(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2010-50906
(P2010-50906A)
(43)公開日　平成22年3月4日(2010.3.4)

(51)Int.Cl.		F I			テーマコード（参考）
H04N 1/387	(2006.01)	H04N	1/387		2C061
B41J 29/00	(2006.01)	B41J	29/00	Z	5B017
G06F 3/12	(2006.01)	G06F	3/12	K	5B021
G09C 1/00	(2006.01)	G09C	1/00	640D	5C076
B41J 29/38	(2006.01)	B41J	29/38	Z	5J104

審査請求 未請求　請求項の数 10　ＯＬ　（全 31 頁）　最終頁に続く

(21)出願番号　特願2008-215669 (P2008-215669)
(22)出願日　平成20年8月25日 (2008.8.25)

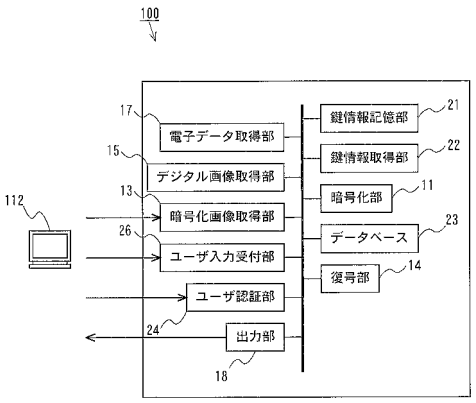
（特許庁注：以下のものは登録商標）
１．ＱＲコード

(71)出願人　000136136
株式会社ＰＦＵ
石川県かほく市宇野気ヌ９８番地の２
(74)代理人　100090516
弁理士　松倉　秀実
(74)代理人　100113608
弁理士　平川　明
(74)代理人　100105407
弁理士　高田　大輔
(74)代理人　100089244
弁理士　遠山　勉
(74)代理人　100123098
弁理士　今堀　克彦

最終頁に続く

(54)【発明の名称】改竄検出用情報出力システム、方法およびプログラム

(57)【要約】
【課題】紙媒体に記録された情報の改竄を、改竄箇所および改竄内容を把握可能に検出可能なシステムを提供することを課題とする。
【解決手段】改竄検出の対象情報を画像として含むデジタル画像を取得するデジタル画像取得部１５と、暗号鍵に基づいてデジタル画像を変換することで、暗号化画像を生成する暗号化部１１と、暗号化部１１によって生成された暗号化画像を、対象情報のイメージが記録されるかまたは記録された紙媒体に記録されるように出力する出力部１８と、を備える、改竄検出用情報出力システム１００とした。
【選択図】図２



【特許請求の範囲】
【請求項１】
改竄検出の対象情報を画像として含むデジタル画像を取得するデジタル画像取得手段と、
暗号鍵に基づいて前記デジタル画像を変換することで、暗号化画像を生成する暗号化手段と、
前記暗号化手段によって生成された前記暗号化画像を、前記対象情報のイメージが記録されるかまたは記録された紙媒体に記録されるように出力する暗号化画像出力手段と、
を備える、改竄検出用情報出力システム。
【請求項２】
前記暗号化画像出力手段による前記暗号化画像の出力と共に、改竄検出の対象となる前記対象情報のイメージを、前記紙媒体に記録されるように出力する対象情報出力手段を更に備える、
請求項１に記載の改竄検出用情報出力システム。
【請求項３】
前記対象情報出力手段は、前記対象情報のイメージを、前記紙媒体の一方の面に記録されるように出力し、
前記暗号化画像出力手段は、前記暗号化画像を、前記紙媒体の他方の面に記録されるように出力する、
請求項２に記載の改竄検出用情報出力システム。
【請求項４】
前記対象情報を含む電子データの入力を受け付ける電子データ取得手段を更に備え、
前記デジタル画像取得手段は、前記電子データに基づいて、前記デジタル画像を生成することで、前記デジタル画像を取得し、
前記対象情報出力手段は、前記紙媒体に記録される前記対象情報のイメージとして、前記デジタル画像を出力する、
請求項２または３に記載の改竄検出用情報出力システム。
【請求項５】
前記暗号化手段は、前記デジタル画像の少なくとも一部の領域の画像を、暗号鍵に基づいて処理画像に変換し、更に前記処理画像の画素値を規則的に変換することで、復号の際に前記部分領域の位置の特定に用いられる規則性を有する変換画像を生成し、前記変換画像を含む暗号化画像を生成する、
請求項１から４の何れか一項に記載の改竄検出用情報出力システム。
【請求項６】
改竄検出の対象情報のイメージと、該対象情報が含まれるデジタル画像が暗号化されることで生成された暗号化画像と、が記録された紙媒体から取得された該暗号化画像を取得する暗号化画像取得手段と、
前記暗号化画像を、該暗号化画像の生成に用いられた暗号鍵に対応する復号鍵に基づいて復号することで、前記対象情報が含まれる復号デジタル画像を生成する復号手段と、
前記復号手段によって生成された復号デジタル画像を、前記紙媒体に記録された前記対象情報のイメージと比較可能に出力するデジタル画像出力手段と、
を備える、改竄検出用情報出力システム。
【請求項７】
コンピュータシステムによって、
改竄検出の対象情報を画像として含むデジタル画像を取得するデジタル画像取得ステップと、
暗号鍵に基づいて前記デジタル画像を変換することで、暗号化画像を生成する暗号化ステップと、
前記暗号化ステップで生成された前記暗号化画像を、前記対象情報のイメージが記録されるかまたは記録された紙媒体に記録されるように出力する暗号化画像出力ステップと、

が実行される、改竄検出用情報出力方法。
【請求項８】
コンピュータシステムによって、
改竄検出の対象情報のイメージと、該対象情報が含まれるデジタル画像が暗号化されることで生成された暗号化画像と、が記録された紙媒体から取得された該暗号化画像を取得する暗号化画像取得ステップと、
前記暗号化画像を、該暗号化画像の生成に用いられた暗号鍵に対応する復号鍵に基づいて復号することで、前記対象情報が含まれる復号デジタル画像を生成する復号ステップと、
前記復号ステップで生成された復号デジタル画像を、前記紙媒体に記録された前記対象情報のイメージと比較可能に出力するデジタル画像出力ステップと、
が実行される、改竄検出用情報出力方法。
【請求項９】
コンピュータを、
改竄検出の対象情報を画像として含むデジタル画像を取得するデジタル画像取得手段と、
暗号鍵に基づいて前記デジタル画像を変換することで、暗号化画像を生成する暗号化手段と、
前記暗号化手段によって生成された前記暗号化画像を、前記対象情報のイメージが記録されるかまたは記録された紙媒体に記録されるように出力する暗号化画像出力手段と、
として機能させる、改竄検出用情報出力プログラム。
【請求項１０】
コンピュータを、
改竄検出の対象情報のイメージと、該対象情報が含まれるデジタル画像が暗号化されることで生成された暗号化画像と、が記録された紙媒体から取得された該暗号化画像を取得する暗号化画像取得手段と、
前記暗号化画像を、該暗号化画像の生成に用いられた暗号鍵に対応する復号鍵に基づいて復号することで、前記対象情報が含まれる復号デジタル画像を生成する復号手段と、
前記復号手段によって生成された復号デジタル画像を、前記紙媒体に記録された前記対象情報のイメージと比較可能に出力するデジタル画像出力手段と、
として機能させる、改竄検出用情報出力プログラム。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、文書の改竄を防止する技術に関する。
【背景技術】
【０００２】
紙文書の改竄を検出するための技術として、文書から黒画素密度等を含む特徴データを算出し、これをバーコード等の形式で文書の余白に付加することで、文書の改竄が行われた場合に、これを検出可能とする技術がある（特許文献１を参照）。また、規則性を持ったドットパターンを重畳印刷することで、改竄によるドットパターンの規則性の乱れを検出可能とする技術があり、（特許文献２を参照）その他、文書の改竄を防止するいくつかの技術が提案されている（特許文献３から８を参照）。
【特許文献１】特開２００１－３０９１５７号公報
【特許文献２】特開２００５－１２５３０号公報
【特許文献３】特開２００２－１０９１１３号公報
【特許文献４】特開２００３－２６４６８５号公報
【特許文献５】特開２００３－２０９６７６号公報
【特許文献６】特開２００６－１４１８９号公報
【特許文献７】特開２００７－２８３２４号公報

【特許文献８】特開２００７－２８１５３９号公報
【発明の開示】
【発明が解決しようとする課題】
【０００３】
上述のように、従来、紙媒体に記録された情報の改竄を検出するための技術としては、印刷された情報の特徴データを算出し、これをコンピュータ読取可能な形式（バーコード等）で同一の紙媒体に印刷することで、改竄の有無を検出可能とするものがあった。
【０００４】
しかし、このような改竄検出技術は、改竄検出のために文書に付加された特徴データを、改竄チェック時点における文書に基づいて算出された特徴データと比較して改竄の有無を検出するものであったため、改竄が行われたことを検出できたとしても、改竄前の正しい情報の内容を知ることは出来ず、改竄が行われた位置を検出することも困難であった。更に、改竄前の情報が残らないため、仮に改竄が検出された場合でも、この検出が誤検出でないことを確認することが困難であった。特に、このような技術では、情報が記録される対象が紙媒体であるため、改竄検出用の特徴データの算出後に、改竄検出の対象となる部分に汚れや印刷の滲みが生じる可能性があり、改竄が行われていない場合であっても、改竄が誤検出される虞があった。
【０００５】
また、その他の従来技術として、元の文書に改竄検出用の画像を重畳して印刷するものがあるが、このような方法では、元の文書との同一性が損なわれる上、改竄の検出を行う際に元の文書と改竄検出用に重畳された画像との分離に失敗すると、改竄を検出できなかったり、誤検出が発生したりする可能性がある。
【０００６】
本発明は、上記した問題に鑑み、紙媒体に記録された情報の改竄を、改竄箇所および改竄内容を把握可能に検出可能なシステムを提供することを課題とする。
【課題を解決するための手段】
【０００７】
本発明は、上記した課題を解決するために、以下の手段を採用した。即ち、本発明は、改竄検出の対象情報を画像として含むデジタル画像を取得するデジタル画像取得手段と、暗号鍵に基づいて前記デジタル画像を変換することで、暗号化画像を生成する暗号化手段と、前記暗号化手段によって生成された前記暗号化画像を、前記対象情報のイメージが記録されるかまたは記録された紙媒体に記録されるように出力する暗号化画像出力手段と、を備える、改竄検出用情報出力システムである。
【０００８】
ここで、対象情報とは、紙媒体に記録される（一般的には、印刷等の手段によって記録される）情報のうち、改竄が行われたか否かの検出の対象とする情報である。このような情報としては、例えば、何らかの証明を行う者から取得されて、その後、他の者に提出される文書（例えば、住民票や印鑑証明等の証明書、および処方箋等）に含まれる情報がある。但し、上記したような情報でなくとも、紙媒体に記録される情報のうち、ユーザが改竄を検出したい情報であれば、改竄検出の対象情報となり得る。
【０００９】
また、デジタル画像とは、所謂ビットマップデータ等、画素の集合としての画像である。本発明に係る改竄検出用情報出力ステムは、例えば、デジタル画像をブロック毎に分割して並べ替える処理や画素情報の調整等を行う等の方法で、デジタル画像中の少なくとも一部の領域を変換し、暗号化された変換領域を含む暗号化画像を生成する。
【００１０】
なお、暗号化手段によって生成される暗号化画像も、データの形式はデジタル画像と同様、画素の集合である。暗号化（変換）には、暗号鍵が用いられる。暗号鍵を用いて変換を行うことで、この暗号鍵に対応する復号鍵が用いられた場合に、正しい復号結果が得られるようにすることが出来る。暗号化の方式としては、主に共通鍵暗号、および非対称鍵

暗号（公開鍵暗号）の方式があり、共通鍵暗号方式を用いる場合、暗号鍵と復号鍵は同一である。

【００１１】

そして、本発明では、生成された暗号化画像が紙媒体に記録される。この紙媒体は、改竄検出の対象となる対象情報のイメージが記録される紙媒体であるため、この紙媒体を入手したユーザは、正しい鍵情報（復号鍵）を用いて暗号化画像を復号し、復号結果と対象情報（証明書等において本来証明すべき内容が記載されている部分）とを比較することで、改竄の有無、および改竄があった場合にはその内容を知ることが出来る。改竄の検出は、ユーザの目視確認による検出であってもよいし、復号された画像とスキャナ等を用いて取り込まれた対象情報の画像とを比較することによる機械検出であってもよい。

【００１２】

また、対象情報のイメージと暗号化画像とは、証明書等の完成時点で同一の紙媒体に記録されていればよい。即ち、対象情報のイメージと暗号化画像とは、何れが先に紙媒体に記録されてもよいし、同時に記録されてもよい。

【００１３】

また、本発明に係る改竄検出用情報出力システムは、前記暗号化画像出力手段による前記暗号化画像の出力と共に、改竄検出の対象となる前記対象情報のイメージを、前記紙媒体に記録されるように出力する対象情報出力手段を更に備えてもよい。このようにすることで、ユーザ端末やプリンタ等の、紙媒体に記録を行うための手段は、本発明に係る改竄検出用情報出力システムから、改竄検出の対象となる対象情報と改竄検出のための暗号化画像とを同時に取得することができる。

【００１４】

また、前記対象情報出力手段は、前記対象情報のイメージを、前記紙媒体の一方の面に記録されるように出力し、前記暗号化画像出力手段は、前記暗号化画像を、前記紙媒体の他方の面に記録されるように出力してもよい。このようにすることで、従来発行されていた証明のための文書等のレイアウトや記載情報を変更すること無く、証明書の裏面に改竄検出のための暗号化画像を追加して印刷することで、文書に改竄検出のための機能を付加することが出来る。ただし、暗号化画像の記録位置は、対象情報が記録される面の反対側の面に限られない。例えば、暗号化画像の記録位置は、対象情報と同一面の余白（対象情報が記録されていない部分）であってもよい。

【００１５】

また、改竄検出の対象情報のイメージは、暗号化のために生成されたデジタル画像とは異なる処理で生成されたイメージであってもよい（具体的には、情報のレイアウトやデータ形式等が異なってもよい）が、これらは同一の画像情報であってもよい。即ち、本発明に係る改竄検出用情報出力システムは、前記対象情報を含む電子データの入力を受け付ける電子データ取得手段を更に備え、前記デジタル画像取得手段は、前記電子データに基づいて、前記デジタル画像を生成することで、前記デジタル画像を取得し、前記対象情報出力手段は、前記紙媒体に記録される前記対象情報のイメージとして、前記デジタル画像を出力してもよい。

【００１６】

ここで、電子データとは、文書、図表、イラスト等の何らかの情報を含むデータをいう。これらの電子データは、例えば文書作成アプリケーション、表計算アプリケーション、イラスト作成アプリケーション等によって電子ファイルとして作成される。デジタル画像取得手段は、電子データを表示または印刷する際のイメージを、画素の集合としてのデジタル画像（例えば、ビットマップデータ）として生成する。

【００１７】

これによって、暗号化を行いたい情報が含まれる電子データをデジタル画像化する手間をユーザにかけることなく、改竄検出の対象情報が含まれた電子データに基づく暗号化画像を簡易に生成し、改竄検出機能付きの文書を作成することが出来る。

【００１８】

なお、本発明に係る改竄検出用情報出力システムは、暗号鍵（および復号鍵）を、文書を識別可能な識別情報と関連付けて記憶してもよい。そして、識別情報は、暗号化画像が記録される紙媒体に記録される。このようにすることで、識別情報に基づいて適切な復号鍵を取得して暗号化画像を復号し、文書の改竄を確認することが出来る。また、本システムにおいて管理される鍵情報（暗号鍵および復号鍵）は、システム管理者以外は知ることが出来ないように管理されることが好ましい。復号の際、識別情報は、例えば、暗号化画像に含まれる文字、記号、模様および色のうち少なくとも何れかを画像から検出することで取得されてもよい。より具体的には、画像中のバーコードや文字列、記号等から識別情報を取得する方法がある。

【００１９】

また、前記暗号化手段は、前記デジタル画像の少なくとも一部の領域の画像を、暗号鍵に基づいて処理画像に変換し、更に前記処理画像の画素値を規則的に変換することで、復号の際に前記部分領域の位置の特定に用いられる規則性を有する変換画像を生成し、前記変換画像を含む暗号化画像を生成してもよい。このようにすることで、改竄検出のための復号の際に、暗号化画像のうち実際に暗号鍵を用いて変換された領域を、ユーザによる指定等に依らずに特定することが出来る。

【００２０】

また、本発明は、上記システムを用いて作成された紙媒体において改竄が行われたか否かを検出するための手段を備える改竄検出用情報出力システムとしても把握できる。即ち、本発明は、改竄検出の対象情報のイメージと、該対象情報が含まれるデジタル画像が暗号化されることで生成された暗号化画像と、が記録された紙媒体から取得された該暗号化画像を取得する暗号化画像取得手段と、前記暗号化画像を、該暗号化画像の生成に用いられた暗号鍵に対応する復号鍵に基づいて復号することで、前記対象情報が含まれる復号デジタル画像を生成する復号手段と、前記復号手段によって生成された復号デジタル画像を、前記紙媒体に記録された前記対象情報のイメージと比較可能に出力するデジタル画像出力手段と、を備える、改竄検出用情報出力システムである。

【００２１】

本発明に係る改竄検出用情報出力システムによれば、改竄検出の対象情報と同一の紙媒体に記録された暗号化画像を復号して出力することで、復号されたデジタル画像を対象情報と比較して改竄の有無、および改竄があった場合にはその位置や内容を検出することが可能である。

【００２２】

更に、本発明は、コンピュータが実行する方法、又はコンピュータを上記各手段として機能させるためのプログラムとしても把握することが可能である。また、本発明は、そのようなプログラムをコンピュータその他の装置、機械等が読み取り可能な記録媒体に記録したものでもよい。ここで、コンピュータ等が読み取り可能な記録媒体とは、データやプログラム等の情報を電気的、磁気的、光学的、機械的、または化学的作用によって蓄積し、コンピュータ等から読み取ることができる記録媒体をいう。

【発明の効果】

【００２３】

本発明によって、紙媒体に記録された情報の改竄を、改竄箇所および改竄内容を把握可能に検出可能なシステムを提供することが可能となる。

【発明を実施するための最良の形態】

【００２４】

本発明の実施の形態について、図面に基づいて説明する。

【００２５】

図１は、実施形態に係る改竄検出用情報出力システムのハードウェア構成の概略を示す図である。ここで、改竄検出用情報出力システム１００は、ＣＰＵ（Ｃｅｎｔｒａｌ Ｐｒｏｃｅｓｓｉｎｇ Ｕｎｉｔ）１０１、ＲＡＭ（Ｒａｎｄｏｍ Ａｃｃｅｓｓ Ｍｅｍｏｒｙ）１０２等の主記憶装置、ＨＤＤ（Ｈａｒｄ Ｄｉｓｋ Ｄｒｉｖｅ）１０３等の

補助記憶装置、ＲＯＭ（Ｒｅａｄ　Ｏｎｌｙ　Ｍｅｍｏｒｙ）１０４、およびＮＩＣ（Ｎｅｔｗｏｒｋ　Ｉｎｔｅｒｆａｃｅ　Ｃａｒｄ）１０５を有するコンピュータであり、ＮＩＣ１０５には、インターネット等の広域ネットワーク１１３を介して、ディスプレイ等の表示装置やマウス／キーボード等の入力装置を有するユーザ端末１１２ａ、１１２ｂが接続されている。ここで、ユーザ端末１１２ａ、１１２ｂは、改竄検出用情報出力システム１００とハードウェア的には略同様の構成を備えるコンピュータである。

【００２６】

なお、本実施形態では、ユーザ端末１１２ａ、１１２ｂは夫々異なるＬＡＮ（Ｌｏｃａｌ　Ａｒｅａ　Ｎｅｔｗｏｒｋ）１１４ａ、１１４ｂに属し、夫々のＬＡＮ１１４ａ、１１４ｂには、ユーザ端末１１２ａ、１１２ｂから利用可能なスキャナ１０６ａ、１０６ｂおよびプリンタ１０７ａ、１０７ｂが接続されている。本実施形態に係る改竄検出用情報出力システム１００は、ＬＡＮ１１４ａに属するユーザ端末１１２ａを用いるユーザに対して証明書（例えば、住民票）を発行し（証明書の発行を受けたユーザは、ユーザ端末１１２ａからプリンタ１０７ａを用いて証明書を印刷する）、また、このようにして発行された証明書が提出された提出先（例えば、免許センタ）において、ＬＡＮ１１４ｂに属するユーザ端末１１２ｂを用いる提出先のユーザＢに対して、証明書の改竄チェックを行うための改竄チェック用画像を提供するシステムである。

【００２７】

図２は、本実施形態に係る改竄検出用情報出力システム１００の機能構成の概略を示す図である。図１に示されたコンピュータは、ＨＤＤ１０３から読み出され、ＲＡＭ１０２に展開された改竄検出用情報出力プログラムをＣＰＵ１０１が実行することで、ユーザ認証部２４、ユーザ端末１１２ａ、１１２ｂからの証明書発行要求や改竄チェック用画像出力要求等を受け付けるユーザ入力受付部２６、証明書情報データベース２３、電子データ取得部１７、デジタル画像取得部１５、出力部１８（本発明の暗号化画像出力手段、対象情報出力手段およびデジタル画像出力手段に相当する）、鍵情報記憶部２１、鍵情報取得部２２、および暗号化部１１を備える改竄検出用情報出力システム１００として機能する。

【００２８】

また、図１に示されたコンピュータシステムは、暗号化された暗号化画像を復号するために、ＨＤＤ１０３から読み出され、ＲＡＭ１０２に展開された改竄検出用情報出力プログラムをＣＰＵ１０１が実行することで、更に、暗号化画像取得部１３、および復号部１４を備える改竄検出用情報出力システム１００として機能する。なお、ユーザ認証部２４、出力部１８、鍵情報記憶部２１、および鍵情報取得部２２等の各機能部は、暗号化画像の復号処理においても用いられる。

【００２９】

なお、本実施形態では、本発明に係るシステムを、証明書の印刷用データの出力および証明書の改竄チェック用データの出力の双方の機能を備えた改竄検出用情報出力システム１００として説明しているが、本発明に係る改竄検出用情報出力システム１００は、暗号化の機能を備えた証明書印刷用データの出力システム、または復号の機能を備えた改竄チェック用データの出力システムとして実施されてもよい。

【００３０】

電子データ取得部１７は、ユーザ端末１１２ａから入力された証明書発行要求に従って、証明書の発行に必要な電子データを、証明書情報データベース２３から索出して取得する。ここで、証明書情報データベース２３は、証明書に記載される内容を含む証明書作成用の電子データを、ＨＤＤ１０３に蓄積するデータベースである。例えば、発行される証明書が住民票である場合、証明書情報データベース２３には、住民票に記載される者の氏名や住所等が蓄積されている。なお、本実施形態では、証明書情報データベース２３は改竄検出用情報出力システム１００に接続されたＨＤＤ１１３を用いて構築されるが、証明書情報データベース２３は、改竄検出用情報出力システム１００にネットワークを介して接続された、異なるコンピュータを用いて構築されてもよい。

【００３１】
デジタル画像取得部１５は、電子データ取得部１７によって証明書情報データベース２３から取得された証明書用の電子データに基づいてデジタル画像を生成することで、暗号化の対象となるデジタル画像を取得する。ここで、電子データとは、文書作成アプリケーションや表計算アプリケーション等のアプリケーションによって扱われる電子データ（電子ドキュメント）である。デジタル画像取得部１５は、電子データを紙媒体等へ印刷した場合またはディスプレイ等へ表示した場合のイメージを、所謂ビットマップ形式のデジタル画像へ変換する。通常、例えば文書に係る電子データであれば文字コードや書式情報からなるが、この電子データを表示または印刷した場合のイメージをビットマップ形式の画像として生成することで、暗号化部１１による画像の暗号化を施すことが可能となる。

【００３２】
鍵情報記憶部２１は、鍵情報（暗号鍵および復号鍵）を、発行される証明書を識別するための文書ＩＤと関連付けて鍵情報テーブルに記憶する。なお、本実施形態に係る暗号化方式は、共通鍵暗号方式であるため、暗号鍵と復号鍵は同一である。なお、鍵情報テーブルに蓄積された情報のうち、少なくとも鍵情報は暗号化され、システム管理者にのみ平文での閲覧が許可される。即ち、本実施形態によれば、ユーザは鍵情報を手に入れることが出来ないため、ユーザによって改竄または偽造された証明書に、ユーザが自身で勝手に改竄検出用の暗号化画像を付加することを防止出来る。

【００３３】
鍵情報取得部２２は、暗号化処理時には、鍵情報を新たに生成することで、デジタル画像の暗号化に用いる暗号鍵を取得する。ここで生成された鍵情報は、文書ＩＤと関連付けられて鍵情報テーブルに蓄積される。また、鍵情報取得部２２は、復号処理時には、スキャナ１０６ｂで読み込まれ、暗号化画像が取得された文書の文書ＩＤを検索キーとして鍵情報テーブルを検索することで、文書ＩＤに係る証明書に関連付けられた復号鍵を取得する。

【００３４】
暗号化部１１は、デジタル画像中の少なくとも一部の領域（暗号化領域）を、鍵情報取得部２２によって取得された暗号鍵を用いて変換することで、この暗号鍵に対応する復号鍵を用いて復号可能な変換領域を含む暗号化画像を生成する。また、暗号化部１１は、デジタル画像中に暗号化の対象となる暗号化領域が複数指定された場合、領域毎に異なる暗号鍵を用いて暗号化を行ってもよい。なお、暗号化部１１による暗号化処理の詳細については後述する。

【００３５】
本実施形態における改竄検出用情報出力システム１００は、デジタル画像の少なくとも一部の領域を暗号鍵に基づいて変換することで暗号化画像を生成し、また、暗号化画像中の変換された領域を復号鍵に基づいて復号する。ここで、暗号化画像中の、暗号鍵を用いて変換された領域を、変換領域と称する。なお、単一の画像中に複数の変換領域を指定することが可能であり、夫々の変換領域は、異なる鍵情報を用いて変換することが可能である。

【００３６】
変換領域は、証明書の発行（暗号化処理）の都度ユーザによって指定されてもよいが、予め定められた領域が、変換領域として設定されていてもよい。例えば、証明書中の、特に改竄を防止すべき部分（例えば、印鑑証明書中に記載された印影等）についてのみ暗号鍵を用いて変換を行うこととしてもよい。このようにして変換領域を予め指定しておくことで、フォーマットの定まった証明書発行時におけるユーザの手間を軽減することが出来る。

【００３７】
なお、暗号化部１１によって変換された変換領域を特定するための領域指定情報が、文書ＩＤと共に、生成された前記暗号化画像に付加されてもよい。ここで、領域指定情報とは、デジタル画像中の変換領域を指定するための位置情報等を含む情報である。変換領域

を指定するために用いられる情報としては、デジタル画像中の位置を示す位置情報や、サイズ情報、ベクトル情報等がある。変換領域は、これらの情報の何れか一つ以上を用いて指定される。例えば、後述する暗号化処理では、矩形の変換領域を指定するために、３点の位置情報を用いる。位置情報は、一般にｘ軸と、該ｘ軸に直交するｙ軸とを用いて、ｃｍ、インチ、ピクセル等の単位を用いて表すことが出来る。また、デジタル画像の幅または長さを単位として、ｘ軸およびｙ軸におけるデジタル画像の端からの位置を割合（％）で示してもよい。他に、デジタル画像の全てのピクセルに対して番号を割り当て（例えば、左上のピクセルから右下のピクセルまで連番を割り当てる）、この番号を用いて位置を特定する方法等も考えられる。なお、本実施形態に係る領域指定情報では、ページ番号情報とページ内の位置情報とを組み合わせることで、複数ページに亘る電子データについて、ページ毎に異なる変換領域を特定することが出来る。

【００３８】

暗号化画像取得部１３は、ユーザ端末１１２ｂから、ネットワーク１１３を介して送信された暗号化画像を取得する。また、ユーザ端末１１２ｂは、スキャナ１０６ｂやデジタルカメラ等、証明書を撮像可能な装置を用いて証明書の所定の部分（本実施形態では、証明書の裏面）を撮像することで、暗号化画像を取得する。

【００３９】

復号部１４は、暗号化画像取得部１３によって取得された暗号化画像中の変換領域を、鍵情報取得部２２によって取得された復号鍵を用いて復号することで、復号されたデジタル画像を生成する。なお、復号部１４による復号処理の詳細については後述する。

【００４０】

出力部１８は、暗号化部１１によって生成された暗号化画像を含む証明書印刷用データをユーザ端末１１２ａへ送信し、復号部１４によって復号されたデジタル画像をユーザ端末１１２ｂへ送信する。本実施形態において、証明書印刷用データとは、印刷の際に紙媒体の表面に印刷されるべき、証明書によって証明される内容を示す情報であって、改竄検出の対象となる対象情報のイメージと、印刷の際に紙媒体の裏面に印刷されるべき暗号化画像と、を含む、印刷用の情報である。

【００４１】

図３は、本実施形態に係る証明書発行処理の流れを示すシーケンス図である。証明書発行処理は、ユーザが、ユーザ端末１１２ａを操作して、改竄検出用情報出力システム１００にログインを行うことで開始される。

【００４２】

ステップＳ１０１およびステップＳ１０２では、ログイン処理が行われる。ユーザ端末１１２ａは、ユーザによるログイン指示の入力を受けて、改竄検出用情報出力システム１００にログイン情報を送信する（ステップＳ１０１）。このログイン情報には、端末を操作するユーザを識別する情報の他に、パスワード等が含まれる。改竄検出用情報出力システム１００は、端末より送信されたログイン情報を受信し、ユーザ認証部２４は、受信されたログイン情報と、サーバ側で保持する認証のための情報とを比較することで、ユーザを認証する（ステップＳ１０２）。なお、ログイン処理は、ユーザ端末１１２ａと改竄検出用情報出力システム１００との間での複数回の通信を伴ってもよい。また、ユーザ端末１１２ａを認証するための認証サーバを、改竄検出用情報出力システム１００とは別に用意して、ユーザを認証することとしてもよい。その後、処理はステップＳ１０３へ進む。

【００４３】

ステップＳ１０３からステップＳ１０５では、ユーザが取得したい証明書の指定を含む、証明書の発行に必要な情報が入力され、証明書の発行要求および入力された情報がユーザ端末１１２ａから改竄検出用情報出力システム１００へ送信される。ユーザ端末１１２ａは、ユーザによるマウス／キーボード等の入力装置を介した入力を受け付けることで、ユーザが所望する証明書の種類や内容等を指定する（ステップＳ１０３）。そして、ユーザ端末１１２ａは、ユーザ操作に基づいて指定された、証明書の発行に必要な各種情報を、改竄検出用情報出力システム１００へ送信する（ステップＳ１０４）。改竄検出用情報

出力システム１００のユーザ入力受付部２６は、ユーザ端末１１２ａより送信された各種情報を受信し、ＲＡＭ１０２へ記録する（ステップＳ１０５）。その後、処理はステップＳ１０６へ進む。

【００４４】

ステップＳ１０６では、証明書作成用の電子データが取得される。電子データ取得部１７は、ステップＳ１０５で受信された情報（例えば、発行される証明書が住民票である場合には、発行が要求された住民票に記載される氏名や住所等）を検索キーとして証明書情報データベース２３を検索することで、証明書の作成に必要な電子データを索出し、取得する。その後、処理はステップＳ１０７へ進む。

【００４５】

ステップＳ１０７では、デジタル画像が生成される。デジタル画像取得部１５は、ステップＳ１０６で取得された電子データを予め設定された、紙媒体に印刷される証明書の書式にレイアウトし、印刷用イメージまたは表示用イメージのビットマップデータを作成することで、デジタル画像を取得する。その後、処理はステップＳ１０８へ進む。

【００４６】

ステップＳ１０８では、鍵情報が生成される。鍵情報取得部２２は、ステップＳ１０７で取得されたデジタル画像の暗号化に用いる暗号鍵と復号鍵のセット（以下、鍵情報）を生成する。この際、鍵情報は、推測されにくい、十分な強度を持ったものが生成されることが好ましい。なお、本実施形態では、鍵情報は、証明書の発行処理の都度、自動生成されることとしているが、鍵情報は、証明書発行機関や改竄検出用情報出力システム１００の管理者によって予め決定され、鍵情報テーブルに予め保存されていてもよい。また、この鍵情報は、ユーザが証明書の内容を改竄して改竄後の内容に基づく暗号化画像を作成することが出来ないように、ユーザに対しては秘密にされることが好ましい。その後、処理はステップＳ１０９へ進む。

【００４７】

ステップＳ１０９では、暗号化が行われ、暗号化画像が生成される。暗号化部１１は、ステップＳ１０７で生成されたデジタル画像を、ステップＳ１０８で生成された暗号鍵を用いて暗号化する。この際、デジタル画像は、全体ではなく一部が指定されて暗号化されてもよい。例えば、領域指定情報を用いてデジタル画像のうち一部または全体を指定し、この暗号化領域のみが暗号鍵に基づいて変換されてもよい。暗号化される領域は、領域指定情報を用いて予め設定されていてもよいし、暗号化の都度ユーザ操作によって指定されてもよい。例えば、ユーザは、ユーザ端末１１２ａのディスプレイに表示されたデジタル画像を閲覧しながら、マウスを用いて範囲選択することで、暗号化の対象となる領域を指定することが出来る。その後、処理はステップＳ１１０へ進む。

【００４８】

ステップＳ１１０およびステップＳ１１１では、文書ＩＤの生成および鍵情報の保存が行われる。鍵情報記憶部２１は、発行される証明書を識別するための文書ＩＤを、これまでに発行された証明書の文書ＩＤと重複しないように生成する（ステップＳ１１０）。ここで、新たに生成される文書ＩＤは、この証明書に含まれる暗号化画像の復号鍵を推定不可能な値とすることが好ましい。そして、鍵情報記憶部２１は、生成された文書ＩＤと、ステップＳ１０８で生成された鍵情報とを関連付けて、ＨＤＤ１０３上に構築された鍵情報テーブルに蓄積する（ステップＳ１１１）。その後、処理はステップＳ１１２へ進む。

【００４９】

ステップＳ１１２では、証明書の印刷用データが生成される。出力部１８は、ステップＳ１０７で生成されたデジタル画像を紙媒体の表面に、ステップＳ１０９で生成された暗号化画像を紙媒体の裏面に印刷するための印刷用データを生成する。印刷用データとは、ユーザ端末１１２ａからプリンタ１０７ａを用いて証明書の紙媒体への印刷を行うための、印刷内容を含む電子データであり、データ形式には、例えば、ＰＤＦ（Ｐｏｒｔａｂｌｅ　Ｄｏｃｕｍｅｎｔ　Ｆｏｒｍａｔ）等が挙げられる。また、出力部１８は、復号時に鍵情報の取得を容易にするために、証明書を識別するための文書ＩＤを、紙媒体の裏面の

うち暗号化画像に被らない領域に付加する。文書ＩＤは、暗号化画像中に画像として付加されることで、紙媒体への印刷時に、暗号化画像と共に表示されるように付加される。このようにすることで、証明書の提出先で改竄の有無がチェックされる際にも、暗号化画像と共に文書ＩＤをスキャナ１０６ｂ等で読み込んで、ＯＣＲやバーコードリーダ等の手段で文書ＩＤを取得することが可能である。

【００５０】

ステップＳ１１３からステップＳ１１５では、暗号化画像がユーザ端末１１２ａへ送信され、印刷される。出力部１８は、ステップＳ１１２で生成された証明書の印刷用データを、ユーザ端末１１２ａへ送信する（ステップＳ１１３）。送信された証明書の印刷用データは、ユーザ端末１１２ａによって受信され（ステップＳ１１４）、紙媒体へ印刷される（ステップＳ１１５）。なお、本実施形態では、証明書の印刷用データに含まれる証明書の内容と改竄検出用のイメージとは紙媒体の表裏に印刷されるが、表面と裏面の両面への印刷は、プリンタ１０７ａに備えられた両面印刷機能を用いて一連の印刷処理として行われてもよいし、ユーザによる手差しで一面ずつ行われてもよい。

【００５１】

なお、本実施形態では、証明書発行機関等によって運用される改竄検出用情報出力システム１００は、印刷用データの出力までを行い、実際の印刷はユーザの手に委ねることとしているが、印刷データの生成から印刷までの一連の処理の全てを、改竄検出用情報出力システム１００が行うこととしてもよい。

【００５２】

図４は、本実施形態に係る改竄検出用情報出力システム１００によって発行され、ユーザ端末１１２ａからプリンタ１０７ａを操作して印刷された証明書の概要を示す図である。証明書の表面には、証明書によって証明される内容であって、改竄検出の対象となる対象情報のイメージ４０１が印刷され、裏面には、上記フローチャートを用いて説明した処理によって生成された暗号化画像４０２が印刷される。なお、図４では、表面に印刷される情報の全体を改竄検出の対象とした場合について図示されているが、改竄検出の対象となる情報は、表面に印刷される証明書の内容のうち一部のみであってもよい。また、裏面の暗号化画像が印刷されていない余白部分には、文書ＩＤ４０３が印刷される。文書ＩＤ４０３は、バーコードや文字列、記号等の形式で印刷されてよい。

【００５３】

ユーザは、印刷した証明書を、この証明書の提出を求める第三者に提出することが出来る。本実施形態に係る改竄検出用情報出力システム１００によれば、ユーザはこれまでのように証明書発行機関へ出向くことなく、例えば自宅に居ながらにして、またはコンビニエンスストア等の店舗において、証明書の発行を受けることが出来る。即ち、本実施形態に係る改竄防止情報出力システムによれば、住民票の発行をコンビニエンスストアで行う等、証明書の性格上、従来は証明書を発行することが出来なかったような場所で行うことが可能となる。

【００５４】

この証明書は、従来の証明書のような、特殊な用紙に印刷される等、ユーザによる複製を困難とすることで改竄等の不正行為の防止するものではなく、一般的なプリンタを用いてユーザ自身の手で印刷されたものであるが、証明書の内容を、証明書の発行者しか知り得ない暗号鍵を用いて暗号化して印刷したものである。このため、本実施形態に係る改竄検出用情報出力システム１００によれば、証明書の勝手な複製や改竄等の不正行為を検出、防止することが出来る。このようにして発行された証明書は、証明書の提出を求める者に対して提出され、証明書の提出を受けた者は、以下に説明する処理を改竄検出用情報出力システム１００に行わせることによって、提出された証明書が改竄されたものでないことを確認することが出来る。

【００５５】

図５は、本実施形態に係る改竄チェック用画像出力処理の流れを示すシーケンス図である。改竄チェック用画像出力処理は、提出された証明書を受領したユーザ（図３のフロー

チャートに示した処理において、ユーザ端末１１２ａを操作して証明書の発行を受けたユーザとは異なる）が、ユーザ端末１１２ｂを操作して、改竄検出用情報出力システム１００にログインを行うことで開始される。

【００５６】

ステップＳ２０１からステップＳ２０３では、ログイン処理が行われ、暗号化画像が取得される。ログイン処理の詳細は、上述したステップＳ１０１およびステップＳ１０２と同様であるため、説明を省略する。ログイン処理が行われた後、ユーザは、スキャナ１０６ｂに提出された証明書をセットし、ユーザ端末１１２ｂを介してスキャナ１０６ｂを操作することで、証明書の裏面を撮像し、暗号化画像および文書ＩＤを取得する（ステップＳ２０３）。その後、処理はステップＳ２０４へ進む。

【００５７】

ステップＳ２０４およびステップＳ２０５では、改竄検出用情報出力システム１００における復号に必要な各種情報が、ユーザ端末１１２ｂから改竄検出用情報出力システム１００へ送信される。ユーザ端末１１２ｂは、ステップＳ２０３で取得された暗号化画像と文書ＩＤ等、暗号化画像の復号に必要な情報を、改竄検出用情報出力システム１００へ送信する（ステップＳ２０４）。改竄検出用情報出力システム１００のユーザ入力受付部２６は、ユーザ端末１１２ｂより送信された情報を受信し（ステップＳ２０５）、ＲＡＭ１０２へ記録する。その後、処理はステップＳ２０６へ進む。

【００５８】

ステップＳ２０６およびステップＳ２０７では、文書ＩＤが取得され、暗号化画像の復号に用いる復号鍵が取得される。鍵情報取得部２２は、暗号化画像と共に受信された、証明書の文書ＩＤを、ＯＣＲ／バーコード読み取り等の方法で取得する（ステップＳ２０６）。そして、鍵情報取得部２２は、ステップＳ２０６で取得された文書ＩＤを用いて鍵情報記憶部２１に蓄積された鍵情報を検索することで、今回改竄チェックの対象となっている証明書に係る鍵情報（ここでは復号鍵）を取得する。その後、処理はステップＳ２０８へ進む。

【００５９】

ステップＳ２０８では、復号が行われ、デジタル画像が生成される。復号部１４は、ステップＳ２０５で取得された暗号化画像を、ステップＳ２０７で取得された復号鍵を用いて復号する。その後、処理はステップＳ２０９へ進む。

【００６０】

ステップＳ２０９からステップＳ２１１では、復号されたデジタル画像がユーザ端末１１２ｂへ送信され、ディスプレイ等へ出力される。出力部１８は、ステップＳ２０８で復号されたデジタル画像を、ユーザ端末１１２ｂへ送信する（ステップＳ２０９）。送信されたデジタル画像は、ユーザ端末１１２ｂによって受信され（ステップＳ２１０）、ユーザ端末１１２ｂに接続されたディスプレイに出力される。その後、本フローチャートに示された処理は終了する。

【００６１】

本実施形態に係る改竄検出用情報出力システム１００によれば、ユーザは、証明書裏面の暗号化画像が復号されたデジタル画像を閲覧し、証明書表面の改竄検出の対象情報と比較することが出来る。ユーザは、復号デジタル画像と、証明書表面の情報とを比較することで、改竄の有無、改竄があった場合には改竄された箇所、内容および改竄前の正しい情報を把握することが出来る。なお、本実施形態では、暗号化画像の復号を、証明書発行機関等によって運用される改竄検出用情報出力システム１００が行うこととしているが、このような構成に代えて、証明書発行機関等によって運用されるシステムは、復号鍵の取得までを行い、実際の復号処理はユーザ端末（この場合、ユーザ端末が本発明の改竄検出用情報出力システムに相当する）が行うこととしてもよい。

【００６２】

また、本実施形態に係る改竄検出用情報出力システム１００によれば、改竄検出用のデータである暗号化画像の生成が、証明書の内容のデジタル画像に基づいて行われるため、

従来の改竄防止技術と異なり、テキスト文字だけではなく、写真、イラスト、若しくはテキスト、写真およびイラストが混在した文書まで、紙媒体に印刷される情報であればどのようなものについても改竄の検出を行うことが可能である。特に、テキスト中の外字や特殊文字を画像の嵌め込みで表現しているような証明書（例えば住民票がこれにあたる）についても、複雑な処理を行うことなく、改竄の検出のための暗号化画像を生成することが出来る。

【００６３】

また、本実施形態では、暗号化画像を復号する際に復号鍵を取得する方法として、文書ＩＤを用いて鍵情報テーブルを検索する方法が採用されているが、復号時の鍵情報の取得には、その他の方法が採用されてもよい。例えば、鍵情報を更に別の鍵で暗号化した結果得られた情報を証明書に印刷し、復号時にはこの暗号化された鍵情報をシステム１００で復号することで、復号鍵を取得する方法がある。このようにすることで、ユーザに鍵情報を知らせることなく、鍵情報を証明書に印刷することが出来る。ここで、暗号化された鍵情報は、例えばＱＲコード等の形式で証明書に印刷されてもよい。

【００６４】

また、本実施形態では、一枚の紙媒体で構成される証明書を発行し、この証明書の改竄を検出する場合について説明したが、本発明に係る改竄検出用情報出力システムによって改竄の検出対象となる文書は、一枚の紙媒体からなる文書に限られない。例えば、複数枚に亘る文書の改竄を防止する場合、改竄検出のための暗号化画像は、各ページにつき１つ生成されてもよいが、例えば、複数ページを縮小してサムネイル状に並べた単一のデジタル画像を生成し、このデジタル画像を暗号化することで、単一の暗号化画像を用いて、複数ページに亘る文書の全てのページについて改竄を検出可能としてもよい。また、ページ毎に暗号化画像を生成する場合であっても、改竄検出の対象情報のイメージを縮小して暗号化することで、暗号化画像の印刷に必要な領域を節約することが出来る。

【００６５】

＜暗号化部および復号部＞

次に、上記第一の実施形態から第四の実施形態における、暗号化部および復号部による暗号化処理および復号処理の概要を説明する。

【００６６】

図６は、暗号化処理および復号処理の処理概要（その１）を示す図である。図６において、暗号化部１１（第１乃至第３の各態様においては、それぞれ暗号化部１１Ａ、１１Ｂ、１１Ｃという。）は、入力されたデジタル画像と暗号化方法を示す暗号鍵とに基づいて、前記デジタル画像の一部を暗号化した暗号化画像を出力する。プリンタ出力部１２は、暗号化部１１により暗号化されたデジタル画像を紙などの印刷可能な物理的媒体に印刷する。スキャナ（カメラ）読み込み部１３は、プリンタ出力部１２により出力された印刷画像を、スキャナまたはカメラを用いて読み込む。

【００６７】

そして、復号部１４（第１乃至第３の各態様においては、それぞれ復号部１４Ａ、１４Ｂ、１４Ｃという。）は、プリンタ出力部１２により出力された印刷画像と入力された復号鍵とにより復号画像を得る。この入力された復号鍵が正しい場合に限り暗号化画像を適切に復号でき、暗号化部１１による暗号化で隠された情報を見ることができる。

【００６８】

図７は、暗号化処理および復号処理の処理概要（その２）を示す図である。図７に示したように、本発明を適用した第１の態様乃至第３の態様における暗号化処理および復号処理は、暗号化部１１により暗号化されたデジタル画像をプリンタやスキャナを介さずに電子文書画像のまま復号部１４に入力し、復号画像を得ることも可能である。

【００６９】

次に、本発明を適用した第１の態様乃至第３の態様をそれぞれ説明する。まず、本発明を適用した第１の態様について説明する。

【００７０】

図８は、第１の態様における暗号化処理の概要を示す図である。図８において、暗号化部１１Ａは、暗号化領域決定部３１、画像変換部３２、画素値変換部３３およびマーカー付加部３４を備えている。

【００７１】

暗号化領域指定部３１は、暗号化したい領域を含む入力画像から暗号化する領域を選択する。

【００７２】

図９は、暗号化領域を選択する例を示す図である。すなわち、暗号化領域指定部３１は、図９の（Ａ）に示すように、暗号化したい領域を含むデジタル画像（入力画像）４１から暗号化する領域４２を選択する。この領域４２が後述する画像変換部３２および画素値変換部３３の処理により、図９の（Ｂ）に示したように変換画像４３に変換され、デジタル画像４１が変換画像４３を含む暗号化画像４４に変換される。

【００７３】

図８の説明に戻る。暗号化領域指定部３１により暗号化する領域４２が選択されると、画像変換部３２において暗号化する領域４２および暗号鍵を入力し、暗号鍵に対応する変換方法で暗号化する領域４２の画像を視覚的に変換する。その際の変換パラメータは、入力の暗号鍵から得られるバイナリデータにより作成する。

【００７４】

図１０は、暗号鍵の入力例を示す図である。図１０に示した例は、暗号鍵と、暗号鍵により生成されるバイナリデータの例である。例えば、暗号鍵としての数値「１２３４」は、バイナリデータ「１０００１１０１００１０」として入力され、暗号鍵としての文字列「ａｎｇｏ」は、バイナリデータ「０１１００００１０１１０１１１００１１００１１１０１１０１１１」として入力される。

【００７５】

画像変換方法として、本第１の態様では、画像を微小領域に分割して微小領域を並べ替える処理（スクランブル処理という。）による変換方法と、画像を圧縮処理することによる変換方法の２つを示す。

【００７６】

まず、スクランブル処理について説明する。スクランブル処理は、まず、選択された領域４２の画像を一定の大きさの微小領域に分割して、次に、暗号鍵から得られるバイナリデータにより微小領域の並び替えを行なう。

【００７７】

図１１は、画像変換部におけるスクランブル処理の一例を示す図である。図１１の（Ａ）に示したように、まず暗号化領域指定部３１により選択された領域４２を縦方向に分割し、暗号鍵６１のバイナリ列の各ビットを分割された領域４２の境界に左から順に対応させ、ビットが「１」の場合は隣り合う分割列を交換し、ビットが「０」の場合は何もしない処理を左側から順に行なう。分割境界の数に対してバイナリ列のビット数が足りない場合は、足りなくなった位置から同じバイナリ列を繰り返して領域４２の右端まで交換処理を行なう。

【００７８】

続いて、図１１の（Ｂ）に示すように、上記交換処理を行なった画像領域６２を横方向に分割し、暗号鍵６１のバイナリ列の各ビットを分割された画像領域６２の境界に上から順番に対応させ、縦分割で行ったのと同様の交換処理を行単位で上から順に行なう。

【００７９】

すると、図１１の（Ｃ）に示すように、各分割画像に交換処理を行った結果、元の領域４２がスクランブル処理された処理画像であるスクランブル画像６３が得られる。

【００８０】

このスクランブル処理例の拡張法として、横方向、縦方向ともに２度以上行なうこともでき、また２度目以降の交換において分割領域の大きさを変えることも可能である。さらに、横方向と縦方向で分割領域の交換に別のバイナリ列を用いることもできる。これらの

拡張法は、入力画像のサイズが小さく、かつ暗号鍵のビット長が長い場合に、異なる暗号鍵から全く同じ処理画像が生成されてしまうのを防ぐ手段として特に有効である。

【００８１】

図１２は、画像変換部におけるスクランブル処理の他の例を示す図である。図１１を用いて説明したスクランブル処理とはまた別のスクランブル処理法として、図１２に示したように微小領域単位で画素の交換を行う方法も可能である。すなわち、入力画像を矩形状の微小領域に分割し、分割された微小領域同士を交換する。これにより、上述の横方向と縦方向（行と列）の交換による方法よりもスクランブルの場合の数が多くなり、暗号強度を高めることができる。

【００８２】

図１３は、スクランブル処理における微小領域の形の変形例を示す図である。さらにスクランブル処理の際の微小領域の形は、図１２に示した四角形の他に、例えば図１３の（Ａ）に示したような三角形を用いることも可能である。また図１３の（Ｂ）に示したように、形や大きさの異なる微小領域を共存させることもできる。

【００８３】

次に、画像を圧縮処理することによる変換方法について説明する。

【００８４】

図１４は、画像変換部における圧縮処理を示す図である。入力画像４１が二値画像の場合に、まず図１４の（Ａ）に示したように暗号化領域指定部３１により選択された領域４２の画像を圧縮して、図１４の（Ｂ）に示したようなバイナリ列７１を作成する。ここでの圧縮法は、ファクシミリ装置での二値画像データ転送の際に用いられるランレングス圧縮や、二値画像の標準圧縮方式であるＪＢＩＧ（Ｊｏｉｎｔ　Ｂｉ－ｌｅｖｅｌ　Ｉｍａｇｅ　ｅｘｐｅｒｔｓ　Ｇｒｏｕｐ）圧縮など、あらゆる圧縮方式が適用可能である。

【００８５】

図１５は、変換データを画像化する処理を示す図である。図１４に示したような領域４２の圧縮に続いて、変換圧縮データであるバイナリ列７１の各ビットを、図１５（Ｂ）に示したように、ビットが「０」ならば「白」、ビットが「１」ならば「黒」である指定サイズの方形に拡大して方形画像（処理画像）８１を作成し、暗号化する画像の領域４２に白黒の方形画像８１として配列させる。

【００８６】

変換圧縮データ（バイナリ列７１）を選択された領域４２の画像内に収まるよう配列させたい場合、方形画像８１のサイズは選択された領域４２の圧縮率に依存してくる。例えば圧縮率が１／４以下であれば方形画像８１のサイズは高々２×２ピクセルであり、１／１６以下ならば高々４×４ピクセルである。

【００８７】

一方、予め方形画像８１のサイズを指定し、かつ圧縮データを選択された領域４２の画像内に収めたい場合は、最初の画像圧縮処理において方形画像８１のサイズに依存した圧縮率を達成する必要がある。例えば方形を４×４ピクセルのサイズにする場合は１／１６以上の圧縮率が必要となる。この場合には、選択された領域４２の情報を予め落として圧縮する方法や、非可逆な圧縮方式を用いる方法が有効である。

【００８８】

上記の圧縮データを拡大して画像化する暗号化処理により、例えば低解像度のカメラで暗号化画像を読み取った場合でも拡大された白黒のブロックを認識できるため、暗号化画像を正しく復号できる。

【００８９】

図８の説明に戻る。画素値変換部３３では、画像変換部３２で変換された処理画像６３内の画素を一定の間隔を置いて変換し、変換画像４３が概ね格子状の縞模様を成すようにする。

【００９０】

図１６は、画素値変換部における画素値変換処理の例（その１）を示す図である。画素

値変換部３３では、画像変換部３２により領域４２がスクランブルされた処理画像６３の画素を、一定の間隔で変換し、暗号化画像４４が全体として概ね格子状の縞模様を成すようにする。例えば図１６に示したように、図１６の（Ａ）に示したスクランブル画像６３を（Ｂ）に示した市松模様（チェッカー模様）画像９１の有色部分で反転処理するような変換を実行することにより、（Ｃ）に示したように暗号化画像４４が全体として概ね格子状の縞模様を成す変換画像９２が得られる。これにより、生成される縞状の模様は、暗号化画像４４を復号する際に暗号化領域内の各画素の詳細な位置を検出するために用いられる。

【００９１】

これらの一連の処理に関して、別の変換を実施することも可能である。例えば画素値を反転する処理は、指定の値を加算する処理であってもよい。

【００９２】

また、図１６の（Ｂ）に示した市松模様画像９１は、（Ａ）に示したスクランブル画像６３と略同サイズであるが、スクランブル画像６３より小さいサイズを用いることにより、スクランブル画像６３の周辺以外の中心部分のみ反転処理するようにしてもよい。

【００９３】

図１７は、画素値変換部における画素値変換処理の例（その２）を示す図である。また、画素値を変換する領域４２は、図１７の（Ａ）から（Ｃ）に示したように種々の形状を適用することが可能である。画素値変換は小領域間の境界位置を高精度に検出することを目的とした処理であるため、例えば図１７の（Ａ）のように境界部分のみ画素値変換することも考えられる。また、図１７の（Ｂ）のように微小領域に対して少しずつずらしながら画素値変換を行うことで、変換と非変換の境界がより細かい間隔で現れるため、復号処理において暗号化画像４４の画素位置をさらに詳細に検出できる。また、図１７の（Ｃ）ように微小領域の境界が交差する部分のみに画素値変換を行えば、紙などに印刷した画像をスキャナやカメラで読み込んで復号する際の画質の劣化を最小限に抑えることができる。

【００９４】

ここで、微小領域の形が均一な大きさの四角形ではなく、図１３に示したように三角形（図１３の（Ａ））や異なる大きさ、形が共存する場合（図１３の（Ｂ））は、上述の変換例に限らず形状に応じた方法で画素値変換を行う必要があることを追記しておく。

【００９５】

上述したように、本発明においては、暗号化位置を表す規則的な模様を、特許文献１のように入力画像に上書きして生成するのではなく、入力画像の画素値を変換することで生成している。したがって、従来の技術のように暗号化画像の端部分の画像情報が位置検出のために犠牲にされることがなく、元の画像情報に位置検出情報を共存させる形で効率よく暗号化を行なえる。

【００９６】

なお、模様を構成する部分に何らかの画像情報が含まれるとその規則性が多少崩れてしまうが、後述の復号部１４の処理で述べるように暗号化画像全体の統計的な性質を用いることで暗号化位置を検出することができる。

【００９７】

図８の説明に戻る。マーカー付加部３４では、画素値変換部３３で変換処理された変換画像９２の四隅のうち、例えば右下以外の三箇所に位置決めマーカーを付加し暗号化画像４４を作成する。

【００９８】

マーカー付加部３４は、暗号化された領域４２の位置を特定するための位置決めマーカーを、変換画像９２の四隅のうち例えば右下以外の三箇所に配置する。

【００９９】

図１８は、暗号化処理で用いる位置決めマーカーの例を示す図である。本第１の態様で用いる位置決めマーカーは、図１８の（Ａ）に示すように丸十字の形をしたものとする。

位置決めマーカーの形をより広く言えば、実線の円または多角形とその周と交わる複数の線で構成されるものであればよい。このような例として、図１８の（Ｂ）の位置決めマーカーのように漢字の「田」の形をしたものや、（Ｃ）の位置決めマーカーのように中心から三つの線が円周に向かって放射線状に出ているもの、（Ｄ）の位置決めマーカーのように線が途中で切れているもの、などが挙げられる。

【０１００】

また、位置決めマーカーの色の構成は、最も単純には背景が白で前景を黒にすればよいが、これに限らず変換画像９２の色（画素値）分布に応じて適宜変更しても差し支えない。また背景と前景に決まった色を指定するのではなく、背景の色はデジタル画像４１のままで前景の画素値を反転するなどして位置決めマーカーを形作る方法も考えられる。このようにすれば、位置決めマーカー部分の入力画像情報も保持されたまま画像の暗号化を行なえる。

【０１０１】

図１９は、暗号化画像の例を示す図である。以上の暗号化部１１Ａの処理により、最終的には図１９に示すような暗号化画像４４が生成される。暗号化画像４４には、変換画像９２と位置決めマーカー１２１が含まれる。

【０１０２】

さらに、本第１の態様の暗号化方法において、画像変換部３２で「微小領域を並べ替える処理（スクランブル処理）」を用いた場合は、二値画像だけでなくグレースケールやカラーの画像に対しても暗号化処理を適用できる。

【０１０３】

図２０は、グレースケールの画像を暗号化した例である。図２０において、（Ａ）に示したグレースケール画像１３１は、暗号化部１１Ａの処理により、（Ｂ）に示すように変換画像１３３と位置決めマーカー１３４を含む暗号化画像１３２が生成される。

【０１０４】

次に、復号部１４Ａの説明を行なう。

【０１０５】

図２１は、第１の態様における復号処理の概要を示す図である。図２１において、復号部１４Ａは、マーカー検出部１４１、暗号化領域検出部１４２、暗号化位置検出部１４３および画像逆変換部１４４を備えている。

【０１０６】

マーカー検出部１４１は、一般的な画像認識技術を用いて、上述のマーカー付加部３４により付加した位置決めマーカーの位置を暗号化画像から検出する。検出方法としては、パターンマッチングや図形の連結性に関する解析などが適用可能である。

【０１０７】

暗号化領域検出部１４２は、マーカー検出部１４１により検出された３つの位置決めマーカーの位置関係に基づいて、暗号化されている画像の領域を検出する。

【０１０８】

図２２は、位置決めマーカーから暗号化領域を検出する過程を示す図である。図２２の（Ａ）に示されたように、マーカー検出部１４１によって暗号化画像１５１から少なくとも３つの位置決めマーカー１５２が検出されると、（Ｂ）に示すように、１つの暗号化領域１５３を検出することができる。すなわち、３つの位置決めマーカー１５２は、長方形の暗号化領域１５３の四隅に配置されているため、これら３つの点（位置決めマーカー１５２の位置）を線で結んで得られる図形はおおよそ直角三角形になる。そこで、位置決めマーカー１５２が３つ以上検出された場合は、３つの位置決めマーカー１５２の位置関係が直角三角形に近い形状で構成される領域を含み、３つの位置決めマーカー１５２の位置を４つの角部分のうち３つの角部分とする長方形を暗号化領域１５３とする。なお、検出位置決めマーカー１５２の数が２つ以下の場合は、対応する暗号化領域１５３を特定できないため、暗号化画像は存在しないとして復号処理を終了する。

【０１０９】

図２３は、暗号化領域検出処理の流れを示すフローチャートである。暗号化領域検出部１４２で実行される暗号化領域検出処理は、まず、ステップＳ１６０１において、マーカー検出部１４１によって検出された位置決めマーカー１５２の数を変数ｎに代入し、ステップＳ１６０２において、暗号化領域１５３の検出用フラグｒｅｇ＿ｄｅｔｅｃｔに０を代入する。

【０１１０】

そして、ステップＳ１６０３において、位置決めマーカー１５２の数が代入された変数ｎが３以上であるか否かを判断し、変数ｎが３以上でなければ、すなわち変数ｎが２以下であれば（ステップＳ１６０３：Ｎｏ）、本暗号化領域検出処理を含む復号処理を終了する。

【０１１１】

他方、変数ｎが３以上であれば（ステップＳ１６０３：Ｙｅｓ）、ステップＳ１６０４において、マーカー検出部１４１によって検出された位置決めマーカー１５２のうちの３つの位置決めマーカー１５２を選択し、ステップＳ１６０５において、その選択した３つの位置決めマーカー１５２の位置関係が略直角三角形であるか否かを判断する。

【０１１２】

選択した３つの位置決めマーカー１５２の位置関係が略直角三角形でなければ（ステップＳ１６０５：Ｎｏ）、ステップＳ１６０６において、マーカー検出部１４１によって検出された位置決めマーカー１５２の３点の組み合わせが全て終了したか否かを判断し、終了していなければ（ステップＳ１６０６：Ｎｏ）、ステップＳ１６０４に戻って他の３点を選択し、終了した場合（ステップＳ１６０６：Ｙｅｓ）、ステップＳ１６０８に進む。

【０１１３】

他方、選択した３つの位置決めマーカー１５２の位置関係が略直角三角形であれば（ステップＳ１６０５：Ｙｅｓ）、ステップＳ１６０７において、検出用フラグｒｅｇ＿ｄｅｔｅｃｔに１を代入する。

【０１１４】

そして、ステップＳ１６０８において、検出用フラグｒｅｇ＿ｄｅｔｅｃｔに１が代入されているか、すなわち、３点の位置関係が直角三角形となる３つの位置決めマーカー１５２を検出することができたか否かを判断し、ｒｅｇ＿ｄｅｔｅｃｔに１が代入されていれば（ステップＳ１６０８：Ｙｅｓ）、暗号化位置検出部１４３の処理に進み、ｒｅｇ＿ｄｅｔｅｃｔに１が代入されていなければ（ステップＳ１６０８：Ｎｏ）、本暗号化領域検出処理を含む復号処理を終了する。

【０１１５】

図２１の説明に戻る。暗号化位置検出部１４３は、暗号化画像１５１の復号を正確に行なうために、暗号化領域検出部１４２により検出された暗号化領域１５３の端の部分が規則的な画素分布を成すことを利用して、周波数解析やパターンマッチングなどにより暗号化領域１５３内の各画素の詳細な位置を検出する。この検出は、画素値変換部３３の画素値変換（反転）処理により暗号化画像１５１の全体が周期的な模様を成すという性質を利用する。

【０１１６】

一つの検出方法として、まず模様の周期（幅）を画像の横方向および縦方向に関して高速フーリエ変換（Ｆａｓｔ　Ｆｏｕｒｉｅｒ　Ｔｒａｎｓｆｏｒｍ：ＦＦＴ）などの周波数解析法で求め、その後テンプレートマッチングなどによりの境界位置（オフセット）を検出する方法が考えられる。

【０１１７】

また、暗号化画像にエッジ検出フィルタ（ラプラシアンフィルタ等）をかけると境界部分が直線状になる性質を利用して、境界位置をハフ変換により検出することも可能である。

【０１１８】

図２４は、暗号化位置が検出された例を示す図である。暗号化されたデジタル画像４１

が複雑である場合は、暗号化画像４４の周期性が著しく損なわれる部分が出てくる可能性もある。このような場合、模様の周期と境界位置の計算に用いる画像領域を周期性の比較的強い部分に限定して暗号化位置検出を行なう方法が有効である。

【０１１９】

図２１の説明に戻る。画像逆変換部１４４は、暗号化位置検出部１４３により検出された暗号化位置情報とユーザにより入力された復号鍵とを用いて、暗号化画像４４を復号鍵に対応する方法で画像変換部３２による変換処理の逆変換処理を実行し、復号画像を生成する。復号の処理手順は、暗号化処理と逆の手順で実現されるため説明を省略する。以上が本発明を適用した第１の態様についての説明である。

【０１２０】

次に、本発明を適用した第２の態様について説明する。

【０１２１】

図２５は、第２の態様の全体イメージを示す図である。第２の態様は、暗号化処理の前に、暗号化画像１８３の復号の妥当性を検証するための特定のチェック用マーク１８２を、暗号化する領域１８１の任意の場所に付加して（図２５の（Ａ））暗号化を行ない（図２５の（Ｂ））、暗号化画像１８３を復号した後に事前に付加したチェック用マーク１８２が復号画像１８４から検出されれば正しく復号されたとして復号処理を終了する（図２５の（Ｃ））。チェック用マーク１８２が検出されない場合（図２５の（Ｄ））は、暗号化位置を補正し、チェック用マーク１８２が検出されるまで、または指定の基準を満たすまで復号処理を繰り返す。

【０１２２】

図２６は、第２の態様における暗号化処理の概要を示す図である。図２６において、暗号化部１１Ｂは、暗号化領域決定部３１、チェック用マーク付加部１９２、画像変換部３２および画素値変換部３３を備えている。

【０１２３】

第１の態様と同様、暗号化領域指定部３１は、暗号化したい領域を含む入力画像から暗号化する領域を選択する。

【０１２４】

そして、チェック用マーク付加部１９２は、暗号化画像１８３の復号の妥当性を検証するための特定のチェック用マーク１８２を暗号化する領域１８１の任意の場所に付け加える。チェック用マーク１８２は、なるべく画像情報が少ない画素分布の平坦な領域に付加するのが望ましい。

【０１２５】

指定位置にチェック用マーク１８２を付け加えた後、第１の態様と同様、画像変換部３２において暗号化する領域１８１および暗号鍵を入力し、暗号鍵に対応する変換方法で暗号化する領域１８１の画像を視覚的に変換し、画素値変換部３３では、画像変換部３２で変換された処理画像内の画素を一定の間隔を置いて変換し、変換画像が概ね格子状の縞模様を成すようにする。

【０１２６】

図２７は、第２の態様における復号処理の概要を示す図である。図２７において、復号部１４Ｂは、暗号化領域検出部２０１、暗号化位置検出部１４３、画像逆変換部１４４、チェック用マーク検出部２０４および暗号化位置補正部２０５を備えている。

【０１２７】

まず初めに、暗号化領域検出部２０１は、暗号化画像１８３の大まかな領域を検出する。暗号化部１１Ｂの暗号化処理により、暗号化画像１８３の画素分布はおおよそ市松模様状になっているため、それぞれ横方向と縦方向に関してＦＦＴなどの周波数解析を行なうと、縞の周期に対応する周波数のパワーが際立って強くなる。

【０１２８】

図２８は、暗号化領域の検出方法を説明するための図である。図２８の（Ａ）に示したように、暗号化画像２１１を周波数解析すると、（Ｂ）に示すように、ある周波数（その

周波数の整数倍の周波数）のパワーが突出する領域を「周期性強」２１４と表現している。暗号化領域内では画素分布の周期性が強くなる傾向にあるため、これにより大まかな暗号化領域と縞模様の周期を検出することができる。

【０１２９】

図２７の説明に戻る。暗号化位置検出部１４３は、暗号化領域検出部２０１による暗号化の大まかな領域を特定した後、暗号化領域をさらに正確に検出し、同時に暗号化領域内の各画素の詳細な位置を検出する。位置検出の一例として、まず暗号化領域検出部２０１で求めた縞模様の周期と画素絶対値差分の分布により画素値変換の境界位置（オフセット）を求め、そこからさらに画素絶対値差分が相対的に大きい領域を絞り込む方法が考えられる。また、第１の態様の暗号化位置検出部１４３と同様、暗号化位置検出にハフ変換を用いることも可能である。

【０１３０】

図２９は、暗号化位置（横方向）の検出方法を説明するための図である。上述のような暗号化領域の検出処理を横方向、縦方向それぞれに行なうと、図２９のように暗号化位置２２１が検出される。

【０１３１】

図２７の説明に戻る。画像逆変換部１４４は、暗号化位置情報と復号鍵を用いて第１の態様と同様の方法を行ない、復号画像を生成する。

【０１３２】

チェック用マーク検出部２０４は、画像逆変換部１４４で復号した復号画像からチェック用マークの検出を試みる。検出方法は第１の態様におけるマーカー検出処理と同様であるため説明を省略する。そして、チェック用マークが検出された場合は復号画像を出力して処理を完了する。チェック用マークが検出されない場合は暗号化位置補正部２０５において暗号化位置を補正し、チェック用マークが検出されるまで、または指定の基準を満たすまで復号処理（画像逆変換処理）をやり直す。

【０１３３】

図３０は、暗号化位置の検出を誤った例を示す図である。図３０に示したように、暗号化画像の端を見落としてしまう場合（取りこぼしライン２３１）が考えられる。そこで、チェック用マーク２２１の検出に失敗した場合は、暗号化位置を表すラインを左右端と上下端に追加または削除して画像逆変換処理を行ない、チェック用マーク２２１が検出できるかどうかを各々検討する。ラインをどのように追加または削除してもチェック用マーク２２１を検出できない場合は、復号画像を出力せずに処理を終了する。以上が本発明を適用した第２の態様についての説明である。

【０１３４】

次に、本発明を適用した第３の態様について説明する。本発明の第３の実施形態では、第１の態様で示した暗号化領域を特定する位置決めマーカーと、第２態様の復号画像の妥当性を判断するためのチェック用マークの両方を用いて画像の暗号化、復号を行なう。これら位置検出用の位置決めマーカーと復号画像確認用のチェック用マークの２種類を用いることで、正しい復号鍵が入力された場合の画像復号誤りを低減できる。

【０１３５】

図３１は、第３の態様における暗号化処理の概要を示す図である。図３１において、暗号化部１１Ｃは、暗号化領域決定部３１、チェック用マーク付加部１９２、画像変換部３２、画素値変換部３３およびマーカー付加部３４を備えている。

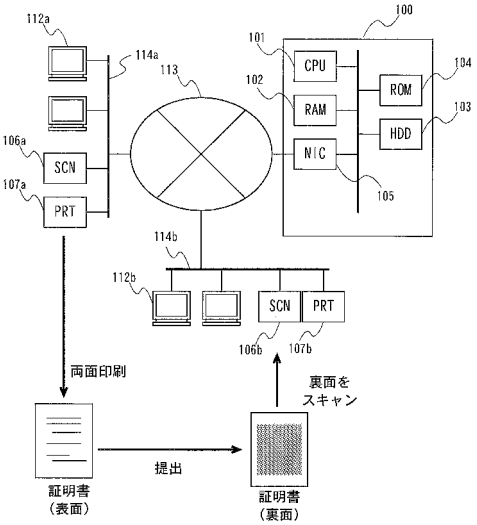
【０１３６】

まず暗号化領域指定部３１で暗号化する画像領域を選択し、チェック用マーク付加部１９２で第２の態様と同様の方法で復号検証用のチェック用マークを付け加える。チェック用マークを付加した後、画像変換部３２と画素値変換部３３において、第１の態様１および２と同様の方法で画像処理を行ない画像を暗号化し、マーカー付加部３４で暗号化領域検出用の位置決めマーカーを第１の態様と同様の方法で付加する。これら各処理の内容は、第１の態様または第２の態様と同様であるため説明を省略する。

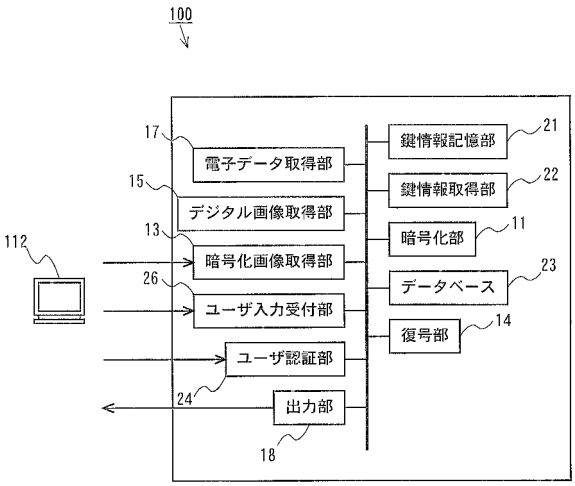
【０１３７】
図３２は、第３の態様における復号処理の概要を示す図である。図３２において、復号部１４Ｃは、マーカー検出部１４１、暗号化領域検出部１４２、暗号化位置検出部１４３、画像逆変換部１４４、チェック用マーク検出部２０４および暗号化位置補正部２０５を備えている。
【０１３８】
まずマーカー検出部１４１において第１の態様と同様の方法で位置決めマーカーを検出し、続く暗号化領域検出部１４２で第１の態様と同様の方法で暗号化領域を検出する。さらに暗号化位置検出部１４３において、第１の態様と同様の方法で暗号化領域内の各画素の詳細な位置を検出する。また、画像逆変換部１４４、チェック用マーク検出部２０４および暗号化位置補正部２０５で実行される各処理手順は、第２の態様と同様であるため説明を省略する。以上が本発明を適用した第３の態様についての説明である。
【図面の簡単な説明】
【０１３９】
【図１】実施形態に係る改竄検出用情報出力システムのハードウェア構成の概略を示す図である。
【図２】実施形態に係る改竄検出用情報出力システムの機能構成の概略を示す図である。
【図３】実施形態に係る証明書発行処理の流れを示すシーケンス図である。
【図４】実施形態に係る改竄検出用情報出力システムによって発行され、ユーザ端末からプリンタを操作して印刷された証明書の概要を示す図である。
【図５】実施形態に係る改竄チェック用画像出力処理の流れを示すシーケンス図である。
【図６】暗号化処理および復号処理の処理概要（その１）を示す図である。
【図７】暗号化処理および復号処理の処理概要（その２）を示す図である。
【図８】第１の態様における暗号化処理の概要を示す図である。
【図９】暗号化領域を選択する例を示す図である。
【図１０】暗号鍵の入力例を示す図である。
【図１１】画像変換部におけるスクランブル処理の一例を示す図である。
【図１２】画像変換部におけるスクランブル処理の他の例を示す図である。
【図１３】スクランブル処理における微小領域の形の変形例を示す図である。
【図１４】画像変換部における圧縮処理を示す図である。
【図１５】変換データを画像化する処理を示す図である。
【図１６】画素値変換部における画素値変換処理の例（その１）を示す図である。
【図１７】画素値変換部における画素値変換処理の例（その２）を示す図である。
【図１８】暗号化処理で用いる位置決めマーカーの例を示す図である。
【図１９】暗号化画像の例を示す図である。
【図２０】グレースケールの画像を暗号化した例である。
【図２１】第１の態様における復号処理の概要を示す図である。
【図２２】位置決めマーカーから暗号化領域を検出する過程を示す図である。
【図２３】暗号化領域検出処理の流れを示すフローチャートである。
【図２４】暗号化位置が検出された例を示す図である。
【図２５】第２の態様の全体イメージを示す図である。
【図２６】第２の態様における暗号化処理の概要を示す図である。
【図２７】第２の態様における復号処理の概要を示す図である。
【図２８】暗号化領域の検出方法を説明するための図である。
【図２９】暗号化位置（横方向）の検出方法を説明するための図である。
【図３０】暗号化位置の検出を誤った例を示す図である。
【図３１】第３の態様における暗号化処理の概要を示す図である。
【図３２】第３の態様における復号処理の概要を示す図である。
【符号の説明】
【０１４０】

１１　暗号化部
１３　暗号化画像取得部
１４　復号部
１５　デジタル画像取得部
１７　電子データ取得部
１８　出力部
２１　鍵情報記憶部
２２　鍵情報取得部
２３　証明書情報データベース
２４　ユーザ認証部
２６　ユーザ入力受付部
１００　改竄検出用情報出力システム

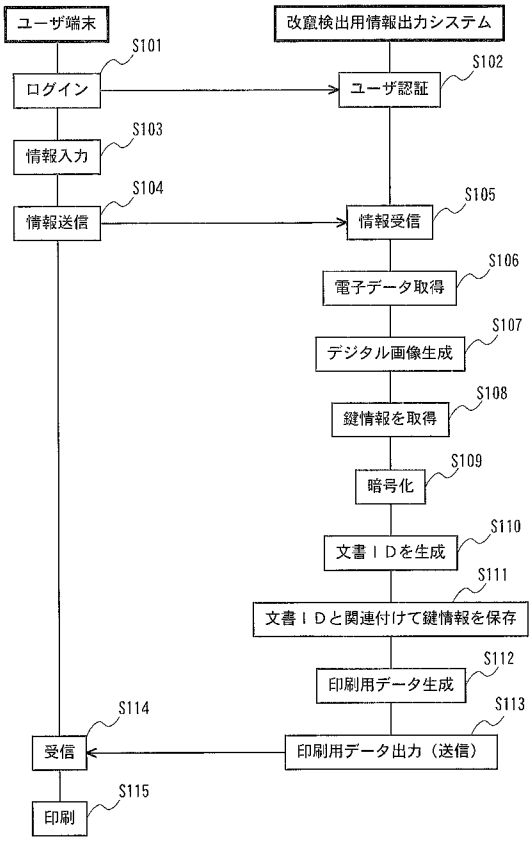
【図１】



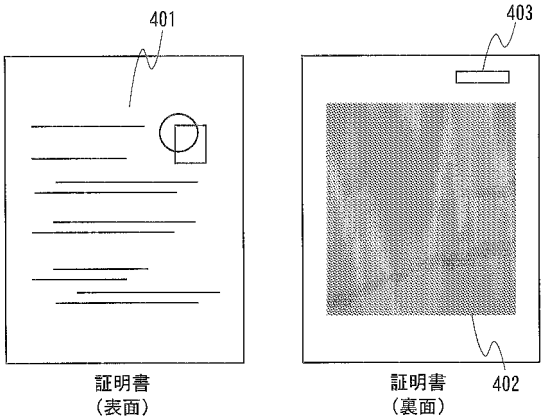
【図２】



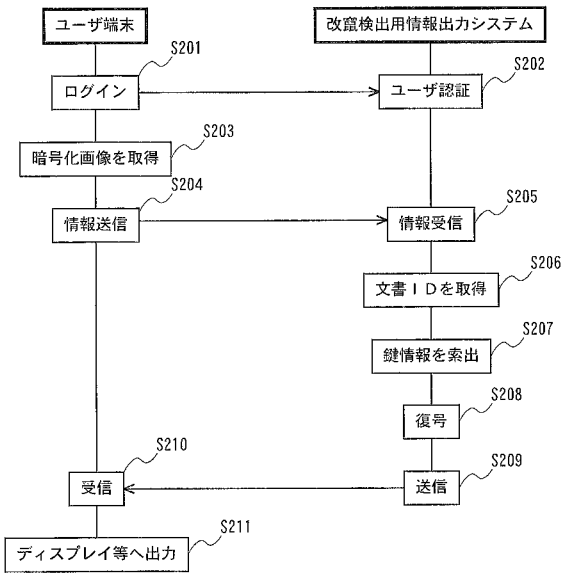
【図３】


ユーザ端末
改竄検出用情報出力システム
S101
ログイン
S102
ユーザ認証
S103
情報入力
S104
情報送信
S105
情報受信
S106
電子データ取得
S107
デジタル画像生成
S108
鍵情報を取得
S109
暗号化
S110
文書ＩＤを生成
S111
文書ＩＤと関連付けて鍵情報を保存
S112
印刷用データ生成
S113
印刷用データ出力（送信）
S114
受信
S115
印刷

【図４】


401
403
証明書
（表面）
証明書
（裏面）
402

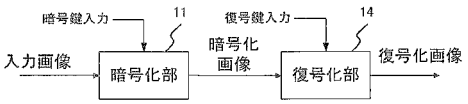
【図５】


ユーザ端末
改竄検出用情報出力システム
S201
ログイン
S202
ユーザ認証
S203
暗号化画像を取得
S204
情報送信
S205
情報受信
S206
文書ＩＤを取得
S207
鍵情報を索出
S208
復号
S209
送信
S210
受信
S211
ディスプレイ等へ出力

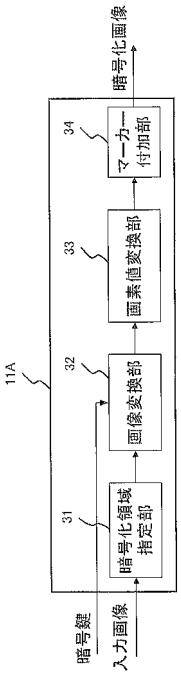
【図６】


復号化画像
14
復号化部
復号鍵入力
スキャン画像
13
スキャナ（カメラ）読み込み部
印刷画像
12
プリンタ出力部
暗号化画像
11
暗号化部
暗号鍵入力
入力画像

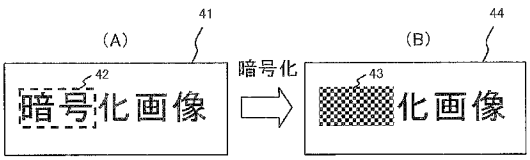
【図７】


暗号鍵入力
11
復号鍵入力
14
入力画像
暗号化部
暗号化画像
復号化部
復号化画像

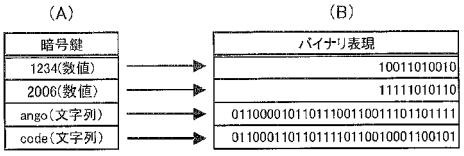
【図８】


暗号化画像
34
マーカー付加部
33
画素値変換部
32
画像変換部
11A
31
暗号化領域指定部
暗号鍵
入力画像

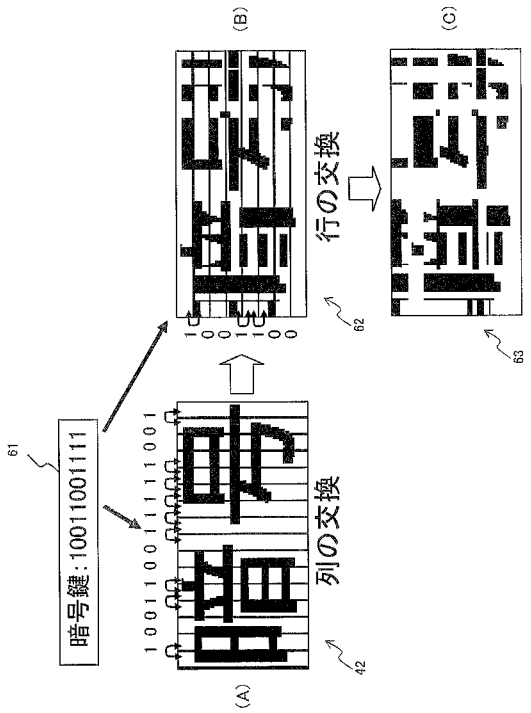
【図９】


41
(A)
42
暗号化画像
暗号化
44
(B)
43
化画像

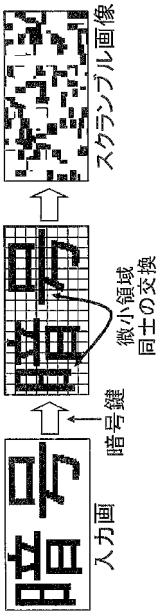
【図１０】


(A)
(B)
暗号鍵
バイナリ表現
1234(数値)
10011010010
2006(数値)
11111010110
ango(文字列)
code(文字列)

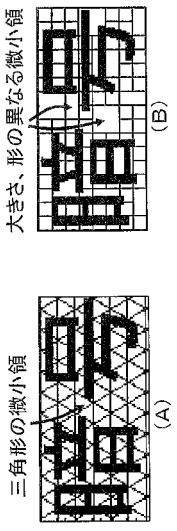
【図１１】



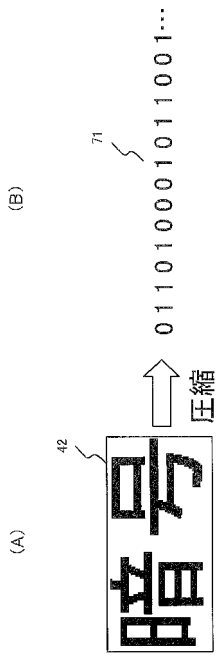
【図１２】



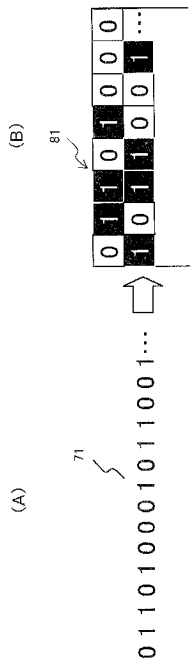
【図１３】



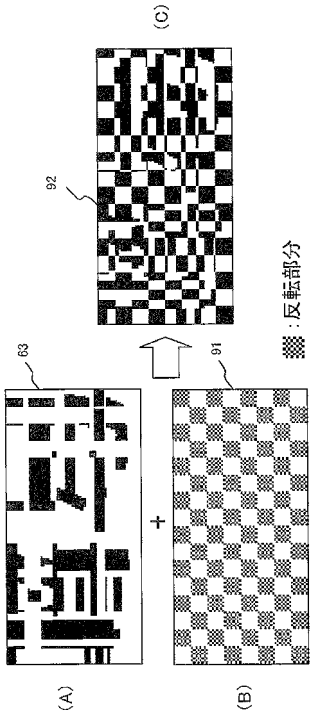
【図１４】



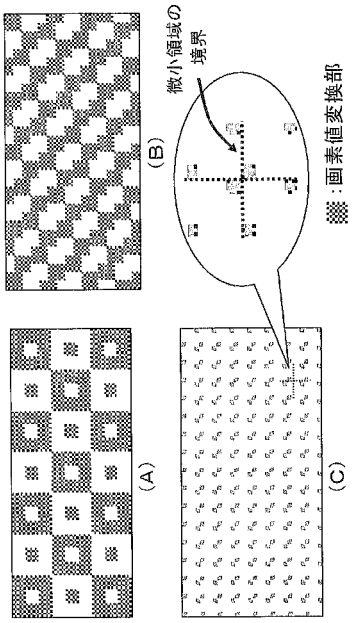
【図１５】



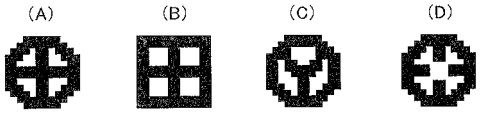
【図１６】



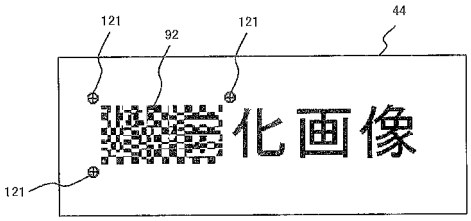
【図１７】



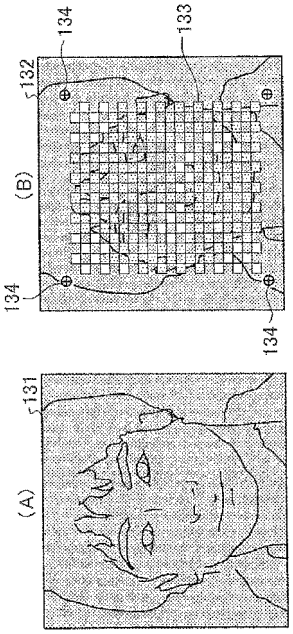
【図１８】



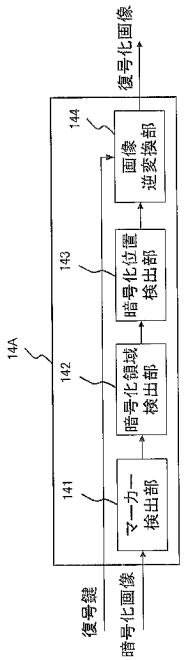
【図１９】



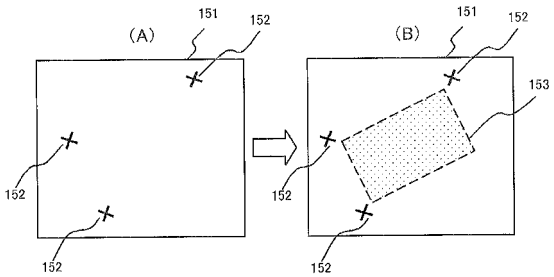
【図２０】



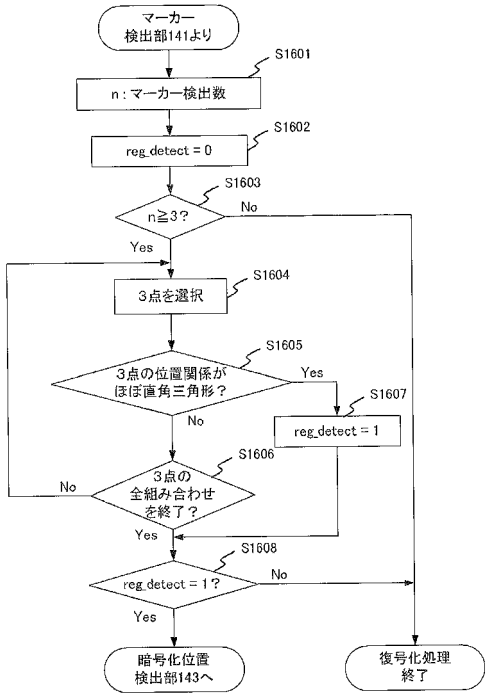
【図２１】



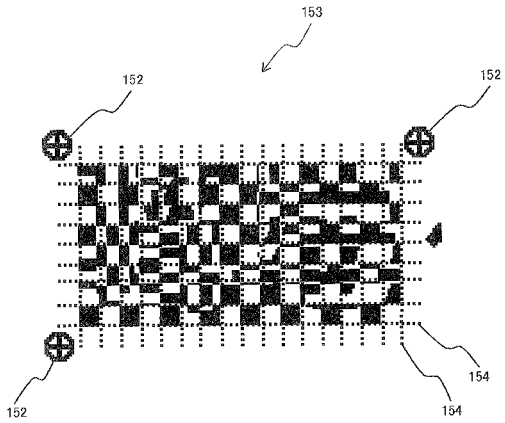
【図２２】



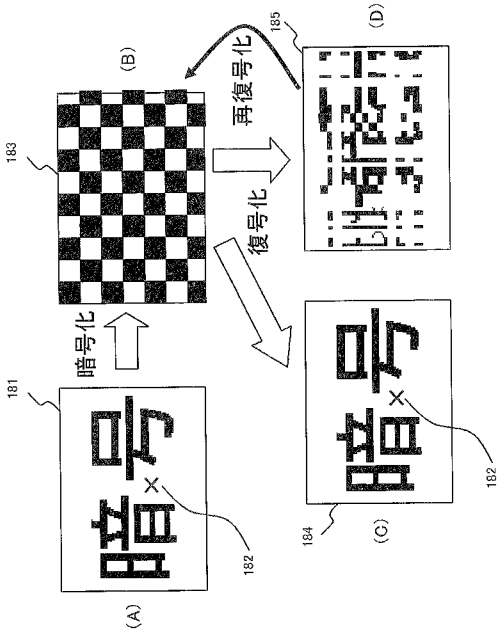
【図２３】



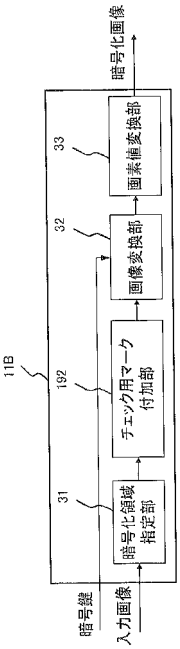
【図２４】



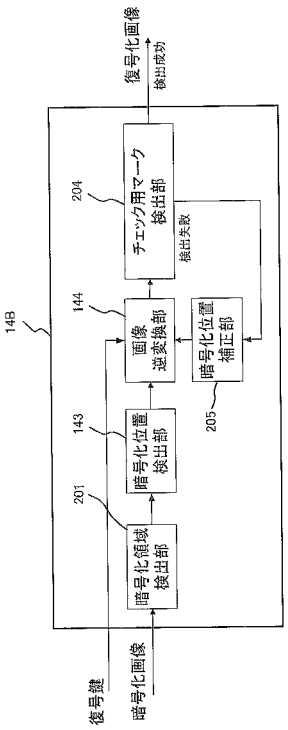
【図２５】



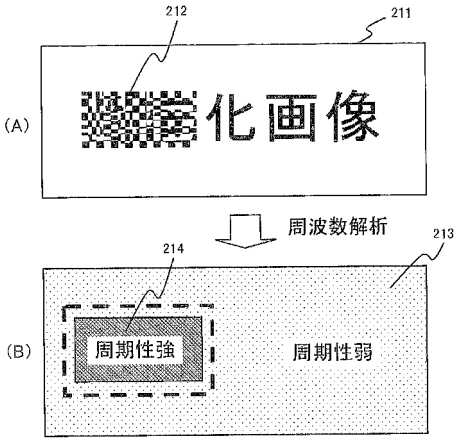
【図２６】



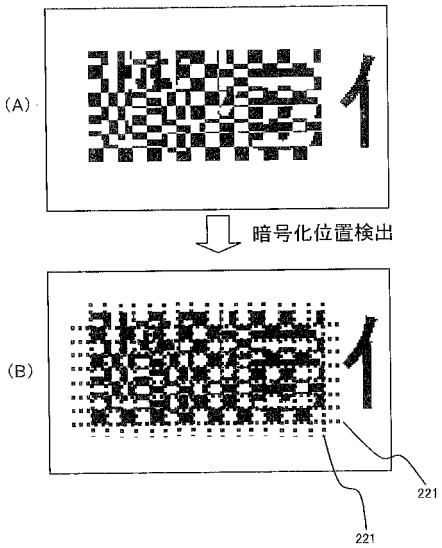
【図２７】



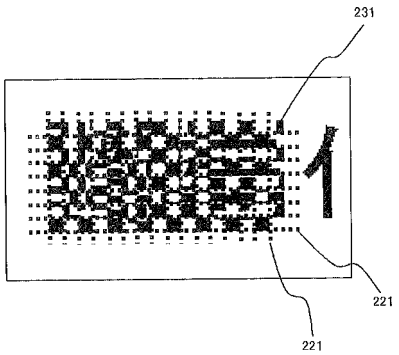
【図２８】



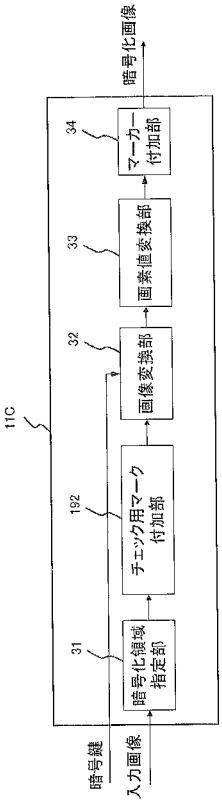
【図２９】



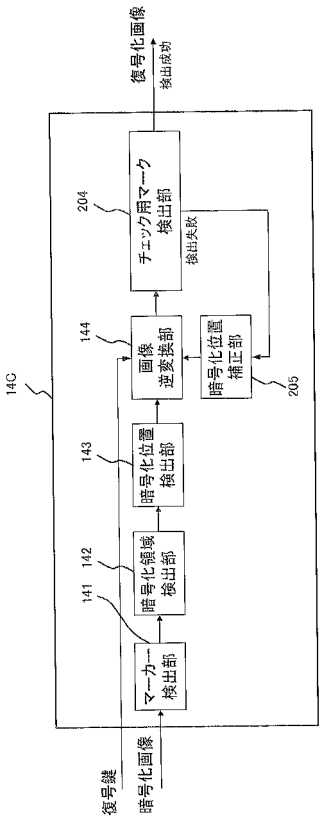
【図３０】



【図３１】


11C
暗号鍵
入力画像
31
暗号化領域指定部
192
チェック用マーク付加部
32
画像変換部
33
画素値変換部
34
マーカー付加部
暗号化画像

【図３２】


14C
復号鍵
暗号化画像
141
マーカー検出部
142
暗号化領域検出部
143
暗号化位置検出部
144
画像逆変換部
204
チェック用マーク検出部
検出成功
検出失敗
205
暗号化位置補正部
復号化画像

フロントページの続き

(51)Int.Cl.	F I	テーマコード（参考）
G06F 21/24 (2006.01)	G06F 12/14 560C	

(72)発明者 井波 康治
石川県かほく市宇野気ヌ９８番地の２ 株式会社ＰＦＵ内
(72)発明者 長島 睦
石川県かほく市宇野気ヌ９８番地の２ 株式会社ＰＦＵ内

Ｆターム(参考) 2C061 CL10
5B017 AA08 BA09 CA16
5B021 BB02 BB03 NN18
5C076 AA14 BA06
5J104 AA08 LA06 PA14