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

特許第4612787号
(P4612787)

(45)発行日　平成23年1月12日(2011.1.12)　(24)登録日　平成22年10月22日(2010.10.22)

(51)Int.Cl.			F I		
H04L	9/16	(2006.01)	H04L	9/00	643
H03M	7/30	(2006.01)	H03M	7/30	A
H04N	1/41	(2006.01)	H04N	1/41	B
H04N	1/44	(2006.01)	H04N	1/44	
H04N	7/30	(2006.01)	H04N	7/133	Z

請求項の数 22　(全 30 頁)

(21)出願番号　特願2003-61863(P2003-61863)
(22)出願日　平成15年3月7日(2003.3.7)
(65)公開番号　特開2004-274358(P2004-274358A)
(43)公開日　平成16年9月30日(2004.9.30)
審査請求日　平成18年2月21日(2006.2.21)

(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　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】画像データの暗号化装置の制御方法及び画像データ変換装置の制御方法、及び、それらの装置、並びにコンピュータプログラム及びコンピュータ可読記憶媒体

(57)【特許請求の範囲】
【請求項１】
画像データを暗号化する画像データ暗号化装置の制御方法であって、
入力手段が、複数のデータブロックで構成される画像データを、前記データブロック単位に入力する入力工程と、
判定手段が、入力したデータブロックが暗号化対象であるか否かを判定する判定工程と、
該判定工程で暗号化対象のデータブロックが入力された場合、暗号化手段が、当該データブロックを暗号化する暗号化工程と、
第１の付加手段が、当該データブロックにおいて、自データより前のデータは意味のあるデータであるとし、自データ以降は無意味なデータであることを示す終端情報を、前記暗号化工程で暗号化されたデータブロックの先頭位置に付加する第１の付加工程と、
切り換え手段が、前記第１の付加工程を実行するか否かを切り換える切り換え工程と、
出力手段が、前記判定工程で暗号化対象外と判定されたデータブロック、前記切り換え工程のもとで生成されたデータブロックを出力する出力工程と
を備えることを特徴とする画像データの暗号化装置の制御方法。
【請求項２】
更に、
第２の付加手段が、前記終端情報を、前記暗号化されたデータブロックの後端位置に付加する第２の付加工程とを備え、

前記切り換え工程は、
前記第１の付加工程による前記終端情報を前記暗号化されたデータブロックの先頭位置に付加するか否か、又は、
前記第１の付加工程、前記第２の付加工程によって前記終端情報を前記暗号化されたデータブロックの先頭位置或いは後端位置のいずれに付加するか
を切り換えることを特徴とする請求項１に記載に記載の画像データの暗号化装置の制御方法。
【請求項３】
暗号化されているか否かを示す情報を、前記終端情報の直後に付加することを特徴とする請求項２に記載の画像データの暗号化装置の制御方法。
【請求項４】
前記終端情報を付加する第１の付加工程は、前記終端情報を、暗号化された画像データと置換し、前記終端情報で置換された箇所の画像データの部分を前記暗号化されたブロックブロックのヘッダに記録することを特徴とする請求項１乃至３のいずれか１項に記載の画像データの暗号化装置の制御方法。
【請求項５】
前記判定工程の判定は、入力したデータブロックが、予め暗号化対象として設定された対象であるか否かを判定することで行ない、
前記切り換え工程は、暗号化されたデータブロックを、非暗号化のデータブロックと同じ扱いで復号処理に渡して良いか否かの設定情報に従って切り換えることを特徴とする請求項１乃至４のいずれか１項に記載の画像データの暗号化装置の制御方法。
【請求項６】
更に、符号化手段が、画像データを圧縮符号化する符号化工程を備え、
前記入力工程は圧縮符号化後の画像データを入力することを特徴とする請求項１乃至４のいずれか１項に記載の画像データの暗号化装置の制御方法。
【請求項７】
前記符号化工程は、
周波数変換手段が、空間領域のデータを周波数領域のデータに変換する周波数変換工程と、
量子化手段が、前記周波数領域のデータを量子化し量子化インデックスを算出する量子化工程と、
エントロピ符号化手段が、前記量子化インデックスをエントロピ符号化するエントロピ符号化工程と
を有することを特徴とする請求項６に記載の画像データの暗号化装置の制御方法。
【請求項８】
前記エントロピ符号化工程は、
領域分割手段が、所定の周波数領域を少なくも一つ以上の互いに重ならない複数の矩形領域に分割する領域分割工程と、
ビットプレーン符号化手段が、前記矩形領域毎にビットプレーン単位で、前記量子化インデックスをエントロピ符号化するビットプレーン符号化工程と、
エントロピ符号列分割手段が、前記矩形領域内のエントロピ符号列を少なくとも一つ以上の符号列の集合に分割するエントロピ符号列分割工程と
を有することを特徴とする請求項７に記載の画像データの暗号化装置の制御方法。
【請求項９】
前記第１の付加工程は、前記矩形領域内の符号列の集合毎に、前記終端情報を付与することを特徴とする請求項８に記載の画像データの暗号化装置の制御方法。
【請求項１０】
前記符号化工程は、
周波数変換手段が、空間領域のデータを周波数領域のデータに変換する周波数変換工程と、

量子化手段が、前記周波数領域のデータを量子化し量子化インデックスを算出する量子化工程と、
エントロピ符号化手段が、前記量子化インデックスをエントロピ符号化するエントロピ符号化工程とを有し、
前記暗号化工程は、前記エントロピ符号化されたエントロピ符号列に対して暗号化処理を実行することを特徴とする請求項６に記載の画像データの暗号化装置の制御方法。
【請求項１１】
前記符号化工程は、
周波数変換手段が、空間領域のデータを周波数領域のデータに変換する周波数変換工程と、
量子化手段が、前記周波数領域のデータを量子化し量子化インデックスを算出する量子化工程と、
エントロピ符号化手段が、前記量子化インデックスをエントロピ符号化するエントロピ符号化工程とを有し、
前記暗号化工程は、前記量子化された量子化インデックスに対して暗号化処理を実行することを特徴とする請求項６に記載の画像データの暗号化装置の制御方法。
【請求項１２】
前記符号化工程は、
周波数変換手段が、空間領域のデータを周波数領域のデータに変換する周波数変換工程と、
量子化手段が、前記周波数領域のデータを量子化し量子化インデックスを算出する量子化工程と、
エントロピ符号化手段が、前記量子化インデックスをエントロピ符号化するエントロピ符号化工程とを有し、
前記暗号化工程は、前記周波数変換された周波数領域のデータに対して暗号化処理を実行することを特徴とする請求項６に記載の画像データの暗号化装置の制御方法。
【請求項１３】
前記エントロピ符号化工程は、
領域分割手段が、所定の周波数領域を少なくも一つ以上の互いに重ならない複数の矩形領域に分割する領域分割工程と、
ビットプレーン符号化手段が、前記矩形領域毎にビットプレーン単位でエントロピ符号化しエントロピ符号列を生成するビットプレーン符号化工程と、
エントロピ符号列分割手段が、前記矩形領域内のエントロピ符号列を少なくとも一つ以上の符号列の集合に分割するエントロピ符号列分割工程と
を備えることを特徴とする請求項１０乃至１２のいずれか１項に記載の画像データの暗号化装置の制御方法。
【請求項１４】
前記第１の付加工程は、前記矩形領域内の符号列の集合毎に、前記終端情報を付与することを特徴とする請求項１３に記載の画像データの暗号化装置の制御方法。
【請求項１５】
暗号化されたデータを含む画像データを再生処理用に変換する画像データ変換装置の制御方法であって、
入力手段が、複数のデータブロックで構成される画像データを、前記データブロック単位に入力する入力工程と、
第１の判定手段が、入力したデータブロックが暗号化されているか否かを判定する第１の判定工程と、
該第１の判定工程で、暗号化されたデータブロックであると判定した場合、第２の判定手段が、暗号化を解除する鍵情報があるか否か判定する第２の判定工程と、
該第２の判定工程で、前記鍵情報があると判定した場合、暗号復号手段が、入力したデータブロックの暗号化を前記鍵情報に従って復号すると共に、当該データブロックにおい

て、自データより前のデータは意味のあるデータであるとし、自データ以降は無意味なデータであることを示す終端情報がある場合には前記終端情報を無効化する暗号復号工程と、

出力手段が、該暗号復号工程で暗号復号されたデータブロック、及び、前記第１の判定工程で非暗号化であると判定されたデータブロック、及び、前記第２の判定工程で前記鍵情報がないと判定されたデータブロックを出力する出力工程と

を備えることを特徴とする画像データ変換装置の制御方法。

【請求項１６】

前記暗号復号工程での、前記終端情報の無効化は、当該終端情報を削除又は暗号復号したデータブロックの後端に配置することを特徴とする請求項１５に記載の画像データ変換装置の制御方法。

【請求項１７】

暗号化されたデータを含む画像データを再生処理用に変換する画像データ変換装置の制御方法であって、

入力手段が、複数のデータブロックで構成される画像データを、前記データブロック単位に入力する入力工程と、

第１の判定手段が、入力したデータブロックが暗号化されているか否かを判定する第１の判定工程と、

該第１の判定工程で、暗号化されたデータブロックであると判定した場合、第２の判定手段が、暗号化を解除する鍵情報があるか否か判定する第２の判定工程と、

該第２の判定工程で、前記鍵情報がないと判定した場合、第３の判定手段が、入力したデータブロックの先頭位置に、有意なデータの終端位置を特定するための終端情報がある場合に、その終端情報を無効化するか否かを判定する第３の判定工程と、

該第３の判定工程で、前記終端情報を無効化すると判定した場合、終端情報無効化手段が、前記終端情報を除去、もしくはデータブロックの後端に位置させる終端情報無効化工程と、

前記第２の判定工程で前記鍵情報があると判定した場合、復号手段が、入力したデータブロックの暗号化を復号する復号工程と、

出力手段が、前記第１の判定工程で暗号化されていないと判定されたデータブロック、前記第３の判定工程で、前記終端情報を無効化しないと判定されたデータブロック、前記終端情報無効化工程で終端情報が無効化されたデータブロック、及び、前記復号工程で復号されたデータブロックを出力する出力工程と

を備えることを特徴とする画像データ変換装置の制御方法。

【請求項１８】

画像データを暗号化する画像データ暗号化装置であって、

複数のデータブロックで構成される画像データを、前記データブロック単位に入力する入力手段と、

入力したデータブロックが暗号化対象であるか否かを判定する判定手段と、

該判定手段で暗号化対象のデータブロックが入力された場合、当該データブロックを暗号化する暗号化手段と、

前記データブロックにおいて、自データより前のデータは意味のあるデータであるとし、自データ以降は無意味なデータであることを示す終端情報を、前記暗号化手段で暗号化されたデータブロックの先頭位置に付加する付加手段と、

前記付加手段を実行するか否かを切り換える切り換え手段と、

前記判定手段で暗号化対象外と判定されたデータブロック、前記切り換え手段のもとで生成されたデータブロックを出力する出力手段と

を備えることを特徴とする画像データの暗号化装置。

【請求項１９】

暗号化されたデータを含む画像データを再生処理用に変換する画像データ変換装置であって、

複数のデータブロックで構成される画像データを、前記データブロック単位に入力する入力手段と、
入力したデータブロックが暗号化されているか否かを判定する第１の判定手段と、
該判定手段で、暗号化されたデータブロックであると判定した場合、暗号化を解除する鍵情報があるか否か判定する第２の判定手段と、
該第２の判定手段で、前記鍵情報があると判定した場合、入力したデータブロックの暗号化を前記鍵情報に従って復号すると共に、当該データブロックにおいて、自データより前のデータは意味のあるデータであるとし、自データ以降は無意味なデータであることを示す終端情報がある場合には前記終端情報を無効化する暗号復号手段と、
該暗号復号手段で暗号復号されたデータブロック、及び、前記第１の判定手段で非暗号化であると判定されたデータブロック、及び、前記第２の判定手段で前記鍵情報がないと判定されたデータブロックを出力する出力手段と
を備えることを特徴とする画像データ変換装置。
【請求項２０】
暗号化されたデータを含む画像データを再生処理用に変換する画像データ変換装置であって、
複数のデータブロックで構成される画像データを、前記データブロック単位に入力する入力手段と、
入力したデータブロックが暗号化されているか否かを判定する第１の判定手段と、
該判定手段で、暗号化されたデータブロックであると判定した場合、暗号化を解除する鍵情報があるか否か判定する第２の判定手段と、
該第２の判定手段で、前記鍵情報がないと判定した場合、入力したデータブロックの先頭位置に、有意なデータの終端位置を特定するための終端情報がある場合に、その終端情報を無効化するか否かを判定する第３の判定手段と、
該第３の判定手段で、前記終端情報を無効化すると判定した場合、前記終端情報を除去、もしくはデータブロックの後端に位置させる終端情報無効化手段と、
前記第２の判定手段で前記鍵情報があると判定した場合、入力したデータブロックの暗号化を復号する復号手段と、
前記第１の判定手段で暗号化されていないと判定されたデータブロック、前記第３の判定手段で、前記終端情報を無効化しないと判定されたデータブロック、前記終端情報無効化手段で終端情報が無効化されたデータブロック、及び、前記復号手段で復号されたデータブロックを出力する出力手段と
を備えることを特徴とする画像データ変換装置。
【請求項２１】
コンピュータに読込ませ実行させることで、前記コンピュータを、請求項１８に記載の暗号化装置の各手段、又は、請求項１９又は請求項２０に記載の画像データ変換装置の各手段として機能させるコンピュータプログラム。
【請求項２２】
請求項２１に記載のコンピュータプログラムを格納したことを特徴とするコンピュータ可読記憶媒体。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】
本発明は画像データの暗号化及び暗号復号技術に関するものである。
【０００２】
【従来の技術】
画像データなどのアクセス制御を目的として、画像データの暗号化やスクランブルなどが行なわれてきた。これは、予め画像データを暗号鍵を用いて暗号化し、前記暗号鍵に対応する復号鍵を有する者だけが正しく再生できるようにする技術である。
【０００３】

一方、画像データは情報量が大きいために、これを効率的に伝送、及び蓄積する際に圧縮符号化を行う場合が多い。圧縮符号化としては、例えば、ＩＳＯ／ＩＥＣ　ＪＴＣ　１／ＳＣ　２９／ＷＧ１にて標準化されているＪＰＥＧ２０００規格と呼ばれる技術などが適応される。前述した画像データの暗号化はＪＰＥＧ２０００規格のような圧縮符号化された画像データに対して施される場合もある。これにより、画像データを効率的に伝送、及び蓄積すると同時に、画像データに対するアクセスを制御できるという利点がある。

【０００４】

特に、ＪＰＥＧ２０００規格のような圧縮符号化技術によれば、画像データは、解像度、画質、空間的領域、画素を構成する成分などに応じて階層的に圧縮符号化できる。こうした階層構造を有する画像データに対して、階層構造に応じた暗号化処理を行うことにより、階層構造に応じたアクセス制御を実現することができる。

【０００５】

例えば、解像度毎にアクセス制御する場合、低解像度成分は暗号化せずに、高解像度成分だけ暗号化するようにすれば、低解像度成分は誰でも再生可能であるが、高解像度成分は許可された利用者（復号鍵の所有者）だけが正しく再生するようにアクセス制御できるようになる。

【０００６】

【発明が解決しようとする課題】

しかしながら、階層構造を有する画像データに当該階層構造に応じた暗号化処理を施した場合、復号鍵を有していない装置では暗号を復号できず、暗号データのままの状態で圧縮復号されるため、画像はスクランブルされた状態となって再生される。即ち、スクランブルされていない状態で画像を再生することは困難であった（例えば、前述した例のように解像度毎にアクセス制御する場合は、高解像度の画像データを再生せずに、低解像度の画像データだけを再生することが困難であった）。

【０００７】

本発明はかかる問題点に鑑みなされたものであり、画像再生装置でスクランブルさせて再生させるか、或いは、非スクランブル状態で再生させるかを暗号化する側で設定可能とする技術を提供しようとするものである。

【０００８】

【課題を解決するための手段】

この課題を解決するため、例えば本発明の画像データの暗号化装置の制御方法は以下の工程を備える。すなわち、

画像データを暗号化する画像データ暗号化装置の制御方法であって、

入力手段が、複数のデータブロックで構成される画像データを、前記データブロック単位に入力する入力工程と、

判定手段が、入力したデータブロックが暗号化対象であるか否かを判定する判定工程と、

該判定工程で暗号化対象のデータブロックが入力された場合、暗号化手段が、当該データブロックを暗号化する暗号化工程と、

第１の付加手段が、当該データブロックにおいて、自データより前のデータは意味のあるデータであるとし、自データ以降は無意味なデータであることを示す終端情報を、前記暗号化工程で暗号化されたデータブロックの先頭位置に付加する第１の付加工程と、

切り換え手段が、前記第１の付加工程を実行するか否かを切り換える切り換え工程と、

出力手段が、前記判定工程で暗号化対象外と判定されたデータブロック、前記切り換え工程のもとで生成されたデータブロックを出力する出力工程とを備える。

【０００９】

【発明の実施の形態】

以下、添付図面に従って本発明に係る実施形態を説明する。

【００１０】

＜全体構成の説明＞

実施形態におけるシステム概要例を図１４に示す。図中、１４０はインターネットであって、１４１は例えばデジタルカメラやイメージスキャナ、フィルムスキャナ等で撮像した画像データを圧縮符号化＆暗号化処理を行う装置である。１４２は画像データを受信し、復号する装置、１４３は復号する際に必要となる暗号化解除鍵を記憶している認証サーバある。装置１４１乃至１４３はパーソナルコンピュータ等の汎用装置で構わない。処理の流れを簡単に説明すると、次の通りである。

【００１１】

装置１４１では、所望とする画像データを圧縮符号化及び暗号化処理を行い、インターネット１４０を介して配布する。配布するのは装置１４１が直接行ってもよいし、適当なサーバを介して配布しても構わない。ただし、暗号化されている関係で、その解除するために必要な鍵情報を、その画像データを特定する情報（例えばＩＤ）と共に認証サーバ１４３が有するＤＢに登録しておく。画像復号装置１４２は所望とする画像を受信し、復号を行ない閲覧するものであるが、暗号化されている画像データを閲覧するには、認証サーバ１４３にその画像を特定する情報を通知して、暗号化解除鍵情報を要求する。この結果、暗号化解除鍵情報が認証サーバ１４３より受信するので、それを用いて暗号化を解除し、復号再生する。

【００１２】

実施形態では説明を簡単なものとするため、暗号化対象の画像（ファイル）はＩＳＯ／ＩＥＣ ＪＴＣ１／ＳＣ２９／ＷＧ１ １０９１８－１において標準化されている、通称ＪＰＥＧ２０００と呼ばれる圧縮符号化方式によって符号化されたデータであるものとして説明するが、ＪＰＥＧ２０００に本発明が限定されることなく、ＪＰＥＧなど種々の圧縮符号化の方式を適応可能であることは以下の説明から明らかになるであろう。

【００１３】

さて、装置１４１での暗号化処理の詳細を説明する前に、実施形態における暗号化処理の操作画面（ウインドウ）について図２０を用いて説明することとする。

【００１４】

図示において、２００がそのウインドウを示し、２０１は暗号化対象となるファイル（ＪＰＥＧ２０００による圧縮符号化されたファイル）を指定する欄であり、不図示のキーボードよりファイルのパス付きで指定しても良いし、その欄２０１の右端に設けられたボタンをクリックすることで、ファイルブラウザを表示し、その中で選択しても構わない。２０２は選択されたファイルで示される画像（復号処理を行う）を表示する領域である。

【００１５】

一方、ウインドウ２００の右側には、暗号化後の出力ファイル名を入力する欄２０３、及び、暗号化を解除する解除鍵のファイル名２０４（解除鍵ファイルは、出力ファイルと同じパスに格納されるものとしているので、ファイル名のみ）を入力する欄が設けられている。

【００１６】

入力対象の画像がＪＰＥＧ２０００による圧縮符号化されているファイルの場合、そのヘッダ部を解析することで、何回のウェーブレット符号化が行われているかが既に決まっていることになる。２０５は、そのファイルのウェーブレット変換回数に基づいて、周波数成分をタイルパートにして示す図である。図示の場合、ウェーブレット変換回数が２回であるので、タイルパートは３つの解像度レベルグループ、すなわち、ＬＬ、｛ＬＨ２＋ＨＨ２＋ＨＬ２｝、及び、｛ＬＨ３＋ＨＨ３＋ＨＬ３｝に別れて示されている。２０７はマウス（登録商標）等のポインティングデバイスに連動して表示されるカーソルである。ユーザは、所望とするタイルパートの上にカーソル２０７を移動させ、その位置でポインティングデバイスが有するボタンをクリックする操作を行うと、そのタイルパートについての暗号化処理の設定ウインドウを表示する。図示の２０８がその設定ウインドウを示している。図示に示す如く、ユーザは該当するタイルパート毎に、暗号化を行うか否か、及び、終端マーカを前、後のいずれにするかを設定することができる（詳細は後述）。なお、これらの項目は２者択一であるのでコンボボックスにしているが、ラジオボタンでも構わ

ない。要するに、表示フォーマットによって本願発明が限定されるものではないことを付言しておく。

【００１７】

なお、ＪＰＥＧ２０００の場合、１画像が複数のタイルで分割されることも有り得る。従って、複数のタイルが存在する場合には、その数に応じた表示を行うことになる。

【００１８】

２０９は本処理を終了させるためのボタンであり、２１０は設定内容に従って暗号化処理を実行開始を行わせるためのボタンである。

【００１９】

ボタン２１０がクリックされた場合には、設定内容（暗号化対象のサブバンドに関する情報、及び、その暗号化するサブバンドの符号化データに終端マーカをどの位置に配置するかという情報）が一時的にＲＡＭ（上記の如く、装置１４１はパーソナルコンピュータ等の汎用情報処理装置でるので、作業用ＲＡＭは備えている）に一時的に格納し、指定されたオリジナル画像ファイルを読み込み、設定された内容に従って暗号化し、その結果を欄２０３に記述されたファイルとして出力することになる。

【００２０】

なお、上記例では、タイルパートが解像度毎のグループに分けている例を説明したが、個々のサブバンド毎、例えば、サブバンドＬＨ３のみ暗号化を行うように指定してもよいし、複数のタイルパートに対して設定するようにしてもよい。

【００２１】

また、図２０では、ウェブレット変換する対象は画像全体に対するもの、すなわち、１タイル＝１画像であるとしたが、タイル数は上記の如く、複数存在数ｒ場合も有り得る。従って、この場合には、設定内容には、タイルを特定する情報も記憶する必要があるし、タイル単位に暗号化する／しないを設定しても構わない。

【００２２】

＜暗号化処理部＞

図１は、実施形態における暗号化処理機能を説明する図である。図１４における装置１４１における処理の一部に対応するものでもあり、図２０においてボタン２１０がクリックされた際の装置の処理機能ブロック図であると言えば分かりやすい。なお、処理対象がＪＰＥＧ２０００以外のデータ形式の場合には、先ず、ＪＰＥＧ２０００による圧縮符号化が行われることになるが、その詳細は後述することとし、ここでは既にＪＰＥＧ２０００により圧縮されたものとして説明する。

【００２３】

図１において、１１はコードストリーム入力部、１２はコードストリーム暗号化部、１３はコードストリーム出力部、１４は図２０の画面で設定した内容を保持する暗号化パラメータ部である。

【００２４】

コードストリーム入力部１１はユーザが指定した画像ファイルをコードストリームとして入力し、それ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、或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。入力されたコードストリームＰはコードストリーム暗号化部１２に出力される。コードストリーム入力部１１には、後述する圧縮符号化処理部から出力されるコードストリームを入力するようにする。

【００２５】

コードストリーム暗号化部１２はコードストリームＰを入力し、コードストリームＰの、暗号化パラメータ部１４よりの設定パラメータにより指定された部分を暗号化処理し、暗号化されたコードストリームＣを出力する。コードストリーム暗号化処理部１２で実行されるコードストリーム暗号化処理の詳細は後述する。暗号化されたコードストリームＣは、コードストリーム出力部１３から外部の記憶装置（例えばハードディスク等）に、ユーザが指定した暗号化後のファイルとして出力される。

【００２６】
コードストリーム出力部１３は、前段のコードストリーム暗号化処理部１２で暗号化されたコードストリームＣが入力され、暗号化されたコードストリームＣとして出力される。また、暗号化を解除する鍵情報は別途作成され、出力されることになる。
【００２７】
次に、コードストリーム暗号化処理部１２で実行されるコードストリーム暗号化処理について、図２を用いて説明する。図２は本実施形態におけるコードストリーム暗号化処理を説明するフローチャートである。
【００２８】
なお、本実施形態におけるコードストリームとは、先に説明したように、ＩＳＯ／ＩＥＣ ＪＴＣ１／ＳＣ２９／ＷＧ１ １０９１８－１において標準化されている、通称ＪＰＥＧ２０００と呼ばれる圧縮符号化方式によって符号化された符号データ列である。従って、コードストリーム入力部１１はこの符号化データ列を入力することになる。
【００２９】
まず、ステップＳ２１では、入力されたコードストリームＰのメインヘッダ及びタイルパートヘッダが解析される。ここで、本実施の形態において適応可能なコードストリームＰの構成を図３を用いて説明する。
【００３０】
ＪＰＥＧ２０００の圧縮符号化時において、画像は先ず複数の矩形領域に分割され、矩形領域毎にウェーブレット変換により独立に符号化処理が施される。この矩形領域を「タイル」と呼ぶ。尚、ＪＰＥＥＧ２０００において、符号化されたタイルに対応するコードストリームは、少なくとも一つ以上のタイルパートと呼ばれる領域に分割できる。ＪＰＥＧ２０００においては、タイル毎に独立に符号化処理を行うことも可能である。
【００３１】
図３（Ａ）は、画像全体が４つのタイルに分割されて圧縮符号化された場合のコードストリームの例を示す。この場合、図３（Ａ）に示すように、コードストリームＰは一つのメインヘッダに続いて、４つのタイルパートから構成されることになる。
【００３２】
メインヘッダは、符号化対象となる画像のサイズ（水平及び垂直方向の画素数）、タイルサイズ、各色成分を表すコンポーネント数、各成分の大きさ、ビット精度を表すコンポーネント情報から構成されている。
【００３３】
次に、本実施形態におけるタイルパートについて説明する。図３（Ｂ）は、一つのタイルパートを構成するコードストリームの構成を示す。図３（Ｂ）に示すように、タイルパートは一つのタイルパートヘッダに続いて、少なくとも一つ以上のパケットと呼ばれる単位から構成される。
【００３４】
なお、通信分野で使われている伝送単位でも「パケット」という表現が使われているが、実施形態で言うパケットとは、通信レベル（プロトコル層）のパケットではなく、アプリケーションレベルのデータの塊を差すことに注意されたい。
【００３５】
タイルパートヘッダは当該タイルパートのビットストリーム長とヘッダ長を含めたタイル長及び当該タイルに対する符号化パラメータから構成される。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（何回ウェーブレットを行ったか）、フィルタ（タップ数の指定）の種類等が含まれている。
【００３６】
次に、本実施形態におけるパケットについて説明する。パケットとは、所定の解像度レベル、所定のレイヤ、所定のプレシンクト、及び所定のコンポーネントにより特定される符号化単位である。また、パケットは、当該パケットに対応するエントロピ符号から構成されるパケットボディ、及び当該パケットボディに関する符号化パラメータを記録したパ

ケットヘッダから構成される。更に、パケットは、図３（Ｃ）に示すように、少なくとも一つ以上のコードブロックと呼ばれる単位から構成される。解像度レベル、レイヤ、プレシンクト、コンポーネント、及びコードブロックについての詳細は後述する。従って、このパケットヘッダを解析すると、当該パケットが如何なる解像度レベル（図２０の周波数成分グループに対応する）、レイヤ、プレシンクト、及びコンポーネントに属するかが判別可能となっている。より分かりやすく説明するのであれば、注目パケットが暗号化対象か否かが判別できることを意味する。

【００３７】

以上、本実施の形態において適応可能なコードストリームＰの構成を説明した。

【００３８】

図２に示すフローチャートの説明に戻る。ステップＳ２２では、パラメータｊが０に初期化される。ｊはパケットを特定するパラメータである。続いて、ステップＳ２３では特定されたパケットｊが暗号化対象であるか否かを、暗号化パラメータ部１４からの情報に従って判定される。パケットｊが暗号化対象である場合には処理をステップＳ２４に進め、暗号化対象でない場合には処理をステップＳ２５に進める。

【００３９】

暗号化対象か否かの設定は、先に図２０で説明した通りであるが、例えば、暗号化パラメータを別途ファイルとして保存しておき、それを使い回しするようにしても構わない。

【００４０】

いずれにしても、「低解像度は誰にでも閲覧可能とし、高解像度は許可されたユーザだけ閲覧可能とする」ようなアクセス制御を行う場合には、ステップＳ２３において高解像度レベルに対応するパケットだけを暗号化対象とし、低解像度レベルに対応するパケットは暗号化対象としないように設定することになる。また、「領域Ａは誰にでも閲覧可能とし、領域Ｂは許可されたユーザだけ閲覧可能とする」ようなアクセス制御を行う場合（タイルが複数存在する場合、或いは特定のサブバンドのみを暗号化する場合等）には、その領域Ｂに対応するパケットだけを暗号化対象とし、領域Ａに対応するパケットは暗号化対象としないように設定すればよい。

【００４１】

また、予めコードストリームに含まれる全てのパケットが暗号化対象である場合には、ステップＳ２３における判定処理を省略することも可能である。更に、後述するパケット暗号化処理内において暗号化対象とするコードブロックを判定するような場合にも、ステップＳ２３における判定処理を省略することが可能である。

【００４２】

次に、ステップＳ２４では、パケットｊに対して、パケット暗号化処理が施される。パケット暗号化処理の詳細は後述する。そして、ステップＳ２５では、パラメータｊの値が１だけ増やされ、ステップＳ２６でパラメータｊとＭの値が比較される。ここでＭはコードストリームに含まれるパケットの総数である。ｊがＭより小さいときは処理をステップＳ２３に進め、ｊがＭ以上の時にはコードストリーム暗号化処理を終了する。

【００４３】

以上、本実施形態におけるコードストリーム暗号化処理について説明した。

【００４４】

次に、本実施の形態におけるパケット暗号化処理の詳細について、図４を用いて説明する。すなわち、暗号化対象のパケットであると判断した場合の処理である。

【００４５】

まず、ステップＳ４１では、入力されたパケットｊのパケットヘッダが解析され、当該パケットに含まれるコードブロック等の構造が解析される。その後、ステップＳ４２ではパラメータｉが０に初期化される。ｉはコードブロックを特定するパラメータである。続いて、ステップＳ４３では、特定されたコードブロックｉが暗号化対象であるか否かが判定される。コードブロックｉが暗号化対象である場合には処理をステップＳ４４に進め、暗号化対象でない場合には処理をステップＳ４８に進める。

【００４６】
尚、前述した図２におけるステップＳ２３などにより、予めパケットに含まれる全てのコードブロックが暗号化対象であることが既知である場合には、ステップＳ４３における判定処理を省略することも可能である。
【００４７】
続いて、ステップＳ４４では、コードブロックｉに暗号化処理が施される。本実施形態においては特に暗号化アルゴリズムについては特に限定しないが、例えばＤＥＳ（Ｄａｔａ Ｅｎｃｒｙｐｔｉｏｎ Ｓｔａｎｄａｒｄ）や、ＡＥＳ（Ａｄｖａｎｃｅｄ Ｅｎｃｒｙｐｔｉｏｎ Ｓｔａｎｄａｒｄ）などの共通鍵暗号アルゴリズムや、ＲＳＡなどの公開鍵暗号アルゴリズムなどの種々の暗号アルゴリズムを適用可能である。適応した暗号アルゴリズムを特定する情報は、メインヘッダ、タイルパートヘッダ、或いは、パケットヘッダなどに記録して、後述する暗号復号処理部に送信するようにすればよい。また、後述する終端マーカの後に付与する付加情報の一部として送信しても良い。また、予め暗号復号処理部と復号処理部で共有するようにしておいても良い。
【００４８】
次に、ステップＳ４５では、暗号化対象のコードブロックｉを、スクランブル再生モードとするか、或いは非スクランブル再生モードとするかが選択される。
スクランブル再生モードの場合には処理をステップＳ４６に進め、一方で非スクランブル再生モードの場合には処理をステップＳ４７に進める。
【００４９】
ここで、スクランブル再生モードと非スクランブル再生モードについて説明する。
【００５０】
一般に、ＪＰＥＧ２０００等の階層構造を有する画像データを再現するときには、低解像度の符号化データから高解像度の符号化に向かって復号処理を行っていく。従って、ウェーブレット変換を利用するＪＰＥＧ２０００の符号化データにおいて、ＬＬを先ず復号し、その復号結果と｛ＬＨ２＋ＨＨ２＋ＨＬ２｝の符号化データとを利用して、更に高い解像度の画像を再現する。そしてその結果と｛ＬＨ３＋ＨＨ３＋ＨＬ３｝の符号化データとを利用して更に高い解像度のデータを再現し、最終的な復号結果となる。
【００５１】
ここで、｛ＬＨ３＋ＨＨ３＋ＨＬ３｝の符号化データが暗号化されていると仮定する。このとき、暗号化を解除する鍵情報を持たないとすると、｛ＬＨ２＋ＨＨ２＋ＨＬ２｝までは正常な像として再現できるものの、続く｛ＬＨ３＋ＨＨ３＋ＨＬ３｝を利用したとたんに無意味なノイズが重畳した像が再現されてしまう。この再生モードを、実施形態ではスクランブル再生モードという。
【００５２】
一方、データとしてはＬＬ、｛ＬＨ２＋ＨＨ２＋ＨＬ２｝が非暗号化され、｛ＬＨ３＋ＨＨ３＋ＨＬ３｝の符号化データが暗号化されている場合、復号処理を｛ＬＨ２＋ＨＨ２＋ＨＬ２｝の符号化データに基づく復号処理で中止する再生モードを、実施形態では、非スクランブル再生モードという。
【００５３】
このスクランブル再生モードと非スクランブル再生モードについて、図７に示す例を用いて説明する。
【００５４】
図７（ａ）は３つの解像度レベル（ウェーブレット変換を２回行った場合）を有するコードストリームのウェーブレット変換領域を示す図である。また、ここでは、上記と同様、最高解像度レベルである｛ＬＨ３，ＨＨ３，ＨＬ３｝に対応するパケットを暗号化し、それ以外の解像度レベルは暗号化しない例を示している。
【００５５】
同図（ｂ）は通常の復号化処理で再生した像を示し、｛ＬＨ３，ＨＨ３，ＨＬ３｝の暗号化された復号データを利用したために、画像にスクランブルされた状態を示している。ま

た、同図（ｃ）は非スクランブル再生モードを適用することで、最高解像度である｛ＬＨ３，ＨＨ３，ＨＬ３｝の暗号化データを利用せず、それより１段階前の解像度で処理を打ち切った場合の例を示している。同図（ｃ）は、最高解像度の画像とはならないので、多少のジャギーが発生するが、少なくとも同図（ａ）よりは意味のある画像が再現できることになる。なお、暗号化を解除する鍵情報を取得した場合、当然、｛ＬＨ３，ＨＨ３，ＨＬ３｝の暗号化を解除して、復号処理が継続することができるので、この場合には、同図（ｄ）に示すようになる。

【００５６】

このように、スクランブル再生モードで処理した場合には、暗号化された解像度レベルは暗号化された状態で再生復号される。即ち、図７（ｂ）に示すように、最高解像度レベル以外（暗号化されていない解像度レベル）は正常に再生されるが、最高解像度レベルのパケット（暗号化されている解像度レベル）はノイズとなって再生される。その結果、画像全体としては、いわゆるスクランブルされたような状態となって見える。

【００５７】

一方、非スクランブル再生モードで処理した場合には、暗号化された解像度レベルは全く再生復号されない。即ち、図７（ｃ）に示すように、暗号化されていない中の最高解像度レベル（図示では｛ＬＨ２＋ＨＨ２＋ＨＬ２｝）まで正常に再生され、それより高い解像度の再現は行わない。その結果、画像全体としては、元の画像の解像度に比べて解像度が低い画像となって見えるものの、違和感のない再現が可能になる。

【００５８】

上記解像度レベルに対する再生制御を行うための処理は、図４のステップＳ４５の判定で行われる。

【００５９】

ステップＳ４６に処理が進むと、終端マーカが暗号化されたコードブロックｉの後ろに付与される。一方、ステップＳ４７では、終端マーカが暗号化されたコードブロックｉの前に付与される。

【００６０】

ここで、終端マーカについて説明する。本実施形態における終端マーカとは、コードブロック内の符号列とコードブロック外の符号列の境界を表す特別なマーカである。例えば、ＪＰＥＧ２０００規格においては、０ｘＦＦ９０以上の値を有する符号が終端マーカに割り当てられている。このため、圧縮復号処理部では終端マーカを受信すると、その後のコードブロック内のビットストリームは復号しないように設計されている。要するに、終端マーカ（終端情報）は、それより前のデータは意味のあるデータであるとし、それ以降は無意味なデータであるとするものである。本実施形態ではこれを利用することになる。

【００６１】

終端マーカについて、更に、図５を用いて説明する。図５において５１、及び５３はビットストリーム、５２は終端マーカを表す。図５に示したような状態の場合、後述する圧縮復号処理部はビットストリーム５１は通常通り圧縮復号していくが、終端マーカ５１を検出した場合、同じコードブロック中の後続するビットストリーム５３は圧縮復号しない。

【００６２】

本発明は、こうした終端マーカの性質を利用して、スクランブル再生モードの場合は終端マーカを暗号文の後ろに付与し、非スクランブル再生モードの場合は終端マーカを暗号文の前に付与するように処理するものである。即ち、スクランブル再生モードにおいては、暗号文は終端マーカの前に位置するためスクランブル状態として再生されるが、非スクランブル再生モードにおいては、暗号文は終端マーカの後に位置するため再生されない。

【００６３】

図２０で説明した、設定ウインドウ２０８における終端マーカの選択パラメータ「前」、「後」はかかる意味である。従って、図２０におけるユーザが選択する項目を別な言い方をすれば、スクランブル再生モードにするか、非スクランブル再生モードにするか、でもある。

【００６４】
また、本実施形態では終端マーカだけを付与するものとして説明したが、本発明はこれに限定されることなく、種々の付加情報を終端マーカの後に付与するようにしてもよい。例えば、当該コードブロックやパケットなどを復号する鍵に関連する情報（暗号化された鍵や、鍵へのポインタなど）や、暗号化のための各種パラメータ（ブロック暗号における利用モードなど）や、暗号化アルゴリズムに関連する情報（暗号化アルゴリズム名や暗号化アルゴリズムを特定する情報）などを付加するようにしても良い。
【００６５】
また、本実施の形態において、ステップＳ４６、及びステップＳ４７において終端マーカ（及び付加情報）を付与する方法については、終端マーカ（及び付加情報）を新たに追加しても良いし、暗号化された、又は、暗号化されていないビットストリームと置換するようにしても良い。終端マーカを付与する場合の例について更に図６を用いて説明する。
【００６６】
終端マーカを追加した場合の例を図６（ａ）、及び（ｂ）に示す。図６（ａ）、及び（ｂ）は暗号化されたパケットボディを示している。図６に示す例では、パケットは図中太線で示す５つのコードブロックから構成されている。また、図中網掛けした箇所は終端マーカを示す。すなわち、図６（ａ）はスクランブル再生モードを示し、図６（ｂ）は非スクランブル再生モードを示すことになるのは、上記理由から明らかである。
【００６７】
図６（ａ）、及び（ｂ）に示すように、終端マーカを追加した場合には、暗号化の前後で追加した終端マーカの分だけコードブロックの長さが長くなる為に、パケットヘッダに記録されている各コードブロックの長さや、タイルパートヘッダに記録されているタイルパートの長さを適当な長さに修正する必要がある。
【００６８】
一方、終端マーカを置換した場合の例を図６（ｃ）、（ｄ）に示す。図６（ｃ）及び（ｄ）は、図６（ａ）、及び（ｂ）と同様に暗号化されたパケットボディを示している。図６（ｃ）、及び（ｄ）に示す例でも、パケットは図中太線で示す５つのコードブロックから構成されている。また、図中網掛けした箇所は終端カーマを示す。即ち、図６（ｃ）はスクランブル再生モードを示し、図６（ｄ）は非スクランブル再生モードを示す。
【００６９】
図６（ｃ）、及び（ｄ）に示すように、終端マーカを置換した場合には、暗号化の前後でコードブロックの長さが変化することはない。終端マーカを置換する前のビットストリームの情報は、タイルパートヘッダやパケットヘッダなどに記録しておくようにすればよい。また、終端マーカを置換する前のビットストリームへ戻す為の鍵情報として、暗号化処理部から復号処理部に送信されるようにしても良い。
【００７０】
尚、本実施形態では、ステップＳ４５においてスクランブルモードが選択された場合、ステップＳ４６において、終端マーカを暗号化したコードブロックｉの後ろに付けるようにした。しかしながら本実施形態はこれに限定されることなく、スクランブルモードの場合には終端マーカを付けないようにすることも可能であることは明らかである。この場合、メインヘッダ、タイルパートヘッダ、或いはパケットヘッダなどに当該コードブロック、或いはパケットが暗号化されていることを記録するようにすれば良い。
【００７１】
また、本実施形態では、前述したように終端マーカの後に更に付加情報を付与することも可能である。図６（ｅ）、及び（ｆ）は、終端マーカの後にパケットに関する付加情報（図中、斜線で示す）を付与した場合の構成を示す。図６（ｅ）はスクランブルモードにおけるパケットの構成を示し、図６（ｆ）は非スクランブルモードにおけるパケットの構成を示す。図６（ｅ）に示すように、スクランブルモードの場合は、パケットに関する付加情報は、パケットに含まれる最初のコードブロックの後だけに、終端マーカに続けて付加するようにすれば良い。一方、図６（ｆ）に示すように、非スクランブルモードの場合は

、パケットに関する付加情報は、パケットに含まれる最初のコードブロックの前に、終端マーカに続けて付加し、更に、最初のコードブロック以外の夫々のコードブロックの前には終端マーカだけを付加するようにすればよい。以上のような構成とすることによって、パケットに関する付加情報を（パケット中の全てのコードブロックに付与することなく）効率的に付与できる。

【００７２】

次に、ステップＳ４８では、パラメータｉの値が１だけ増やされ、ステップＳ４９でパラメータｉとＮの値が比較される。ここで、Ｎはパケットに含まれるコードブロックの総数である。ｉがＮより小さいときは処理をステップＳ４３に進め、ｉがＮ以上の時にはパケット暗号化処理を終了する。

【００７３】

尚、本実施の形態では、「暗号化されているか否か」という情報は終端マーカの直後に暗号化されていることを示す符号によって記録した。この場合、後述する暗号復号処理部において、パケットが暗号化されているか否かを確かめるためには、パケットの構造を解析して、コードブロック内の終端マーカの直後を調べる必要がある。しかしながら、本発明はこれに限定されることなく、終端マーカに加えて、メインヘッダ、タイルパートヘッダ、パケットヘッダの内部或いは外部において、パケットが暗号化されていることを示すような情報を記録するようにしてもよい。このようにすることによって、後述する暗号復号処理部において、パケットの構造を解析することなく、パケットが暗号化されているか否かを調べることが可能である。

【００７４】

以上、本実施形態における暗号化処理部について説明した。

【００７５】

＜暗号復号処理部＞

次に、図８を用いて本実施の形態における暗号復号処理機能を説明する。この処理は、図１４における画像復号装置１４２における処理であると言えば分かりやすい。また、ＪＰＥＧ２０００による復号処理は後段に位置することになる。図８の構成は、あくまで暗号を復号、すなわち、解除する処理機能を示していることに注意されたい。

【００７６】

図８において、８１はコードストリーム入力部、８２はコードストリーム復号部、８３はコードストリーム出力部である。

【００７７】

コードストリーム入力部８１はコードストリームを入力し、それ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、或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。通常は、前述した図１に示す暗号化処理部において暗号化処理されたコードストリームＣが入力される。しかしながら、暗号化が施されていないコードストリームが入力されても構わない。入力されたコードストリームＰはコードストリーム暗号化部１２に出力される。

【００７８】

コードストリーム復号部８２はコードストリームＣを入力し、暗号復号鍵情報に従って（もし存在すれば）、コードストリームＣの所定の部分を復号処理し、復号処理されたコードストリームＰ’が出力される。コードストリームＣに施されている全ての暗号が復号（暗号解除）される場合には、コードストリームＰ'はコードストリームＰと等しいものになる。しかしながら、後述する種々の条件（復号鍵が存在しなかったり、明示的にスクランブル再生が指定された場合など）により、全ての暗号が復号されない場合には、コードストリームＰ'はコードストリームＰと等しいものとはならない。コードストリーム復号処理部８２で実行されるコードストリーム復号処理の詳細は後述する。復号されたコードストリームＣはコードストリーム出力部８３に出力される。

【００７９】

コードストリーム出力部８３は、前段のコードストリーム復号処理部８２で復号されたコ

ードストリームＰ'が入力され、復号されたコードストリームＰ'が出力される。復号されたコードストリームＰ'は、画像として再生するために、後述する圧縮復号処理部に出力される。

【００８０】

次に、コードストリーム復号処理部８２で実行されるコードストリーム復号処理について図９を用いて説明する。図９は本実施形態におけるコードストリーム復号処理を説明するフローチャートである。

【００８１】

まず、入力されたコードストリームＣに対して、ステップＳ９１では、メインヘッダ及びタイルパートヘッダが解析される。次に、ステップＳ９２では、パラメータｊが０に初期化される。ｊはパケットを特定するパラメータである。続いて、ステップＳ９３では、特定されたパケットｊ内に暗号化されたコードブロックがあるか否かが判定される。

【００８２】

実施形態では、パケットを構成するコードブロック中の終端マーカの直後に暗号化されている／いないを示す情報を格納しているので、これを検出することで行うが、例えば、メインヘッダ、タイルパートヘッダ、パケットヘッダの内部或いは外部において、パケットが暗号化されていることを示す情報を調べることによって、判定しても構わない。これらの情報が用いられていない場合には、ステップＳ９３による判定処理をスキップすることも可能である。

【００８３】

ステップＳ９４では、パケットｊに対して、パケット復号処理が施される。パケット復号処理の詳細は後述する。また、ステップＳ９５では、パラメータｊの値が１だけ増やされ、ステップＳ９５でパラメータｊとＭの値が比較される。ここで、Ｍはコードストリームに含まれるパケットの総数である。ｊがＭより小さいときは処理をステップＳ９３に進め、ｊがＭ以上の時にはコードストリーム復号処理を終了する。

【００８４】

次に、本実施形態におけるパケット復号処理の詳細について、図１０を用いて説明する。この処理は、注目パケット内に暗号化されたコードブロックが存在すると判定された場合である。

【００８５】

まず、入力されたパケットｊに対して、ステップＳ１０１では、パケットｊのパケットヘッダが解析され、当該パケットに含まれるコードブロック等の構造が解析される。その後、ステップＳ１０２では、パラメータｉが０に初期化される。パラメータｉはコードブロックを特定するパラメータである。

【００８６】

続いて、ステップＳ１０３では、特定されたコードブロックｉが暗号化されているか否かが判定される。この判断は、先に説明したように、終端マーカの直後に暗号化されていることを示す情報があるか否かで判断するが、メインヘッダ、タイルパートヘッダ、或いはパケットヘッダ内に、暗号化されている箇所を明記する情報を格納しておき、これによって判断しても構わない。

【００８７】

暗号化されていないと判断した場合には、ステップＳ１０７に進み、注目コードブロックはそのままの状態で出力され、変数ｉを１つ増加させ、上記ステップＳ１０３以降の処理（次のコードブロックに対する処理）を行う。

【００８８】

さて、コードブロックｊが暗号化されていると判断した場合、処理はステップＳ１０４に進み、暗号化を解除する鍵情報が存在するか否かを判断する。

【００８９】

もし、その鍵情報が存在しないと判断した場合には、ステップＳ１０７に移って、そのままの状態で後段の処理に渡すことになる。従って、終端マーカがコードブロックの先頭に

ある場合には、そのまま後段に出力され、終端マーカ以降、すなわち、注目コードブロックについては符号化データの復号処理が行われなくなるので、非スクランブル再生が行われることになる。また、終端マーカがコードブロックの後端にある場合には、暗号化されたままの状態で符号化データを復号してしまうので、スクランブル再生が行われることになる（この場合には、終端マーカを削除しても構わない）。

【００９０】

さて、ステップＳ１０４において、暗号を解除する鍵情報が存在すると判断した場合、処理はステップＳ１０６に進む。ここでは、注目の暗号化されたコードブロックを、その鍵情報に従って復号する。このとき、終端マーカがコードブロックの先頭にあった場合には、その後端に移動させる（削除でも良い）。更に、メインヘッダ、タイルパートヘッダ、或いはパケットヘッダに、当該コードブロックが暗号化されている情報が記録されている場合には、これらの情報を暗号化されていないことを表すように変更する。

【００９１】

この後、処理はステップＳ１０７に進み、暗号解除毎のコードブロックを出力し、変数ｉを更新することになる。

【００９２】

以上の処理を、ステップＳ１０８で注目パケットに含まれる全コードブロックに対して行ない、その処理を終えた場合には図９のステップＳ９５に復帰し、次のパケットに対する処理を行うことになる。

【００９３】

以上、本実施形態における暗号復号処理部について説明した。

【００９４】

上記処理を行うと、暗号化を解除する鍵情報が存在しない場合、各パケットを構成するコードブロックの終端マーカは、入力したストリームのまま維持されることになる。換言すれば、暗号化したユーザの意図が反映された状態で、符号化画像データの復号処理が行われることになる。

【００９５】

一方、暗号化を解除する鍵情報が存在した場合には、暗号化されたコードブロックのデータの暗号化が解除され、尚且つ、終端マーカがコードブロックの後端に位置する、もしくは削除されることになり、そのコードブロックを利用した再現処理が行われることになる。

【００９６】

＜圧縮符号化処理部＞

以上であるが、実施形態における装置１４１は、既にＪＰＥＧ２０００で圧縮符号化された画像ファイルを暗号化する例を説明したが、生の画像データを符号化し、それに後続する処理として図１の構成を設けても構わない。

【００９７】

従って、かかる構成にした場合の画像圧縮符号化について説明することとする。

【００９８】

まずはじめに、図１１を用いて本実施形態における圧縮符号化処理を説明する。

【００９９】

図１１において、１１１は画像入力部、１１２は離散ウェーブレット変換部、１１３は量子化部、１１４はエントロピ符号化部、１１５は符号出力部である。

まず、画像入力部１１１に対して符号化対象となる画像を構成する画素信号がラスタースキャン順に入力し、その出力は離散ウェーブレット変換部１１２に入力される。以降の説明では、その説明を容易なものとするため、画像信号はモノクロの多値画像を表現しているが、カラー画像等、複数の色成分を符号化するならば、ＲＧＢ各色成分、或いは輝度、色度成分を上記単色成分として圧縮すればよい。

【０１００】

離散ウェーブレット変換部１１２は、入力した画像信号に対して２次元の離散ウェーブレ

ット変換処理を行い、変換係数を計算して出力するものである。図１２（ａ）は離散ウェーブレット変換部１２の基本構成を表したものであり、入力された画像信号はメモリ１２１に記憶され、処理部１２２により順次読み出されて変換処理が行われ、再びメモリ１２１に書きこまれており、本実施の形態においては、処理部１２２における処理の構成は同図（ｂ）に示すものとする。同図において、入力された画像信号は遅延素子およびダウンサンプラの組み合わせにより、偶数アドレスおよび奇数アドレスの信号に分離され、２つのフィルタｐおよびｕによりフィルタ処理が施される。同図ｓおよびｄは、各々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およびハイパス係数を表しており、次式により計算されるものとする。

d(n) = x(2*n + 1) - floor((x(2*n) + x(2*n + 2))/2)　　（式１）

s(n) = x(2*n) + floor((d(n - 1) + d(n))/4)　　（式２）

ただし、x(n)は変換対象となる画像信号であり、floor(x)はｘを越えない最大整数を返す関数である。

【０１０１】

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。図１２（ｃ）は２次元の変換処理により得られる２レベルの変換係数群の構成例であり、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。なお、以降の説明ではこれらの係数列をサブバンドと呼ぶ。また、同じ分割レベルに属するサブバンドの集合を解像度レベルと呼ぶ。例えば、ＨＨ１、ＨＬ１、ＬＨ１は同じ解像度レベルに属する。各サブバンドの係数は後続の量子化部１１３に出力される。

【０１０２】

量子化部１１３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。ここで、量子化は次式により行われる。

q = sign (c) floor(abs(c) / Δ)　　（式３）

sign(c) = 1; c >= 0　　（式４）

sign(c) = -1; c < 0　　（式５）

ここで、ｃは量子化対象となる係数である。

【０１０３】

また、本実施の形態においては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ず、量子化部１１３に入力された変換係数はそのまま後続のエントロピ符号化部１１４に出力される。

【０１０４】

エントロピ符号化部１１４は入力したサブバンドを互いに重ならない複数の矩形領域に分割し、夫々の分割した矩形領域に含まれる量子化インデックスをビットプレーンに分解し、ビットプレーンを単位として２値算術符号化を行ってコードストリームを出力する。ここで、エントロピ符号化部における符号化単位となる矩形領域をコードブロックと呼ぶ。

【０１０５】

図１３はエントロピ符号化部１４の動作を説明する図であり、この例においては４×４の大きさを持つコードブロックにおいて非０の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。エントロピ符号化部１４はコードブロックを走査して最大値ＭＡＸを求め、次式により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。

S = ceil(log2(abs(MAX)))　　（式６）

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関数である。

【０１０６】

図１３においては、最大の係数値は１３であるのでＳは４であり、シーケンス中の１６個の量子化インデックスは同図（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。最初にエントロピ符号化部１１４は最上位ビットプレーン(同図ＭＳＢで表

す)の各ビットをエントロピ符号化（本実施の形態では２値算術符号化）し、ビットストリームとして出力する。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（同図ＬＳＢで表す）に至るまで、ビットプレーン内の各ビットを符号化し符号出力部１５に出力する。なお上記エントロピ符号化時において、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ビットが検出されると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２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は効率良く符号化される。

【０１０７】

尚、以上の様にエントロピ符号化されたエントロピ符号を所定の符号量となるように集めた処理単位をレイヤと呼ぶ。複数のレイヤを構成することにより、復号時に種々の符号量に対応した画像を再生することが可能となる。

【０１０８】

また、最上位のビットプレーンの情報が各値に支配的であることに注意されたい。つまり、先に説明した例では、ウェーブレット変換する際のサブバンド、もしくは周波数成分グループに対して暗号化する／しないを設定したが、上記の如く、各ビットプレーンのどのレベルについて暗号化する／しないを設定したとしても同様の効果が期待できる。例えば、最下位（ビット０）のビットプレーンに対して暗号化を行えば、それより１つ上位（ビット１）のプレーンまでの復号化でもって再生される画像は、最高解像度よりも１つ下の解像度となって再現できることになり、図７とほぼ等価の状態となる。

【０１０９】

＜圧縮復号処理部＞

次に以上述べた圧縮符号化処理部による符号列を復号する方法について説明する。

【０１１０】

図１５は本実施の形態における圧縮復号化処理部の構成を表すブロック図であり、１５１が符号入力部、１５２はエントロピ復号部、１５３は逆量子化部、１５４は逆離散ウェーブレット変換部、１５５は画像出力部である。

【０１１１】

符号入力部１５１は符号列を入力し、それ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。図８に示すコードストリーム出力部８３からの出力を、入力すると言えばわかり易い。また、符号列に含まれるビットストリームはエントロピ復号部１５２に出力される。

【０１１２】

エントロピ復号部１５２はビットストリームをコードブロックに分割し、コードブロック内においてビットプレーン単位で復号し、出力する。この時の復号化手順を図１６に示す。図１６（ａ）は復号対象となるコードブロックをビットプレーン単位で順次復号化し、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される。復元された量子化インデックスは逆量子化部１５３に出力される。

【０１１３】

次に、逆量子化部１５３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。

$c' = \Delta * q ; \quad q \neq 0$ （式７）

$c' = 0 \quad ; \quad q = 0$ （式８）

ここで、ｑは量子化インデックス、Δは量子化ステップであり、Δは符号化時に用いられたものと同じ値である。ｃ'は復元された変換係数であり、符号化時ではｓまたはｄで表される係数の復元したものである。変換係数ｃ'は後続の逆離散ウェーブレット変換部１５４に出力される。

【０１１４】

図１７は逆離散ウェーブレット変換部１５４の構成および処理のブロック図を示したものである。同図（ａ）において、入力された変換係数はメモリ１７１に記憶される。処理部１７２は１次元の逆離散ウェーブレット変換を行い、メモリ１７１から順次変換係数を読み出して処理を行うことで、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。また同図（ｂ）は処理部１７２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およびｐの２つのフィルタ処理を施され、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。

x'(2*n) = s'(n) - floor ((d'(n-1) + d'(n))/4)　　（式９）

x'(2*n+1) = d'(n) + floor ((x'(2*n) + x'(2*n+2))/2)　　（式１０）

ここで、式（１）、式（２）、および式（９）、式（１０）による順方向およ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、本実施形態において量子化ステップΔが１であり、ビットプレーン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。

【０１１５】

以上の処理により画像が復元されて画像出力部１５５に出力される。 画像出力部１５５はモニタ等の画像表示装置であってもよいし、あるいは磁気ディスク等の記憶装置であってもよい。

【０１１６】

＜第１の実施形態の変形例＞

上記実施形態では、例えば、図７の如く、｛ＬＨ３＋ＨＨ３＋ＨＬ３｝について暗号化され、それ以外では非暗号化の符号化データを装置１４２が受信し再生するときであって、その装置１４２が暗号解除鍵情報を持たない場合には、上記最高解像度に相当するデータが暗号化されたまま再生することになり、結果的に、図７（ｂ）に示すようなスクランブルされた画像が表示されてしまう。

【０１１７】

しかしながら、もともと暗号化する側である装置１４１のユーザは、｛ＬＨ２＋ＨＨ２＋ＨＬ２｝までの、最高解像度よりも１つ手前までの再生を許容しているわけであるから、装置１４２のユーザが仮に暗号化を解除する鍵情報を所有していなくても、必要に応じて｛ＬＨ３＋ＨＨ３＋ＨＬ３｝のデータを利用する直前までの状態で再現できるようにすることが望まれる。

【０１１８】

そこで、本第１の実施形態における変形例では、この問題を解決する。

【０１１９】

図１０Ｂは、先に説明した図１０Ａに置き換わるものである。それ以外の装置構成は第１の実施形態と同様であるものとし、以下では、図１０Ｂについて説明することとする。

【０１２０】

図１０Ｂにおいて、図１０Ａと異なる点は、ステップＳ１０５、１０９、１１０が追加された点であるが、以下、順に説明することとする。なお、以下の処理をはじめるに当たって、装置１４２のユーザは、スクランブルを解除するか否かを設定しているとする。この設定は、暗号化解除する際に適宜設定しても良いし、予め、そのユーザの設定事項をファイル等に記憶保持しておくようにしてもよい。前者の場合には、個々の画像を再生する際に、その都度行えることになり、後者の場合には特に変更しない限りは、その設定内容が全ての画像復号に反映されることになる。

【０１２１】

まず、入力されたパケットｊに対して、ステップＳ１０１では、パケットｊのパケットヘッダが解析され、当該パケットに含まれるコードブロック等の構造が解析される。その後、ステップＳ１０２では、パラメータｉが０に初期化される。パラメータｉはコードブロックを特定するパラメータである。

【０１２２】

続いて、ステップＳ１０３では、特定されたコードブロックｉが暗号化されているか否かが判定される。この判断は、先に説明したように、終端マーカの直後に暗号化されていることを示す情報があるか否かで判断するが、メインヘッダ、タイルパートヘッダ、或いはパケットヘッダ内に、暗号化されている箇所を明記する情報を格納しておき、これによって判断しても構わない。

【０１２３】

暗号化されていないと判断した場合には、ステップＳ１０７に進み、注目コードブロックはそのままの状態で出力され、変数ｉを１つ増加させ、上記ステップＳ１０３以降の処理（次のコードブロックに対する処理）を行う。

【０１２４】

また、コードブロックｊが暗号化されていると判断した場合、処理はステップＳ１０４に進み、暗号化を解除する鍵情報が存在するか否かを判断する。

【０１２５】

もし、その鍵情報が存在しないと判断した場合には、ステップＳ１０９に分岐し、鍵情報が存在すると判断した場合には、ステップＳ１０５に進むことになる。

【０１２６】

ステップＳ１０５では、所定のコードブロックをスクランブル再生するか、或いは非スクランブル再生するかが判定される。これは先に説明したように、装置１４２のユーザの設定内容によって判断することになる。通常、復号鍵を有している場合は非スクランブル再生することが多い。しかしながら、暗号化されているコードストリームの一部だけを復号し、一部の暗号文を復号しない場合などに、ステップＳ１０５により明示的にスクランブル再生を選択することが可能である。尚、復号鍵を有する全ての暗号文を復号する場合には、ステップＳ１０５は省略可能であることは明らかである。

【０１２７】

そして、ステップＳ１０６に進むと、コードブロックｉが暗号の復号処理（暗号解除処理）される。暗号復号処理は、前述した図４におけるステップＳ４４で用いた暗号アルゴリズムに対応したものでなければならない。ステップＳ４４で用いた暗号アルゴリズムは、メインヘッダ、タイルパートヘッダ、或いはパケットヘッダに記録してある情報を調べることにより知ることができる。また、前述したする終端マーカの後に付与されている付加情報を調べるようにしても良い。

また、暗号復号処理が施されたコードブロック内の終端マーカはコードブロックの終端に位置させるか、或いは、除去する。更に、メインヘッダ、タイルパートヘッダ、或いはパケットヘッダに、当該コードブロックが暗号化されている情報が記録されている場合には、これらの情報を暗号化されていないことを表すように変更する。

【０１２８】

一方、ステップＳ１０４で暗号を解除する鍵情報がないと判断した場合、処理はステップＳ１０９に進むことになる。このステップＳ１０９では、復号鍵がない場合に、非スクランブル再生するか否かが判定される。この判定は、ステップＳ１０５と同様であり、ユーザによって明示的に指示するようにしても良いし、予めＲＡＭやＨＤＤに記憶されている情報を用いて判定するようにしても良い。そして、非スクランブル再生する場合にはステップＳ１１０に進み、スクランブル再生する場合にはステップＳ１０７に進む。ステップＳ１１０では、終端マーカが暗号文の前に付与されている場合には暗号文の後ろに移動させる。或いは、終端マーカを消去するようにしても構わない。

【０１２９】

ステップＳ１０９、及びステップＳ１１０における処理について説明する。前述した暗号化処理部において、非スクランブル再生モードとした場合には、コードブロックｉ内において暗号文の前に終端マーカが付加されている。これにより、当該終端マーカにより暗号文を復号しないために、通常は非スクランブル再生モードとなる。しかしながら、本実施形態によれば判定処理Ｓ１０９により、スクランブル再生とするか非スクランブル再生とするかを選択することが可能となる。

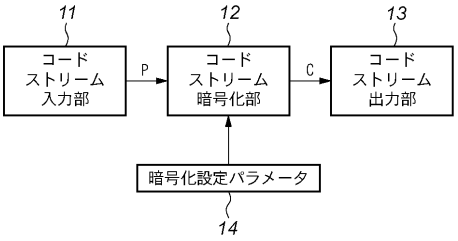
【０１３０】
処理が、ステップＳ１０７に進むと、そのコードブロックを出力し、変数ｉをインクリメントし、ステップＳ１０８で注目パケットに含まれる全コードブロックに対して行なったか否かを判断し、否の場合には、ステップＳ１０３以降の処理を繰り返す。また、注目パケットの全コードブロックに対する処理が終了したと判断した場合には、図９のステップＳ９５に復帰し、次のパケットに対する処理を行うことになる。
【０１３１】
以上の結果、この変形例によれば、暗号化を解除する鍵情報を有しなくても、暗号化したユーザが認めた最高解像度レベルでの非スクランブル再生が行えるようになり、少なくともオリジナル画像そのものとはいかないまでも、許容された範囲内で最高画質を閲覧することが可能になる。
【０１３２】
なお、上記例では、暗号化されているか否かは、終端マーカの直後に、暗号化されているか否かの情報を付加し、それを識別することで行うものとして説明したが、ＪＰＥＧ２０００では、通常、終端マーカを使うことが少ない。従って、終端マーカが存在するか否かで判定するようにしてもよい。この場合、終端マーカが存在すれば、暗号化が行われ、尚且つ、非スクランブル再生モードが設定されると見なすことになるであろう。
【０１３３】
＜第２の実施形態＞
上記実施形態（第１の実施形態及びその変形例）においては、図４に示したように暗号化をコードブロック単位で行うようにしたが、本発明はこれに限定されることなく、入力されたコードストリームを構成する種々の論理単位毎や、階層構造毎に暗号化をするようにすることも可能であることは明らかである。
【０１３４】
ここで、論理単位としては、パケット、タイルパート、タイル、コードストリーム、及びこれらの組み合わせなどを適応可能である。また、階層構造としては、解像度レベル、レイヤ、プレシンクト、コンポーネント、及びこれらの組み合わせなどを適応可能である。更に、階層構造毎に暗号化が施された場合には、メインヘッダ、タイルパートヘッダ、或いはパケットヘッダなどに、「どの階層構造が暗号されているか」ということを特定する情報を記録するようにしておく。
【０１３５】
これらの論理単位や階層構造ごとに暗号化が施された場合でも、第１の実施形態に示したように、非スクランブル再生モードの場合は、暗号化が施された論理単位や階層構造に含まれる全てのコードブロック内の暗号文の前に終端マーカを付与するようにすることによって、非スクランブル再生モードとすることが可能である。
【０１３６】
また、前述したように、論理単位毎や階層構造毎に暗号化を施した場合には、当該暗号化されている論理単位や階層構造を特定し、特定された論理単位や解像構造の暗号を復号するようにすればよい。
【０１３７】
＜第３の実施形態＞
上記第１、第２の実施形態においては、図１に示したように暗号化処理部への入力は既に圧縮符号化された後のコードストリームであった。これは、圧縮符号化処理の実行と暗号化処理の実行を夫々独立な処理とし、一旦、圧縮符号化処理を実行した後に暗号化処理を実行するような構成とするものである。つまり、画像圧縮符号化は既存のアプリケーション等で行い、暗号化処理をそれとは独立したものとするのに都合が良い。
【０１３８】
同様に、図８に示したように暗号復号部からの出力もコードストリームであった。これは、暗号復号処理と圧縮復号処理とをそれぞれ独立にし、圧縮復号ｓ取りを既存のアプリケーションで行うのに都合が良いものと言える。

【０１３９】
しかしながら本発明はこれに限定されることなく、圧縮符号化処理と暗号化処理とを同じアプリケーションとして実行、或いは、暗号符号化処理と圧縮復号処理を同じアプリケーションとして実行するような構成とすることも可能である。
【０１４０】
まずはじめに、図１８を用いて本実施の形態における画像圧縮処理と暗号化処理部の構成を説明する。
【０１４１】
図１８において、１８１は画像発生部（ＣＣＤスキャナやデジタルカメラ等のデバイスから画像データ入力するユニット）、１８２は離散ウェーブレット変換部、１８３は量子化部、１８４はエントロピ符号化部、１８５は暗号化部、１８６はコードストリーム出力部である。
【０１４２】
画像発生部１８１、離散ウェーブレット変換部１８２、量子化部１８３、エントロピ符号化部１８４、及びコードストリーム出力部１８６の動作は、夫々、前述した図１１における、画像発生部１１１、離散ウェーブレット変換部１１２、量子化部１１３、エントロピ符号化部１１４、及びコードストリーム出力部１１５の動作と同様の動作であるので詳細な説明は省略する。ただし、ウェーブレット変換する多少のタイル数、変換回数、量子化部での量子化ステップ等がユーザの設定に応じて処理される。
【０１４３】
本実施形態では、エントロピ符号化部１８４においてエントロピ復号されたビットストリームに対して、暗号化部１８５において暗号化処理が実行される。暗号化処理の対象は第２の実施形態に示したように、種々の論理単位や階層構造に対応するビットストリームを選択可能である。また、非スクランブル再生モードの場合には、当該暗号化された論理単位や階層構造に含まれる全てのコードブロック内の暗号文の前に終端マーカを付与するようにすることによって、非スクランブル再生モードとすることが可能である。
【０１４４】
尚、本実施形態ではエントロピ符号化部１８４の後に暗号化部１８５が続く構成例を説明した。これは、暗号化部１８５でエントロピ復号されたビットストリームを暗号化の対象とするものである。しかしながら、本発明はこれに限定されることなく、量子化部１８３、離散ウェーブレット変換部１８２、或いは画像発生部１８１の後に暗号化部１８５が続く構成とすることも可能であるであることは明らかである。
【０１４５】
暗号化部１８５が量子化部１８３の後に続く場合には量子化インデックス（或いは、量子化インデックスを構成するビット列）が暗号化対象となる。また、離散ウェーブレット変換部１８２の後に続く場合には離散ウェーブレット変換係数（或いは、離散ウェーブレット変換係数を構成するビット列）が暗号化対象となる。更に、画像発生部１８１の後に続く場合には画素（或いは、画素を構成するビット列）が暗号化対象となる。
【０１４６】
なお、上記の処理を行う場合、生の画像データ（非圧縮の画像データ）を指定することになるので、暗号化対象ファイルは非圧縮の画像（例えば拡張子がＢＭＰ）が選択可能になる。従って、この場合のＧＵＩの例は、図２１のようになる。また、また、ＪＰＥＧ２０００では、１つの画像に対して複数のタイルを設定できるので、図２０の画面にはタイル数の設定の入力欄□×□（デフォルトで１×１＝１画像１タイル）を設け、更に、ウェーブレット変換回数をユーザが指定できるようにする。
【０１４７】
図２１の場合、タイル数を２×２としているので、先ず、タイルを選択し、その中で暗号化対象を第１の実施形態と同様に設定することになる。なお、タイルそのものをも圧縮させることも可能であるので、図示の設定ウインドウ２０８には、タイル全体（２×２の１つ）について暗号化させることも可能とした。従って、オリジナル画像中の所望とする位

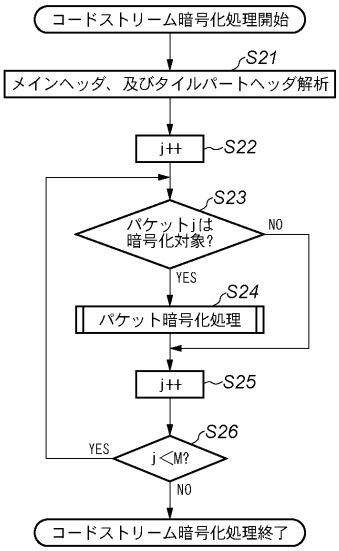
置の、所望とする解像度について暗号化させることも可能となる。
【０１４８】
次に、図１９を用いて本実施形態における暗号復号処理部の構成を説明する。
【０１４９】
図１９において、１９１はコードストリーム入力部、１９２は暗号復号部、１９３はエントロピ復号部、１９４は逆量子化部、１９５は逆離散ウェーブレット変換部、１９６は画像データ出力部である。
【０１５０】
コードストリーム入力部１９１、エントロピ復号部１９３、逆量子化部１９４、逆離散ウェーブレット変換部１９５、及び画像データ出力部１９６の動作は、夫々、前述した図１５における、コードストリーム入力部１５１、エントロピ復号部１５２、逆量子化部１５３、逆離散ウェーブレット変換部１５４、及び画像出力部１５５と同様の動作であるので詳細な説明は省略する。
【０１５１】
本実施形態では、コードストリーム入力部１９１において入力されたビットストリームに対して、暗号復号部１９２において暗号復号処理が実行される。暗号復号処理の対象は第２の実施形態に示したように、種々の論理単位や階層構造に対応するビットストリームである。
【０１５２】
尚、本実施形態ではコードストリーム入力部１９１の後に暗号復号部１９２が続く構成例を説明した。これは、暗号復号部１９２で入力された暗号化されたビットストリームを暗号復号の対象とするものである。しかしながら、本発明はこれに限定されることなく、エントロピ復号部１９３、逆量子化部１９４、逆離散ウェーブレット変換部１９５の後に暗号復号部１９２が続く構成とすることも可能であることは明らかである。
【０１５３】
暗号復号部１９２がエントロピ復号部１９３の後に続く場合には暗号化された量子化インデックス（或いは、量子化インデックスを構成するビット列）が暗号復号の対象となる。また、逆量子化部１９４の後に続く場合には暗号化された離散ウェーブレット変換係数（或いは、離散ウェーブレット変換係数を構成するビット列）が暗号復号の対象となる。更に、逆離散ウェーブレット変換部１９５の後に続く場合には暗号化された画素（或いは、画素を構成するビット列）が暗号復号の対象となる。
【０１５４】
以上、本発明に係る実施形態を説明した。実施形態では、ＪＰＥＧ２０００を例にして説明したが、上記実施形態で説明した終端マーカ或いはそれと等価の意味を持つ終端情報を有する画像データであれば適用可能なので、上記実施形態で本願発明が限定されるものではない。また、暗号化対象は伝送効率の点で圧縮符号化されていて、尚且つ、階層構造を持つ、或いは、それに類する圧縮符号化データ（例えばＪＰＥＧ）等であることが望ましいが、これは好適な例であって、必須のものではない。
【０１５５】
また、実施形態での説明から明らかなように、装置１４１、１４２はパーソナルコンピュータ等の汎用情報処理装置上で動作するプログラムでもって実現できるわけであるから、本願発明はかかるコンピュータプログラムをもその範疇するのは明らかである。更にまた、通常コンピュータプログラムは、ＣＤＲＯＭ等のコンピュータ可読記憶媒体に記録され、それをコンピュータにセットすることで、システムにコピーもしくはインストールすることで実行可能になるわけであるから、本発明はかかるコンピュータ可読記憶媒体をもその範疇とするのは明らかである。
【０１５６】
【発明の効果】
以上説明したように本発明によれば、画像再生装置でスクランブルさせて再生させるか、或いは、非スクランブル状態で再生させるかを暗号化する側で設定可能となる。

【図面の簡単な説明】
【図１】実施形態における暗号化処理部の構成を示す図である。
【図２】図１におけるコードストリーム暗号化部の処理手順を示すフローチャートである。
【図３】実施形態におけるコードストリームのデータフォーマットを示す図である。
【図４】図２におけるパケット暗号化処理の詳細を示すフローチャートである。
【図５】終端マーカの配置位置の一例を示す図である。
【図６】実施形態における暗号化後のコードブロックのデータフォーマットを示す図である。
【図７】実施形態における暗号化処理と、その再生例との対応関係を示す図である。
【図８】実施形態における暗号復号処理部の構成を示す図である。
【図９】図８におけるコードストリーム暗号復号処理部の処理手順を示すフローチャートである。
【図１０Ａ】図９におけるパケット復号処理の処理手順の詳細を示すフローチャートである。
【図１０Ｂ】図９におけるパケット復号処理の他の処理手順の詳細を示すフローチャートである。
【図１１】実施形態における画像圧縮符号化処理を行う際の構成を示す図である。
【図１２】図１１における離散ウェーブレット変換部の構成とその動作を説明するための図である。
【図１３】図１１におけるエントロピー符号化部の処理内容を説明するための図である。
【図１４】実施形態におけるシステム全体の構成を示す図である。
【図１５】実施形態における圧縮符号化データの復号処理を行う際の構成を示す図である。
【図１６】図１５におけるエントロピー復号部の処理内容を説明するための図である。
【図１７】図１５における逆離散ウェーブレット変換部の構成とその動作を説明するための図である。
【図１８】第３の実施形態における画像圧縮・暗号化装置のブロック構成図である。
【図１９】第３の実施形態における暗号復号・圧縮画像復号装置のブロック構成図である。
【図２０】実施形態における暗号化処理におけるユーザインタフェースとなる設定ウインドウの一例を示す図である。
【図２１】第３の実施形態における暗号化処理におけるユーザインタフェースとなる設定ウインドウの一例を示す図である。

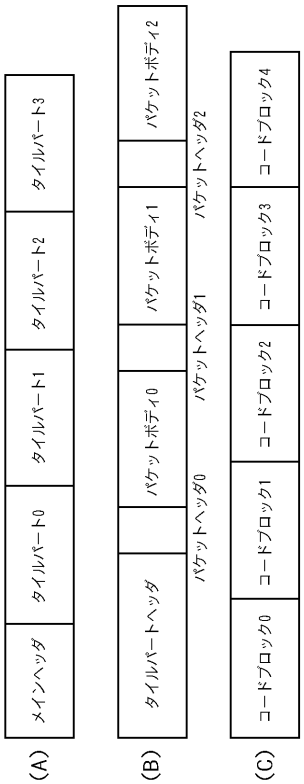
【図１】



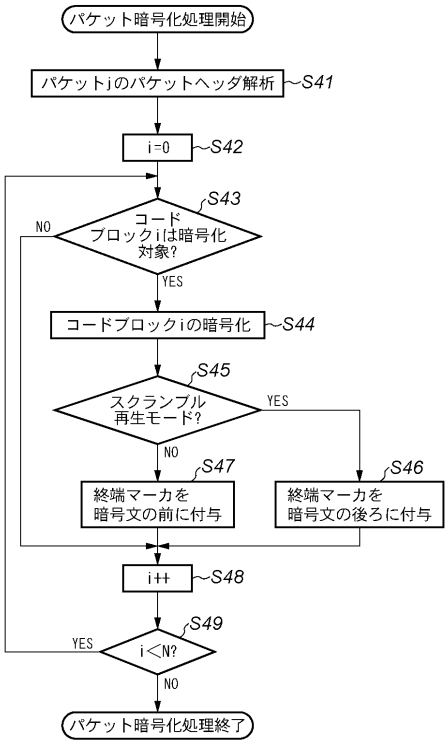
【図２】



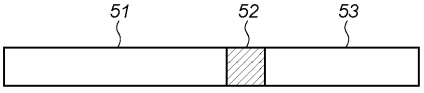
【図３】



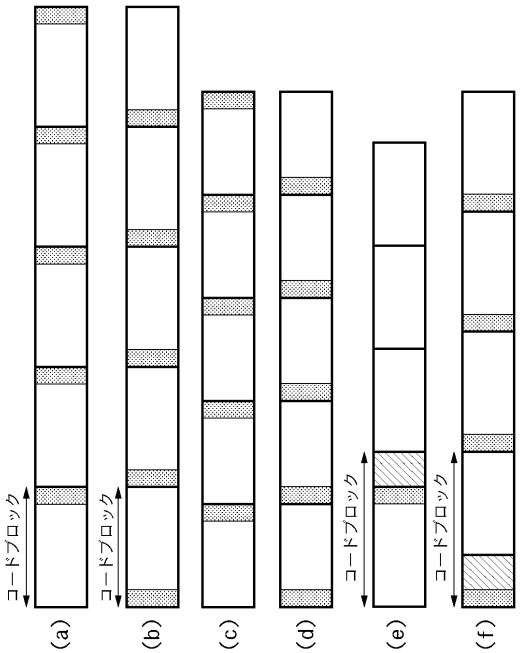
【図４】



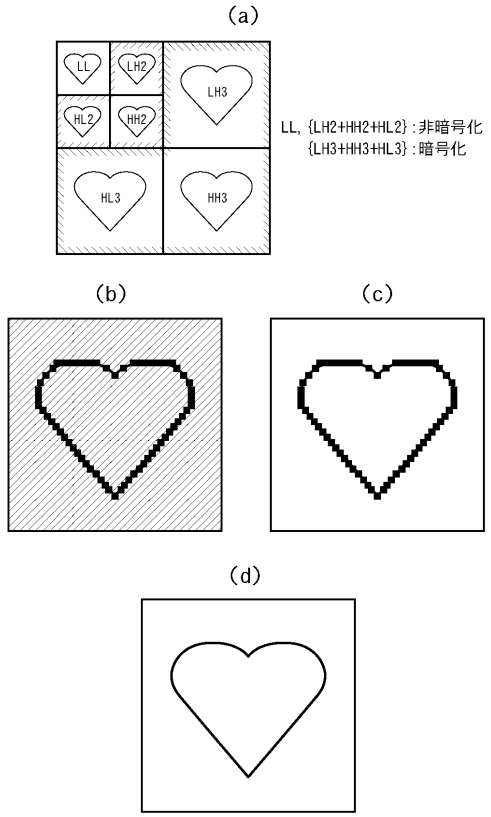
【図５】



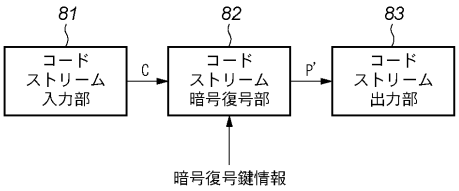
【図６】



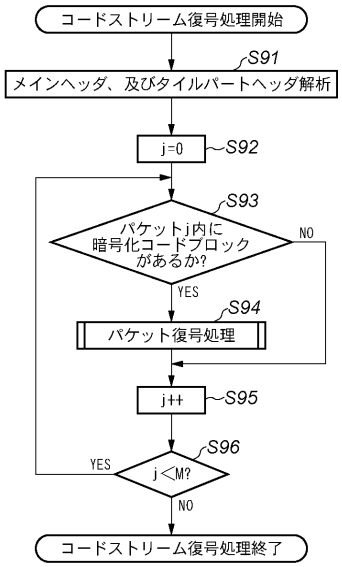
【図７】



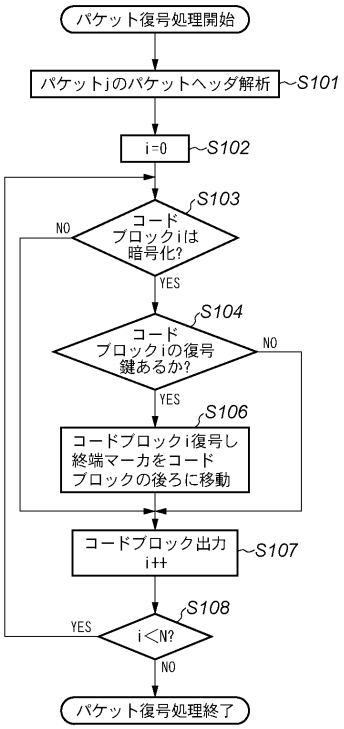
【図８】



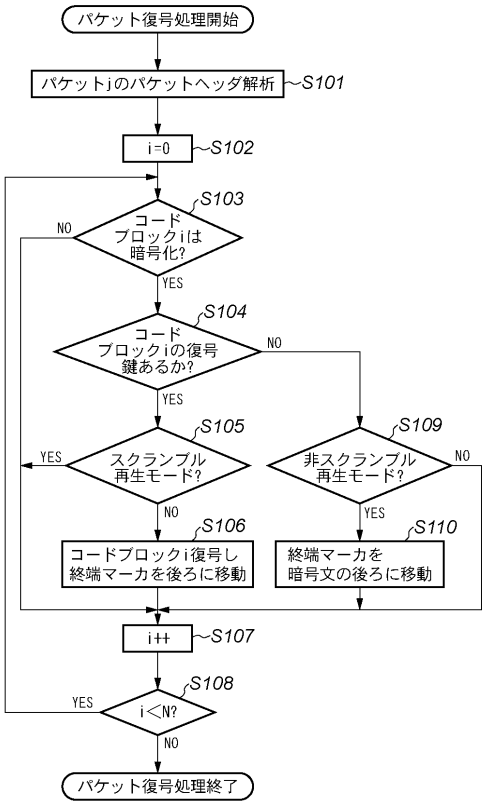
【図９】



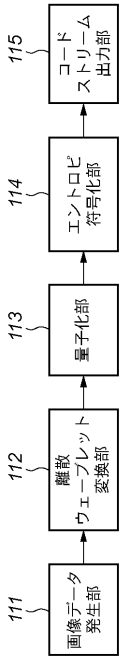
【図１０Ａ】



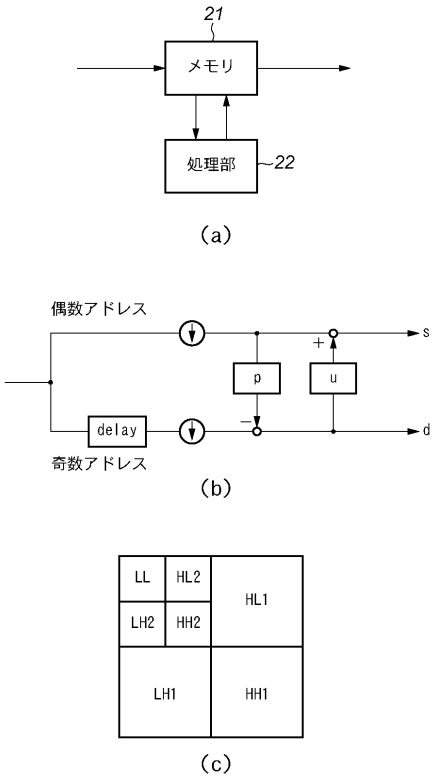
【図１０Ｂ】



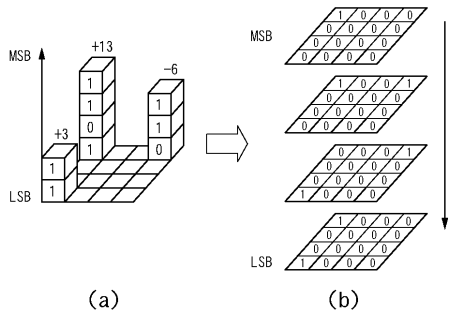
【図１１】



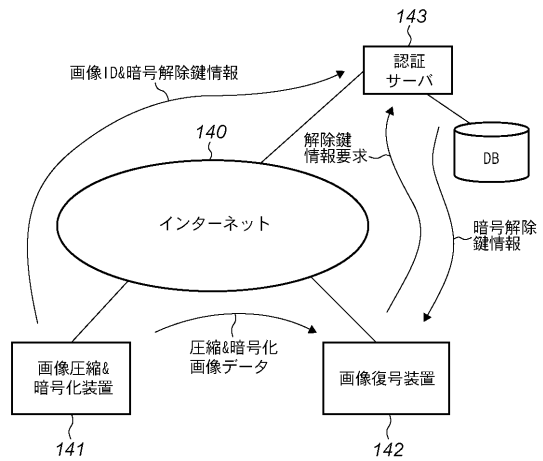
【図１２】



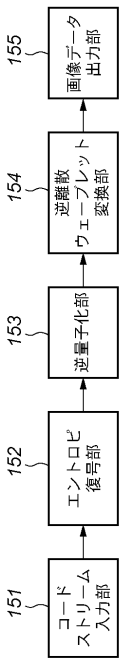
【図１３】



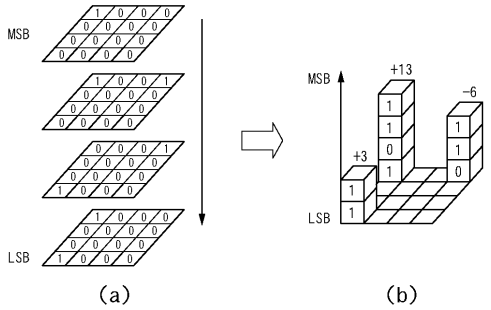
【図１４】



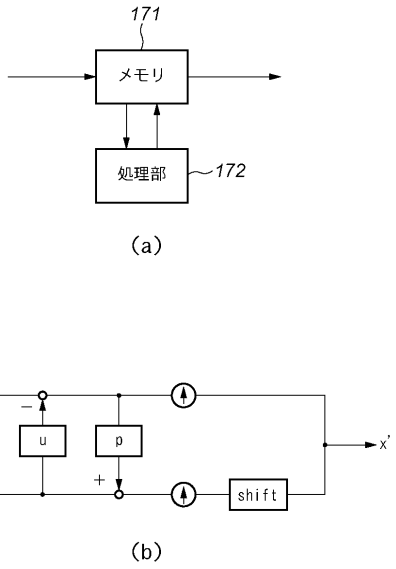
【図１５】



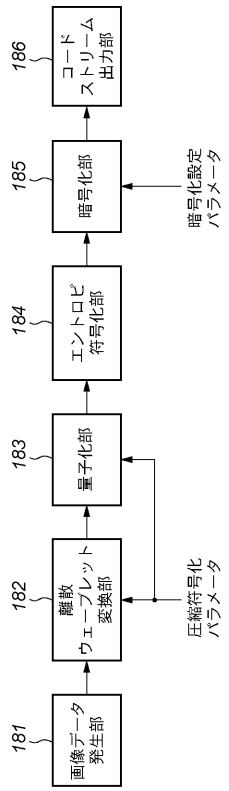
【図１６】



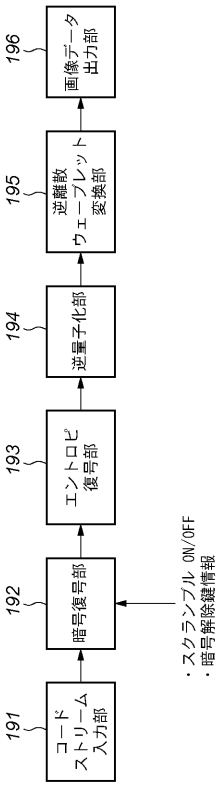
【図１７】



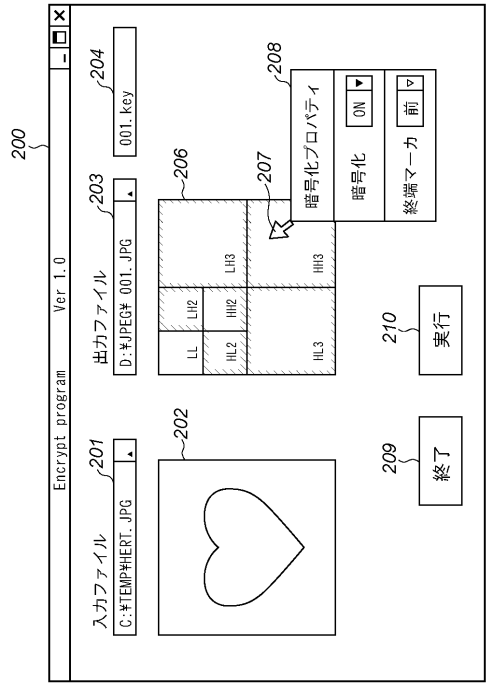
【図１８】



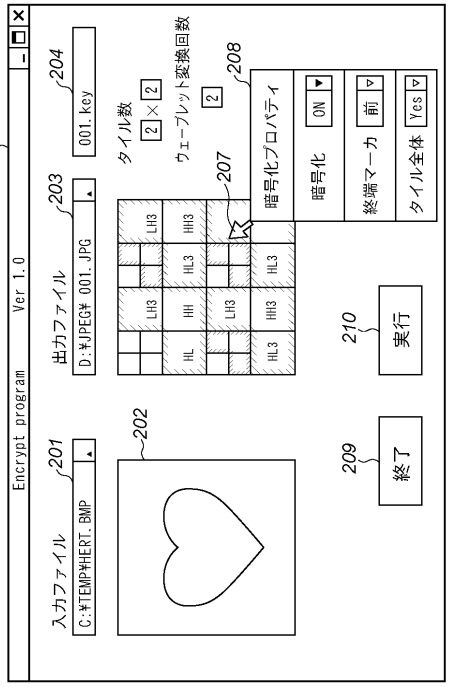
【図１９】



【図２０】


200
Encrypt program Ver 1.0
入力ファイル
C:¥TEMP¥HERT.JPG
201
202
出力ファイル
D:¥JPEG¥ 001.JPG
203
001.key
204
206
LL
LH2
HL2
HH2
LH3
HL3
HH3
207
208
暗号化プロパティ
暗号化
ON
終端マーカ
前
209
終了
210
実行

【図２１】


200
Encrypt program Ver 1.0
入力ファイル
C:¥TEMP¥HERT.BMP
201
202
出力ファイル
D:¥JPEG¥ 001.JPG
203
001.key
204
タイル数
2 × 2
ウェーブレット変換回数
2
207
208
暗号化プロパティ
暗号化
ON
終端マーカ
前
タイル全体
Yes
209
終了
210
実行

フロントページの続き

審査官　青木　重徳

(56)参考文献　特開平１１－０７５１７８（ＪＰ，Ａ）
特表２００２－５３９５４５（ＪＰ，Ａ）
特開平１１－３３１６１８（ＪＰ，Ａ）
特開平１１－３４１２９１（ＪＰ，Ａ）
安藤勝俊，渡邊修，貴家仁志，“ＪＰＥＧ２０００に基づく静止画像の情報半開示方式”，電子情報通信学会技術研究報告，日本，社団法人電子情報通信学会，２０００年１０月１６日，Ｖｏｌ．１００，Ｎｏ．３８８，ｐ．２９－３５
安藤勝俊，渡邊修，貴家仁志，“レイヤー構造を利用したＪＰＥＧ２０００符号化画像の効果的暗号化法”，電子情報通信学会技術研究報告，日本，社団法人電子情報通信学会，２００１年１１月１５日，Ｖｏｌ．１０１，Ｎｏ．４５６，ｐ．７－１４
安藤勝俊，渡邊修，貴家仁志，“ＪＰＥＧ２０００符号化画像の情報半開示法”，電子情報通信学会論文誌　Ｄ－ＩＩ，日本，社団法人電子情報通信学会，２００２年　２月　１日，Ｖｏｌ．Ｊ８５－Ｄ－ＩＩ，Ｎｏ．２，ｐ．２８２－２９０
安藤勝俊，渡邊修，貴家仁志，“伝送路誤りを考慮したＪＰＥＧ２０００画像の暗号化法”，電子情報通信学会技術研究報告，日本，社団法人電子情報通信学会，２００１年　１月２３日，Ｖｏｌ．１００，Ｎｏ．６０６，ｐ．６７－７１

(58)調査した分野(Int.Cl.，ＤＢ名)

H04L　9/16
H03M　7/30
H04N　1/41
H04N　1/44
H04N　7/30