(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第4261724号
(P4261724)
(45)発行日　平成21年4月30日(2009.4.30)　(24)登録日　平成21年2月20日(2009.2.20)

(51)Int.Cl.　F I
H04N 1/387 (2006.01)　H04N 1/387

請求項の数 16　(全 35 頁)

(21)出願番号	特願2000-57077(P2000-57077)	(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
(22)出願日	平成12年3月2日(2000.3.2)	(74)代理人	100090538 弁理士　西山　恵三
(65)公開番号	特開2000-324334(P2000-324334A)	(74)代理人	100096965 弁理士　内尾　裕一
(43)公開日	平成12年11月24日(2000.11.24)	(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
審査請求日	平成19年3月2日(2007.3.2)	(72)発明者	岩村　恵市 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
(31)優先権主張番号	特願平11-63174		
(32)優先日	平成11年3月10日(1999.3.10)		
(33)優先権主張国	日本国(JP)		

審査官　渡辺　努

最終頁に続く

(54)【発明の名称】署名データ生成装置及び画像検証装置

(57)【特許請求の範囲】

【請求項１】

署名データ生成装置であって、

ディジタル画像データを生成するディジタル画像データ生成手段と、

前記署名データ生成装置を識別するための情報と、前記署名データ生成装置に接続された外部装置を識別するための情報とを用いて、秘密情報を生成する秘密情報生成手段と、

前記ディジタル画像データと、前記秘密情報とを用いて、所定の演算を行う演算手段と、

前記所定の演算の結果を用いて、前記ディジタル画像データに対する不正な処理を検出するための署名データを生成する署名データ生成手段と

を有することを特徴とする署名データ生成装置。

【請求項２】

前記演算手段は、前記ディジタル画像データと、前記秘密情報とを用いて、逆演算可能な演算を行うことを特徴とする請求項１に記載の署名データ生成装置。

【請求項３】

前記署名データ生成手段は、逆演算の困難な演算を用いて前記署名データを生成することを特徴とする請求項１又は２に記載の署名データ生成装置。

【請求項４】

前記逆演算の困難な演算は、ハッシュ関数を用いた演算であることを特徴とする請求項３に記載の署名データ生成装置。

【請求項５】
前記逆演算の困難な演算は、共通鍵暗号を実現する演算であることを特徴とする請求項３に記載の署名データ生成装置。
【請求項６】
前記所定の演算が行われる前に、前記ディジタル画像データを圧縮する圧縮手段をさらに有することを特徴とする請求項１から５のいずれか１項に記載の署名データ生成装置。
【請求項７】
前記署名データ生成装置は、撮像機能を有する電子機器であることを特徴とする請求項１から６のいずれか１項に記載の署名データ生成装置。
【請求項８】
前記ディジタル画像データと、前記署名データとを外部装置に送信する送信手段をさらに有することを特徴とする請求項１から７のいずれか１項に記載の署名データ生成装置。
【請求項９】
前記ディジタル画像データと、前記署名データとを記録媒体に記録する記録手段をさらに有することを特徴とする請求項１から８のいずれか１項に記載の署名データ生成装置。
【請求項１０】
画像検証装置であって、
ディジタル画像データと、前記ディジタル画像データに対する不正な処理を検出するための第１の署名データとを入力手段と、
前記ディジタル画像データ及び前記第１の署名データを生成した署名データ生成装置を識別するための情報と、前記画像検証装置に接続された外部装置を識別するための情報とを用いて、秘密情報を生成する秘密情報生成手段と、
前記ディジタル画像データと、前記秘密情報とを用いて、所定の演算を行う演算手段と、
前記所定の演算の結果を用いて、前記ディジタル画像データに対する不正な処理を検出するための第２の署名データを生成する署名データ生成手段と、
前記第１の署名データと、前記第２の署名データとを用いて、前記ディジタル画像データに不正な処理がされているか否かを判定する判定手段と
を有することを特徴とする画像検証装置。
【請求項１１】
前記演算手段は、前記ディジタル画像データと、前記秘密情報とを用いて、逆演算可能な演算を行うことを特徴とする請求項１０に記載の画像検証装置。
【請求項１２】
前記署名データ生成手段は、逆演算の困難な演算を用いて前記第２の署名データを生成することを特徴とする請求項１０又は１１に記載の署名データ生成装置。
【請求項１３】
前記逆演算の困難な演算は、ハッシュ関数を用いた演算であることを特徴とする請求項１２に記載の画像検証装置。
【請求項１４】
前記逆演算の困難な演算は、共通鍵暗号を実現する演算であることを特徴とする請求項１２に記載の画像検証装置。
【請求項１５】
前記ディジタル画像データは、圧縮されたディジタル画像データであることを特徴とする請求項１０から１４のいずれか１項に記載の画像検証装置。
【請求項１６】
前記判定手段の判定結果を表示する表示手段をさらに有することを特徴とする請求項１０から１５のいずれか１項に記載の画像検証装置。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】

本発明は、ディジタル画像データに対する不正な処理を検出するための技術に関する。
【０００２】
【従来の技術】
近年、撮影した画像を従来の銀塩写真や８ｍｍフィルムに記録するのではなく、ディジタルデータとして記録媒体に記録する画像入力装置（例えば、デジタルカメラ）が実用化されている。
【０００３】
【発明が解決しようとする課題】
ところが、通常、ディジタルデータは、アナログデータと異なり加工が容易で、修正、改竄、偽造、合成等を簡単に行うことができる。このため、ディジタルデータは、銀塩写真等と比較して信憑性が低く、証拠能力に乏しいという問題があった。
【０００４】
このような問題を解決するために、ディジタルデータに対する修正、改竄、偽造、合成等を検出するための技術が提案されている。例えば、この技術の一例として、ハッシュ関数と公開鍵暗号方式とを組み合わせたシステムが提案されている。
【０００５】
以下、図２８を用いて従来のシステムを説明する。公開鍵暗号方式とは、暗号鍵と復号鍵とが異なり、暗号鍵を公開し、復号鍵を秘密に保持する方式である。
【０００６】
まず、送信側（出力側）の構成と動作について説明する。
▲１▼ディジタルデータＭをハッシュ関数Ｈを用いて圧縮し、一定長の出力ｈを演算する。
▲２▼暗号鍵Ｋｅを用いて上述のｈを暗号化し、出力ｓを求める。この出力ｓをディジタル署名データと呼ぶ。
▲３▼出力回路は、ディジタル署名データｓとディジタルデータＭとを一組として出力する。
【０００７】
次に、受信側（検出側）構成と動作について説明する。
▲４▼ディジタルデータＭとそれに対応するディジタル署名データｓとを入力する。
▲５▼ディジタル署名データｓを暗号鍵Ｋｅに対応する復号鍵Ｋｄで復号し、出力ｈ''を生成する。
▲６▼ディジタルデータＭを送信側と同じハッシュ関数Ｈを用いて演算し、出力ｈ'を求める。
▲７▼比較回路は、▲５▼で求めた出力ｈ''と▲６▼で求めた出力ｈ'とを比較し、一致すれば入力されたディジタルデータＭを不正な処理のされていない正当なデータであると判断し、不一致であれば不正な処理のされたデータと見なす。
【０００８】
このように従来のシステムでは、ハッシュ関数Ｈと暗号鍵Ｋｅとにより生成したディジタル署名データｓを用いて、ディジタルデータＭに対する修正、改竄、偽造、合成等を検出していた。
【０００９】
しかしながら、上述のシステムには次のような問題がある。
【００１０】
まず、公開鍵暗号方式の暗号化回路及びその復号化回路は、回路構成が複雑であり、小型化が難しいという問題がある。また、それらの回路の演算量は膨大であり、処理時間が長くなるという問題もある。特に、公開鍵暗号方式は、べき乗演算と剰余演算とが必要であり、共通鍵暗号方式（暗号鍵と復号鍵とが同一となる暗号方式）に比べて演算が複雑且つ膨大となるため、処理速度の高速化が大変難しい。つまり、従来のシステムでは、処理速度の高速化とシステムの小型化の双方を両立させることは難しいという問題がある。
【００１１】

又、処理速度を早くするためには、より高性能のＣＰＵ（中央演算処理装置）とより大容量のメモリとを用いて、ハードウェアの性能を向上させる必要がある。しかしながら、このような構成では、システム全体の大規模化やコストアップを招くだけであり、安価で小型で高速なシステムをユーザに提供することはできない。

【００１２】

そこで、本発明は、ディジタル画像データに対する不正な処理（改竄、偽造等）を、簡単な構成で、安価に且つ安全に検出することのできる署名データ生成装置及び画像検証装置を提供することを目的とする。

【００１３】

【課題を解決するための手段】

上述のような目的を達成するために、本発明に係る署名データ生成装置は、署名データ生成装置であって、ディジタル画像データを生成するディジタル画像データ生成手段と、前記署名データ生成装置を識別するための情報と、前記署名データ生成装置と接続可能な外部装置を識別するための情報とを用いて、秘密情報を生成する秘密情報生成手段と、前記ディジタル画像データと、前記秘密情報とを用いて、所定の演算を行う演算手段と、前記所定の演算の結果を用いて、前記ディジタル画像データに対する不正な処理を検出するための署名データを生成する署名データ生成手段とを有することを特徴とする。

【００１４】

本発明に係る画像検証装置は、画像検証装置であって、ディジタル画像データと、前記ディジタル画像データに対する不正な処理を検出するための第１の署名データとを入力手段と、前記ディジタル画像データ及び前記第１の署名データを生成した署名データ生成装置を識別するための情報と、前記画像検証装置に接続された外部装置を識別するための情報とを用いて、秘密情報を生成する秘密情報生成手段と、前記ディジタル画像データと、前記秘密情報とを用いて、所定の演算を行う演算手段と、前記所定の演算の結果を用いて、前記ディジタル画像データに対する不正な処理を検出するための第２の署名データを生成する署名データ生成手段と、前記第１の署名データと、前記第２の署名データとを用いて、前記ディジタル画像データに不正な処理がされているか否かを判定する判定手段とを有することを特徴とする。

【００２３】

【発明の実施の形態】

以下、本発明に係る署名データ生成装置及び画像検証装置について図面を用いて詳細に説明する。

【００２４】

（基本構成）

まず、図１を用いて、各実施例に共通するディジタル画像検証システムの基本構成と処理手順とについて説明する。このシステムは、ディジタル画像データからディジタル署名データを生成するディジタル画像入力装置１０と、そのディジタル署名データを用いてディジタル画像データに対する不正な処理を検出する画像検証装置２０とからなる。各装置は、ネットワーク（例えば、インターネット、電話回線網、移動体通信網等）、各機器に共通のディジタルインタフェース、取り外し可能な記憶媒体（例えば、光ディスク、磁気ディスク、光磁気ディスク、半導体メモリ等）を介して接続される。

【００２５】

尚、図１において、画像入力装置１０と画像検証装置２０とは、同一の秘密情報Ｓ１２を共有する。この秘密情報Ｓ１２は、読み出し専用の記録媒体等に記録され、外部に漏れることがないように管理する。

【００２６】

まず、画像入力装置１０は、ディジタル画像データＰ１１と秘密情報Ｓ１２とに基づいて、ディジタル署名データｈ１３を生成する。具体的に説明すると、画像入力装置１０は、秘密情報Ｓ１２を用いてディジタル画像データＰ１１に所定の操作（例えば、付加、多重、或いは合成）を加えた後、その結果を一方向性関数（例えば、ハッシュ関数等の逆関数

の生成が困難或いは不可能な関数）で演算し、その演算結果からディジタル署名データｈ１３を生成する。このディジタル署名データｈ１３は、対応するディジタル画像データＰ１１と共に一時的に記録され、必要に応じて外部出力される。

【００２７】

このような処理によって得られたディジタル署名データｈ１３は、ディジタル画像データＰ１１と秘密情報Ｓ１２とに対して固有の情報となる。従って、秘密情報Ｓ１２と所定の操作とを知らなければ、ディジタル画像データＰ１１に対応するディジタル署名データｈ１３を不正に作り出すことはできないため、ディジタル署名データｈ１３に基づいてディジタル画像データＰ１１の正当性を安全に検証することができる。又、一方向性関数の性質により、ディジタル署名データｈ１３から元のデータ（即ち、秘密情報Ｓ１２を用いて所定の操作を加えたディジタル画像データＰ１１）を知ることもできないため、ディジタル署名データｈ１３に基づいてディジタル画像データＰ１１の正当性（或いは、完全性（integrity）ともいう）を安全に検証することができる。

【００２８】

次に、画像検証装置２０は、ディジタル画像データＰ'２１と共にディジタル署名データｈ'２３を外部入力する。画像検証装置２０は、ディジタル画像データＰ'２１と秘密情報Ｓ２２（上述の秘密情報Ｓ１２と同一の情報である）とを用いて画像入力装置１０と同様の処理を行い、ディジタル署名データｈ''２４を生成する。

【００２９】

このディジタル署名データｈ''２４は、ディジタル画像データＰ'２１と共に外部入力されたディジタル署名データｈ'２３と比較される。両者が一致した場合、画像検証装置２０は、ディジタル画像データＰ'２１を正当なデータであると判断する。一方、ディジタル画像データＰ'２１が外部入力される前に不正に処理されていた場合、両者は不一致となる。この場合、画像検証装置２０は、ディジタル画像データＰ'２１を不正に処理されたデータであると判断する。

【００３０】

このような手順により、画像検証処装置２０は、外部入力されたディジタル画像データＰ'２１に対して不正な処理（例えば、修正、改竄、偽造、合成等の改変処理）が施されているか否かを検出することができる。

【００３１】

以上のように、本実施例では、公開鍵暗号方式のような複雑な暗号化技術を用いることなく、簡単で安価な回路構成と少ない演算量で高速にディジタル署名データを生成することができる。そして、このディジタル署名データにより、ディジタル画像データの著作権を保護し、該ディジタル画像データに対する不正な処理（修正、改竄、偽造、合成等の改変処理）を確実に検出することができる。

【００３２】

次に、図２に示す画像入力装置１０及び画像検証装置２０の基本的な構成について詳細に説明する。

【００３３】

（１）画像入力装置の構成

図２は、画像入力装置１０の構成の一例を示す図である。ここで、画像入力装置１０は、デジタルカメラ、カメラ一体型デジタルレコーダ、スキャナ等の撮像機能を有する電子機器である。

【００３４】

図２において、撮像部２０１は、ＣＣＤやレンズ等からなり、被写体の光学像を電気信号に変換し、その電気信号を更に所定フォーマットのディジタル画像データに変換する。作業用メモリ２０２は、ディジタル画像データ等を一時的に保管し、ディジタル画像データに対する高能率符号化処理、後述のディジタル署名データの生成等に使用される。

【００３５】

記録再生部２０３は、取り外し可能な記録媒体（例えば、光ディスク、磁気ディスク、光

磁気ディスク、半導体メモリ等）に、撮像部２０１により生成され、高能率符号化されたディジタル画像データとそれに対応するディジタル署名データとを一組として記録する。駆動部２０４は、撮像部２０１や記録再生部２０３の機械的動作を制御する。

【００３６】

外部インタフェース部２０５は、ネットワーク（例えば、インターネット、電話回線網、移動体通信網等）に接続可能なディジタルインタフェースであり、ディジタル署名データを付加したディジタル画像データを、所定の外部装置に送信する。

【００３７】

制御／演算部２０６は、ＲＯＭ２０７に格納されている各種のプログラムに従って画像入力装置１０全体の動作を制御する制御回路２１０、ディジタル画像データを高能率符号化する（例えば、ＤＣＴ変換やウェーブレット変換されたディジタル画像データを量子化し、可変長符号化する）画像処理回路２１１、後述のディジタル署名データの生成に必要なハッシュ関数演算や各種の演算処理を行う演算回路２１２、ディジタル署名データの生成に必要な秘密情報（例えば、画像入力装置１０を識別するためのＩＤ情報等）を格納するメモリ２１３、演算回路２１２に必要な乱数を生成する乱数発生回路２１４を含む。

【００３８】

ＲＯＭ２０７は読み出し専用メモリであり、画像入力装置１０全体の動作を制御するプログラム、画像処理を制御するプログラム、ディジタル署名データの生成処理を制御するプログラム等を格納している。操作部２０８は、ユーザからの各種の指示を受け付け、その指示に対応する制御信号を制御／演算部２０６に供給する。

【００３９】

（２）画像検証装置の構成

図３は、画像検証装置２０の構成の一例を示す図である。ここで、画像検証装置２０は、パーソナルコンピュータ、ワークステーション等の情報処理装置やそれらに接続可能な拡張ボードである。

【００４０】

図３において、外部インタフェース部３０１は、ネットワークからディジタル署名データを付加したディジタル画像データ（ここで、ディジタル画像データは、高能率符号化されている）を入力するディジタルインタフェースである。又、外部インタフェース部３０１は、取り外し可能な記録媒体とも接続可能である。そして、その記録媒体に記録されたディジタル画像データをディジタル署名データと共に入力する。

【００４１】

作業用メモリ３０２は、ディジタル画像データ等を一時的に保管し、ディジタル画像データに対する伸長復号処理、後述のディジタル署名データの生成等に使用される。

【００４２】

制御／演算部３０３は、ＲＯＭ３０５に格納されている各種のプログラムに従って画像検証装置２０全体の動作を制御する制御回路３１０、ディジタル画像データを伸長復号する（例えば、可変長復号し、逆量子化した後、逆ＤＣＴ変換や逆ウェーブレット変換する）画像処理回路３１１、後述のディジタル署名データの生成に必要なハッシュ関数演算やディジタル画像データを検証するための演算処理を行う演算回路３１２、ディジタル署名データの生成に必要な秘密情報を格納するメモリ３１３、演算回路３１２に必要な乱数を生成する乱数発生回路３１４を含む。

【００４３】

表示部３０４は、ディジタル画像データを視覚的に表示する。又、表示部３０４は、そのディジタル画像データの検証結果をユーザに視覚的に表示する。尚、表示部３０４は、画像検証装置２０と取り外し可能である。

【００４４】

ＲＯＭ３０５は、読み出し専用メモリであり、画像検証装置２０全体の動作を制御するプログラム、画像処理を制御するプログラム、ディジタル画像データの検証処理を制御するプログラムを格納している。操作部３０６は、ユーザからの各種の指示を受け付け、その

指示に対応する制御信号を制御／演算部３０３に供給する。
【００４５】
以下、第１～第６の実施例では、図２の画像入力装置１０が、ディジタル画像データと秘密情報とに基づいて、ディジタル署名データを生成する手順について詳細に説明する。
【００４６】
又、第７～第１２の実施例では、図４の画像検証装置２０が、画像入力装置１０にて生成されたディジタル署名データに基づいて、ディジタル画像データの正当性を検証する手順について詳細に説明する。
【００４７】
（第１の実施例）
第１の実施例では、画像入力装置１０が、機器固有の秘密情報Ｓとハッシュ関数とを用いてディジタル署名データｈを生成する処理について説明する。具体的に説明すると、ディジタル画像データＰと秘密情報Ｓとを用いて予め定められた規則の演算を行い、ハッシュ関数を用いてその演算結果を演算し、その演算結果をディジタル画像データＰに対するディジタル署名データｈとする。
【００４８】
図４は、第１の実施例の処理手順を説明するフローチャートである。以下、図４を用いて、ディジタル署名データｈを生成する手順を説明する。
【００４９】
ステップＳ４０１において、操作部２０８は、ある被写体の光学像を撮像するか否かを指示する。撮像が指示された場合、制御／演算部２０６はステップＳ４０２を実行する。
【００５０】
ステップＳ４０２において、撮像部２０１は、被写体の光学像を電気信号に変換し、その電気信号を更に所定フォーマットのディジタル画像データＰを生成する。その後、ディジタル画像データＰは、作業用メモリ２０２に格納される。
【００５１】
ステップＳ４０３において、制御／演算部２０６（に含まれる画像処理回路２１１）は、作業用メモリ２０２に格納されたディジタル画像データＰを１画面分の静止画像毎に高能率符号化する。１つの静止画像を高能率符号化する手法として例えば、ＤＣＴ変換方式（具体的には、複数画素からなるブロック毎にＤＣＴ変換、量子化及び可変量符号化する方式）、ウェーブレット変換方式（具体的には、複数画素からなるブロック毎にウェーブレット変換、量子化及び可変長符号化する方式）、ＪＰＥＧ方式、ＪＢＩＧ方式、ＭＨ方式、ＭＭＲ方式、ＭＰＥＧ方式等を用いてもよい。尚、以下の実施例では、ＪＰＥＧ方式を用いて高能率符号化する場合について説明する。
【００５２】
ステップＳ４０４において、制御／演算部２０６は、画像入力装置１０の持つ秘密情報Ｓをメモリ２１３から読み出す。
【００５３】
ステップＳ４０５において、制御／演算部２０６（に含まれる演算回路２１２）は、上述の秘密情報Ｓと例えばＪＰＥＧ方式で高能率符号化されたディジタル画像データＰ（以下、ＪＰＥＧデータと称する）とを用いて、予め定められた規則に基づく所定の演算を行う。
【００５４】
ここで、秘密情報Ｓと所定の演算処理とについて説明する。
【００５５】
まず、秘密情報Ｓとは、画像入力機器１０の製造時に設定される機器固有の情報であり、一般に公開されることのない情報である。この秘密情報Ｓは、外部から容易に入手することができないように制御／演算部２０６の内部に組み込まれている。以下、第１の実施例では、上述の秘密情報Ｓを例えば“１１１１１１１１”として説明する。
【００５６】

次に、上述の所定の演算処理について図５を用いて説明する。所定の演算処理とは、あるＪＰＥＧデータ列から所定の位置のバイトデータを選択した後、そのバイトデータと秘密情報Ｓとをビット毎に排他的論理和演算し、そのバイトデータを別のデータに変換する処理のことである。ここで、所定の位置とは、ＪＰＥＧデータ列上の任意の位置に設定することができるが、第１の実施例では最上位のバイトデータを演算対象として説明する。

【００５７】

ステップＳ４０６において、制御／演算部２０６（に含まれる演算回路２１２）は、ハッシュ関数を用いて、所定の演算処理の施されたＪＰＥＧデータを演算し、ディジタル署名データｈを生成する。

【００５８】

ここで、ハッシュ関数について説明する。

【００５９】

ハッシュ関数Ｈとは、任意のビット長のディジタルデータＭから、一定のビット長となる出力ｈを生成する機能を持つ。この出力ｈは、ハッシュ値と呼ばれる（又は、ディジタル署名、メッセージダイジェスト、ディジタル指紋等とも呼ばれる）。通常、ハッシュ関数には、一方向性と衝突耐性とが要求される。一方向性とは、ハッシュ値ｈが与えられた際に、ｈ＝Ｈ（Ｍ）となるディジタルデータＭの算出が計算量的に困難であることを示す。又、衝突耐性とは、ディジタルデータＭが与えられた際に、Ｈ（Ｍ）＝Ｈ（Ｍ'）となるディジタルデータＭ'（Ｍ≠Ｍ'）の算出およびＨ（Ｍ）＝Ｈ（Ｍ'）且つＭ≠Ｍ'となるディジタルデータＭ、Ｍ'の算出が計算量的に困難であることを示す。ハッシュ関数には、ＭＤ－２、ＭＤ－４、ＭＤ－５、ＳＨＡ－１、ＲＩＰＥＭＤ－１２８、ＲＩＰＥＭＤ－１６０等の方式が知られている。第１の実施例では、ＭＤ－５方式を使用する例について説明する。尚、このＭＤ－５方式を用いて生成されるディジタル署名データのビット長は１２８ビットとなる。

【００６０】

ステップＳ４０７において、記録再生部２０３は、制御／演算部２０６にて生成されたディジタル署名データとそれに対応するディジタル画像データとを、取り外し可能な記録媒体に記録したり、ネットワークを介して他の機器に出力したりする。

【００６１】

尚、図４に示す一連の処理手順を制御するプログラムは、ＲＯＭ２０７に格納されている。このプログラムは、制御／演算部２０６（に含まれる制御回路２１０）によって読み出され、ユーザの撮像指示毎に起動される。これにより、ディジタル画像Ｐを撮像する毎に、それに対応したディジタル署名データｈを生成することができる。

【００６２】

以上説明したように第１の実施例では、高能率符号化されたディジタル画像データＰと画像入力装置１０に固有の秘密情報Ｓとを用いて所定の演算を行い、その演算結果をハッシュ関数で演算した結果が、ディジタル署名データｈとなる。このように構成することによって、第１の実施例では、安全性も信頼性も高いディジタル署名データｈを、従来のシステムに比べて非常に簡単な構成によって実現することができる。又、従来のシステムに比べて安価に構成することも、処理速度を高速化することもできる。

【００６３】

この結果、秘密情報Ｓと所定の演算とを知らなければ、ディジタル画像データＰに対応するディジタル署名データｈを不正に作り出すことはできないため、ディジタル署名データｈに基づいてディジタル画像データＰの正当性を安全に検証することができる。又、一方向性関数の性質により、ディジタル署名データｈから元のデータ（即ち、秘密情報Ｓを用いて所定の演算を行なったディジタル画像データＰ）を知ることもできないため、ディジタル署名データｈからディジタル画像データＰの正当性を安全に検証することができる。

【００６４】

尚、第１の実施例では、秘密情報Ｓを画像入力装置１０の製造時に設定された情報としたがそれに限るものではない。画像検証装置２０の秘密情報と共有できるものであれば、乱

数発生回路２１４が所定のアルゴリズムに基づいて生成したビット列でもよい。
【００６５】
又、第１の実施例では、上述の所定の演算処理の一例として、ＪＰＥＧデータのバイトデータと秘密情報とを排他的論理和演算する構成について説明したがそれに限るものではない。秘密情報Ｓを、高能率符号化されたディジタル画像データＰの一部に付加、合成、あるいは多重する処理で且つ逆演算可能な処理であれば、いかなる演算処理であってもよい。
【００６６】
又、第１の実施例では、ディジタル画像データＰとディジタル署名データｈとを同じタイミングで生成する手順について説明したがそれに限るものではない。ディジタル画像データＰを画像入力装置１０から外部へ出力する前に必ずディジタル署名データｈを生成する構成であれば、ディジタル署名データｈはどのタイミングで生成してもよい。例えば、ディジタル画像データＰを外部インタフェース２０５を介して外部に出力する場合には、一度記録媒体に格納した後、そのディジタル画像データＰを外部へ出力する前に、ディジタル署名データｈを生成するようにしてもよい。但し、ディジタル画像データＰを取り外し可能な記録媒体に記憶する場合には、上述の手順でディジタル署名データｈを生成する。
【００６７】
（第２の実施例）
第２の実施例では、第１の実施例に比べてより安全性の高いディジタル署名データｈを生成する手順について詳細に説明する。
【００６８】
図６は、第２の実施例の処理手順を説明するフローチャートである。以下、図６を用いて、ディジタル署名データｈを生成する手順を説明する。
【００６９】
ステップＳ６０１～Ｓ６０３の処理は、上述の第１の実施例のステップＳ４０１～Ｓ４０３と同様の処理としてその説明を省略する。
ステップＳ６０４において、制御／演算部２０６（に含まれる乱数発生回路２１４）は、所定の情報（例えば、高能率符号化されたディジタル画像データＰのデータ量）を基にして、ビット長ｍの乱数Ｒを生成する。この乱数Ｒが第２の実施例の秘密情報Ｓである。
【００７０】
次のステップＳ６０５～Ｓ６０６では、第２の実施例における所定の演算を説明する。
【００７１】
ステップＳ６０５において、制御／演算部２０６（に含まれる演算回路２１２）は、図７に示すように、１画像分のＪＰＥＧデータを所定の大きさ（例えば１２８ビット長）のブロックＤｉ（ｉ＝１，２，３…ｎ）に分割する。ここで、Ｄ１を最上位ブロックとする。ＪＰＥＧデータの総量が１２８の倍数にならない場合、１２８の倍数となるようにパディングする。例えば、図７に示すように、最後のブロックに“０００・・・０００”を付加する。
【００７２】
ステップＳ６０６において、制御／演算部２０６（に含まれる演算回路２１２）は、上述の乱数Ｒと上述のｎ個のブロックとを用いて以下に示す手順の演算を行う。
【００７３】
まず、制御／演算部２０６は、図８に示すように、乱数Ｒのビット数ｍをｎビット（図７に示すブロックＤｉの個数ｎと同じ）とする。例えば、ｍ≧ｎの場合、最上位ビットからｎビットまでのビット列を有効とし、それ以外のビット列を切り捨てる。又、ｍ＜ｎの場合、不足分のデータとして“１１１…１１１”を付加する。
【００７４】
次に、制御／演算部２０６は、図９に示すように、各ブロックＤ１～Ｄｎと各乱数Ｒ１～Ｒｎとを用いて所定の演算を行う。具体的に説明すると、乱数ＲのビットＲｉとブロックＤｉの最下位ビットとの間で排他的論理和演算を行い、その演算をｉ＝１～ｎまで繰り返

す。
【００７５】
ここで、ステップＳ６０６の演算は、乱数ＲｉとブロックＤｉの最下位ビットとの間の排他的論理和演算としたがそれに限るものではない。各ブロックＤｉの一部に秘密情報（ビット長ｍの乱数Ｒの一部）を付加、合成、多重する処理で且つ逆演算可能な処理であればいかなる演算処理であってもよい。
【００７６】
ステップＳ６０７において、制御／演算部２０６（に含まれる演算回路２１２）は、ステップＳ６０６の出力をハッシュ関数で演算し、ディジタル署名データｈを生成する。尚、第２の実施例では、第１の実施例と同様に、ＭＤ－５方式のハッシュ関数を用いる。従って、ディジタル署名データｈのビット長は、１２８ビットとなる。
【００７７】
ステップＳ６０７の演算処理の一例について詳細に説明する。
【００７８】
まず、制御／演算部２０６は、ステップＳ６０６の出力から１つまたは複数個のブロックＤを選択する。その後、制御／演算部２０６は、選択されたブロックをハッシュ関数で演算し、ディジタル署名データｈを生成する。
【００７９】
また、ステップＳ６０５～Ｓ６０７の演算処理の他の例について、図１０～１２を用いて詳細に説明する。
【００８０】
制御／演算部２０６は、後述する３つの動作モードの何れか１つ又はこれらの組み合わることによりハッシュ値を求める。特に、第１のモードや第３のモードでは、あるブロック（１ブロックは、ｋビット）の演算結果を用いて他のブロックのハッシュ値を求めるため、より安全性の高いディジタル署名データｈを生成することができる。又、前のブロックの演算結果が、次のブロックの演算結果に反映されるため、ブロック毎にＪＰＥＧデータの正当性を検証することもできる。
【００８１】
▲１▼第１のモード
第１のモードについて図１０を用いて説明する。図１０は、制御／演算部２０６の構成の一部を示す図である。
【００８２】
図１０において、演算回路２１２は、所定のビット単位でハッシュ関数演算を行うハッシュ関数回路１００１と、ハッシュ関数回路１００１の出力ｈの一部（Ｋビット）を記憶するレジスタ１００２と、ＪＰＥＧデータをＫビットのブロックに分割する演算回路１００３と、演算回路１００３の出力とレジスタ１００２の出力とを排他的論理和演算する演算回路１００４とから構成される。
【００８３】
ハッシュ関数回路１００１の出力である１２８ビットのハッシュ値ｈの一部（Ｋビット）は、レジスタ１００２に入力される。レジスタ１００２には、例えば、ハッシュ値ｈの上位６４ビットが一時的に格納される。
【００８４】
レジスタ１００２に格納されたＫビットは、１ブロックのＪＰＥＧデータと排他的論理和演算され、その演算結果はハッシュ関数回路１００１に供給される。
【００８５】
上述の演算は、所定のブロックに達するまで、各ブロックに対して繰り返される。そして、その所定のブロックから求めたハッシュ値がディジタル署名データとして出力される。
【００８６】
ここで、最初の演算では、レジスタ１００２に初期値を格納しておく必要がある。その初期値は、例えば図１３に示すように、乱数Ｒの下位Ｋビットを用いることができる。

【００８７】
尚、ブロックＤｉの大きさが６４の倍数とならない場合には、例えば後述の第３のモードと組合せて余りのビット列を演算するように構成してもよい。
【００８８】
▲２▼第２のモード
第２のモードについて図１１を用いて説明する。図１１は、制御／演算部２０６の構成の一部を示す図である。
【００８９】
図１１において、演算回路２１２は、所定のビット単位でハッシュ関数演算を行うハッシュ関数回路１１０１と、ハッシュ関数回路１１０１に必要な入力値を供給するレジスタ１１０２と、ハッシュ関数回路１１０１の出力ｈの一部（Ｋビット）を出力するセレクタ１１０３と、ＪＰＥＧデータをＫビットのブロックに分割する演算回路１１０４と、演算回路１１０４の出力とセレクタ１１０３の出力とを排他的論理和演算する演算回路１１０５とから構成される。
【００９０】
ハッシュ関数回路１１０１は、乱数発生回路２１４にて生成された秘密情報（即ち、乱数Ｒ）を初期値とするレジスタ１１０２の値をハッシュ関数で演算する。
【００９１】
ハッシュ関数回路１１０１の出力である１２８ビットのハッシュ値ｈは、セレクタ１１０３に入力される。セレクタ１１０３は、１２８ビットのハッシュ値ｈの内、例えば下位Ｋビットを出力する。このＫビットは、次にハッシュ関数演算されるデータとしてレジスタ１１０２に格納される。
【００９２】
上述の演算は、所定のブロックに達するまで、各ブロックに対して繰り返される。そして、その所定のブロックから求めたハッシュ値がディジタル署名データとして出力される。
【００９３】
尚、最初のハッシュ関数演算に必要な初期値は、例えば図１３に示すように、上述の乱数Ｒの下位Ｋビットを用いることができる。
【００９４】
▲３▼第３のモード
第３のモードについて図１２を用いて説明する。図１２は、制御／演算部２０６の構成の一部を示す図である。
【００９５】
図１２において、演算回路２１２は、所定のビット単位でハッシュ関数演算を行うハッシュ関数回路１２０１と、ハッシュ関数回路１２０１に必要な入力値を供給するレジスタ１２０２と、ハッシュ関数回路１２０１の出力ｈの一部（Ｋビット）を出力するセレクタ１２０３と、ＪＰＥＧデータをＫビットのブロックに分割する演算回路１２０４と、演算回路１２０４の出力とセレクタ１２０３の出力とを排他的論理和演算する演算回路１２０５とから構成される。
【００９６】
ハッシュ関数回路１２０１は、乱数発生回路２１４にて生成された秘密情報を初期値とするレジスタ１２０２の値を順次ハッシュ関数演算する。
【００９７】
ハッシュ関数回路１２０１の出力である１２８ビットのハッシュ値ｈは、セレクタ１２０３に入力される。セレクタ１２０３は、１２８ビットのハッシュ値ｈの内、例えば下位Ｋビットを出力する。このＫビットは、１ブロックのＪＰＥＧデータと排他的論理和演算され、その演算結果の一部は再びレジスタ１２０２に格納される。
【００９８】
上述の演算は、所定のブロックに達するまで、各ブロックに対して繰り返される。そして、その所定のブロックから求めたハッシュ値がディジタル署名データとして出力される。

【００９９】
尚、最初のハッシュ関数演算に必要な初期値は、例えば図１３に示すように、上述の乱数Ｒの下位Ｋビットを用いることができる。
【０１００】
ステップＳ６０８において、記録再生部２０３は、制御／演算部２０６にて生成されたディジタル署名データｈとそれに対応するディジタル画像データＰとを、取り外し可能な記録媒体に記録したり、ネットワークを介して他の機器に出力したりする。
【０１０１】
尚、図６に示す一連の処理手順を制御するプログラムは、ＲＯＭ２０７に格納されている。このプログラムは、制御／演算部２０６（に含まれる制御回路２１０）によって読み出され、ユーザの撮像指示毎に起動される。
【０１０２】
以上のように第２の実施例では、ある長さの乱数Ｒから生成された秘密情報Ｓと高能率符号化されたディジタル画像データＰとを用いて所定の演算を行い、その演算結果をハッシュ関数で演算してディジタル署名データｈを生成する。このように構成することによって、第２の実施例では、従来のシステムに比べて安全性も信頼性も高いディジタル署名データｈを簡単な構成によって実現することができる。又、従来のシステムに比べて安価に構成することも、処理速度を高速化することもできる。
【０１０３】
又、第２の実施例では、ハッシュ関数演算を上述の動作モードの１つまたは複数を組み合わせて実現することにより、第１の実施例に比べてより安全性の高いディジタル署名データ生成アルゴリズムを提供することができる。
【０１０４】
更に、第２の実施例では、第１の実施例と同様に、ディジタル署名データｈを用いて、ディジタル画像データＰがどの画像入力装置にて撮像されたかを特定することもできる。
【０１０５】
（第３の実施例）
第１、第２の実施例では、ハッシュ関数を用いてディジタル署名データｈを生成する手順について説明した。
【０１０６】
これに対して、第３の実施例では、ハッシュ関数ではなく、共通鍵暗号を用いてディジタル署名データｈを生成する手順について詳細に説明する。
【０１０７】
図１４は、第３の実施例の処理手順を説明するフローチャートである。以下、図１４を用いて、ディジタル署名データｈを生成する手順を説明する。
【０１０８】
ステップＳ１４０１～Ｓ１４０３の処理は、上述の第１の実施例のステップＳ４０１～Ｓ４０３と同様の処理としてその説明を省略する。
【０１０９】
ステップＳ１４０４において、制御／演算部２０６は、画像入力装置１０の持つ固有の秘密情報Ｓをメモリ２１３から読み出す。第３の実施例では、“１１１１…１１１１”（１２８ビット）を秘密情報Ｓとして説明する。
【０１１０】
ステップＳ１４０５において、制御／演算部２０６（に含まれる演算回路２１２）は、作業用メモリ２０２に保持されたＪＰＥＧデータを共通鍵暗号方式に基づいて暗号化する。ここで、ＪＰＥＧデータを共通鍵暗号化する暗号鍵は、秘密情報Ｓから生成する。
【０１１１】
共通鍵暗号方式には現在様々なものが提案されているが、第３の実施例ではＤＥＳ方式を用いる。ＤＥＳ方式を使用する場合、暗号鍵のビット長は５６ビットであるので、秘密情報Ｓの上位５６ビットを暗号鍵とする（図１５参照）。ここで、この暗号鍵のビット長は

、使用する共通鍵暗号方式の種類によって異なるものである。従って、FEAL-nX,MITSY,IDEAを使用する場合、暗号鍵は１２８ビットであるので、秘密情報Ｓの上位１２８ビットを暗号鍵とする。又、FEAL-n,MULTI2を使用する場合、暗号鍵は６４ビットであるので、秘密情報Ｓの上位６４ビットを暗号鍵とする。

【０１１２】

ステップＳ１４０５における共通鍵暗号化処理について詳細に説明する。

【０１１３】

制御／演算部２０６は、後述する３つの動作モード（即ち、ＣＢＣモード、ＣＦＢモード、ＯＦＢモード）の何れか１つ又はこれらの組み合わせにより、ＪＰＥＧデータを暗号化する。何れの動作モードにおいても、入力データを撹乱しながら暗号化することができるため、より安全性の高い暗号化処理を実現できる。

【０１１４】

▲１▼ＣＢＣ（Cipher Block Chaining）モード

ＣＢＣモードを図１６を用いて説明する。図１６は、制御／演算部２０６の一部（即ち、演算回路２１２）を示す図である。

【０１１５】

図１６において、演算回路２１２は、６４ビット単位で暗号化を行う暗号化回路１６０１と、暗号化回路１６０１の出力を一時的に保持するレジスタ１６０２と、ＪＰＥＧデータとレジスタ１６０２の出力とを排他的論理和演算する演算回路１６０３とから構成される。

【０１１６】

暗号化回路１６０１は、６４ビットからなるブロック毎に、ＪＰＥＧデータを暗号化する。暗号化回路１６０１の出力は、レジスタ１６０２に一時的に格納される。レジスタ１６０２に格納された６４ビットのデータは、次のブロックと排他的論理和演算され、その演算結果は暗号化回路１６０１に供給される。最終的に、全てのブロックを暗号化した結果が暗号データとして出力される。この暗号データの一部が、ディジタル署名データｈとなる。

【０１１７】

ここで、最初のブロックの暗号化では、レジスタ１６０２に初期値を格納しておく必要がある。その初期値は、例えば、秘密情報Ｓの下位６４ビットを用いる（図１５参照）。

【０１１８】

尚、ブロックの大きさが６４の倍数とならない場合には、例えば後述のＯＦＢモードと組合せて余りのビット列を暗号化するように構成してもよい。

【０１１９】

▲２▼ＯＦＢ（Output Feedback）モード

ＯＦＢモードについて図１７を用いて説明する。図１７は、制御／演算部２０６の一部（即ち、演算回路２１２）を示す図である。

【０１２０】

図１７において、演算回路２１２は、６４ビット単位で暗号化を行う暗号化回路１７０１と、暗号化回路１７０１に必要な入力値を供給するレジスタ１７０２と、暗号化回路１７０１の出力を選択的に出力するセレクタ１７０３と、ＪＰＥＧデータとセレクタ１７０３の出力とを排他的論理和演算する演算回路１７０４とから構成される。

【０１２１】

暗号化回路１７０１は、レジスタ１７０２に格納された６４ビットのデータを暗号化する。暗号化回路１７０１の出力は、セレクタ１７０３に入力される。セレクタ１７０３は、例えば下位Ｋビットを出力する。このＫビットは、次に暗号化されるデータとしてレジスタ１７０２に格納される。セレクタ１７０３から出力されたＫビットは、ＪＰＥＧデータの各ブロック（１ブロックは、Ｋビット）と排他的論理和演算され、その結果が暗号データとなる。この暗号データの一部が、ディジタル署名データｈとなる。

【０１２２】

尚、最初の暗号化に必要な初期値は、例えば、秘密情報Ｓの下位６４ビットを用いる（図１５参照）。

【０１２３】

▲３▼ＣＦＢ（Cipher Feedback）モード

ＣＦＢモードについて図１８を用いて説明する。図１８は、制御／演算部２０６の一部（即ち、演算回路２１２）を示す図である。

【０１２４】

図１８において、演算回路２１２は、６４ビット単位で暗号化を行う暗号化回路１８０１と、暗号化回路１８０１に必要な入力値を供給するレジスタ１８０２と、暗号化回路１８０１の出力を選択的に出力するセレクタ１８０３と、ＪＰＥＧデータとセレクタ１８０３の出力とを排他的論理和演算する演算回路１８０４とから構成される。

【０１２５】

暗号化回路１８０１は、レジスタ１８０２に格納された６４ビットのデータを暗号化する。暗号化回路１８０１の出力は、セレクタ１８０３に入力される。

セレクタ１８０３は、例えば下位Ｋビットを出力する。セレクタ１８０３から出力されたＫビットは、１ブロック（Ｋビット）のＪＰＥＧデータと排他的論理和演算され、その結果は再びレジスタ１８０２に格納される。最終的に、全てのブロックを処理した結果が暗号データとして出力される。この暗号データの一部が、ディジタル署名データｈとなる。

【０１２６】

尚、最初の暗号化に必要な初期値は、例えば、秘密情報Ｓの下位６４ビットを用いる（図１５参照）。

【０１２７】

ステップＳ１４０６において、制御／演算部２０６（に含まれる演算回路２１２）は、ステップＳ１４０５にて生成された暗号データから特定のビット列をディジタル署名データとして抽出する。例えば、上述の暗号データの下位１２８ビットをディジタル署名データとする。

【０１２８】

ステップＳ１４０７において、記録再生部２０３は、制御／演算部２０６（に含まれる演算回路２１２）にて生成されたディジタル署名データｈとそれに対応するディジタル画像データＰとを、取り外し可能な記録媒体に記録したり、ネットワークを介して他の機器に出力したりする。

【０１２９】

尚、図１４に示す一連の処理手順を制御するプログラムは、ＲＯＭ２０７に格納されている。このプログラムは、制御／演算部２０６（に含まれる制御回路２１０）によって読み出され、ユーザの撮像指示毎に起動される。

【０１３０】

以上のように第３の実施例では、秘密情報Ｓの一部から生成した暗号鍵と高能率符号化されたディジタル画像データＰとを用いて共通鍵暗号方式による暗号化を行い、暗号化されたデータからディジタル署名データｈを生成する。このように構成することにより、第３の実施例では、第１、第２の実施例に比べて安全性も信頼性も向上させたディジタル署名データを生成することができる。又、従来のシステムに比べて安価に構成することも、処理速度を高速化することもできる。

【０１３１】

又、第３の実施例では、ディジタル署名データｈを用いて、ディジタル画像データがどの画像入力装置にて撮像されたかを特定することもできる。

【０１３２】

尚、第３の実施例では、秘密情報Ｓを“１１１１…１１１１”（１２８ビット）としたがこれに限るものではない。例えば、乱数発生回路２１４が所定のアルゴリズムに基づいて発生させた乱数とすることも可能である。但し、この秘密情報Ｓは画像検証装置２０と共有される。

【０１３３】
（第４の実施例）
第３の実施例では、ハッシュ関数ではなく共通鍵暗号を用いてディジタル署名データｈを生成する手順について説明した。
【０１３４】
これに対して、第４の実施例では、所定の演算（例えば、ビット挿入を含む逆演算可能な演算）を行い、その演算結果を共通鍵暗号方式で暗号化した後、暗号化されたデータからディジタル署名データｈを生成する手順について説明する。
【０１３５】
図１９は、第４の実施例の処理手順を説明するフローチャートである。以下、図１９を用いて、ディジタル署名データｈを生成する手順を説明する。
【０１３６】
ステップＳ１９０１～Ｓ１９０３の処理は、上述の第１の実施例のステップＳ４０１～Ｓ４０３と同様の処理としてその説明を省略する。
【０１３７】
ステップＳ１９０４～Ｓ１９０６の処理は、上述の第２の実施例のステップＳ６０４～Ｓ６０６と同様の処理（即ち、秘密情報である乱数ＲのビットＲｉとＪＰＥＧデータのブロックＤｉとを用いた排他的論理和演算）としてその説明を省略する。
【０１３８】
ここで、ステップＳ１９０６の演算は、上述のステップＳ６０６と同様に、乱数Ｒｉとブロック Ｄｉの最下位ビットとの間の排他的論理和演算としたがそれに限るものではない。各ブロックＤｉの少なくとも一部に秘密情報Ｓ（ビット長ｍの乱数Ｒ）の一部を付加、合成、多重する処理で且つ逆演算可能な処理であれば、いかなる演算処理であってもよい。
【０１３９】
ステップＳ１９０７において、制御／演算部２０６（に含まれる演算回路２１２）は、ステップＳ１９０６の出力を共通鍵暗号方式に従って暗号化する。ここで、制御／演算部２０６は、第３の実施例と同様に、ＤＥＳ方式を利用するものとし、その暗号化に必要な暗号鍵は、ステップＳ１９０４で生成した秘密情報Ｓの上位５６ビットとする（図２０参照）。
【０１４０】
ステップＳ１９０７における暗号化処理について詳細に説明する。
【０１４１】
制御／演算部２０６は、上述した３つの動作モード（即ち、ＣＢＣモード、ＣＦＢモード、ＯＦＢモード）の何れか１つ又はこれらの組み合わせ、乱数ＲのビットＲｉとＪＰＥＧデータのブロックＤｉとを排他的論理和演算した結果を、順次暗号化する。何れの動作モードにおいても、入力データを撹乱しながら暗号化することができるため、より安全性の高い暗号化を実現できる。
【０１４２】
ステップＳ１９０８において、制御／演算部２０６（に含まれる演算回路２１２）は、ステップＳ１９０７にて生成された暗号データから特定のビット列をディジタル署名データｈとして抽出する。例えば、暗号データの下位１２８ビットをディジタル署名データｈとする。
【０１４３】
ステップＳ１９０９において、記録再生部２０３は、制御／演算部２０６（に含まれる演算回路２１２）にて生成されたディジタル署名データｈとそれに対応するディジタル画像データＰとを、取り外し可能な記録媒体に記録したり、ネットワークを介して他の機器に出力したりする。
【０１４４】
尚、図１９に示す一連の処理手順を制御するプログラムは、ＲＯＭ２０７に格納されている。このプログラムは、制御／演算部２０６（に含まれる制御回路２１０）によって読み

出され、ユーザの撮像指示毎に起動される。

【０１４５】

以上のように第４の実施例では、乱数Ｒから生成された秘密情報Ｓと高能率符号化されたディジタル画像データＰとを用いて所定の演算を行い、その演算結果を共通鍵暗号方式により暗号化し、暗号化されたデータからディジタル署名データｈを生成する。このように構成することにより、第４の実施例では、第３の実施例に比べて安全性も信頼性も向上させたディジタル署名データを生成することができる。又、従来のシステムに比べて安価に構成することも、処理速度を高速化することもできる。

【０１４６】

又、第４の実施例では、ディジタル署名データｈを用いて、あるディジタル画像データＰがどの画像入力装置にて撮像されたかを特定することもできる。

【０１４７】

（第５の実施例）

第１～第４の実施例では、画像入力装置１０に固有の秘密情報Ｓに基づいて、ディジタル署名データｈを生成する構成について説明した。このような構成により第１～第４の実施例では、ディジタル署名データｈを用いて、あるディジタル画像データＰがどの画像入力装置にて撮像されたものであるかを特定することができる。

【０１４８】

これに対して、第５の実施例では、外部装置（例えば，ＩＣカード等）を画像入力装置１０に接続し、この外部装置に固有の秘密情報Ｓに基づいて、ディジタル署名データｈを生成する構成について説明する。外部機器の持つ秘密情報Ｓは、例えば、画像入力装置１０を識別するためのＩＤ情報、画像入力装置１０を使用するユーザを識別するためのＩＤ情報とすることができる。このように構成することにより、第５の実施例では、ディジタル署名データｈを用いて、ディジタル画像データがどの外部機器と接続された画像入力装置によって撮像されたものか、或いはどのユーザによって撮像されたものであるかを特定することができる。

【０１４９】

図２１は、第５の実施例の処理手順を説明するフローチャートである。以下、図２１を用いて、ディジタル署名データｈを生成する手順を説明する。

【０１５０】

ステップＳ２１０１において、画像入力装置１０の制御/演算処理部２０６は、外部Ｉ／Ｆ部２０５に外部装置４０が接続されているか否かを検出する。

【０１５１】

ステップＳ２１０２において、画像入力装置１０と外部装置４０とは、相互認証を行い、互いに正当なものであるかどうかをチェックする。

【０１５２】

図２２を用いて、画像入力装置１０と外部装置４０との相互認証処理について説明する。

【０１５３】

画像入力装置１０は、乱数発生回路２１４を用いて認証用の乱数ａを発生させ、その乱数ａを外部Ｉ／Ｆ部２０５を介して外部装置４０に送信する。

【０１５４】

次に外部装置４０の暗号化回路４３は、認証用の暗号鍵を用いて乱数ａをＡに変換し、その暗号データＡを外部Ｉ／Ｆ部４１を介して画像入力装置１０へ送信する。

【０１５５】

又、画像入力装置１０の暗号化回路２２０１は、乱数ａを認証用の暗号鍵を用いてＡ’に変換する。比較回路２２０２は、その暗号データＡ’を外部装置４０から送信された暗号データＡと比較し、それらが一致すれば外部装置４０を認証する。

【０１５６】

同様にして、外部装置４０は、乱数発生回路４２を用いて認証用の乱数ｂを発生させ、その乱数ｂを外部Ｉ／Ｆ部２０５を介して画像入力装置１０に送信する。

【０１５７】
次に画像入力装置１０の暗号化回路２２０１は、認証用の暗号鍵を用いて乱数ｂをＢに変換し、その暗号データＢを外部Ｉ／Ｆ部２０５を介して外部装置４０へ送信する。
【０１５８】
又、外部装置４０の暗号化回路４３は、乱数ｂを認証用の暗号鍵を用いてＢ’に変換する。比較回路４４は、その暗号データＢ’を画像入力装置１０から送信された暗号データＢと比較し、それらが一致すれば画像入力装置１０を認証する。
【０１５９】
双方が正常に認証された場合、外部装置４０は、メモリ４５に格納された秘密情報Ｓを外部Ｉ／Ｆ部４１を介して画像入力装置１０に送信する。
【０１６０】
ステップＳ２１０３～Ｓ２１０５の処理は、上述の第１の実施例のステップＳ４０１～Ｓ４０３と同様の処理としてその説明を省略する。
【０１６１】
ステップＳ２１０６において、制御／演算部２０６は、外部Ｉ／Ｆ部２０５を介して入力された秘密情報Ｓをメモリ２１３に格納する。
【０１６２】
ステップＳ２１０７において、制御／演算部２０６（に含まれる演算回路２１２）は、秘密情報ＳとＪＰＥＧ方式で高能率符号化されたディジタル画像データＰ（以下、ＪＰＥＧデータと称する）とを用いて、予め定められた規則に基づく所定の演算を行う。ここで、演算回路２１２は、第１の実施例のステップＳ４０５と同様の演算を行う。
【０１６３】
ステップＳ２１０８において、制御／演算部２０６（に含まれる演算回路２１２）は、ステップＳ２１０７の演算結果をハッシュ関数で演算し、その結果からディジタル署名データｈを生成する。ここで、演算回路２１２は、第１の実施例のステップＳ４０６と同様の演算処理を行う。
【０１６４】
ステップＳ２１０９において、記録再生部２０３は、制御／演算部２０６にて生成されたディジタル署名データｈとそれに対応するディジタル画像データＰとを、取り外し可能な記録媒体に記録したり、ネットワークを介して他の機器に出力したりする。
【０１６５】
尚、図２１に示す一連の処理手順を制御するプログラムは、ＲＯＭ２０７に格納されている。このプログラムは、制御／演算部２０６（に含まれる制御回路２１０）によって読み出され、ユーザの撮像指示毎に起動される。これにより、ディジタル画像を撮像する毎にその画像に対応したディジタル署名データｈを生成することができる。
【０１６６】
以上のように第５の実施例では、高能率符号化されたディジタル画像データＰと外部装置４０の有する秘密情報Ｓとを用いて所定の演算を行い、その演算結果をハッシュ関数で演算した後、その演算結果からディジタル署名データｈを生成する。このように構成することにより、第５の実施例では、従来のシステムに比べて安全性も信頼性も向上させたディジタル署名データを生成することができる。又、従来のシステムに比べて安価に構成することも、処理速度を高速化することもできる。
【０１６７】
この結果、外部機器の秘密情報Ｓと所定の演算とを知らなければ、ディジタル画像データＰに対応するディジタル署名データｈを不正に作り出すことはできないため、ディジタル署名データｈに基づいてディジタル画像データＰの正当性を安全に検証することができる。又、一方向性関数の性質により、ディジタル署名データｈから元のデータ（即ち、秘密情報Ｓを用いて所定の演算を行なったディジタル画像データＰ）を知ることもできないため、ディジタル署名データｈからディジタル画像データＰの正当性を安全に検証することができる。

【０１６８】
又、ディジタル署名データｈを用いて、ディジタル画像データがどのユーザによって撮像されたかを特定することもできる。
【０１６９】
尚、第５の実施例では、ディジタル署名データｈを生成する手順を第１の実施例と同様の手順としたがそれに限るものではない。上述の第２～第４の実施例の何れも適用することができる。
【０１７０】
（第６の実施例）
第５の実施例では、画像入力装置１０に外部装置４０を接続し、この外部装置４０の持つ固有の秘密情報に基づいてディジタル署名データを生成する構成について説明した。
【０１７１】
これに対して、第６の実施例では、画像入力装置１０を外部装置４０に接続し、この外部装置４０に固有の秘密情報Ｓ２と画像入力装置１０に固有の秘密情報Ｓ１の双方に基づいて、ディジタル署名データｈを生成する構成について説明する。このように構成することにより第６の実施例では、ディジタル署名データｈを用いて、ディジタル画像データＰがどの外部機器と接続されたどの画像入力装置によって撮像されたものか、或いはどのユーザが使用するどの画像入力装置によって撮像されたものであるかを特定することができる。
【０１７２】
図２１を用いて第６の実施例の処理手順を詳細に説明する。
【０１７３】
ステップＳ２１０１において、画像入力装置１０の制御/演算処理部２０６は、外部Ｉ／Ｆ部２０５に外部装置４０が接続されているか否かを検出する。
【０１７４】
ステップＳ２１０２において、画像入力装置１０と外部装置４０とは、相互認証を行い、互いに正当なものであるかどうかをチェックする。
【０１７５】
ステップＳ２１０３～Ｓ２１０５の処理は、上述の第１の実施例のステップＳ４０１～Ｓ４０３と同様の処理としてその説明を省略する。
【０１７６】
ステップＳ２１０６において、制御／演算部２０６は、画像入力装置１０の持つ秘密情報Ｓ１をメモリ２１３から読み出すと共に、外部装置４０の持つ秘密情報Ｓ２を外部Ｉ／Ｆ部２０５を介して入力する。そして、これらの秘密情報Ｓ１，Ｓ２を結合させ、新しい秘密情報Ｓを生成する。
【０１７７】
ここで、画像入力装置１０の秘密情報Ｓ１を例えば“１１１１”とし、外部装置４０の秘密情報Ｓ２を例えば“００００”とすると、新たに生成される秘密情報Ｓは、例えば“１１１１００００”となる。尚、第６の実施例では、２つの秘密情報を単に結合することにより新たな秘密情報Ｓを生成する場合について説明したが、秘密情報Ｓから秘密情報Ｓ１，Ｓ２を抽出できる演算であれば、いかなる演算であってもよい。
【０１７８】
ステップＳ２１０７において、制御／演算部２０６（に含まれる演算回路２１２）は、秘密情報ＳとＪＰＥＧ方式で高能率符号化されたディジタル画像データＰ（以下、ＪＰＥＧデータと称する）とを用いて、予め定められた規則に基づく所定の演算を行う。ここで、演算回路２１２は、第１の実施例のステップＳ４０５と同様の演算を行う。
【０１７９】
ステップＳ２１０８において、制御／演算部２０６（に含まれる演算回路２１２）は、ステップＳ２１０７の演算結果をハッシュ関数で演算し、その結果からディジタル署名データｈを生成する。

【０１８０】
ステップＳ２１０９において、記録再生部２０３は、制御／演算部２０６にて生成されたディジタル署名データｈとそれに対応するディジタル画像データＰとを、取り外し可能な記録媒体に記録したり、ネットワークを介して他の機器に出力したりする。
【０１８１】
尚、図２１に示す一連の処理手順を制御するプログラムは、ＲＯＭ２０７に格納されている。このプログラムは、制御／演算部２０６（に含まれる制御回路２１０）によって読み出され、ユーザの撮像指示毎に起動される。これにより、ディジタル画像を撮像する毎にその画像に対応したディジタル署名データを生成することができる。
【０１８２】
以上説明したように、第６の実施例では、高能率符号化されたディジタル画像データＰと、画像入力装置１０の秘密情報Ｓ１と外部装置４０の秘密情報Ｓ２とから生成された秘密情報Ｓとを用いて所定の演算を行い、その演算結果をハッシュ関数で演算した後、その演算結果を用いてディジタル署名データｈを生成する。このように構成することにより、第６の実施例では、従来のシステムに比べて安全性も信頼性も向上させたディジタル署名データを生成することができる。又、従来のシステムに比べて安価に構成することも、処理速度を高速化することもできる。
【０１８３】
又、ディジタル署名データｈを用いて、ディジタル画像データがどの外部機器と接続された画像入力装置によって撮像されたものか、或いはどのユーザによって使用された画像入力装置にて撮像されたものかを特定することもできる。
【０１８４】
尚、第６の実施例では、ディジタル署名データｈを生成する手順を第１の実施例と同様の手順としたがそれに限るものではない。上述の第２～第４の実施例の何れも適用することができる。
【０１８５】
（第７の実施例）
第７の実施例では、第１の実施例の画像入力装置１０が生成したディジタル署名データｈを用いて、ディジタル画像データＰの正当性を確認する画像検証装置２０について説明する。
【０１８６】
図２３は、第７の実施例の処理手順の一例を説明するフローチャートである。以下、図２３を用いて、画像検証装置２０がディジタル画像データＰを検証する手順を説明する。
【０１８７】
ステップＳ２３０１において、外部Ｉ／Ｆ部３０１は、画像入力装置１０が生成したディジタル画像データＰとそれに対応するディジタル署名データｈとを入力し、それらを画像検証装置２０の作業用メモリ３０２に格納する。ここで、ディジタル画像データＰは、例えば、ＪＰＥＧ方式で高能率符号化されている（以下、ディジタル画像データＰを単にＪＰＥＧデータと称する）。
【０１８８】
ステップＳ２３０２において、操作部３０６は、ユーザの操作入力に基づき、どのＪＰＥＧデータの正当性を検証するか否かを選択する。検証が指示された場合、制御／演算部３０３はステップＳ２３０３を実行する。
【０１８９】
ステップＳ２３０３において、制御／演算部３０３は、メモリ３１３から秘密情報Ｓを読み出す。ここで、この秘密情報Ｓは、第１の実施例の画像入力装置１０と本実施例の画像検証装置２０との間で秘密に共有する情報である。従って、本実施例の秘密情報Ｓは、第１の実施例と同様に“１１１１１１１１”である。尚、この秘密情報Ｓは、読み出し専用の記録媒体等の中に保存され、外部に出力できないように管理されている。
【０１９０】

ステップＳ２３０４において、制御／演算部３０３（に含まれる演算回路３１２）は、秘密情報ＳとＪＰＥＧデータとを用いて、第１の実施例のステップＳ４０５と同様の演算を行う。つまり、ＪＰＥＧデータの最上位バイトと秘密情報Ｓとを、ビット毎に排他的論理和演算する。

【０１９１】

ステップＳ２３０５において、制御／演算部３０３（に含まれる演算回路３１２）は、ステップＳ２３０４の演算結果をハッシュ関数で演算する。ここでは、第１の実施例と同様のハッシュ関数を使用して、ステップＳ４０６と同様の処理を行う。

【０１９２】

ステップＳ２３０６において、制御／演算部３０３（に含まれる演算回路３１２）は、ステップＳ２３０５の演算結果と選択されたＪＰＥＧデータのディジタル署名データｈとを比較する。比較の結果、これらのデータが一致した場合には、ＪＰＥＧデータを正当なものと判断し、一致しなかった場合には、ＪＰＥＧデータに何らかの不正な処理（即ち、ＪＰＥＧデータに対する修正、改竄、偽造、合成等の改変処理）が行われたものと判断する。

【０１９３】

ステップＳ２３０７において、表示部３０４は、ステップＳ２３０６の比較結果が一致した場合、選択したＪＰＥＧデータが正常で、不正な処理の施されていないことを示す表示画像或いはメッセージを表示する。又、この比較結果が一致しなかった場合、不正な処理を示す警告画像或いは警告メッセージを表示する。これにより、ユーザは、選択したＪＰＥＧデータの正当性を視覚的に分かり易く認識することができる。

【０１９４】

尚、図２３に示す一連の処理手順を制御するプログラムは、ＲＯＭ３０５に格納されている。このプログラムは、制御／演算部３０３（に含まれる制御回路３１２）によって読み出され、所望の画像の検証を指示する毎に起動する。

【０１９５】

以上の手順により、選択されたＪＰＥＧデータの正当性が確認されなかった場合、制御回路３１０は各処理回路を制御して該ＪＰＥＧデータを廃棄する。

【０１９６】

以上説明したように、第７の実施例では、第１の実施例の画像入力装置１０にて撮像され、高能率符号化されたディジタル画像データＰの正当性を、従来のシステムに比べて簡単な構成で認識することができる。又、従来のシステムに比べて安価に構成することも、処理速度を高速化することもできる。

【０１９７】

（第８の実施例）

第８の実施例では、第２の実施例の画像入力装置１０が生成したディジタル署名データｈを用いて、ディジタル画像データＰの正当性を確認する画像検証装置２０について説明する。

【０１９８】

図２４は、第８の実施例の処理手順の一例を説明するフローチャートである。以下、図２４を用いて、画像検証装置２０がディジタル画像データＰを検証する手順を説明する。

【０１９９】

ステップＳ２４０１、Ｓ２４０２の処理は、上述の第７の実施例のステップＳ２３０１、Ｓ２３０２と同様の処理としてその説明を省略する。

【０２００】

ステップＳ２４０３において、制御／演算部３０３（に含まれる乱数発生回路）は、ビット長ｍの乱数Ｒ（即ち、秘密情報Ｓ）を生成する。乱数Ｒを生成するためのプログラムは、ＲＯＭ３０５に格納されている。このプログラムは、第２の実施例の画像入力装置１０の保持するプログラムと同一であり、乱数Ｒは、第２の実施例の乱数Ｒと同一である。尚、このプログラム及び乱数Ｒは、外部に出力できないように管理されている。

【０２０１】
ステップＳ２４０４において、制御／演算部３０３（に含まれる演算回路３１２）は、図７に示すように、選択されたＪＰＥＧデータを１２８ビットのブロックＤｉ（ｉ＝１～ｎ）に分割する。データ量が１２８ビットにならないブロックについては、“０００…０００”をパディングする。尚、ステップＳ２４０４の処理は、第２の実施例のステップＳ６０５と同様の処理である。
【０２０２】
ステップＳ２４０５において、制御／演算部３０３（に含まれる演算回路３１２）は、乱数Ｒとｎ個のブロックとを用いて、第２の実施例のステップＳ６０６と同様の演算を行う。つまり、乱数ＲのビットＲｉとブロックＤｉの最下位ビットとの間の排他的論理和演算を、ｉ＝１～ｎとなるまで繰り返す。
【０２０３】
ステップＳ２４０６において、制御／演算部３０３（に含まれる演算回路３１２）は、ステップＳ２４０５の演算結果に対してハッシュ関数演算を行う。ここでは、第２の実施例と同様のハッシュ関数を使用して、ステップＳ６０７と同様の処理を行う。
【０２０４】
ステップＳ２４０７において、制御／演算部３０３（に含まれる演算回路３１２）は、ステップＳ２４０６の演算結果と選択されたＪＰＥＧデータのディジタル署名データｈとを比較する。比較の結果、これらのデータが一致した場合には、ＪＰＥＧデータを正当なものと判断し、一致しなかった場合には、ＪＰＥＧデータに何らかの不正な処理（即ち、ＪＰＥＧデータに対する修正、改竄、偽造、合成等の改変処理）が行われたものと判断する。
【０２０５】
ステップＳ２４０８において、表示部３０４は、ステップＳ２４０７の比較結果を画像或いはメッセージで表示する。これにより、ユーザは、選択したＪＰＥＧデータの正当性を視覚的に分かり易く認識することができる。
【０２０６】
尚、図２４に示す一連の処理手順を制御するプログラムは、ＲＯＭ３０５に格納されている。このプログラムは、制御／演算部３０３（に含まれる制御回路３１２）によって読み出され、所望の画像の検証を指示する毎に起動する。
【０２０７】
以上の手順により、選択されたＪＰＥＧデータの正当性が確認されなかった場合、制御回路３１０は各処理回路を制御して該ＪＰＥＧデータを廃棄する。
【０２０８】
以上説明したように、第８の実施例では、第２の実施例の画像入力装置１０にて撮像され、高能率符号化されたディジタル画像データＰの正当性を、従来のシステムに比べて簡単な構成で認識することができる。又、従来のシステムに比べて安価に構成することも、処理速度を高速化することもできる。
【０２０９】
（第９の実施例）
第９の実施例では、第３の実施例の画像入力装置１０が生成したディジタル署名データｈを用いて、ディジタル画像データＰの正当性を確認する画像検証装置２０について説明する。
【０２１０】
図２５は、第９の実施例の処理手順の一例を説明するフローチャートである。以下、図２５を用いて、画像検証装置２０がディジタル画像データＰを検証する手順を説明する。
【０２１１】
ステップＳ２５０１、Ｓ２５０２の処理は、上述の第７の実施例のステップＳ２３０１、Ｓ２３０２と同様の処理としてその説明を省略する。
【０２１２】

ステップＳ２５０３において、制御／演算部３０３は、メモリ３１３から秘密情報Ｓを読み出す。ここで、この秘密情報Ｓは、第３の実施例の画像入力装置１０と本実施例の画像検証装置２０との間で共有する情報である。従って、本実施例の秘密情報Ｓは、第３の実施例と同様に“１１１１１１１１”である。尚、この秘密情報は、読み出し専用の記録媒体等の中に保存され、外部に出力できないように管理されている。

【０２１３】

ステップＳ２５０４において、制御／演算部３０３（に含まれる演算回路３１２）は、第３の実施例のステップＳ１４０５と同様に、選択されたＪＰＥＧデータを共通鍵暗号方式で暗号化する。

【０２１４】

ステップＳ２５０５において、制御／演算部３０３（に含まれる演算回路３１２）は、ステップＳ２５０４にて生成された暗号データから特定のビット列を抽出する。例えば、第３の実施例と同様に、上述の暗号データの下位１２８ビットを抽出する。

【０２１５】

ステップＳ２５０６において、制御／演算部３０３（に含まれる演算回路３１２）は、ステップＳ２５０５の抽出結果と選択されたＪＰＥＧデータのディジタル署名データｈとを比較する。比較の結果、これらのデータが一致した場合には、ＪＰＥＧデータを正当なものと判断し、一致しなかった場合には、ＪＰＥＧデータに何らかの不正な処理（即ち、ＪＰＥＧデータに対する修正、改竄、偽造、合成等の改変処理）が行われたものと判断する。

【０２１６】

ステップＳ２５０７において、表示部３０４は、ステップＳ２５０６の比較結果を画像或いはメッセージで表示する。これにより、ユーザは、選択したＪＰＥＧデータの正当性を視覚的に分かり易く認識することができる。

【０２１７】

尚、図２５に示す一連の処理手順を制御するプログラムは、ＲＯＭ３０５に格納されている。このプログラムは、制御／演算部３０３（に含まれる制御回路３１２）によって読み出され、所望の画像の検証を指示する毎に起動する。

【０２１８】

以上の手順により、選択されたＪＰＥＧデータの正当性が確認されなかった場合、制御回路３１０は各処理回路を制御して該ＪＰＥＧデータを廃棄する。

【０２１９】

以上説明したように、第９の実施例では、第３の実施例の画像入力装置１０にて撮像され、高能率符号化されたディジタル画像データＰの正当性を、従来のシステムに比べて簡単な構成で認識することができる。又、従来のシステムに比べて安価に構成することも、処理速度を高速化することもできる。

【０２２０】

（第１０の実施例）

第１０の実施例では、第４の実施例の画像入力装置１０が生成したディジタル署名データｈを用いて、ディジタル画像データＰの正当性を確認する画像検証装置２０について説明する。

【０２２１】

図２６は、第１０の実施例の処理手順の一例を説明するフローチャートである。以下、図２６を用いて、画像検証装置２０がディジタル画像データＰを検証する手順を説明する。

【０２２２】

ステップＳ２６０１、Ｓ２６０２の処理は、上述の第７の実施例のステップＳ２３０１、Ｓ２３０２と同様の処理としてその説明を省略する。

【０２２３】

ステップＳ２６０３～Ｓ２６０５の処理は、上述の第８の実施例のステップＳ２４０３～Ｓ２４０５と同様の処理としてその説明を省略する。

【０２２４】
ステップＳ２６０６において、制御／演算部３０３（に含まれる演算回路３１２）は、第４の実施例のステップＳ１９０７と同様に、選択されたＪＰＥＧデータを共通鍵暗号方式で暗号化する。
【０２２５】
ステップＳ２６０７において、制御／演算部３０３（に含まれる演算回路３１２）は、ステップＳ２６０６にて生成された暗号データから特定のビット列を抽出する。例えば、第３の実施例と同様に、上述の暗号データの下位１２８ビットを抽出する。
【０２２６】
ステップＳ２６０８において、制御／演算部３０３（に含まれる演算回路３１２）は、ステップＳ２６０７の抽出結果と選択されたＪＰＥＧデータのディジタル署名データｈとを比較する。比較の結果、これらのデータが一致した場合には、ＪＰＥＧデータを正当なものと判断し、一致しなかった場合には、ＪＰＥＧデータに何らかの不正な処理（即ち、ＪＰＥＧデータに対する修正、改竄、偽造、合成等の改変処理）が行われたものと判断する。
【０２２７】
ステップＳ２６０９において、表示部３０４は、ステップＳ２６０８の比較結果を画像或いはメッセージで表示する。これにより、ユーザは、選択したＪＰＥＧデータの正当性を視覚的に分かり易く認識することができる。
【０２２８】
尚、図２６に示す一連の処理手順を制御するプログラムは、ＲＯＭ３０５に格納されている。このプログラムは、制御／演算部３０３（に含まれる制御回路３１２）によって読み出され、所望の画像の検証を指示する毎に起動する。
【０２２９】
以上の手順により、選択されたＪＰＥＧデータの正当性が確認されなかった場合、制御回路３１０は各処理回路を制御して該ＪＰＥＧデータを廃棄する。
【０２３０】
以上説明したように、第１０の実施例では、第４の実施例の画像入力装置１０にて撮像され、高能率符号化されたディジタル画像データＰの正当性を、従来のシステムに比べて簡単な構成で認識することができる。又、従来のシステムに比べて安価に構成することも、処理速度を高速化することもできる。
【０２３１】
（第１１の実施例）
第１１の実施例では、第５の実施例の画像入力装置１０が生成したディジタル署名データｈを用いて、ディジタル画像データＰの正当性を確認する画像検証装置２０について説明する。
【０２３２】
図２７は、第１１の実施例の処理手順の一例を説明するフローチャートである。以下、図２７を用いて、画像検証装置２０がディジタル画像データＰを検証する手順を説明する。
【０２３３】
ステップＳ２７０１において、画像検証装置２０の制御/演算処理部３０３は、外部Ｉ／Ｆ部３０１に外部装置４０が接続されているか否かを検出する。
【０２３４】
ステップＳ２７０２において、画像検証装置２０と外部装置４０とは、相互認証を行い、互いに正当なものであるかどうかをチェックする。
【０２３５】
ステップＳ２７０３、Ｓ２７０４の処理は、上述の第７の実施例のステップＳ２３０１、Ｓ２３０２と同様の処理としてその説明を省略する。
【０２３６】
ステップＳ２７０５において、制御／演算部３０３は、外部Ｉ／Ｆ部３０１を介して入力

された外部装置４０に固有の秘密情報Ｓをメモリ３１３に格納し、管理する。
【０２３７】
ステップＳ２７０６において、制御／演算部３０３（に含まれる演算回路３１２）は、秘密情報ＳとＪＰＥＧデータとを用いて、予め定められた規則に基づく所定の演算を行う。ここで、演算回路３１２は、第７の実施例のステップＳ２３０４と同様の演算を行う。
【０２３８】
ステップＳ２７０７において、制御／演算部３０３（に含まれる演算回路３１２）は、ステップＳ２７０６の演算結果をハッシュ関数で演算する。ここで、演算回路３１２は、第７の実施例のステップＳ２３０５と同様の演算を行う。
【０２３９】
ステップＳ２７０８において、制御／演算部３０３（に含まれる演算回路３１２）は、ステップＳ２７０７の演算結果と選択されたＪＰＥＧデータのディジタル署名データｈとを比較する。比較の結果、これらのデータが一致した場合には、ＪＰＥＧデータを正当なものと判断し、一致しなかった場合には、ＪＰＥＧデータに何らかの不正な処理（即ち、ＪＰＥＧデータに対する修正、改竄、偽造、合成等の改変処理）が行われたものと判断する。
【０２４０】
ステップＳ２７０９において、表示部３０４は、ステップＳ２７０８の比較結果を画像或いはメッセージで表示する。これにより、ユーザは、選択したＪＰＥＧデータの正当性を視覚的に分かり易く認識することができる。
【０２４１】
尚、図２７に示す一連の処理手順を制御するプログラムは、ＲＯＭ３０５に格納されている。このプログラムは、制御／演算部３０３（に含まれる制御回路３１２）によって読み出され、所望の画像の検証を指示する毎に起動する。
【０２４２】
以上の手順により、選択されたＪＰＥＧデータの正当性が確認されなかった場合、制御回路３１０は各処理回路を制御して該ＪＰＥＧデータを廃棄する。
【０２４３】
以上説明したように、第１１の実施例では、第５の実施例の画像入力装置１０にて撮像され、高能率符号化されたディジタル画像データＰの正当性を、従来のシステムに比べて簡単な構成で認識することができる。又、従来のシステムに比べて安価に構成することも、処理速度を高速化することもできる。更に、ディジタル署名データｈを用いて、ディジタル画像データがどの外部機器によって撮像されたものか、或いはどのユーザにて撮像されたものかを特定することもできる。
【０２４４】
（第１２の実施例）
第１２の実施例では、第６の実施例の画像入力装置１０が生成したディジタル署名データｈを用いて、ディジタル画像データＰの正当性を確認する画像検証装置２０について説明する。
【０２４５】
図２７を用いて、第１２の実施例の処理手順の一例を説明する。
【０２４６】
ステップＳ２７０１～Ｓ２７０４の処理は、上述の第１１の実施例と同様の処理としてその説明を省略する。
【０２４７】
ステップＳ２７０５において、制御／演算部３０３は、画像入力装置１０と供給する秘密情報Ｓ１をメモリ３１３から読み出し、外部装置４０に固有の秘密情報Ｓ２を外部Ｉ／Ｆ部３０１を介して入力する。そして、第６の実施例と同様に、これらの秘密情報Ｓ１，Ｓ２を結合し、新しい秘密情報Ｓを生成する。
【０２４８】

ステップＳ２７０６において、制御／演算部３０３（に含まれる演算回路３１２）は、秘密情報ＳとＪＰＥＧデータとを用いて、予め定められた規則に基づく所定の演算を行う。ここで、演算回路３１２は、第７の実施例のステップＳ２３０４と同様の演算処理を行う。

【０２４９】

ステップＳ２７０７において、制御／演算部３０３（に含まれる演算回路３１２）は、ステップＳ２７０６の演算結果をハッシュ関数で演算する。ここで、演算回路３１２は、第７の実施例のステップＳ２３０５と同様の演算処理を行う。

【０２５０】

ステップＳ２７０８において、制御／演算部３０３（に含まれる演算回路３１２）は、ステップＳ２７０７の演算結果と選択されたＪＰＥＧデータのディジタル署名データｈとを比較する。比較の結果、これらのデータが一致した場合には、ＪＰＥＧデータを正当なものと判断し、一致しなかった場合には、ＪＰＥＧデータに何らかの不正な処理（即ち、ＪＰＥＧデータに対する修正、改竄、偽造、合成等の改変処理）が行われたものと判断する。

【０２５１】

ステップＳ２７０９において、表示部３０４は、ステップＳ２７０８の比較結果を画像或いはメッセージで表示する。これにより、ユーザは、選択したＪＰＥＧデータの正当性を視覚的に分かり易く認識することができる。

【０２５２】

尚、図２７に示す一連の処理手順を制御するプログラムは、ＲＯＭ３０５に格納されている。このプログラムは、制御／演算部３０３（に含まれる制御回路３１２）によって読み出され、所望の画像の検証を指示する毎に起動する。

【０２５３】

以上の手順により、選択されたＪＰＥＧデータの正当性が確認されなかった場合、制御回路３１０は各処理回路を制御して該ＪＰＥＧデータを廃棄する。

【０２５４】

以上説明したように、第１２の実施例では、第６の実施例の画像入力装置１０にて撮像され、高能率符号化されたディジタル画像データＰの正当性を、従来のシステムに比べて簡単な構成で認識することができる。又、従来のシステムに比べて安価に構成することも、処理速度を高速化することもできる。更に、上述のディジタル署名データｈを用いて、ディジタル画像データがどの外部機器と接続された画像入力装置によって撮像されたものか、或いはどのユーザによって使用された画像入力装置にて撮像されたものかを特定することもできる。

【０２５５】

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

【０２５６】

例えば、第１～第６の実施例では、画像入力装置１０内においてディジタル署名データを生成したが、該ディジタル署名データを画像入力装置１０に接続された外部装置４０にて生成することも可能である。このように構成した場合、各装置が互いの装置を認証した後、ディジタル署名データの生成に必要な処理プログラム、高能率符号化されたディジタル画像データ等を画像入力装置１０から外部装置４０に送信し、ディジタル署名データを生成する。

【０２５７】

又、第１～第６の実施例では、ディジタル署名データの生成に必要な演算処理を画像入力装置１０と外部装置４０とに分散させ、各装置が共同してディジタル署名データを生成することも可能である。このように構成した場合、各装置が互いの装置を認証した後、ディジタル署名データの生成に必要な処理プログラム、高能率符号化されたディジタル画像データ等の中で必要な部分のみを画像入力装置１０から外部装置４０に送信し、ディジタル

署名データを生成する。

【０２５８】

又、第７～第１２の実施例では、画像検証装置２０が外部入力されたディジタル画像データを用いてディジタル署名データを生成したが、該ディジタル署名データを画像検証装置２０に接続された外部装置４０にて生成することも可能である。このように構成した場合、各装置が互いの装置を認証した後、ディジタル署名データの生成に必要な処理プログラム、外部入力されたディジタル画像データ等を画像検証装置２０から外部装置４０に送信し、ディジタル署名データを生成する。

【０２５９】

又、第７～第１２の実施例では、ディジタル署名データの生成に必要な演算処理を画像検証装置２０と外部装置４０とに分散させ、各装置が共同してディジタル署名データを生成することも可能である。このように構成した場合、各装置が互いの装置を認証した後、ディジタル署名データの生成に必要な処理プログラム、外部入力されたディジタル画像データ等の中で必要な部分のみを画像検証装置２０から外部装置４０に送信し、ディジタル署名データを生成する。

【０２６０】

又、第７～第１２の実施例では、図２３～図２７に示す一連の処理手順を制御するプログラムは、所望の画像の検証を指示する毎に起動する構成として説明したが、所望の画像を外部入力することに自動的に起動するように構成してもよい。

【０２６１】

従って、前述の各実施例ではあらゆる点で単なる例示に過ぎず、限定的に解釈してはならない。

【０２６２】

【発明の効果】

以上のように、本発明によれば、ディジタル画像データに対する不正な処理（改竄、偽造等）を、簡単な構成で、安価に且つ安全に検出することができる。

【図面の簡単な説明】

【図１】本実施例のディジタル画像検証システムについて説明する図。

【図２】本実施例の画像入力装置の基本構成について説明するブロック図。

【図３】本実施例の画像検証装置の基本構成について説明するブロック図。

【図４】第１の実施例の処理手順を説明するフローチャート。

【図５】第１の実施例における所定の演算処理を説明する図。

【図６】第２の実施例の処理手順を説明するフローチャート。

【図７】第２の実施例におけるＪＰＥＧデータを表す図。

【図８】第２の実施例における秘密情報を説明する図。

【図９】第２の実施例における所定の演算処理を説明する図。

【図１０】第２の実施例におけるハッシュ関数演算の第１のモードを説明する図。

【図１１】第２の実施例におけるハッシュ関数演算の第２のモードを説明する図。

【図１２】第２の実施例におけるハッシュ関数演算の第３のモードを説明する図。

【図１３】第１～第３のモードにおける使用される初期値を説明する図。

【図１４】第３の実施例の処理手順を説明するフローチャート。

【図１５】第３の実施例における秘密情報を説明する図。

【図１６】第３の実施例におけるＣＢＣモードを説明する図。

【図１７】第３の実施例におけるＣＦＢモードを説明する図。

【図１８】第３の実施例におけるＯＦＢモードを説明する図。

【図１９】第４の実施例の処理手順を説明するフローチャート。

【図２０】第４の実施例における秘密情報を説明する図。

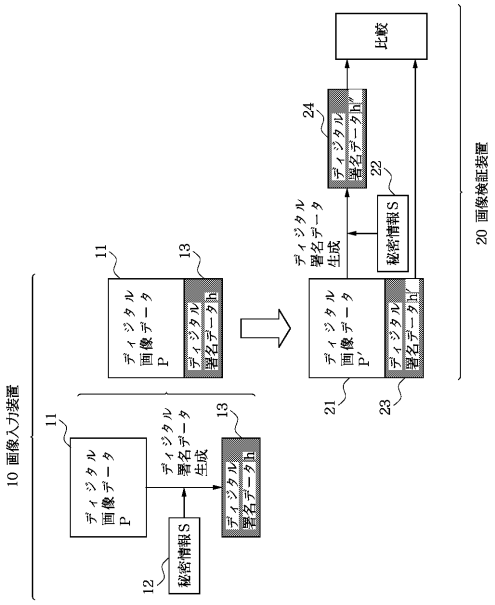
【図２１】第５、第６の実施例の処理手順を説明するフローチャート。

【図２２】画像入力装置と外部装置とを説明する図。

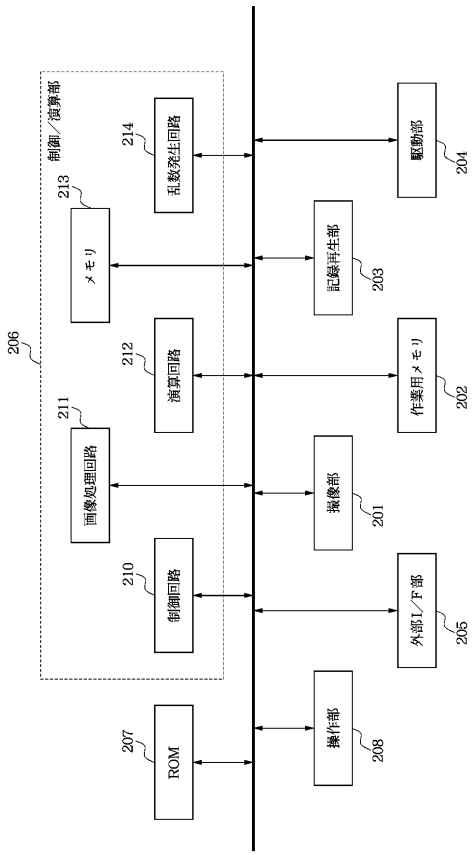
【図２３】第７の実施例の処理手順を説明するフローチャート。

【図２４】第８の実施例の処理手順を説明するフローチャート。
【図２５】第９の実施例の処理手順を説明するフローチャート。
【図２６】第１０の実施例の処理手順を説明するフローチャート。
【図２７】第１１、第１２の実施例の処理手順を説明するフローチャート。
【図２８】従来のシステムを説明する図。

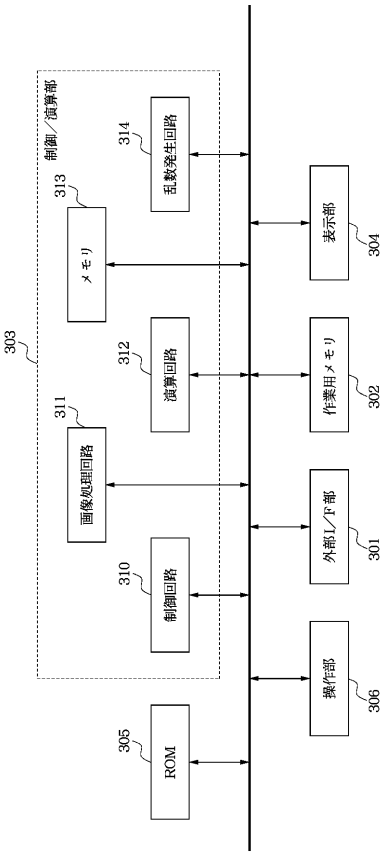
【図１】



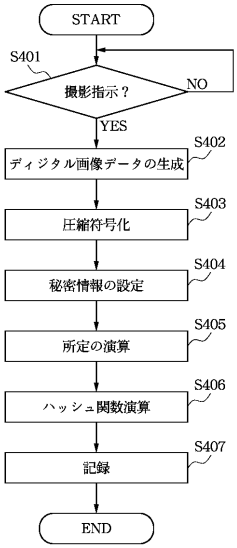
【図２】



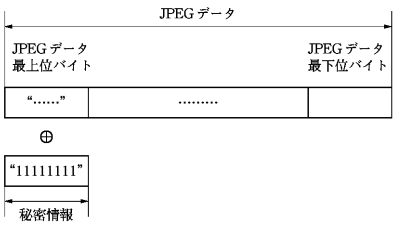
【図３】


制御／演算部
303
乱数発生回路
314
メモリ
313
表示部
304
演算回路
312
作業用メモリ
302
画像処理回路
311
外部I／F部
301
制御回路
310
操作部
306
ROM
305

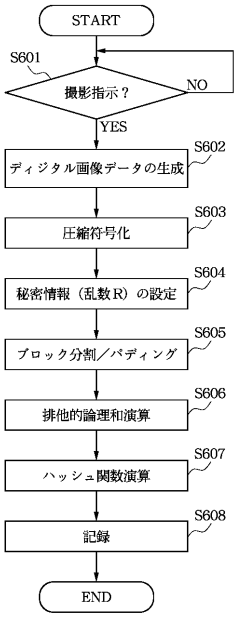
【図４】


START
S401
撮影指示？
NO
YES
ディジタル画像データの生成
S402
圧縮符号化
S403
秘密情報の設定
S404
所定の演算
S405
ハッシュ関数演算
S406
記録
S407
END

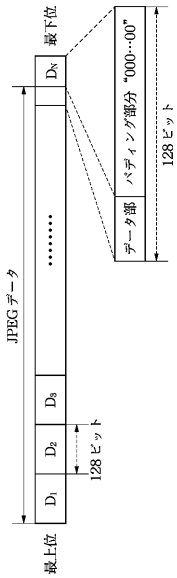
【図５】


JPEG データ
JPEG データ
最上位バイト
JPEG データ
最下位バイト
“……”
……
⊕
“11111111”
秘密情報

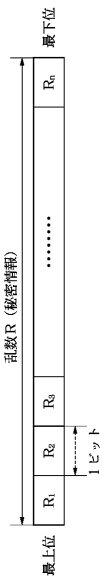
【図６】


START
S601
撮影指示？
NO
YES
ディジタル画像データの生成
S602
圧縮符号化
S603
秘密情報（乱数R）の設定
S604
ブロック分割／パディング
S605
排他的論理和演算
S606
ハッシュ関数演算
S607
記録
S608
END

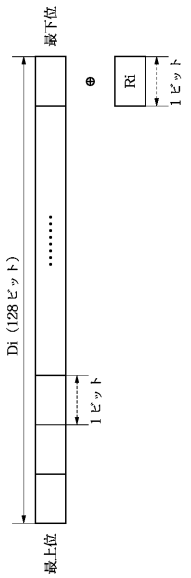
【図７】


JPEGデータ
最上位
最下位
D1
D2
D3
Dk
128ビット
データ部
パディング部分 "000…00"
128ビット

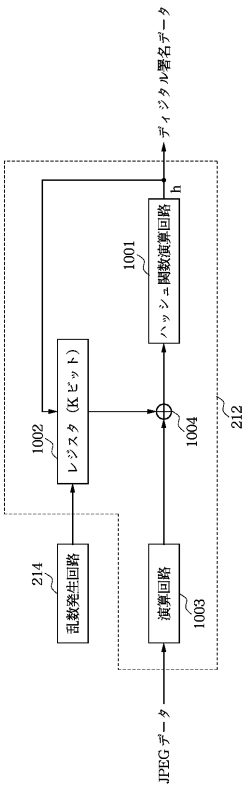
【図８】


乱数R（秘密情報）
最上位
最下位
R1
R2
R3
Rn
1ビット

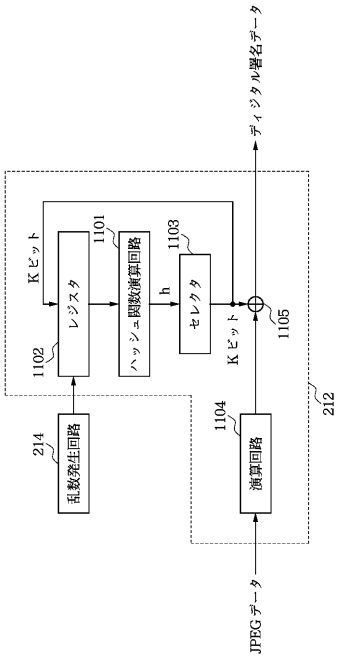
【図９】


Di（128ビット）
最上位
最下位
1ビット
⊕
Ri
1ビット

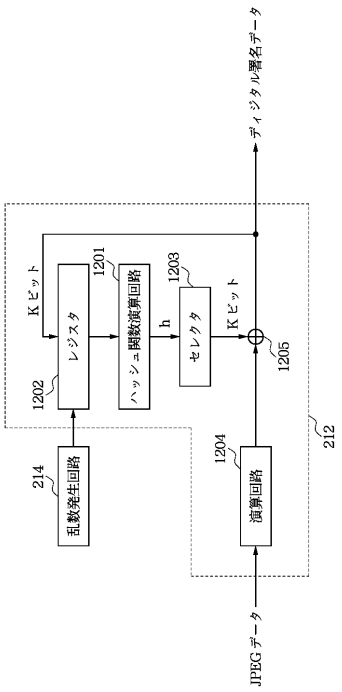
【図１０】


JPEGデータ
ディジタル署名データ
214
乱数発生回路
1002
レジスタ（Kビット）
1003
演算回路
1004
1001
ハッシュ関数演算回路
h
212

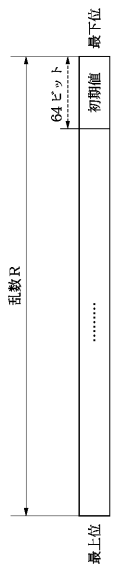
【図１１】



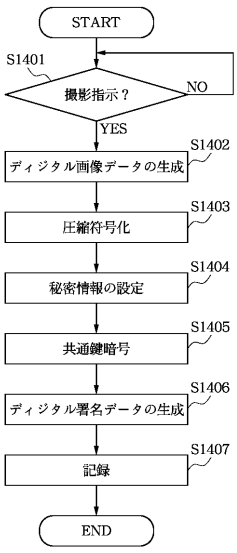
【図１２】



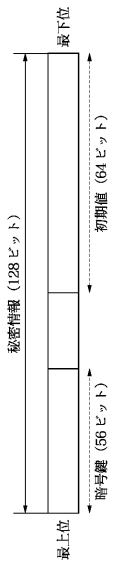
【図１３】



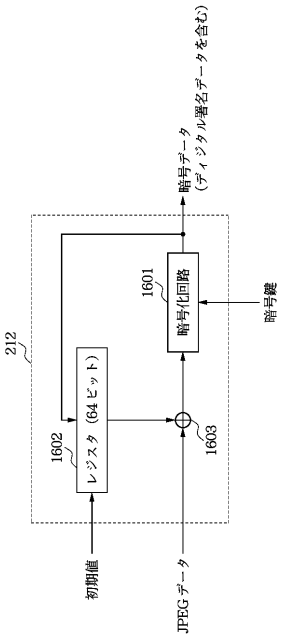
【図１４】



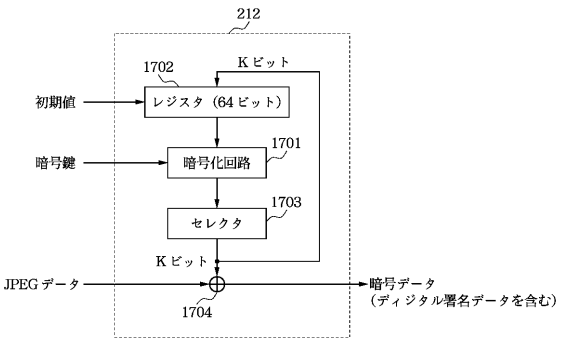
【図１５】



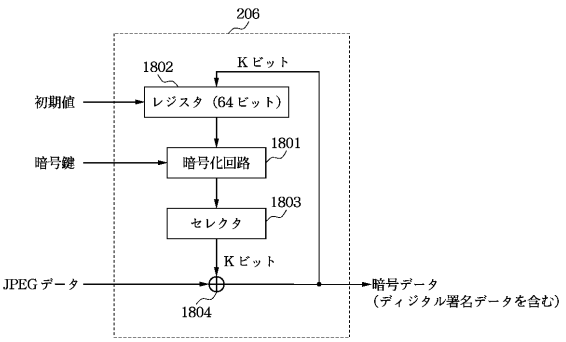
【図１６】



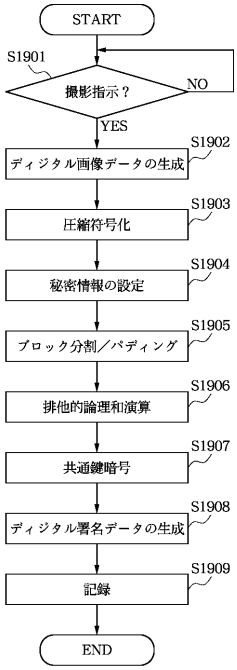
【図１７】



【図１８】

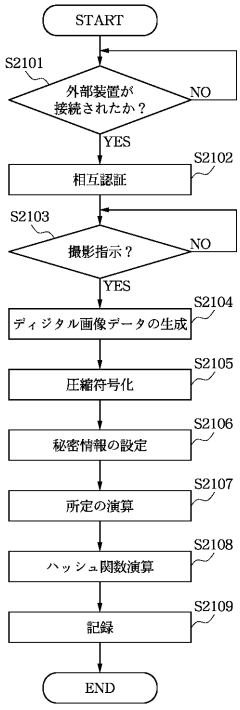


【図１９】

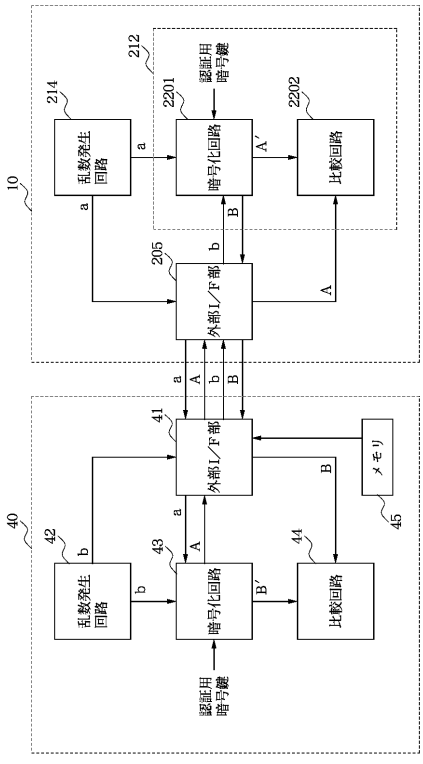


【図２０】

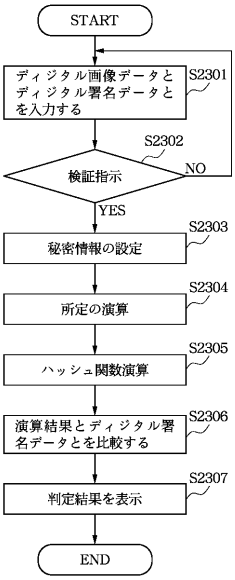
【図２１】



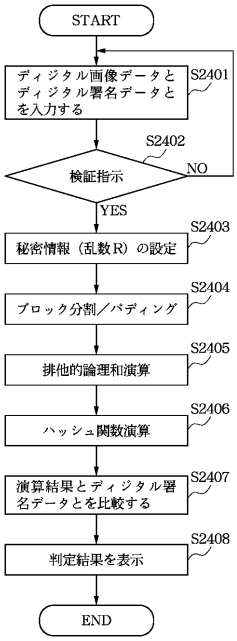
【図２２】



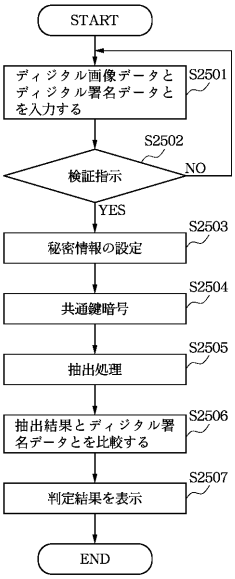
【図２３】



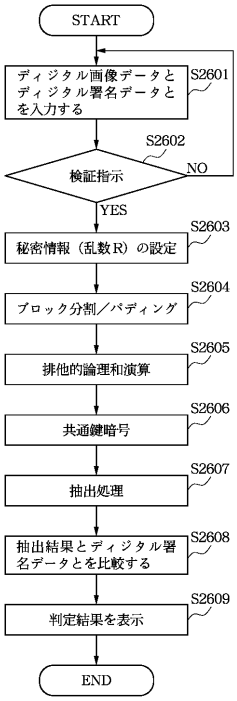
【図２４】



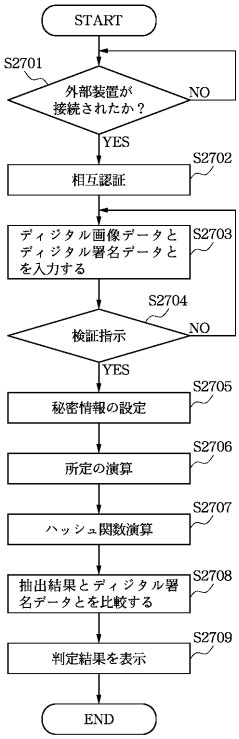
【図２５】



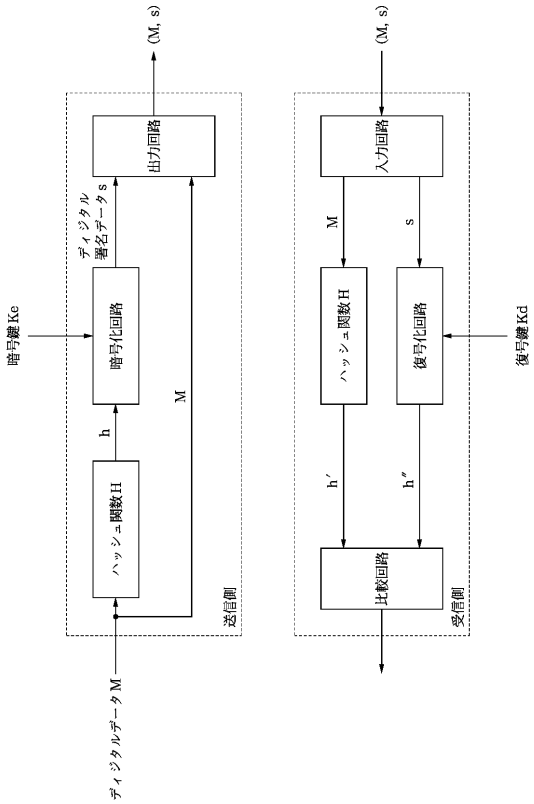
【図２６】



【図２７】


START
S2701
外部装置が接続されたか？
NO
YES
S2702
相互認証
S2703
ディジタル画像データとディジタル署名データとを入力する
S2704
検証指示
NO
YES
S2705
秘密情報の設定
S2706
所定の演算
S2707
ハッシュ関数演算
S2708
抽出結果とディジタル署名データとを比較する
S2709
判定結果を表示
END

【図２８】


(M, s)
出力回路
ディジタル署名データs
暗号鍵Ke
暗号化回路
h
ハッシュ関数H
M
送信側
ディジタルデータM
(M, s)
入力回路
M
s
ハッシュ関数H
復号化回路
復号鍵Kd
h′
h″
比較回路
受信側

フロントページの続き

(56)参考文献 特開平１０－１６４５４９（ＪＰ，Ａ）
特開平１０－１０７７８８（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
H04N 1/387