもよい。

【 0 0 5 6 】

特徴情報算出部 1 0 3 は、量子化部 1 0 2 が出力する量子データのうち、第 1 の周波数領域に属する量子データに基づいて特徴情報を算出する。

【 0 0 5 7 】

特徴情報算出部 1 0 3 が算出する特徴情報は、基になる値を固有に表現できる情報であり、本形態では、基になる値のハッシュ値とする。

【 0 0 5 8 】

本形態では、特徴情報をハッシュ値としたが、これに限定したものではない。例えば、周波数係数値の 1 つの変更に対して、全く異なる値に変わる特徴情報であれば何でもよい。

【 0 0 5 9 】

情報埋め込み部 1 0 4 は、量子化部 1 0 2 が出力する量子データのうち、第 1 の周波数領域とは異なる第 2 の周波数領域に属する量子データに、特徴情報を埋め込み、埋め込みデータを出力する。

【 0 0 6 0 】

第 1 の周波数領域と第 2 の周波数領域は、最高周波数領域よりも周波数が低い、最低周波数領域または中低域周波数領域である。第 1 の周波数領域と第 2 の周波数領域については、後に詳述する。

10

20

30

40

50

【 0 0 6 1 】

画像符号化部 1 0 5 は、情報埋め込み部 1 0 4 が出力する埋め込みデータを符号化して画像圧縮データを生成する。

【 0 0 6 2 】

次に、図 2 を参照しながら、周波数変換として、離散ウェーブレット変換を使用する場合について説明する。図 2 (a) は、原画像を示し、図 2 (b) は、離散ウェーブレット変換後の周波数係数を示す。

【 0 0 6 3 】

図 2 (b) において、右側あるいは下側が周波数が高く、左側あるいは上側は周波数が低い。周波数成分 H H 1 は、最高周波数領域に属し、周波数成分 L L 2 は、最低周波数領域に属する。また、周波数成分 H L 2、L H 2、H H 2 は、中低周波数領域に属する。

10

【 0 0 6 4 】

なお、図 2 (b) には、2 次のウェーブレット変換による周波数係数を示しているが、3 次など他の次数を用いても良い。

【 0 0 6 5 】

上述したように、特徴情報算出部 1 0 3 は、量子化部 1 0 2 で量子化された複数の周波数成分から第 1 の周波数領域を選択する。ここで、本形態では、最低周波数領域（周波数成分 L L 2）を第 1 の周波数領域として選択する。

【 0 0 6 6 】

したがって、特徴情報算出部 1 0 3 は、周波数成分 L L 2 の係数データから所定の演算により特徴情報を算出する。

20

【 0 0 6 7 】

また本形態では、中低周波数領域（周波数成分 H L 2、L H 2、H H 2）を第 2 の周波数領域として選択し、周波数成分 H L 2、L H 2、H H 2 に、所定の規則で、特徴情報（ハッシュ値 H）を埋め込む。

【 0 0 6 8 】

ここで、低周波領域の周波数係数は、非可逆的な画像処理では変化しにくい。画像処理により変化しにくい領域に、特徴情報を埋め込んでいるので、特徴情報を欠落から保護できる。

【 0 0 6 9 】

30

次に、図 3 を参照しながら、周波数変換として、離散コサイン変換（D C T）を使用する場合について説明する。

【 0 0 7 0 】

画像の符号化方式として、J P E G や M P E G が使用される場合には、離散コサイン変換（D C T）を用いたほうがより好ましい。なぜなら、既に D C T / I D C T（I n v e r s e D C T）のための変換要素が実装済であることが多いから、既存の回路又は要素を転用でき、規模拡大を防止できるからである。

【 0 0 7 1 】

さて、図 3 (a) は、原画像を示し、図 3 (b) は、図 3 (a) に矩形で示すブロック（8 × 8 画素）が変換された後の D C T 係数を示す。

40

【 0 0 7 2 】

図 3 (b) において、横軸 i あるいは縦軸 j が「7」に近いほど周波数が高く、横軸 i あるいは縦軸 j が「0」に近いほど周波数が低い。（i，j）=（0，0）なる係数は、直流（D C）係数であり、それ以外は、全て交流（A C）係数である。係数（7，7）は、最高周波数領域に属し、係数（0，0）は、最低周波数領域に属する。

【 0 0 7 3 】

離散コサイン変換を用いた場合、全てのブロック（8 × 8 画素）において、第 1 の周波数領域として D C 係数を除く 6 3 個の A C 係数を、第 2 の周波数係数として D C 係数を、選択するとよい。あるいは、第 1 の周波数領域として D C 係数を使用し、第 2 の周波数領域として A C 係数で D C 係数の近傍にあるものを使用することもできる。

50

【 0 0 7 4 】

なお、埋め込み手法自体は、周知の技術を用いることができるが、図 4 に示すようなビットプレーンを使用することもできる。

【 0 0 7 5 】

図 4 は、本発明の第 1 の実施の形態におけるビットプレーンと特徴情報との関係図である。図 2 (b) に示した周波数係数 $L L 2$ 、 \dots 、 $H H 1$ は、図 2 (b) の紙面と平行な $x y$ 平面に対して、高さ成分 z を有する。

【 0 0 7 6 】

図 4 に示すように、この高さ成分 z が、 n (例えば、 $n = 8$ 等) ビットで表現されるとき、 $L S B$ (又は $M S B$) を 1 枚目のビットプレーン $P 1$ に割り当て、同様に、 $M S B$ (又は $L S B$) を n 枚目のビットプレーン $P n$ に割り当てる。

10

【 0 0 7 7 】

このようにして、特徴情報を、該当するビットプレーンに埋め込むことができる。そうしても、本形態に包含される。そして、ビットプレーンの使用形態は種々考えられるが、例えば、特徴情報を $M S B$ のビットプレーン (第 1 の周波数係数として使用) から求め、 $M S B$ の次のビットプレーン (第 2 の周波数係数として使用) に特徴情報を埋め込むようにするとよい。

【 0 0 7 8 】

以下、図 5 を参照して、本発明の第 1 の実施の形態に係る情報埋め込み装置の動作について説明する。図 5 は、本発明の第 1 の実施の形態に係る情報埋め込み装置のフローチャートである。

20

【 0 0 7 9 】

まず、ステップ 1 にて、周波数変換部 1 0 1 は、入力されるデジタル画像信号を周波数変換する。

【 0 0 8 0 】

次に、ステップ 2 にて、量子化部 1 0 2 は、周波数変換部 1 0 1 で出力された周波数係数を所定の規則に従う量子化ステップサイズで量子化処理を行う。

【 0 0 8 1 】

次に、ステップ 3 にて、特徴情報算出部 1 0 3 は、第 1 の周波数領域の係数に基づいて特徴情報 (ハッシュ値 H) を算出する。

30

【 0 0 8 2 】

次に、ステップ 4 にて、情報埋め込み部 1 0 4 は、特徴情報算出部 1 0 3 が算出した特徴情報 (ハッシュ値 H) を、第 1 の周波数領域と異なる領域である第 2 の周波数領域中の係数に、所定の規則で操作して埋め込む。

【 0 0 8 3 】

次に、ステップ 5 にて、画像符号化部 1 0 5 は、複数の周波数成分を表す周波数係数を符号化し画像圧縮データを生成する。

【 0 0 8 4 】

以上のように、本発明の第 1 の実施の形態に係る情報埋め込み装置は、デジタル画像信号を周波数変換した周波数係数から直接ハッシュ値を算出し、所定の規則に基づき周波数係数を操作することにより、ハッシュ値を周波数係数に埋め込む。

40

【 0 0 8 5 】

これにより、画像符号化の過程で埋め込みが可能であることから、より簡易な手順で画像圧縮データの改ざん検出を可能であり、画像符号化との親和性がある。

【 0 0 8 6 】

なお、複数の周波数成分から周波数領域を選択する手法は、本形態で説明した組み合わせ以外にも、第 1 の周波数領域と第 2 の周波数領域が相異なる組み合わせを選択すれば、これに限定されない。例えば、第 1 の周波数領域として $L L 2$ を、第 2 の周波数係数として $H H 2$ を選択するような組み合わせでもよい。つまり、複数の周波数成分から全てを選択する必要はない。

50

【 0 0 8 7 】

(第 2 の実施の形態)

【 0 0 8 8 】

図 6 は、本発明の第 2 の実施の形態に係る改ざん検出装置のブロック図である。本形態の改ざん検出装置 3 0 0 は、実施の形態 1 の情報埋め込み装置に対応するものであり、第 1 の特徴情報および第 2 の特徴情報は、基になる値のハッシュ値である。

【 0 0 8 9 】

図 6 に示すように、本形態の改ざん検出装置 3 0 0 は、画像復号部 3 0 1 と特徴情報算出部 3 0 2 と特徴情報抽出部 3 0 3 と改ざん判定部 3 0 4 を備える。

【 0 0 9 0 】

画像復号部 3 0 1 は、画像圧縮データを復号して周波数係数（量子データ）を出力する。即ち、画像復号部 3 0 1 は、周波数係数を出力できさえすれば十分であって、必ずしも、逆量子化部や可変長復号部等を備えていなくとも良い。

【 0 0 9 1 】

この周波数係数は、画像圧縮データを復号する過程で出力される量子化された周波数成分のデータである。

【 0 0 9 2 】

また、第 1 の周波数領域と第 2 の周波数領域は、最高周波数領域よりも周波数が低い領域、中低周波数領域が望ましい。

【 0 0 9 3 】

特徴情報算出部 3 0 2 は、画像復号部が出力する周波数係数（量子データ）に基づいて第 1 の特徴情報を算出し、改ざん判定部 3 0 4 へ出力する。

【 0 0 9 4 】

特徴情報抽出部 3 0 3 は、画像復号部が出力する周波数係数（量子データ）に基づいて第 2 の特徴情報を算出し、改ざん判定部 3 0 4 へ出力する。

【 0 0 9 5 】

改ざん判定部 3 0 4 は、第 1 の特徴情報と第 2 の特徴情報とを比較して改ざんの有無を判定する。より具体的には、改ざん判定部 3 0 4 は、第 1 の特徴情報と前記第 2 の特徴情報とを比較し、一致する場合には、改ざんされていないと判定する。

【 0 0 9 6 】

なお、改ざん判定部 3 0 4 の判定結果は、本形態の改ざん検出装置 3 0 0 の外部に位置する、主メモリ 4 0 0 へ格納された後、表示制御部 4 0 1 に制御されるディスプレイ 4 0 2 に表示される。

【 0 0 9 7 】

以下、図 7 を参照して、本発明の第 2 の実施の形態に係る改ざん検出装置の動作について説明する。図 7 は、本発明の第 2 の実施の形態に係る改ざん検出装置のフローチャートである。

【 0 0 9 8 】

まず、ステップ 1 1 にて、画像復号部 3 0 1 は、画像圧縮データを所定の復号化処理を行い、量子データを、特徴情報算出部 3 0 2 と特徴情報抽出部 3 0 3 とに出力する。

【 0 0 9 9 】

次に、ステップ 1 2 にて、特徴情報算出部 3 0 2 は、量子データのうち、第 1 の周波数領域に属する成分に基づいて演算し、第 1 の特徴情報を算出する。

【 0 1 0 0 】

なお、特徴情報としては、第 1 の周波数領域全体の係数データから計算したハッシュ値 H 1 とする。

【 0 1 0 1 】

次に、ステップ 1 3 にて、特徴情報抽出部 3 0 3 は、量子データのうち、第 2 の周波数領域に属する成分から、第 2 の特徴情報を抽出する。

【 0 1 0 2 】

10

20

30

40

50

次に、ステップ１４にて、改ざん判定部３０４は、特徴情報算出部３０２で算出した第１の特徴情報と、特徴情報抽出部３０３で抽出した第２の特徴情報とを、比較し、これらの特徴情報が一致する場合には、対象の画像圧縮データが改変されていないと判定する。

【０１０３】

一方、改ざん判定部３０４は、第１の特徴情報と第２の特徴情報とが一致しない場合には、画像圧縮データが改ざんされていると判定する。

【０１０４】

改ざん判定部３０４の判定結果は、メモリ４００に一旦格納された後、表示制御部４０１を経てディスプレイ４０２に表示される。

【０１０５】

以上のように、本発明の第２の実施の形態に係る改ざん検出装置によれば、画像圧縮データを所定の復号化処理する過程において出力される周波数成分から直接、改ざん判定を行うことができる。

【０１０６】

これにより、より簡易な手順で画像圧縮データの改ざん検出が可能になり、しかも、完全な復号なしに、改ざん検出をおこなうことができる。

【０１０７】

(第３の実施の形態)

【０１０８】

図８は、本発明の第３の実施の形態に係る情報埋め込み装置のブロック図である。図８に示すように、本形態の情報埋め込み装置は、周波数変換部１０１と量子化部１０２と特徴情報算出部１０３と情報埋め込み部７０１と画像符号化部１０５を備える。

【０１０９】

なお、周波数変換部１０１、量子化部１０２、特徴情報算出部１０３、及び画像符号化部１０５は、上記第１の実施の形態に係る同様の構成であるので、以下当該構成については同一の符号を付してその説明を省略し、第１の実施の形態との相違点を中心に説明する。

【０１１０】

情報埋め込み部７０１は、第２の周波数領域に属する量子データと第３の周波数領域に属する量子データとの両方に、特徴情報を埋め込み、埋め込みデータを出力する。

【０１１１】

第１の周波数領域と第２の周波数領域と第３の周波数領域は、互いに異なる領域であり、第１の周波数領域と第２の周波数領域は、低周波領域とし、第３の周波数領域は、高周波数領域とする。

【０１１２】

本形態では、図２（ｂ）において、最低周波数領域（周波数成分ＬＬ２）を第１の周波数領域として選択する。

【０１１３】

また、中低周波数領域（周波数成分ＨＬ２、ＬＨ２、ＨＨ２）を第２の周波数領域として選択し、高周波数領域（周波数成分ＨＬ１、ＬＨ１、ＨＨ１）を第３の周波数領域として選択する。

【０１１４】

ここで、高周波数領域の周波数成分ＨＬ１、ＬＨ１、ＨＨ１は、画像圧縮などの画像処理に対する耐性が低い。ここでいう耐性とは、画像処理後に情報が欠落しない度合いである。

【０１１５】

また、中低周波数領域の周波数成分ＨＬ２、ＬＨ２、ＨＨ３は、耐性が高い。さらに、最低周波数領域の周波数成分ＬＬ２は、耐性が最高である。

【０１１６】

ここで、画像データに対して、不可逆な画像処理等を施すと、第３の周波数領域（耐性が低い高周波数領域）の周波数成分は、変化することがあるが、第１の周波数領域（中低周

10

20

30

40

50

波数領域)の周波数成分及び第2の周波数領域(最低周波数領域)の周波数成分は、一般に変化しない。

【0117】

一方、画像データに対し故意の改ざん(例えば、画像中の人物像の顔を入れ替える等)を加えると、全ての周波数領域の周波数成分が変化する。即ち、このとき、第1の周波数領域の周波数成分や第2の周波数領域の周波数成分も変化する。

【0118】

以上により、耐性が高い周波数領域(第1、第2の周波数領域)において変化があれば、故意の改ざんであると判定することができる。

【0119】

また、耐性が高い周波数領域において変化がなく、耐性が低い周波数領域(第3の周波数領域)においてのみ、変化があるときは、画像データに対して、故意の改ざんがされたのではなく、不可逆な画像処理等が施されたものであると判定できる。

【0120】

よって、本形態では、次のようにする。特徴情報算出部103は、第1の周波数領域の周波数成分LL2の量子データに基づいて特徴情報(ハッシュ値H)を算出する。

【0121】

情報埋め込み部701は、この特徴情報(ハッシュ値H)を、第2の周波数領域の周波数成分(HL2、LH2、HH2)と第3の周波数領域の周波数成分(HL1、LH1、HH1)に埋め込む。埋め込みについては、第1の実施の形態と同様である。

【0122】

以下、図9を用いて、本発明の第3の実施の形態に係る情報埋め込み装置の動作について説明する。図9は、本発明の第3の実施の形態に係る情報埋め込み装置のフローチャートである。

【0123】

まず、ステップ21にて、周波数変換部101は、入力されるデジタル画像信号を周波数変換する。

【0124】

次に、ステップ22にて、量子化部102は、周波数変換部101で出力された周波数係数を所定の規則に従う量子化ステップサイズで量子化し量子データを出力する。

【0125】

次に、ステップ23にて、特徴情報算出部103は、第1の周波数領域の周波数成分LL2の量子データに基づいて特徴情報(ハッシュ値H)を算出する。

【0126】

次に、ステップ24からステップ25にて、情報埋め込み部701は、この特徴情報(ハッシュ値H)を、第2の周波数領域の周波数成分(HL2、LH2、HH2)と第3の周波数領域の周波数成分(HL1、LH1、HH1)に埋め込む。

【0127】

次に、ステップ26にて、画像符号化部105は、特徴情報が埋め込まれた複数の周波数成分に基づいて符号化処理を行い画像圧縮データを生成する。

【0128】

以上のように、本発明の第3の実施の形態に係る情報埋め込み装置は、デジタル画像信号を周波数変換した周波数係数から直接ハッシュ値を算出し、所定の規則に基づき周波数係数を操作することにより、ハッシュ値を埋め込む。

【0129】

これにより、画像符号化プロセスの途中で特徴情報を埋め込むことができるから、より簡易な手順で画像圧縮データの改ざん検出を可能であり、画像符号化との親和性が高い。

【0130】

なお、複数の周波数成分から周波数領域を選択する組み合わせは、本形態で説明した組み合わせに限定されないが、第1の周波数領域と第2の周波数領域が相異なるようにする。

10

20

30

40

50

【 0 1 3 1 】

好ましくは、第 1 の周波数領域は、最低周波数成分もしくは中低域周波数成分である。また、第 2 の周波数領域は、最低周波数成分もしくは中低域周波数成分である。さらに、第 3 の周波数領域は、最低周波数成分を除く中高域周波数成分である。

【 0 1 3 2 】

(第 4 の実施の形態)

【 0 1 3 3 】

図 1 0 は、本発明の第 4 の実施の形態に係る改ざん検出装置のブロック図である。本形態の改ざん検出装置 5 0 0 は、実施の形態 3 の情報埋め込み装置に対応するものであり、第 1 の特徴情報、第 2 の特徴情報および第 3 の特徴情報は、基になる値のハッシュ値である。

10

【 0 1 3 4 】

以下第 2 の実施の形態と同様の構成要素については同一の符号を付して説明を省略し、第 2 の実施の形態との相違点を中心に説明する。

【 0 1 3 5 】

図 1 0 に示すように、本形態の改ざん検出装置 5 0 0 は、画像復号部 3 0 1 と特徴情報算出部 3 0 2 と特徴情報抽出部 9 0 1、9 0 2 と改ざん判定部 9 0 3 を備える。

【 0 1 3 6 】

図 1 0 において、画像復号部 3 0 1 は、画像圧縮データを復号して周波数係数を出力する。

20

【 0 1 3 7 】

特徴情報算出部 3 0 2 は、画像復号部 3 0 1 が出力する周波数係数に基づいて第 1 の特徴情報を算出する。

【 0 1 3 8 】

特徴情報抽出部 9 0 1 は、画像復号部 3 0 1 が出力する周波数係数に基づいて第 2 の特徴情報を算出し、特徴情報抽出部 9 0 2 は、画像復号部が出力する周波数係数に基づいて第 3 の特徴情報を算出する。

【 0 1 3 9 】

改ざん判定部 9 0 3 は、第 1 の特徴情報と第 2 の特徴情報と第 3 の特徴情報のうち、いずれか 2 つ以上の特徴情報を比較し、改ざんの有無を判定する。

30

【 0 1 4 0 】

改ざん判定部 9 0 3 は、第 1 の特徴情報と第 2 の特徴情報とが一致する場合や、第 1 の特徴情報と第 3 の特徴情報とが一致する場合には、画像圧縮データが改ざんされていないと判定する。

【 0 1 4 1 】

第 3 の実施の形態の説明で述べたように、第 2 の周波数領域は第 1 の周波数領域よりも高い周波数を持ち、第 3 の周波数領域は第 2 の周波数領域よりも高い周波数を持つ。

【 0 1 4 2 】

そして、改ざん判定部 9 0 3 は、第 1 の特徴情報と第 2 の特徴情報とが一致し、かつ、第 1 の特徴情報と第 3 の特徴情報とが一致しないとき、改ざんはなく、かつ、画像処理が行われたものと判定する。

40

【 0 1 4 3 】

さて、本形態の改ざん検出装置は、第 3 の実施の形態における情報埋め込み装置に対応するものであるから、第 3 の実施の形態と同様に、次のように周波数領域を定める。

【 0 1 4 4 】

第 1 の周波数領域と第 2 の周波数領域と第 3 の周波数領域は、互いに異なる領域であり、第 1 の周波数領域と第 2 の周波数領域は、低周波領域とし、第 3 の周波数領域は、高周波数領域とする。

【 0 1 4 5 】

本形態では、図 2 (b) において、最低周波数領域 (周波数成分 L L 2) を第 1 の周波数

50

領域として選択する。

【 0 1 4 6 】

また、中低周波数領域（周波数成分 $H L 2$ 、 $L H 2$ 、 $H H 2$ ）を第 2 の周波数領域として選択し、高周波数領域（周波数成分 $H L 1$ 、 $L H 1$ 、 $H H 1$ ）を第 3 の周波数領域として選択する。

【 0 1 4 7 】

第 1 の特徴情報は、特徴情報算出部 3 0 2 が、第 1 の周波数領域（周波数成分 $L L 2$ ）に基づいて計算するハッシュ値 $H 1$ である。

【 0 1 4 8 】

第 2 の特徴情報は、特徴情報抽出部 9 0 1 が、第 2 の周波数領域（周波数成分 $H L 2$ 、 $L H 2$ 、 $H H 2$ ）に基づいて計算するハッシュ値 $H 2$ である。

10

【 0 1 4 9 】

第 3 の特徴情報は、特徴情報抽出部 9 0 2 が、第 3 の周波数領域（周波数成分 $H L 1$ 、 $L H 1$ 、 $H H 1$ ）に基づいて計算するハッシュ値 $H 3$ である。

【 0 1 5 0 】

次に、図 1 1 を用いて、本発明の第 4 の実施の形態に係る改ざん検出装置の動作について説明する。図 1 1 は、本発明の第 4 の実施の形態に係る改ざん検出装置のフローチャートである。

【 0 1 5 1 】

まず、ステップ 3 1 にて、画像復号部 3 0 1 は、画像圧縮データを復号し量子化された周波数係数（量子データ）を出力する。

20

【 0 1 5 2 】

次に、ステップ 3 2 にて、特徴情報算出部 3 0 2 は、量子データのうち、第 1 の周波数領域に属する成分に基づいて、第 1 の特徴情報（ハッシュ値 $H 1$ ）を算出する。

【 0 1 5 3 】

次に、ステップ 3 3 にて、特徴情報抽出部 9 0 1 は、量子データのうち、第 2 の周波数領域に属する成分に基づいて、第 2 の特徴情報（ハッシュ値 $H 2$ ）を算出する。

【 0 1 5 4 】

次に、ステップ 3 4 にて、特徴情報抽出部 9 0 2 は、量子データのうち、第 3 の周波数領域に属する成分に基づいて、第 3 の特徴情報（ハッシュ値 $H 3$ ）を算出する。

30

【 0 1 5 5 】

次に、ステップ 3 5 にて、改ざん判定部 9 0 3 は、これら 3 つの特徴情報（ハッシュ値 $H 1$ 、 $H 2$ 、 $H 3$ ）を比較し、一致する場合には、対象の画像圧縮データが改変されていないと判定する。

【 0 1 5 6 】

ここで、第 3 の実施の形態の説明において述べたように、耐性が高い周波数領域（第 1、第 2 の周波数領域）において変化があれば、故意の改ざんであると判定することができる。

【 0 1 5 7 】

耐性が高い周波数領域において変化がなく、耐性が低い周波数領域（第 3 の周波数領域）においてのみ、変化があるときは、画像データに対して、故意の改ざんがされたのではなく、不可逆な画像処理等が施されたものであると判定できる。

40

【 0 1 5 8 】

言い換えれば、

（ a ） $H 2 = H 3 = H 1$ ならば、改ざんなしと判定できる。

（ b ） $H 2 = H 1$ かつ $H 3 \neq H 1$ ならば、画像データが、故意の改ざんではなく画像処理により、変更されていると判定できる。

（ c ） $H 2 \neq H 1$ かつ $H 3 \neq H 1$ ならば、画像データが、故意に改ざんされていると判定できる。

【 0 1 5 9 】

50

以上のように、本発明の第４の実施の形態に係る改ざん検出装置は、画像の高周波成分だけでなく、非可逆的な画像処理では比較的变化しにくい低周波成分の周波数係数にもハッシュ値を埋め込む。これにより、画像の改ざん行為と非可逆的な画像処理とが、区別できる。

【０１６０】

繰り返しになるが、以下ポイントを説明する。例えば、画像の一部を改変するような改ざん行為では、低域から高域のすべての周波数係数が変化する可能性が高いため、ハッシュ値Ｈ１、Ｈ２、Ｈ３がすべて変化する。この場合は、改ざんありと判定できる。

【０１６１】

しかし、画像圧縮などの画像処理を施した場合には、高周波成分の周波数係数は変化するが、低周波成分の周波数係数は変化しにくいため、ハッシュ値Ｈ１とハッシュ値Ｈ２は同一となり、改ざんなしと判定できる。

10

【０１６２】

また、ハッシュ値Ｈ１とハッシュ値Ｈ２が一致し、ハッシュ値Ｈ１とハッシュ値Ｈ３とが異なる場合は、非可逆的な画像処理が施された可能性がより高いと予想できる。したがって、画像の改ざん行為と非可逆的な画像処理とを区別できることになる。

【０１６３】

（記録媒体）

【０１６４】

図１２に示すように、第１の実施の形態から第４の実施の形態において述べた、情報埋め込み装置、符号化装置、改ざん検出装置における各構成要素をプログラムとして構築し、コンピュータ６００にインストールする、または、ネットワーク７００を介してサーバ８００に接続された記憶装置８０１からこのプログラムを流通させることも可能である。

20

【０１６５】

このプログラムには、周波数変換部１０１、量子化部１０２、特徴情報算出部１０３、３０２、情報埋め込み部１０４、７０１、画像符号化部１０５、特徴情報抽出部３０３、９０１、９０２、改ざん判定部３０４、９０３の全部又は一部の要素が、プロセス又はプログラムモジュール等として、実装されることになる。

【０１６６】

このプログラムは、典型的には、ＣＤ－ＲＯＭやフレキシブルディスク等の記録媒体４０７に格納され、ドライブ４０８、インターフェイス４０６を介してハードディスク４０９等の記憶装置にインストールされる。

30

【０１６７】

そして、ＣＰＵ４０３が、バス４０５を介して、ＲＯＭ４０４、主メモリ４００、ハードディスク４０９等をアクセスしながら、このプログラムを実行することにより、上記実施の形態に係る情報埋め込み装置、符号化装置及び改ざん検出装置が実現されることになる。

【０１６８】

【発明の効果】

本発明によれば、画像圧縮データの処理過程において、改ざん検出用情報（ハッシュ値）を埋め込むことができるので、より簡易な手順で画像圧縮データの改ざん検出を可能にする。

40

【０１６９】

しかも、画像符号化と親和性がある。さらに、画像圧縮データの完全な復号化を必要とせずに、改ざん検出の検証をおこなうことができる。

【０１７０】

また、画像の改ざん行為と非可逆的な画像処理とを区別できる。

【図面の簡単な説明】

【図１】本発明の第１の実施の形態における情報埋め込み装置のブロック図

【図２】（ａ）本発明の離散ウェーブレット変換の説明図（原画像）

50

(b) 本発明の離散ウェーブレット変換の説明図 (周波数係数)

【図 3】(a) 本発明の離散コサイン変換の説明図 (原画像)

(b) 本発明の離散コサイン変換の説明図 (周波数係数)

【図 4】本発明における埋め込み処理の説明図 (ビットプレーン)

【図 5】本発明の第 1 の実施の形態における情報埋め込み装置のフローチャート

【図 6】本発明の第 2 の実施の形態における改ざん検出装置のブロック図

【図 7】本発明の第 2 の実施の形態における改ざん検出装置のフローチャート

【図 8】本発明の第 3 の実施の形態における情報埋め込み装置のブロック図

【図 9】本発明の第 3 の実施の形態における情報埋め込み装置のフローチャート

【図 10】本発明の第 4 の実施の形態における改ざん検出装置のブロック図

10

【図 11】本発明の第 4 の実施の形態における改ざん検出装置のフローチャート

【図 12】本発明の記録媒体を使用したシステム構成の例示図

【図 13】従来の電子認証システムの概略図

【図 14】(a) 従来の画像認証システムの動作説明図

(b) 従来の画像認証システムの動作説明図

(c) 従来の画像認証システムの動作説明図

【符号の説明】

1 0 1 周波数変換部

1 0 2 量子化部

1 0 3 特徴情報算出部

20

1 0 4、7 0 1 情報埋め込み部

1 0 5 画像符号化部

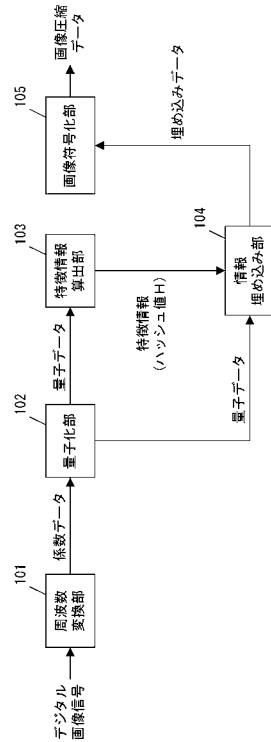
3 0 1 画像復号部

3 0 2 特徴情報算出部

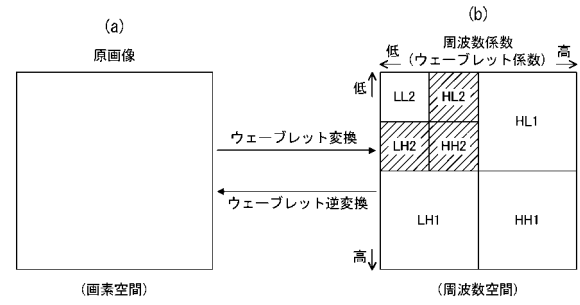
3 0 3、9 0 1、9 0 2 特徴情報抽出部

3 0 4、9 0 3 改ざん判定部

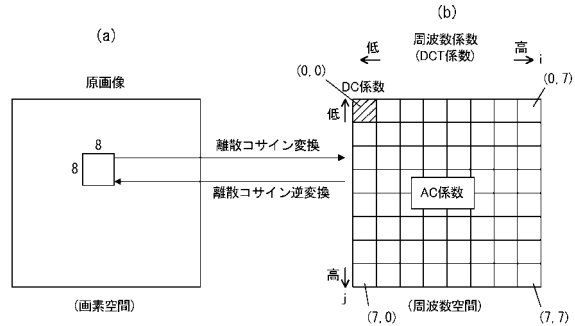
【図 1】



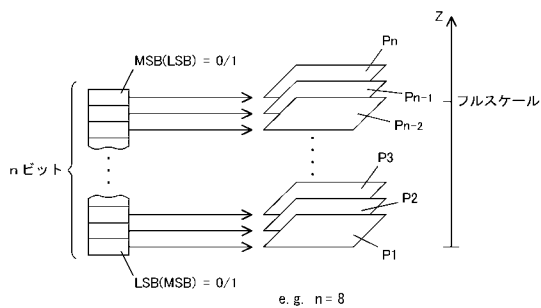
【図 2】



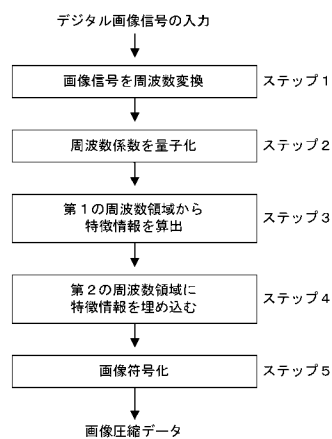
【図 3】



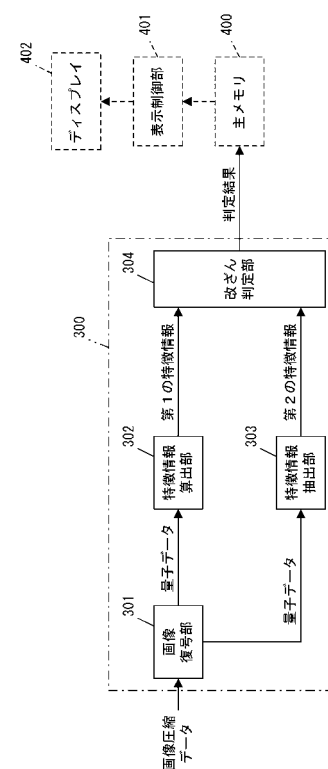
【図 4】



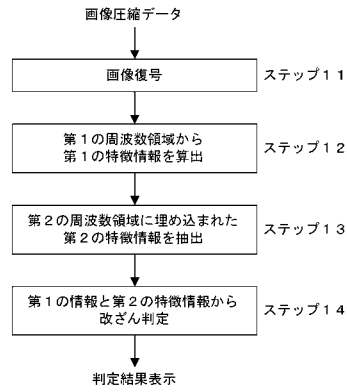
【図 5】



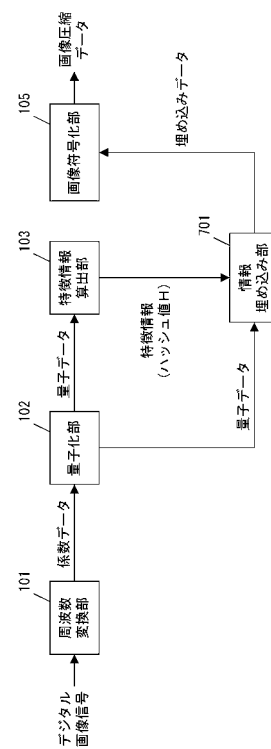
【図 6】



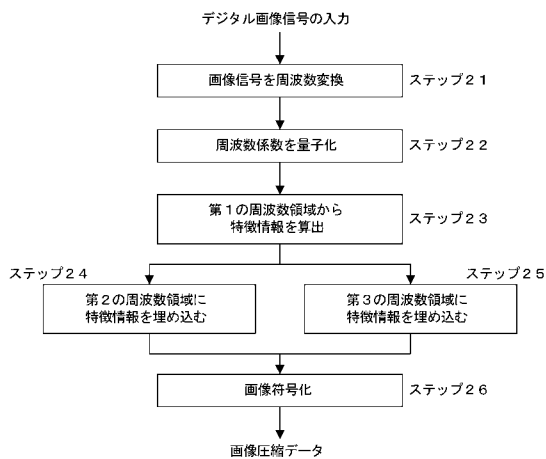
【図 7】



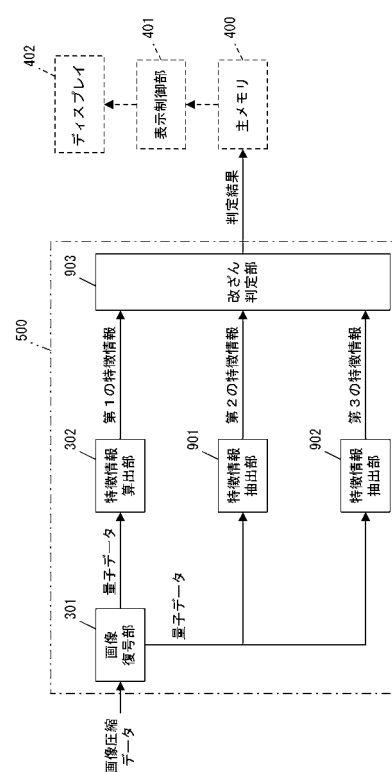
【図 8】



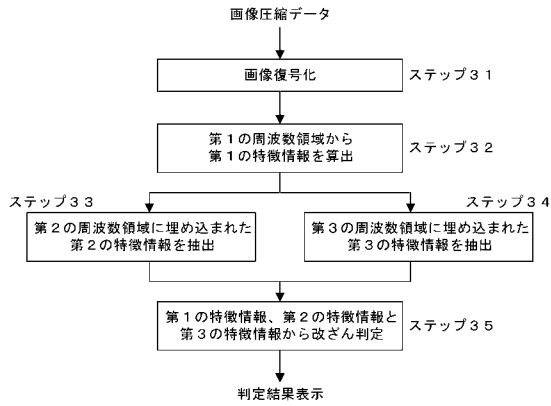
【図 9】



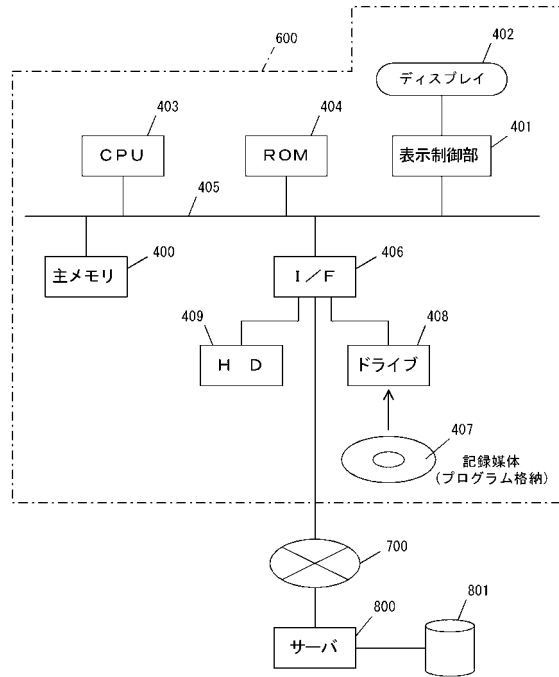
【図 10】



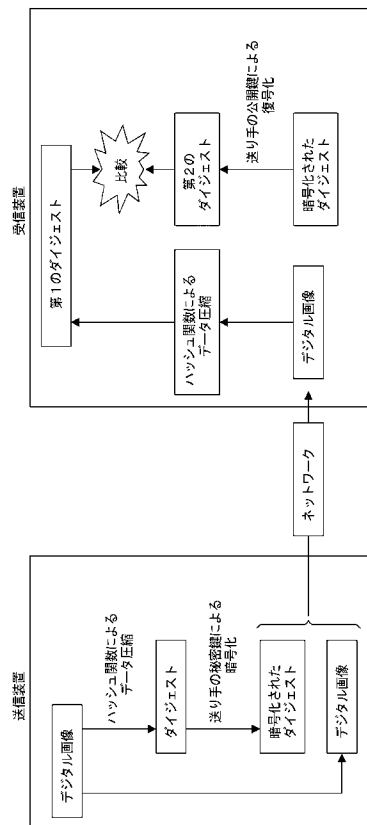
【図 1 1】



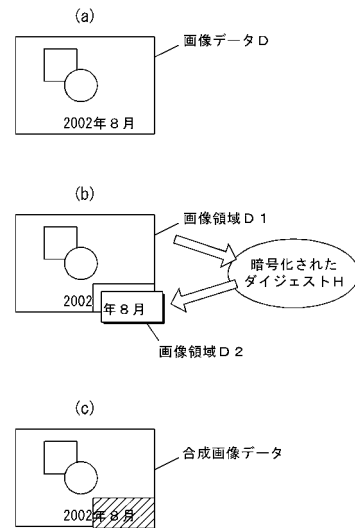
【図 1 2】



【図 1 3】



【図 1 4】



フロントページの続き

(51)Int.Cl.

F I

H 0 4 N 7/08 (2006.01)
H 0 4 N 7/081 (2006.01)
H 0 3 M 7/30 (2006.01)

H 0 4 N 7/08 Z
H 0 3 M 7/30 A

(58)調査した分野(Int.Cl. , D B 名)

H04N 1/38- 1/393

G06T 1/00

G09C 5/00