(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2004-32538
(P2004-32538A)
(43)公開日　平成16年1月29日(2004.1.29)

(51)Int.Cl.[7]		F I			テーマコード（参考）
H04N	1/44	H04N	1/44		5C075
H04L	9/16	H04N	1/41	Z	5C078
H04N	1/41	H04L	9/00	643	5J104

審査請求 未請求　請求項の数 31　ＯＬ　（全 23 頁）

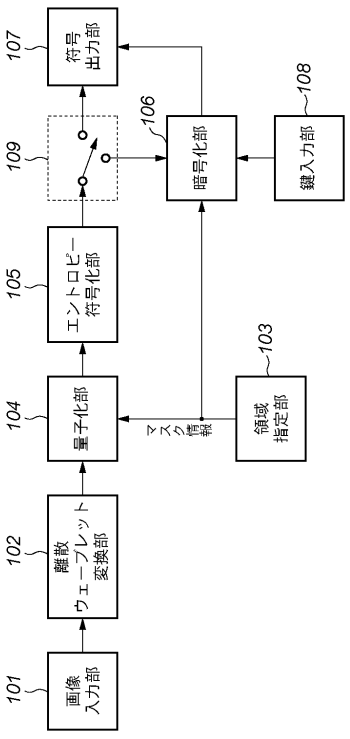
(21)出願番号　特願2002-188354(P2002-188354)
(22)出願日　平成14年6月27日(2002.6.27)

(71)出願人　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　100076428
弁理士　大塚　康徳
(74)代理人　100112508
弁理士　高柳　司郎
(74)代理人　100115071
弁理士　大塚　康弘
(74)代理人　100116894
弁理士　木村　秀二
(72)発明者　林　淳一
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

最終頁に続く

(54)【発明の名称】情報処理装置及び情報処理方法

(57)【要約】
【課題】画像データの一部領域を暗号化した場合であっても、暗号化された領域を指定する情報を必要とせず、暗号化処理及び復号処理に必要な処理量を軽減することができる情報処理装置及び情報処理方法を提供する。
【解決手段】画像入力部１０１から入力された画像データは離散ウェーブレット変換部１０２で周波数変換され、その変換係数が量子化部１０４で量子化されてビット列が生成される。次に、領域指定部１０３で指定された領域に属するビット列が所定シフト量だけビットシフトする。このビット列がエントロピー符号化部１０５で符号化される。また、この符号化データのうち指定された領域に属する符号化データが暗号化部１０６で暗号化される。
【選択図】　図１



【特許請求の範囲】
【請求項１】
画像データの所定領域に属するビット列を所定シフト量だけビットシフトするビットシフト手段と、
前記ビット列がビットシフトされた前記画像データをエントロピー符号化して符号化データを生成する符号化手段と、
前記符号化データのうち前記所定領域に属する符号化データを暗号化する暗号化手段と
を備えることを特徴とする情報処理装置。
【請求項２】
画像データの所定領域に属するビット列を所定シフト量だけビットシフトするビットシフト手段と、
ビットシフトされた前記ビット列を暗号化する暗号化手段と、
前記ビット列が暗号化された前記画像データをエントロピー符号化する符号化手段と
を備えることを特徴とする情報処理装置。
【請求項３】
画像データを周波数変換する周波数変換手段と、
周波数変換された画像データの所定周波数帯域の変換係数を量子化してビット列を生成する量子化手段と
をさらに備えることを特徴とする請求項１又は２に記載の情報処理装置。
【請求項４】
前記画像データ内の暗号化する領域を指定する指定手段をさらに備えることを特徴とする請求項１から３までのいずれか１項に記載の情報処理装置。
【請求項５】
前記シフト量は、前記画像データにおける暗号化されない領域に属するビット列がとり得る値の範囲外の量であることを特徴とする請求項１から４までのいずれか１項に記載の情報処理装置。
【請求項６】
前記周波数変換手段が、前記画像データを複数の周波数帯域成分に分解し、
分解された周波数帯域成分ごとに前記画像データの符号化及び暗号化処理を実行することを特徴とする請求項３記載の情報処理装置。
【請求項７】
前記暗号化手段が、所定の秘密鍵を用いて暗号化処理を実行することを特徴とする請求項１から６までのいずれか１項に記載の情報処理装置。
【請求項８】
前記暗号化手段が、公開鍵システムにおける所定の公開鍵を用いて暗号化処理を実行することを特徴とする請求項１から６までのいずれか１項に記載の情報処理装置。
【請求項９】
所定領域が暗号化された符号化画像データを復号する情報処理装置であって、
前記符号化画像データの前記所定領域に属する部分を暗号復号する暗号復号手段と、
前記所定領域が暗号復号された前記符号化画像データをエントロピー復号してビット列を生成する復号手段と、
前記ビット列の前記所定領域に属する部分を所定シフト量だけビットシフトするビットシフト手段と
を備えることを特徴とする情報処理装置。
【請求項１０】
所定領域が暗号化された符号化画像データを復号する情報処理装置であって、
前記符号化画像データをエントロピー復号してビット列を生成する復号手段と、
前記ビット列の前記所定領域に属する部分を暗号復号する暗号復号手段と、
暗号復号された前記ビット列のうち、前記所定領域に属するビット列を所定シフト量だけビットシフトするビットシフト手段と

を備えることを特徴とする情報処理装置。
【請求項１１】
前記ビット列を逆量子化して所定の周波数変換係数を生成する逆量子化手段と、
前記周波数変換係数を逆変換する逆変換手段と、
逆変換された複数の周波数変換係数を統合して一の画像データを復元する復元手段と
をさらに備えることを特徴とする請求項９又は１０に記載の情報処理装置。
【請求項１２】
前記シフト量は、前記符号化画像データの符号化時にビットシフトされた値と同一であることを特徴とする請求項９から１１までのいずれか１項に記載の情報処理装置。
【請求項１３】
前記復号手段が、所定の秘密鍵を用いて復号処理を実行することを特徴とする請求項９から１２までのいずれか１項に記載の情報処理装置。
【請求項１４】
前記復号手段が、公開鍵システムにおける公開鍵を用いて復号処理を実行することを特徴とする請求項９から１２までのいずれか１項に記載の情報処理装置。
【請求項１５】
画像データの所定領域に属するビット列を所定シフト量だけビットシフトするビットシフト工程と、
前記ビット列がビットシフトされた前記画像データをエントロピー符号化して符号化データを生成する符号化工程と、
前記符号化データのうち前記所定領域に属する符号化データを暗号化する暗号化工程と
を有することを特徴とする情報処理方法。
【請求項１６】
画像データの所定領域に属するビット列を所定シフト量だけビットシフトするビットシフト工程と、
ビットシフトされた前記ビット列を暗号化する暗号化工程と、
前記ビット列が暗号化された前記画像データをエントロピー符号化する符号化工程と
を有することを特徴とする情報処理方法。
【請求項１７】
画像データを周波数変換する周波数変換工程と、
周波数変換された画像データの所定周波数帯域の変換係数を量子化してビット列を生成する量子化工程と
をさらに有することを特徴とする請求項１５又は１６に記載の情報処理方法。
【請求項１８】
前記画像データ内の暗号化する領域を指定する指定工程をさらに有することを特徴とする請求項１５から１７までのいずれか１項に記載の情報処理方法。
【請求項１９】
前記シフト量は、前記画像データにおける暗号化されない領域に属するビット列がとり得る値の範囲外の量であることを特徴とする請求項１５から１８までのいずれか１項に記載の情報処理方法。
【請求項２０】
前記周波数変換工程が、前記画像データを複数の周波数帯域成分に分解し、
分解された周波数帯域成分ごとに前記画像データの符号化及び暗号化処理を実行することを特徴とする請求項１７記載の情報処理方法。
【請求項２１】
前記暗号化工程が、所定の秘密鍵を用いて暗号化処理を実行することを特徴とする請求項１５から２０までのいずれか１項に記載の情報処理方法。
【請求項２２】
前記暗号化工程が、公開鍵システムにおける所定の公開鍵を用いて暗号化処理を実行することを特徴とする請求項１５から２０までのいずれか１項に記載の情報処理方法。

【請求項２３】
所定領域が暗号化された符号化画像データを復号する情報処理方法であって、
前記符号化画像データの前記所定領域に属する部分を暗号復号する暗号復号工程と、
前記所定領域が暗号復号された前記符号化画像データをエントロピー復号してビット列を生成する復号工程と、
前記ビット列の前記所定領域に属する部分を所定シフト量だけビットシフトするビットシフト工程と
を有することを特徴とする情報処理方法。
【請求項２４】
所定領域が暗号化された符号化画像データを復号する情報処理方法であって、
前記符号化画像データをエントロピー復号してビット列を生成する復号工程と、
前記ビット列の前記所定領域に属する部分を暗号復号する暗号復号工程と、
暗号復号された前記ビット列のうち、前記所定領域に属するビット列を所定シフト量だけビットシフトするビットシフト工程と
を有することを特徴とする情報処理方法。
【請求項２５】
前記ビット列を逆量子化して所定の周波数変換係数を生成する逆量子化工程と、
前記周波数変換係数を逆変換する逆変換工程と、
逆変換された複数の周波数変換係数を統合して一の画像データを復元する復元工程と
をさらに有することを特徴とする請求項２３又は２４に記載の情報処理方法。
【請求項２６】
前記シフト量は、前記符号化画像データの符号化時にビットシフトされた値と同一であることを特徴とする請求項２３から２５までのいずれか１項に記載の情報処理方法。
【請求項２７】
前記復号工程が、所定の秘密鍵を用いて復号処理を実行することを特徴とする請求項２３から２６までのいずれか１項に記載の情報処理方法。
【請求項２８】
前記復号工程が、公開鍵システムにおける公開鍵を用いて復号処理を実行することを特徴とする請求項２３から２６までのいずれか１項に記載の情報処理方法。
【請求項２９】
画像データの所定領域に属するビット列を所定シフト量だけビットシフトするビットシフト工程と、
前記ビット列がビットシフトされた前記画像データをエントロピー符号化して符号化データを生成する符号化工程と、
前記符号化データのうち前記所定領域に属する符号化データを暗号化する暗号化工程と
をコンピュータに実行させるためのコンピュータプログラム。
【請求項３０】
コンピュータに、所定領域が暗号化された符号化画像データを復号させるためのコンピュータプログラムであって、
前記符号化画像データの前記所定領域に属する部分を暗号復号する暗号復号工程と、
前記所定領域が暗号復号された前記符号化画像データをエントロピー復号してビット列を生成する復号工程と、
前記ビット列の前記所定領域に属する部分を所定シフト量だけビットシフトするビットシフト工程と
をコンピュータに実行させるためのコンピュータプログラム。
【請求項３１】
請求項２９又は３０に記載のコンピュータプログラムを格納することを特徴とするコンピュータ読み取り可能な記録媒体。
【発明の詳細な説明】
【０００１】

【発明の属する技術分野】
本発明は、ディジタル画像データの暗号化処理又は復号処理を好適に行う情報処理装置及び情報処理方法に関する。
【０００２】
【従来の技術】
従来、画像データ等を秘匿して伝送するために、画像データ全体の暗号化やスクランブル等が行われてきた。これらの技術は、予め画像データ全体を暗号鍵を用いて暗号化し、その暗号鍵に対応する復号鍵を有するものだけが正しく復号することを可能にするものである。
【０００３】
【発明が解決しようとする課題】
しかしながら、大容量の画像データ全体を暗号化するためには多くの処理時間が必要であり、特に、処理能力の小さな情報処理装置では画像データの暗号化を実施することが困難であった。
【０００４】
この問題を解決した技術が、特公平０８－０３４５８７号公報に開示されている。特公平０８－０３４５８７号公報に開示された技術は、画像データ全体を暗号化するのではなく、画像データ中で重要と思われる領域を指定し、指定された領域にだけ暗号化処理を施すものである。このように指定領域だけを暗号化することにより、暗号化及び復号に要する処理時間を軽減することが可能である。
【０００５】
また、特公平０８－０３４５８７号公報に開示された技術によれば、画像データ中に複数の領域を指定し、指定された領域毎にそれぞれ重要度を設定し、領域毎に異なる暗号鍵で重要度の高い順に暗号化処理を行うことが可能である。さらに、上記技術によれば、画像データの暗号化の際には、「暗号化された部分領域を含む部分領域を暗号化する」ようにすることにより、重要な領域については複数回の暗号化処理を行うことによって暗号強度を大きくすることが可能になっている。
【０００６】
しかしながら、上述した特公平０８－０３４５８７号公報に開示されている技術を用いて暗号化された画像データを復号するためには、その画像データ中のどの領域が暗号化されたかという領域情報が画像データとは別に必要になる。また、画像データと領域情報の２種類の情報を復号側に伝送する必要がある。また、２種類の情報を取り扱うことは不便である。さらに、画像データ中に領域情報を含めるケースも考えられるが、どちらの場合も暗号化側から復号側に伝送するデータ全体の容量が大きくなるという問題が発生する。このように、従来の技術を用いて画像データの暗号化処理をするためには、多くの処理量が必要であり、画像データ中の重要領域だけを暗号化した場合でも、暗号化側から復号側に伝送するデータの容量が大きくなるという問題があった。
【０００７】
本発明は、このような事情を考慮してなされたものであり、画像データの一部領域を暗号化した場合であっても、暗号化された領域を指定する情報を必要とせず、暗号化処理及び復号処理に必要な処理量を軽減することができる情報処理装置及び情報処理方法を提供することを目的とする。
【０００８】
【課題を解決するための手段】
上記課題を解決するために、本発明は、画像データの所定領域に属するビット列を所定シフト量だけビットシフトするビットシフト手段と、前記ビット列がビットシフトされた前記画像データをエントロピー符号化して符号化データを生成する符号化手段と、前記符号化データのうち前記所定領域に属する符号化データを暗号化する暗号化手段とを備えることを特徴とする。
【０００９】

また、本発明は、画像データの所定領域に属するビット列を所定シフト量だけビットシフトするビットシフト手段と、ビットシフトされた前記ビット列を暗号化する暗号化手段と、前記ビット列が暗号化された前記画像データをエントロピー符号化する符号化手段とを備えることを特徴とする。

【００１０】

さらに、本発明に係る情報処理装置は、画像データを周波数変換する周波数変換手段と、周波数変換された画像データの所定周波数帯域の変換係数を量子化してビット列を生成する量子化手段とをさらに備えることを特徴とする。

【００１１】

さらにまた、本発明に係る情報処理装置は、前記画像データ内の暗号化する領域を指定する指定手段をさらに備えることを特徴とする。

【００１２】

さらにまた、本発明に係る情報処理装置は、前記シフト量は、前記画像データにおける暗号化されない領域に属するビット列がとり得る値の範囲外の量であることを特徴とする。

【００１３】

さらにまた、本発明に係る情報処理装置は、前記周波数変換手段が、前記画像データを複数の周波数帯域成分に分解し、分解された周波数帯域成分ごとに前記画像データの符号化及び暗号化処理を実行することを特徴とする。

【００１４】

さらにまた、本発明に係る情報処理装置は、前記暗号化手段が、所定の秘密鍵を用いて暗号化処理を実行することを特徴とする。

【００１５】

さらにまた、本発明に係る情報処理装置は、前記暗号化手段が、公開鍵システムにおける所定の公開鍵を用いて暗号化処理を実行することを特徴とする。

【００１６】

さらにまた、本発明は、所定領域が暗号化された符号化画像データを復号する情報処理装置であって、前記符号化画像データの前記所定領域に属する部分を暗号復号する暗号復号手段と、前記所定領域が暗号復号された前記符号化画像データをエントロピー復号してビット列を生成する復号手段と、前記ビット列の前記所定領域に属する部分を所定シフト量だけビットシフトするビットシフト手段とを備えることを特徴とする。

【００１７】

さらにまた、本発明は、所定領域が暗号化された符号化画像データを復号する情報処理装置であって、前記符号化画像データをエントロピー復号してビット列を生成する復号手段と、前記ビット列の前記所定領域に属する部分を暗号復号する暗号復号手段と、暗号復号された前記ビット列のうち、前記所定領域に属するビット列を所定シフト量だけビットシフトするビットシフト手段とを備えることを特徴とする。

【００１８】

さらにまた、本発明に係る情報処理装置は、前記ビット列を逆量子化して所定の周波数変換係数を生成する逆量子化手段と、前記周波数変換係数を逆変換する逆変換手段と、逆変換された複数の周波数変換係数を統合して一の画像データを復元する復元手段とをさらに備えることを特徴とする。

【００１９】

さらにまた、本発明に係る情報処理装置は、前記シフト量は、前記符号化画像データの符号化時にビットシフトされた値と同一であることを特徴とする。

【００２０】

さらにまた、本発明に係る情報処理装置は、前記復号手段が、所定の秘密鍵を用いて復号処理を実行することを特徴とする。

【００２１】

さらにまた、本発明に係る情報処理装置は、前記復号手段が、公開鍵システムにおける公開鍵を用いて復号処理を実行することを特徴とする。

【００２２】
【発明の実施の形態】
以下、図面を参照して、本発明の一実施形態について説明する。
【００２３】
＜第１の実施形態＞
［暗号化処理装置］
図１は、第１の実施形態による画像データを暗号化するための暗号化処理装置の構成を示すブロック図である。図１に示すように、本実施形態による暗号化処理装置は、画像入力部１０１、離散ウェーブレット変換部１０２、領域指定部１０３、量子化部１０４、エントロピー符号化部１０５、暗号化部１０６、符号出力部１０７、鍵入力部１０８及び切り替え部１０９から構成される。尚、以下で説明する暗号化処理は、ソフトウェア処理によって実現するようにしてもよい。この場合には、上記各部は、暗号化処理に必要な機能を概念的なものとして捉えたものと考慮する。
【００２４】
図２は、第１の実施形態による暗号化処理装置の各部の動作手順を説明するためのフローチャートである。まず、画像入力部１０１に対して符号化対象となる画像データを構成する画素信号がラスタースキャン順に入力される（ステップＳ１１）。次に、画像入力部１０１に入力された画像信号は、離散ウェーブレット変換部１０２に入力される。尚、以降の説明では、入力された画像データはモノクロの多値画像として処理しているが、カラー画像等の複数の色成分を符号化する場合は、ＲＧＢ各色成分、或いは輝度、色度成分等を上記単色成分として処理するようにすればよい。
【００２５】
離散ウェーブレット変換部１０２では、入力された画像信号に対して２次元離散ウェーブレット変換処理が行われ、変換係数が計算されて出力される（ステップＳ１２）。図３は、離散ウェーブレット変換部１０２の構成及び機能を説明するための概要図である。図３（ａ）は、離散ウェーブレット変換部１０２の基本構成を示した図である。離散ウェーブレット変換部１０２では、入力された画像信号はメモリ２０１に記憶され、処理部２０２により順次読み出されて離散ウェーブレット変換処理が行われ、再びメモリ２０１に書き込まれる。
【００２６】
尚、本実施形態においては、処理部２０１の構成は図３（ｂ）に示すものとする。図３（ｂ）に示すように、処理部２０１に入力された画像信号は、遅延素子２０３及びダウンサンプラ２０４、２０５の組み合わせにより、偶数アドレス及び奇数アドレスの信号に分離され、２つのフィルタｐ、ｕを用いてフィルタ処理が施される。図３（ｂ）において、符号ｓ及びｄは、それぞれ１次元の画像信号に対して１レベルの分解を行った際のローパス係数及びハイパス係数を示す。
【００２７】
ここで、ローパス係数ｓ及びハイパス係数ｄは、それぞれ次式によって計算されるものとする。
【００２８】
ｄ（ｎ）＝ｘ（２＊ｎ＋１）－ｆｌｏｏｒ（（ｘ（２＊ｎ）＋ｘ（２＊ｎ＋２））／２）　（１）
ｓ（ｎ）＝ｘ（２＊ｎ）＋ｆｌｏｏｒ（（ｄ（ｎ－１）＋ｄ（ｎ））／４）　（２）
但し、ｘ（ｎ）は、変換対象となる画像信号である。
【００２９】
以上の処理により、画像信号に対する１次元の離散ウェーブレット変換処理が行われる。２次元の離散ウェーブレット変換は、１次元の変換を画像の水平・垂直方向に対して順次行うものであり、その詳細は公知であるのでここでは説明を省略する。
【００３０】

また、図３（ｃ）は、２次元の離散ウェーブレット変換処理によって得られる２レベルの変換係数群の構成例を示すものである。離散ウェーブレット変換部１０２に入力された画像信号は、異なる周波数帯域の係数列ＨＨ１，ＨＬ１，ＬＨ１，…、ＬＬに分解される。尚、以降の説明では、これらの係数列を「サブバンド」と称す。各サブバンドの係数は、量子化部１０４に出力される。

【００３１】

一方、領域指定部１０３では、符号化対象となる画像データ内で後述する暗号化処理を施す領域が決定され、対象画像を離散ウェーブレット変換した際にどの係数が指定領域に属しているかを示すマスク情報が生成される（ステップＳ１３）。すなわち、本発明に係る暗号化処理装置は、画像データ内の暗号化する領域を指定する領域指定部１０３を有することを特徴とする。

【００３２】

図４は、領域指定部１０３で生成されるマスク情報の一例を示す図である。図４において、符号４１に示すように所定の指示入力により画像データ内に星型の領域が指定された場合、領域指定部１０３は、この指定領域を含む画像データを２次元の離散ウェーブレット変換が実行された際に、当該指定領域が各サブバンドに占める部分を計算する。符号４１に示すような指定領域を有する画像データに対して、計算されたマスク情報の例を符号４２に示す。この例においては、符号４１で示される画像データに対して２レベルの２次元離散ウェーブレット変換を施したときのマスク情報が計算される。

【００３３】

符号４２で示される離散ウェーブレット変換後の画像データにおいて星型の部分が指定領域であり、この領域内のマスク情報のビットは１、それ以外のマスク情報のビットは０となっている。このようにして得られたマスク情報は、２次元離散ウェーブレット変換による変換係数の構成と同じであるため、マスク情報内のビットを検査することで対応する位置の係数が指定領域内に属しているかどうかを識別することができる。このように生成されたマスク情報は量子化部１０４に出力される。

【００３４】

量子化部１０４では、入力した係数を所定の量子化ステップにより量子化し、その量子化値に対するインデックスを出力する（ステップＳ１４）。ここで、係数の量子化は次式により行われる。

【００３５】

$$q = sign(c) \cdot floor(abs(c) / \Delta) \quad (3)$$

$$sign(c) = 1 ; c \geqq 0 \quad (4)$$

$$sign(c) = -1 ; c < 0 \quad (5)$$

ここで、ｃは量子化対象となる係数である。また、本実施形態においては、Δの値として１を含むものとする。この場合、実際に量子化は行われない。

【００３６】

すなわち、本発明に係る暗号化処理装置は、画像データを周波数変換する離散ウェーブレット変換部１０２と、周波数変換された画像データの所定周波数帯域の変換係数を量子化してビット列を生成する量子化部とを有することを特徴とする。また、本発明に係る暗号化処理装置は、離散ウェーブレット変換部１０２が、画像データを複数の周波数帯域成分に分解し、分解された周波数帯域成分ごとに画像データの符号化及び暗号化処理を実行することを特徴とする。

【００３７】

次に、量子化部１０４は、領域指定部１０３から入力したマスク情報及びシフト量Ｂに基づいて、次式を用いて量子化インデックスを変更する（ステップＳ１５）。

$$q' = q * 2 \wedge B ; \quad m = 1 \quad (6)$$

$$q' = q ; \quad m = 0 \quad (7)$$

ここで、ｍは、当該量子化インデックスの位置におけるマスクの値である。以上の処理により、領域指定部１０３において指定された空間領域に属する量子化インデックスのみが

Ｂビット上方にシフトアップされる。

【００３８】

図５は、量子化部１０４で行われるシフトアップによる量子化インデックスの変化を説明するための図である。図５（ａ）は、あるサブバンドの量子化インデックス群を示す図である。例えば、網掛けされた部分の量子化インデックスにおけるマスクの値が「１」でシフトアップ数Ｂが４の場合、シフト後の量子化インデックスは図５（ｂ）に示すようになる。尚、このビットシフトにより生じる各空欄には図５（ｂ）に示すようにビット０が補完される。

【００３９】

尚、本実施形態においては、シフトアップ数Ｂをビットシフト処理の対象となる各量子化インデックスのビット数と同数（例えば、上記例では４ビット）にするようにする。このようにすることによって、マスク情報を復号化側に送出しなくても、後述する暗号化処理の対象となる領域とそれ以外の領域とを復号化側で容易に判断することができるとともに、正確な原画像の復元が可能になる。すなわち、本発明は、シフトアップ数Ｂが、画像データにおける暗号化されない領域に属するビット列がとり得る値の範囲外の量であることを特徴とする。

【００４０】

また、エントロピー符号化部１０５は、入力された量子化インデックスをビットプレーンに分解し、ビットプレーン単位に二値算術符号化を行ってビットストリームを出力する（ステップＳ１６）。図６は、エントロピー符号化部１０５における二値算術符号化処理動作を説明するための図である。図６に示される例では、４×４の大きさを持つサブバンド内の領域において「０」でない量子化インデックスが３個存在しており、それぞれ＋１３、－６、＋３の値を持っている。エントロピー符号化部１０５では、この領域を走査して最大値Ｍを求め、次式を用いて最大の量子化インデックスを表現するために必要なビット数Ｓを計算する。

【００４１】

Ｓ＝ｃｅｉｌ（ｌｏｇ２（ａｂｓ（Ｍ）））　　（８）

ここでｃｅｉｌ（ｘ）は、ｘ以上の整数の中で最も小さい整数値を表す。

【００４２】

図６に示す例では、最大の係数値は１３であるのでビット数Ｓは４になる。従って、シーケンス中の１６個の量子化インデックスは図６（ｂ）に示すように４つのビットプレーンを単位として処理が行われる。最初に、エントロピー符号化部１０５は、最上位ビットプレーン（ＭＳＢ）の各ビットをエントロピー符号化し、ビットストリームとして出力する。尚、本実施形態では、エントロピー符号化として二値算術符号化を用いている。

【００４３】

次に、ビットプレーンを１レベル下げ、以下同様に対象ビットプレーンが最下位ビットプレーン（ＬＳＢ）に至るまで、ビットプレーン内の各ビットを符号化し出力する。尚、上記エントロピー符号化時において、各量子化インデックスの符号は、上位から下位へのビットプレーン走査において最初（最上位）に符号化されるべき非０ビットが検出された場合、そのすぐ後に当該量子化インデックスの正負符号を示す１ビットを続けて二値算術符号化することとする。これにより、０以外の量子化インデックスの正負符号を効率良く符号化することが可能になる。

【００４４】

切り替え部１０９は、エントロピー符号化部１０５から出力されたビットストリームの暗号化部１０６への出力（以降、「暗号モード」と呼ぶ。）、又は、符号出力部１０７への出力（以降、「通常モード」と呼ぶ。）を切り替える（ステップＳ１７）。これは、暗号化処理をすべての画像データに対して実行する必要はなく、必要に応じて暗号化処理をしないことも可能にするための処理である。尚、後述する復号処理装置において、入力された符号列が暗号モードで処理されたか否かを判断して処理する必要があるため、どちらのモードが選択されたかを示すモード情報を、後述する符号出力部１０７から出力する符号

列に含めるものとする。

【００４５】

尚、本発明はこれに限定されることなく、入力されたすべての画像データに対して暗号化処理を実行するようにすれば、切り替え器１０９及びモード情報は必ずしも必要なものではない。

【００４６】

暗号化部１０６は、暗号化モードの場合、入力したビットストリームのうち領域指定部１０３で指定された領域に属するビットストリームを、鍵入力部１０８から入力された鍵を用いて暗号化処理する（ステップＳ１８）。本実施形態では、エントロピー符号化部１０５から出力されるビットストリームは、量子化インデックスをエントロピー符号化した符号列であるので、入力されたビットストリーム全てに対して暗号化処理を施す。

【００４７】

すなわち、本発明に係る暗号化処理装置は、暗号化部１０６が、所定の秘密鍵を用いて暗号化処理を実行することを特徴とする。或いは、暗号化部１０６が、公開鍵システムにおける所定の公開鍵を用いて暗号化処理を実行することを特徴とする。

【００４８】

しかしながら、本発明はこれに限定されることなく、例えば、ビットストリームに所定のヘッダが付加されたコードストリーム等が入力された場合は、ヘッダに対しては暗号化処理を実行せず、コードストリーム中のビットストリームにだけ暗号化処理を実行するようにすることも可能である。このようにすることによって、後述する復号処理装置において、暗号化部１０６で暗号化されたビットストリームが正しく復号されなかった場合にも、画像データを復号させることが可能になる。

【００４９】

また、本実施形態では、領域指定部１０３で指定されたマスク情報を入力し、マスク情報を用いて暗号化処理するビットストリームを指定しているが、本発明はこれに限定されることなく、マスク情報を入力しないようにすることも可能である。上述したように、マスク情報で示された領域は、図５（ｂ）に示すようにビットシフトが施されている。従って、所定のビットプレーン（例えば、図５に示される例の場合は上位４ビット）を暗号化処理の対象とすることにより、暗号化処理の際にマスク情報を必要としないようにすることが可能である。

【００５０】

また、暗号化処理としては、ＤＥＳやＡＥＳなどの秘密鍵方式や、ＲＳＡ等の公開鍵方式を利用することが可能である。尚、暗号化処理は公知技術であるので、詳細な説明は省略する。すなわち、本発明に係る暗号化処理装置では、画像データの所定領域に属するビット列が所定シフト量だけビットシフトされる。そして、ビット列がビットシフトされた画像データをエントロピー符号化して符号化データを生成する。さらに、符号化データのうち所定領域に属する符号化データを暗号化することを特徴とする。

【００５１】

図７は、符号出力部１０７から出力される符号列の構成を説明するための概略図である。ステップＳ１８で暗号化処理が行われた後及びステップＳ１７で通常モードの場合、ビットストリームは符号列として出力される（ステップＳ１９）。図７（ａ）は、符号列の全体の構成を示したものであり、「ＭＨ」はメインヘッダ、「ＴＨ」はタイルヘッダ、「ＢＳ」はビットストリームを示す。

【００５２】

メインヘッダＭＨは、図７（ｂ）に示すように、符号化対象となる画像サイズ７１（すなわち、水平及び垂直方向の画素数）、画像を複数の矩形領域であるタイルに分割した際のタイルサイズ７２、各色成分数を表すコンポーネント数７３、各成分の大きさ、ビット精度を表すコンポーネント情報７４から構成されている。尚、本実施形態では、画像はタイルに分割されていないので、タイルサイズと画像サイズは同じ値を取り、対象画像がモノクロの多値画像の場合、コンポーネント数は１になる。

【００５３】
次に、図７（ｃ）は、タイルヘッダＴＨの構成を示す図である。タイルヘッダＴＨは、当該タイルのビットストリーム長とヘッダ長を含めたタイル長７５、当該タイルに対する符号化パラメータ７６及び指定領域を示すマスクと当該領域に属する係数に対するビットシフト数７７から構成される。符号化パラメータには、離散ウェーブレット変換のレベル、フィルタの種別等が含まれている。
【００５４】
図７（ｄ）は、本実施形態において生成されるビットストリームの構成を示す概要図である。図７（ｄ）に示すように、ビットストリームは、解像度の小さいサブバンドを先頭として順次解像度が高くなる順番に、各サブバンド毎にまとめられて配置されている。さらに、各サブバンド内は、上位ビットプレーン（Ｂｉｔ　Ｐｌａｎｅ　Ｓ－１）から下位ビットプレーン（Ｂｉｔ　Ｐｌａｎｅ　０）に向かい、ビットプレーンを単位として符号が配列されている。
【００５５】
上述したような符号配列にすることによって、後述する階層的復号処理を行うことが可能となる。また、本実施形態においては、符号出力部１０７から出力される符号列は順次解像度が高くなるような構成としたが、本発明はこれに限定されず、ＳＮＲ、位置、コンポーネント等を優先させたような構成にすることも可能である。
【００５６】
［復号処理装置］
次に、上述した暗号化処理装置によるビットストリームを復号するための方法について説明する。図８は、第１の実施形態における復号処理装置の構成を示すブロック図である。図８に示すように、復号処理装置は、符号入力部６０１、暗号復号部６０２、エントロピー復号部６０３、逆量子化部６０４、逆離散ウェーブレット変換部６０５、画像出力部６０６、鍵入力部６０７及び切り替え部６０８から構成される。
【００５７】
図９は、第１の実施形態による復号処理装置の動作手順を説明するためのフローチャートである。まず、符号入力部６０１に符号列が入力される（ステップＳ２１）。また、符号入力部６０１は、符号列に含まれるヘッダを解析して後続の処理に必要なパラメータを抽出し必要な場合は処理の流れを制御し、あるいは後続の処理ユニットに対して該当するパラメータを送出するものである。そして、符号列に含まれるビットストリームは、切り替え部６０８に出力される。さらに、符号列の中にモード情報がある場合には、モード情報も切り替え部６０８に出力される。
【００５８】
切り替え部６０８は、入力されたモード情報に従って、入力されたビットストリームを暗号復号部６０２に出力するか、エントロピー復号部６０３に出力するかを切り替える（ステップＳ２２）。すなわち、切り替え部６０８では、入力された符号列中に含まれているモード情報を参照し、モード情報が暗号処理モードである場合、暗号復号部６０２に出力する。一方、モード情報が通常モードである場合、又はモード情報が入力されていない場合、エントロピー復号部６０３に出力するようにする。
【００５９】
暗号復号部６０２は、入力されたビットストリームを鍵入力部６０７から入力された鍵を用いて暗号復号処理する（ステップＳ２３）。すなわち、本発明に係る復号処理装置は、エントロピー復号部６０３が、所定の秘密鍵を用いて復号処理を実行することを特徴とする。或いは、エントロピー復号部６０３が、公開鍵システムにおける公開鍵を用いて復号処理を実行することを特徴とする。
【００６０】
ここで、暗号復号部６０２で暗号復号処理の対象とするのは、前述した暗号処理部１０６で暗号化処理が施された所定のビットプレーンに属するビットストリームに限定する。従って、所定のビットプレーンに含まれないビットストリームは、暗号復号部６０２では何

も処理がなされない。ここで、所定のビットプレーンは、タイルヘッダから読み出されたビットシフト数Ｂを参照し、上位Ｂビットプーレンであって、これを暗号復号処理の対象とする。このようにして処理されたビットストリームは、エントロピー復号部６０３に出力される。すなわち、本発明に係る復号処理装置では、ビットシフト数Ｂは、符号化画像データの符号化時にビットシフトされた値と同一であることを特徴とする。

【００６１】

エントロピー復号部６０３は、入力されたビットストリームをビットプレーン単位でエントロピー復号し、出力する（ステップＳ２４）。図１０は、エントロピー復号部６０３で復号されるビットストリームの様子を説明するための概要図である。図１０（ａ）は、復号対象となるサブバンドの一領域をビットプレーン単位で順次復号し、最終的に量子化インデックスを復元する流れを図示したものであり、同図の矢印の順にビットプレーンが復号処理される。そして、復元された量子化インデックスは逆量子化部６０４に出力される。

【００６２】

逆量子化部６０４は入力した量子化インデックスから、次式に基づいて離散ウェーブレット変換係数を復元する（ステップＳ２５）。

【００６３】

$$c' = \Delta * q / 2 \wedge U ; \quad q \neq 0 \qquad (11)$$

$$c' = 0 ; \quad q = 0 \qquad (12)$$

$$U = B ; \quad q \geqq 2 \wedge B \qquad (13)$$

$$U = 0 ; \quad q < 2 \wedge B \qquad (14)$$

ここで、ｑは量子化インデックス、Δは量子化ステップを示し、Δは符号化時に用いられたものと同じ値である。また、Ｂはタイルヘッダから読み出されたビットシフト数を示す。ｃ’は復元された変換係数を示し、符号化時ではｓ又はｄで表される係数の復元したものである。そして、変換係数ｃ’は後続の逆離散ウェーブレット変換部６０５に出力される。

【００６４】

図１１は、逆離散ウェーブレット変換部の構成及び処理について説明するための図である。図１１（ａ）に示すように、入力された変換係数は、まずメモリ８０１に記憶される。そして、処理部８０２は、１次元の逆離散ウェーブレット変換をメモリ８０１から順次変換係数を読み出して行うことで、２次元の逆離散ウェーブレット変換を実行する。２次元の逆離散ウェーブレット変換は、順変換と逆の手順により実行されるが、詳細は公知であるので説明を省略する。

【００６５】

また、図１１（ｂ）は、処理部８０２の処理ブロックを示したものであり、入力された変換係数はｕ及びｐの２つのフィルタ処理が施され、アップサンプリングされた後に、重ね合わされて画像信号ｘ’が出力される。これらの処理は次式により行われる。

【００６６】

$$x'(2*n) = s'(n) - floor((d'(n-1) + d'(n))/4) \qquad (15)$$

$$x'(2*n+1) = d'(n) + floor((x'(2*n) + x'(2*n+2))/2) \qquad (16)$$

ここで、（１）、（２）及び（１５）、（１６）による順方向及び逆方向の離散ウェーブレット変換は完全再構成条件を満たしているため、量子化ステップΔが１であり、エントロピー復号において全てのビットプレーンが復号されていれば、復元された画像信号ｘ’は原画像の信号ｘと一致する。

【００６７】

すなわち、本発明に係る復号処理装置は、所定領域が暗号化された符号化画像データを復号する。そのため、暗号復号部６０２は、符号化画像データの前記所定領域に属する部分を暗号復号する。次に、エントロピー復号部６０３は、所定領域が暗号復号された符号化

画像データをエントロピー復号してビット列を生成する。さらに、逆量子化部６０４は、ビット列の所定領域に属する部分を所定シフト量だけビットシフトする。また、本発明に係る復号処理装置では、逆量子化部６０４が、ビット列を逆量子化して所定の周波数変換係数を生成する。さらに、逆離散ウェーブレット変換部６０５が周波数変換係数を逆変換する。そして、逆変換された複数の周波数変換係数を統合して一の画像データが復元される。

【００６８】

以上の処理によって、元の画像データが復元されて画像出力部６０６に出力される（ステップＳ２６）。　尚、画像出力部６０６は、モニタ等の画像表示装置であってもよいし、磁気ディスク等の記憶装置であってもよい。

【００６９】

図１２は、本実施形態による復号処理装置により画像データを復元表示した際の画像データの表示形態について説明するための図である。図１１（ａ）は符号列の例を示したものである。図１２（ａ）の符号列の基本的な構成は図７の符号列に基づいている。尚、ここでは画像全体をタイルとして設定されているものとし、従って符号列中には唯一つのタイルヘッダ及びビットストリームが含まれている。ビットストリームＢＳ０には、図１２（ａ）に示すように、最も低い解像度に対応するサブバンドであるＬＬから順次解像度が高くなる順に符号が配置されており、さらに各サブバンド内は上位ビットプレーン（Ｂｉｔ　Ｐｌａｎｅ　Ｓ－１）から下位ビットプレーン（Ｂｉｔ　Ｐｌａｎｅ　０）に向かって符号が配置されている。

【００７０】

復号処理装置は、このビットストリームを順次読みこみ、各ビットプレーンに対応する符号を復号した時点で画像を表示する。図１２（ｂ）は、各サブバンドごとに表示される画像の大きさの対応と、サブバンド内の符号列を復号することによって伴われる画像データの変化を示したものである。図１２（ｂ）において、サブバンドＬＬに相当する符号列が順次読み出され、各ビットプレーンの復号処理が進むに従って画質が徐々に改善されている。

【００７１】

図１３は、本発明における画像データの復号結果を説明するための図である。図１３（ａ）に示すように、符号化時に指定領域となった星型の部分は、暗号復号部６０２において正しく復号されている場合には画像として復元される。一方、図１３（ｂ）に示すように、暗号復号部６０２において正しく復号されていない場合（鍵情報を入力しなかったり、正しい鍵情報を入力しなかった場合等）は、ノイズのように復号される。

【００７２】

上述したように、本実施形態に示したような暗号化処理装置及び復号処理装置を用いることにより、画像データ中の指定された領域に対して暗号化処理を施し、暗号化処理が施された領域は許可された利用者（正しく復号可能な鍵の所有者）だけが閲覧可能となった。また、画像データ全体を暗号化処理することに対して、暗号化及び復号に必要な演算コストを軽減することが可能となり、計算能力の小さな装置で実施する場合に有益である。さらに、暗号化処理が施された領域情報を復号処理部に送出する必要がないため、通信コストを軽減することが可能になった。

【００７３】

＜第２の実施形態＞

第１の実施形態では、暗号化処理装置においてエントロピー符号化処理の後に暗号化処理を実行し、復号処理装置において暗号復号処理の後にエントロピー復号処理を実行するようにしていた。この構成は、エントロピー符号化処理の効率を考慮したことによるものである。ここで、エントロピー符号化の効果とは、情報圧縮率のことであり、暗号化処理されたビットストリームよりも暗号化処理される前のビットストリームをエントロピー符号化処理した場合のほうが、より情報圧縮率が大きい。

【００７４】

しかしながら、本発明はこれに限定されることなく、エントロピー符号化の前に暗号化処理を実行するようにし、またエントロピー復号の後に暗号復号処理を実行するようにすることも可能である。

【００７５】

図１４は、エントロピー符号化の前に暗号化処理を実行する暗号化処理装置の構成を示すブロック図である。また、図１５は、エントロピー復号の後に暗号復号処理を実行する復号処理装置の構成を示す図である。

【００７６】

まず、図１４を用いて、第２の実施形態における暗号化処理部について説明する。図１４に示すように、本実施形態における暗号化処理装置は、図１に示した暗号化処理装置とはエントロピー符号化部１００５の位置が異なるだけである。従って、図１に示した暗号化処理装置との違いについてのみ説明する。

【００７７】

本実施形態においては、量子化部１００４からの出力が切り替え部１００９に入力され、切り替え部１００９は、暗号モードにするか通常モードにするかを切り替える。その結果、暗号モードにする場合、入力された量子化インデックスは暗号化部１００６に出力され、通常モードにする場合、入力された量子化インデックスはエントロピー符号化部１００５に出力される。

【００７８】

暗号化部１００６は、入力された量子化インデックスのうち、領域指定部１００３によって指定された領域に属する量子化インデックスに対して暗号化処理を実行する。そして、それ以外の量子化インデックスに対しては何も処理されない。このように処理された量子化インデックスはエントロピー符号化部１００５に出力される。

【００７９】

すなわち、本発明に係る暗号化処理装置は、画像データの所定領域に属するビット列を所定シフト量だけビットシフトする。次に、ビットシフトされたビット列を暗号化する。さらに、ビット列が暗号化された画像データをエントロピー符号化することを特徴とする。

【００８０】

尚、本実施形態では、暗号化部１００６に領域指定部１００３によって指定された領域情報を入力するようにしたが、本発明はこれに限定されることなく、領域情報を入力しないような構成にすることも可能である。この場合、暗号化部１００６においては、入力された量子化インデックスのうち所定値以上の値を有する量子化インデックスに対して暗号化処理を実行するようにすればよい。これは、領域指定部１００３において指定された領域が、量子化部１００４においてビットシフト処理が施されていることにより実現可能となる。

【００８１】

次に、図１５を用いて、第２の実施形態における復号処理装置について説明する。図１５に示すように、本実施形態における復号処理装置は、図８に示された復号処理装置とはエントロピー復号部の位置が異なるだけである。従って、図８に示された復号処理装置との違いについてだけ説明する。

【００８２】

本実施形態においては、符号入力部１１０１に入力された符号列は、エントロピー復号部１１０３に出力され、エントロピー復号されたビットストリームが切り替え部１１０８に入力される。そして、切り替え部１０８は、入力された符号列が暗号モードで符号化された符号列か、通常モードで符号化された符号列かをタイルヘッダ中のモード情報により判断し、ビットストリームの出力先を切り替える。その結果、暗号モードの場合、ビットストリームを暗号復号部１１０２に出力し、通常モードの場合、ビットストリームを逆量子化部１１０４に出力するようにする。

【００８３】

暗号復号部１１０２は、入力された量子化インデックスのうち、所定値以上の値を有する

量子化インデックスに対して暗号復号処理を実行する。そして、これ以外の量子化インデックスに対しては暗号復号処理を実行しない。これは、前述したように暗号処理装置において暗号処理が施されている量子化インデックスはビットシフト処理が施されていることにより実現可能となる。こうして処理された量子化インデックスは逆量子化部１１０４に出力される。

【００８４】

すなわち、本発明に係る復号処理装置は、所定領域が暗号化された符号化画像データを復号する。そのため、符号化画像データをエントロピー復号してビット列が生成される。次に、ビット列の所定領域に属する部分が暗号復号される。さらに、暗号復号されたビット列のうち、所定領域に属するビット列を所定シフト量だけビットシフトすることを特徴とする。

【００８５】

＜第３の実施形態＞

第１の実施形態では、暗号化処理装置においてはエントロピー符号化処理の後に暗号化処理が実行されていた。また、復号処理装置においては暗号復号処理の後にエントロピー復号処理が実行されていた。これは、通常の圧縮処理などで用いられるエントロピー符号化部を変更することなく利用することを考慮した上での構成である。

【００８６】

しかしながら、本発明はこれに限定されることなく、エントロピー符号化部の内部で暗号化処理を実行するようにし、また、エントロピー復号部の内部で暗号復号処理を実行するようにすることも可能である。

【００８７】

図１６は、エントロピー符号化部の内部で暗号化処理を実行する暗号化処理装置の構成を示すブロック図である。また、図１７は、エントロピー復号部の内部で暗号復号処理を実行する復号処理装置の構成を示す図である。図１６及び図１７に示すように、本実施形態における暗号化処理装置及び復号処理装置の構成は、通常の圧縮符号化及び圧縮復号等のために必要な装置の構成と同様の構成になっている。本実施形態による構成においては、暗号化処理装置におけるエントロピー符号化部１３０５及び復号処理装置におけるエントロピー復号部１４０３における処理が異なるため、これらの内部構成について説明する。

【００８８】

まず、本実施形態におけるエントロピー符号化部１３０５の詳細について説明する。図１８は、第３の実施形態におけるエントロピー符号化部１３０５の内部構成を示す図である。本実施形態では、ビットプレーン符号化部１５０１には量子化インデックスが入力され、入力された量子化インデックスがビットプレーン毎にエントロピー符号化される。尚、入力される量子化インデックスは、前段の量子化部１３０４において式（６）及び式（７）を用いて暗号化処理の対象となる領域に属する量子化インデックスがビットシフトされているものとする。

【００８９】

ビットプレーン符号化部１５０１から出力されたビット列は、切り替え部１５０２に入力され、暗号化部１５０３に出力されるか或いはパケット生成部１５０５に出力されるかが切り替えられる。切り替え部１５０２における処理の詳細は、図１に示された暗号化処理装置における切り替え部１０９での処理と同様であるので説明は省略する。

【００９０】

暗号化部１５０３では、入力されたビット列が鍵入力部１５０４から入力された鍵情報を用いて暗号化処理される。暗号化処理されたビット列は、パケット生成部１５０５に出力される。暗号化部１５０３における処理の詳細は、図１で示された暗号化処理装置における暗号化部１０６での処理と同様であるので説明は省略する。

【００９１】

パケット生成部１５０５では、入力されたビット列がパケット単位に分割され、各パケットには該パケットを特定する属性情報がヘッダとして付加され、ヘッダが付加されたパケ

ット列が出力される。ここで、属性情報には、パケットが属するレイヤー、コンポーネント、コードブロック及びサブバンドに関する情報等が含まれる。

【００９２】

図１９は、第３の実施形態におけるエントロピー復号部の内部構成を示す図である。本実施形態では、パケット結合部１６０１にパケット列が入力され、入力されたパケット列がビット列に結合される。

【００９３】

パケット結合部１６０１から出力されたビット列は、切り替え部１６０２に入力され、切り替え部１６０２において暗号復号部１６０５に出力されるか、ビットプレーン復号部１６０３に出力されるかが切り替えられる。尚、切り替え部１６０２における処理の詳細は、図８の切り替え部６０８における処理と同様であるので説明は省略する。

【００９４】

また、暗号復号部１６０５では、入力されたビット列が鍵入力部１６０４からあらかじめ入力された鍵情報を用いて暗号復号処理される。暗号復号処理されたビット列は、ビットプレーン復号部１６０３に出力される。暗号復号部１６０５における処理の詳細は、図８で示される暗号復号部６０２における処理と同様であるので説明は省略する。

【００９５】

ビットプレーン復号部１６０３では、入力されたビット列がビットプレーン毎にエントロピー復号され、量子化インデックスが生成され、出力される。

【００９６】

以上説明したような構成をすることにより、暗号化部１５０３及び暗号復号部１６０５においてヘッダ部分とそれ以外の部分を区別することなく暗号化処理及び暗号復号を実行することが可能となり、効率的に暗号化処理を実行することが可能となる。

【００９７】

尚、本発明は、複数の機器（例えば、ホストコンピュータ、インタフェース機器、リーダ、プリンタ等）から構成されるシステムに適用しても、一つの機器からなる装置（例えば、複写機、ファクシミリ装置等）に適用してもよい。

【００９８】

また、本発明の目的は、前述した実施形態の機能を実現するソフトウェアのプログラムコードを記録した記録媒体（または記憶媒体）を、システムあるいは装置に供給し、そのシステムあるいは装置のコンピュータ（またはＣＰＵやＭＰＵ）が記録媒体に格納されたプログラムコードを読み出し実行することによっても、達成されることは言うまでもない。この場合、記録媒体から読み出されたプログラムコード自体が前述した実施形態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録した記録媒体は本発明を構成することになる。また、コンピュータが読み出したプログラムコードを実行することにより、前述した実施形態の機能が実現されるだけでなく、そのプログラムコードの指示に基づき、コンピュータ上で稼働しているオペレーティングシステム（ＯＳ）などが実際の処理の一部または全部を行い、その処理によって前述した実施形態の機能が実現される場合も含まれることは言うまでもない。

【００９９】

さらに、記録媒体から読み出されたプログラムコードが、コンピュータに挿入された機能拡張カードやコンピュータに接続された機能拡張ユニットに備わるメモリに書込まれた後、そのプログラムコードの指示に基づき、その機能拡張カードや機能拡張ユニットに備わるＣＰＵなどが実際の処理の一部または全部を行い、その処理によって前述した実施形態の機能が実現される場合も含まれることは言うまでもない。

【０１００】

本発明を上記記録媒体に適用する場合、その記録媒体には、先に説明したフローチャートに対応するプログラムコードが格納されることになる。

【０１０１】

【発明の効果】

以上説明したように、本発明によれば、画像データの一部領域を暗号化した場合であっても、暗号化された領域を指定する情報を必要とせず、暗号化処理及び復号処理に必要な処理量を軽減することができるという効果が得られる。

【図面の簡単な説明】

【図１】第１の実施形態による画像データを暗号化するための暗号化処理装置の構成を示すブロック図である。

【図２】第１の実施形態による暗号化処理装置の各部の動作手順を説明するためのフローチャートである。

【図３】離散ウェーブレット変換部１０２の構成及び機能を説明するための概要図である。

【図４】領域指定部１０３で生成されるマスク情報の一例を示す図である。

【図５】量子化部１０４で行われるシフトアップによる量子化インデックスの変化を説明するための図である。

【図６】エントロピー符号化部１０５における二値算術符号化処理動作を説明するための図である。

【図７】符号出力部１０７から出力される符号列の構成を説明するための概略図である。

【図８】第１の実施形態における復号処理装置の構成を示すブロック図である。

【図９】第１の実施形態による復号処理装置の動作手順を説明するためのフローチャートである。

【図１０】エントロピー復号部６０３で復号されるビットストリームの様子を説明するための概要図である。

【図１１】逆離散ウェーブレット変換部の構成及び処理について説明するための図である。

【図１２】本実施形態による復号処理装置により画像データを復元表示した際の画像データの表示形態について説明するための図である。

【図１３】本発明における画像データの復号結果を説明するための図である。

【図１４】エントロピー符号化の前に暗号化処理を実行する暗号化処理装置の構成を示すブロック図である。

【図１５】エントロピー復号の後に暗号復号処理を実行する復号処理装置の構成を示す図である。

【図１６】エントロピー符号化部の内部で暗号化処理を実行する暗号化処理装置の構成を示すブロック図である。

【図１７】エントロピー復号部の内部で暗号復号処理を実行する復号処理装置の構成を示す図である。

【図１８】第３の実施形態におけるエントロピー符号化部１３０５の内部構成を示す図である。

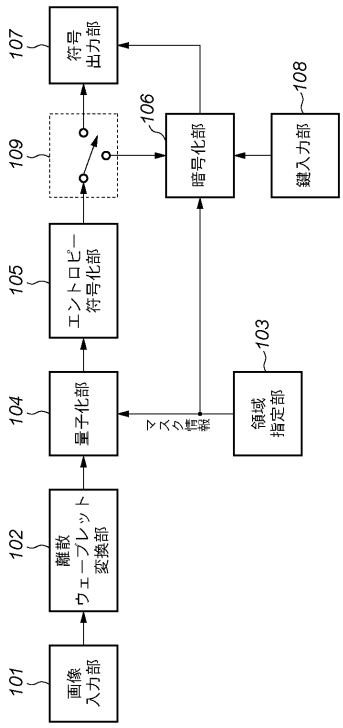
【図１９】第３の実施形態におけるエントロピー復号部の内部構成を示す図である。

【符号の説明】

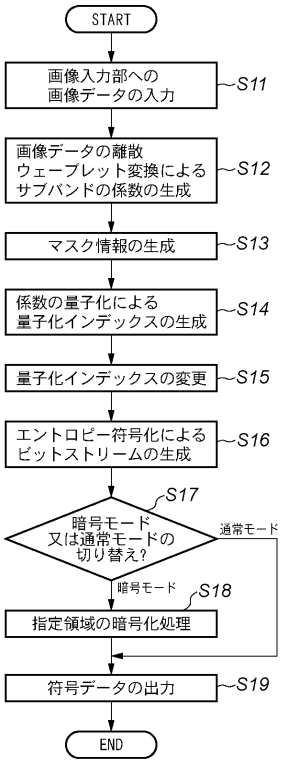
１０１、１００１　画像入力部
１０２、１００２　離散ウェーブレット変換部
１０３、１００３　領域指定部
１０４、１００４　量子化部
１０５、１００５　エントロピー符号化部
１０６、１００６　暗号化部
１０７、１００７　符号出力部
１０８、６０７、１００８、１１０７　鍵入力部
１０９、６０８、１００９、１１０８　切り替え部
６０１、１１０１　符号入力部
６０２、１１０２　暗号復号部
６０３、１１０３　エントロピー復号部

６０４、１１０４　逆量子化部
６０５、１１０５　逆離散ウェーブレット変換部
６０６、１１０６　画像出力部

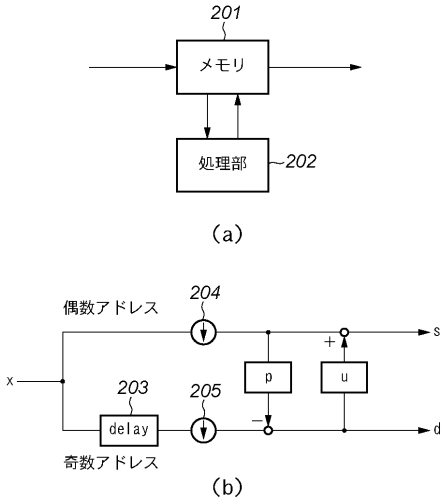
【図１】



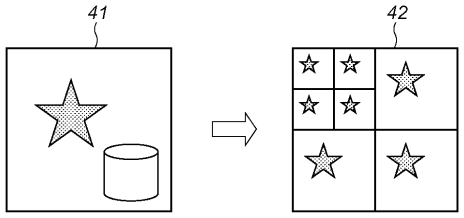
【図２】



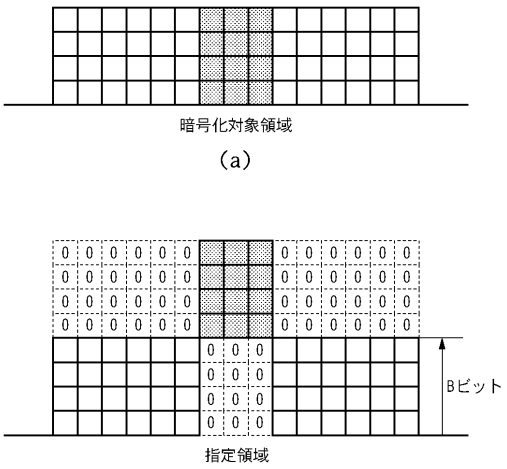
【図３】


201
メモリ
処理部
202
(a)
偶数アドレス
204
s
x
203
205
p
u
delay
d
奇数アドレス
(b)
LL
HL2
HL1
LH2
HH2
LH1
HH1
(c)

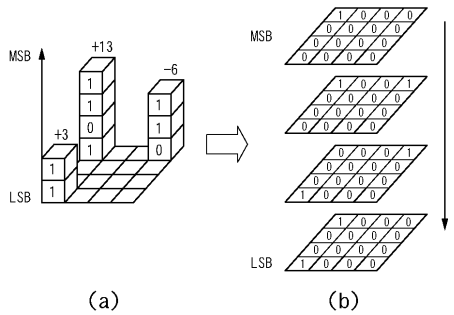
【図４】


41
42

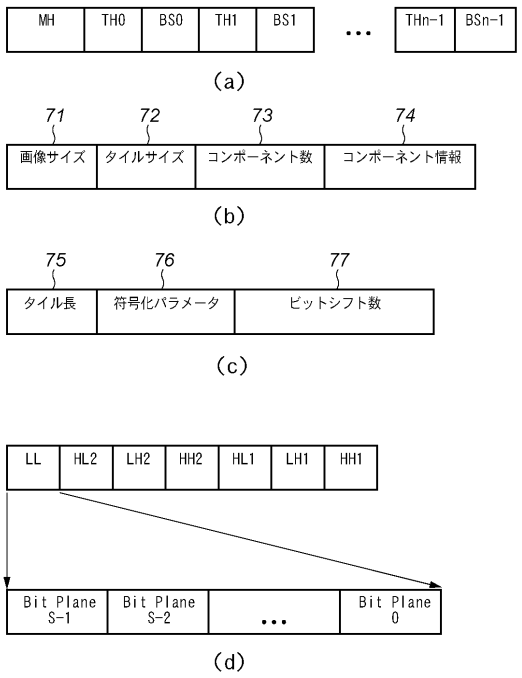
【図５】


暗号化対象領域
(a)
Bビット
指定領域
(b)

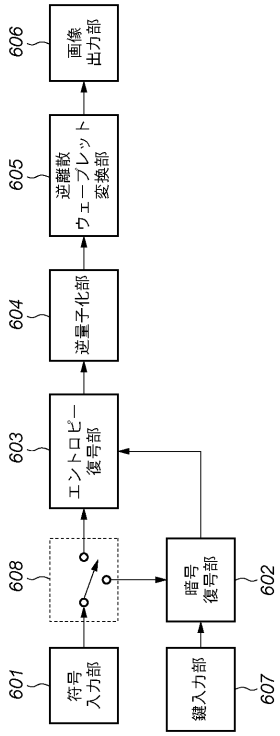
【図６】


MSB
+13
−6
+3
LSB
(a)
MSB
LSB
(b)

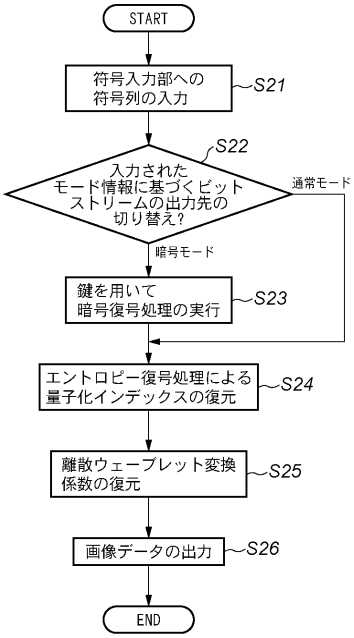
【図７】


MH
TH0
BS0
TH1
BS1
THn−1
BSn−1
(a)
71
72
73
74
画像サイズ
タイルサイズ
コンポーネント数
コンポーネント情報
(b)
75
76
77
タイル長
符号化パラメータ
ビットシフト数
(c)
LL
HL2
LH2
HH2
HL1
LH1
HH1
Bit Plane S-1
Bit Plane S-2
Bit Plane 0
(d)

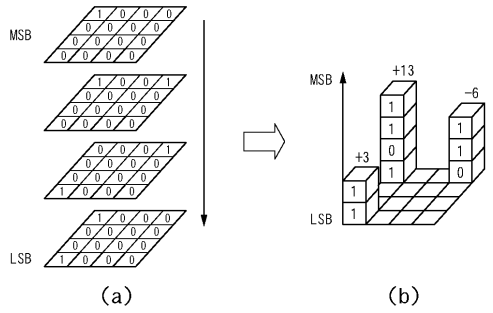
【図８】


606
画像出力部
605
逆離散ウェーブレット変換部
604
逆量子化部
603
エントロピー復号部
608
暗号復号部
602
601
符号入力部
607
鍵入力部

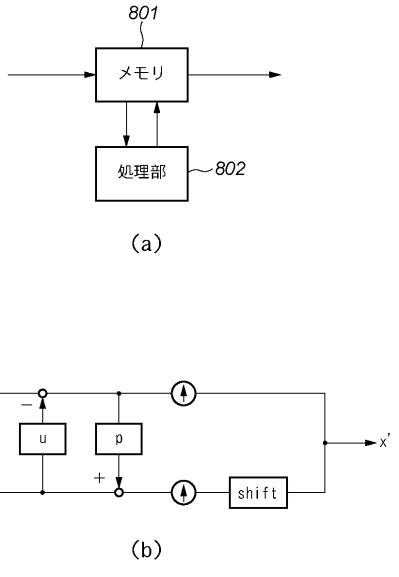
【図９】


START
符号入力部への符号列の入力
S21
S22
入力されたモード情報に基づくビットストリームの出力先の切り替え?
通常モード
暗号モード
鍵を用いて暗号復号処理の実行
S23
エントロピー復号処理による量子化インデックスの復元
S24
離散ウェーブレット変換係数の復元
S25
画像データの出力
S26
END

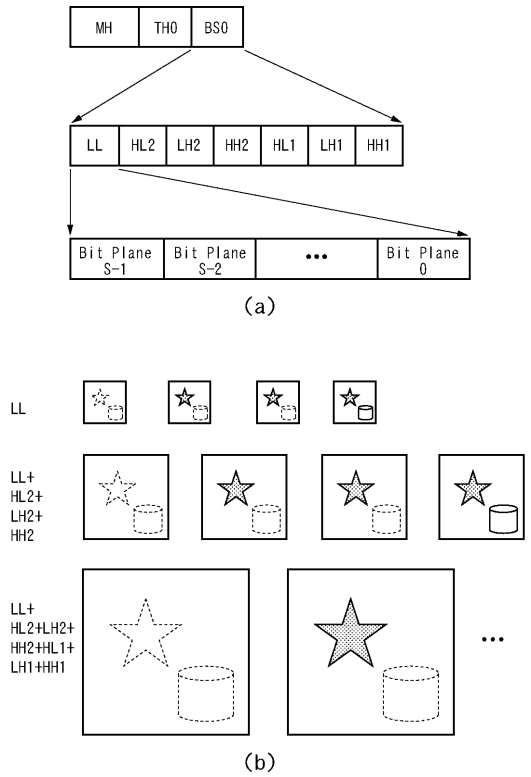
【図１０】


MSB
LSB
+13
+3
−6
(a)
(b)

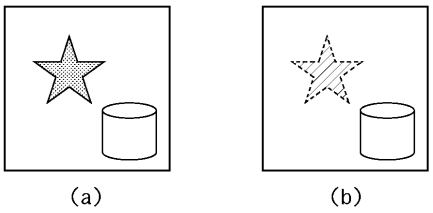
【図１１】


801
メモリ
処理部
802
(a)
s'
d'
u
p
shift
x'
(b)

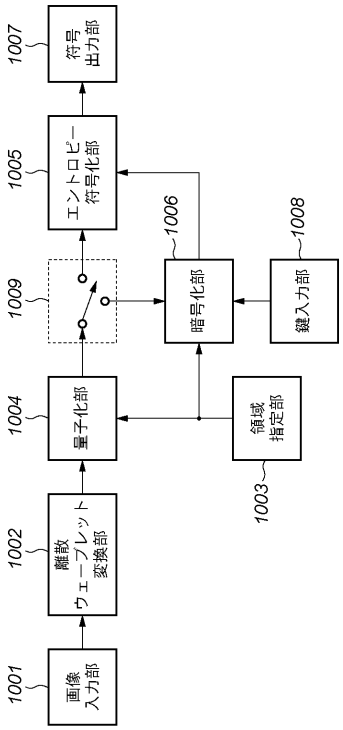
【図１２】



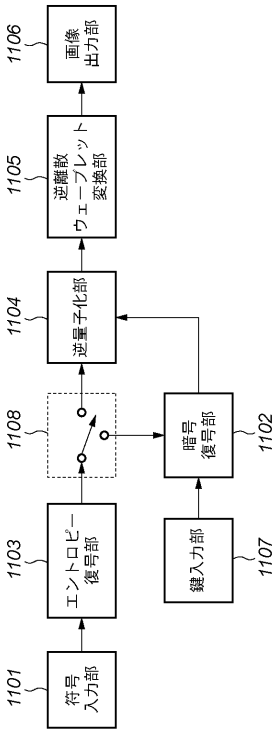
【図１３】



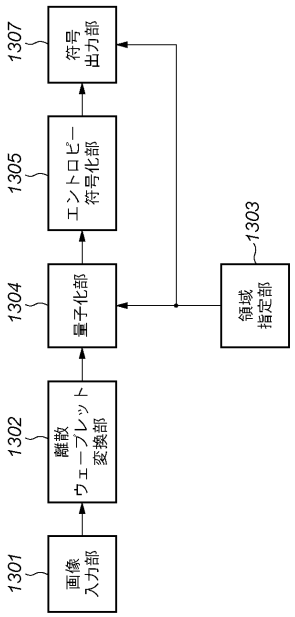
【図１４】



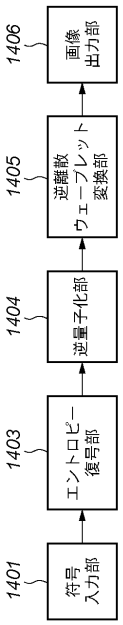
【図１５】



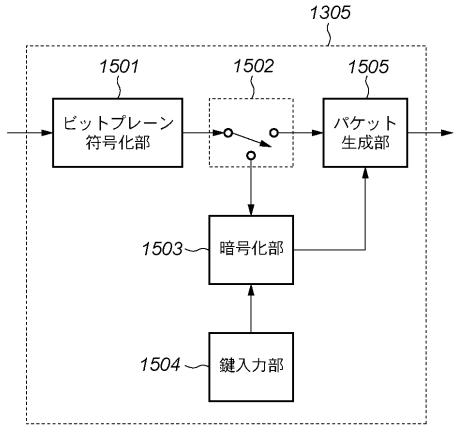
【図１６】



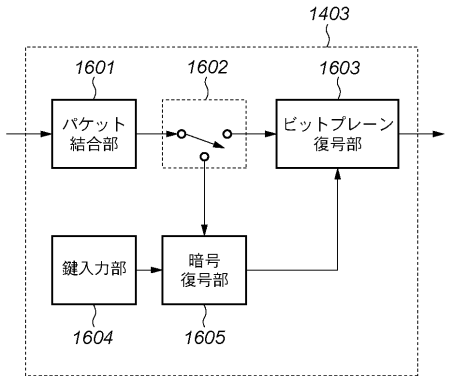
【図１７】



【図１８】



【図１９】



フロントページの続き

(72)発明者　若尾　聡
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
(72)発明者　田頭　信博
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

Ｆターム(参考) 5C075 EE03
5C078 BA53 CA31 CA47 DA01
5J104 AA12 JA03 JA21 PA14