(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2008-42906
(P2008-42906A)
(43)公開日　平成20年2月21日(2008.2.21)

(51)Int.Cl.			F I			テーマコード（参考）
H04N	1/387	(2006.01)	H04N	1/387		2C187
G06F	3/12	(2006.01)	G06F	3/12	K	5B021
G06T	1/00	(2006.01)	G06T	1/00	500B	5B057
B41J	5/30	(2006.01)	B41J	5/30	Z	5C076
G09C	5/00	(2006.01)	G09C	5/00		5J104

審査請求 未請求　請求項の数 20　ＯＬ　（全 19 頁）

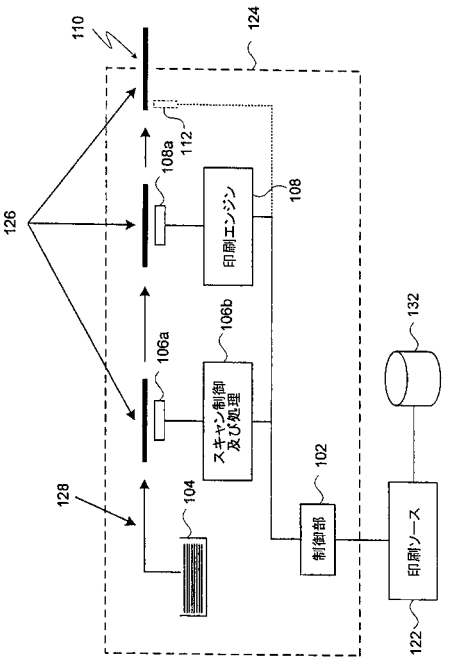
(21)出願番号　特願2007-197790 (P2007-197790)
(22)出願日　平成19年7月30日 (2007.7.30)
(31)優先権主張番号　11/494,829
(32)優先日　平成18年7月28日 (2006.7.28)
(33)優先権主張国　米国 (US)

(71)出願人　000006747
株式会社リコー
東京都大田区中馬込１丁目３番６号
(74)代理人　100070150
弁理士　伊東　忠彦
(72)発明者　カート　ピアソル
アメリカ合衆国，カリフォルニア　９４０２５－７０５４，メンロ・パーク，サンド・ヒル・ロード　２８８２番，スイート　１１５　リコー　イノベーション　インク内

最終頁に続く

(54)【発明の名称】電子書類の印刷方法及び印刷装置

(57)【要約】　（修正有）
【課題】セキュアな印刷書類を効果的に提供する。
【解決手段】印刷方法及び装置は、フィンガープリントを取得するために、紙のような印刷可能媒体のシートをフィンガープリント処理する。フィンガープリントは、書類を印刷することを希望するユーザだけが知っている暗号キーで暗号化される。そして暗号化されたフィンガープリントは、マシン読取可能な情報として書類にエンコードされ移される。
【選択図】図１Ａ



【特許請求の範囲】
【請求項１】
電子書類を印刷する方法であって、
書類を印刷するための通知を印刷ソースから受けるステップと、
書類が印刷される印刷可能な媒体の少なくとも第１シートについて、印刷可能な媒体の前記第１シートに固有の構造から決定される第１フィンガープリントデータを生成するステップと、
少なくとも前記第１フィンガープリントデータから第２フィンガープリントデータを生成するステップと、
前記印刷ソースに前記第２フィンガープリントデータを伝送するステップと、
前記印刷ソースから、暗号化されたフィンガープリントデータ及び第１解読鍵を受けるステップであって、前記暗号化されたフィンガープリントデータは前記第２フィンガープリントデータの暗号化された形式を含み、前記第１解読鍵は前記暗号化されたフィンガープリントデータを復号して前記第２フィンガープリントデータを復元するためのものであるところのステップと、
印刷可能な媒体の前記第１シートに前記書類を印刷するステップと、
を有し、該印刷は前記印刷可能な媒体の前記第１シートにマシン読取可能な情報を移すことを含み、前記暗号化されたフィンガープリントデータ及び前記第１解読鍵は前記マシン読取可能な情報から取得可能である
ことを特徴とする電子書類を印刷する方法。
【請求項２】
前記第１フィンガープリントを生成するステップが、印刷可能な媒体の前記第１シートの第１領域を光ビームでスキャンし、前記第１領域の表面に固有の構造により散乱した光の測定に基づいて光学データを取得し、該光学データを処理して前記第１フィンガープリントデータを生成することを含む
ことを特徴とする請求項１記載の方法。
【請求項３】
前記マシン読取可能な情報が、前記暗号化されたフィンガープリントデータ及び前記解読鍵の双方をエンコードしている
ことを特徴とする請求項１記載の方法。
【請求項４】
印刷される書類について実行されたハッシュ演算により算出されたハッシュ値を前記印刷ソースから受け取るステップを更に含み、前記マシン読取可能な情報は前記暗号化されたフィンガープリントデータ、前記第１解読鍵及び前記ハッシュ値をエンコードしている
ことを特徴とする請求項１記載の方法。
【請求項５】
前記第２フィンガープリントデータが、暗号化されていない形式における前記第１暗号化データを含む
ことを特徴とする請求項１記載の方法。
【請求項６】
前記第２フィンガープリントデータを生成するステップが前記第１フィンガープリントデータ、前記第１フィンガープリントデータの暗号化より成る前記第２フィンガープリントデータ、及び前記第１フィンガープリントデータの暗号化を解除して前記第１フィンガープリントデータを復元するための第２解読キーの暗号化を行うことを含み、
ことを特徴とする請求項１記載の方法。
【請求項７】
前記第１フィンガープリントデータの暗号化が、前記第１フィンガープリントデータを第２暗号鍵で暗号化することを含む
ことを特徴とする請求項６記載の方法。
【請求項８】

前記第２フィンガープリントデータが前記第１フィンガープリントデータを平文形式で含み、前記移すことが、暗号化されるフィンガープリントデータを暗号化することを含み、前記マシン読取可能な情報が、暗号化されるフィンガープリントデータ及び暗号化されたフィンガープリントデータの暗号化を解除して暗号化されるフィンガープリントデータを復元するための第２解読キーを暗号化した者を含む、
ことを特徴とする請求項１記載の方法。
【請求項９】
前記移すことが、マシン読取可能な情報を印刷可能な媒体の第1シートに印刷すること、又は印刷可能な媒体の第1シートに埋め込まれているタグの電子メモリに前記マシン読取可能な情報を格納することを含む
ことを特徴とする請求項１記載の方法。
【請求項１０】
前記第１フィンガープリントデータは印刷可能な媒体の第１シートの第1領域から取得され、当該方法は前記印刷可能な媒体の追加的な領域に関する追加的なフィンガープリントデータを生成するステップを更に有し、前記伝送する及び受けるステップが前記追加的なフィンガープリントデータについて実行され、追加的なマシン読取可能な情報が印刷可能な媒体の第1シートに移される
ことを特徴とする請求項１記載の方法。
【請求項１１】
印刷装置であって、
当該印刷装置における動作を制御するよう構成され、当該印刷装置外部にあり且つ印刷要求元である印刷ソースと通信するよう構成された制御要素と、
印刷可能な媒体のソースと、
印刷可能な媒体の第1シートに固有の構造に基づいて決定されるフィンガープリントデータを該印刷可能な媒体の第１シートから取得するフィンガープリント処理部と、
印刷可能な媒体のシートに印刷されるものを生成するよう構成されたプリンタ要素と、
を有し、前記印刷可能な媒体のソースは、電子書類を印刷するように求める要求を前記印刷ソースから受けたことに応答して、印刷可能な媒体の第1シートを用意し、前記制御要素は、
印刷可能な媒体の前記第1シートの一部分から第1フィンガープリントデータを前記フィンガープリント処理部に取得させるように、
前記第１フィンガープリントデータに少なくとも基づく第２フィンガープリントデータを前記印刷ソースに送信するように、
暗号化されたフィンガープリントデータと、暗号化されたフィンガープリントデータを解読して第２フィンガープリントデータを受信するための第１解読キーとを有するフィンガープリント情報を前記印刷ソースから受信するように、
印刷可能な媒体の前記第1シートに印刷されるものを前記印刷要素に生成させるように、及び
マシン読取可能な情報を印刷可能な媒体の第1シートに伝送するように構成され、
前記フィンガープリント情報は前記マシン読取可能な情報から取得可能である
ことを特徴とする印刷装置。
【請求項１２】
前記第１フィンガープリントデータは、印刷可能な媒体の第1シートの第1領域の表面に固有の構造により散乱した光の測定から得られた光学データに基づく
ことを特徴とする請求項１１記載の印刷装置。
【請求項１３】
前記マシン読取可能な情報は、印刷可能な媒体の第1シートに印刷された印を有する
ことを特徴とする請求項１１記載の印刷装置。
【請求項１４】
前記マシン読取可能な情報は、前記フィンガープリント情報をエンコードしている

ことを特徴とする請求項１１記載の印刷装置。
【請求項１５】
前記フィンガープリント情報は、印刷される電子書類に施されるハッシュ演算により算出されるハッシュ値を更に有すること
ことを特徴とする請求項１４記載の印刷装置。
【請求項１６】
印刷可能な媒体のシートに埋め込まれた電子タグのデータ格納部にデータを伝送するよう構成された書込装置を更に有し、前記マシン読取可能な情報は、印刷可能な媒体のシートに埋め込まれた電子タグのデータ格納部に、前記書込装置により伝送されるデータを有する
ことを特徴とする請求項１１記載の印刷装置。
【請求項１７】
前記印刷可能な媒体のソースが、印刷可能な媒体の単一のシートを分配することにより、印刷可能な媒体の前記第１シートを用意する
ことを特徴とする請求項１１記載の印刷装置。
【請求項１８】
前記制御要素は、暗号化されたデータを生成するために前記フィンガープリントデータを暗号化するように更に構成され、前記第２フィンガープリントデータは暗号化されたデータを含む
ことを特徴とする請求項１１記載の印刷装置。
【請求項１９】
前記制御要素は、前記フィンガープリント情報を暗号化するよう構成される
ことを特徴とする請求項１１記載の印刷装置。
【請求項２０】
電子書類を印刷する方法であって、
書類を印刷するための要求を印刷ソースから受けるステップと、
書類が印刷される印刷可能な媒体の少なくとも第１シートについて、印刷可能な媒体の前記第１シートに固有の構造から決定される第１フィンガープリントデータを生成するステップと、
少なくとも前記第１フィンガープリントデータから生成された第２フィンガープリントデータを前記印刷ソースに伝送するステップであって、前記印刷ソースは、前記第２フィンガープリントデータを暗号化し、暗号化された第２フィンガープリントデータ及び第１解読キーをデータ格納部に格納し、前記第１解読キーは暗号化された第２フィンガープリントデータから第２フィンガープリントデータを復元するためのものであるところのステップと、
暗号化された第２フィンガープリントデータ及び格納された第１解読キーをデータ格納部から取得するのに使用可能なロケーション指標を前記印刷ソースから受信するステップと、
印刷可能な媒体の前記第１シートに前記書類を印刷するステップと、
を有し、該印刷は前記印刷可能な媒体の前記第１シートにマシン読取可能な情報を移すことを含み、前記ロケーション指標は前記マシン読取可能な情報から取得可能である
ことを特徴とする電子書類を印刷する方法。

【発明の詳細な説明】
【技術分野】
【０００１】
本発明は一般に印刷技術に関連し、特に検証可能な印刷に関連する。
【背景技術】
【０００２】
保護される（secured）用紙は一般に通貨、株及び他の金融文書に関連付けられる。従

来の保護される用紙の生成は、紙の蓄え（セキュリティ属性を有する特殊な用紙が必要とされる）や印刷装置（特別なリンク及び印刷機器が必要とされる）等の観点からコスト高である。保護された紙書類処理機能がコスト効果的に利用可能ならば、多くの企業にとって有意義であろう。

【０００３】

用紙固有の属性に基づいて用紙を固有に署名する様々な技法が知られている。これは、対象とする用紙の署名を取得し、それを書類署名の記憶済みデータと比較することで、書類の真正を受領者が確認することを可能にする。

【特許文献１】国際公開第WO2005/088533号パンフレット

【発明の開示】

【発明が解決しようとする課題】

【０００４】

本発明の課題は保護された（セキュアな）印刷書類をコスト効果的にもたらすことである。

【課題を解決するための手段】

【０００５】

用紙を固有に識別するために、印刷する用紙の指紋又はフィンガープリント(fingerprint)を利用する印刷装置が用意される。結果のフィンガープリントは暗号化され、暗号文を生成する。暗号化はユーザ（署名する権能を有する者）によって用意された暗号キーを用いて実行される。そして暗号文は対応する解読キーとペアにされ、そのデータペアは或る暗号化手法で暗号化され；例えば、バーコード暗号化を利用して暗号文及び解読キーのバーコード表現を生成することができる。

【発明を実施するための最良の形態】

【０００６】

印刷されたシートはそのシートの暗号化されたフィンガープリント及び解読キーを含む。印刷されたマシン読取可能な情報をデコードし、暗号化されたフィンガープリントデータ及び解読キーを取得し、解読キーを用いて暗号化されたフィンガープリントの平文形式を引き出し、受け取った印刷シートのフィンガープリントと比較することで、印刷された用紙の受領者は、そのシートが本来の印刷されたシートであって複製でないことを確認することができる。更に、受信した印刷シートは署名する権能のある者によって生成されていることが受領者に保証される。なぜなら解読キーは署名する権能のある者に帰属するように保証されるからである。

【実施例１】

【０００７】

図１Ａの概略図には本発明の一実施例が示されている。印刷ソース１２２は、印刷装置１２４と及びデータベース１３２とデータ通信を行う。印刷ソース１２２は典型的にはパーソナルコンピュータであるが、印刷サービスを必要としてそれを起動する如何なるコンピュータベースの装置でもよい。印刷ソース１２２及び印刷装置１２４間のデータ通信は、２つの要素間の直接的なコネクションを介して、通信ネットワークを介して、無線コネクション等を介して行われてよい。

【０００８】

印刷装置１２４は、印刷ソース１２２のような外部コンピュータとのデータ通信用の制御部１０２を含み、制御部は印刷装置の様々な動作を制御する。特定の実施例では制御部１０２は、プロセッサを制御するための適切なプログラミングコード及び適切なサポートロジックと共にプロセッサを含んでよい。

【０００９】

ソース１０４は紙のような印刷媒体を用意し、印刷媒体は印刷装置１２４の他の要素による処理のためにプロセス経路１２８に沿う処理に委ねられながら供給される。図１Ａは印刷可能な媒体１２６（例えば、紙であることが一般的である）のシートを、それが（矢印で示される）プロセス経路１２８に沿って搬送されるように示す。図１Ａはソース１０

４を従来のプリンタに見受けられるような用紙トレイとして描いているが、印刷媒体の性質に相応しい形式で印刷媒体を提供するよう構成可能であることが理解されるであろう。本発明における「印刷可能な媒体のシート」は或る単位の印刷された出力の概念を伝えるために使用されることに留意を要する。例えばロール用紙の場合、ロール全体は大きなシートをなすように考えられてもよい。しかしながら、本発明では印刷ジョブのサービス中にロールから個々のシートが切断される。

【００１０】

印刷可能な媒体のシート１２６は、プロセス経路１２８に沿って、指紋処理部に供給され、指紋処理部はスキャン制御及び処理部１０６ｂ及びスキャナ１０６ａを有し、シートの一部をスキャンし、印刷可能な媒体特有のシートを一意に識別できるフィンガープリントを取得する。プロセス経路１２８の更に下流は、プリントヘッド１０８ａを有する印刷エンジンである。印刷エンジン１０８はレーザプリンタ技術、インクジェット印刷技術、又は印刷装置１２４に相応しい他の如何なる印刷技術を利用してもよい。印刷可能な媒体１２６のシートはプロセス経路１２８に沿って終点に進み、完了した印刷ジョブとして印刷装置から出る。

【００１１】

制御モジュール１０２は適切なプログラム命令を含み、そのプログラム命令は印刷ソース１２２から印刷要求を受信し、印刷要求サービスを提供するために本発明に従って印刷ソースと相互作用するためのものである。印刷ソース１２２はプリンタドライバ（図示せず）として一般に言及される関連するソフトウエアを含み、プリンタドライバは制御モジュール１０２と相互作用するように機能し、以下にて更に説明される。

【００１２】

図１Ｂには本発明の別の実施例が示されている。図１Ａ及び図１Ｂに共通の要素は同じ参照番号で参照される。この特定の実施例では、印刷装置１２４ａは印刷要素１０８，１０８ａから構成される。スキャン制御及び処理部１０６ｂ及びスキャナ１０６ａは指紋処理部１２４ｂに含まれている。制御モジュール１０２はスキャン制御及び処理部１０６ｂを制御するために指紋処理部１２４ｂとデータ通信を行い、指紋処理部１２４ｂ及び印刷装置１２４ａ間で如何なるデータ交換をも行う。

【００１３】

プロセス経路１２８’は指紋処理部１２４ｂのソース１０４から始まり、印刷可能な媒体１２６のシートが取り出され、スキャナ１０６ａに配布され、印刷可能な媒体のフィンガープリントを取得する。指紋処理部１２４ｂ及び指紋処理部１２４ａ間に適切な結合部（図示せず）が用意され、印刷可能な媒体のシートを印刷装置にプロセス経路１２８’で供給可能にする。印刷ジョブが完了すると、印刷されたシートはプロセス経路１２８’の終点１１０で生成される。当然に、同様な組み合わせ機能をもたらす他の実施例も可能であることが理解されるであろう。

【００１４】

図２は本発明の一実施例によるスキャナ１０６ａの一例を示す概略図である。スキャナ１０６ａの基本的な動作は特許文献１（Cowburn等の発明）に詳細に説明されている。本発明の一形態でのスキャナ１０６ａの変形例は特許文献１によっては開示も示唆もされておらず、以下で説明される。スキャナ１０６ａの更なる詳細は本発明に関係せず、それについては特許文献１を参照されたい。

【００１５】

図２におけるスキャナ１０６ａの主要な光学要素は、コヒーレントなレーザビーム２２４を生成するレーザ源２２２と、複数のフォトディテクタ要素２３２ａ－２３２ｄを含むディテクタ配置２３２とを含む。図２に示される特定の実施例は４つのフォトディテクタ要素を示しているが、別の数のフォトディテクタ要素が使用されてもよいことは理解されるであろう。レーザビーム２２４はレンズ２２６によって焦点に合わせられ、ｙ軸方向（紙面に垂直方向）に伸びる細長いフォーカスを形成し、読取空間２２８を通って伝搬する。光学要素は光アセンブリ２０２内に含まれている。

【００１６】
フォトディテクタ２３２ａ－２３２ｄはビーム周辺に異なる角度で分散され、コヒーレントビームが読取空間から散乱する場合に、読取空間２２８の中にある物品(article)の一部から散乱された光を収集し、物品により散乱された光を検出する。図２に示されるように、レーザソース２２２はｚ軸に平行な光線軸に沿ってレーザビーム２２４を向ける。本発明の一実施例によれば、レーザソース２２２は、ｚ軸に関してゼロでない角度の光線軸でレーザビーム２２４を向けるように選択的に操作される。
【００１７】
図１Ａ及び１Ｂは、印刷可能な媒体１２６がスキャナ１０６ａを通過してプロセス経路１２８に沿って搬送されることを示す。これらの例ではスキャナ１０６ａは静的である。しかしながら代替実施例では、印刷可能な媒体１２６はプロセス経路１２８に沿う或る位置に搬送され、その位置に維持され、スキャナ１０６ａがスキャン操作を実行するように制御されてもよい。そのような例ではスキャナ１０６ａは駆動手段と共に備えられる。図２に示されるように、そのような駆動手段の一例はドライブモータ２０４を含み、ドライブモータは適切なベアリング２０６を利用して光アセンブリ２０２の線形な運動機能をもたらす。本発明の一実施例では、光アセンブリ２０２は矢印２０８で示されるようにｘ軸に沿って動かされる。本発明の別の実施例では、ドライブモータ２０４はｘ－ｙ方向に光アセンブリ２０２を動かすように制御可能である。
【００１８】
図３は図２のスキャナ１０６ａを利用して物品のシグネチャ（「フィンガープリント」又は「指紋」と言及される）を生成するプロセスを示す上位概念的フローチャートである。更なる詳細は本発明の本質でなく、特許文献１等で説明されている。
【００１９】
ステップ３０２では物品がスキャナ１０６ａに供給される。物品の一部が読取空間２２８を通過すると、物品表面に入射したレーザビーム２２４は、物品表面に固有の不均一な構造による反射に起因して散乱させられる。散乱光はフォトディテクタ２３２ａ－２３２ｄによって検出される。ステップ３０６では、フォトディテクタ２３２ａ－２３２ｄが散乱光を検出すると、それらから出力されたアナログ信号をアナログディジタル変換することでデータが取得される。このステップは適切なプログラミングコードに従って制御されるスキャン制御及び処理部１０６ｂでプロセッサにより実行可能である。スキャン動作中に生じた散乱光はフォトディテクタ２３２ａ－２３２ｄの出力信号における固有の光応答になる。特許文献１に詳細に説明されているように、散乱光は物品表面の顕微鏡レベルの不規則な微細構造による反射なので、入射光の固有の散乱により固有の光応答が生じる。例えば紙のような物品は、顕微鏡レベルでは交錯した繊維その他の材料（紙を形成する材料）構造の表面属性を有し、概してその構造は物品固有の構造に関連する。
【００２０】
ステップ３０８では、フォトディテクタ２３２ａ－２３２ｄからの信号のＡ／Ｄ変換により集められたデータが、スキャン制御及び処理部１０６ｂにより処理され、シグネチャが生成され、シグネチャ自体については本発明の範囲外であり、それについては特許文献１を参照されたい。そのプロセスの結果得られるデータは物品を固有に識別し、本願では「フィンガープリントデータ」又は「シグネチャデータ」とも呼ばれる。スキャン制御及び処理部１０６ｂにおけるプログラミングコードは本ステップを実行するようにプロセッサを制御可能である。
【００２１】
本発明の一実施例によれば、印刷するプロセスはディジタル的に署名された書類を用意し、その書類の真正を保証し、本来的に印刷された書類であって複製でないこと或いは本来の書類の偽造物でないことを保証する。図４Ａ及び５Ａは印刷要求を処理するための本発明の一実施例によるプロセスフローを示す。図４は印刷要求に関連する主要な要素間での情報の流れを示す概略図である。図５はそのプロセスでのステップを強調している。
【００２２】

ユーザ４０２は１以上の書類を印刷するために印刷ソース４２２（典型的には、例えばＰＣのようなコンピュータ）に要求を送信することでプロセスを開始する（ステップ５０１）。ユーザは人的なユーザでもよいし、マシンによる「ユーザ又は者」（例えば、同じコンピュータで又は異なるコンピュータで動作している自動印刷タスク）でもよい。

【００２３】

適切なプリンタドライバ４２２ａがこの機能をもたらすように印刷ソース４２２にインストールされてもよい。プリンタドライバはプログラムコードであり、ユーザインターフェースをもたらすようにデータプロセッサを制御し、ユーザに印刷ジョブを構成可能にし、インサブジョブサービスを提供するためにプリンタと通信するようにする。本発明によるプリンタドライバ４２２ａはプログラミングコードより成り、印刷ソース４２２にてプロセッサを制御し、図５Ａ－５Ｃのフローチャートに示される動作を実行するようにし、その動作はユーザインターフェースを用意すること及びプリンタ側の要素４２４との通信を実行することを含むことが理解されるであろう。

【００２４】

ステップ５０２では印刷ソース４２２が暗号キーを取得し、そのキーは所有される或いはユーザ４０２に関連付けられる。人的なユーザの場合、このステップは問い合わせ（クエリ）を例えばＧＵＩを用いることでユーザに表示し、ユーザの暗号キーを入力させる或いはユーザの暗号キーを取得するための何らかの情報を入力させてもよい。例えば、印刷ソース４２２はユーザリスト及び各自の暗号キーを含むコンフィギュレーションファイルにアクセスしてもよい。

【００２５】

ユーザは１以上の暗号キーを有してもよく、暗号キーの各々は異なる権能を表現してもよい。例えば、同じ検査プログラムによるチェックを、同じコンピュータを用いて同じプリンタに印刷する場合に、ユーザは事業主として或いは私的な個人として署名してもよい。署名権能者は組織でもよく、暗号／解読キーが特定のユーザ以外の組織に関連するようにしてもよい。その組織内のユーザは同じ暗号／解読キーを共有するであろう。マシン型のユーザの場合、暗号キーのテーブルが用意され、特定の暗号キーが印刷される書類の性質に基づいて選択される、或いはそのマシンに唯１つの暗号キーが割り当てられてもよい。

【００２６】

続いて、印刷ソース４２２は、ユーザの要求に応じながら、印刷ジョブ要求をプリンタ側要素４２４に送信する（ステップ５０３）。プリンタ側要素４２４は図１Ａ，１Ｂで例示されているに過ぎず、同様な如何なる構成がなされてもよいことに留意を要する。以下のステップで明らかになるように、本発明による印刷プロセスは、印刷ソース４２２及びプリンタ側要素４２４間の双方向通信を含む。多くの印刷プロトコルは本発明を実現するのに必要な形式の通信に適していない。ほとんどの印刷プロトコルはジョブＩＤを例えばメタデータの一部として用意し、メタデータは一般に印刷要求に関連付けられる。

【００２７】

ステップ５０４では、「フィンガープリント」の処理が印刷可能な媒体に施され、印刷可能な媒体のフィンガープリントデータを取得するために、書類が印刷可能な媒体に印刷される。上記の図２及び図３は印刷可能な媒体のフィンガープリントデータを生成するための基本構造及びプロセスを概説している。上記に概説したようにフィンガープリントデータは印刷可能な媒体に固有の構造に基づいている。特許文献１は更なる詳細を説明しているが、それは本発明の本質ではない。

【００２８】

一実施例ではフィンガープリントデータは印刷可能な媒体の予め決められた表面領域をスキャンすることによって取得される。フィンガープリントを出得するための更なる方法は次の文献に開示されている：“TECHNIQUES FOR GENERATIGN AND USING A FINGER PRINT FOR AN ARRICLE”と題する米国特許出願（代理人管理番号015358-010910US）。単なる説明の便宜上、フィンガープリントデータ処理は所定の表面領域をスキャンするこ

とに基づくものとする。“TECHNIQUES FOR GENERATIGN AND USING A FINGERPRINT FOR AN ARRICLE”に開示されているフィンガープリント処理方法（エリア選択のような方法）を本発明は容易に組み込むことができることは理解されるべきである。図１Ａを再び参照するに、制御モジュール１０２はスキャン制御を行うための適切なプログラミングコードや、フィンガープリントデータを取得するプロセス（即ち、フィンガープリンティング）を開始させる処理部１０６ｂを含むことができる。

【００２９】

フィンガープリントデータが取得されると、プリンタ側要素４２４はフィンガープリントデータを印刷ソース４２２に送信する（ステップ５０５）。複数ページの書類の場合、印刷可能な媒体のページ数が決定され、各シートがフィンガープリント処理可能である。この場合、プリンタ側要素４２４はフィンガープリントデータのリストを印刷ソース４２２に送信することができる（バッチ動作モード）。或いは、印刷ソース４２２及びプリンタ側要素４２４は、印刷可能な媒体の複数シートについて、一度にシート１つずつフィンガープリントデータを処理することができる。

【００３０】

ステップ５０６では、印刷ソース４２２は、ステップ５０２で取得したユーザの用意した暗号キーを用いてプリンタ側要素４２４により用意されたフィンガープリントデータの暗号化を実行し、暗号化されたフィンガープリントデータを生成する（a.k.a.サイファーテキスト（平文））。一実施例ではプリンタドライバ４２２ａは暗号化を実行するよう構成可能である。或いは、プリンタドライバ４２２ａは別のマシンに暗号化タスクを実行させてもよい（オフロード）。暗号化アルゴリズムは対称的なアルゴリズムでもよく、その場合暗号化及び解読キーは同じである。暗号化アルゴリズムは非対称でもよく（例えば、公開鍵暗号化）、その場合、一対の暗号鍵が使用され；それらの鍵は公開鍵及び秘密鍵と呼ばれる。一般性を失うことなしに、公開鍵暗号化が使用されるように仮定されてよい。

【００３１】

ステップ５０７では結果として生じた暗号化されたフィンガープリントデータが解読キーと組み合わせられ（暗号解除され）、解読キーはユーザの用意した暗号キーに関連するものである。以下に説明されるように、解読キーは、暗号化されたフィンガープリントデータからフィンガープリントデータを復元するのに使用されてよい。公開鍵／秘密鍵暗号化の場合、ユーザの用意した暗号鍵は秘密鍵として言及される。解読キーは公開鍵として言及される。秘密鍵－公開鍵のペアについての公開鍵認証が信頼できる認証者により発行されると、その公開鍵は、対応する秘密鍵を用いて暗号化データを作成したユーザ（署名する権能を有する者）の信頼できる指標と考えることができる。プリンタドライバ４２２ａは暗号化されたフィンガープリントデータ及び公開キーを、印刷ジョブを構成するデータと共にプリンタ側要素４２４に送信する。或いは、暗号化されたフィンガープリントデータ及び公開鍵はメタデータとして送信されてもよい。

【００３２】

「フィンガープリント情報」なる用語が本発明の説明を更に促すようにここで導入される。フィンガープリント情報は、印刷可能な媒体に移される情報であり（例えば、意刷可能な媒体に印刷される）、以後印刷可能な媒体のフィンガープリントデータを取得するのに使用される。この特定の実施例（図４Ａ及び５Ａ）では、フィンガープリント情報は暗号化されたフィンガープリントデータ及び公開鍵を踏む。フィンガープリント情報は本発明の別の実施例では別様に定義されてもよい。

【００３３】

ステップ５０８ではプリンタ側要素４２４は要求された印刷ジョブサービスを提供するのに必要な処理を実行し、その印刷ジョブは印刷可能な媒体４２６のシートを印刷し、印刷された書類４２６’を生成することを含む。本発明によれば、印刷された書類４２６’はマシン読取可能な情報４０４を含む。印刷可能な媒体への印刷に適したマシン読取可能な情報を用意するためにフィンガープリント情報はエンコードされている。例えばマシン読取可能な情報４０４はフィンガープリント情報をエンコードしているバーコードでもよ

い。この場合、バーコード（例えば、２次元バーコード）は、フィンガープリント情報を含むデータを直接的に表現する；即ち、そのバーコードはフィンガープリント情報を含むデータをエンコードしている。フィンガープリント情報は（例えばバーコードスキャナを利用して）単にそのバーコードを適切にデコードすることで抽出可能である。当然に、フィンガープリント情報をエンコードするために他のエンコード技法を利用して、印刷可能な媒体に印刷することができるコードを生成してもよい。

【００３４】

印刷可能な媒体に印刷されるマシン読取可能な情報を用意する代わりに、単なる２進データであるフィンガープリント情報が、例えば２進表記で又は１６進表記で人により読取可能な形式で印刷可能であることに気付くであろう。当然に、フィンガープリントデータのデータサイズはこの手法を実用不可能にするかもしれない。マシン読取可能な情報は印刷領域によって更に効率化できる。また、フィンガープリントオペレーションを表すマシン読取可能な情報を用いることは、印刷された書類の自動確認を促し、これについては後述される。

【００３５】

印刷された書類４２６’の確認が後続の受領者によって実行可能である。先ず、フィンガープリント情報を抽出するためにマシン読取可能な情報４０４がデコードされる。例えば、マシン読取可能な情報が印刷された書類に印刷されたバーコードである場合、バーコードスキャナを用いてそのバーコードをスキャンし、バーコードをデコードし、フィンガープリント情報を抽出することができる（即ち、この例では暗号化されたフィンガープリントデータ及び公開鍵が使用される。）。ステップ５０７を参照するに、公開鍵は受信した印刷書類の署名権能者を（信用のある認証機関を介して）識別する。平文（a.k.a.プレインテキスト）のフィンガープリントデータを検索するために、公開鍵が暗号化されたフィンガープリントデータに適用される。受信した印刷書類のフィンガープリントを得るためにフィンガープリント処理が実行される。平文のフィンガープリントデータ及びフィンガープリント間の比較結果が一致を示していた場合、受信した印刷書類が本来の書類であり、その書類にマシン読取可能な情報が印刷されていること及びその書類が署名権能者により印刷されたことを受領者は確信する。本プロセスは或るシステムでは自動化可能であり、そのシステムは図１Ａに示されるもののようなフィンガープリント処理要素及びバーコードリーダを利用してよいことが理解されるであろう。

【００３６】

しかしながら、受信した印刷書類の本質的内容がそれを受信する前に変えられていないことを保証する必要がある。例えば印刷書類の中間的な受領者はその書類をこすることでトナーを落とし、記載内容を書き換えることができ（即ち、パリンプセスト(palimpsest)）、最終的な受領者が改変された書類を受けてしまうかもしれない。書類がある種の法的な契約書であった場合、例えば、書類は異なる文言を含むがそれでも同じフィンガープリント及びマシン読取可能な情報を維持するように書き換えられてしまうかもしれない。ハッシュがどのように機能するかに起因して、単にハッシュ値を再スキャン及び検査することで確認を実行することは不可能である。その理由は、再度書類をスキャンしても同じビットマップをおそらくほとんど生成しないからである。従ってかくビットマップをハッシュすることに起因するハッシュ値は一致しないようになる。

【００３７】

図５Ａを参照するに、ステップ５０９が用意されている。プリンタドライバ４２２ａは暗号化されていないフィンガープリントデータ及び印刷書類の画像（印刷画像）をデータ格納部４３２に、印刷ジョブが印刷側要素４２４に送られた時点で又はその近辺で送信する。データ格納部４３２はローカルなストレージでも、遠隔的なストレージ機能部でも、（ローカルな又はリモートの）データベース等でもよい。図６Ａはフィンガープリントデータ及び印刷画像を格納するためのデータ構造を示す。「ハッシュ値」のフィールドは以下に説明される本発明の代替実施例で使用される。

【００３８】

スキャンされた内容を維持することで、データ格納部４３２に格納された印刷書類の画像に対する、受信した印刷書類の内容の視覚的な確認を受領者が行えるようにできる。或いは、自動プロセスが或る照合を実行することもできる；例えば、受信した印刷書類のＯＣＲ（光文字認識）により得られた文字が、記憶済みの書類画像の文字と比較される場合に、テキストの確認が実行されてもよい。受信された印刷書類及び記憶済みの書類画像間の光学的な差について更に別の測定が実行されてもよい。平文のフィンガープリントデータは、データ格納部４３２に対する探索キーとして使用され、格納済みのフィンガープリントデータ及び対応する記憶済み画像を見出すのに使用可能である。

【００３９】

本発明の別の実施例では、格納済みの書類画像の整合性が確認可能である。この例では、ステップ５０７は印刷画像についてハッシュ処理を実行し、コンテンツ確認ハッシュを生成することを更に含む。かくてフィンガープリント情報は、暗号化されたフィンガープリントデータ及び公開鍵に加えてコンテンツ確認ハッシュも含む。このハッシュはＪＰＥＧ、ＴＩＦＦ、ＰＢＭのような或る画像エンコーディングシステム又は同様なエンコーディングシステムに従って印刷されたページ画像の印刷されたビットをエンコードすることで取得可能である。結果のビットストリームはＭＤ５，ＳＨＡ－１のような一方向の暗号化ハッシュ関数を用いて又はそのような様々なハッシュアルゴリズムのどれを用いて処理されてもよい。ステップ５０９ではハッシュはフィンガープリントデータ及び印刷画像と共に図６Ａのデータ構造に格納可能である。

【００４０】

確認の最中に、受信印刷書類に印刷された印のようにエンコードされたフィンガープリント情報から受信されたコンテンツ確認ハッシュは、図６Ａのデータ構造で格納されたハッシュ値と比較可能である。肯定的な比較結果は格納済みの書類画像の整合性を裏付ける。或いはハッシュ値は比較の際に記憶済み書類画像について演算されてもよい。記憶済み書類画像の整合性が確認された場合には、受信した印刷書類及び記憶済み書類画像間の視覚的な比較は、内容を確認するように実行可能である。

【００４１】

図４Ｂ及び５Ｂは上述のプロセスの変形例を示す。図４Ａ及び図５Ａに共通する図４Ｂ中の要素及び図５Ｂ中のステップは同じ参照番号で示される。図４Ａ及び図５Ａに示される例では、マシン読取可能な情報４０４はフィンガープリント情報を直接的にエンコードしている（即ち、エンコードされたフィンガープリントデータ及び公開鍵が用意される。）。代替的に、図４Ｂ及び５Ｂはマシン読取可能な情報４０４ａが識別子をエンコードする例を示し、その識別子は、データ構造中の他のどこかに格納された公開鍵及び暗号化されたフィンガープリントデータでなく、暗号化されたフィンガープリントデータ及び公開鍵にアクセスするために使用される。例えば図６Ｂは複数行に組織されたそのようなデータ構造例を示す。各行は暗号化されたフィンガープリントデータ、解読キー及び書類画像の３つ組を含む。１つのインデックスはデータ構造中の各行を区別する。ハッシュ値のフィールド（図６Ｂには示されていない）は上述した追加的な整合性検査機能をもたらすことができる。

【００４２】

かくて図４Ｂ及び図５Ｂでは適切に構成されたプリンタドライバ４２２ａは、暗号化されたフィンガープリントデータ、解読キー及び書類画像の３つ組を適切なデータ構造で格納する（ステップ５０７ａ）。プリンタドライバ４２２ｂは、そのデータ構造からデータの３つ組に以後アクセスするのに使用可能な探索キー（サーチキー）を取得する。ステップ５０７ｂでは、プリンタドライバ４２２ｂはサーチキーをプリンタ側要素４２４に送信する。例えば図６のデータ構造の場合、サーチキーはデータ構造中の行を見分けるインデックスであり、そのデータ構造に暗号化されたフィンガープリントデータ、解読キー及び書類画像の３つ組が格納されている。ステップ５０８では、サーチキーは適切なマシン読取可能な情報４０４’でエンコード可能であり、その情報は印刷可能な媒体に印刷される。この特定の例ではフィンガープリント情報はサーチキーを含む。

【００４３】
図４Ｂ及び図５Ｂに示される例に従って生成される印刷書類４２６’についての確認手順は、マシン読取可能な情報４０４ａを読み取ること、及びサーチキー（フィンガープリント情報）を取得することを含む。（例えば、図６のデータ構造を指定することで）サーチキーはそのデータ構造からデータの３つ組を抽出するために使用される。この時点で、暗号化されたフィンガープリントデータ及び公開鍵が取得され、上述した手法で確認が進められる。
【００４４】
図１Ａ及び７を参照するに、本発明の別の実施例では、印刷装置１２４はＲＦＩＤ（無線周波数ＩＤ）ライタ１１２を含む。ＲＦＩＤライタ１１２は破線で示されている。同様にＲＦＩＤライタ１１２は代替実施例として図１Ｂの印刷装置１２４ａにも導入可能である。ＲＦＩＤライタ１１２は印刷可能な媒体１２６に埋め込まれたＲＦＩＤタグ７０２にフィンガープリント情報を伝えることができる。従ってこの特定の例では、マシン読取可能な情報はフィンガープリント情報の電子データを含み、その電子データは、フィンガープリント情報を取得するために使用される印刷されたグリフではなく、ＲＦＩＤタグ７０２に格納されている。プリンタ側要素４２４における制御モジュール１０２は、印刷ソース４２２からフィンガープリント情報を受け取ると、ＲＦＩＤライタ１１２を操作し、フィンガープリント情報を埋め込まれたＲＦＩＤタグ７０２に、印刷可能な媒体１２６がＲＦＩＤライタ１１２を通過するような適切な時点で写す。紙のような印刷可能な媒体中に埋め込まれているＲＦＩＤタグに関する技術自体は知られている。ＲＦＩＤタグにデータを伝えるＲＦＩＤ書込装置自体も既知である。
【００４５】
ＲＦＩＤリーダはＲＦＩＤタグからフィンガープリント情報を読み出すように使用可能である。上述したように確認プロセスが進められる。ＲＦＩＤリーダ自体は既知である。
【００４６】
かくて本発明によれば、フィンガープリント情報をエンコードしているマシン読取可能な情報をバーコードその他のグリフの形式で印刷することで、或いはフィンガープリント情報を埋め込まれたＲＦＩＤタグに格納することで、フィンガープリント情報は印刷可能な媒体に移されることが可能である。
【００４７】
図８は印刷可能な媒体のシートに複数のイメージ８２６（例えば、クーポン又は紙幣でさえよい）を印刷する様子を示す。各画像８２６ｘは、各画像に印刷されたマシン読取可能な情報の形式で、或いは埋め込まれたＲＦＩＤタグに格納された電子情報形式でフィンガープリント情報８０４を搬送する。この印刷技術は各シートがＮ（Ｎ＞１）個のコピー画像を有する大きなスケールの印刷に特に有用である。
【００４８】
図２に示されるスキャナ１０６ａを参照するに、ｘ－ｙ方向に移動するように構成されたドライブモータ２０４は、印刷される画像８２６各々の中で印刷媒体８０２の領域に渡ってスキャナを動かすために使用可能である。画像８２６ｘ内の各領域は、その画像についてのフィンガープリントを取得するようにスキャン可能である。印刷可能な媒体の印刷されたシートは各画像に切断するために切断ツールにより更に処理される。
【００４９】
図８は画像の各々全てがフィンガープリント情報８０４を持ち運ぶ必要のない例を示す。この図はいくつかの画像８２６がフィンガープリント情報を有していない様子を示す。この図は更に、各画像８２６ｘのフィンガープリント情報の場所が画像間で異なってよいことも示す。
【００５０】
図８に示されている例は印刷ソース４２２による追加的なプロセスを必要とする。プリンタドライバ４２２ａは更に、シートに印刷される個々の画像数、フィンガープリント情報の場所等のような追加的なコンフィギュレーション情報を取得するように構成される。

コンフィギュレーション情報は、ＧＵＩを介してユーザ４０２から対話式に、コンフィギュレーションファイルから、画像８２６を生成するのに使用されたアプリケーションと共に対話式に、等々の手法により得られてもよい。プリンタドライバ４２２ａはコンフィギュレーション情報をプリンタ側要素４２４に伝えるように更に構成可能である。プリンタ側要素４２４は印刷される各画像８２６ｘの領域でフィンガープリント処理を実行し、各画像についてフィンガープリントデータを生成する。フィンガープリントデータは（例えば用紙のような）シートに固有の構造に基づくことに留意を要する。固有の構造はシートの領域に依存して異なり、フィンガープリント処理される領域各々は、そのフィンガープリント処理される領域に対応する画像に固有のものになる。

【００５１】

プリンタドライバ４２２ａはプリンタ側要素４２４と通信を行って複数のフィンガープリントデータを生成するよう更に構成され、そのフィンガープリントは複数の画像８２６のフィンガープリント処理による結果である。例えば、図５Ａを参照するに、ステップ５０４－５０７は、複数の画像８２６の中でフィンガープリント処理される領域各々について反復可能である。或いは、プロセスはバッチモードでも実行可能であり、その場合画像８２６各々についてのフィンガープリントデータが集められ（ステップ５０４）、複数のフィンガープリントデータが暗号化される印刷ソース４２２に送られる（ステップ５０５，５０６）。暗号化される複数のフィンガープリントデータはステップ５０７に関して印刷側要素４２４に送信可能である。

【００５２】

図８は更に本発明の他の実施例を示すことにも使用され、シート８０２は裏面接着ラベルのような複数のラベル８２６を有し、ラベルは剥がされることも品目に付されることも可能である。各ラベルは上述の例に従って印刷可能である。各ラベルについて、ラベルはフィンガープリント処理可能であり、ラベルのフィンガープリント及び特定用途情報を暗号化して暗号文を生成し、その暗号文は、ラベルに印刷されるマシン読取可能な情報を生成するようにエンコード可能である。そのようなラベルは或る権限のある当局により付され、ラベルがその品目に付されて以来不変である。

【００５３】

本発明の別の実施例では、印刷側要素４２４は、ユーザのディジタル署名に加えて、印刷書類をディジタル的に署名することができる。図４Ｃ及び図５Ｃはこの特定の実施例を示す。図５Ａ－５Ｃの中で共通する図５Ｃ中のステップは、同じ参照番号で表現され、それらは説明済みである。

【００５４】

図４Ｃ，５Ｃ及び９を参照する。ステップ５０４でフィンガープリントデータを取得する印刷側要素４２４に続いて、フィンガープリントデータは、プリンタ側要素に関連するプライベートキーを用いて暗号化される（ステップ５１５）。図９は平文のフィンガープリントデータ９０２、及び暗号化されたフィンガープリントデータ９０４（プリンタ側プライベートイー（K_{EI}）を用いて得られる）を示す。

【００５５】

ステップ５１６では、暗号化されたフィンガープリントデータが、上記の秘密鍵に対応する暗号化されていない公開鍵K_{D1}と共に組み合わせられ、その結果のデータ対９０６が印刷ソース４２２に送信される。上述のコンテンツ確認ハッシュが包含されてもよいことに留意を要する（図９（９－２）の代替的シーケンス中の９０６’には、コンテンツ確認ハッシュＨが含まれている。）。

【００５６】

ステップ５１７では、データ対９０６がプリンタドライバ４２２ａにより、ステップ５０２で得られたユーザの用意した暗号鍵（秘密鍵）を用いて暗号化される。図９はユーザの用意した秘密鍵（K_{E2}）を用いて取得された暗号化されたデータ対９０８を示す。暗号化された結果のデータ対９０８はユーザの秘密鍵に関連する公開鍵（K_{D2}）と共にペアにされ、プリンタ側要素４２４にデータ対９１０として送られ、そのペアはこの特定の

実施例に関するフィンガープリント情報を構成する。プリンタ側要素４２４デの処理はステップ５０８，５０９に関して上述したように進行し、印刷書類４２６’を生成し、その処理はフィンガープリント情報を印刷シート４２６’に、印刷されたマシン読取可能な情報４０４の形式で移すことを含む。

【００５７】

本発明のこの実施例により得られる印刷書類４２６’の確認は、マシン読取可能な情報４０４をデコードすることを含む。デコード処理の結果はデータ対９１０になる。公開鍵K_{D2}は暗号化されたデータ対９０８に適用され、データ対９０６を得る。公開鍵K_{D1}は暗号化されたフィンガープリントデータ９０４に適用され、フィンガープリントデータ９０２を得る。この時点で、フィンガープリントデータ９０２が抽出され、確認プロセスは上述したように進行可能である。

【００５８】

上述のコンテンツ確認ハッシュを用いる代替実施例では、図９（９－２）のシーケンスが適用される。本発明の代替実施例で得られる印刷書類４２６’の確認は、マシン読取可能な情報４０４をデコードすることを含む。デコード処理の結果はデータ対９１０’になる。公開鍵K_{D2}は暗号化された３つ組データ９０８’に適用され、データの３つ組９０６を得る（３つ組は暗号化されたフィンガープリントデータ、公開鍵及びハッシュ値を含む。）。公開鍵K_{D1}は暗号化されたフィンガープリントデータ９０４に適用され、フィンガープリントデータ９０２を得る。この時点で、フィンガープリントデータ９０２及びコンテンツ確認ハッシュＨが抽出され、確認プロセスが上述のように進行可能である。

【００５９】

図９に示される暗号シーケンスの上記の説明は、プリンタ側要素４２４が第１の暗号化を実行し、印刷ソース４２２が第２の暗号化を実行することを述べていた。図９は別の暗号化シーケンスを説明することにも使用可能であり、印刷ソース４２２が第１の暗号化を実行し、プリンタ側要素４２４が第２の暗号化を実行してもよい。この特定の実施例では、（図４Ａ及び５Ａに示される例のように）プリンタ側要素４２４はフィンガープリントデータ９０２を印刷ソース４２２に送信し、後者がユーザの用意した暗号鍵K_{E1}をフィンガープリントデータに適用し、暗号化されたフィンガープリントデータ９０４を生成してもよい。データ対９０６はプリンタ側要素４２４に送信され、プリンタ側要素はプリンタ側の秘密鍵（ＫＥ２）を用いて暗号化し、暗号化されたデータ対９０８を取得してもよい。暗号化されたデータ対９０８はプリンタ側の公開鍵（K_{D2}）とペアにされ、データ対９１０を形成する。最終的にデータ対９１０はエンコードされ、印刷されるマシン読取可能な情報として印刷書類４２６’に移される。

【図面の簡単な説明】

【００６０】

【図１Ａ】本発明の一実施例による印刷装置の要素を示す概略図である。

【図１Ｂ】本発明の別の実施例による印刷装置の要素を示す概略図である。

【図２】図１に示されるスキャン装置１０２の一例を示す概略図である。

【図３】図２のスキャン装置を利用して物品のシグネチャを生成するプロセスを示す上位概念的フローチャートである。

【図４Ａ】本発明の一実施例による印刷要求に関連する要素間の情報の流れを示す上位概念的な表現図である。

【図４Ｂ】本発明の一実施例による印刷要求に関連する要素間の情報の流れを示す上位概念的な表現図である。

【図４Ｃ】本発明の一実施例による印刷要求に関連する要素間の情報の流れを示す上位概念的な表現図である。

【図５Ａ】図４Ａに示される要素間で行われる処理の上位概念的フローチャートである。

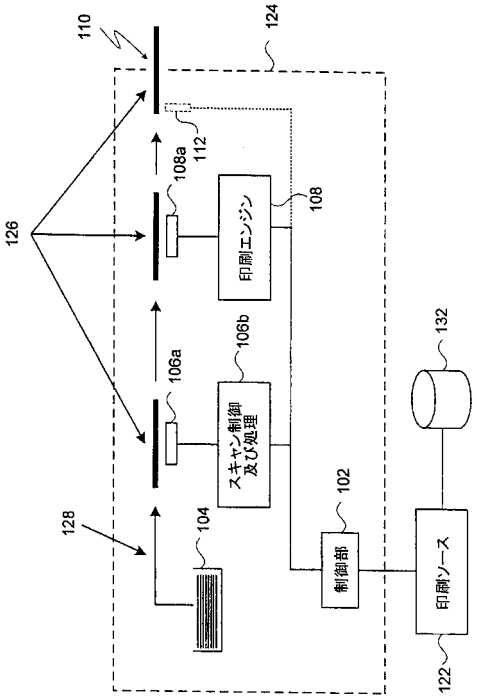
【図５Ｂ】図４Ｂに示される要素間で行われる処理の上位概念的フローチャートである。

【図５Ｃ】図４Ｃに示される要素間で行われる処理の上位概念的フローチャートである。

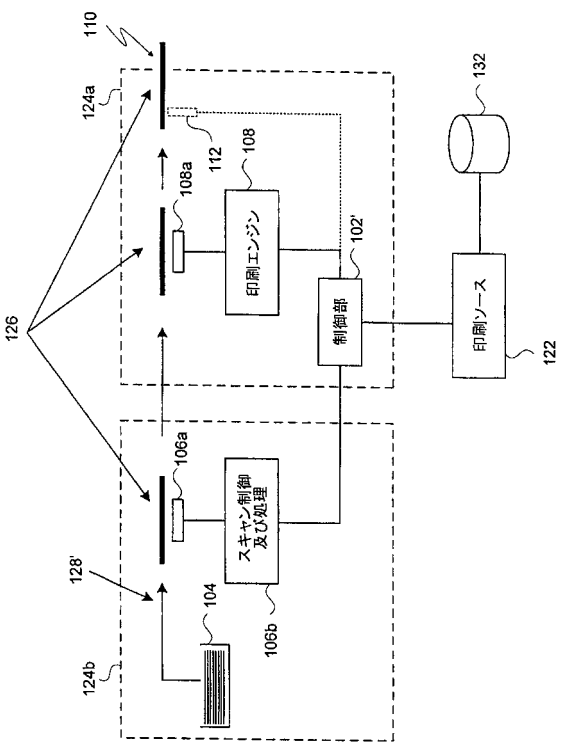
【図６Ａ】本発明の一実施例によるデータを格納するためのデータ構造を示す図である。

【図６Ｂ】本発明の一実施例によるデータを格納するためのデータ構造を示す図である。
【図７】ＲＦＩＤタグを埋め込まれた印刷可能な媒体のシートを示す図である。
【図８】本発明の一実施例により印刷可能な媒体のシートに複数のイメージを印刷する様子を示す図である。
【図９】本発明の一実施例による暗号化シーケンスを示す図である。
【符号の説明】
【００６１】
１０２　制御部
１０４　ソース
１０６ａ　スキャナ
１０６ｂ　処理部
１０８　印刷要素
１１０　末端
１１２　ＲＦＩＤライタ
１２２　印刷ソース
１２４　印刷装置
１２６　印刷媒体
１３２　データベースサブシステム

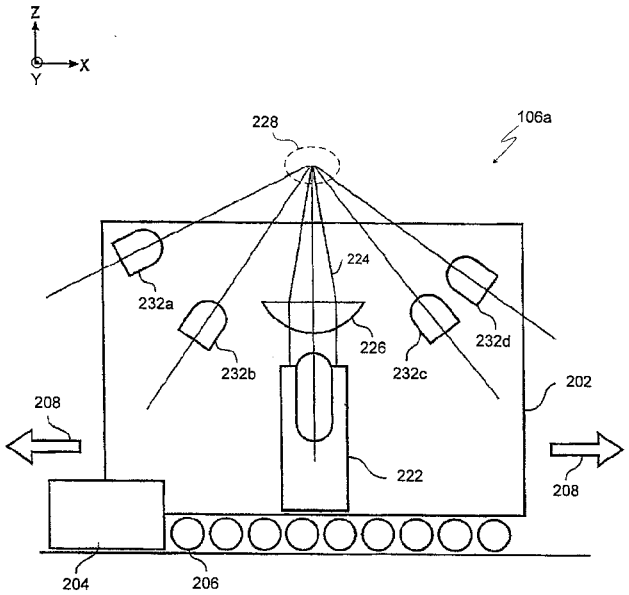
【図１Ａ】



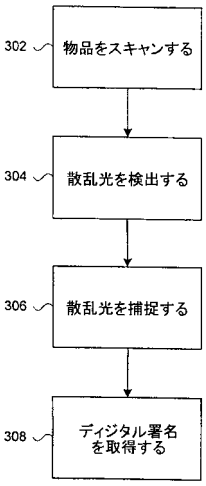
【図１Ｂ】



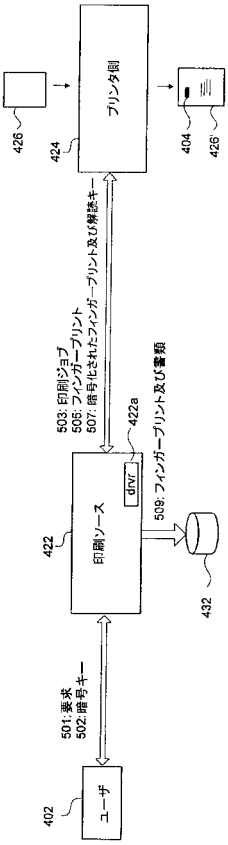
【図２】


Z
X
Y
228
106a
224
232a
232b
226
232c
232d
202
208
208
222
204
206

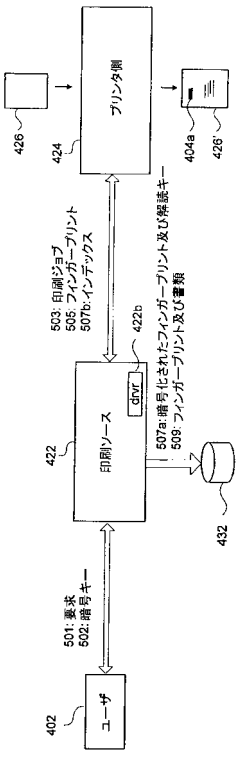
【図３】


302
物品をスキャンする
304
散乱光を検出する
306
散乱光を捕捉する
308
ディジタル署名を取得する

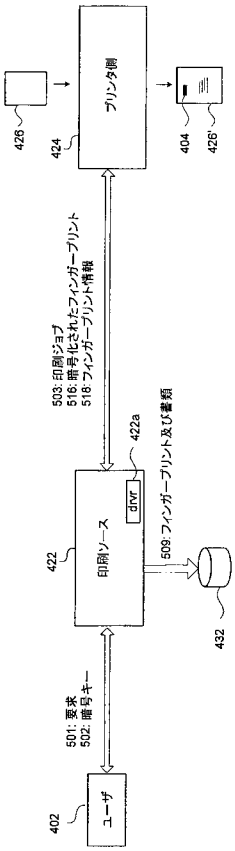
【図４Ａ】


プリンタ側
426
424
404
426
503: 印刷ジョブ
505: フィンガープリント
507: 暗号化されたフィンガープリント及び解読キー
422a
dvr
509: フィンガープリント及び書類
422
印刷ソース
432
501: 要求
502: 暗号キー
402
ユーザ

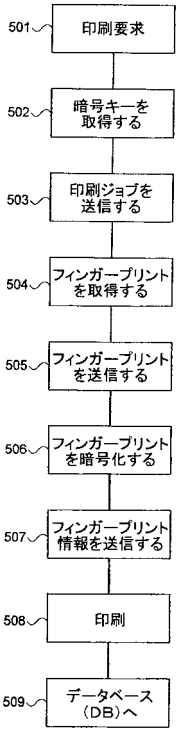
【図４Ｂ】


プリンタ側
426
424
404a
426
503: 印刷ジョブ
505: フィンガープリント
507b: インデックス
422b
dvr
507a: 暗号化されたフィンガープリント及び解読キー
509: フィンガープリント及び書類
422
印刷ソース
432
501: 要求
502: 暗号キー
402
ユーザ

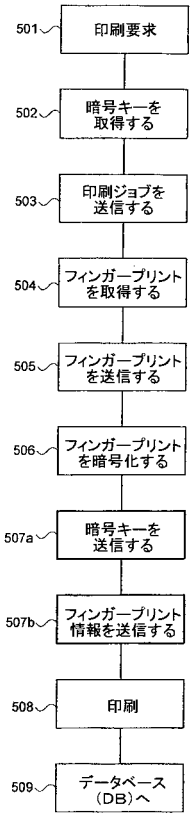
【図４Ｃ】



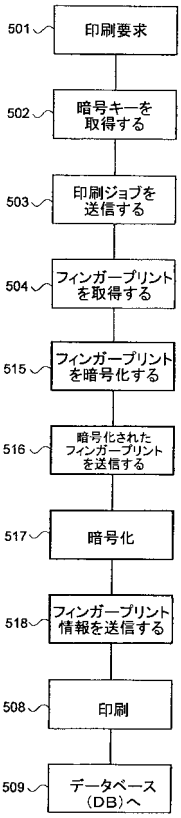
【図５Ａ】



【図５Ｂ】



【図５Ｃ】



【図６Ａ】

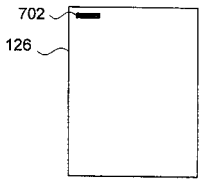
フィンガープリント	ハッシュ値	書類画像
.....	.....	.....

【図６Ｂ】

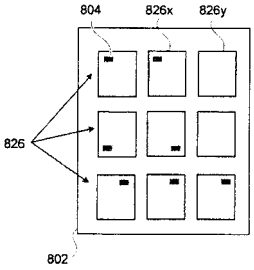
index

	暗号化されたフィンガープリント	解読キー	ハッシュ値	書類画像
1				
2				
3				
4				
	.....	.....	.....	.....

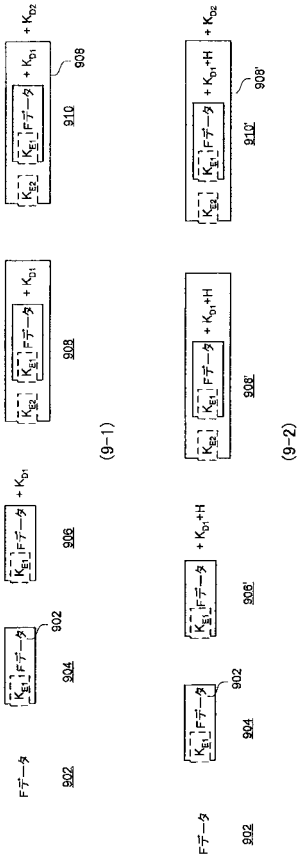
【図７】



【図８】



【図９】



フロントページの続き

(72)発明者　ステフェン　ウェイル
アメリカ合衆国，カリフォルニア　９４０２５－７０５４，メンロ・パーク，サンド・ヒル・ロード　２８８２番，スイート　１１５　リコー　イノベーション　インク内

Ｆターム(参考) 2C187 AC07 AD04 AE07 BF34 CC08 GD06
5B021 BB09 LL07 NN18
5B057 AA11 CA12 CA16 CB12 CB16 CB19 CE08 CG07
5C076 AA14 AA40 BA01 BA06
5J104 AA08 LA01 NA12 PA07 PA14