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

特許第4143441号
(P4143441)

(45)発行日　平成20年9月3日(2008.9.3)　(24)登録日　平成20年6月20日(2008.6.20)

(51)Int.Cl.			F I		
H04N	1/387	(2006.01)	H04N	1/387	
G06T	1/00	(2006.01)	G06T	1/00	500B
G09C	5/00	(2006.01)	G09C	5/00	
G09C	1/00	(2006.01)	G09C	1/00	640D

請求項の数 4　(全 31 頁)

(21)出願番号　特願2003-53894(P2003-53894)
(22)出願日　平成15年2月28日(2003.2.28)
(65)公開番号　特開2004-7442(P2004-7442A)
(43)公開日　平成16年1月8日(2004.1.8)
審査請求日　平成18年2月21日(2006.2.21)
(31)優先権主張番号　特願2002-122600(P2002-122600)
(32)優先日　平成14年4月24日(2002.4.24)
(33)優先権主張国　日本国(JP)

(73)特許権者　000001007
キヤノン株式会社
東京都大田区下丸子３丁目３０番２号
(74)代理人　100076428
弁理士　大塚　康徳
(74)代理人　100112508
弁理士　高柳　司郎
(74)代理人　100115071
弁理士　大塚　康弘
(74)代理人　100116894
弁理士　木村　秀二
(72)発明者　林　淳一
東京都大田区下丸子３丁目３０番２号　キヤノン株式会社内

最終頁に続く

(54)【発明の名称】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】
ドキュメントに付加情報を埋め込む情報処理方法であって、
ドキュメントデータ入力手段により、文字列を含むドキュメントデータを入力するドキュメントデータ入力入力工程と、
抽出手段により、前記入力したドキュメントデータ中の文字を認識し、当該認識結果に基づき、前記入力したドキュメントデータをユニークに識別するための識別情報を付加情報として抽出する抽出工程と、
判定手段により、前記入力したドキュメントデータ中の前記文字列が位置する領域位置を判定し、判定された領域位置を表わす位置情報を生成する判定工程と、
前記画像入力手段により、所定の画像を背景画像データとして入力する画像入力工程と、
埋め込み手段により、前記抽出工程で抽出した識別情報を、前記背景画像データ内の、前記位置情報で示される領域外の領域に、電子透かしの強度を定義する第１のパラメータを用いて埋め込むとともに、前記抽出工程で抽出した識別情報を、前記位置情報で示される前記背景画像データ中の該当する領域内に、前記第１のパラメータよりも高い強度を示す第２のパラメータを用いて埋め込む埋め込み工程と、
合成手段により、前記埋め込み工程による埋め込み後の背景画像データと、前記ドキュメントデータ入力工程で入力したドキュメントデータとを合成する合成工程と、
出力手段により、前記合成工程による合成後のドキュメントデータを出力する出力工程

と
を備えることを特徴とする情報処理方法。
【請求項２】
ドキュメントに付加情報を埋め込む情報処理装置であって、
文字列を含むドキュメントデータを入力するドキュメントデータ入力入力手段と、
前記入力したドキュメントデータ中の文字を認識し、当該認識結果に基づき、前記入力したドキュメントデータをユニークに識別するための識別情報を付加情報として抽出する抽出手段と、
前記入力したドキュメントデータ中の前記文字列が位置する領域位置を判定し、判定された領域位置を表わす位置情報を生成する判定手段と、
所定の画像を背景画像データとして入力する画像入力手段と、
前記抽出手段で抽出した識別情報を、前記背景画像データ内の、前記位置情報で示される領域外の領域に、電子透かしの強度を定義する第１のパラメータを用いて埋め込むとともに、前記抽出手段で抽出した識別情報を、前記位置情報で示される前記背景画像データ中の該当する領域内に、前記第１のパラメータよりも高い強度を示す第２のパラメータを用いて埋め込む埋め込み手段と、
前記埋め込み手段による埋め込み後の背景画像データと、前記ドキュメントデータ入力手段で入力したドキュメントデータとを合成する合成手段と、
前記合成手段による合成後のドキュメントデータを出力する出力手段と
を備えることを特徴とする情報処理装置。
【請求項３】
コンピュータに、請求項２に記載の情報処理装置として機能させることを特徴とするコンピュータプログラム。
【請求項４】
請求項３に記載のコンピュータプログラムを格納したことを特徴とするコンピュータ可読記憶媒体。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】
本発明はドキュメントデータが改ざんされているか否かを検証する方法及び装置、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に関するものである。
【０００２】
【従来の技術】
近年、コンピュータとそのネットワークの急速な発達及び普及により、文字データ、画像データ、音声データなど、多種の情報がディジタル化されている。こうした情報のディジタル化に伴い、従来、紙等を用いていた種々の書類もディジタルデータとして取り扱われることが多くなっている。しかしながら、ディジタルデータは容易に改ざんすることが可能であり、ディジタルデータの改ざん防止が大きな問題となっている。そのため、改ざん防止のためのセキュリティ技術は急速に重要性を増している。そこでディジタルデータの改ざん、偽造が行われていた場合にそれを検出するような方式、システムが提案されてきた。
【０００３】
例えばディジタル署名を利用するシステムは、前記改ざん、偽造を検出するシステムとしてよく知られている。ここでディジタル署名について簡単に説明する。
【０００４】
ディジタル署名とは、送信者がデータと一緒に該データに対応する署名データを送り、受信者がその署名データを検証して該データの正当性を確認することである。ディジタル署名データ生成にハッシュ（Ｈａｓｈ）関数と公開鍵暗号を用いたデータの正当性の確認は以下のようになる。
【０００５】

秘密鍵をＫｓ、公開鍵をＫｐとすると、発信者は、平文データＭをハッシュ関数により圧縮して一定長の出力ｈ（例えば１２８ビット）を算出する演算を行う。次に秘密鍵Ｋｓでｈを変換してディジタル署名データｓを作成する演算、すなわちD(Ｋｓ,ｈ)=ｓを行う。その後、該ディジタル署名データｓと平文データＭとを送信する。

【０００６】

一方受信者は受信したディジタル署名データｓを公開鍵Ｋｐで変換する演算、すなわちE(Ｋｐ,ｓ)= E(Ｋｐ,D(Ｋｓ,ｈ''))= ｈ''と、受信した平文データM'を発信者と同じハッシュ関数により圧縮してｈ' を算出する演算を行い、ｈ'とｈ''が一致した場合、受信したデータM'が正当であると判断する。

【０００７】

平文データＭが送受信間で改ざんされた場合にはE(Ｋｐ,ｓ)= E(Ｋｐ,D(Ｋｓ,ｈ''))= ｈｈ''と、受信した平文データM'を発信者と同じハッシュ関数により圧縮したｈ'が一致しないので改ざんを検出できるわけである。

【０００８】

ここで、平文データＭの改ざんに合わせてディジタル署名データｓの改ざんも行われてしまうと改ざんの検出ができなくなる。しかし、これはｈから平文データＭを求める必要があり、このような計算はハッシュ関数の一方向性により不可能である。以上、説明したように、公開鍵暗号方式とハッシュ関数を用いたディジタル署名によって、正しくデータの認証を行うことが可能である。

【０００９】

次にハッシュ関数について説明する。ハッシュ関数は上記ディジタル署名の生成を高速化するため等に用いられる。ハッシュ関数は任意の長さの平文データＭに処理を行い、一定の長さの出力ｈを出す機能を持つ。ここで、出力ｈを平文データＭのハッシュ値（またはメッセージダイジェスト、ディジタル指紋）という。ハッシュ関数に要求される性質として、一方向性と衝突耐性が要求される。一方向性とはｈを与えた時、h=H(M)となる平文データＭの算出が計算量的に困難であることである。衝突耐性とは平文データＭを与えた時、H(M)=H(M')となる平文データM'(M≠M')の算出が計算量的に困難であること、及び、H(M)=H(M')かつM≠M'となる平文データM,M'の算出が計算量的に困難であることである。

【００１０】

ハッシュ関数としてはＭＤ－２，ＭＤ－４，ＭＤ－５，ＳＨＡ－１，ＲＩＰＥＭＤ－１２８,ＲＩＰＥＭＤ－１６０等が知られており、これらのアルゴリズムは一般に公開されている。

【００１１】

続いて公開鍵暗号について説明する。公開鍵暗号は暗号鍵と復号鍵が異なり、暗号鍵を公開、復号鍵を秘密に保持する暗号方式である。公開鍵暗号の特徴としては、

（ａ） 暗号鍵と復号鍵とが異なり暗号鍵を公開できるため、暗号鍵を秘密に配送する必要がなく、鍵配送が容易である。

（ｂ） 各利用者の暗号鍵は公開されているので、利用者は各自の復号鍵のみ秘密に記憶しておけばよい。

（ｃ） 送られてきた通信文の送信者が偽者でないこと及びその通信文が改ざんされていないことを受信者が確認するための認証機能を実現できる。が挙げられる。

【００１２】

例えば、平文データＭに対して、公開の暗号鍵Ｋｐを用いた暗号化操作をE(Ｋｐ,M)とし、秘密の復号鍵Ｋｓを用いた復号操作をD(Ｋｓ,M)とすると、公開鍵暗号アルゴリズムは、まず次の２つの条件を満たす。（１） Ｋｐが与えられたとき、E(Ｋｐ,M)の計算は容易である。Ｋｓが与えられたとき、D(Ｋｓ,M)の計算は容易である。（２） もしＫｓを知らないなら、ＫｐとＥの計算手順と、Ｃ＝E(Ｋｐ,M)を知っていても、Ｍを決定することは計算量の点で困難である。

【００１３】

次に、上記（１）、（２）に加えて、次の（３）の条件が成立することにより秘密通信が実現できる。（３） 全ての平文データMに対し、E(Ｋｐ,M) が定義でき、D(Ｋｓ,E(Ｋｐ,M))＝Mが成立する。つまり、Ｋｐは公開されているため誰もがE(Ｋｐ,M) を計算することができるが、D(Ｋｓ,E(Ｋｐ,M)) を計算してMを得ることができるのは秘密鍵Ｋｓを持っている本人だけである。

【００１４】

一方、上記（１）、（２）に加えて、次の（４）の条件が成立することにより認証通信が実現できる。（４） すべての平文データMに対し、D(Ｋｓ,M) が定義でき、E(Ｋｐ,D(Ｋｓ,M))＝Mが成立する。つまり、D(Ｋｓ,M) を計算できるのは秘密鍵Ｋｓを持っている本人のみであり、他の人が偽の秘密鍵Ｋｓ'を用いて D(Ｋｓ',M) を計算しＫｓを持っている本人になりすましたとしても、E(Ｋｐ,D(Ｋｓ',M))≠M なので受信者は受けとった情報が不正なものであることを確認できる。また、D(Ｋｓ,M) が改ざんされても E(Ｋｐ,D(Ｋｓ,M)')≠M となり、受信者は受けとった情報が不正なものであることを確認できる。

【００１５】

上記の秘密通信と認証通信とを行うことができる代表例としてＲＳＡ暗号やR暗号やW暗号等が知られている。

【００１６】

ここで、現在最も使用されている、ＲＳＡ暗号の暗号化、復号は次式で示される。

暗号化： 暗号化鍵（ｅ,ｎ） 暗号化変換C=Ｍｅ(ｍｏｄ ｎ)

復号： 復号鍵（ｄ,ｎ） 復号変換M=Ｃｄ(ｍｏｄ ｎ)

ｎ＝ｐ・ｑ ここでｐ、ｑは大きな異なる素数である。

【００１７】

上記のように、ＲＳＡ暗号は暗号化にも復号にもべき乗演算と剰余演算が必要であるので、ＤＥＳをはじめとする共通鍵暗号と比較すると演算量が膨大なものとなり高速な処理は難しい。

【００１８】

以上説明したように、従来技術における改ざん、及び偽造の検出は、ディジタルデータに加えて、前記ディジタル署名を必要とする方式である。通常、ディジタル署名は、ディジタルデータのヘッダ部分などに添付する方式で送信することが行われる。しかしながら、ディジタルデータのフォーマット変換などによって添付されたディジタル署名は容易に除去される可能性がある。ディジタル署名が除去された場合、ディジタルデータの認証をすることはできない。

【００１９】

これを解決した方法が、特許文献１に示されている。この特許文献１においては、署名装置において、ディジタル情報をふたつの領域に分割し、分割された第１の領域からディジタル署名を生成し、生成されたディジタル署名を、分割された第２の領域に電子透かしとして埋め込むことにより、署名が施されたディジタル情報を生成する。一方、認証装置においては、署名が施されたディジタル情報を前記第１の領域と第２の領域に分割し、前記第１の領域から第１のディジタル署名を生成し、第２の領域から電子透かしとして埋め込まれている第２のディジタル署名を抽出する。そして第１のディジタル署名と第２のディジタル署名が等しい時に前記ディジタル情報が改ざん、及び偽造されていないことを認証する方法である。

【００２０】

【特許文献１】

特開平１０－１６４５４９号公報

【００２１】

【発明が解決しようとする課題】

以上説明したように、ディジタルデータの認証をするためには、ディジタル署名などの認証情報をディジタル情報と不可分の状態にしておくことが重要である。被署名データが画

像データの場合は、前記特許文献１の方法を適用することが可能であるが、被署名データがドキュメントなどの場合には適用することが困難である。

【００２２】

本発明はかかる問題点に鑑みなされたものであり、文書等のドキュメントデータの改ざんを検証できる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を提供しようとするものである。

【００２３】

【課題を解決するための手段】

かかる課題を解決するため、例えば本発明の情報処理方法は以下の構成を備える。すなわち、

ドキュメントに付加情報を埋め込む情報処理方法であって、

ドキュメントデータ入力手段により、文字列を含むドキュメントデータを入力するドキュメントデータ入力入力工程と、

抽出手段により、前記入力したドキュメントデータ中の文字を認識し、当該認識結果に基づき、前記入力したドキュメントデータをユニークに識別するための識別情報を付加情報として抽出する抽出工程と、

判定手段により、前記入力したドキュメントデータ中の前記文字列が位置する領域位置を判定し、判定された領域位置を表わす位置情報を生成する判定工程と、

前記画像入力手段により、所定の画像を背景画像データとして入力する画像入力工程と、

埋め込み手段により、前記抽出工程で抽出した識別情報を、前記背景画像データ内の、前記位置情報で示される領域外の領域に、電子透かしの強度を定義する第１のパラメータを用いて埋め込むとともに、前記抽出工程で抽出した識別情報を、前記位置情報で示される前記背景画像データ中の該当する領域内に、前記第１のパラメータよりも高い強度を示す第２のパラメータを用いて埋め込む埋め込み工程と、

合成手段により、前記埋め込み工程による埋め込み後の背景画像データと、前記ドキュメントデータ入力工程で入力したドキュメントデータとを合成する合成工程と、

出力手段により、前記合成工程による合成後のドキュメントデータを出力する出力工程とを備える。

【００２４】

また、他の発明は、以下の構成を備える。すなわち、

ドキュメントデータが改ざんされているか否かを検証する情報処理方法であって、

ドキュメントデータを入力する入力工程と、

入力したドキュメントデータ中の識別情報を認識する識別情報抽出工程と、

前記ドキュメントデータの背景に付加されている付加情報を抽出する付加情報抽出工程と、

前記識別情報抽出工程で抽出された識別情報と、前記付加情報抽出工程で抽出された付加情報を比較する比較工程とを備える。

【００２５】

また、他の発明は、以下の構成を備える。すなわち、

ドキュメントデータに付加情報を埋め込む情報処理方法であって、

ドキュメントデータを入力する工程と、

所定の画像を入力する工程と、

前記ドキュメントデータから特徴領域を抽出する特徴領域抽出工程と、

前記特徴領域に従って異なる強度で前記画像データに付加情報を埋め込む埋め込み工程と、

埋め込まれた画像を前記ドキュメントデータの背景画像として合成する合成工程とを備える。

【００２６】

【本発明の実施の形態】

以下、添付図面に従って本発明に係る実施形態を詳細に説明する。

【００２７】

図３は本実施の形態に適用可能な情報処理装置の全体構成を示したものである。同図において、ホストコンピュータ３０１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、スキャナ３１９から読み取られた画像を入力し、編集・保管することが可能である。同様に、デジタルカメラ３２１を用いて撮影された画像を入力し、同様に編集・保管することも可能である。更に、ここで得られた画像をプリンタ３１７から印刷させることが可能である。また、ユーザーからの各種マニュアル指示等は、マウス３１１、キーボード３１２からの入力により行われる。更に、モデム３１３やＮＩＣ（Network Interface Card）３１５を用いて他のコンピュータと種々のデータを送受信することが可能である。

【００２８】

ホストコンピュータ３０１の内部では、バス３２３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。

【００２９】

図中、３０２は、ホストコンピュータ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。

【００３０】

３０３は、内部の各ブロックの動作を制御、或いは内部に記憶されたプログラムを実行することのできるＣＰＵである。３０４は、ＢＩＯＳやブートプログラムを記憶しているＲＡＭである。３０５はＣＰＵ３０３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や実施形態で説明する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。

【００３１】

３０６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。３０８は、外部記憶媒体の一つであるＣＤ（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ドライブである。３０９は、３０８と同様にＦＤ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。３１０も、３０８と同様にＤＶＤからの読み込み、ＤＶＤへの書き出しができるＤＶＤドライブである。尚、ＣＤ，ＦＤ，ＤＶＤ等に画像編集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ＨＤ３０６上にインストールし、必要に応じてＲＡＭ３０５に転送されるようになっている。

【００３２】

３１４は、ポインティングデバイス（マウス（Ｒ）等）３１１或いはキーボード３１２からの入力指示を受け付けたり、モデム３１３を用いて他のコンピュータとデータを送受信するためにこれらと接続されるインターフェイス（Ｉ／Ｆ）である。

【００３３】

３１６は、ＮＩＣ３１５を用いて、ＨＤ３０６、ＣＤ３０８、ＦＤ３０９、ＤＶＤ３１０などに記憶されている種々のデータを他のコンピュータと送受信するためにこれらと接続されるインターフェイス（Ｉ／Ｆ）である。

【００３４】

３１８は、ＨＤ３０６、ＣＤ３０８、ＦＤ３０９、ＤＶＤ３１０などに記憶されている画像データや文字データをプリンタ３１７を用いて紙の媒体に出力するためにこれらと接続されるプリンタインターフェイス（Ｉ／Ｆ）である。

【００３５】

３２０は、スキャナ３１９から入力された画像データを受け付け、ＨＤ３０６やＲＡＭ３０５に記憶するためにこれらと接続されるインターフェイス（Ｉ／Ｆ）である。

【００３６】

３２２は、デジタルカメラ３２１を用いて撮影された画像データを受け付け、ＨＤ３０６やＲＡＭ３０５に記憶するためにこれらと接続されるインターフェイス（Ｉ／Ｆ）である。

【００３７】
[署名処理部]
以下、図１を用いて本実施の形態に適用される署名処理部（機能）を説明する。なお、以下の説明では、ホストコンピュータ３０１に電源が投入され、ＯＳがＲＡＭ３０５にロードされ、しかる後に、本実施形態で説明する処理を行うアプリケーションがＲＡＭ３０５にロードされている場合である。従って、各処理部は、該当するプログラム及びそれを実行するＣＰＵ３０３、場合によっては周辺のハードウェアでもって実現することになる。
【００３８】
図１に示すように、本実施の形態における署名処理部は、画像発生部１０１、ドキュメントデータ発生部１０２、識別情報抽出部１０３、付加情報埋め込み部１０４、合成部１０５、ドキュメントデータ出力部１０６から構成される。
【００３９】
なお、ここで説明する署名処理はソフトウェア処理により実現されても良い。その場合には、上記各部は上記処理に必要な機能を概念的なものとして捉えたものと考慮されるべきものである。
【００４０】
まず、画像発生部１０１の機能について説明する。画像発生部１０１は、後述するドキュメントデータの背景に設定される画像データＩ１を発生する。発生した画像データＩ１は、付加情報埋め込み部１０４に入力される。
【００４１】
以降の説明では、説明を簡単にするために、画像データＩ１はモノクロの多値画像を表現しているものとするが、本発明はこのような場合には限定されず、フルカラー画像等の任意画像を適用することも可能であることは明らかである。
【００４２】
画像発生部１０１が画像データＩ１を発生するには、図３におけるＲＯＭ３０４，ＲＡＭ３０５，ＨＤ３０６，ＣＤ３０８，ＦＤ３０９，ＤＶＤ３１０などに予め記憶されている画像データを読み出すことや、モデム３１３、ＮＩＣ３１５などを用いてネットワークを通じて画像データを受信して用いることや、スキャナ３１９、デジタルカメラ３２１などを用いて紙に印刷されている原稿をデジタル化して用いることなど種々の手段を用いることが可能であり、入力元は如何なるものでも構わない。画像発生部１０１において発生した画像データＩ１は一旦ＲＡＭ３０５に保持される。
【００４３】
次に、ドキュメントデータ発生部１０２の機能について説明する。ドキュメントデータ発生部１０２では、本実施の形態における署名処理部において署名が施されるドキュメントデータＤが発生する。発生したドキュメントデータＤは、識別情報抽出部１０３に入力される。
【００４４】
以降の説明では、説明を簡単にするために、ドキュメントデータＤは文書（白地に黒文字）の２値画像を表現しているものとするが、本発明はこのような場合には限定されず、多値画像やフルカラー画像を適用することも可能であることは明らかである。また、ドキュメントデータＤとしてＰＤＦなどの非画像データが発生した場合には、画像データに変換してから処理を行えばよい。
【００４５】
ドキュメントデータ発生部１０２でドキュメントデータを発生させる手段としては、前述した画像発生部１０１における手段と同様の手段が適用可能である。また、ドキュメントデータとして、テキストデータ（アスキーコードなどによる記述）やアプリケーションに依存したデータ（ＰＤＦなど）などが入力された場合には、これらのデータを画像データに変換するためにラスタライズ処理をするようにすれば良い。
【００４６】
ドキュメントデータ発生部１０２において発生したドキュメントデータＤは一旦ＲＡＭ３

０５に保持される。
【００４７】
次に、識別情報抽出部１０３の機能について説明する。識別情報抽出部１０３では、前記ドキュメントデータ発生部１０２からＲＡＭ３０５に出力されたドキュメントデータＤを読出し、その中から所定の識別情報Ｉｎｆ１を抽出し、抽出された識別情報Ｉｎｆ１を出力する。
【００４８】
ここで、識別情報抽出部１０３で実行される識別情報抽出処理について、図２０を用いて詳細に説明する。
【００４９】
図２０に示すように、本実施の形態における識別情報抽出部１０３は、識別情報認識領域切り出し部２００１、文字認識部２００２から構成される。
【００５０】
まず、識別情報認識領域切り出し部２００１の機能について説明する。識別情報認識領域切り出し部２００１には、ドキュメントデータＤ（文字画像が含まれるデータ）が入力され、ドキュメントデータＤ中から後段の文字認識処理の対象となる領域の切り出しを行い、切り出された領域データＲが出力される。
【００５１】
次に、文字認識部２００２の機能について説明する。文字認識部２００２には、前記識別情報認識領域切り出し部２００１において切り出された領域データＲを入力し、その領域データＲに対し、文字認識処理を実行し、文字認識処理された結果Ｉｎｆ１を出力する。
【００５２】
以上説明した識別情報抽出部１０３は、文字認識すべき領域が一つの場合の処理である。文字認識すべき領域が複数ある場合には、複数回文字認識を行い、更に、対象文字が異なる場合には、それに最適な文字認識手法に切り替えて、識別情報を取り出す。以上説明した処理によって抽出された情報が、識別情報Ｉｎｆ１として出力される。出力された識別情報Ｉｎｆ１は、一旦ＲＡＭ３０５に保持される。
【００５３】
尚、本実施形態において識別情報抽出部１０３で実行される処理は、上記識別情報抽出処理に限定されることはなく種々の処理が適用可能である。
【００５４】
例えば、ユーザーに対話的に識別情報を選択させる方法として、ドキュメントデータＤをモニタ３０２などに表示し、ユーザーがマウス３１１やキーボード２１２を用いてドキュメントデータＤ中の所望の情報を指定し、指定された位置の情報を抽出することにより識別情報Ｉｎｆ１を抽出可能である。
【００５５】
また、ドキュメントデータＤが領収書や契約書などの場合、予めフォーマットが定められており、金額や契約者などの被署名データの位置がわかっていることが多い。このような場合に、予め判っている被署名データの位置の情報を領域データＲとして用いるようにしても良い。
【００５６】
また、以上説明したような領域データＲは、後で署名を検証する際に必要となるために、後述する検証処理と共通でなければならない。これは、署名処理部と検証処理部において予め共有しておいたり、署名処理部から検証処理部に対してネットワークを通じて送信したりするようにすればよい。また、ドキュメントデータＤが予め定められたフォーマットである場合、このフォーマットを表す情報を送信するようにしても良い。更に、フォーマットを表す情報を前記ドキュメントデータＤに可視、或いは不可視の方法で付加しても良い。
【００５７】
また、抽出された識別情報Ｉｎｆ１は、識別情報Ｉｎｆ１が容易に悪用されない様に暗号

化されても良い。且つ／または、識別情報Ｉｎｆ１は、識別情報Ｉｎｆ１が後述する電子透かしとして埋め込まれた画像データＩ２に対して、悪意を持った人間により、画像データＩ２から抽出できない様に内容変更（以下攻撃と呼ぶ）が施された場合にも、正しくその情報を抽出できる様に、誤り訂正符号化が施されても良い。こうして出力された識別情報Ｉｎｆ１は、一旦ＲＡＭ３０５に保持される。

【００５８】

次に、付加情報埋め込み部１０４の機能について説明する。前記画像発生部１０１において発生した画像データＩ１、及び前記識別情報抽出部１０３において抽出された識別情報Ｉｎｆ１はＲＡＭ３０５に一旦格納さている。付加情報埋め込み部１０４は、このＲＡＭ３０５からそれぞれのデータを入力し、入力識別情報Ｉｎｆ１が、付加情報として画像データＩ１に電子透かしとして埋め込み、その埋め込まれた画像データＩ２を出力する。電子透かしの埋め込み方法の詳細については後述する。付加情報Ｉｎｆ１が埋め込まれた画像データＩ２は、一旦ＲＡＭ３０５に保持される。

【００５９】

次に、合成部１０５の機能について説明する。合成部１０５には、前記ドキュメントデータ発生部１０２において発生したドキュメントデータＤ、及び前記付加情報埋め込み部１０４において付加情報Ｉｎｆ１が埋め込まれた画像データＩ２を、ＲＡＭ３０５から入力し、入力されたドキュメントデータＤと画像データＩ２が合成し、合成されたデータＩ３を出力する。

【００６０】

ここで、合成部１０５において実行される処理の例を図４を用いて説明する。同図において、４０１は合成部１０５に入力された画像データＩ２（付加情報埋め込み後のデータ）、４０２は合成部１０５に入力されたドキュメントデータＤ，４０３は合成部１０５において前記画像データ４０１とドキュメントデータ４０２が合成された画像データＩ３である。

【００６１】

図４に示すように、画像データＩ２はドキュメントデータＤの背景としてドキュメントデータＤの上に重ねられるように合成される。以上のように合成された画像データＩ３は、一旦ＲＡＭ３０５に保持される。

【００６２】

次に、ドキュメントデータ出力部１０６の機能について説明する。ドキュメントデータ出力部１０６には、前記合成部１０５において合成された画像データＩ３をＲＡＭ０３０５から入力し、入力された画像データＩ３を出力する。

【００６３】

ここで、画像データＩ３を出力する手段としては、図３におけるＲＡＭ３０５，ＨＤ３０６，ＣＤ３０８（ＣＤＲやＣＤＲＷの場合），ＦＤ３０９，ＤＶＤ３１０（ＤＶＤ－ＲＡＭやＤＶＤ－Ｒ等の場合）などに記録することや、モデム３１３、ＮＩＣ３１５などを用いてネットワークを通じて送信することや、プリンター１１７などを用いて紙に印刷することなど種々の手段を含む。

【００６４】

以上、本実施の形態における署名処理部の動作について説明した。

【００６５】

[検証処理部]

次に、図２を用いて本実施の形態に適用される検証処理部（機能）を説明する。

【００６６】

図２に示すように、本実施の形態における検証処理部は、ドキュメントデータ発生部２０１、識別情報抽出部２０２、付加情報抽出部２０３、及び検証部２０４から構成される。

【００６７】

尚、個々で説明する検証処理はソフトウェア処理により実現されても良い。その場合には、上記各部は上記処理に必要な機能を概念的なものとして備えたものとして考慮されるべ

きものである。説明を簡単なものとするため、検証する側の装置構成も図３に則って説明するが、別装置であっても構わないのは勿論である。

【００６８】

まず、ドキュメントデータ発生部２０１の機能について説明する。ドキュメントデータ発生部２０１では、検証対象となるドキュメントデータＩ４が発生する。発生したドキュメントデータＩ４は識別情報抽出部２０２に供給される。ここで、ドキュメントデータ発生部２０１でドキュメントデータＩ４を発生させる手段としては、前述した図１における画像発生部１０１における手段と同様の手段を用いることが可能であるので詳細な説明は省略する。尚、ドキュメントデータ発生部２０１が発生するドキュメントデータＩ４は、望ましくは図１におけるドキュメントデータ出力部１０６から出力されたドキュメントデータＩ３である。或いは、ドキュメントデータＩ３がコピー機などによりコピーされたものがドキュメントデータＩ４として入力されてもよい。また、本実施の形態における署名処理部において署名処理されたドキュメントデータではないものが入力されてもよい。本実施の形態における検証処理部の目的は、これらを識別することが可能な方法を提供することである。ドキュメントデータ発生部２０１において発生したドキュメントデータＩ４は一旦ＲＡＭ３０５に保持される。

【００６９】

次に、識別情報抽出部２０２の機能について説明する。前記ドキュメントデータ発生部２０１から出力されたドキュメントデータＩ４はＲＡＭ０３０５に保持されているので、識別情報抽出部２０２は、そのデータを入力する。そして、入力されたドキュメントデータＩ４の所定の位置の識別情報を抽出し、抽出された識別情報Ｉｎｆ２を出力する。

【００７０】

ここで、識別情報抽出処理の対象となる所定の位置とは、前述した図１における識別情報抽出部１０３において識別情報が抽出された位置と等しくなければならない。この位置に関する情報は、署名処理部と検証処理部において予め共有しておくことや、署名処理部から検証処理部に対してネットワークを通じて送信することなどによって等しく設定することが可能である。また、ドキュメントデータＤが予め決められたフォーマットである場合、このフォーマットを表す情報を前述した署名処理部から受信し、位置に関する情報を決めても良い。更に、ドキュメントデータＤに可視、或いは不可視の方法で付加してあるフォーマットを表す情報を抽出して、位置に関する情報を決めても良い。

【００７１】

尚、識別情報抽出部２０２で実行される処理は、図１における識別情報抽出部１０３で実行される処理と同様であるため詳細な説明は省略する。抽出された識別情報Ｉｎｆ２は、一旦ＲＡＭ３０５に保持される。

【００７２】

次に、付加情報抽出部２０３の機能について説明する。付加情報抽出部２０３は、前記ドキュメントデータ発生部２０１からＲＡＭ３０５に出力されたドキュメントデータデータＩ４を入力する。そして、入力されたドキュメントデータＩ４から電子透かしとして埋め込まれている付加情報Ｉｎｆ３を抽出し、抽出された付加情報Ｉｎｆ３を出力する。電子透かしの抽出方法の詳細については後述する。

【００７３】

ここで、抽出した付加情報Ｉｎｆ３が誤り訂正符号化されている場合には誤り訂正復号処理を、また暗号化されている場合には暗号復号処理を実行するようにする。抽出された付加情報Ｉｎｆ３は、一旦ＲＡＭ３０５に保持される。

【００７４】

次に、検証部２０４の機能について説明する。検証部２０４は、前記識別情報抽出部２０２において抽出された識別情報Ｉｎｆ２、及び前記付加情報抽出手段２０３において抽出された付加情報Ｉｎｆ３をＲＡＭ３０５から入力し、入力した識別情報Ｉｎｆ２と付加情報Ｉｎｆ３を比較することにより検証処理を行う。

【００７５】

ここで、検証処理とは、入力された識別情報Ｉｎｆ２と付加情報Ｉｎｆ３を比較し、両者が等しい場合には「改ざんされていない」と判断し、両者が異なる場合には「改ざんされている」と判断する処理である。また、「改ざんされている」と判断された場合には、識別情報Ｉｎｆ２中のどの位置が異なっているかを通知することも可能である。更に、以上のような検証処理の結果は、改ざんされている識別情報Ｉｎｆ２の位置を示すために、画像データとしてモニタ１０２上に表示することも可能である。

【００７６】

ここで、検証部２０４において実行される検証処理の一例を図５を用いて説明する。図５において、５０１は改ざんされていない場合の処理の流れの例、５０２は改ざんされている場合の処理の流れの例を示している。処理例５０２中の５０３は改ざんされている位置を示す画像データの例を示している。

【００７７】

５０１において、識別情報Ｉｎｆ２「￥４０，０００」と付加情報Ｉｎｆ３「￥４０，０００」は等しいことから「改ざんされていない」と判断する。一方で、５０２においては、識別情報Ｉｎｆ２「￥６０，０００」と付加情報Ｉｎｆ３「￥４０，０００」は異なることから「改ざんされている」と判断する。更に、「改ざんされている」と判断された場合には、改ざんされている位置を目視しやすい様に、枠を付けたり、網掛けなどの処理を施した画像データを生成し、モニタ３０２などに表示することにより、ユーザーに改ざんされている位置５０３を明示することが可能である。

【００７８】

以上、本実施の形態における検証処理部について説明した。

【００７９】

[電子透かし埋め込み]

以下、図６を用いて本発明に適用される電子透かしの埋め込み処理部（機能）を説明する。

【００８０】

まず、以下で説明する電子透かし（デジタルウォーターマーク）とは、“不可視の”電子透かしとも呼ばれ、人間の視覚では殆ど認識できないレベルの変化を、オリジナル画像データＩに対して付加させることである。そして、この各変化量の１つ或いはその組み合わせが何らかの付加情報を表している。

【００８１】

図６に示すように、本実施形態における埋め込み処理部（付加情報埋め込み部１０４に相当する）は、画像入力部６０１、埋め込み情報入力部６０２、鍵情報入力部６０３、電子透かし生成部６０４、電子透かし埋め込み部６０５、画像出力部６０６から構成される。

【００８２】

なお、ここで説明する埋め込み処理はソフトウェア処理により実現されても良い。その場合には、上記各部は上記処理に必要な機能を概念的なものとして捉えたものと考慮されるべきものである。

【００８３】

まず、画像入力部６０１の機能について説明する。画像入力部６０１には電子透かしの埋め込み対象となる画像を表す画像データＩが入力される。その画像データＩは画像入力部６０１から出力され、電子透かし埋め込み部６０５に入力される。

【００８４】

以降の説明では、説明を簡単にするために、画像データＩはモノクロの多値画像を表現しているものとするが、本発明はこのような場合には限定されない。例えばカラー画像データ等の複数の色成分からなる画像データに対して電子透かしを埋め込むならば、その複数の色成分である例えばＲＧＢ成分、或いは輝度、色差成分の夫々を上記モノクロの多値画像として扱う様にし、各成分に対して電子透かしを埋め込めばよい。この場合には、モノクロ多値画像へ電子透かしを埋め込む場合と比較して、約３倍のデータ量を埋め込むことが可能となる。

【００８５】
次に、埋め込み情報入力部６０２の機能について説明する。埋め込み情報入力部６０２には、上記画像データＩに電子透かしとして埋め込むべきバイナリデータ列が入力される。そのバイナリデータ列は埋め込み情報入力部６０２から出力され、電子透かし生成部６０４に入力される。
【００８６】
以下、上記バイナリデータ列を付加情報Ｉｎｆとして説明する。付加情報Ｉｎｆは“０”または“１”の何れかを表すビットの数個の組み合わせによって構成される情報である。
【００８７】
なお、上記付加情報Ｉｎｆは、その付加情報Ｉｎｆが容易に悪用されない様に暗号化されていても良い。かつ／または、上記付加情報Ｉｎｆは、この付加情報Ｉｎｆが電子透かしとして埋め込まれた画像データＩに対して、悪意を持った人間により、付加情報Ｉｎｆが画像データＩから抽出できない様に内容変更（以下攻撃と呼ぶ）が施された場合にも、正しくその付加情報Ｉｎｆを抽出できる様に、誤り訂正符号化が施されても良い。
【００８８】
なお上記攻撃には故意によらない攻撃も有る。例えば、一般的な画像処理（非可逆圧縮、輝度補正、幾何変換、フィルタリングなど）が、結果として電子透かしを除去してしまうことも有り、この場合も攻撃であると言える。
【００８９】
なお上記暗号化、及び誤り訂正符号化などの処理の詳細は公知であるので、本実施形態でのこれ以上の詳しい説明は省略する。以降では、ｎビットで表現される付加情報を埋め込む例について詳しく説明する。
【００９０】
次に、鍵情報入力部６０３の機能について説明する。鍵情報入力部６０３は、付加情報Ｉｎｆの埋め込み、及び抽出に必要な鍵情報ｋを入力し、それを出力する。鍵情報入力部６０３から出力された鍵情報ｋは、電子透かし生成部６０４に入力される。
【００９１】
ここで鍵情報ｋとはＬ（正数）ビットで表される実数である。Ｌ＝８の正数として表現する場合には、例えば“０１０１０１０１”が鍵情報ｋの一例であり、正の整数として表現する場合には“８５（１０進数）”として与えられる。鍵情報ｋは、後述する擬似乱数発生部７０２で実行される擬似乱数発生処理に初期値として与えられる。電子透かし埋め込み処理部、及び後述する電子透かし抽出処理部において共通の鍵情報ｋを使用した場合に限り、電子透かしとして埋め込まれている付加情報Ｉｎｆを正しく抽出することが可能である。即ち、鍵情報ｋを所有している利用者だけが付加情報Ｉｎｆを正しく抽出することができる。
【００９２】
次に、電子透かし生成部６０４の機能について説明する。電子透かし生成部６０４は、埋め込み情報入力部６０２から付加情報Ｉｎｆ、及び鍵情報入力部６０３から鍵情報ｋを入力し、入力された付加情報Ｉｎｆと鍵情報ｋに基づいて電子透かしｗが生成し、出力する。
【００９３】
電子透かし生成部６０４の機能の詳細について図７を用いて説明する。図７に示すように、電子透かし生成部６０４は基本行列生成部７０１、擬似乱数発生部７０２、及び擬似乱数割り当て部７０３から構成される。
【００９４】
まずはじめに基本行列生成部７０１の機能について説明する。基本行列生成部７０１では、基本行列ｍが生成される。生成された基本行列ｍは擬似乱数割り当て部７０３に供給される。ここで基本行列ｍとは付加情報Ｉｎｆを構成する各ビットの位置と、前記各ビットが埋め込まれる画像データＩ上の画素位置を対応付けるために用いられる行列である。
【００９５】

ここでは、基本行列生成部７０１は複数の基本行列を選択的に利用することが可能である。そしてどの基本行列を用いるかは、その時の目的／状況に応じて変化させる必要が有り、本発明ではこれら基本行列の切り替えにより最適な電子透かし（付加情報Ｉｎｆ）の埋めこみが可能である。

【００９６】

基本行列ｍの具体例を図８に示す。８０１は１６ビットから構成される付加情報Ｉｎｆを埋め込む場合に用いられる基本行列ｍの一例を示したものである。８０１に示す様に１６ビットの付加情報Ｉｎｆを埋め込むために、例えば４ｘ４の基本行列ｍが用いられ、更に１から１６の数字が基本行列内の各要素に割り当てられている。

【００９７】

図から分かる様に、基本行列ｍ内の要素の値と付加情報Ｉｎｆのビット位置が対応付けられている。具体的には、基本行列内の要素の値が“１”の位置に付加情報Ｉｎｆの最上位ビットを埋め込み、同様に、基本行列内の要素の値が“２”の位置に付加情報Ｉｎｆの最上位ビットの次のビットを埋め込む。以下、順番に各ビットを埋め込む。

【００９８】

以下は、上記８０１からの埋めこみ方法の変形例について説明する。

【００９９】

図８の８０２は８ビットから構成される付加情報Ｉｎｆを埋め込む場合に用いられる基本行列の一例を示したものである。８０２に示す基本行列は、８０１に示す基本行列の全要素のうち１から８までの値を持つ要素だけを用いたものである。値を持たない要素の部分には付加情報Ｉｎｆを埋め込まない。上記８０２の様に付加情報Ｉｎｆを表す各ビットの埋めこみ位置を散らすことにより、８０１よりも、電子透かし（付加情報Ｉｎｆ）の埋めこみによる画像の変化（画質劣化）を認識しずらくできる。

【０１００】

図８の８０３は８０２と同様に８ビットから構成される付加情報Ｉｎｆを埋め込む場合に用いられる基本行列ｍの一例を示したものである。上記８０２と８０３は夫々８ビットの付加情報Ｉｎｆを埋め込むことが可能な基本行列ｍであるが、８０２は全画素の５０％にあたる画素を付加情報Ｉｎｆの埋め込みに用いているのに対して、８０３は全画素（１００％）を付加情報Ｉｎｆの埋め込みに用いている。即ち、１ビット埋め込むために８０２は基本行列中の１画素を用いているのに対して、８０３では基本行列中の２画素を用いて付加情報Ｉｎｆの１ビットを埋め込んでいる。上記８０３の様に、付加情報Ｉｎｆを表す各ビットを埋めこむ回数を増やすことにより、電子透かしが埋め込まれた画像に攻撃が加えられた場合には、８０１や８０２よりも、その電子透かし（付加情報Ｉｎｆ）を確実に抽出できる（攻撃耐性が有る）ことになる。

【０１０１】

ここで、全画素中で電子透かしの埋め込みのために使用する画素の割合を、以降では充填率と呼ぶことにする。前記８０１を用いた場合充填率は１００％、前記８０２を用いた場合は充填率５０％、前記８０３を用いた場合は充填率１００％である。

【０１０２】

図８の８０４は、８０３と同様に全画素を付加情報Ｉｎｆの埋め込みに用いている。即ち、充填率は１００％である。しかしながら、８０３は８ビットの付加情報Ｉｎｆを埋め込むのに対して、８０４は４ビットの付加情報Ｉｎｆしか埋め込まない。しかし、１ビット埋め込むために８０３では基本行列中の２画素を用いているのに対して、８０４では基本行列中の４画素を用いて付加情報Ｉｎｆの１ビットを埋め込んでいる。上記８０４の様に、付加情報Ｉｎｆを表す各ビットを埋めこむ回数を増やすことにより、電子透かしが埋め込まれた画像に攻撃が加えられた場合には、８０１や８０２や８０３よりも、その電子透かし（付加情報Ｉｎｆ）を確実に抽出できる（攻撃耐性が有る）ことになる。ただし、攻撃耐性が非常に有る代わりに、埋め込む付加情報Ｉｎｆの情報量は４ビットとなり、８０１や８０２や８０３よりも少ない。

【０１０３】

上述した４つの例を表にまとめると次のようになる。

【０１０４】

＜表１＞

基本行列	充填率	使用画素数／１ビット	埋め込み可能な情報量
８０１	１００％	１画素	１６ビット
８０２	５０％	１画素	８ビット
８０３	１００％	２画素	８ビット
８０４	１００％	４画素	４ビット

このように、基本行列ｍをどのような構成にするかによって、充填率と１ビットを埋め込むのに使用する画素数と埋め込み可能な情報量を選択的に設定することができる。上記表１では、充填率は主に電子透かしを埋め込んだ画像の画質に影響するパラメータであり、１ビットを埋め込むために使用する画素数は主に攻撃に対する耐性に影響するパラメータである。充填率を大きくすると電子透かしを埋め込んだ画像の質の劣化は大きくなり、１ビット埋め込むために使用する画素数を多くすると攻撃に対する耐性は強くなる。

【０１０５】

以上から分かる様に、電子透かしを実現する際には、埋めこみ対象の画質と電子透かしの攻撃に対する耐性と埋め込める付加情報Ｉｎｆの情報量がトレードオフの関係にある。

【０１０６】

本実施形態においては、上述した複数種類の基本行列ｍを適応的に選択することによって、電子透かしの耐性と画質と情報量を制御、及び設定することが可能である。

【０１０７】

以上説明したように生成された基本行列ｍは擬似乱数割り当て部７０３に出力される。

【０１０８】

次に、擬似乱数発生部７０２の機能について説明する。擬似乱数発生部７０２では、鍵情報ｋが入力され、鍵情報ｋを元に擬似乱数列ｒが生成される。生成された擬似乱数列ｒが出力され、擬似乱数割り当て部７０３に入力される。ここで擬似乱数列ｒとは、｛－１，１｝の範囲に含まれる一様分布に従う実数列（複数の実数）である。更に、鍵情報ｋは擬似乱数を発生させる場合の初期値として用いる。即ち、第１の鍵情報を用いて生成した第１の擬似乱数列と、前記第１の鍵情報とは異なる第２の鍵情報を用いて生成した第２の擬似乱数列は異なる。擬似乱数列ｒを生成する方法は公知の技術であるので詳細な説明は省略する。生成された擬似乱数列ｒは擬似乱数割り当て部７０３に出力される。

【０１０９】

次に、擬似乱数割り当て部７０３の機能について説明する。擬似乱数割り当て部７０３には基本行列ｍと擬似乱数列ｒが入力され、擬似乱数列ｒの各要素が基本行列ｍの所定の要素に割り当てられる。以降では、基本行列ｍの所定の要素に乱数列が割り当てられた行列を電子透かしｗと呼ぶ。擬似乱数割り当て部７０３からは生成された電子透かしｗが出力される。

【０１１０】

ここで、擬似乱数列ｒの各要素を基本行列ｍの所定の要素に割り当てる処理の詳細について例を用いて説明する。

【０１１１】

まず、例として図８に示した基本行列８０４を用いる場合を説明する。前述したように基本行列８０４を用いることにより４ビットの情報を埋め込み可能である。

【０１１２】

まずはじめに、基本行列８０４に示す基本行列内の各要素のうち、値として“１”を持つ要素をラスタースキャン順にスキャンして、順に擬似乱数列ｒの各要素を割り当てる。割り当てる際には、付加情報Ｉｎｆに応じて付加情報Ｉｎｆのビットが“１”の時は擬似乱

数列ｒの要素をそのまま割り当て、一方で付加情報Ｉｎｆのビットが“０”の時は擬似乱数列ｒの要素に“－１”をかけた値を割り当てる。

【０１１３】

次に、値として“２”をもつ要素において同様の処理を実行する。以上の処理を、値としてｎ（埋め込みビット数）を持つ要素までに対して実行する。以上の示した例によって生成された電子透かしｗの一例を図９に示す。同図の９０１は擬似乱数列ｒとしてｒ＝｛０．７，－０．６、－０．９，０．８…｝という実数列、付加情報Ｉｎｆとして“１００１”という４ビットの情報を用いた場合の例である。

【０１１４】

詳しく説明すると、次のようになる。ただし、スキャン順は、左端から右端スキャンすることを、１行目、２行目と順に行うものとする。

【０１１５】

付加情報Ｉｎｆの最上位ビットは“１”であり、対応する乱数の最初の値は０．７である。従って、基本行列８０４をスキャンした際に最初に検出された“１”の位置には先頭の擬似乱数“０．７”が割り当てられる。そして、次に検出された“１”の位置には、２番目の擬似乱数“－０．６”が割り当てられる。以下、同様に、基本行列の“１”を検出する毎に、対応する順番の擬似乱数を割り当てる。

【０１１６】

次に、付加情報Ｉｎｆの最上位ビットの次のビット“０”を埋め込む場合には、擬似乱数に対して－１を乗算した値を割振る。すなわち、上記の場合には｛－０．７，０．６，０．９，－０．８…｝と、符号を反転させた擬似乱数を、基本行列の“２”を検出する毎に割り当てる。

【０１１７】

以下、付加情報Ｉｎｆの３ビット目、４ビット目についても同様に行うことで、図９の９０１に示す電子透かしｗを得ることができる。

【０１１８】

こうして生成された電子透かしｗは電子透かし生成部６０４の出力として出力され、電子透かし埋め込み部６０５に入力される。

【０１１９】

尚、以上では説明のために１６ビット、８ビット及び４ビットの付加情報を埋め込むために４ｘ４の基本行列を用いたが、本実施形態ではこれに限らず、１ビット埋め込むために更に多くの画素を利用し、より大きなサイズの基本行列を用いる場合も本発明の範疇に含む。より大きなサイズの基本行列を用いた場合には、擬似乱数列もより長い実数列を用いることになる。実際には、説明に用いたような４要素から構成される乱数列では、後述する電子透かし抽出処理が正しく動作しない可能性がある。（具体的には、付加情報Ｉｎｆが埋め込まれているにも関わらず、集積画像ｃと電子透かしｗ１、ｗ２、…、ｗｎとの相関係数が小さくなる可能性がある。）よって、例えば６４ビットの付加情報を埋め込むために充填率５０％において２５６ｘ２５６の基本行列を用いるような構成とすることも可能である（この場合、１ビット埋め込むために５１２画素使用することになる）。

【０１２０】

次に、電子透かし埋め込み部６０５の機能について説明する。電子透かし埋め込み部６０５では、画像データＩ及び電子透かしｗが入力され、画像データＩに電子透かしｗが埋め込まれ、電子透かしｗが埋め込まれた画像データＩ'が出力される。

【０１２１】

電子透かし埋め込み部６０５の処理の詳細について説明する。電子透かし埋め込み部６０５では、

$$I'_{i,j} = I_{i,j} + a w_{i,j} \quad （式１）$$

という式に従って、電子透かしの埋め込み処理が実行される。ここで、$I'_{i,j}$は電子透かしが埋め込まれた画像データ、$I_{i,j}$は電子透かしが埋め込まれる前の画像データ、$w_{i,j}$は電子透かし、ｉ及びｊは夫々Ｉ、Ｉ'及びｗのｘ座標及びｙ座標を表すパラメータ、ａは

電子透かしの強度を設定するパラメータである。

【０１２２】

例えば、ａを“１０”とすると、埋め込む電子透かしの値は－１０乃至＋１０の範囲となる。ａの値を大きく設定することによって耐性の強い電子透かしを埋め込むことが可能であるが、画質劣化が大きくなる。一方で、ａの値を小さく設定することによって電子透かしの耐性は弱くなるが、画質劣化は小さくすることが可能である。前述した基本行列ｍの構成と同様に、ａの値を適当に設定することにより（例えば、埋め込む際に、ＧＵＩ画面等でマウスやキーボードでもってａの値を設定する等）、電子透かしの攻撃に対する耐性と電子透かしを埋め込んだ後の画像の画質のバランスを設定することが可能である。

【０１２３】

式１に示した電子透かし埋め込み処理の具体例として、４×４の基本行列ｍを用いた場合の例を図１０に示す。図１０において１００１は式１におけるＩ'、１００２はＩ、１００３はｗを表す。図１０に示すように、式１の演算は行列内の各要素に対して実行される。

【０１２４】

以上、式１（図１０）に示した演算処理は実際には入力された画像データＩの全体に対して繰り返し実行される。例えば、入力された画像データIが２４ｘ２４画素から構成されている場合には、図１１に示す如く４×４画素が縦横とも６×６個備えることになり、各ブロック（４×４画素）に埋め込みが行われる。

【０１２５】

図１１に示すように、入力された画像データＩは４×４画素から構成される互いに重ならないブロックに分割され、分割された夫々のブロックに対して式１（図１０）に示した演算処理が繰り返し実行される。このように式１（図１０）に示した処理が実行されるブロックを、以下マクロブロックと呼ぶ。

【０１２６】

全てのマクロブロックに対して繰り返し電子透かしの埋め込み処理を実行することにより、結果的に画像全体に電子透かしを埋め込むことが可能である。更に、１つのマクロブロックにはｎビットから構成される付加情報Ｉｎｆの全体が埋め込まれている。このことから、少なくともマクロブロックが１つあれば埋め込んだ付加情報Ｉｎｆを抽出することができる。即ち、埋め込んだ付加情報Ｉｎｆを抽出するために画像データＩの全体を必要とはせず、画像データＩの一部（少なくともひとつのマクロブロック）があれば十分である。

【０１２７】

このように画像データＩの一部から電子透かしを完全に抽出可能であることを「切り取り耐性がある」と呼ぶ。マクロブロック単位の電子透かし埋め込み処理を画像全体に繰り返し実行することにより、電子透かしに切り取り耐性を持たせることが可能である。こうして生成された電子透かし埋め込み済み画像Ｉ'は、画像出力部６０６を通じて、電子透かしの埋め込み処理部の最終的な出力として出力される。

【０１２８】

[電子透かし抽出処理部]

次に、以上で述べた電子透かしの埋め込み処理部によって埋め込まれた電子透かしを抽出する方法について説明する。以下、図１２を用いて本実施形態に適用される電子透かしの抽出処理部（機能）を説明する。

【０１２９】

図１２に示すように、実施形態における抽出処理部は、画像入力部１２０１、鍵情報入力部１２０２、抽出パターン生成部１２０３、電子透かし抽出部１２０４、電子透かし出力部１２０５から構成される。

【０１３０】

なお、ここで説明する抽出処理はソフトウェア処理により実現されても良い。その場合には、上記各部は上記処理に必要な機能を概念的なものとして捉えたものと考慮されるべき

ものである。
【０１３１】
まず、画像入力部１２０１の機能について説明する。画像入力部１２０１には電子透かしが埋め込まれている可能性がある画像データＩ''が入力され、その出力は電子透かし抽出部１２０４に入力される。ここで、画像入力部１２０１の動作は前述した画像入力部６０１と同様であるので詳細な動作の説明は省略する。尚、画像入力部１２０１によって入力される画像データＩ''は、前述した電子透かしの埋め込み処理部によって電子透かしが埋め込まれた画像データ（Ｉ'）に限定されることはない。もちろん、電子透かしが埋め込まれた画像データＩ'であってもよいし、画像データＩ'が攻撃された画像であっても良い。更に、電子透かしが埋め込まれていない画像データＩであっても良い。
【０１３２】
次に、鍵情報入力部１２０２の機能について説明する。鍵情報入力部１２０２において電子透かしを抽出するための鍵情報ｋが入力され、その出力は抽出パターン生成部１２０３に入力される。ここで、入力される鍵情報ｋは、前述した電子透かしの埋め込み処理部における鍵情報入力部６０３によって入力されたものと同一のものでなければならない。異なる鍵情報が入力された場合には正しく付加情報を抽出することは出来ない。即ち、正しい鍵情報ｋを有する利用者だけが正しい付加情報Ｉｎｆ'を抽出することが可能である。
【０１３３】
次に、抽出パターン生成部１２０３の機能について説明する。抽出パターン生成部１２０３には鍵情報生成部１２０２から鍵情報ｋが入力され、入力された鍵情報ｋに基づいて抽出パターンが生成され、生成された抽出パターンが出力される。
【０１３４】
抽出パターン生成部１２０３の処理の機能の詳細について図１３を用いて説明する。図１３に示すように、抽出パターン生成部１２０３は基本行列生成部１３０１、擬似乱数発生部１３０２、及び擬似乱数割り当て部１３０３から構成される。
【０１３５】
ここで、基本行列生成部１３０１は前述した基本行列生成部７０１と、更に擬似乱数発生部１３０２は擬似乱数発生部７０２と同じ動作であるので詳細な説明は省略する。但し、基本行列生成部１３０１において生成される基本行列と基本行列生成部７０１において生成される基本行列は同一のものでなければ正しく付加情報を抽出することはできない。
【０１３６】
次に、擬似乱数割り当て部１３０３の機能の詳細について説明する。擬似乱数割り当て部１３０３には基本行列ｍと擬似乱数列ｒが入力され、擬似乱数列ｒの各要素が基本行列ｍの所定の要素に割り当てられる。ここで、前述した埋め込み処理部で用いられた擬似乱数割り当て部７０３との違いは、擬似乱数割り当て部７０３においては出力される抽出パターンｗは一つであったのに対して、擬似乱数割り当て部１３０３からは埋め込み情報量の数（本実施形態では、ｎ個）だけ出力されることである。
【０１３７】
ここで、擬似乱数列ｒの各要素を基本行列ｍの所定の要素に割り当てる機能の詳細について例を用いて説明する。例として図８に示した基本行列８０４を用いる例を説明する。基本行列８０４を用いた場合、４ビットの付加情報を埋め込み可能であるので、即ち４個の抽出パターンｗ１、ｗ２、ｗ３、ｗ４が出力される。
【０１３８】
まずはじめに、基本行列８０４の各要素のうち、値として“１”を持つ要素をラスタースキャン順にスキャンして、順に擬似乱数列ｒの各要素を割り当てる。基本行列８０４の各要素のうち、値として“１”を持つ要素全てに擬似乱数列ｒの各要素の割り当てが終了したら、擬似乱数列ｒを割り当てた行列を抽出パターンｗ１として生成する。図１４に抽出パターンの例を示す。抽出パターンｗ１（１４０１）は擬似乱数列ｒとしてｒ＝｛０．７，－０．６、－０．９，０．８｝という実数列を用いた場合の例である。
【０１３９】

以上の処理を、基本行列８０４の各要素のうち、値として“２”、“３”、“”，“４”を持つ要素全てに対して実行し、夫々抽出パターンｗ２（１４０２）、抽出パターンｗ３（１４０３）、抽出パターンｗ４（１４０４）として生成する。こうして生成された抽出パターンｗ１、ｗ２、ｗ３、ｗ４は全てあわせると、電子透かしの埋め込み処理部で用いられた電子透かしｗに等しくなる。生成された抽出パターンｗ１、ｗ２、ｗ３、ｗ４が抽出パターン生成部１２０３から出力され、電子透かし抽出部１２０４に入力される。

【０１４０】

次に、電子透かし抽出部１２０４の機能について説明する。電子透かし抽出部１２０４では、画像データＩ'及び抽出パターンｗ１、ｗ２、…、ｗｎが入力され、抽出パターンｗ１、ｗ２、…、ｗｎを用いて画像データＩ'から付加情報Ｉｎｆ'が抽出され、抽出された付加情報Ｉｎｆ'が出力される。ここで、望ましくは抽出された付加情報Ｉｎｆ'は埋め込んだ付加情報Ｉｎｆに等しい。しかしながら、電子透かしを埋め込んだ画像データＩ'が種々の攻撃を受けている場合には必ずしも付加情報Ｉｎｆと付加情報Ｉｎｆ'は一致しない。

【０１４１】

電子透かし抽出部１２０４の機能の詳細について説明する。電子透かし抽出部１２０４では、入力された画像データＩ'から生成された集積画像ｃと抽出パターンｗ１、ｗ２、…、ｗｎとの相互相関が夫々計算される。ここで、集積画像ｃとは、入力された画像データＩ''をマクロブロックの大きさ（基本行列の大きさ）の互いに重ならないブロックに分割し、分割された夫々のブロックの要素の値の平均値を算出した画像である。

【０１４２】

集積画像ｃについて図１５に示した具体例を用いて説明する。図１５は４×４画素の抽出パターンと２４ｘ２４画素の画像Ｉ''が入力された場合の集積画像ｃの例である。図１５において、１５０１は２４×２４画素の画像データＩ'が４×４画素の互いに重ならないブロックに分割された例を示す。図１５に示す例の場合、３６個のブロックに分割されている。この３６個のブロックの各要素の値の平均値を求めたものが集積画像ｃ（１５０２）である。

【０１４３】

こうして生成された集積画像ｃと抽出パターンｗ１、ｗ２、…、ｗｎとの相互相関が各々計算される。相関係数を計算する具体的な方法について、集積画像ｃと抽出パターンｗｎの相関係数を計算する場合の例を用いて説明する。

【０１４４】

相関係数は、集積画像ｃと抽出パターンｗｎの類似度を測定する統計量であり、

ρ＝ｃ'Ｔ・ｗ'ｎ／｛｜ｃ'Ｔ｜・｜ｗ'ｎ｜｝　　（式２）

と表される。ここで、ｃ'及びｗｎ'は夫々各要素から、夫々の行列の要素の平均値を引いた値を要素とする行列であり、ｃＴはｃの転置行列である。ρは－１から＋１の値の範囲の値をとる。集積画像ｃと抽出パターンｗｎが正の相関が強い時にρは＋１に近づき、一方で集積画像ｃと抽出パターンｗｎが負の相関が強い時にρは－１に近づく。ここで「正の相関が強い」とは、「集積画像ｃが大きいほど抽出パターンｗｎが大きくなる」という関係のことであり、「負の相関が強い」とは「集積画像ｃが大きいほど抽出パターンｗｎが小さくなる」という関係のことである。また、集積画像ｃと抽出パターンｗｎが無相関の時には、ρは０となる。

【０１４５】

こうして算出した相互相関の結果によって、入力された画像データＩ''に付加情報Ｉｎｆ'が電子透かしとして埋め込まれているか否か、更に、埋め込まれている場合には付加情報Ｉｎｆ'を構成する各ビットが“１”であるか“０”であるかを判定する。

【０１４６】

集積画像ｃと抽出パターンｗ１、ｗ２、…、ｗｎとの相関係数を夫々算出し、算出された相互相関の結果が０に近い場合には「付加情報が埋め込まれていない」、相互相関の結果が０から離れた正数の場合には「ビット１」、相互相関の結果が０から離れた負数の場合

には「ビット０」であると夫々判断する。

【０１４７】

以上説明した相互相関を求めることは、集積画像ｃと抽出パターンｗ１、ｗ２、…、ｗｎの夫々が、どれくらい類似しているかを評価することに等しい。即ち、前述した電子透かしの埋め込み処理部によって、画像データＩ''（集積画像ｃ）の中に抽出パターンｗ１、ｗ２、…、ｗｎが埋め込まれている場合には、これらは比較的類似しており、この類似の度合いが相互相関値として算出される。更に、ビット“１”が埋め込まれている場合（抽出パターンｗ１、ｗ２、…、ｗｎが加えられている場合）には相互相関値は正となり、一方で、ビット“０”が埋め込まれている場合（抽出パターンｗ１、ｗ２、…、ｗｎが減じられている場合）には相互相関値は負になる。

【０１４８】

具体例として、図１６に前述した４ビットの付加情報“１００１”が埋め込まれた画像データＩ''（集積画像ｃ）からｗ１、ｗ２、ｗ３、ｗ４を用いて電子透かしを抽出する例を示す。

【０１４９】

まず、集積画像ｃと４つの抽出パターンｗ１、ｗ２，ｗ３、ｗ４（４ビットの付加情報Ｉｎｆ'に対応）との相互相関値が夫々算出される。入力された画像データＩ'（集積画像ｃ）に付加情報Ｉｎｆ'が埋め込まれている場合には、相関係数は夫々“１、－１、－１，１”と算出され、このことから付加情報Ｉｎｆ'は“１００１”と判定でき、最終的に４ビットの付加情報Ｉｎｆ'を抽出することが可能である。

【０１５０】

こうして抽出されたｎビットから構成される付加情報Ｉｎｆ'は電子透かし出力部１２０５を通じて出力される。この際に、前述した電子透かしの埋め込み処理部において、付加情報Ｉｎｆが埋め込まれる時に、誤り訂正符号化処理や暗号化処理が施されている場合には、夫々誤り訂正復号処理や暗号復号処理が実行される。得られた情報が最終的に抽出されたバイナリデータ列（付加情報Ｉｎｆ'）として出力される。

【０１５１】

＜第２の実施形態＞

上記実施の形態（第１の実施形態）では、検証処理部において処理されるドキュメントデータは、署名処理部から出力された画像データに対して傾いていないような場合を考えた。しかしながら、署名処理部からプリンタ３１７などを用いてプリントアウトされた原稿が、検証処理部においてスキャナー３１９などを用いて入力される場合、入力されたドキュメントデータは、署名処理部から出力された画像データに対して傾いている場合が多い。傾いているドキュメントデータを用いて識別情報抽出処理、或いは付加情報抽出処理を実行することは困難であるため、傾きを補正することにより、署名処理部から出力された画像データと同じ状態にする必要がある。そこで、本第２の実施形態は、傾いて入力されたドキュメントデータに対する検証処理について説明する。

【０１５２】

[検証処理部]

以下、図１７を用いて本実施の形態に適用される検証処理部（機能）を説明する。

【０１５３】

図１７に示すように、本実施の形態における検証処理部は、画像発生部１７０１、傾斜補正部１７０２、識別情報抽出部１７０３、付加情報抽出部１７０４、検証部１７０５から構成される。

【０１５４】

ここで、図１７に示した検証処理部１７０２は、図２に示した検証処理部に、傾斜補正部１７０２が追加された構成である。よって、傾斜補正部１７０２についてだけ説明をする。画像発生部２０１と画像発生部１７０１、識別情報抽出部２０２と識別情報抽出部１７０３、付加情報抽出部２０３と付加情報抽出部１７０４、検証部２０４と検証部１７０５は、夫々同様の処理が実行されるので詳細な説明は省略する。

【０１５５】
傾斜補正部１７０２の機能について説明する。傾斜補正部１７０２には、ドキュメントデータ発生部１７０１において発生されたドキュメントデータデータＩ４が、ＲＡＭ３０５から入力され、入力されたドキュメントデータＩ４に対して傾斜補正処理が実行され、傾斜補正処理が施された画像データＩ５が出力される。
【０１５６】
ここで、図１８、及び図１９を用いて傾斜補正処理の一例の詳細な説明をする。
【０１５７】
図１９に示すように、本実施の形態における傾斜補正処理部は、エッジ位置検出部１９０１、直線決定部１９０２、回転角度算出部１９０３、回転処理部１９０４から構成される。
【０１５８】
まず、エッジ位置検出部１９０１の機能について説明する。エッジ位置検出部１９０１では、ドキュメントデータ発生部１７０１において発生したドキュメントデータＩ４が入力され、入力されたドキュメントデータＩ４中のエッジ位置ｅが検出され、検出されたエッジ位置ｅが出力される。
【０１５９】
エッジ位置検出処理について図１８を用いて説明する。図１８において１８０１は傾斜補正処理部に入力されたドキュメントデータＩ４、１８０２はドキュメントデータが含まれている（電子透かしが埋め込まれている）画像領域を示す。ドキュメントデータ１８０１の夫々４辺から、図１８に示す矢印１８０３のように４辺に垂直な方向に対して、画素値（輝度や濃度）の変化が大きなエッジの位置ｅ（図示の三角印）の検出を行う。
【０１６０】
次に、直線決定処理部１９０２の機能について説明する。直線決定処理部１９０２では、エッジ位置検出処理部１９０１で検出されたエッジ位置ｅが入力され、エッジ位置ｅを用いて４本の直線ｌ（画像データ１８０２の４辺に相当）が決定され、決定された４本の直線ｌが出力される。
【０１６１】
４本の直線ｌの決定方法の一例として、検出されるエッジ位置ｅをｘｙ座標における極大・極小位置を元に、４つの区間に区分けし、それぞれの区間でそれぞれ直線を最小２乗近似法を用いて決定する方法や、ハフ変換を用いて決定する方法などが適用可能である。
【０１６２】
尚、直線から大きく外れる位置のエッジは除外するなどの改良を導入すると直線近似の精度を向上させることが出来る。
【０１６３】
次に、回転角度算出部１９０３の機能について説明する。回転角度算出部１９０３では、直線決定処理部１９０２で決定された４本の直線ｌが入力され、入力された４本の直線ｌを用いて画像データ１８０２の回転角θを算出し、算出された回転角度θが出力される。
【０１６４】
回転角度θの算出方法としては、４本の直線ｌの何れかと画像データ１８０１の縦または横と成す角度を計算することで、画像データ１８０１に対する画像データ１８０２の回転角を算出することができる。一般的には、この方法で回転角θを求めると、θ±90×ｎ（ｎは整数）の不定性を持つが、本実施の形態において、回転角θは微小な回転角であると仮定すると、回転角θとして比較的小さな角度を選ぶことにより回転角を算出することが可能である。
【０１６５】
次に、回転処理部１９０４の機能について説明する。回転処理部１９０４では、ドキュメントデータＩ４、及び回転角θが入力され、回転角θだけ画像データＩ４を回転処理し、更に、回転処理した後、前記検出されたエッジ位置の内部の領域１８０２だけを切り取り、切り取られた領域が画像データＩ５として出力される。

【０１６６】
以上、本実施の形態における傾斜補正処理の一例を説明した。尚、本発明はこれに限定されることなく、種々の傾斜補正処理を用いることが可能である。
【０１６７】
こうして傾斜補正処理が施された画像データＩ５が識別情報抽出部１７０３、及び付加情報抽出部１７０４に入力されることによって、正しく識別情報抽出処理、及び付加情報抽出処理を実行することが可能である。即ち、本実施の形態における検証処理部を用いることにより、検証処理部に入力されたドキュメントデータが傾いている場合でも、正しく検証処理を実行することが可能である。
【０１６８】
また、一般に、スキャナに原稿をセットする際、ユーザは原稿をランドスケープ、ポートレートのいずれかで読み取らせようとして原稿をセットする。従って、場合によっては、上記傾斜補正を行ったとしても、９０°ずれている場合もあり得る。従って、上記補正を行った場合であっても、付加情報の抽出が失敗したとしても、入力した画像を９０°回転させて再度抽出する処理を行うことが望ましい。
【０１６９】
＜第３の実施形態＞
上記実施の形態（第１の実施形態、及び第２の実施形態）では、署名処理部において生成された画像データＩ３中の文字データ部分に改竄が施された場合に、検証処理部において、文字データが改竄されたこと、更に、改竄された場合には、改竄された文字データ部分を特定可能な方式を説明した。この方式では、署名処理部において電子透かしとして埋め込まれた識別情報Ｉｎｆ１は、検証処理部において正しく付加情報Ｉｎｆ３として抽出されるが、一方で検証処理部において識別情報Ｉｎｆ２が正しく識別されなかった場合をも想定している。
【０１７０】
これは、付加情報Ｉｎｆ３が検証処理部において正しく（識別情報Ｉｎｆ１と等しい値として）抽出可能であることを前提としている。しかしながら、万一、攻撃や画質劣化などの原因で、付加情報Ｉｎｆ３が検証処理部において正しく抽出できなかった場合には、検証処理部において識別情報Ｉｎｆ２と付加情報Ｉｎｆ３は一致しないことから、「何らかの攻撃がされている」という判定は可能である。しかしながら、例えば、画質劣化により付加情報Ｉｎｆ３が抽出できず、更に文字データ部分は全く改竄されていない場合（識別情報Ｉｎｆ２が正しく抽出された場合）にも「何らかの攻撃がされている」と判定されてしまう。よって、付加情報Ｉｎｆ３は攻撃や画質劣化に対してできるだけ耐性が強く、検証処理部において正しく抽出できるようにすることが望ましい。
【０１７１】
一般的に、攻撃に対して耐性を強くするためには、電子透かしを強く埋め込むようにすれば良い。このために、例えば、前述した式１においてａの値を大きくするようにする。しかしながら、単純に電子透かしを強く埋め込むだけでは、画質劣化が大きくなり望ましくない場合がある。
【０１７２】
そこで、本実施の形態においては、出来るだけ人間の目に見えにくいように、且つ、強い電子透かしとして付加情報Ｉｎｆ３を埋め込む方法を説明する。
【０１７３】
以下、図２１を用いて本実施の形態に適用される署名処理部（機能）を説明する。なお、以下の説明では、ホストコンピュータ３０１に電源が投入され、ＯＳがＲＡＭ３０５にロードされ、しかる後に、本実施形態で説明する処理を行うアプリケーションがＲＡＭ３０５にロードされている場合である。従って、各処理部は、該当するプログラム及びそれを実行するＣＰＵ３０３、場合によっては周辺のハードウェアでもって実現することになる。
【０１７４】

図２１に示すように、本実施の形態における署名処理部は、画像発生部２１１、ドキュメントデータ発生部２１２、識別情報抽出部２１３、付加情報埋め込み部２１４、合成部２１５、ドキュメントデータ出力部２１６、及び特徴情報抽出部２１７から構成される。

【０１７５】

尚、ここで説明する署名処理はソフトウェア処理により実現されても良い。その場合には、上記各部は上記処理に必要な機能を概念的なものとして捉えたものと考慮されるべきものである。

【０１７６】

ここで、画像発生部２１１、ドキュメントデータ発生部２１２、識別情報抽出部２１３、付加情報埋め込み部２１４、合成部２１５、ドキュメントデータ出力部２１６は、夫々、図１における、画像発生部１０１、ドキュメントデータ発生部１０２、識別情報抽出部１０３、合成部１０５、ドキュメントデータ出力部１０６と同様の機能であるので詳細な説明は省略する。以降では、機能の異なる特徴情報抽出部２１７、及び付加情報埋め込み部２１４の機能について説明する。

【０１７７】

まず、特徴情報抽出部２１７の機能について説明する。特徴情報抽出部２１７は、ドキュメントデータ発生部２１２において発生したドキュメントデータＤが入力され、入力されたドキュメントデータＤ中の特徴情報Ｃが抽出され、抽出された特徴情報Ｃが出力される。

【０１７８】

本実施の形態における特徴情報Ｃとは、後述する付加情報埋め込み部２１４において、電子透かしを強く埋め込む箇所である。特徴情報Ｃについて図２２に具体例を示して説明する。

【０１７９】

図２２において、２２１は入力されたドキュメントデータＤである。２２２は２２１に示すドキュメントデータ中の文字データ部分を全て含むような特徴情報Ｃである。また、２２３は２２１に示すドキュメントデータ中の印鑑などの重要な部分だけを含むような特徴情報Ｃである。更に、２２４は２２１に示すドキュメントデータ中の金額などの改竄されないようにすべき部分だけを含むような特徴情報Ｃである。

【０１８０】

本実施形態においては、図２２に示すように、ドキュメントデータＤを互いに重ならない複数の矩形領域に分割し、矩形領域毎に特徴情報か否かを判定し、特徴情報である領域を（図中、黒色領域として示した矩形領域）後段の付加情報埋め込み部２１４に電子透かしを強く埋め込む領域として出力する。

【０１８１】

尚、本実施形態では説明の為に、特徴情報を矩形領域として示したが本発明はこれに限定されることなく特徴情報Ｃとして任意の形状を指定可能であることは明らかである。

【０１８２】

また、本実施形態では特に特徴領域として重要な部分を抽出するような説明をしたが、本発明はこれに限定されることなく、種々の領域を特徴領域として抽出可能であることは明らかである。特徴情報抽出部２１７において抽出された特徴情報Ｃには、後述するように強い電子透かしが埋め込まれるために画質劣化が大きくなる場合がある。特徴情報Ｃとしてドキュメントデータ中の重要な部分を抽出するようにした場合に、当該重要な部分の背景の画質劣化が大きくなってしまい問題となる場合がある。よって、重要な部分の画質劣化を小さくするために、重要な部分を避け、重要な部分の周囲の領域を特徴情報Ｃとして抽出するようにしても良い。

【０１８３】

以上、説明したような特徴情報Ｃはユーザにより手動で指定するようにしても良いし、或いは自動的に抽出するようにしても良い。ユーザにより手動で指定する場合には、ドキュメントデータＤをモニタ３０２などに表示し表示されたモニタ上のドキュメントデータＤ

をマウス３１１などを用いて指定するようにすればよい。また、自動的に抽出する場合には、ドキュメントデータＤに二値化処理を施し、黒色画素を多く含む領域を特徴情報Ｃとして指定したりすればよい。しかしながら、本発明はこれに限定されることなく、様々な特徴情報抽出処理を用いることが可能である。

【０１８４】

以上、本実施形態における特徴情報Ｃについて説明した。抽出された特徴情報Ｃは付加情報埋め込み部２１４に入力される。

【０１８５】

次に、付加情報埋め込み部２１４の機能について説明する。付加情報埋め込み部２１４は、画像データＩ１、識別情報Ｉｎｆ１、及び特徴情報Ｃが入力され、特徴情報Ｃを用いて識別情報Ｉｎｆ１が電子透かしとして画像データＩ１に埋め込まれ、電子透かしが埋め込まれた画像データＩ２が出力される。

【０１８６】

本実施形態における付加情報埋め込み処理は、前段の特徴情報抽出部２１７で抽出された特徴情報Ｃに示された領域について、それ以外の領域に比べて強く電子透かしを埋め込むように、矩形領域毎に処理する。例えば、特徴情報の領域（図２２における黒色領域）では式１におけるａを“２０”とし、特徴情報以外の領域（図２２における白色領域）では式１におけるａを“１０”として、付加情報埋め込み処理を実行する。

【０１８７】

しかしながら、本発明はこれに限定されることなく、種々の方法で電子透かしの強度を変化させて、領域毎に異なる強度で電子透かしを埋め込むことを含む。

【０１８８】

以上のように電子透かしを埋め込むことによって、画像全体の画質を劣化させることなく電子透かしを強く埋め込むことが可能である。また、ドキュメントデータＤ中で印鑑や文字データ部分などの重要な領域は攻撃される可能性が高いことから、特徴情報Ｃとしてこれらの領域を設定することにより、電子透かしの耐性をより強くすることが可能となる。

【０１８９】

＜第４の実施形態＞

上記実施の形態（第１の実施形態、第２の実施形態、及び第３の実施形態）では、図２０に示すように、識別情報認識領域切り出し部２００１において領域データＲを抽出し、文字認識部２００２において抽出された領域Ｒ内の文字を認識し、認識された文字データＩｎｆ１を背景データに埋め込むようにしていた。

【０１９０】

この場合、前述したように署名処理部と検証処理部とで領域データＲを共通に設定する必要がある。しかしながら、本発明はこれに限定されることなく、領域データＲを必要としないようにすることも可能である。

【０１９１】

以下、図２３を用いて本実施形態に適応される識別情報抽出部１０３（及び２０２）を説明する。

【０１９２】

図２３に示すように、本実施形態における識別情報抽出部は、文字認識部２３１、及び特定文字選択部から構成される。

【０１９３】

まず、文字認識部２３１の機能について説明する。文字認識部２３１は、ドキュメントデータＤを入力し、入力されたドキュメントデータに含まれる全ての文字を認識し、認識された全ての文字を文字列Ｃとして出力する。文字認識部２３１における処理は、図２０における文字認識部２００２と同様であるので詳細な説明は省略する。

【０１９４】

次に、特定文字選択部２３２の機能について説明する。特定文字選択部２３２は、前段の

文字認識部２３１で認識された全ての文字列Ｃを入力し、文字列Ｃの中から特定の文字を選択し、選択された全ての文字を文字列Ｉｎｆ１として出力する。

【０１９５】

特定文字選択部２３２では、入力された文字列Ｃの中から予め決められた所定の文字に一致する文字列が選択する。例えば、領収書などの金額情報を被署名データとする場合には、「０」から「９」の数字や「￥」や「＄」などの記号を選択するするようにすればよい。

【０１９６】

或いは、入力された文字列Ｃの中から予め決められた所定の文字に一致する文字列を抽出し、その後に続く所定数の文字列を選択するようにしても良い。例えば、契約書などの契約番号を被署名データとする場合には、「契約番号」という文字列を抽出し、抽出された文字列の後に続く数桁の文字列を選択するようにすれば良い。

【０１９７】

以上、本実施形態に適応可能な識別情報抽出部の動作を説明した。本実施形態によれば、文字認識部２３１においてドキュメントデータＤの全領域を文字認識処理の対象とし、且つ、特定文字選択部２３２において署名処理部と検証処理部で共通の文字を選択するようにすることによって、署名処理部と検証処理において領域データＲを共有する必要がないようにできる。

【０１９８】

＜適用例の説明＞

以上説明した実施形態での適用例としては様々なものが考えられる。ここでは、パーソナルコンピュータ上で動作するプリンタドライバに適用させた例を説明する。

【０１９９】

通常、プリンタドライバは、ワープロアプリケーションから印刷させる対象のデータを受信し、それを出力対象のプリンタが解釈できる記述にして出力する。従って、アプリケーション上で印刷を指示した際に、先ず、背景となる画像を予め登録していた複数の中から選択させ、印刷の指示を行う。

【０２００】

文章を印刷させる場合には、文字コードを含むデータがプリンタドライバに渡されるので、その中の文字列を抽出することで、埋め込むべき付加情報を抽出できる。すなわち、この場合には、先に説明した文字認識は不要となる。アプリケーションから指定された背景画像にその付加情報を埋め込む。そして、埋め込み結果と印刷させようとするデータとを合成したデータをプリンタに適用するデータに変換し、ＯＳを介して出力すれば良いであろう。

【０２０１】

以上説明したように、本実施形態によれば、ドキュメントの背景に前記ドキュメントの内容を電子透かしとして埋め込むことによって、前記電子透かしが埋め込まれたドキュメントが改ざんされているか否かを検証可能であり、且つ、改ざんされていると判断された場合には改ざんされている位置を特定することが可能である。

【０２０２】

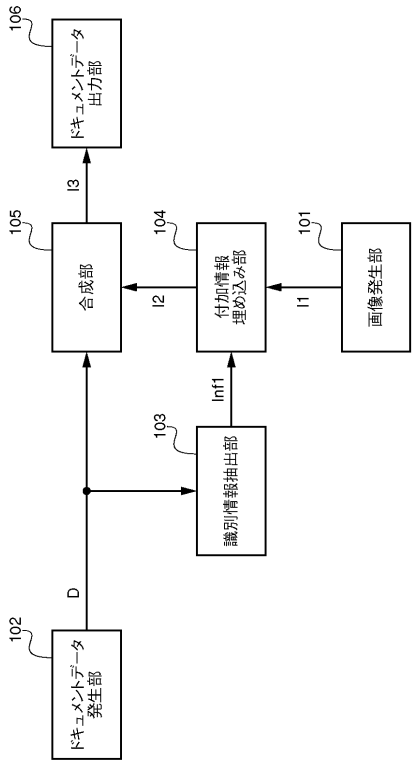
なお、実施形態で説明した付加情報の埋め込み及びその抽出方法はその一例であって、他の手法を用いても良く、上記実施形態によって本発明が限定されるものではない。

【０２０３】

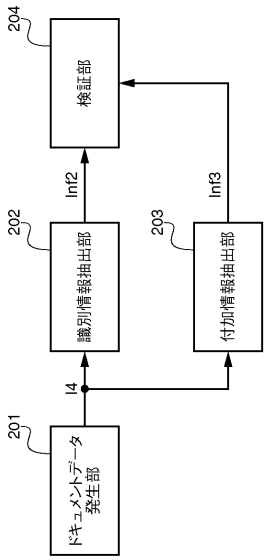
また、上記実施形態での説明から明らかなように、本発明の主要部分はパーソナルコンピュータ上で動作するアプリケーションとして提供できるものである。従って、本発明はコンピュータプログラムをもその範疇とするものである。更に、通常、コンピュータプログラムはフロッピー（Ｒ）ディスクやＣＤＲＯＭ等を可搬性のコンピュータ可読記憶媒体に格納されており、その媒体をコンピュータにセットしてコピー或いはインストールすることで実行可能となるわけであるから、コンピュータ可読記憶媒体も本発明の範疇に含まれることも明らかである。

【０２０４】
【発明の効果】
以上説明したように本発明によれば、ドキュメントの背景に前記ドキュメントの内容を電子透かしとして埋め込むことによって、前記電子透かしが埋め込まれたドキュメントが改ざんされているか否かを検証可能であり、且つ、改ざんされていると判断された場合には改ざんされている位置を特定することが可能である。
【図面の簡単な説明】
【図１】第１の実施の形態における署名処理部の構成を示す図である。
【図２】第１の実施の形態における検証処理部の構成を示す図である。
【図３】本実施形態に適用可能な情報処理装置の構成を示す図である。
【図４】本実施形態における合成処理部の説明をする図である。
【図５】本実施形態における検証処理部の説明をする図である。
【図６】本実施形態における電子透かしの埋め込み処理を説明するブロック図である。
【図７】本実施形態における電子透かし生成部を説明するブロック図である。
【図８】本実施形態における基本行列の一例を示す図である。
【図９】本実施形態における電子透かしの一例を示す図である。
【図１０】本実施形態における電子透かし埋め込み演算の例を示す図である。
【図１１】本実施形態におけるマクロブロックを示す図である。
【図１２】本実施形態における電子透かしの抽出処理を説明するブロック図である。
【図１３】本実施形態における抽出パターン生成部の一例を示す図である。
【図１４】本実施形態における抽出パターンの一例を示す図である。
【図１５】本実施形態における集積画像を用いた電子透かしの抽出の例を説明する図である。
【図１６】本実施形態における集積画像を用いた電子透かしの抽出演算の例を説明する図である。
【図１７】第２の実施の形態における検証処理部の構成を示す図である。
【図１８】第２の実施の形態における傾斜補正を説明する図である。
【図１９】第２の実施の形態における傾斜補正部の構成を示す図である。
【図２０】本実施形態における識別情報抽出部の構成を示す図である。
【図２１】第３の実施形態における署名処理部の構成を示す図である。
【図２２】第３の実施形態における特徴情報を説明する図である。
【図２３】第４の実施形態における識別情報抽出部を説明する図である。

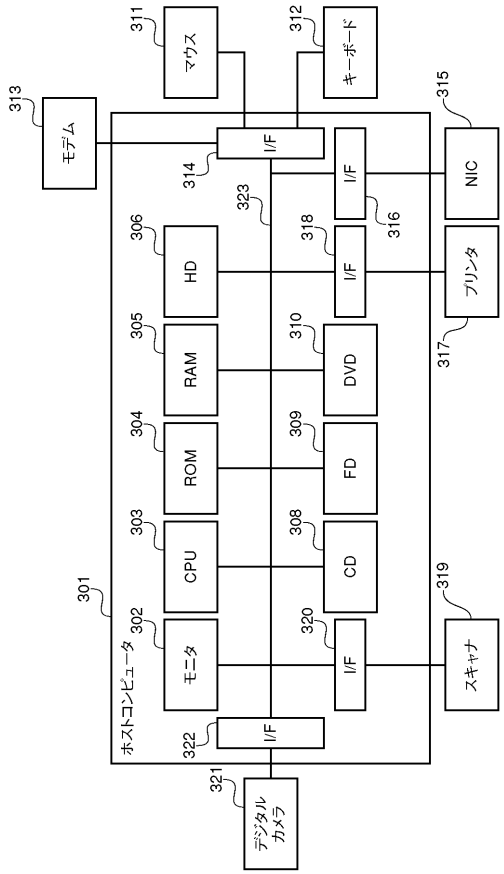
【図１】


106
ドキュメントデータ出力部
I3
105
合成部
104
付加情報埋め込み部
101
画像発生部
I2
I1
Inf1
103
識別情報抽出部
D
102
ドキュメントデータ発生部

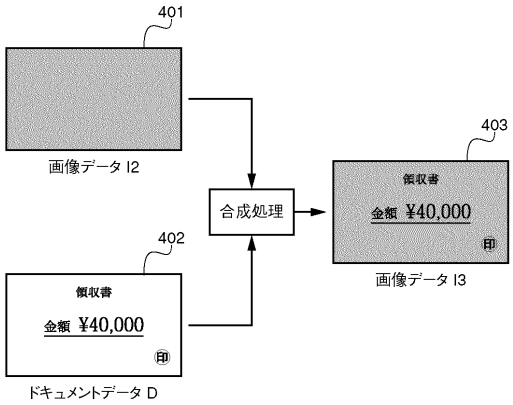
【図２】


204
検証部
Inf2
Inf3
202
識別情報抽出部
203
付加情報抽出部
I4
201
ドキュメントデータ発生部

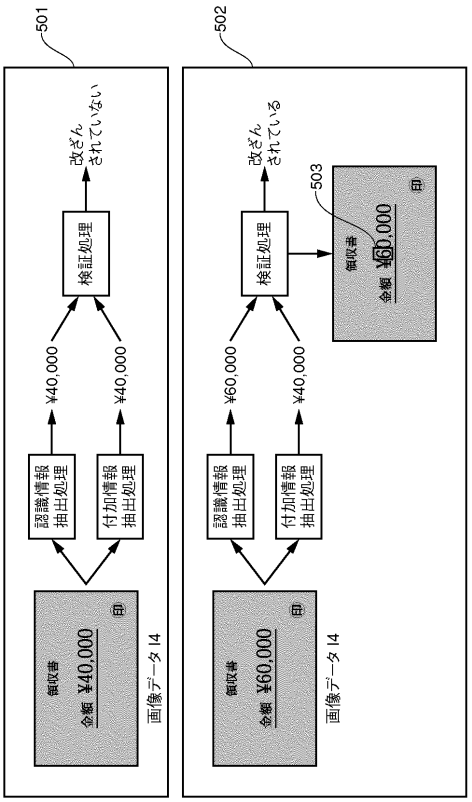
【図３】


311
マウス
312
キーボード
313
モデム
315
NIC
I/F
314
323
316
306
HD
318
プリンタ
305
RAM
310
DVD
317
304
ROM
309
FD
303
CPU
308
CD
301
302
モニタ
320
319
スキャナ
ホストコンピュータ
322
321
デジタルカメラ

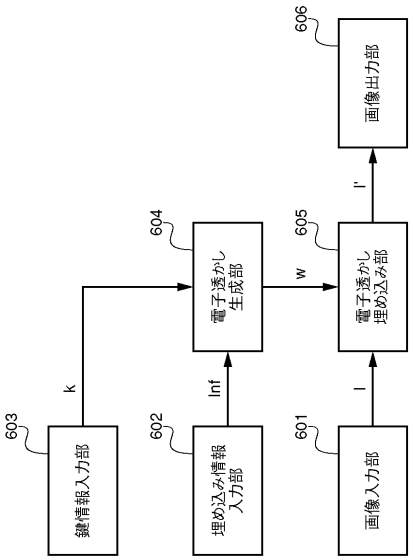
【図４】


401
画像データ I2
合成処理
403
領収書
金額 ¥40,000
印
画像データ I3
402
領収書
金額 ¥40,000
印
ドキュメントデータ D

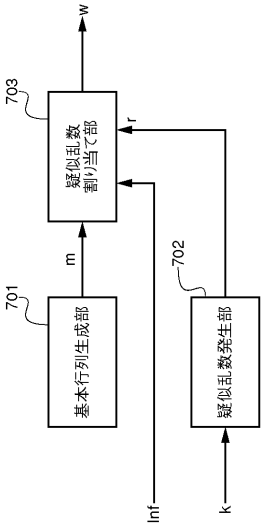
【図５】



【図６】



【図７】



【図８】

1	15	14	4
12	6	7	9
8	10	11	5
13	3	2	16

801

1			4
	6	7	
8			5
	3	2	

802

1	8	7	2
6	3	4	5
4	5	6	3
7	2	1	8

803

1	4	4	1
3	2	2	3
2	3	3	2
4	1	1	4

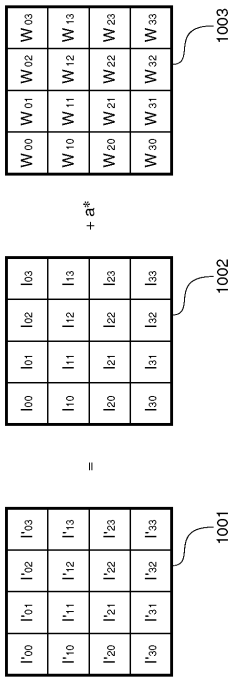
804

【図９】

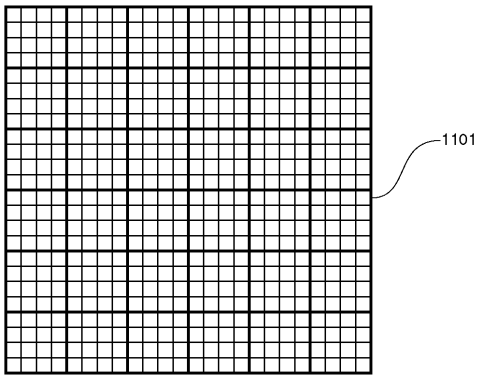
0.7	0.7	-0.6	-0.6
-0.7	-0.7	0.6	0.6
0.9	-0.9	-0.8	-0.8
0.9	-0.9	0.8	0.8

901

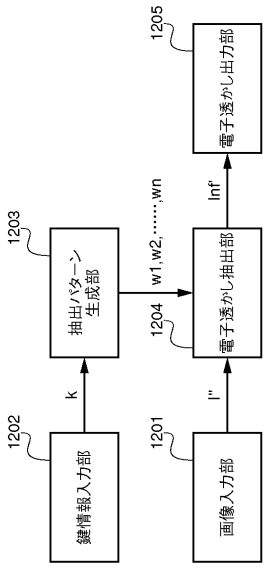
【図１０】



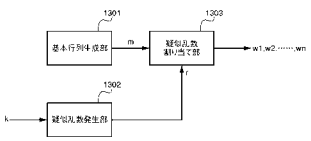
【図１１】



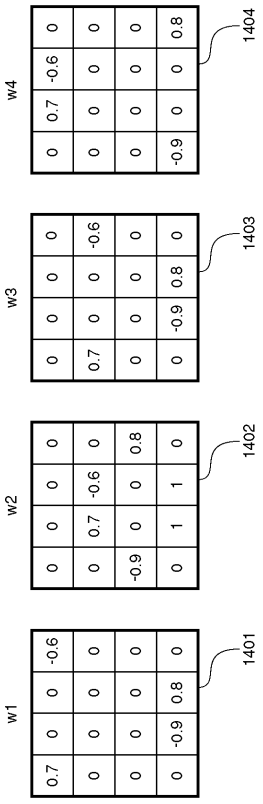
【図１２】



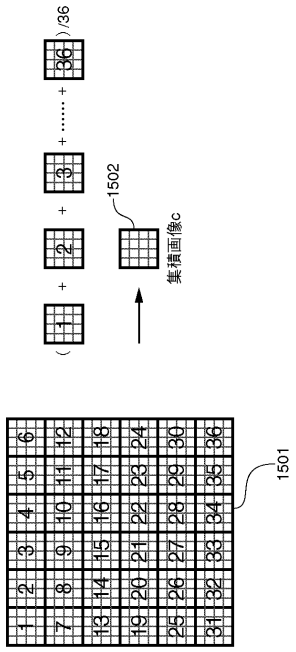
【図１３】



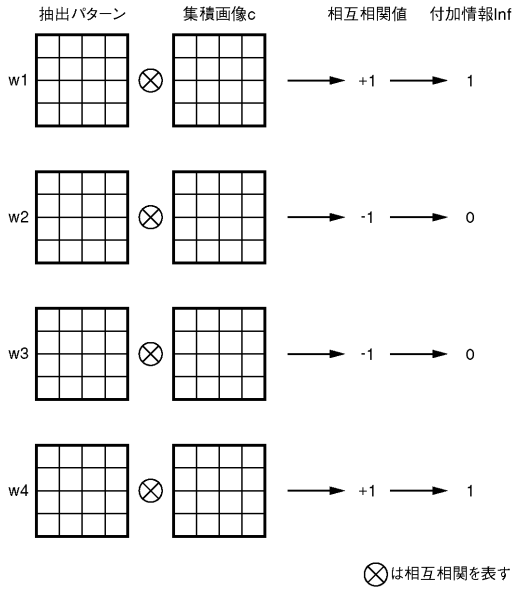
【図１４】



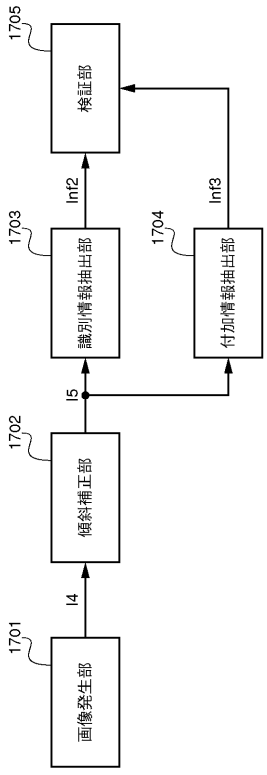
【図１５】



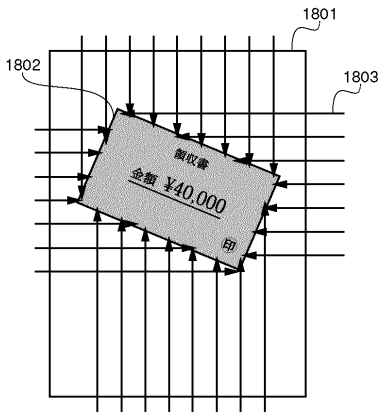
【図１６】



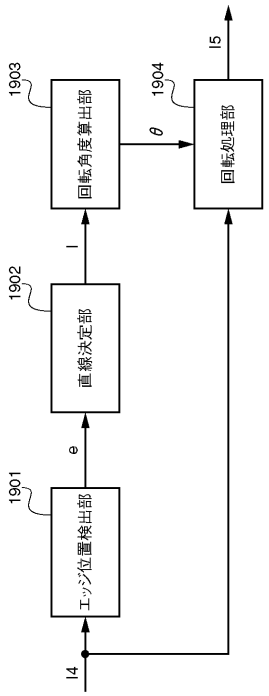
【図１７】



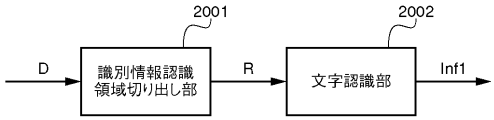
【図１８】



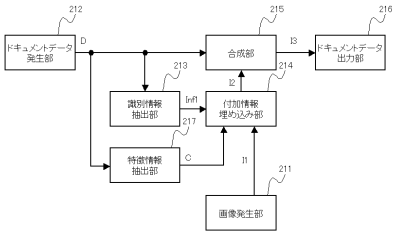
【図１９】



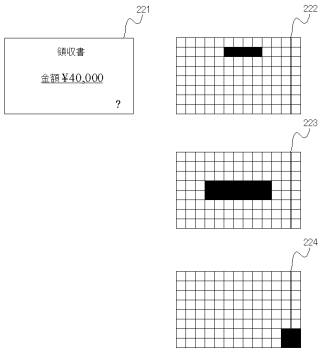
【図２０】



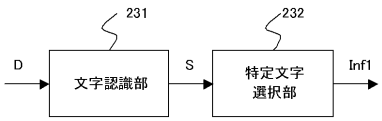
【図２１】



【図２２】



【図２３】



フロントページの続き

審査官　橋爪　正樹

(56)参考文献　特開平０９－１９１３９５（ＪＰ，Ａ）
特開２００１－３４６０３３（ＪＰ，Ａ）
特開２０００－２８７０６６（ＪＰ，Ａ）
特開２００１－０４２７６８（ＪＰ，Ａ）
特開平１０－１６４５４９（ＪＰ，Ａ）
特開平０７－１２３２４４（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
H04N 1/38- 1/393
G06T 1/00
G09C 5/00