(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2006-287587
(P2006-287587A)
(43)公開日　平成18年10月19日(2006.10.19)

(51)Int.Cl.			F I			テーマコード（参考）
H04N	1/387	(2006.01)	H04N	1/387		5B057
G06T	1/00	(2006.01)	G06T	1/00	500B	5C076
G09C	1/00	(2006.01)	G09C	1/00	660D	5C077
G09C	5/00	(2006.01)	G09C	5/00		5J104
H04N	1/40	(2006.01)	H04N	1/40	Z	

審査請求 未請求　請求項の数 11　ＯＬ　（全 13 頁）

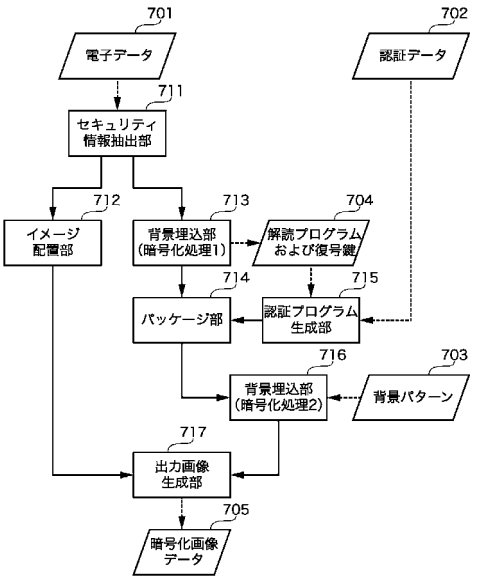
(21)出願番号　特願2005-104362 (P2005-104362)
(22)出願日　平成17年3月31日 (2005.3.31)

(71)出願人　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　鵜沢　充
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】情報処理装置およびその方法

(57)【要約】　（修正有）
【課題】情報の開示が認証システム、セキュリティシステムなどに依存しない文書への情報埋め込み方法を提供する。
【解決手段】セキュリティ情報抽出部711は、電子データ701をセキュリティ情報と非セキュリティ情報に分離する。イメージ配置部712は、非セキュリティ情報を紙面に配置した可読画像データに変換する。暗号化処理部713は、セキュリティ情報を暗号化する。認証プログラム生成部715は、認証データ702により認証を実行する認証プログラムを生成する。パッケージ部714は、暗号化情報および認証プログラムをパッケージ化する。背景埋込部716は、パッケージデータを背景パターン703に埋め込んだ背景画像データを作成する。出力画像生成部717は、背景画像データと可読画像データを合成して暗号化画像データ705を生成する。
【選択図】図５



【特許請求の範囲】
【請求項１】
情報処理装置を利用して電子データを画像データに変換する情報処理方法であって、
電子データを入力し、
前記電子データからセキュリティ情報と非セキュリティ情報を分離し、
前記セキュリティ情報を暗号化し、
認証データを入力し、
前記暗号化したセキュリティ情報、並びに、前記認証データおよび前記暗号化に対応する復号プログラムを含む認証プログラムをパッケージ化し、
前記パッケージ化したデータを背景パターンに埋め込み、
前記非セキュリティ情報を可読画像データに変換し、
前記背景パターンと前記可読画像データを合成することを特徴とする情報処理方法。
【請求項２】
さらに、前記合成したデータを記録媒体に印刷することを特徴とする請求項1に記載された情報処理方法。
【請求項３】
前記埋め込みは、前記合成後、前記可読画像データの画像に重ならない位置に前記パッケージ化したデータを埋め込むことを特徴とする請求項1または請求項2に記載された情報処理方法。
【請求項４】
さらに、前記可読画像データの配置、および、前記パッケージ化したデータの特性に基づき、前記埋め込みの方法を選択することを特徴とする請求項1または請求項2に記載された情報処理方法。
【請求項５】
情報処理装置を利用して文書に埋め込まれた情報を抽出する情報処理方法であって、
文書画像を入力し、
前記文書画像に埋め込まれた第一の情報を抽出し、
認証データを入力し、
前記認証データを入力データとして、前記第一の情報に含まれる認証プログラムを実行し、前記第一の情報に含まれる第二の情報を抽出することを特徴とする情報処理方法。
【請求項６】
前記認証プログラムは復号プログラムを含み、前記認証データによる認証に成功した場合、前記復号プログラムを実行して、前記第一の情報に含まれる暗号化された前記第二の情報を復号することを特徴とする請求項5に記載された情報処理方法。
【請求項７】
さらに、前記第二の情報を記録媒体に印刷することを特徴とする請求項5または請求項6に記載された情報処理方法。
【請求項８】
情報処理装置を制御して、請求項1から請求項7の何れかに記載された情報処理を実現することを特徴とするプログラム。
【請求項９】
請求項8に記載されたプログラムが記録されたことを特徴とする記録媒体。
【請求項１０】
電子データを画像データに変換する情報処理装置であって、
電子データを入力する第一の入力手段と、
前記電子データからセキュリティ情報と非セキュリティ情報を分離する分離手段と、
前記セキュリティ情報を暗号化する暗号化手段と、
認証データを入力する第二の入力手段と、
前記暗号化手段によって暗号化されたセキュリティ情報、並びに、前記認証データおよび前記暗号化に対応する復号プログラムを含む認証プログラムをパッケージ化するパッケ

ージ手段と、
前記パッケージ手段によりパッケージ化されたデータを背景パターンに埋め込む埋込手段と、
前記非セキュリティ情報を可読画像データに変換する変換手段と、
前記背景パターンと前記可読画像データを合成する合成手段とを有することを特徴とする情報処理装置。
【請求項１１】
文書に埋め込まれた情報を抽出する情報処理装置であって、
文書画像を入力する第一の入力手段と、
前記文書画像に埋め込まれた第一の情報を抽出する第一の抽出手段と、
認証データを入力する第二の入力手段と、
前記認証データを入力データとして、前記第一の情報に含まれる認証プログラムを実行し、前記第一の情報に含まれる第二の情報を抽出する第二の抽出手段とを有することを特徴とする情報処理装置。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は情報処理装置およびその方法に関し、例えば、文書へ情報を埋め込むための情報処理に関する。
【背景技術】
【０００２】
近年、プライバシ保護、企業機密の漏洩防止といったセキュリティに関する意識の高まりに伴い、例えば文書に記録された機密内容を保護し、紙によって情報を伝達する際は、特定の者だけがその情報にアクセスできるようなシステムが望まれている。このようなシステムによれば、文書に記録された情報が第三者の目に触れることで不用意に漏洩することを防止することができる。
【０００３】
文書に埋め込まれた情報を解読するには、文書に記録された情報の開示を判断する公開鍵インフラストラクチャ(Public Key Infrastructure: PKI)サーバ、もしくは、認証サーバ、それに、暗号化された情報を解読する解読エンジンが必須である。
【０００４】
例えば、暗号化された電子情報は、暗号化に使用した鍵情報がなければ解読（復号）することができない。言い換えれば、鍵をもつこと自体が認証処理になる。これは、電子情報の暗号化は、電子情報自体が不変であり、鍵さえあればいつでも確実に復号することができるからである。
【０００５】
一方、文書に情報を埋め込む場合は、紙自体が変化に富む物理媒体であるため、周期性をもつパターンによって、できるだけ耐性をもたせた埋め込み方法が採用される。つまり、埋め込んだ情報を正確に検出、解析、認識、抽出することに主眼が置かれている。
【０００６】
ところで、ネットワーク上で扱うことが前提の電子データの電子署名はサーバで管理する方が簡易である。一方、紙のような持ち運び可能な物理媒体における認証は、ネットワークを介さないサーバレスシステムの方が便利である。機密情報が埋め込まれた文書を読み込むシステムが、セキュリティ情報へアクセスする手段を有し、認証された特定者が機密情報へアクセスする、というサーバレスシステムが開示されている（例えば、特許文献1）。
【０００７】
しかし、特許文献1に開示されたようなサーバレスシステムを実現する場合、文書に埋め込む情報は、その認証システム、セキュリティシステムに依存する。つまり、文書に情報を埋め込み、それを開示するようなサーバレスシステムにおいて、あるシステムを前提

に埋め込んだ情報は、同じシステムがない場所では開示することができない。
【０００８】
【特許文献１】特開2004-058410公報
【発明の開示】
【発明が解決しようとする課題】
【０００９】
本発明は、情報の開示が認証システム、セキュリティシステムなどに依存しない、文書への情報埋め込み方法を提供することを目的とする。
【００１０】
また、文書に埋め込んだ情報の耐性を保ちつつ、より多くの情報を埋め込むことを他の目的とする。
【課題を解決するための手段】
【００１１】
本発明は、前記の目的を達成する一手段として、以下の構成を備える。
【００１２】
本発明は、電子データを画像データに変換する際に、電子データを入力し、電子データからセキュリティ情報と非セキュリティ情報を分離し、セキュリティ情報を暗号化し、認証データを入力し、暗号化したセキュリティ情報、並びに、認証データおよび暗号化に対応する復号プログラムを含む認証プログラムをパッケージ化し、パッケージ化したデータを背景パターンに埋め込み、非セキュリティ情報を可読画像データに変換し、背景パターンと可読画像データを合成することを特徴とする。
【００１３】
好ましくは、さらに、可読画像データの配置、および、パッケージ化したデータの特性に基づき、埋め込みの方法を選択する。
【００１４】
また、文書に埋め込まれた情報を抽出する際に、文書画像を入力し、文書画像に埋め込まれた第一の情報を抽出し、認証データを入力し、認証データを入力データとして、第一の情報に含まれる認証プログラムを実行し、第一の情報に含まれる第二の情報を抽出することを特徴とする。
【発明の効果】
【００１５】
本発明によれば、情報の開示が認証システム、セキュリティシステムなどに依存しない、文書への情報埋め込み方法を提供することができる。
【００１６】
また、文書に埋め込んだ情報の耐性を保ちつつ、より多くの情報を埋め込むことができる。
【発明を実施するための最良の形態】
【００１７】
以下、本発明の実施例を図面を参照して詳細に説明する。
【実施例１】
【００１８】
図1は実施例のシステムの全体像を示す概念図である。
【００１９】
図1において、ドメインAには複合機(MFP)102が所属し、ドメインBにはMFP 103が所属し、ドメインCにはクライアントPC 104、スキャナ105およびプリンタ106が所属する。なお、MFP 102および103、並びに、クライアントPC 104は、後述する処理を実行する。また、各ドメインはそれぞれオフィスなどの区分で、互いにネットワーク環境が異なり、ネットワークを介した通信はできない。
【００２０】
本実施例の処理対象の文書100、101は、例えば銀行口座の開設申込書、保険契約に関す

る書類といった、個人情報に関する書類、または、企業内の機密文書などが想定される。文書100、101の紙面には、セキュリティ上、表示してよい内容のみが可視表示され、プライバシに関する情報、もしくは、機密情報は例えば暗号化して電子透かしパターンとして紙面の画像に埋め込まれている。なお、以下では、プライバシに関する情報、機密情報などをまとめて「セキュリティ情報」と呼ぶ。

【００２１】

例えば、ドメインAでは、MFP 102により、機密情報を埋め込んだ文書100、101を作成する。文書100、101はドメインB（またはC）に送られて、ドメインBでMFP 103により文書100、101の情報が開示される。あるいは、ドメインCでクライアントPC 104により文書100、101の情報が開示される。

【００２２】

図2は実施例の処理対象の文書400について詳細を説明する図である。

【００２３】

文書400は、図2(a)に示す紙面に表示された情報501～508と、図2(b)に示す電子透かしなどで埋め込まれた情報411～413を備える。埋め込まれた情報には、認証プログラムインストーラ411、認証プログラム412、および、暗号化情報413がある。暗号化情報413を解読する鍵情報および復号プログラムは認証プログラム412に備わる。従って、例えばMFP 102で作成された文書100、101は、MFP 103において、原稿画像に埋め込まれた認証プリグラム412によって承認された場合、暗号化情報413を復号して開示することが可能である。

【００２４】

以上、本実施例のシステムの全体像を概略的に説明したが、以下、具体的な実現方法を説明する。

【００２５】

［装置の構成］

図3は実施例のMFP 102、103の構成例を示すブロック図である。なお、クライアントPC 104も、スキャナ105およびプリンタ106との接続により、ほぼ同様の構成をとるものとする。

【００２６】

MFP 102(103)は、ROM 202またはハードディスクなどの大容量の記憶装置(HD)210に記憶されたソフトウェアを実行するCPU 201を備える。CPU 201は、RAM 203をワークメモリとして、システムバス213に接続される後述する各部を総括的に制御する。また、HD 210は、ディスクコントローラ(DKC) 209を介して制御され、後述する様々なデータの格納、画像データなどの一時記憶にも利用される。

【００２７】

外部入力コントローラ(PANELC) 205は、各種ボタンまたはタッチパネルを備えるMFPの操作パネル206からユーザの指示を入力する。ディスプレイコントローラ(DISPC) 207は、例えば液晶ディスプレイなどで構成されるディスプレイ208の表示を制御する。

【００２８】

ネットワークインタフェイスカード(NIC) 204は、ローカルエリアネットワーク(LAN) 214を介して、同じドメイン内の他のネットワーク機器またはサーバと双方向にデータをやり取りする。

【００２９】

プリンタ211は、電子写真方式またはインクジェット方式などの記録方式により記録紙に画像を印刷する。スキャナ212は、原稿画像を読み取る。多くの場合、スキャナ212には、オプションとして図示しないオートドキュメントフィーダ(ADF)が装着され、複数枚の原稿の画像を連続して読み取ることができる。

【００３０】

［処理の概要］

次に、上記のMFPを用いて図2に示す情報を埋め込んだ画像を生成する方法を説明する。

【００３１】

図4はセキュリティ情報をもつ電子データから、セキュリティ情報を暗号化して埋め込んだ文書を作成する処理を示すフローチャートで、CPU 201によって実行される処理である。

【００３２】

ユーザは、ディスプレイ208に表示される情報を参照して操作パネル206を操作し、文書化する電子データ（HD 210の所定の記憶領域もしくはLAN 214に接続された他のデータベース（不図示）に格納されている）の取得を指示する。CPU 201は、指示された電子データを取得してRAM 203に格納する(S301)。

【００３３】

次に、ユーザは、操作パネル206を操作して、取得した電子データの暗号化出力を指示し、暗号を解読するためのパスワードまたはID（以下「認証データ」と呼ぶ）を設定する。CPU 201は、暗号化出力の指示、認証データを入力し(S302)、暗号化出力用のプログラムをROM 202からRAM 203にロードして、取得した電子データを処理して、セキュリティ情報を図2に示す暗号化された情報413として埋め込んだ画像（以下「暗号化画像」と呼ぶ）を生成する(S303)。そして、CPU 201は、プリンタ211により、生成した暗号化画像を記録紙に印刷して文書を作成する(S304)。

【００３４】

以上の処理により、電子データのセキュリティ情報が暗号化されて埋め込まれた文書100、101が作成される。ユーザは、この文書100、101を任意の方法で他のドメインへ送付する。

【００３５】

［電子データの暗号化］

図5は電子データを暗号化する処理の流れを示す図である。なお、図5に示すセキュリティ情報抽出部711、イメージ配置部712、暗号化部713、認証プログラム生成部715、パッケージ部714、背景埋込部716、出力画像生成部717は、それぞれRAM 203にロードされ実行される暗号化出力用のプログラムのモジュールである。

【００３６】

セキュリティ情報抽出部711は、ステップS301で取得した電子データ701を入力して、電子データ701をセキュリティ情報と非セキュリティ情報に分離して、セキュリティ情報を暗号化部713へ、非セキュリティ情報をイメージ配置部712へそれぞれ出力する。

【００３７】

図6は電子データ701の一例を示す図である。電子データ701は、図6に示す例では、XML (Extensible Markup Language)で表現され、符号502～510で示す文書を表現する複数の情報ブロックから構成されている。なお、セキュリティ情報を考慮せずに、電子データ701をディスプレイ206に表示した場合、ブロック情報502～510によって図7に示すような表示が得られる。

【００３８】

各情報ブロック502～510には、ブロックごとにセキュリティレベルがメタ情報521～529として設定されている。セキュリティ情報抽出部701は、メタ情報521～529から各情報ブロック502～510のセキュリティレベルを判断し、情報ブロックごとにセキュリティ情報と非セキュリティ情報に分離する。なお、以下では、メタ情報(security level)によって表されるセキュリティレベルが「1」以上のものをセキュリティ情報として扱う例を説明するが、セキュリティ情報と非セキュリティ情報を区別するセキュリティレベルは任意に設定することができる。

【００３９】

イメージ配置部712は、入力される非セキュリティ情報をそれぞれ紙面の矩形領域に配置した画像データ（以下「可読画像データ」と呼ぶ）に変換する。図8は非セキュリティ情報を可読画像データに変換する例を示す図である。図8(a)に示す、セキュリティ情報抽出部711によって抽出された非セキュリティ情報502、503、505、509、510は、イメージ配置部712によって、その画像サイズなどが整えられた後、紙面上で重ならないように図8(b

)に示すように配置される。

【００４０】

一方、暗号化処理部713は、入力されるセキュリティ情報を例えば予め乱数から生成した鍵を用いて暗号化する。この暗号化とは、文字、記号、ビット列を鍵と呼ぶパラメータを用いて、所定の手順に従い、異なる文字、記号、ビット列に変換する操作である。暗号化情報は、暗号化に用いた鍵を知らなければ復号できない。なお、暗号化処理部713で用いる暗号化アルゴリズムは、暗号鍵と復号鍵が同一の対称アルゴリズムでも、暗号鍵と復号鍵が異なる非対称アルゴリズムでもよく、様々なアルゴリズムから選択可能である。ここでは、セキュリティ上、最も安全と判断し得る公知の手法を用いることにする。なお、使用する暗号化アルゴリズムをユーザが選択することも可能である。

【００４１】

暗号化処理部713は、暗号化情報をパッケージ部714へ出力し、暗号化に対応する復号プログラムおよび復号鍵704を認証プログラム生成部715へ出力する。

【００４２】

認証プログラム生成部713は、復号プログラムおよび復号鍵704と、ステップS302でユーザが入力した認証データ702を入力し、認証データ702により認証を実行する認証プログラムを生成し、復号鍵を用いる復号プログラムを含む認証プログラムをパッケージ部714へ出力する。この認証プログラムは、認証データにより認証に成功した場合、復号鍵を用いる復号プログラムの実行を可能にするものである。

【００４３】

パッケージ部714は、入力される暗号化情報および認証プログラムと、認証プログラムインストーラ（およびアンインストーラ）をパッケージ化し、パッケージデータを背景埋込部716へ出力する。

【００４４】

背景埋込部716は、パッケージデータおよび背景パターン703を入力し、パッケージデータを、例えば周期性をもつ電子透かし手法など耐性の高い方法で背景パターン703に埋め込んだ背景画像データを作成し、背景画像データを出力画像生成部717に出力する。パッケージデータを電子透かしとして背景パターンに埋め込む際、イメージ配置部712によって生成された可読画像データを取得し、非セキュリティ情報と重ならないように電子透かしを埋め込めば、より多くの情報を高い耐性で埋め込むことができる。また、背景パターン703は、複数の背景パターンの中から選択するようにしてもよいし、ユーザが選択するようにしてもよい。

【００４５】

出力画像生成部717は、入力される背景画像データと可読画像データを合成して、暗号化画像データ705を生成する。

【００４６】

以上の処理により、入力電子データから、セキュリティ情報を埋め込んだ背景パターンに可読画像データが重畳された文書100、101用の暗号化画像データ705が生成される。

【００４７】

［暗号化画像の復号］

次に、文書100、101に埋め込まれたセキュリティ情報を復号して開示する方法を説明する。

【００４８】

図9は背景パターンに電子透かしとして埋め込まれたセキュリティ情報を復号して開示する処理例を示すフローチャートで、CPU 201によって実行される処理である。

【００４９】

文書100（または101）を受信したドメインのユーザは、スキャナ212の読取部に文書100（または101）を載置し、MFPの操作パネル205を操作して、文書に埋め込まれた情報の開示を指示する。CPU 201は、スキャナ212に文書画像を読み取らせ、スキャナ212が出力する画像信号を例えば600dpiの画像データに変換する(S401)。

【００５０】
次に、CPU 201は、解読プログラムをROM 202（またはHD 210）からRAM 203にロードして、文書から読み取った画像データを入力として電子透かしの抽出プログラムを実行する。抽出プログラムは、画像データを解析して、文書画像に電子透かしが埋め込まれているか否かを判定する(S402)。なお、抽出プログラムは複数あってもよく、複数の抽出プログラムを実行した場合、以降は、スキャナ212で読み取った文書画像に埋め込まれている電子透かしを検出可能な抽出プログラムが機能することになる。
【００５１】
CPU 201は、文書画像から電子透かしが検出されない場合は処理をステップS412へ進め、ディスプレイ208に文書に埋め込まれた情報の解読が不可、または、文書に情報が埋め込まれていない旨をユーザに通知する。一方、文書画像から電子透かしが検出された場合は、抽出プログラムにより電子透かしを抽出し、解釈して、文書に埋め込まれたデータを抽出してRAM 203（またはHD 210）に一時記憶する(S403)。
【００５２】
次に、CPU 201は、RAM 203に記憶したデータに認証プログラムが含まれているか否かを判定し(S404)、含まれていなければ処理をステップS412へ進め、ディスプレイ208に文書に埋め込まれた情報を開示するための認証が不可能である旨をユーザに通知する。一方、認証プログラムが含まれている場合は、当該認証プログラムを実行するか否かをユーザに判断させるために、ディスプレイ208に認証を行うか否かの旨を表示する(S405)。
【００５３】
ユーザが操作パネル206を操作して認証の実行を指示すると、CPU 201は、ディスプレイ208に認証データ（パスワードまたはID）の入力を要求する旨を表示する(S406)。ユーザが操作パネル206を操作して認証データを入力すると、CPU 201は、認証プログラムをインストールし、入力された認証データを入力データとして認証プログラムを起動する(S407)。なお、認証がキャンセルされた場合、CPU 201は、処理を終了する。
【００５４】
認証プログラムは、保持する認証データに一致するデータが入力されたか否かを判定し(S408)、一致（認証成功）した場合は保持する復号プログラムを起動し、RAM 203に格納されたデータのうち暗号化情報の部分（図2(b)に示す暗号化情報413）を復号する(S409)。他方、認証に失敗した場合、CPU 201は、処理をステップS411に進める。
【００５５】
復号された情報はRAM 203へ一時記憶され、CPU 201は、復号が終了するとRAM 203に一時記憶された情報をプリンタ211で印刷（またはディスプレイ208に表示）してセキュリティ情報を開示する(S410)。
【００５６】
セキュリティ情報の開示後、または、認証に失敗した場合、CPU 201は、認証プログラムをアンインストールし(S411)、RAM 203、HD 210などに一時記憶したデータを削除して(S412)、処理を終了する。
【００５７】
このように、暗号化情報とともに認証プログラムを文書に埋め込むので、認証システムが異なるシステム間でも、セキュリティ情報の開示が可能になる。さらに、非セキュリティ情報と重ならないように電子透かしを埋め込むことで、より多くの情報を高い耐性で埋め込むことができる。
【実施例２】
【００５８】
以下、本発明にかかる実施例2を説明する。なお、実施例2において、実施例1と略同様の構成については、同一符号を付して、その詳細説明を省略する。
【００５９】
実施例1の背景埋込部716（図5参照）716は、パッケージ部714によりパッケージされたデータを、例えば、電子透かしとして周期性をもつノイズパターンに埋め込むものである

。一方、文書に情報を埋め込む方式として、文書上の可読情報（実施例では非セキュリティ情報）の特徴を生かした方式が数多く研究開発されている。例えば、文書の文字と文字の間隔を操作して情報を埋め込む方法、また、図形が描かれている場合は図形を直線近似し、その近似精度に情報を埋め込む方法などがある。

【００６０】

図10は実施例2における電子データを暗号化する処理の流れを示す図である。なお、図10に示す情報埋込方法選択部1001、情報埋込部1002は、それぞれRAM 203にロードされ実行される暗号化出力用のプログラムのモジュールである。

【００６１】

情報埋込方法選択部1001は、セキュリティ情報と非セキュリティ情報を、紙面の限られた空間に、耐性を保ちつつ埋め込むために、イメージ配置部712によって生成される可読画像データの配置と、パッケージ部714によって生成されるパッケージデータの特性から、埋め込み方法を選択する。情報埋込部1002は、選択された埋め込み方法により、イメージ配置部712が出力する可読画像データに、パッケージ部714が出力するパッケージデータを埋め込み、暗号化画像データ705として出力する。

【００６２】

このような構成によれば、例えば、パッケージデータの特性が文字の多い文章であれば、文字と文字の間隔を利用して情報を埋め込む方式を選択し、文字と文字の間にパッケージデータを埋め込んだ文書を作成する。また、パッケージデータの特性が情報量が少ないであれば、二次元コードによってパッケージデータを耐性をもって埋め込む、といったことが可能になる。なお、実施例では、認証自体は文書に埋め込まれた認証プログラムを用いて行う。従って、情報を開示するシステムが、文書に埋め込まれた情報を抽出、解析する抽出プログラムを保有することで、ある特定のドメインにのみセキュリティ情報を開示可能なシステムを実現することができる。

【００６３】

［他の実施例］

なお、本発明は、複数の機器（例えばホストコンピュータ、インタフェイス機器、リーダ、プリンタなど）から構成されるシステムに適用しても、一つの機器からなる装置（例えば、複写機、ファクシミリ装置など）に適用してもよい。

【００６４】

また、本発明の目的は、前述した実施例の機能を実現するソフトウェアのプログラムコードを記録した記憶媒体（または記録媒体）を、システムあるいは装置に供給し、そのシステムあるいは装置のコンピュータ（またはCPUやMPU）が記憶媒体に格納されたプログラムコードを読み出し実行することによっても、達成されることは言うまでもない。この場合、記憶媒体から読み出されたプログラムコード自体が前述した実施例の機能を実現することになり、そのプログラムコードを記憶した記憶媒体は本発明を構成することになる。また、コンピュータが読み出したプログラムコードを実行することにより、前述した実施例の機能が実現されるだけでなく、そのプログラムコードの指示に基づき、コンピュータ上で稼働しているオペレーティングシステム(OS)などが実際の処理の一部または全部を行い、その処理によって前述した実施例の機能が実現される場合も含まれることは言うまでもない。

【００６５】

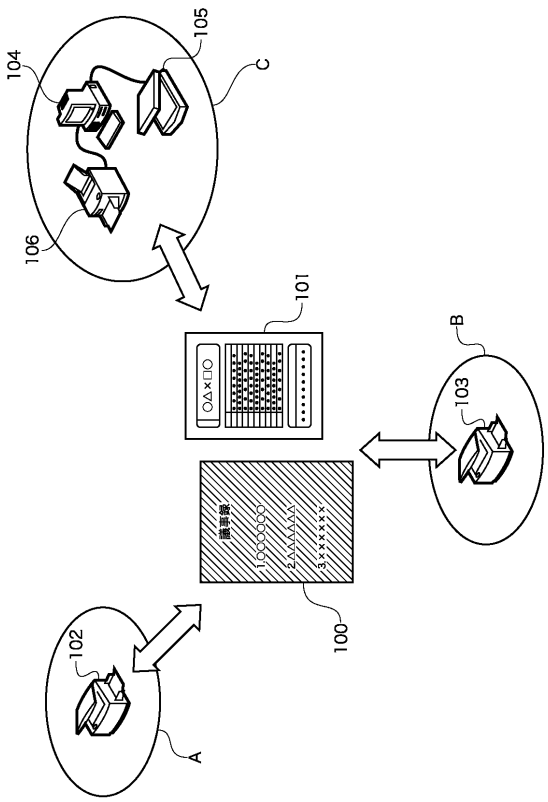
さらに、記憶媒体から読み出されたプログラムコードが、コンピュータに挿入された機能拡張カードやコンピュータに接続された機能拡張ユニットに備わるメモリに書込まれた後、そのプログラムコードの指示に基づき、その機能拡張カードや機能拡張ユニットに備わるCPUなどが実際の処理の一部または全部を行い、その処理によって前述した実施例の機能が実現される場合も含まれることは言うまでもない。

【００６６】

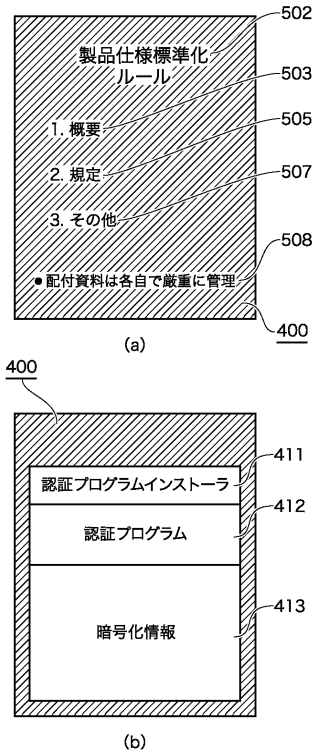
本発明を上記記憶媒体に適用する場合、その記憶媒体には、先に説明したフローチャートに対応するプログラムコードが格納されることになる。

【図面の簡単な説明】
【００６７】
【図１】実施例のシステムの全体像を示す概念図、
【図２】実施例の処理対象の文書について詳細を説明する図、
【図３】MFPの構成例を示すブロック図、
【図４】セキュリティ情報をもつ電子データから、セキュリティ情報を暗号化して埋め込んだ文書を作成する処理を示すフローチャート、
【図５】電子データを暗号化する処理の流れを示す図、
【図６】電子データの一例を示す図、
【図７】電子データをディスプレイに表示した場合の表示例を示す図、
【図８】非セキュリティ情報を可読画像データに変換する例を示す図、
【図９】背景パターンに電子透かしとして埋め込まれたセキュリティ情報を復号して開示する処理例を示すフローチャート、
【図１０】実施例2における電子データを暗号化する処理の流れを示す図である。

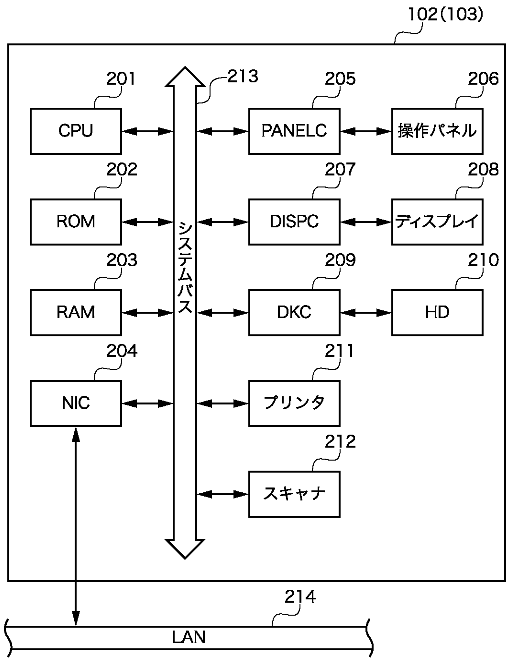
【図１】



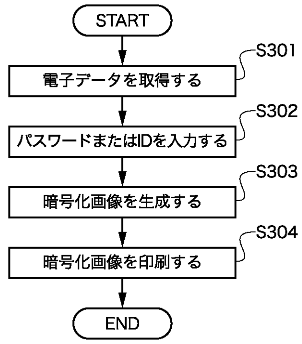
【図２】



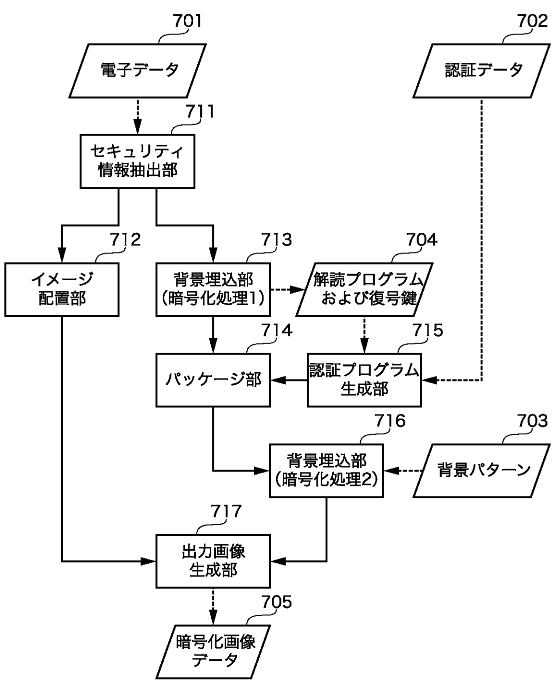
【図３】


102(103)
201
CPU
213
205
PANELC
206
操作パネル
202
ROM
207
DISPC
208
ディスプレイ
203
RAM
システムバス
209
DKC
210
HD
204
NIC
211
プリンタ
212
スキャナ
214
LAN

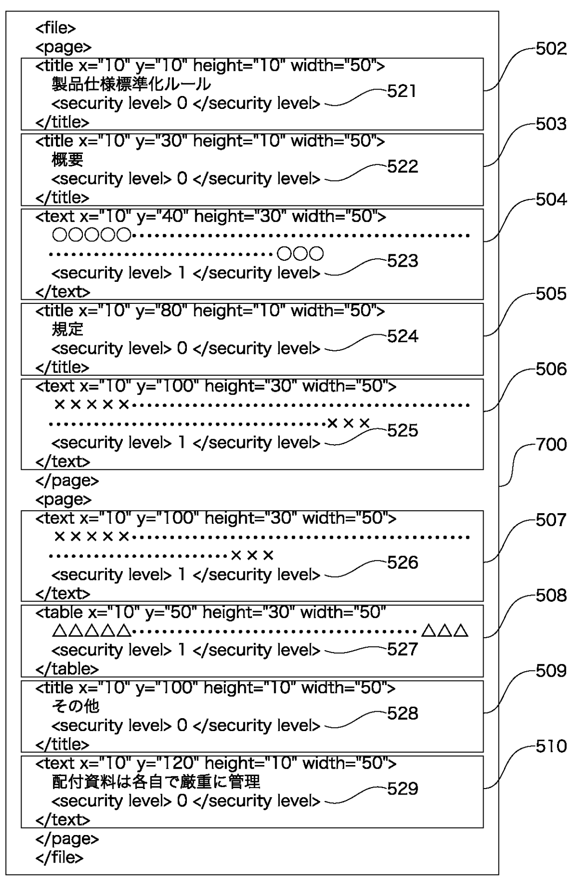
【図４】


START
S301
電子データを取得する
S302
パスワードまたはIDを入力する
S303
暗号化画像を生成する
S304
暗号化画像を印刷する
END

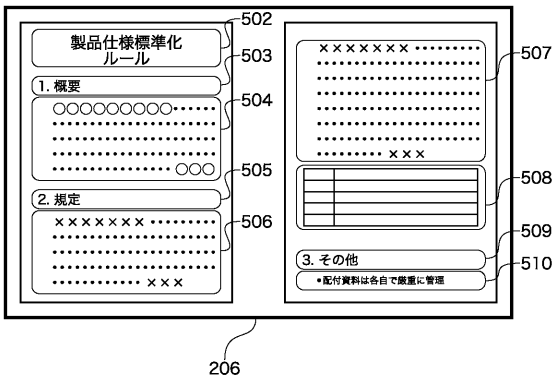
【図５】


701
電子データ
702
認証データ
711
セキュリティ情報抽出部
712
イメージ配置部
713
背景埋込部(暗号化処理1)
704
解読プログラムおよび復号鍵
714
パッケージ部
715
認証プログラム生成部
716
背景埋込部(暗号化処理2)
703
背景パターン
717
出力画像生成部
705
暗号化画像データ

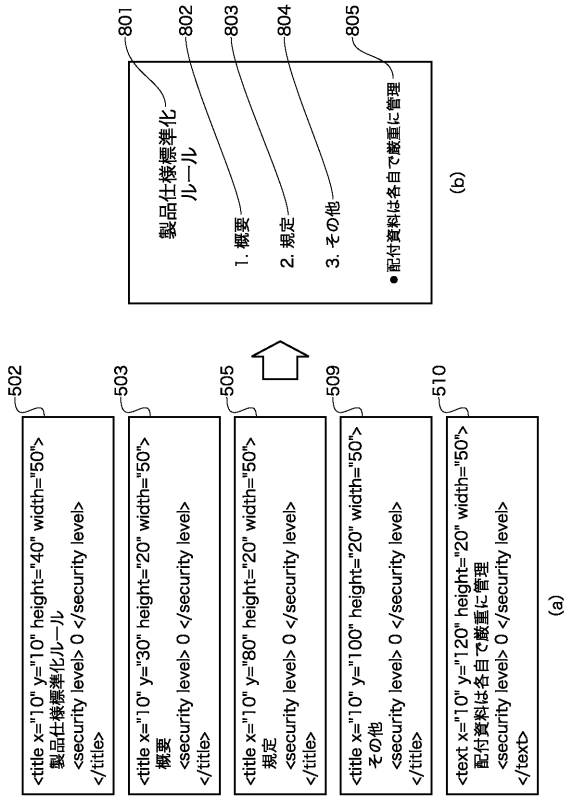
【図６】


<file>
<page>
<title x="10" y="10" height="10" width="50">
製品仕様標準化ルール
<security level> 0 </security level>
521
</title>
502
<title x="10" y="30" height="10" width="50">
概要
<security level> 0 </security level>
522
</title>
503
<text x="10" y="40" height="30" width="50">
○○○○○・・
・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・○○○
<security level> 1 </security level>
523
</text>
504
<title x="10" y="80" height="10" width="50">
規定
<security level> 0 </security level>
524
</title>
505
<text x="10" y="100" height="30" width="50">
×××××・・
・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・×××
<security level> 1 </security level>
525
</text>
506
</page>
700
<page>
<text x="10" y="100" height="30" width="50">
×××××・・
・・・・・・・・・・・・・・・・・・・・・・・・・×××
<security level> 1 </security level>
526
</text>
507
<table x="10" y="50" height="30" width="50"
△△△△△・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・△△△
<security level> 1 </security level>
527
</table>
508
<title x="10" y="100" height="10" width="50">
その他
<security level> 0 </security level>
528
</title>
509
<text x="10" y="120" height="10" width="50">
配付資料は各自で厳重に管理
<security level> 0 </security level>
529
</text>
510
</page>
</file>

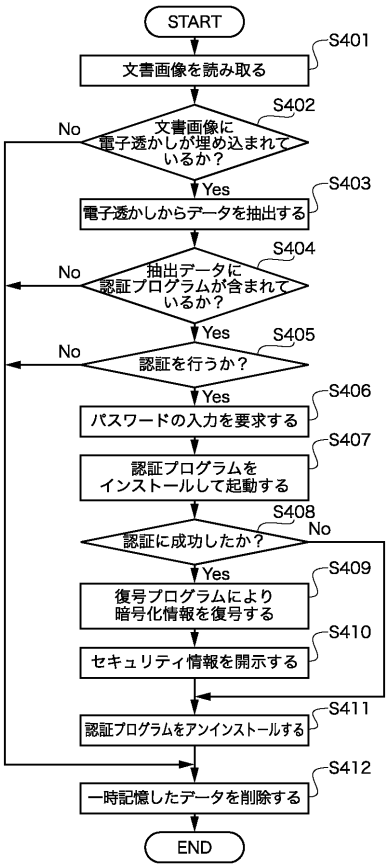
【図７】


502
製品仕様標準化ルール
503
1. 概要
504
505
2. 規定
506
507
508
509
3. その他
510
●配付資料は各自で厳重に管理
206

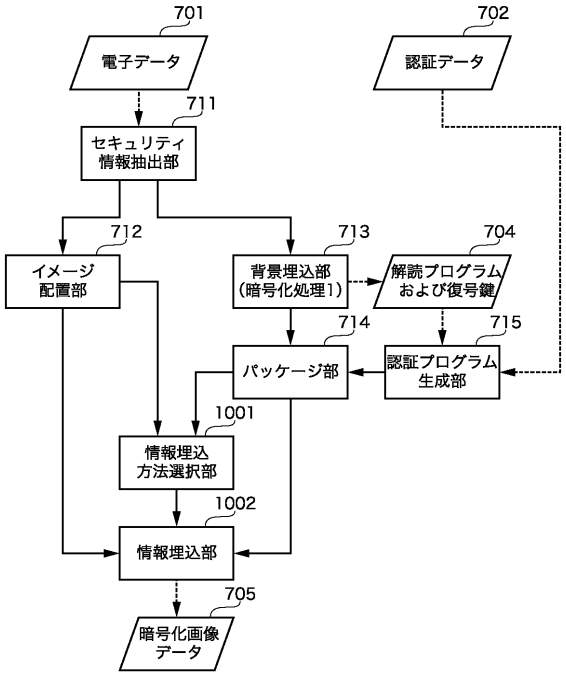
【図８】


801
802
803
804
805
製品仕様標準化ルール
1. 概要
2. 規定
3. その他
●配付資料は各自で厳重に管理
(b)
502
503
505
509
510
<title x="10" y="10" height="40" width="50">
製品仕様標準化ルール
<security level> 0 </security level>
</title>
<title x="10" y="30" height="20" width="50">
概要
<security level> 0 </security level>
</title>
<title x="10" y="80" height="20" width="50">
規定
<security level> 0 </security level>
</title>
<title x="10" y="100" height="20" width="50">
その他
<security level> 0 </security level>
</title>
<text x="10" y="120" height="20" width="50">
配付資料は各自で厳重に管理
<security level> 0 </security level>
</text>
(a)

【図９】


START
S401
文書画像を読み取る
S402
文書画像に電子透かしが埋め込まれているか？
No
Yes
S403
電子透かしからデータを抽出する
S404
抽出データに認証プログラムが含まれているか？
No
Yes
S405
認証を行うか？
No
Yes
S406
パスワードの入力を要求する
S407
認証プログラムをインストールして起動する
S408
認証に成功したか？
No
Yes
S409
復号プログラムにより暗号化情報を復号する
S410
セキュリティ情報を開示する
S411
認証プログラムをアンインストールする
S412
一時記憶したデータを削除する
END

【図１０】


701
電子データ
702
認証データ
711
セキュリティ情報抽出部
712
イメージ配置部
713
背景埋込部（暗号化処理1）
704
解読プログラムおよび復号鍵
714
パッケージ部
715
認証プログラム生成部
1001
情報埋込方法選択部
1002
情報埋込部
705
暗号化画像データ

フロントページの続き

Ｆターム(参考) 5B057 CA08 CA12 CA16 CB08 CB12 CB16 CE08 CG07 DA16
5C076 AA14 BA06
5C077 LL14 MP01 PP23
5J104 AA12 PA14