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

特許第4310285号
(P4310285)

(45)発行日　平成21年8月5日(2009.8.5)　(24)登録日　平成21年5月15日(2009.5.15)

(51)Int.Cl.			F I		
H04N	1/387	(2006.01)	H04N	1/387	
G06T	1/00	(2006.01)	G06T	1/00	500B
H04N	1/40	(2006.01)	H04N	1/40	Z

請求項の数 9　(全 20 頁)

(21)出願番号　特願2005-33016(P2005-33016)
(22)出願日　平成17年2月9日(2005.2.9)
(65)公開番号　特開2006-222628(P2006-222628A)
(43)公開日　平成18年8月24日(2006.8.24)
審査請求日　平成20年2月1日(2008.2.1)

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

審査官　白石　圭吾

最終頁に続く

(54)【発明の名称】情報処理方法及び装置、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】
デジタルデータの部分的な完全性を検証するための検証データを生成する情報処理方法であって、
前記デジタルデータに含まれる部分データを取得する部分データ取得工程と、
前記デジタルデータを識別する識別情報と前記部分データを特定する特定情報を取得する情報取得工程と、
前記デジタルデータの識別情報と前記部分データの特定情報と前記部分データとから、検証データを生成する検証データ生成工程とを有することを特徴とする情報処理方法。
【請求項２】
前記デジタルデータは画像データであり、前記部分データの特定情報は、前記画像データに含まれる領域、解像度、画質、成分、或いは、これらの組み合わせを特定する情報であることを特徴とする請求項１に記載の情報処理方法。
【請求項３】
前記デジタルデータは複数の要素内容から構成される文書データであり、前記部分データの特定情報は、前記文書データに含まれる要素内容を特定する情報、及び前記部分データは、前記文書データに含まれる要素内容であることを特徴とする請求項１に記載の情報処理方法。
【請求項４】
前記デジタルデータはデータベース情報であり、前記部分データ特定情報は、前記デー

タベース情報に含まれるレコードを特定する情報、及び前記部分データは、前記データベース情報に含まれるレコードであることを特徴とする請求項１に記載の情報処理方法。
【請求項５】
請求項１～４の何れか１項に記載された情報処理方法で生成された検証データを用いて、前記デジタルデータの部分的な完全性を検証する情報処理方法であって、
前記検証データを取得する検証データ取得工程と、
前記デジタルデータに含まれる部分データを取得する部分データ取得工程と、
前記デジタルデータを識別する識別情報と前記部分データを特定する特定情報を取得する情報取得工程と、
前記デジタルデータの識別情報と前記部分データの特定情報と前記部分データとから、検証データを生成する検証データ生成工程と、
前記検証データ取得工程で取得した検証データと、前記検証データ生成工程で生成した検証データを用いて、前記部分データと前記デジタルデータとの関連が正しいかを検証する検証工程とを有することを特徴とする情報処理方法。
【請求項６】
デジタルデータの部分的な完全性を検証するための検証データを生成する情報処理装置であって、
前記デジタルデータに含まれる部分データを取得する部分データ取得手段と、
前記デジタルデータを識別する識別情報と前記部分データを特定する特定情報を取得する情報取得手段と、
前記デジタルデータの識別情報と前記部分データの特定情報と前記部分データとから、検証データを生成する検証データ生成手段とを有することを特徴とする情報処理装置。
【請求項７】
請求項６に記載された情報処理装置で生成された検証データを用いて、前記デジタルデータの部分的な完全性を検証する情報処理装置であって、
前記検証データを取得する検証データ取得手段と、
前記デジタルデータに含まれる部分データを取得する部分データ取得手段と、
前記デジタルデータを識別する識別情報と前記部分データを特定する特定情報を取得する情報取得手段と、
前記デジタルデータの識別情報と前記部分データの特定情報と前記部分データとから、検証データを生成する検証データ生成手段と、
前記検証データ取得手段で取得した検証データと、前記検証データ生成手段で生成した検証データを用いて、前記部分データと前記デジタルデータとの関連が正しいかを検証する検証手段とを有することを特徴とする情報処理装置。
【請求項８】
コンピュータに、請求項１～５の何れか１項に記載の情報処理方法を実行させるコンピュータプログラム。
【請求項９】
請求項８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可読記憶媒体。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明はデジタルデータの検証技術に関するものである。
【背景技術】
【０００２】
従来、画像データの全体ではなく部分的な領域データが改ざんされているか否かを検証することを目的とした署名方法が提案されていた（特許文献１参照）。特許文献１で提案されているデジタル画像に対する署名方法は、図１７に示すように、まず、画像のＲＯＩを選択し（ステップＳ１３１）、選択したＲＯＩのハッシュ値を算出し（ステップＳ１３

２）、算出したハッシュ値を秘密鍵で暗号化することによってデジタル署名を生成しステップＳ１３３、デジタル署名を画像に添付する（ステップＳ１３４）ものである。
【特許文献１】ＵＳＰ５，８９８，７７９
【発明の開示】
【発明が解決しようとする課題】
【０００３】
以上説明したように、従来の技術によれば、原画像データ中の領域データが改竄されているか否かを検証することは可能であったが、前記領域データと原画像データにある部分画像データであるのかを検証することや、部分画像データが原画像データ中の正しい位置の領域データであるのかなど、領域データと原画像データの関連が正しいかを検証することは困難であった。つまり、本来の原画像データとは異なる原画像データに、デジタル署名を有する部分画像データを付加するといった改ざんが行われたとしても、検出することはできなかった。また、部分画像データを本来の原画像データ中の異なる領域データに置き換えるという改ざんがされたとしても、異なる領域データのデジタル署名が存在すれば改ざんを検出することはできなかった。
【０００４】
本発明は、かかる問題点に鑑みなされたものであり、画像データ中の領域データが改竄されているか否かを検証することに加え、前記領域データが本来の原画像データ中とは異なる原画像データ中の領域データであることを検証可能、且つ／或いは、前記領域データが本来の原画像データ中の異なる領域データであることを検証可能とする技術を提供しようとするものである。
【課題を解決するための手段】
【０００５】
上記課題を解決するため、本発明に係る情報処理方法は、デジタルデータの部分的な完全性を検証するための検証データを生成する情報処理方法であって、前記デジタルデータに含まれる部分データを取得する部分データ取得工程と、前記デジタルデータを識別する識別情報と前記部分データを特定する特定情報を取得する情報取得工程と、前記デジタルデータの識別情報と前記部分データの特定情報と前記部分データとから、検証データを生成する検証データ生成工程とを有することを特徴とする。
【０００６】
また、上記課題を解決するため、本発明に係る情報処理装置は、デジタルデータの部分的な完全性を検証するための検証データを生成する情報処理装置であって、前記デジタルデータに含まれる部分データを取得する部分データ取得手段と、前記デジタルデータを識別する識別情報と前記部分データを特定する特定情報を取得する情報取得手段と、前記デジタルデータの識別情報と前記部分データの特定情報と前記部分データとから、検証データを生成する検証データ生成手段とを有することを特徴とする。
【発明の効果】
【０００７】
以上説明したように本発明によれば、画像データ中の領域データが改竄されているか否かを検証することに加え、前記領域データが本来の原画像データ中とは異なる原画像データ中の領域データであること、且つ／或いは、前記領域データが本来の原画像データ中の異なる領域データであることが検証可能となる。
【発明を実施するための最良の形態】
【０００８】
＜全体構成の説明＞
まずはじめに、本実施形態におけるシステム概要例を図１に示す。本実施形態におけるシステムは、画像再生クライアント１１、画像配信サーバ１２、画像ＤＢ１３、及びネットワーク１４から構成される。
【０００９】
図中、装置１１は画像再生クライアントであって、画像配信サーバ１２に対し所望の画

像データの取得要求を送信し、画像配信サーバ１２からネットワーク１４経由で配信された画像データ再生を行う。また、本実施形態においては、画像データに加え、当該画像データに対応する検証データを受信し、画像データが改竄されているか否かの検証も行う。

【００１０】

装置１２は、画像再生クライアント１１から受信した画像データの取得要求に応答し、画像ＤＢ１３に蓄積されている画像データを配信する画像配信サーバである。また、本実施形態においては、画像データに加え、当該画像データが改竄されているか否かを画像再生クライアント１１で検証可能な検証データを生成し、画像再生クライアント１１へ送信する。

【００１１】

装置１１、及び装置１２はインターネットなどのネットワーク１４によって接続されており、各種データを互いに交換可能である。また、装置１１、及び装置１２は通常の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。

【００１２】

画像閲覧者は、画像再生クライアント１１を利用して、所望の画像データを画像配信サーバ１２に要求する。この際に、画像閲覧者は、画像データ全体ではなく、部分的な画像データを指定し、要求することが可能である（図１における「１．部分データ要求」）。

【００１３】

画像配信サーバ１２は、画像再生クライアント１１から要求された部分画像データを画像ＤＢ１３から取得し（図１における「２．部分データ取得」）、当該部分画像データに対応する検証データを生成する（図１における「３．検証データ生成処理」）。そして、取得した部分画像データ、及び生成した検証データを画像再生クライアント１１に送信する（図１における「４．部分データ，及び検証データ送信」）。

【００１４】

画像再生クライアント１１は、部分データ、及び検証データを受信し、当該検証データを利用して、受信した部分画像データが正しい部分画像データか否かを検証し、検証結果を表示する。更に、受信した部分データを再生する。

【００１５】

以上が、本実施形態におけるシステムの概要例である。

【００１６】

ここで、以上説明したような画像配信システムにおいて、画像再生クライアント１１に適応可能な部分データ要求、画像データ検証処理、及び、画像データ再生処理の操作画面例（ウィンドウ）について図２を用いて説明する。

【００１７】

図２において、２１はそのウィンドウである。ウィンドウ２１の上部には、所望の画像データの「画像ＩＤ」を指定するための欄２２を有する。欄２２は不図示のキーボード等により画像ＩＤを直接入力することにより指定する。欄２２の右部には、欄２２によって指定された画像ＩＤのサムネイルを取得し、表示するためのボタン２３を有する。

【００１８】

不図示のマウス等によりボタン２３をクリックすることにより、欄２２で指定された画像ＩＤに対応する画像データのサムネイルがサムネイルビューア２４に表示される。

【００１９】

サムネイルが表示された後、利用者はマウス等を利用してサムネイル中の所望の領域２５を自由に選択できる。サムネイルビューア２４の下部には、領域２５によって指定された領域の詳細な情報表示するためのボタン２６を有する。所望の領域２５を選択した状態で、マウス等によりボタン２６をクリックすることにより、領域２５で指定された部分データの詳細が画像ビューア２７に表示される。更に、画像ビューア２７に表示された部分データが正しい部分データか否かを示す検証処理結果が、欄２８に表示される。

【００２０】

ボタン２６をクリックすることにより、図１における「１．部分データ要求」、「２．部分データ取得」、「３．署名生成」、「４．部分データ、及び署名送信」、及び「５．部分データ再生、及び署名検証」の一連の処理が自動的に実行されると考えれば理解しやすい。

【００２１】

尚、図２に示したウィンドウは本発明に適応可能な一実施例を示すものであり、本発明はこれに限定されるものでないことは明らかである。

【００２２】

次に、図３を用いて、本実施の形態に適応可能なホストコンピュータについて説明する。図３は本実施形態に係る画像再生クライアント、及び画像配信サーバとして機能するホストコンピュータの基本構成を示すと共に、その周辺機器との関係を示す図である。同図において、ホストコンピュータ２１２は、例えば一般に普及しているパーソナルコンピュータであり、ＨＤ１２６、ＣＤ１２７、ＦＤ１２８、及びＤＶＤ１２９などに蓄積したり、或いは、蓄積されている画像データをモニタ１２２に表示したりすることが可能である。更に、ＮＩＣ１２１０などを用いて、これらの画像データをインターネットなどを介して配布させることが可能である。また、ユーザからの各種指示等は、マウス１２１３、及びキーボード１２１４からの入力により行われる。ホストコンピュータ１２１の内部では、ます１２１６により後述する各ブロックが接続され、種々のデータの受け渡しが可能である。

【００２３】

図中、１２２は、ホストコンピュータ１２１からの種々の情報を表示することの出来るモニタである。

【００２４】

１２３は、ホストコンピュータ１２１内の各部の動作を制御、或いはＲＡＭ１２５にロードされたプログラムを実行することのできるＣＰＵである。１２４は、ＢＩＯＳやブートプログラムを記憶しているＲＯＭである。１２５はＣＰＵ１２３にて処理を行うために一時的にプログラムや処理対象の画像データを格納しておくＲＡＭであり、ここにＯＳやＣＰＵ３３が後述の各種処理を行うためのプログラムがロードされることになる。

【００２５】

１２６は、ＲＡＭ等に転送されるＯＳやプログラムを格納したり、装置が動作中に画像データを格納したり、読出すために使用されるハードディスク（ＨＤ）である。１２７は、外部記憶媒体の一つであるＣＤ－ＲＯＭ（ＣＤ－Ｒ）に記憶されたデータを読み込み或いは書き出すことのできるＣＤ－ＲＯＭドライブである。

【００２６】

１２８は、ＣＤ－ＲＯＭドライブ３７と同様にＦＤ（フロッピー（登録商標）ディスク）からの読み込み、ＦＤへの書き出しができるＦＤドライブである。１２９も、ＣＤ－ＲＯＭドライブ１２７と同様にＤＶＤ－ＲＯＭからの読み込み、ＤＶＤ－ＲＡＭへの書き出しができるＤＶＤ－ＲＯＭ（ＤＶＤ－ＲＡＭ）ドライブである。尚、ＣＤ－ＲＯＭ、ＦＤ、ＤＶＤ－ＲＯＭ等に画像処理用のプログラムが記憶されている場合には、これらプログラムをＨＤ１２６にインストールし、必要に応じてＲＡＭ１２５に転送されるようになっている。

【００２７】

３１１は、ＲＡＭ１２５、ＨＤ１２６、ＣＤ－ＲＯＭ１２７、ＦＤ１２８、ＤＶＤ１２９などに記憶されている画像データを、インターネットなどのネットワークに接続するＮＩＣ１２１０にホストコンピュータ１２１を接続するためのＩ／Ｆで、Ｉ／Ｆ１２１１を介してホストコンピュータ１２１は、Ｉ／Ｆ１２１１を介してインターネットへデータを送信したり、インターネットからデータを受信したりする。

【００２８】

１２１５は、ホストコンピュータ１２１にマウス１２１３やキーボード１２１４を接続するためのＩ／Ｆで、Ｉ／Ｆ１２１５を介してマウス１２１３やキーボード１２１４から

入力された各種の指示がＣＰＵ１２３に入力される。

【００２９】

＜検証データ生成処理＞

次に、本実施形態に適応可能な検証データ生成処理部、及び方法について図４を用いて説明する。

【００３０】

図４は、本実施形態における検証データ生成処理機能、及び方法を説明する図である。図４において、３１は画像識別情報取得部、３２は部分データ特定情報取得部、３３は部分データ取得部、３４は結合処理部、３５は鍵取得部、３６は検証データ生成処理部である。

【００３１】

図４に示す検証データ生成処理機能は、前述した画像配信サーバ１２（図１）に搭載される一機能である。

【００３２】

まず、画像識別情報取得部３１、及び部分データ特定情報取得部３２について説明する。画像識別情報取得部３１、及び部分データ特定情報取得部３２は、夫々、画像再生クライアント１１から要求された画像識別情報ＩＤ、及び部分データ特定情報Ｚを取得し、出力する。

【００３３】

ここで、画像識別情報ＩＤとは画像データを特定するための情報、及び、部分データ特定情報Ｚとは、前記画像データ中の部分的なデータを特定するための情報である。

【００３４】

本実施形態では、画像識別情報ＩＤとして、画像データのファイル名を用いる場合の例を説明するが、本発明はこれに限定されることなく、画像データの存在位置を示すＵＲＬ、画像データを一意に識別するＵＲＩ、画像データのハッシュ値など種々の値を適応可能であることは明らかである。

【００３５】

また、本実施形態では、部分データとして、図２における領域２５で示したような画像データ中の部分的な矩形領域を用いる。部分データとして矩形領域を用いた場合、部分データ特定情報Ｚとして、矩形領域の左上の座標情報（ｘ１、ｙ１）、及び右下の座標情報（ｘ２、ｙ２）を利用すればよい。

【００３６】

尚、本発明はこれに限定されることなく、矩形領域の他にも、領域を特定可能な種々の部分データ特定情報が適用可能であることは明らかである。

【００３７】

例えば、任意形状領域を部分データとして指定する場合、部分データ特定情報Ｚとしては、部分データとして指定された位置に対応する画素を「０」、及び部分データとして指定されない位置に対応する画素を「１」としたような二値画像データを利用すればよい。例えば、図５に示すように、ハートの外部（１７１）が「０」、ハートの内部（１７２）が「１」であるような二値画像を部分データ特定情報Ｚとして適用可能である。

【００３８】

また、画像データが互いに重ならない複数のタイルに分割されている場合、部分データ特定情報Ｚとして、タイルを識別するようなタイルインデックスを利用すればよい。

【００３９】

何れにせよ、部分データを一意に特定可能な種々の情報を部分データ特定情報として適用可能である。

【００４０】

次に、部分データ取得部３３について説明する。部分データ取得部３３は、前述した画像識別情報取得部３１、及び部分データ特定情報取得部３２によって取得された画像識別情報ＩＤ、及び部分データ特定情報Ｚを用いて、ＩＤ，及びＺに対応する部分データＭを

画像ＤＢ１３から取得し、出力する。

【００４１】

前述したように、本実施形態においては、部分データＭとしては、画像データ中の部分的な矩形領域のデータが出力される。

【００４２】

次に、結合処理部３４について説明する。結合処理部３４では、前段の画像識別情報取得部３１、部分データ特定情報取得部３２、及び部分データ取得部３３から出力された、画像識別情報ＩＤ、部分データ特定情報Ｚ、及び部分データＭが入力され、これらを結合し、結合データＤが出力される。

【００４３】

ここで、本実施形態における結合データＤについて図６を用いて説明する。図６に示すように、本実施形態では、画像識別情報ＩＤ、部分データ特定情報Ｚ、及び部分データＭを所定の順序で連結した情報を結合データＤとする。尚、連結する順序は、図６の順でなくてもよいのは言うまでもない。

【００４４】

次に、鍵取得部３５について説明する。鍵取得部３５では、後述する検証データ生成処理部３６における検証データ生成処理のために必要な鍵情報Ｋｓが取得され、出力される。

【００４５】

尚、本実施形態における鍵情報Ｋｓの詳細については、後述する。

【００４６】

次に、検証データ生成処理部３６について説明する。検証データ生成処理部３６では、前段の結合処理部３４から出力された結合データＤ、及び鍵取得部３５から出力された鍵情報Ｋｓが入力され、鍵情報Ｋｓを利用して結合データＤに対応する検証データＳが生成され、生成された検証データＳが出力される。

【００４７】

本実施形態では、検証データ生成処理としては特に限定せず、ＲＳＡやＤＳＡなどのデジタル署名生成アルゴリズムや、ＨＭＡＣやＣＭＡＣなどのＭＡＣ生成アルゴリズムなど種々の検証データ生成処理を適応可能である。検証データ生成処理として、デジタル署名生成アルゴリズムを用いる場合、前述した鍵取得部３５で取得される鍵情報Ｋｓは画像配信サーバ１２の秘密鍵とする。また、ＭＡＣ生成アルゴリズムを用いた場合は、鍵情報Ｋｓは画像配信サーバ１２、及び画像配信サーバ１１とで安全に共有される共有鍵とする。

【００４８】

尚、結合データＤに対して検証データ生成処理を施す前に、ＭＤ５やＳＨＡ１などのハッシュ関数を結合データＤに適用し、ハッシュ関数の出力値に対して検証データ生成処理を適用するようにしてもよい。

【００４９】

以上、本実施形態における検証データ生成処理、及び方法について説明した。

【００５０】

次に、以上説明したような検証データ生成処理、及び方法の流れを図７を用いて説明する。図７は本実施形態に適応可能な検証データ生成処理を説明するフローチャートである。

【００５１】

まず、ステップＳ５１は、画像識別情報ＩＤ、及び部分データ特定情報Ｚを取得する（図４の３１、及び３２）。そして、ステップＳ５２は、前記画像識別情報ＩＤ、及び部分データ特定情報Ｚに対応する部分データＭを取得する（図４の３３）。その後、ステップＳ５３は、取得された画像識別情報ＩＤ、部分データ特定情報Ｚ、及び部分データＭを結合し、結合データＤを生成する（図４の３４）。そして、ステップＳ５４が、検証データを生成するための鍵情報Ｋｓを取得した後、ステップＳ５５が結合データＤの検証データＳを鍵情報Ｋｓを用いて生成し、検証データ生成処理を終了する。

【００５２】
＜検証処理、及び方法＞
次に、本実施形態に適応可能な検証処理、及び方法について図８を用いて説明する。
【００５３】
図８は、本実施形態における検証処理、及び方法を説明する図である。図８において、６１は検証データ取得部、６２は鍵取得部、６３は検証データ復号部、６４は画像識別情報取得部、６５は部分データ特定情報取得部、６６は部分データ取得部、６７は結合処理部、及び６８は比較部である。
【００５４】
図８に示す検証処理機能は、前述した画像再生クライアント１１（図１）に搭載される一機能である。
【００５５】
まず、検証データ取得部６１について説明する。検証データ取得部６１では、画像配信サーバ１２から送信された検証データＳを取得し、出力する。ここで取得される検証データＳは、図４における検証データ生成処理部３６から出力されたデータであると考えれば理解しやすい。
【００５６】
次に、鍵取得部６２について説明する。鍵取得部６２では、後段の検証データ復号部６３で検証データ復号処理のために必要な鍵情報Ｋｐが取得され、出力される。
【００５７】
鍵取得部６２において取得される鍵情報Ｋｐは、図４における鍵取得部３５において取得された鍵情報Ｋｓに対応する情報である。即ち、鍵取得部３５において画像配信サーバ１２の秘密鍵が鍵情報Ｋｓとして取得された場合、鍵取得部６２では、鍵情報Ｋｓと対になる画像配信サーバ１２の公開鍵を鍵情報Ｋｐとして取得するようにする。一方、鍵取得部３５において共有鍵が鍵情報Ｋｓとして取得された場合、鍵取得部６２では、鍵情報Ｋｓと等しい値を鍵情報Ｋｐとして取得するようにする。
【００５８】
次に、検証データ復号部６３について説明する。検証データ復号部６３では、検証データ取得部で取得された検証データＳ、及び鍵取得部Ｋｐで取得された鍵情報Ｋｐが入力され、鍵情報Ｋｐを用いて検証データＳを復号し、復号された値Ｄが出力される。
【００５９】
検証データ復号部６３で実行される検証データ復号処理は、図４における検証データ生成処理部３６で実行された検証データ生成処理に対応する処理を適用するようにする。
【００６０】
尚、特に、検証データとしてＭＡＣを利用している場合には、検証データ復号処理を実行しないようにしても良い。この場合、入力された検証データＳと同じ値がＤとして出力される。
【００６１】
次に、画像識別情報取得部６４、及び部分データ特定情報取得部６５について説明する。画像識別情報取得部６４、及び部分データ特定情報取得部６５は、夫々、後述する部分データ取得部６６で取得される部分データに対応する画像データ、及び部分データを特定するための情報を取得し、出力する。
【００６２】
画像識別情報ＩＤ、及び部分データ特定情報Ｚは、夫々図４における画像識別情報取得部３１、及び部分データ特定情報取得部３２において取得された画像識別情報ＩＤ、及び部分データ特定情報Ｚと等しい情報を取得するようにする。本実施形態では、部分データ要求処理の前に、予め図２における欄２２、及び領域２５によって指定される画像識別情報、及び部分データ特定情報をＲＡＭ１２５（図３）に保持しておき、検証処理段階において、ＲＡＭ１２５に保持されている画像識別情報ＩＤ、及び部分データ特定情報Ｚを取得するようにすれば良い。

【００６３】
尚、本発明はこれに限定されることなく、画像配信サーバ１２から画像再生クライアント１１へ、結合データＤ（図６）が配信されるようにし、且つ、受信した結合データＤ中の画像識別情報ＩＤ、及び部分データ特定情報Ｚを、画像識別情報取得部６４、及び部分データ特定情報取得部６５において取得するようにしてもよい。この場合、部分データ要求時に指定した画像識別情報ＩＤ、及び部分データ特定情報Ｚと、取得した画像識別情報ＩＤ、及び部分データ特定情報Ｚを比較し、一致しない場合には、「受信した部分データＭ’は正しくない」と判定し、処理を中止するようにしても良い。
【００６４】
次に、部分データ取得部６６について説明する。部分データ取得部６６では、画像配信サーバ１２から送信された部分データＭ’を取得し、出力する。ここで取得される部分データＭ’は、図４における部分データ取得部３３から出力されたデータであると考えれば理解しやすい。
【００６５】
次に、結合処理部６７について説明する。結合処理部６７では、前段の画像識別情報取得部６４、部分データ特定情報取得部６５、及び部分データ取得部６６において取得された、画像識別情報ＩＤ、部分データ特定情報Ｚ、及び部分データＭ’が入力され、これらを結合し、結合データＤ’が出力される。
【００６６】
ここで、結合データＤ’は、前段の画像識別情報取得部６４、部分データ特定情報取得部６５、及び部分データ取得部６６から取得された画像識別情報ＩＤ、部分データ特定情報Ｚ、及び部分データＭ’を図４における結合処理部３４と同様の方法で結合して生成される。
【００６７】
尚、前述したように、検証データ生成処理部３６（図４）において、ハッシュ関数が適用されている場合には、結合処理部６７でＤ’を生成した後、検証データ生成処理部３６で適用したハッシュ関数と同じハッシュ関数をＤ’に対して適用し、ハッシュ値を出力するようにする。もちろん、その後、ハッシュ値を秘密鍵で暗号化し、デジタル署名を生成しても構わないのは言うまでもない。
【００６８】
更に、検証データとしてＭＡＣを利用している場合には、鍵取得部６３で取得したＫｐを用いて、結合データＤ（或いは、そのハッシュ値）のＭＡＣを生成し、生成したＭＡＣを出力するようにする。
【００６９】
次に、比較部６８について説明する。比較部６８では、前段の検証データ復号部６３から出力された値Ｄ、及び比較部６８から出力された値Ｄ’を比較し、検証結果を出力する。
【００７０】
本実施形態においては、値Ｄと値Ｄ’が値が一致していたら「部分データＭ’は正しいデータ（検証成功）」であると判定する。一方、値Ｄと値Ｄ’が異なっていたら「部分データＭ’は正しいデータではない（検証失敗）」と判定する。
【００７１】
以上、本実施形態における検証処理、及び方法について説明した。
【００７２】
次に、以上説明したような検証データ生成処理、及び方法の流れを図９を用いて説明する。図９は本実施形態適応可能な検証データ生成処理を説明するフローチャートである。
【００７３】
まず、ステップ７１は、検証データＳ、及び鍵情報Ｋｐを取得する（図８の６１、及び６２）。そして、ステップ７２は、前記検証データＳを前記鍵情報Ｋｐを用いて復号し、Ｄを算出する（図８の６３）。また、ステップＳ７３は、画像識別情報ＩＤ、部分データ

特定情報Ｚ、及び部分データＭ’を取得する（図８の６４、６５、及び６６）。そして、ステップＳ７４は、画像識別情報ＩＤ、及び部分データ特定情報Ｚ、及び部分データＭ’を結合し、Ｄ’を生成する（図８の７４）。その後、ステップＳ７５は、Ｄ、及びＤ’が等しいか否かを判定する。等しい場合には「部分データＭ’は正しいデータ（検証成功）」、また等しくない場合には「部分データＭ’は正しいデータではない（検証失敗）」と表示し、検証処理を終了する。

【００７４】

以上、本実施形態に適応可能な検証データ生成処理（方法）、及び検証処理（方法）について説明した。

【００７５】

＜検証結果例＞

ここで、以上説明したような検証データ生成処理、及び検証処理を適応した場合の種々の検証結果について、従来技術と本実施形態を比較しながら、具体的な例を用いて説明する。

【００７６】

まず、前述した本実施形態におけるシステム（図１）に対して、従来の技術であるＵＳＰ５，８９８，７７９を適用した場合の例を説明する。この場合、サーバにおいて領域データを配信する際に、配信すべき領域データ（ＲＯＩ）に対してデジタル署名を生成し、領域データと共に領域データに対するデジタル署名をクライアントに配信するようにする。その後、クライアントにおいて受信した領域データをデジタル署名を用いて検証することにより、受信した領域データがネットワークの途中で改竄されたか否かを検証することが可能である。

【００７７】

この具体例を、図１０を用いて説明する。図１０において、１６１はサーバに保持されている画像データ、１６２はクライアントによって要求された領域、１６３は領域１６２を切り出した領域データ、１６４は領域データ１６３のデジタル署名である。

【００７８】

クライアントからサーバに対して、画像データ１６１に含まれる領域１６２の配信要求が発生した際に、サーバは、領域１６２を画像データ１６１から切り出して領域データ１６３を生成すると共に、領域データ１６３のデジタル署名１６４を生成する。そして、生成した領域データ１６３、及びそのデジタル署名１６４をクライアントに配信する。すると、クライアントでは、領域データ１６３、及びそのデジタル署名１６４を用いて、領域データ１６３がネットワークの途中で改竄されたか否かをクライアントで検証することが可能である。

【００７９】

さて、まず、従来技術による検証結果例について、図１１を用いて説明する。図１１において、１４１はクライアントによって要求された画像データＩ０００１、１４２はクライアントによって要求された画像データＩ０００１中の一部の領域、１４３は画像データＩ０００１とは異なる画像データＩ０００２、１４４は画像データＩ０００２において領域１４２と同じ位置に対応する領域、１４９は画像データＩ０００１中で領域１４２と異なる位置の領域である。ここで、画像データＩ０００１、及び画像データＩ０００２はサーバ上に蓄積されているものとする。

【００８０】

まず、１４５に示すように、領域１４２、及び領域１４２に対応するデジタル署名を受信した場合は、「改竄なし（検証成功）」と判定可能である。また、１４６に示すように、領域１４２が改竄されたデータ、及び領域１４２に対応するデジタル署名を受信した場合は、「改竄されている（検証失敗）」と判定可能である。

【００８１】

一方、１４７に示すように、領域１４２を要求したにも関わらず、領域１４９、及び領域１４９に対応するデジタル署名を受信した場合、「改竄なし（検証成功）」と判定され

てしまう。何故なら、受信した領域１４９とそのデジタル署名を用いて検証処理を行った場合、領域１４９、及びそのデジタル署名は共に改竄されていないからである。即ち、この場合、「領域１４２ではなく領域１４９が受信されたこと」は検出できない。

【００８２】

更に、１４８に示すように、画像データ１４１中の領域１４２を要求したにも関わらず、領域１４４、及び領域１４４に対応するデジタル署名を受信した場合も、「改竄なし（検証成功）」と判定されてしまう。何故なら、受信した領域１４４、及びそのデジタル署名を用いて検証処理を行った場合、領域１４４、及びそのデジタル署名は共に改竄されていないからである。即ち、「領域１４２ではなく領域１４４が受信されたこと」は検出できない。

【００８３】

以上、従来技術による、検証結果例の具体例を説明した。

【００８４】

次に、本実施形態による検証結果例について、図１２を用いて説明する。図１２において、８１は画像再生クライアント１１（図１）において、欄２２（図２）を用いて指定された画像データ全体（画像識別情報はＩＤ０００１）、また、８２は領域２５（図２）を用いて指定された部分データである。

【００８５】

また、８９は、画像データＩ０００１中において、欄２２で指定された領域８２とは異なる領域を示す部分データである。即ち、８９は８２と同じ画像識別情報ＩＤを有するが、異なる部分データ特定情報Ｚ’を有する。

【００８６】

更に、８４は、画像データＩ０００１とは異なる画像データ（画像識別情報はＩ０００２）中において、欄２２で指定された領域８２と同じ領域（左上の座標、及び右下の座標が等しい）を示す部分データである。即ち、８４は８２と異なる画像識別情報ＩＤ’を有するが、等しい部分データ特定情報Ｚを有する。

【００８７】

表８１０は、画像再生クライアント１１が、画像データ８１（画像識別情報ＩＤはＩ０００１）中の部分データ８１（部分データ特定情報はＺ）を要求した場合に、実際に受信した部分データと、夫々の検証結果を示す。

【００８８】

まず、８５に示すように、領域８２、及び領域８２に対応する検証データを受信した場合は、図８において、画像識別情報ＩＤ、部分データ特定情報Ｚ、及び部分データＭ’は、夫々、検証データＤ（図６）中の画像識別情報ＩＤ、部分データ特定情報Ｚ、及び部分データＭと等しい値となり、結果としてＤとＤ’は等しい値となる。結果として、「受信した部分データＭ’は正しい（検証成功）」と判定可能である。

【００８９】

次に、８６に示すように、領域８２が改竄されたデータ、及び領域８２に対応する検証データを受信した場合は、図８において、画像識別情報ＩＤ、及び部分データ特定情報Ｚは、夫々、検証データＤ（図６）中の画像識別情報ＩＤ、及び部分データ特定情報Ｚと等しい値となる。一方、部分データＭ’は、検証データＤ（図６）中の部分データＭと異なるデータとなり、結果としてＤとＤ’は異なる値となる。結果として、「受信した部分データＭ’は正しくない（検証失敗）」と判定される。

【００９０】

また、８７に示すように、領域８２を要求したにも関わらず、領域８９、及び領域８９に対応する検証データを受信した場合、図８において、画像識別情報ＩＤ、及び部分データＭ’は、検証データＤ中の画像識別情報ＩＤ、及び部分データＭと等しい値となる。一方、部分データ特定情報取得部Ｚは、検証データＤ中の部分データ特定情報Ｚとは異なる値となる。何故なら、この場合、検証データＤ中の部分データ特定情報は、領域８２を特定する情報ではなく、領域８９を特定する情報であるからである。よって、ＤとＤ’は異

なる値となる。結果として、「受信データＭ’は正しくない（検証失敗）」と判定される。

【００９１】

更に、８８に示すように、領域８２を要求したにも関わらず、領域８４、及び領域８４に対応する検証データを受信した場合、図８において、部分データ特定情報Ｚ、及び部分データＭ’は、検証データＤ中の部分データ特定情報Ｚ、及び部分データＭと等しい値となる。一方、画像識別情報ＩＤは、検証データ中の画像識別情報ＩＤとは異なる。何故なら、この場合、検証データＤ中の画像識別情報ＩＤは、画像データＩ０００１ではなく、画像データＩ０００２であるからである。よって、ＤとＤ’は異なる値となる。結果として、「受信データＭ’は正しくない（検証失敗）」と判定される。

【００９２】

以上、本実施形態における検証データ生成処理、及び検証処理による検証結果について説明した。

【００９３】

さて、ここで、実際にネットワーク上でどのような攻撃がなされた場合に、以上説明したような８６乃至８８のような部分データを受信し得るかを説明する。

【００９４】

８６のような部分データは、部分データＭ’が画像配信サーバ１２から画像再生クライアント１１に配信される際に、ネットワーク１４の途中で、悪意のある攻撃者により部分データＭ’が改竄された場合に受信され得る。

【００９５】

一方、８７、及び８８のような部分データは、ある時刻における部分データの配信において、部分データＭ’が悪意のある攻撃者により傍受され、その後の部分データの配信において、前記傍受された部分データＭ’が画像再生クライアント１１に送信された場合（所謂、再送攻撃）に受信され得る。

【００９６】

尚、本実施形態においては、説明のためにネットワーク上に配置されたサーバ、及びクライアントを用いるオンラインの例を説明したが、本発明はこれに限定されることなく、サーバ、及びクライアントを用いないオフラインの場合も同様に適応可能であることは明らかである。オフラインの場合は、図８に示した検証方法を用いて検証可能とするために、部分データＭ’を取得した際に、対応する画像識別情報ＩＤ、部分データ識別情報Ｚ、及び検証データＳも同時に取得し、これらの情報を関連付けて保持しておく。そして、検証が必要となった際に、改めて図８に示した方法を用いて検証処理を実行するようにすれば良い。

【００９７】

＜変形例１＞

本実施形態においては、部分データ特定情報取得部３２（図４）、及び部分データ特定情報取得部６５（図８）において取得される部分データ特定情報Ｚは、画像データ中の空間的な一部の領域を特定する情報であった。しかしながら、本発明はこれに限定されることなく、画像データ中の部分データを特定する情報であれば、解像度、画質、及び成分などを特定する種々の情報を適用可能であることは明らかである。更に、これらのうち少なくとも２つ以上の情報を組み合わせて適用可能であることも明らかである。

【００９８】

ここで、部分データ特定情報Ｚとして、領域に加え、解像度、画質、及び成分を組み合わせて指定する場合の部分データ特定情報Ｚの取得方法について、図１３を用いて説明する。

【００９９】

図１３は、前述した部分データ特定情報取得部３２（図４）、及び部分データ特定情報取得部６５（図８）の代わりに適応される部分データ特定情報取得部を説明する図である。

【０１００】
部分データ特定情報取得部９１は、領域特定情報取得部９２、解像度特定情報取得部９３、画質特定情報取得部９４、成分特定情報取得部９５、及び結合処理部９６から構成される。
【０１０１】
まず、領域特定情報取得部９２では、前述した部分データ特定情報取得部３２（図４）、及び部分データ特定情報取得部６５（図８）と同様に、画像中の空間的な領域を指定する情報が取得される。解像度特定情報取得部９３では、画像の解像度を指定する情報が取得される。例えば、ＪＰＥＧ　２０００においては所定の解像度レベル識別子を取得するようにする。また、画質特定情報取得部９４では、画像の画質を指定する情報が取得される。例えば、ＪＰＥＧ　２０００においては所定のレイヤを取得するようにする。更に、成分特定情報取得部９５では、画像中の成分を指定する情報が取得される。例えば、ＪＰＥＧ　２０００においては、輝度成分や所定の色成分を取得するようにする。
【０１０２】
次に、結合処理部９６について説明する。結合処理部９６では、前段で指定された領域特定情報Ｐ、解像度特定情報Ｒ、画質特定情報Ｌ、及び成分特定情報Ｃを結合し、結合されたデータを部分データ特定情報Ｚとして出力する。
【０１０３】
部分データ特定情報取得部９１から取得された部分データ特定情報Ｚは、結合処理部３４（図４）、或いは結合データ処理部６７（図８）に入力され、更に、画像識別情報ＩＤ、及び部分データＭ（或いは、Ｍ’）と結合され、結合データＤ（或いは、Ｄ’）となる。結果として、結合データＤ（或いは、Ｄ’）は、図１４に示すようなデータとなる。
【０１０４】
図１４に示すように、複数の部分データを特定する情報（Ｐ、Ｒ、Ｌ、及びＣ）が指定された場合、それら全てを連結し、連結したデータを部分データ特定情報Ｚとするようにすれば良い。
【０１０５】
以上、本変形例は少なくとも２つ以上の情報を組み合わせて部分データ特定情報を表現可能であることを説明した。尚、少なくとも２つ以上の情報を組み合わせて部分データ特定情報を表現可能な例は、この例に限らないのは言うまでもない。
【０１０６】
＜変形例２＞
本実施形態においては、画像データ、及びその部分データ（領域、解像度、画質、成分、及びこれらの組み合わせ）を処理の対象として説明した。しかしながら、本発明はこれに限定されることなく、複数の部分データから構成されるような種々のデータに対して適応可能であることは明らかである。
【０１０７】
ここで、例として、ＸＭＬやＰＤＦなどのように階層構造を有するような文書データに対して適応する場合の例を、図１５を用いて説明する。図１５に示すように、本実施形態における文書データは、一つの「会社名」要素と複数の「社員情報」要素から構成される「会社情報」要素から構成される。更に、夫々の「社員情報」要素は、夫々一つの「社員番号」要素、「名前」要素、「性別」要素、及び「担当」要素から構成される。
【０１０８】
図１５に示すような文書情報の場合、画像データ識別情報の代わりに、夫々の文書を識別する文書名（「会社名」要素の要素内容）を、文書データ識別情報ＩＤとして利用する。また、部分データ特定情報Ｚとして「社員番号」要素の要素内容、及び部分データＭとして「社員情報」要素の要素内容を用いるようにする。
【０１０９】
本実施形態を用いることによって、サーバ上に保持されている文書データから、「社員番号」要素の要素内容を用いて、所望の「社員情報」要素の要素内容を取得し、取得した

「社員情報」要素の要素内容が正しい情報か否かを検証可能となる。

【０１１０】

また、他の例として、データベース情報に対して適応する場合の例を、図１６を用いて説明する。図１６に示すように、本実施形態におけるデータベース情報は、社員番号、名前、性別、及び担当から構成される社員情報（レコード）の集合である。

【０１１１】

図１６に示すようなデータベース情報の場合、画像データ識別情報の代わりに、夫々のデータベース情報を識別するデータベース名を、データベース識別情報ＩＤとして用いる。また、部分データ特定情報Ｚとして各社員番号、及び部分データＭとして各社員情報を用いるようにする。

【０１１２】

本実施形態を用いることによって、会社Ａ（即ち、会社識別情報ＩＤ）のデータベース情報から、社員番号（即ち、部分データ特定情報Ｚ）を用いて所望の社員情報（即ち、部分データＭ）を取得した場合、取得した社員情報が正しい社員情報か否かを検証可能となる。

【０１１３】

尚、本実施形態においては、部分データＭの内部に部分データ特定情報Ｚが含まれるような例を示したが、本発明はこれに限定されることなく、部分データＭの内部に部分データ特定情報Ｚを含まないようにすることも可能である。この場合、所望の部分データの中から、部分データ特定情報Ｚを除いたデータを部分データＭとするようにすれば良い。

【０１１４】

また、同じデータベース情報を用いた場合であっても、データベース識別情報ＩＤや、部分データ特定情報Ｚを適宜設定可能な例を説明する。

【０１１５】

図１６の会社ＹＹＹのデータベースでは、データベース情報識別情報ＩＤは、ＵＲＬを用い、部分データ特定情報Ｚとして、「社員番号が０００００２、かつ、氏名」とし、その部分データＭを「ＤＤＤ」とすることもできる。このように、生成側が検証したい対象に応じて、検証データを生成することが可能である。さらに、データベース識別情報ＩＤや部分データ特定情報Ｚをどのように設定するかに関するルールを生成側と検証側とで秘密に共有することで、さらに改ざんされにくくなるという効果を有する。

【０１１６】

＜変形例３＞

以上本発明にかかる実施形態を説明したが、先に説明したように、画像データを暗号化、暗号復号する装置は、通常のパーソナルコンピュータ等の汎用情報処理装置であって、それ上で動作するコンピュータプログラムで実現できるものであるから、本発明はコンピュータプログラムをその範疇とすることは明らかである。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憶されており、それをコンピュータの対応するドライブにセットしてシステムにコピーやインストール処理することで実行可能となるわけであるから、本発明は当然にそのようなコンピュータ可読記憶媒体をもその範疇とすることも明らかである。

【図面の簡単な説明】

【０１１７】

【図１】実施形態におけるシステム全体構成を示す図である。

【図２】実施形態における画像再生クライアントにおいて適用可能なＧＵＩ画面の例を示す図である。

【図３】実施形態におけるホストコンピュータを示す図である。

【図４】実施形態における検証データ生成処理部の構成を示すブロック図である。

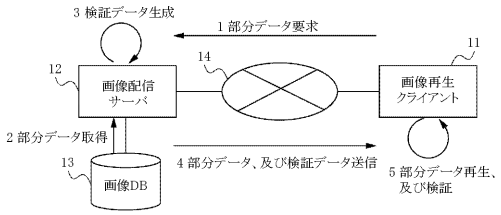
【図５】実施形態における部分データ特定情報を説明する図である。

【図６】実施形態における結合データを説明する図である。

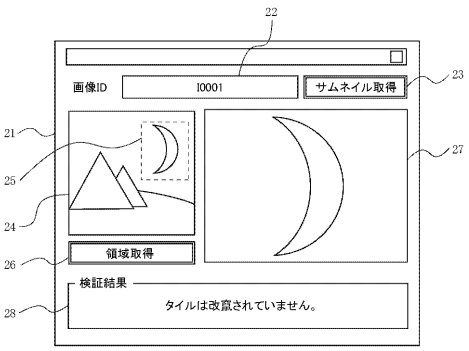
【図７】実施形態における検証データ生成処理のフローチャートである。

【図８】実施形態における検証処理部の構成を説明するブロック図である。
【図９】実施形態における検証処理のフローチャートである。
【図１０】従来技術におけるデジタル署名生成処理を説明する図である。
【図１１】従来技術における検証結果を説明する図である。
【図１２】実施形態における検証結果を説明する図である。
【図１３】実施形態における部分データ特定情報取得部の構成を示すブロック図である。
【図１４】実施形態における結合データを説明する図である。
【図１５】実施形態における文書データを示す図である。
【図１６】実施形態におけるデータベース情報を説明する図である。
【図１７】従来技術における署名処理のフローチャートである。

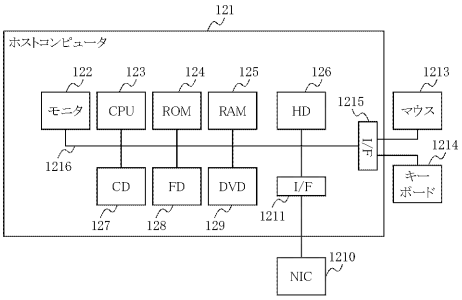
【図１】



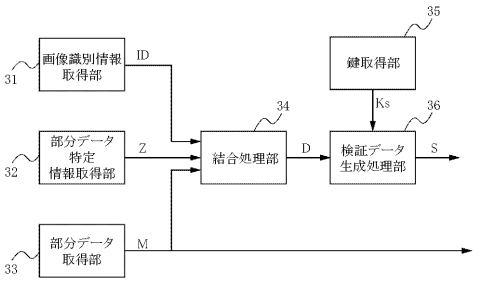
【図２】



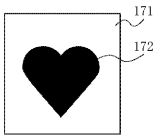
【図３】



【図４】



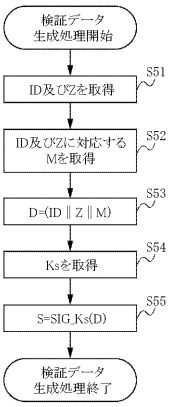
【図５】



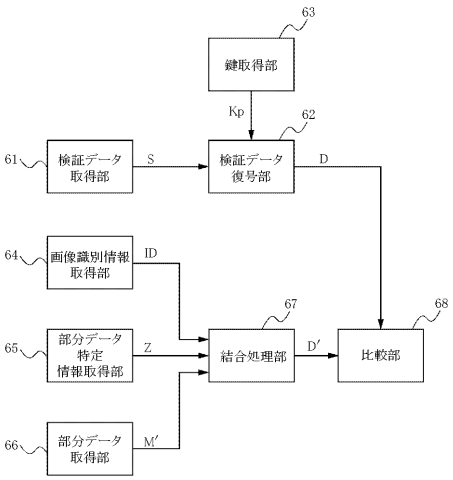
【図６】

ID	Z	M

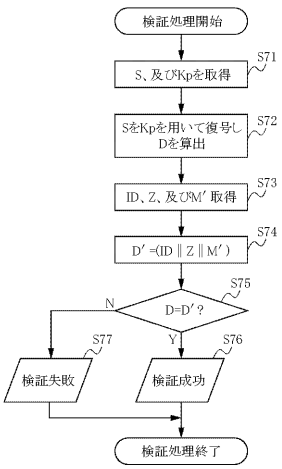
【図７】


検証データ
生成処理開始
ID及びZを取得
S51
ID及びZに対応する
Mを取得
S52
D=(ID ‖ Z ‖ M)
S53
Ksを取得
S54
S=SIG,Ks(D)
S55
検証データ
生成処理終了

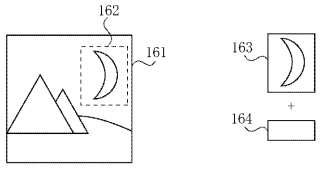
【図８】


63
鍵取得部
Kp
62
61
検証データ
取得部
S
検証データ
復号部
D
64
画像識別情報
取得部
ID
67
68
65
部分データ
特定
情報取得部
Z
結合処理部
D′
比較部
66
部分データ
取得部
M′

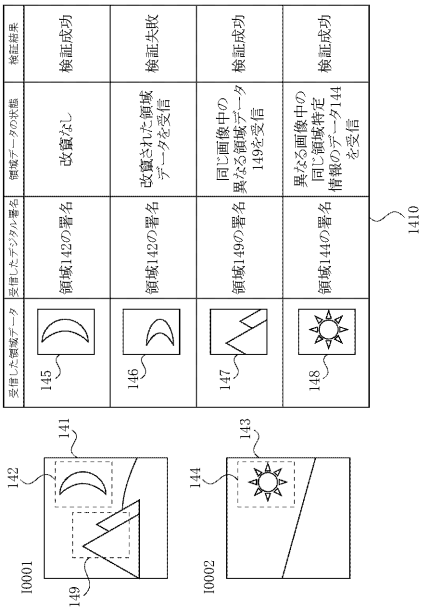
【図９】


検証処理開始
S、及びKpを取得
S71
SをKpを用いて復号し
Dを算出
S72
ID、Z、及びM′取得
S73
D′=(ID ‖ Z ‖ M′)
S74
S75
D=D′?
N
Y
S77
S76
検証失敗
検証成功
検証処理終了

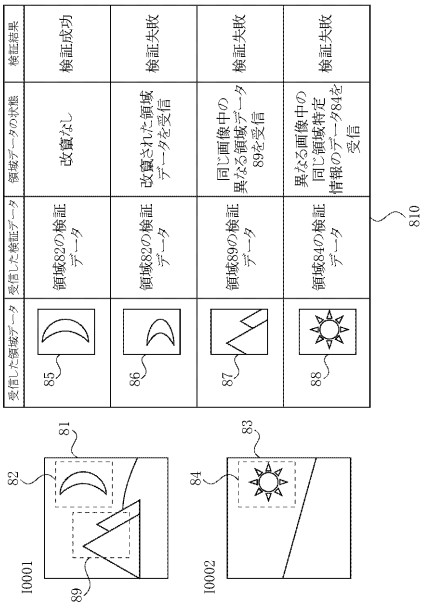
【図１０】


162
161
163
+
164

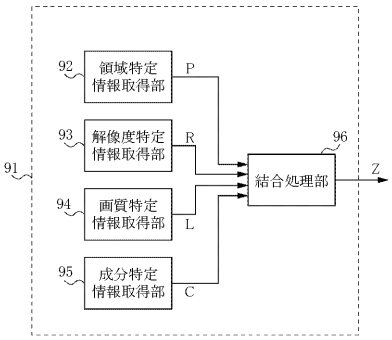
【図１１】



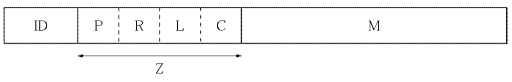
【図１２】



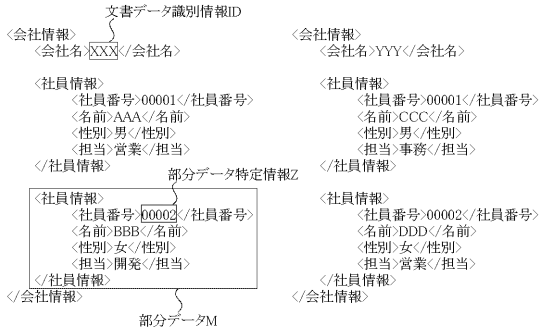
【図１３】



【図１４】



【図１５】

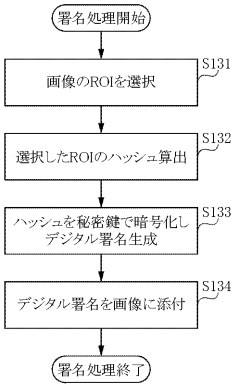


【図１６】

レコード番号	社員番号	氏名	性別	担当
1	000001	AAA	男	営業
2	000002	BBB	女	開発
…	…	…	…	…

レコード番号	社員番号	氏名	性別	担当
1	000001	CCC	男	事務
2	000002	DDD	女	営業
…	…	…	…	…

【図１７】



フロントページの続き

(56)参考文献 特開２０００－１９４８３２（ＪＰ，Ａ）
特開２０００－３４１６３２（ＪＰ，Ａ）
特開２００３－１５２９７９（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｈ０４Ｎ　１／３８７
Ｇ０６Ｔ　１／００
Ｈ０４Ｎ　１／４０