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

特許第4557765号
(P4557765)

(45)発行日　平成22年10月6日(2010.10.6)　(24)登録日　平成22年7月30日(2010.7.30)

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

請求項の数 10　(全 20 頁)

(21)出願番号　特願2005-84513(P2005-84513)
(22)出願日　平成17年3月23日(2005.3.23)
(65)公開番号　特開2006-270418(P2006-270418A)
(43)公開日　平成18年10月5日(2006.10.5)
審査請求日　平成20年3月14日(2008.3.14)

(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　平井　達彦
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】画像処理装置およびその方法

(57)【特許請求の範囲】
【請求項１】
ユーザそれぞれのセキュリティレベルを記憶する記憶手段と、
ユーザの認証を行う認証手段と、
読み取った画像を属性ごとの領域に分割する分割手段と、
前記分割された領域それぞれについてのポインタ情報を、前記読み取った画像から抽出する抽出手段と、
前記ポインタ情報が抽出されず、前記認証手段により認証されたユーザによりベクトル化処理が指示された前記分割された領域の画像を再利用可能なデータに変換する変換手段と、
前記変換によって得られた、前記分割された領域の再利用可能なデータに、前記ユーザが指定するセキュリティレベルを設定する設定手段と、
前記セキュリティレベルが設定された、前記分割された領域の再利用可能なデータをサーバに登録する登録手段と、
前記ポインタ情報が抽出された前記分割された領域の再利用可能なデータに設定されたセキュリティレベルを、当該ポインタ情報によって特定されるサーバから取得する取得手段と、
前記ポインタ情報が抽出された前記分割された領域の再利用可能なデータに設定されたセキュリティレベルと、前記認証手段により認証されたユーザの、前記記憶手段が記憶するセキュリティレベルとを比較して、前記再利用可能なデータの編集または印刷の可否を

判定する判定手段と、
前記編集または印刷が可と判定された再利用可能なデータの編集または印刷が行えるように、前記編集または印刷が不可と判定された再利用可能なデータの編集または印刷を行わないように、前記編集または印刷を制御する制御手段とを有することを特徴とする画像処理装置。
【請求項２】
前記登録手段は、前記認証手段が認証したユーザのIDを前記再利用可能なデータに記録することを特徴とする請求項1に記載された画像処理装置。
【請求項３】
さらに、前記ポインタ情報によって特定されるサーバから前記分割された領域の再利用可能なデータを取得するデータ取得手段と、
前記編集が可と判定された、前記データ取得手段が取得した再利用可能なデータを編集する編集手段とを有することを特徴とする請求項1に記載された画像処理装置。
【請求項４】
さらに、前記ポインタ情報によって特定されるサーバから前記分割された領域の再利用可能なデータを取得するデータ取得手段と、
前記印刷が可と判定された、前記データ取得手段が取得した再利用可能なデータを用いて画像を印刷する印刷手段とを有することを特徴とする請求項1に記載された画像処理装置。
【請求項５】
前記印刷手段は、印刷する各領域の画像に、その領域の前記再利用可能なデータへの前記ポインタ情報を埋め込むことを特徴とする請求項4に記載された画像処理装置。
【請求項６】
さらに、前記登録手段によりサーバに登録された前記再利用可能なデータのセキュリティレベルを変更する変更手段を有することを特徴とする請求項1から請求項5の何れか一項に記載された画像処理装置。
【請求項７】
さらに、原稿画像を読み取る読取手段を有することを特徴とする請求項1から請求項6の何れか一項に記載された画像処理装置。
【請求項８】
記憶手段、認証手段、分割手段、抽出手段、変換手段、設定手段、登録手段、取得手段、判定手段および制御手段を有する画像処理装置の画像処理方法であって、
前記記憶手段により、ユーザそれぞれのセキュリティレベルを記憶し、
前記認証手段により、ユーザの認証を行い、
読み取った画像を、前記分割手段により、属性ごとの領域に分割し、
前記抽出手段により、前記分割された領域それぞれについてのポインタ情報を、前記読み取った画像から抽出し、
前記変換手段により、前記ポインタ情報が抽出されず、前記認証手段により認証されたユーザによりベクトル化処理が指示された前記分割された領域の画像を再利用可能なデータに変換し、
前記設定手段により、前記変換によって得られた、前記分割された領域の再利用可能なデータに、前記ユーザが指定するセキュリティレベルを設定し、
前記登録手段により、前記セキュリティレベルが設定された、前記分割された領域の再利用可能なデータをサーバに登録し、
前記取得手段により、前記ポインタ情報が抽出された前記分割された領域の再利用可能なデータに設定されたセキュリティレベルを、当該ポインタ情報によって特定されるサーバから取得し、
前記判定手段により、前記ポインタ情報が抽出された前記分割された領域の再利用可能なデータに設定されたセキュリティレベルと、前記認証手段により認証されたユーザの、前記記憶手段が記憶するセキュリティレベルとを比較して、前記再利用可能なデータの編

集または印刷の可否を判定し、
前記制御手段により、前記編集または印刷が可と判定された再利用可能なデータの編集または印刷が行えるように、前記編集または印刷が不可と判定された再利用可能なデータの編集または印刷を行わないように、前記編集または印刷を制御することを特徴とする画像処理方法。
【請求項９】
コンピュータを、請求項1から請求項7の何れか一項に記載された画像処理装置の各手段として機能させるためのプログラム。
【請求項１０】
請求項9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、コンピュータが読み取り可能な記録媒体。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は画像処理装置およびその方法に関し、例えば、文書（画像）データを再利用する画像処理に関する。
【背景技術】
【０００２】
機能が拡張された記録装置であるMFP（マルチファンクション複合機）を用いて、画像記憶装置に文字や画像のオリジナルデータを格納し、オリジナルデータを記録紙に文書として印刷する際に、オリジナルデータをベクトルデータに変換して編集可能な状態にすることができる。このベクトルデータは、再編集して印刷することが可能である。しかし、容易に編集可能なベクトルデータは、改竄が容易だけでなく、著作権保護の問題もある。従って、ベクトルデータごとにセキュリティレベルを設定する必要がある。
【０００３】
セキュリティレベルを設定する方法として、例えば、人間が知覚することができない電子透かしなどの情報を文書（画像）に埋め込む方法が提案されている。また、電子透かしの技術としては、特開2000-106624公報に記載された画像データをウェーブレット変換し、周波数空間での冗長性を利用して電子透かしを埋め込む方法などが知られている。
【０００４】
しかし、電子透かしとしてセキュリティ情報を埋め込むにしても、オリジナルデータ（またはベクトルデータ）の印刷後にセキュリティレベルが変更された場合は、印刷文書のセキュリティレベルを変更することは不可能である。従って、印刷文書からベクトルデータを生成すれば、セキュリティレベルが低いままのベクトルデータが得られ、セキュリティレベルを高めたにもかかわらず、当該ベクトルデータの編集および印刷が可能になってしまう。
【０００５】
【特許文献１】特開2000-106624公報
【発明の開示】
【発明が解決しようとする課題】
【０００６】
本発明は、文書（画像）の再利用可能なデータの再利用の可否を判定する際に、当該再利用可能なデータのセキュリティレベルの変更を反映することを目的とする。
【課題を解決するための手段】
【０００７】
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。
【０００８】
本発明にかかる画像処理は、ユーザそれぞれのセキュリティレベルを記憶し、ユーザの認証を行い、読み取った画像を属性ごとの領域に分割し、前記分割された領域それぞれについてのポインタ情報を、前記読み取った画像から抽出し、前記ポインタ情報が抽出されず

、前記認証されたユーザによりベクトル化処理が指示された前記分割された領域の画像を再利用可能なデータに変換し、前記変換によって得られた、前記分割された領域の再利用可能なデータに、前記ユーザが指定するセキュリティレベルを設定し、前記セキュリティレベルが設定された、前記分割された領域の再利用可能なデータをサーバに登録し、前記ポインタ情報が抽出された前記分割された領域の再利用可能なデータに設定されたセキュリティレベルを、当該ポインタ情報によって特定されるサーバから取得し、前記ポインタ情報が抽出された前記分割された領域の再利用可能なデータに設定されたセキュリティレベルと、前記認証手段により認証されたユーザの、前記記憶手段が記憶するセキュリティレベルとを比較して、前記再利用可能なデータの編集または印刷の可否を判定し、前記編集または印刷が可と判定された再利用可能なデータの編集または印刷が行えるように、前記編集または印刷が不可と判定された再利用可能なデータの編集または印刷を行わないように、前記編集または印刷を制御することを特徴とする。

【発明の効果】

【００１１】

本発明によれば、文書（画像）の再利用可能なデータの再利用の可否を判定する際に、当該再利用可能なデータのセキュリティレベルの変更を反映することができる。

【発明を実施するための最良の形態】

【００１２】

以下、本発明の実施例の画像処理を図面を参照して詳細に説明する。

【実施例１】

【００１３】

［画像処理システム］

図1は複合機を使用して情報の電子化を行う画像処理システムの構成例を示すブロック図である。

【００１４】

この画像処理システムは、オフィス（のような複数の区分）10と20がインターネットのようなWAN 104で接続された環境で実現される。

【００１５】

オフィス10内に構築されたLAN 107には、複合機(MFP: Multi-Function Processor) 100、MFP 100を制御するマネージメントPC 101、クライアントPC 102、文書管理サーバ106、文書管理サーバによって管理されるデータベース105などが接続されている。オフィス20はオフイス10とほぼ同様の構成を有するが、オフィス20内に構築されたLAN 108には、少なくとも文書管理サーバ106、文書管理サーバによって管理されるデータベース105などが接続されている。オフィス10のLAN 107とオフィス20のLAN 108は、LAN 107に接続されたプロキシサーバ103、WAN 104、および、LAN 108に接続されたプロキシサーバ103を介して、相互に接続されている。

【００１６】

MFP 100は、文書画像を読み取り、読み取った画像を処理する画像処理の一部を担当する。MFP 100から出力される画像信号は、通信線109を介してマネージメントPC 101に入力される。マネージメントPC 101は、通常のパーソナルコンピュータ(PC)で、画像記憶するハードディスクなどのメモリ、ハードウェアまたはソフトウェアで構成される画像処理部、CRTやLCDなどのモニタ、マウスやキーボードなどの入力部を有するが、その一部はMFP 100に一体化して構成されている。なお、以下では、マネージメントPC 101において、下記の処理などを実行する例を説明するが、マネージメントPC 101が行う処理をMFP 100で実行するようにしても構わない。

【００１７】

［MFP］

図2はMFP 100の構成例を示すブロック図である。

【００１８】

オートドキュメントフィーダ(ADF)を含む画像読取部110は、一枚または重ねられた複数

の原稿それぞれの画像を、光源で照射し、原稿からの反射像をレンズで固体撮像素子上に結像し、固体撮像素子からラスタ順の画像読取信号（例えば600dpi、8ビット）を得る。原稿を複写する場合は、この画像読取信号をデータ処理部115で記録信号へ変換し、複数枚の記録紙に複写する場合は、一旦、記憶部111に一頁分の記録信号を記憶した後、記録信号を繰り返し記録部112に出力することで、複数の記録紙に画像を形成する。

【００１９】

一方、クライアントPC 102から出力されるプリントデータは、LAN 107を介してネットワークインタフェイス(I/F)114へ入力され、データ処理部装置115によって記録可能なラスタデータに変換された後、記録部112によって記録紙上に画像として形成される。

【００２０】

MFP 100に対する操作者の指示は、MFP 100に装備されたキー操作部とマネージメントPC 101のキーボードやマウスからなる入力部113によって行われる。操作入力の表示および画像処理状態の表示などは表示部116によって行われる。

【００２１】

上記のMFP 100の動作は、データ処理部115内の、例えばワンチップマイクロコントローラで構成される制御部115aで制御される。

【００２２】

なお、記憶部111は、マネージメントPC 101からも制御可能である。MFP 100とマネージメントPC 101と間のデータの授受および制御は、ネットワークI/F 117および両者を直結する信号線109を介して行われる。

【００２３】

なお、MFP100は、ディジタルカメラやディジタルビデオなどの撮像装置、ポータブルデータアシスタント(PDA)などの携帯端末装置、ファクシミリなどから画像データを入手するインタフェイスを入力部113の一部として備えていてもよい。

【００２４】

また、入力部113には、ユーザを識別するためのユーザ認識部118が接続されている。ユーザ認識部118は、例えばICカードリーダ、IDや暗証入力用のキー、あるいは、指紋、手紋、毛細血管パターンや虹彩などの生体情報を識別する生体認証装置などで、MFP 100を使用するユーザを特定する情報（以下「ユーザ特定情報」と呼ぶ）を入力し、入力部113を介してデータ処理部115へユーザ特定情報を出力する。

【００２５】

一方、データ処理部115が管理する不揮発性メモリ、または、マネージメントPC 101の不揮発性メモリ（例えばハードディスク）には、MFP 100のユーザごとのセキュリティレベルを示す情報が設定され、記憶されている。従って、データ処理部115は、ユーザ認識部118から入力されるユーザ特定情報に対応するセキュリティレベルを取得することができる。また、ユーザ認識部118としてICカードリーダを使用する場合、ユーザ認識部118からデータ処理部115へICカード内のメモリに記憶されたセキュリティレベルが通知されるようにしてもよい。

【００２６】

なお、以下では、データ処理部115が、ユーザ認識部118により取得されたユーザ特定情報に対応するセキュリティレベルを取得する（または、ユーザ認識部118から直接、セキュリティレベルを取得する）ことを「ユーザ認証」と呼ぶ。

【００２７】

［処理の概要］

入力部113から文書の蓄積が指示されると、MFP 100は、画像読取部110で原稿画像を読み取り、データ処理部115で画像記録が可能な記録信号に変換した原稿画像を、ネットワークI/F 114または117を介して、文書管理サーバ106、クライアントPC 102に送信したり、記憶部111に蓄積する。

【００２８】

また、操作部113から文書の検索が指示されると、MFP 100は、画像読取部110で原稿画像

を読み取り、原稿画像の特定領域にあるポインタ情報を検出する。ポインタ情報はオリジナルデータの所在を示すもので、原稿画像に例えば二次元バーコードで付加されている。ポインタ情報の付加は、二次元バーコードに限らず、隣接する文字列の間隔の変化を利用して画像中に情報を埋め込む方法、ハーフトーン画像に埋め込む方法など、直接視認されない、いわゆる電子透かしによる方法を利用してもよい。

【００２９】

MFP 100は、検出したポインタ情報に従い、記憶部111、データベースサーバ105、クライアントPC 102から、原稿画像のオリジナルデータを検索し、オリジナルデータを検出するとオリジナルデータに基づきオリジナル文書をプリントアウトしたり、読み取った原稿画像とオリジナルデータの一致の判定や改竄の有無を判定するために、マネージメントPC 101に読み取った原稿画像およびオリジナルデータを供給したりする。

【００３０】

図3は上記の画像処理システムによる処理の概要を説明するフローチャートで、マネージメントPC 101またはデータ処理部115、あるいは、それらの組み合わせによって実行される処理である。

【００３１】

まず、MFP 100は、ユーザ認証を行い(S300)、入力されたID、暗証または生体情報が登録されていない場合は、認証不能の旨を表示部116に表示する。なお、セキュリティレベルは、例えば、下記のように、文書（画像）のセキュリティレベルと合わせて五段階に区別される。

ユーザのセキュリティレベル	印刷、編集が可能な文書（画像）のセキュリティレベル
5	すべて（制限なし）
4	レベル4以下
3	レベル3以下
2	レベル2以下
1	レベル1

【００３２】

上記において、セキュリティレベル1の文書（画像）はセキュリティが未設定であり、セキュリティレベル1のユーザは、セキュリティレベルが2以上に設定された文書（画像）の印刷、編集は不可である。

【００３３】

MFP 100は、ユーザ認証に成功すると、画像読取部110を動作させて、一枚の原稿の画像をラスタ走査して、画像読取信号を取得する。画像読取信号は、データ処理部115によって前処理され、入力画像の一頁分の画像データとして、記憶部111に保存される(S301)。

【００３４】

次に、マネージメントPC 101は、ブロックセレクション(BS)処理を行い、記憶部111に格納された画像データを、文字または線画を含む文字・線画領域、ハーフトーンの写真領域、不定形の画像領域、その他の領域に分割する。さらに、文字・線画領域については、主に文字を含む文字領域、主に表、図形などを含む線画領域を分離し、線画領域は表領域および図形領域に分離する(S302)。なお、実施例1では連結画素を検知し、連結画素の外接矩形領域の形状、サイズ、画素密度などを用いて、属性ごとの領域に分割するが、その他の領域分割手法を用いても構わない。

【００３５】

文字領域は、段落などの塊をブロックとして矩形ブロック（文字領域矩形ブロック）にセグメント化する。線画領域は、表、図形などの個々のオブジェクト（表領域矩形ブロック、線画領域矩形ブロック）ごとに、矩形ブロックにセグメント化する。また、ハーフト

ーンで表現される写真領域は、画像領域矩形ブロック、背景領域矩形ブロックなどの矩形ブロックにセグメント化する。なお、これら矩形ブロックの情報を「領域分割情報」という。

【００３６】

次に、データ処理部115は、BS処理によって得られた領域分割情報と、入力画像を合成して、図4に一例を示すように、表示部116の操作画面上に表示する(S303)。操作画面の左側には入力画像そのものが表示され、右側に領域分割情報が矩形ブロックとして表示される。なお、図4には、矩形ブロックの理解を容易にするため、各ブロックに、その属性を示す文字列TEXT、PICTURE、LINE、TABLEなどを示すが、実際の操作画面には属性情報は表示されず、矩形ブロックが枠線として表示される。属性情報TEXTは文字属性を、PICTUREは図画属性を、PHOTOは写真属性を、LINEは線画属性を、TABLEは表属性をそれぞれ表す。勿論、図4のように入力画像と領域分割情報とを左右に並置表示する以外に、これらを重ね合わせて入力画像上に矩形ブロックを表示するなど、多様な表示形態が可能である。

【００３７】

次に、ユーザは、操作画面に表示された矩形ブロックからベクトル化の対象にする矩形ブロック（セグメント）を指定する(S304)。領域の指定方法としては、例えば、ユーザがポインティングデバイスを用いて、一または複数のセグメントを指示してもよいし、操作画面をタッチパネルにして、ユーザが所望するセグメントを指で触れて指示する方法など、種々の方法を採用し得る。

【００３８】

次に、マネージメントPC 101は、データ処理部115から通知される指定領域に以下の処理を施すために、指定領域の画像データを切り出し(S305)、切り出した指定領域の画像および画像全体に埋め込まれたオリジナルデータへのポインタ情報を検出するため、OCR、OMR処理を行う(S306)。具体的には、入力画像中に付加情報として記録された二次元バーコード、あるいは、URLに該当するオブジェクトを検出し、OCRによってURLを文字認識し、OMRによって二次元バーコードを解読して、ポインタ情報を検出する。なお、ポインタ情報を付加する手段は、二次元バーコードに限定されるものではなく、隣接する文字列の間隔の変化として情報を埋め込む方法、ハーフトーンの画像に埋め込む方法など、直接視認されない、いわゆる電子透かしによる方法などがある。

【００３９】

次に、マネージメントPC 101は、OCR、OMR処理の結果もしくは電子透かし情報からポインタ情報を抽出する(S307)。ポインタ情報は、例えばファイルサーバ名およびファイル名からなるパス名、あるいは、対応するファイルを示すURLなどで構成される。

【００４０】

次に、マネージメントPC 101は、画像全体に埋め込まれたポインタ情報が抽出されたか否かを判定し(S308)、抽出されなかった場合は処理をステップS311に進めるが、抽出された場合はポインタ情報に基づき、クライアントPC 102の記憶部（ハードディスク等）、データベースサーバ105またはMFP 100の記憶部111などから画像全体（文書）のオリジナルデータに設定された最新のセキュリティレベルを取得する(S309)。そして、取得したセキュリティレベルとユーザのセキュリティレベルを比較して、当該文書の編集が可能か否かを判定する(S310)。ユーザのセキュリティレベルが「3」の場合、文書のセキュリティレベルが「4」以上であれば、その文書を編集することはできないので処理は終了するが、セキュリティレベルが「3」以下の文書であれば指定領域の画像データを再利用可能なデータに変換して登録することが可能であるから、以下の処理が実行される。

【００４１】

文書（画像）のオリジナルデータの登録者は、その文書（画像）のセキュリティレベルを任意に変更することが可能である。クライアントPC 102、データベースサーバ105、MFP 100などの記憶部に格納された文書（画像）のオリジナルデータには、登録者のID情報が記録されている。登録者は、入力部113を操作して、自分が登録した文書（画像）を登録日、ファイル名、データ量、データ種別などの情報から検索し、表示部116にリストされた

文書（画像）の中からセキュリティレベルを変更したい文書（画像）を指定し、セキュリティレベルを変更することが可能である。従って、セキュリティレベルは、状況に応じ刻々と変化する。そのため、過去に印刷された文書に埋め込まれたセキュリティレベルは、現在のセキュリティレベルと異なる可能性があり、常に、上記の記憶部から最新のセキュリティレベルを取得する必要がある。

【００４２】

編集が可能な場合、マネージメントPC 101は、指定領域ごとにポインタ情報が抽出されたか否かを判定し(S311)、ポインタ情報が抽出された指定領域については既にオリジナルデータが登録されているので以下の処理を行わず、ポインタ情報が抽出されなかった指定領域について以下の処理を実行する。なお、指定領域とポインタ情報の抽出結果の関係をユーザに通知するために、表示部116に表示することが好ましい。

【００４３】

マネージメントPC 101は、ポインタ情報が抽出されなかった指定領域は、後述するベクトル化処理により指定領域の画像データをベクトル化し、再利用可能なデータに変換し(S312)、ユーザから指定領域の画像の重要度に応じたセキュリティレベルの指定を受け付け、再利用可能なデータにセキュリティレベルを設定する(S313)。セキュリティレベルが指定されなかった場合は、既定値である最低のセキュリティレベル「1」を設定する。また、指定領域が複数ある場合、ユーザは指定領域ごとにセキュリティレベルを指定することも可能だが、ユーザがセキュリティレベルを変更しない限り、全指定領域に同一のセキュリティレベルを設定する。

【００４４】

次に、マネージメントPC 101は、セキュリティレベルおよび登録者のID情報を記録した、指定領域の再利用可能なデータをデータベースサーバ105またはMFP 100の記憶部111に登録し(S314)、処理を終了する。

【００４５】

このように、ポインタ情報を有する（言い換えればオリジナルデータがある）セグメントの画像データをベクトル化することはないから、セキュリティレベルの変更が未反映の再利用可能なデータを生成することはない。このようにして登録された再利用可能なデータが印刷されると、そのセグメントには、当該データのポインタ情報およびセキュリティ情報などが埋め込まれる。

【００４６】

また、再利用可能なデータについて簡単に説明すると、データ形式は使用するアプリケーションに依存するため、目的に応じたファイル形式に変換する必要がある。例えば、代表的なアプリケーションソフトウェアのワードプロセッサソフトウェアや表計算ソフトウェアなどでは、それぞれ目的に応じたファイル形式が定義され、後述するベクトル化処理により得られるベクトルデータを、そのファイル形式（アプリケーションデータ形式）に変換する。より汎用的なファイル形式としては、例えばMicrosoft(R)が策定したRich Text Format (RTF)形式や、近年使用されるようになった、World Wide Web Consortium (W3C)が提唱するScalable Vector Graphics (SVG)形式、あるいは、単純にテキストデータのみを扱うプレーンテキスト形式などがあり、これらのデータ形式はアプリケーションソフトウェアにおいて共通に使用できる可能が高い。

【００４７】

以下では、図3に示した主要なステップの処理について詳細に説明する。

【００４８】

［ブロックセレクション(S302)］

ブロックセレクションは、図4に示す一頁の画像をオブジェクトの集合体と認識して、各オブジェクトの属性を文字(TEXT)、図画(PICTURE)、写真(PHOTO)、線画(LINE)、表(TABLE)に判別し、異なる属性を持つセグメント（ブロック）に分割する処理である。次に、ブロックセレクションの具体例を説明する。

【００４９】

先ず、処理すべき画像を白黒画像に二値化して、輪郭線追跡によって黒画素で囲まれる画素の塊を抽出する。所定面積以上の黒画素の塊については、その内部の白画素について輪郭線追跡を行い白画素の塊を抽出する。さらに、所定面積以上の白画素の塊の内部の黒画素の塊を抽出するというように、黒画素および白画素の塊の抽出を再帰的に繰り返す。

【００５０】

このようにして得られた画素塊に外接する矩形ブロックを生成し、矩形ブロックの大きさおよび形状に基づき属性を判定する。例えば、縦横比が1に近く、大きさが所定範囲の画素塊を文字属性の画素塊とし、さらに、近接する文字属性の画素塊が整列していてグループ化が可能な場合はそれらを文字領域とする。また、縦横比が小さい扁平な画素塊を線画領域に、所定以上の大きさで、かつ、矩形に近い形状を有し、整列した白画素塊を内包する黒画素塊が占める範囲を表領域に、不定形の画素塊が散在する領域を写真領域、その他の任意形状の画素塊を図画領域に、のようにそれぞれ分類する。

【００５１】

図5はブロックセレクションの結果の一例を示す図で、図5(a)は抽出された各矩形ブロックのブロック情報を示す。ブロック情報には、各ブロックの属性、位置の座標X、Y、幅W、高さH、OCR情報などが含まれる。属性は1～5の数値で与えられ、「1」は文字属性、「2」は図面属性、「3」は表属性、「4」は線画属性、「5」は写真属性を表す。また、座標X、Yは入力画像における各矩形ブロックの始点のXY座標（左上角の座標）を、幅W、高さHは矩形ブロックのX座標方向の幅、Y座標方向の高さを、ポインタ情報の有無をそれぞれ表す。

【００５２】

また、図5(b)は入力ファイル情報で、ブロックセレクションによって抽出された矩形ブロックの総数を示す。

【００５３】

これら矩形ブロックごとのブロック情報は特定領域のベクトル化に利用される。また、ブロック情報によって、ベクトル化された特定領域とラスタデータの相対位置関係を特定することができ、入力画像のレイアウトを損わずにベクトル化領域とラスタデータ領域を合成することが可能になる。

【００５４】

［ポインタ情報の抽出(S307)］

図6はセグメントの画像データからポインタ情報を抽出する処理を示すフローチャートで、抽出対象の画像データがデータ処理部115のページメモリ（不図示）に格納された後、データ処理部115（またはマネージメントPC 101）によって実行される処理である。なお、抽出対象の印刷文書310には、図7に一例を示すように、文字領域312、313、写真領域314、および、二次元バーコード（例えばQRコード）のシンボル311があるとする。

【００５５】

まず、ブロックセレクションの処理結果であるブロック情報から、二次元バーコードシンボルの位置を検出する(S701)。QRコードシンボルは、四隅のうちの三隅に、特定の位置検出要素パターンが設けられ、位置検出要素パターンを検出することで、QRコードシンボルを検出することができる。

【００５６】

次に、位置検出要素パターンに隣接する形式情報を復元し、シンボルに適用されている誤り訂正レベルおよびマスクパターンを取得し(S702)、シンボルの型番（モデル）を決定し(S703)、取得したマスクパターンを使って、QRコードのシンボルの符号化領域ビットパターンを排他的論理和(XOR)演算し、QRコードシンボルのマスク処理を解除する(S704)。

【００５７】

続いて、決定したモデルに基づき配置規則を取得し、この配置規則に基づきシンボルキャラクタを読み取り、メッセージおよび誤り訂正コード語を復元する(S705)。そして、復元されたメッセージについて、誤り訂正コード語に基づき、誤りを検出し(S706)、誤りを検出した場合は復元したメッセージを訂正する(S707)。

【００５８】
次に、復元されたメッセージより、モード指示子および文字数指示子に基づき、データコード語をセグメントに分割し、データコード語を復元し(S708)、検出した仕様モードに基づきデータコード文字を復号して、ポインタ情報として出力する(S709)。
【００５９】
二次元バーコードに組み込まれたデータは、オリジナルデータファイルのポインタ情報およびセキュリティ情報を表す。ポインタ情報は、例えばファイルサーバ名およびファイル名からなるパス名、あるいは、対応するファイルを示すURLなどで構成される。また、セキュリティ情報に含まれるセキュリティレベルは、文書310が印刷された際に設定されていたセキュリティレベル、もしくは、セキュリティレベルが未登録の場合は印刷時にユーザが設定したセキュリティレベルであり、現在のセキュリティレベルと異なる場合がある。
【００６０】
図8は二次元バーコードに組み込まれるデータ（三例）を示す図である。画像名（またはファイル名でもよい）、文書内のレイアウト位置情報（エリア座標）、セキュリティレベル、ポインタ情報から構成され、ポインタ情報にはIPアドレス、パス名、URLなどが利用可能である。
【００６１】
上記では、ポインタ情報が二次元バーコードの形で付加された画像データの例を説明したが、ポインタ情報の記録形態として様々な方法を採用し得る。例えば、所定のルール（例えば暗号化）に従う文字列によってポインタ情報を直接文字列として記録し、ブロックセレクションによって文字列の矩形ブロックを検出してもよい。検出された文字列を認識（例えば復号）することによりポインタ情報を取得し得る。あるいは、文字領域において、隣接する文字列の間隔に視認し難い程度の変調を加え、当該文字列の間隔の変調情報によってポインタ情報を表現し得る。このような電子透かし情報は、後述する文字認識処理を行う際に、各文字の間隔を検出することによって検出することができ、ポインタ情報を取得し得る。勿論、写真領域や図面領域に電子透かしとしてポインタ情報を付加することも可能である。
【００６２】
ポインタ情報の抽出に関しても、ベクトル化すべき領域を指定することで、指定領域から迅速かつ確実にポインタ情報を取得することができる。言い換えれば、ユーザが二次元バーコードが記録されているセグメントを指定したり、電子透かしなどが埋め込まれているだろうセグメントを指定したりすることで、ポインタ情報を効率的に抽出することが可能である。
【００６３】
［セキュリティ情報の取得(S309)］
マネージメントPC 101は、ポインタ情報に基づき、ファイルサーバを特定し、ファイルサーバ（MPF 100のデータ処理部115、クライアントPC 102または文書管理サーバ106に相当する）にアクセスしてオリジナルデータのセキュリティ情報を要求する。この要求を受信したファイルサーバは、要求に添付されたポインタ情報に基づきオリジナルデータを検索する。
【００６４】
ファイルサーバは、オリジナルデータを検出した場合は、オリジナルデータに設定されたセキュリティレベルをマネージメントPC 101に返す。もし、オリジナルデータを検出できなかった場合は、その旨をマネージメントPC 101に通知する。
【００６５】
勿論、マネージメントPC 101は、ポインタ情報に基づき、オリジナルデータを要求することもできる。ファイルサーバは、オリジナルデータを検出した場合、そのオリジナルデータをMFP 100のデータ処理部115に転送する。もし、オリジナルデータを検出できなかった場合は、その旨をマネージメントPC 101に通知する。

【００６６】
［ベクトル化処理(S312)］
まず、ベクトル化方法には、次の手法が存在する。
【００６７】
（a）文字属性のセグメントの場合は、OCR処理により文字画像を文字コードに変換する、または、文字のサイズ、スタイル、字体を認識して視覚的に忠実なフォントデータに変換する。
【００６８】
（b）線画または文字属性のセグメントで、OCR処理による文字認識が不可能な場合は、線画または文字の輪郭を追跡し、輪郭情報（アウトライン）を線分のつながりとして表現する形式に変換する。
【００６９】
（c）図面属性のセグメントの場合は、図形オブジェクトの輪郭を追跡し、輪郭情報を線分のつながりとして表現する形式に変換する。
【００７０】
（d）上記(b)または(c)の手法で得られた線分形式のアウトライン情報をベジェ関数などでフィッティングして関数情報に変換する。
【００７１】
（e）上記(c)の手法で得られた図形オブジェクトの輪郭情報から、図形の形状を認識し、円、矩形、多角形などの図形定義情報に変換する。
【００７２】
（f）表属性のセグメントの場合、罫線や枠線を認識し、所定のフォーマットの帳票フォーマット情報に変換する。
【００７３】
以上の手法のほかにも、画像データをコード情報、図形情報、関数情報などのコマンド定義形の情報に置き替える種々のベクトル化処理が考えられる。
【００７４】
［文字領域のベクトル化］
図9はベクトル化処理(S312)の詳細を示すフローチャートで、データ処理部115（またはマネージメントPC 101）によって実行される処理である。
【００７５】
まず、ブロック情報を参照して文字属性のセグメントか否か判断し(S901)、文字属性のセグメントであればステップS902に進んでパターンマッチングの一手法を用いて文字認識を行い、対応する文字コードを得る。
【００７６】
また、文字属性のセグメント以外の場合は、詳細は後述するが、画像の輪郭に基づくベクトル化を実行する(S912)。
【００７７】
文字属性のセグメントの場合は、横書き、縦書きの判定（組み方向の判定）を行うために、画素値に対する水平、垂直の射影をとり(S902)、射影の分散を評価し(S903)、水平射影の分散が大きい場合は横書き、垂直射影の分散が大きい場合は縦書きと判定して、その判定結果に基づき、行の切り出した後、文字を切り出して文字画像を得る(S904)。
【００７８】
文字列および文字への分解は、横書きならば水平方向の射影を利用して行を切り出し、切り出した行に対する垂直方向の射影から文字を切り出す。縦書きの文字領域に対しては、水平と垂直について逆の処理を行えばよい。なお、行、文字の切り出しに際して、文字のサイズも検出し得る。
【００７９】
次に、切り出した各文字について、文字画像から得られる特徴を数十次元の数値列に変換した観測特徴ベクトルを生成する(S905)。特徴ベクトルの抽出には種々の公知手法がある

が、例えば、文字をメッシュ状に分割し、各メッシュ内の文字線を方向別に線素としてカウントして、メッシュ数の次元ベクトルをもつ特徴ベクトルとする方法がある。

【００８０】

次に、観測特徴ベクトルと、予め字種ごとに求めてある辞書特徴ベクトルとを比較して、観測特徴ベクトルと辞書特徴ベクトルの距離を算出し(S906)、算出した距離を評価して、最も距離の近い字種を認識結果とする(S907)。さらに、距離の評価結果から最短距離と閾値を比較して、最短距離が閾値未満であれば類似度が高いと判定し、最短距離が閾値以上であれば類似度が低いと判定する(S908)。最短距離が閾値以上の場合（類似度が低い場合）は、形状が類似する他の文字と誤認識している可能性が高いので、ステップS907の認識結果を採用せず、文字画像を線画と同様に扱い、文字画像のアウトラインをベクトル化する(S911)。言い換えれば、誤認識の可能性が高い文字画像は、視覚的に忠実なアウトラインのベクトルデータを生成する。

【００８１】

一方、類似度が高い場合は、ステップS907の認識結果を採用するとともに、文字認識に用いる字種数分の辞書特徴ベクトルを、文字形状種すなわちフォント種に対して複数用意しておき、パターンマッチングの際に、文字コードとともにフォント種を出力することで文字フォントを認識する(S909)。続いて、文字認識およびフォント認識よって得られた文字コードおよびフォント情報を参照し、文字コードおよびフォント情報それぞれに対応して予め用意されたアウトラインデータを用いて、各文字をベクトルデータに変換する(S910)。なお、カラー画像データの場合は、文字の色を抽出してベクトルデータとともに記録する。

【００８２】

以上の処理により、文字属性のセグメントに含まれる文字画像をほぼ形状、大きさ、色が忠実なベクトルデータに変換することができる。

【００８３】

［文字領域以外のベクトル化］

文字属性のセグメント以外、すなわち図面属性、線画属性、表属性と判定されるセグメントは、黒画素塊を抽出し、その輪郭をベクトルデータに変換する。なお、写真属性のセグメントは、ベクトル化せず画像データのままにする。

【００８４】

文字領域以外のベクトル化は、まず、線画などを直線および/または曲線の組み合わせとして表現するために、曲線を複数の区間（画素列）に区切る「角」を検出する。図10はベクトル化における角抽出処理を説明する図で、角は曲率が極大になる点で、図10の曲線上の画素Piが角か否かは以下のように判定する。

【００８５】

画素Piを起点とし、線画曲線に沿って画素Piから両方向に所定画素数kずつ離れた画素Pi-k、Pi+kを線分Lで結ぶ。画素Pi-k、Pi+k間の距離をd1、画素Piから線分Lに直交するように下した線分の長さ（画素piと線分Lの距離）をd2が極大になる場合、あるいは、画素Pi-k、Pi+k間の弧の長さをAと距離d1の比d1/Aが所定の閾値以下になる場合、画素Piを角と判定する。

【００８６】

角を検出後、角によって分割された線画曲線の画素列を直線あるいは曲線で近似する。直線への近似は最小二乗法などにより実行し、曲線への近似は三次スプライン関数などを用いる。画素列を分割する角の画素は近似直線あるいは近似曲線における始端または終端になる。

【００８７】

さらに、ベクトル化された輪郭内に白画素塊の内輪郭が存在するか否かを判定し、内輪郭が存在する場合はその輪郭をベクトル化し、内輪郭の内輪郭というように、再帰的に黒画素塊および白画素塊の内輪郭をベクトル化する。

【００８８】

以上のように、輪郭の区分線を直線または曲線で近似する方法を用いれば、任意形状の図形のアウトラインをベクトル化することができる。また、入力画像がカラーの場合は、カラー画像から図形の色を抽出してベクトルデータとともに記録する。

【００８９】

図11はベクトル化において輪郭線をまとめる処理を説明する図である。

【００９０】

輪郭線の注目区間で外輪郭PRjと、内輪郭PRj+1または他の外輪郭が近接している場合、二つまたは三つ以上の輪郭線をひとまとめにして、太さをもつ線として表現することができる。例えば、輪郭PRj+1上の画素Piと、画素Piと最短距離の輪郭PRj上の画素Qi間の距離PQiを算出し、複数の画素間の距離PQiのばらつきが僅かである場合は、輪郭PRjおよびPRj+1を注目区間を線分PQiの中点Miの点列に沿う直線または曲線で近似する。そして、中点Miの点列に沿う近似直線または近似曲線の太さは、例えば、距離PQiの平均値とすればよい。

【００９１】

線や線の集合体である表罫線は、太さをもつ線の集合として表すことにより、効率よくベクトル表現することができる。

【００９２】

［図形の認識］

以上で線図形などのアウトラインをベクトル化した後、ベクトル化された区分線を図形オブジェクトごとにグループ化する。

【００９３】

図12はベクトル化で生成したベクトルデータのグループ化処理を示すフローチャートで、ベクトルデータを図形オブジェクトごとにグループ化する処理を示している。

【００９４】

まず、各ベクトルデータの始点および終点を算出し(S1401)、始点および終点の情報を用いて、図形要素を検出する(S1402)。図形要素とは、区分線によって構成される閉図形であり、検出に際しては、始点、終点になっている共通の角の画素においてベクトルを連結する。すなわち、閉形状を構成するベクトル群はそれぞれ、その両端に連結するベクトルを有するという原理を応用する。

【００９５】

次に、図形要素内に他の図形要素もしくは区分線が存在するか否かを判定し(S1403)、存在すれば、ステップS1401およびS1402を再帰的に繰り返して、それらをグループ化して一つの図形オブジェクトとし(S1404)、存在しなければ、その図形要素を図形オブジェクトとする(S1405)。

【００９６】

なお、図12には一つの図形オブジェクト分の処理しか示さないが、他の図形オブジェクトが存在すれば、その分、図12の処理を繰り返す。

【００９７】

●図形要素の検出(S1402)

図13は図形要素の検出処理を示すフローチャートである。

【００９８】

まず、ベクトルデータより、両端に連結するベクトルを有しないベクトルを除去して、閉図形を構成するベクトルを抽出する(S1501)。

【００９９】

次に、閉図形を構成するベクトルについて、ベクトルの何れかの端点（始点または終点）を開始点として、一定方向（例えば時計回り）に順にベクトルを探索する。すなわち、他端点において他のベクトルの端点を探索し、所定距離内の最近接端点を連結ベクトルの端点とする。閉図形を構成するベクトルを一回りして開始点に戻ると、通過したベクトルすべてを一つの図形要素を構成する閉図形としてグループ化する(S1502)。また、閉図形内部にある閉図形を構成するベクトルもすべて再帰的にグループ化する。さらに、グルー

プ化されていないベクトルの始点を開始点とし、上記と同様の処理を繰り返す。

【０１００】

そして、除去したベクトルのうち、閉図形としてグループ化したベクトルに端点が近接しているベクトル（閉図形に連結するベクトル）を検出し、検出したベクトルをそのグループにグループ化する(S1503)。

【０１０１】

［画像の編集、印刷］

図14は画像を編集し印刷する処理の流れを示すフローチャートである。

【０１０２】

図3に示す処理によって、原稿画像の各画像について再利用可能なデータが生成され、再利用可能なデータおよびオリジナルデータのポインタ情報が得られると、それら画像の編集が可能になる。勿論、オリジナルデータのセキュリティレベルがユーザのセキュリティレベルより上位ならば、そのオリジナルデータの編集、印刷は不可能である。

【０１０３】

図3の処理に引き続き、ユーザが入力部113を操作して画像編集（または印刷）を指示すると、データ処理部115は文書を表示部116に再表示する(S1601)。図15は再表示文書310を示す図で、文書310には再利用可能なデータまたはオリジナルデータのセキュリティレベル（以下「オブジェクトのセキュリティレベル」と呼ぶ）が「1」の文字オブジェクト312、同「2」の文字オブジェクト313、同「5」の写真オブジェクト314が配置されている。

【０１０４】

ユーザのセキュリティレベルが「4」の場合、ユーザは、下位のセキュリティレベルを有する文字オブジェクト312、313の編集（拡大・縮小、移動・回転、全部または一部削除を含む変更）は可能であるが、上位のセキュリティレベルを有する写真オブジェクト314は例えば網掛け表示になり編集不可能であることが示される。

【０１０５】

次に、ユーザは、オブジェクトを編集する場合、対象のオブジェクトを表示部116上で指定し、入力部113を操作して編集を指示する(S1602)。オブジェクトの指定には、例えばタッチパネルやポインティングデバイスを使用すればよい。

【０１０６】

次に、データ処理部115は、指定されたオブジェクトのセキュリティレベルとユーザのセキュリティレベルを比較して、指定オブジェクトが編集可能か否かを判定し(S1603)、例えば写真オブジェクト314が指定された場合は編集不可であるから、その旨を表示部116に表示して処理をステップS1602に戻す。一方、編集可能であれば、指定オブジェクトの編集処理を可能にする(S1604)。ユーザは、入力部113を操作して指定オブジェクトを編集する。ユーザが入力部113を操作して指定オブジェクトの編集終了を指示すると、データ処理部115は、処理をステップS1602に戻す。

【０１０７】

図16はオブジェクトの編集例を示す図で、文字オブジェクト312について、「プレスリリース」の文字列を拡大し、アンダラインを付加し、さらに日付を追加した例である。

【０１０８】

他方、印刷が指示された場合(S1602)、データ処理部115は、オブジェクトのセキュリティレベルとユーザのセキュリティレベルを比較して、各オブジェクトについて印刷可能か否かを決定し(S1605)、印刷可能なオブジェクトの再利用可能なデータまたはオリジナルデータをレンダリングして印刷データに変換し、印刷データに文書全体および各オブジェクトのポインタ情報およびセキュリティ情報などを埋め込んだ後、印刷データを記録部112に送る(S1607)。

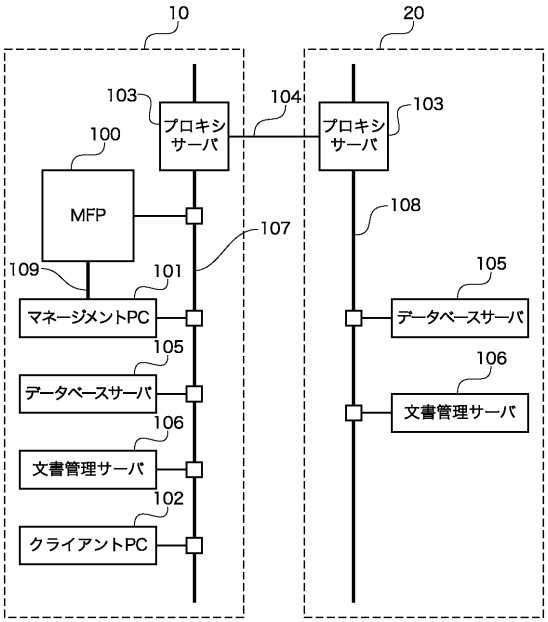
【０１０９】

上述と同様のセキュリティレベルの組み合わせで、図16に示す文書を印刷した場合、写真オブジェクト314を除いた文書が印刷される。勿論、セキュリティレベル5のユーザが印刷を指示した場合は写真オブジェクト314を含む文書が印刷される。

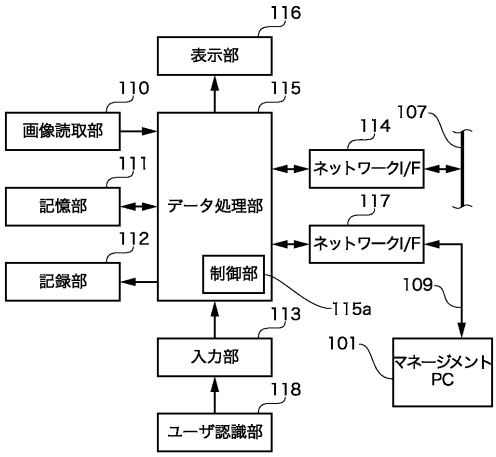
【０１１０】
［変形例］
上記では、二次元バーコードや電子透かしにより、文書全体、各画像のポインタ情報およびセキュリティレベル情報を文書に埋め込む方法を説明したが、図8に示すような情報をフォームデータとして例えばデータベースサーバ105に登録し、二次元バーコードや電子透かしにより、フォームデータが登録されているサーバのポインタ情報およびフォームデータ名を文書に埋め込んでもよい。そうすれば、文書画像をスキャンした際にポインタ情報およびフォームデータ名を抽出し、サーバから必要なデータを取得することができる。
【０１１１】
［他の実施例］
なお、本発明は、複数の機器（例えばホストコンピュータ、インタフェイス機器、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。
【０１１２】
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。
【０１１３】
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。
【０１１４】
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】
【０１１５】
【図１】複合機を使用して情報の電子化を行う画像処理システムの構成例を示すブロック図、
【図２】MFPの構成例を示すブロック図、
【図３】画像処理システムによる処理の概要を説明するフローチャート、
【図４】操作画面の表示例を示す図、
【図５】ブロックセレクションの結果の一例を示す図、
【図６】セグメントの画像データからポインタ情報を抽出する処理を示すフローチャート、
【図７】ポインタ情報を含む原稿画像の一例を示す図、
【図８】二次元バーコードに組み込まれるデータ（三例）を示す図、
【図９】ベクトル化処理の詳細を示すフローチャート、
【図１０】ベクトル化における角抽出処理を説明する図、
【図１１】ベクトル化において輪郭線をまとめる処理を説明する図、

【図１２】ベクトル化で生成したベクトルデータのグループ化処理を示すフローチャート、
【図１３】図形要素の検出処理を示すフローチャート、
【図１４】画像を編集し印刷する処理の流れを示すフローチャート、
【図１５】再表示文書を示す図、
【図１６】オブジェクトの編集例を示す図である。

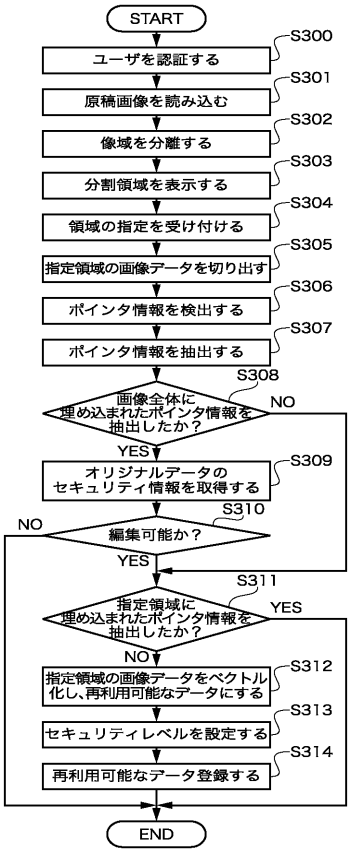
【図１】



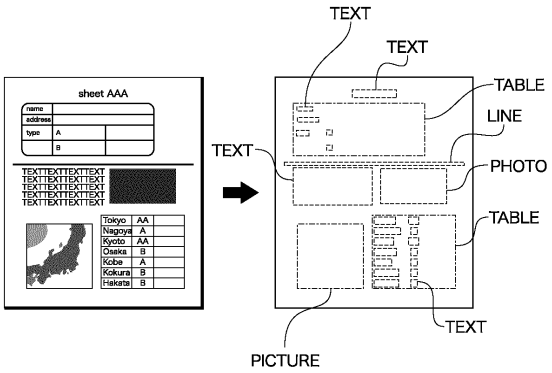
【図２】



【図３】



【図４】



【図５】

ブロック情報

(a)

	属性	座標X	座標Y	幅W	高さH	ポインタ情報
ブロック1	1	X1	Y1	W1	H1	有
ブロック2	3	X2	Y2	W2	H2	有
ブロック3	2	X3	Y3	W3	H3	無
ブロック4	1	X4	Y4	W4	H4	有
ブロック5	3	X5	Y5	W5	H5	有
ブロック6	5	X6	Y6	W6	H6	無

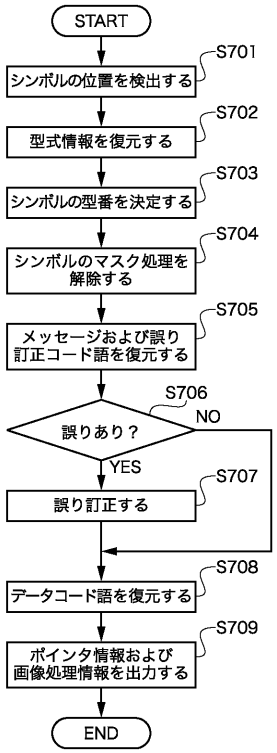
＊ 属性 1:TEXT 2:PICTURE 3:TABLE 4:LINE 5:PHOTO

入力ファイル情報

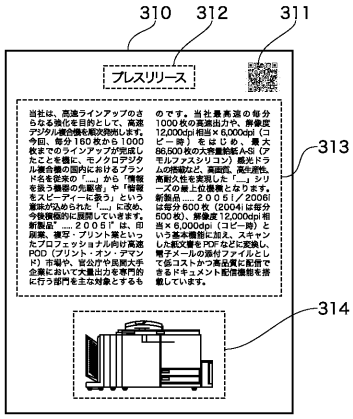
(b)

ブロック総数	N(= 6)

【図６】



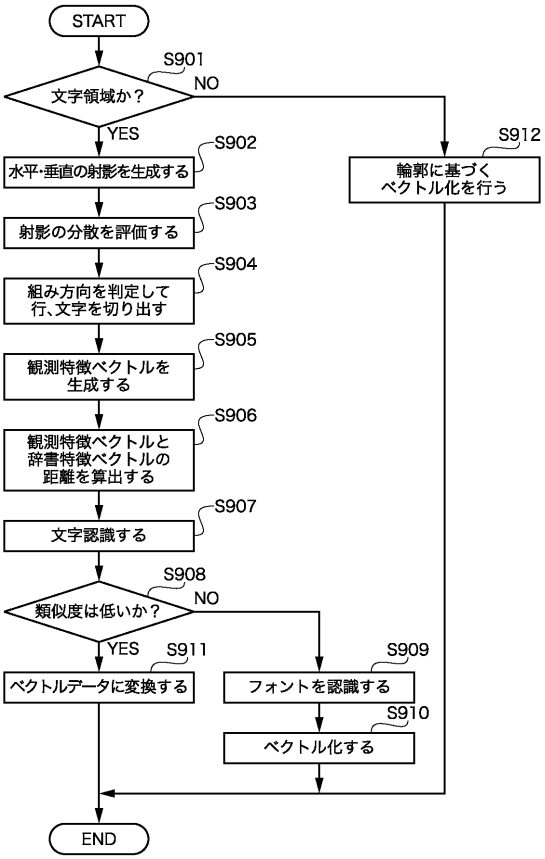
【図７】



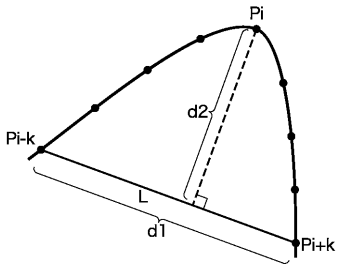
【図８】

画像名	エリア座標	セキュリティレベル	ポインタ情報
Word040211	(10, 10) (100, 200)	1	192.168.100.5
Word040122	(10, 300) (4000, 5000)	2	//server/home/word/
Pict_MFP04	(500, 1500) (5000, 7000)	5	pict…….co. jp

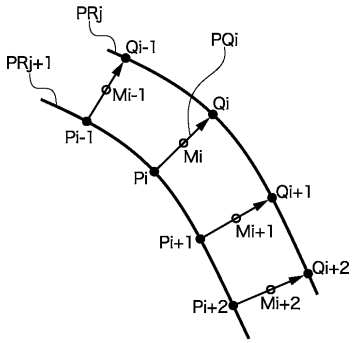
【図９】



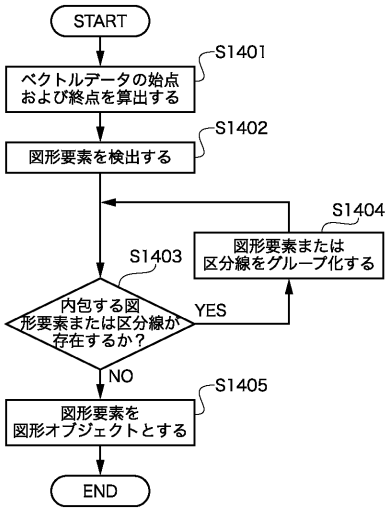
【図１０】



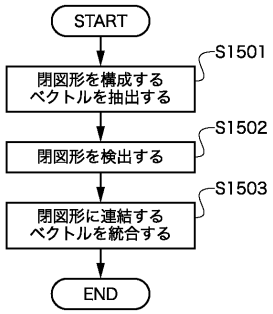
【図１１】



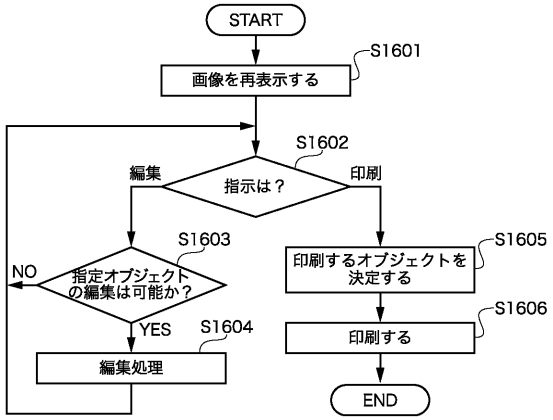
【図１２】



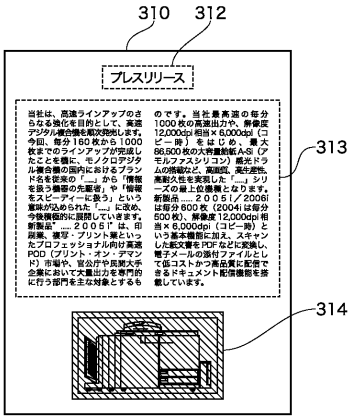
【図１３】



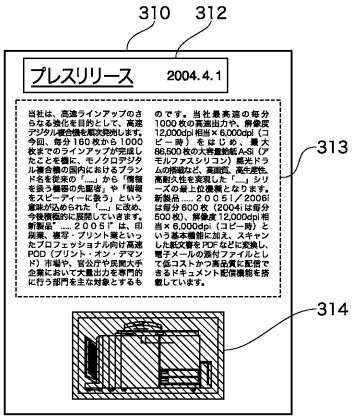
【図１４】



【図１５】



【図１６】



フロントページの続き

(72)発明者　中塚　忠則
東京都大田区下丸子３丁目３０番２号　キヤノン株式会社内

審査官　橋爪　正樹

(56)参考文献　特開２００３－００８８７１（ＪＰ，Ａ）
特開２００４－２２２１８９（ＪＰ，Ａ）
特開２００３－０３２４８８（ＪＰ，Ａ）

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