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

特許第4981641号
(P4981641)

(45)発行日　平成24年7月25日(2012.7.25)　(24)登録日　平成24年4月27日(2012.4.27)

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

請求項の数 20　(全 31 頁)

(21)出願番号	特願2007-313195 (P2007-313195)
(22)出願日	平成19年12月4日 (2007.12.4)
(62)分割の表示	特願2004-505966 (P2004-505966)の分割
原出願日	平成15年5月14日 (2003.5.14)
(65)公開番号	特開2008-160827 (P2008-160827A)
(43)公開日	平成20年7月10日 (2008.7.10)
審査請求日	平成19年12月4日 (2007.12.4)
審判番号	不服2011-11508 (P2011-11508/J1)
審判請求日	平成23年6月1日 (2011.6.1)
(31)優先権主張番号	60/380,189
(32)優先日	平成14年5月14日 (2002.5.14)
(33)優先権主張国	米国 (US)
(31)優先権主張番号	10/287,206
(32)優先日	平成14年11月4日 (2002.11.4)
(33)優先権主張国	米国 (US)

(73)特許権者　511130715
シュレイナー　グループ　ゲーエムベーハー　ウント　コー．カーゲー
ドイツ連邦共和国　オーバーシュライスハイム　ブルックマンリング　２２
(74)代理人　100102978
弁理士　清水　初志
(74)代理人　100102118
弁理士　春名　雅夫
(74)代理人　100160923
弁理士　山口　裕孝
(74)代理人　100119507
弁理士　刑部　俊
(74)代理人　100142929
弁理士　井上　隆一

最終頁に続く

(54)【発明の名称】印刷文書のための可視認証パターン

(57)【特許請求の範囲】

【請求項１】

オブジェクトのアナログ形式がオリジナルアナログ形式であるかどうかを判断する方法であって、以下の工程を含む方法：

認証パターンのオリジナルデジタル表現を作成する工程；

その後で、該オリジナルデジタル表現から可視認証パターンを含む少なくとも１つのオリジナルアナログ形式を生成する工程であって、該少なくとも１つのオリジナルアナログ形式における情報の第１の損失を生じさせる、工程；

該少なくとも１つのオリジナルアナログ形式の認証パターンまたは該少なくとも１つのオリジナルアナログ形式から導出された他のアナログ形式の認証パターンから、デジタル記録を作成する工程であって、作成された該デジタル記録における情報の第２の損失を生じさせる、工程；

作成された該デジタル記録と該オリジナルデジタル表現の非類似性の程度を決定するために、該デジタル記録を該オリジナルデジタル表現と比較する工程；

該記録が少なくとも１つのオリジナルアナログ形式から作成されたことを決定するために、情報の第１の損失と情報の第２の損失の合計である非類似性の程度を使用するとともに、該記録が他のアナログ形式から作成されたことを決定するために、情報の第１の損失と情報の第２の損失の合計より大きい非類似性の程度を使用する、工程；および

多数のテスト認証パターンを生成する工程、該テスト認証パターンを記録する工程、及び該記録されたテスト認証パターンと該オリジナルデジタル表現とを比較する工程を含む

、トレーニングプロセスによって、情報の第１の損失と情報の第２の損失の合計を決定する、工程。
【請求項２】
ネットワーク内のノードで実践され、
少なくとも１つのオリジナルアナログ形式または他のアナログ形式から作成された、該記録をネットワークの別のノードから受け取る工程をさらに含む、
請求項1記載の方法。
【請求項３】
ネットワーク内のノードで実践され、
該デジタル記録が該少なくとも１つのオリジナルアナログ形式または他のアナログ形式から作成されたと判断されたかどうかの表示を別のノードに返す工程をさらに含む、
請求項1記載の方法。
【請求項４】
デジタル記録装置及び出力装置が接続されるプロセッサで実践され、
デジタル記録装置から受け取られる入力からデジタル記録を作成する工程、および、
該デジタル記録が少なくとも１つのオリジナルアナログ形式から作成されたと判断されたかどうかの表示を出力装置に提供する工程、
をさらに含む、請求項1記載の方法。
【請求項５】
非類似性の程度を決定する工程において、決定される内容が該部分のデジタル記録の特徴と該部分のオリジナルデジタルパターンの非類似性であり、該非類似性がオリジナルではないアナログ形式の作成に関与するデジタル記録と印刷を含む動作により引き起こされる、請求項1記載の方法。
【請求項６】
部分のオリジナルデジタルパターンが、人間によってアナログ形式内に認識されうるノイズのあるパターンを有する、請求項1記載の方法。
【請求項７】
ノイズのあるパターンがキーを使用して生成され、
オリジナルデジタルパターンを生成するためにキーを使用する工程をさらに含む、
請求項6記載の方法。
【請求項８】
アナログ形式が少なくとも１つのオリジナルアナログ形式であるかどうかの判断を可能にすることに加え、ノイズのあるパターンがアナログ形式の関数を有する、請求項6記載の方法。
【請求項９】
メッセージが、ノイズのあるパターンから引き出される、請求項8記載の方法。
【請求項１０】
キーを引き出すためにメッセージを使用する工程、および
オリジナルデジタル表現を生成するためにキーを使用する工程、
をさらに含む、請求項9記載の方法。
【請求項１１】
メッセージが、そのために確保されるノイズのあるパターンの部分内にある、請求項9記載の方法。
【請求項１２】
ノイズのあるパターンの少なくとも一部が、背景画像の中またはバーコードの中にある、請求項8記載の方法。
【請求項１３】
認証符号での真正性チェックを実行するために比較する工程の結果を使用する工程
をさらに含む、請求項1～12の何れか1項記載の方法。
【請求項１４】

比較する工程の結果が、記録されたアナログ形式で破壊された記録された認証パターンの一部を示す、請求項13記載の方法。
【請求項１５】
比較する工程の結果が、少なくとも１つのオリジナルアナログ形式からである記録された認証パターンの一部を示す、請求項13記載の方法。
【請求項１６】
認証パターンが、さらにメッセージを含む、請求項13記載の方法。
【請求項１７】
比較する工程の結果が、作成されたテキストによって上書きされる認証パターンの一部を示す、請求項13記載の方法。
【請求項１８】
該オリジナルデジタル表現が画像であって、少なくとも１つのオリジナルアナログ形式を生成する工程がオブジェクト上に該画像を印刷する工程を含む、請求項1記載の方法。
【請求項１９】
該オリジナルデジタル表現がグレースケールイメージまたはカラーイメージである、請求項18記載の方法。
【請求項２０】
オリジナルデジタル表現を作成する工程が、文書のオリジナルデジタル表現を作成する工程であって、
少なくとも１つのオリジナルアナログ形式を生成するために該文書を印刷する工程をさらに含む、
請求項1記載の方法。
【発明の詳細な説明】
【技術分野】
【０００１】
関連出願の相互参照
本願は、本願と同じ発明者を有し、2002年5月14日に出願された米国仮出願第60/380,189号、Method and Apparatus for Copy Protection with Copy-Detectable Patternsから優先権を主張し、さらに2002年11月4日に出願された米国特許出願第10/287,206号、J.Zhaoら、Apparatus and methods for improving detection of watermarks in content that has undergone a lossy transformationからの優先権も主張する。その出願のメッセージベースのキーを使用して埋め込まれる透かし（Watermarks that are embedded using message-based keys）及びデジタル文書及びデジタル文書から作成されるアナログ文書において改変の位置を突き止めるために透かしを使用する（Using watermarks to loate alterations in digital documents and analog documents made from digital documents）の項は参照として本明細書に組み入れられる。米国特許出願第20/287,206号の全てがさらに全ての目的のために本明細書に参考のために添付される。
【背景技術】
【０００２】
発明の背景
1.発明の分野
本発明は概して印刷文書のセキュリティ機能に関し、さらに詳細には印刷文書の可視認証パターンに関する。可視認証パターンは原本の印刷文書をそれらの印刷文書の写真複写と区別し、文書の改変箇所を検出するため、及び非表示及び/または可視メッセージを搬送するために使用できる。
【０００３】
2.関連技術の説明
商業的社会の前提条件とは、偽の製品または偽造品から本物の製品を区別することができることである。文書では、文書の真正性を判断するために答えられる必要のある質問は以下を含む。

・文書は原本または原本の写しか。
・文書は、それが初めて作成されてから改変されたことがあるか。
・文書は認証されているか？
【０００４】
文書自体からこれらの質問に答えることを無理なく可能にするための多くの技法が開発されてきた。文書が原本であるのか、それとも写しであるのかを判断することをさらに容易にする技法は、紙幣に使用される複雑なエッチング、IDカードに使用される写真、及び特殊な用紙を含む。特殊な用紙とインクは改変箇所を検出するために使用されてきた。文書が許可されたものであることを示すための技法は署名及び捺印を含んでいた。
【０００５】
デジタル走査印刷技法の到来により、印刷文書を認証するためには電子透かし（電子透かし）が使用されている。電子透かしは、文書中のグラフィック要素にメッセージを搬送するノイズを加えることにより、文書のデジタル表現の中に埋め込まれるメッセージである。認証目的で使用されるとき、前記メッセージは一般的に目に見えず、グラフィック要素中のメッセージを構成する情報の場所が既知である場合にだけ読み取ることができる。電子透かし技法の調査については、全ての目的のために参照として本明細書に組み入れられる米国特許第6,345,104号、Rhoads、2002年2月5日に発行されたDigital watermarks and methods for security documentsの第17段、27行目から始まる付録Aを参照すること。電子透かしが認証目的のためにどのように使用されてよいのかの例については、2001年6月5日に発光された、米国特許第6,243,480号、Jian Zhao、Digital authentication with analog documentsを参照すること。
【０００６】
複写技術の進歩は、文書の外観からそれが本物であるかどうかを判断できるようにする技法の全ての価値を下落させてきた。この進歩のため、パッケージとラベルの偽造だけではなく、金銭及び金融証書だけではなくIDカードと公文書などの他の文書の偽造も、商標がついた製品の世界的な売上高の5%から8%に及ぶ莫大な損失を引き起こし、ブランド品自体の評判と価値を危うくする。さらに、インターネットの成長が、ウェブ上の数百の会社から容易に且つ匿名で購入できる偽造文書（偽のID、大学の卒業証書、小切手等）のビジネスを動かしている。スキャナ、デジタルイメージングソフトウェア、及びプリンタの精度が高まるにつれ、問題は悪化する一方である。
【０００７】
スキャナ、デジタルイメージングソフトウェア及びプリンタの改良に伴ない必要とされているのは、文書に、文書が原本であるのか、あるいは写しであるのか、文書が改変されているかどうか、及び/または文書が許可されているかどうかを判断できるようにするために情報を追加する新しい方法である。この分野での取り組みには以下が含まれる。
【０００８】
複数の透かしを文書に埋め込む
2001年12月18日に発行された米国特許第6,332,031号、Rhoadsら、Multiple watermarking techniques for documents and other dataは、文書に、そのそれぞれが異なる特性を備える、あるいは異なるドメインにある複数の透かしを埋め込むことを開示している。文書が、偽者を作るために写真複写されるか、走査され、印刷される場合、埋め込まれる透かしは改変されるか、損傷を受ける。透かしの特性またはそれが埋め込まれる領域は、文書が複写プロセスにより改変される程度に影響を及ぼす。したがって、それぞれの透かしの相対的な改変の程度が、文書が原本であるのか、それとも写しであるのかを示すことができる。このようにして透かしを使用することには、以下に挙げる多くの優位点がある。
・それは柔軟である。電子透かしは、単に目立たない修正を文書に取り入れるにすぎないため、理論的にはあらゆる文書に挿入できる。
・それは目に見えないため、それは偽造物の出所を突き止めるために使用できる。
・透かしが存在する可能性により偽造者は文書全体を非常に高い忠実度で複製せざるを得なくなる。

透かしの優位点は、それらの不利な点でもある。機密保護の目的で使用される電子透かしは目に見えないノイズを文書に加えることにより作成されるため、それらは、それらを含む文書が擦り切れに曝される場合、多くの場合読み取ることはできない。それらは文書中のノイズの中に隠されているため、意匠のあらゆる要素が固定され、したがってノイズのための余地がない紙幣などの文書に透かしを隠すことは困難である。

【０００９】

複写機による再生できない情報を埋め込む

文書は、紫外線光では可視であるインクを用いて印刷されるために、可視光範囲では目に見えない部分を含むことがある。可視光を使用して動作する複写機は、それを再生できない。1999年2月9日に発行された米国特許第5,868,432号、Mantegazza、Documents with anticopying means to prevent reproducibility by photocopyingを参照すること。

【００１０】

情報は、依然として走査印刷プロセスが可能とするよりさらに多くの解像度を必要とすることがある。ソースイメージと、特殊なデコーダレンズを通して見られるときにだけ可視である潜像を結合する方法を開示する、1998年11月13日に発行された米国特許第5,708,717号、Alosia、Digital anti-counterfeiting software method and apparatusを参照すること。この潜像は、例えば複数回繰り返される単語「本物」、あるいはIDカードのポートレートにおける個人情報などのさらに文書に特定的な情報を含むことがある。しかしながら、潜像は「サブピクセル」精度で印刷されるため、それは容易に再生できない。今日「サブピクセル」であることが、明日には容易に再生できるようになる可能性があることは言うまでもない。

【００１１】

ホログラムは、それらが人間の目により検出しやすく、高い忠実度で再生するのが困難であると仮定されるためIDカードと紙幣などの文書に挿入される。しかしながら、誰もがホログラムが文書上に存在するかどうかを確かめることができる一方、訓練を受けていない観察者は概してホログラムが本物なのか、あるいはコピーなのかを検出することはできない。

【００１２】

目に見えないコピー防止特徴の共通の問題点

目に見えないコピー防止特徴の全てが抱える問題点は、それらは目に見えないため、それらを読み取るために必要とされる特殊な機器を有していない人にとってはそれらは完全に無用であるという点である。さらに、特徴が目に見えないことにより印刷及び/または検出にまつわる問題点が生じる。透かしを用いた場合、透かしを目に見えない状態にしておく必要性により、必ずやそれらは検出するのが困難であり、それは特に擦り切れが文書に余分なノイズを加えている場合に当てはまる。目に見えないインクを用いた場合は、印刷と検出の両方とも複雑化し、それは「サブピクセル精度」で印刷された潜像でも当てはまる。

【００１３】

必要とされているのは、さらに低い費用で文書が原本であるのか、それとも写しであるのか、文書が改変されているのかどうか、あるいは文書が許可されているのかどうかを確実に判断することができ、一般の人々が、文書が容易に認証されてよいことを確認できるようにし、文書を認証するための他の技法と容易に統合できる技法である。このような技法を提供することが本明細書に開示されている発明の目的である。

【特許文献１】米国特許第6,345,104号
【特許文献２】米国特許第6,243,480号
【特許文献３】米国特許第6,332,031号
【特許文献４】米国特許第5,868,432号
【特許文献５】米国特許第5,708,717号

【発明の開示】

【発明が解決しようとする課題】

【００１４】
発明の要約
本発明の目的は、1つの局面においては、オブジェクトのアナログ形式がオリジナルのアナログ形式である、つまりアナログ形式を写真複写または走査する代わりにオリジナルのデジタル表現から作られたアナログ形式であるのかどうかを判断するための技法により達成される。技法を利用する方法では、アナログ形式から作られるデジタル記録の一部がアナログ形式の一部のオリジナルのデジタル表現と比較され、記録された部分と前記部分のオリジナルのデジタル表現の間の非類似性の程度を決定し、前記非類似性の程度を使用して、アナログ形式がオリジナルのアナログ形式かどうかを判断する。本発明の追加の特徴は、判断される非類似性が、オリジナルではないアナログ形式を作成する上で必要とされる動作により生じる非類似性であるという点である。
【００１５】
この局面の他の特徴は、デジタル記録装置と出力装置が取り付けられているプロセッサにおいて方法を実践することだけではなく、ネットワークの別のノードからデジタル記録を受信するネットワーク内のノードにおいて方法を実践し、別のノードに対し、アナログ形式がオリジナルのアナログ形式であると判断されたかどうかの表示を返すことでもある。プロセッサはデジタル記録装置から受信される入力からデジタル記録を作成し、アナログ形式がオリジナルのアナログ形式であると判断されたかどうかの表示を出力装置に提供する。
【００１６】
本発明の有利な態様においては、部分のオリジナルのデジタル表現は、ノイズのあるパターンを有している。オリジナルデジタル表現はキーを使用して作成されてよく、オリジナルデジタル表現は、アナログ形式がオリジナルであるかどうかの判断を可能にする事に加え、アナログ形式の機能を有する場合がある。前記機能は、バーコードまたは背景画像としての機能を果たすか、あるいはメッセージを搬送することであってよい。
【００１７】
本発明の別の局面は、アナログ形式に関して真正性チェックを実行する方法である。前記方法はアナログ形式のノイズのあるパターンのデジタル記録を、ノイズのあるパターンのオリジナルのデジタル表現と比較し、比較の結果は真正性チェックを実行するために使用される。技法は、ノイズのあるパターンの一部がアナログ形式で破壊されているかどうかを判断するために使用されてよい。ノイズのあるパターンはさらにメッセージを含んでよい。
【００１８】
本発明のさらに別の局面は、アナログ形式でメッセージを隠す方法である。前記方法では、メッセージが隠されている可視のノイズのあるパターンのデジタル表現が作成され、アナログ形式で含まれる。
他の目的及び優位点は、以下の詳細な説明および図面を精読すると、本発明が関係する当業者には明らかとなるであろう。
【００１９】
図面中の参照番号は３桁または４桁以上である。右側２桁は、残りの数字によって示される図面の中の参照番号である。したがって、参照番号２０３の項目は、最初に図２の項目２０３として表示される。
【００２０】
詳細な説明
文書を認証するために透かしの単なる存在だけを使用する
一般的には、透かしを含む文書のための認証技法は、文書中の図形要素に、文書のためのある種の認証情報を隠すために透かしを使用する。例は、前記に言及された米国特許第6,243,480号に説明されるように、文書のキャラクタコードから作成される摘要を隠すために透かしを使用することである。文書の図形要素の中に認証情報を隠すために透かしを使用する技法の困難は、多くの場合文書の擦り切れによって透かしが判読できなくなって

いるという点である。

【００２１】

本願の特許である米国特許出願第10/287,206号は、判読できない透かしから少なくとも何らかの情報を取得する方法、及び透かしを文書の擦り切れにより生じる変形などの劣化を伴なう変形を前にして透かしをさらにロバストにする方法を探っている。米国特許出願第10/287,206号の発明者がその研究の過程で実感した事の中には、第1に、透かしの単なる存在が文書を認証するために使用されること、第2に透かしの単なる存在が、文書がどこを改変されたのかを発見するために使用できるということがある。これらの実現に対処する米国特許出願第10/287,206号の部分は以下のとおりである。

【００２２】

メッセージベースのキーを使用して埋め込まれる透かし：図8及び図9

電子透かしの標準的な応用例は、デジタル表現の中にメッセージを隠すことである。このようなメッセージの用途の1つは、デジタル表現の妥当性を検査すること、あるいはデジタル表現認証することである。つまり、妥当性が検査されているデジタル表現は特定のメッセージを含む透かしを含むと考えられている。透かしは読み取られ、そのコンテンツは特定のメッセージに比較される。それらが一致する場合、デジタル表現は有効、つまり本物である。デジタル表現が劣化を伴なう変形を受けている場合、透かしは判読できなくなる。米国特許出願第10/287,206号で説明される技法により、このような状況における限られた妥当性検証または認証が可能になる。透かしに含まれるメッセージによる妥当性検証にまつわる一般的な問題点は、このような長いメッセージを含む透かしは短いメッセージを含む透かしよりロバストではなく、したがって劣化を伴なう変形により判読できなくなる可能性が高い一方で、妥当性検証が多くの場合社会保障番号や口座番号などの長いメッセージを必要とするという点である。

【００２３】

この一般的な問題点に対する解決策は、妥当性検証または認証の目的で、透かしが、妥当性検証または認証の基礎となるメッセージを実際に含んでいる必要はないという所見に基づいている。つまり必要とされているのは、所与の透かしが、前記透かしが妥当性検証の根拠となるメッセージを使用して作成された場合に限りデジタル表現の中に存在することである。その場合、透かしが判読できる必要はない。代わりに、透かしが単に存在することで、デジタル表現を妥当性検証できる。さらに、デジタル表現が有効、つまり真正であることを示すのは透かしの存在であり、そのコンテンツではないため、透かしのコンテンツは透かしの存在を示す以上に何も行うことはなく、それを行うために必要とされるより長い必要はない。実際には、このような透かしの透かしベクトルは単一のビットの値を指定しさえすればよい。言い換えると、これにより透かしは妥当性検証または認証の根拠となるメッセージを含む透かしよりはるかにロバストになる。

【００２４】

デジタル表現におけるその単なる存在がデジタル表現を妥当性検証する、あるいは認証する透かしを作成する1つの方法は、メッセージを使用して、デジタル表現の中の透かしの場所を突き止めることである。これは図8の801に示されている。キー関数805（ｆ）は、メッセージ803（ｍ）からキー806（K2）を生成するために使用される。K2＝ｆ（ｍ）。必要とされる場合、関数805はキーを生成するためのmだけではなく、秘密鍵K1も使用してよい。K2＝ｆ（K1,ｍ）。次にキー806が、短い（最小1ビット）透かしベクトルVM807と共に透かし埋め込み器809に与えられ、透かし埋め込み器809は、キー806により示される透かしデジタル表現813の中の場所で透かしベクトル807を使用して作成される透かしを埋め込む。透かしはデジタル表現813の中に807とラベルが付けられた点線のボックスにより図8に示されている。メッセージ803はもはや透かしには含まれていないが、代わりにキー806と短い透かしベクトル807を生成するために使用されるため、長さは1ビットあれば十分であり、メッセージの長さは透かしのロバストネスには何の影響も及ぼさない。数学では周知であるように、キー806、したがってそれを用いて作成される透かしがメッセージにとって一意的となるような方法でメッセージ803からキー806を生成するために使用できる多くの

関数がある。必要とされる唯一性の程度は言うまでもなく応用例に応じて変化する。関数が、アイデンティティ関数であってよい、つまりキーがメッセージ自体である場合もある。前記技法の優位点は、関数が透かしキーの長さを決定し、したがってキーは、それが特定の応用例に必要とされる長さに生成できるという点である。

【００２５】

図9は、901で、デジタル表現903がちょうど説明した方法で作成された透かしを含むと考えられているかどうかを判断するシステムが本物であることを示している。デジタル表現903は、デジタル表現903が実際にデジタル表現813から引き出されている場合に透かしベクトル807を含まなければならない場所905の集合を含んでいる。場所は、デジタル表現813においてキー806によって決定された位置にある。認証を行っているシステムはメッセージ803を取得し、キー関数805も取得する、あるいは所有している。キー関数805は前述したようにキー806を生成するためにメッセージ803に適用される。システムは、次にキー806を、それを使用して場所905を検出する透かし読取装置907に提供する。場所が検出されると、それは909に示されるようにコンパレータ909に出力される。短い透かしベクトル807もシステム901を所有しており、それは順々に場所905のそれぞれの値と比較するためにコンパレータ911に提供される。それぞれの比較の結果912は集約器913に移動し、そこで結果は集約させ、デジタル表現813の中に埋め込まれた透かしがデジタル表現903の中に存在するかどうかを示す全体的な結果915を作成する。コンパレータ911及び集積器913は、前記比較及び前記集約を行うために判読できない透かしに関して前述した技法のどれかを使用できる。前述したように、判読できない透かしと共に使用される技法について、デジタル表現813の中の透かしに一致する場所905のパターンが、デジタル表現903が改変された場所を示すために使用されてよい。

【００２６】

いくつかの応用例では、集約器913は比較の視覚的な結果を作成する。このような比較の例は図5の501に示されている。そこでは、透かしが適用されたブロックは、透かしの存在が検出された程度に応じてさまざまな陰影を有する。ブロックが明るいほど、ブロックの中での透かしの存在は強い。画像501は劣化を伴なう変形を受けているため、強力な透かしのあるブロックの分布はオリジナルにおいてと同じではないが、劣化を伴なう変形により生じるエラーは無作為であり、その結果として、画像が本物である場合には、透かしを含む全ての領域が501に示されるように明るいブロックのほぼ同じ分布を有するはずである。この視覚化技法は、言うまでもなく、メッセージが透かしのコンテンツを決定する透かしと共に使用できる。

【００２７】

デジタル文書及びデジタル文書から作成されるアナログ文書での改変箇所を突き止めるために透かしを使用する

デジタル文書または前記デジタル文書から作成されるアナログ形式を攻撃する1つの方法は、前記文書または形式の中の画像を局所的に修正し、その意味論的なコンテンツを変更することである。局所的な修正の例は、以下の場合がある。

・事故/犯罪の場面でDVRによって捕捉される車の画像のプレートナンバーを修正すること；または

・IDカード上のポートレートの領域を修正すること；または

・ID文書のポートレートを置換すること。

文書または形式が透かしを入れられる場合、偽造者の目標は、透かしを間違いに、または判読不能にせずにデジタル文書または形式の意味論的なコンテンツを変更することである。一般的には、透かしが判読できるほど十分にロバストであるとき、偽造者が透かしを間違いにまたは判読不能にせずに文書または形式で小さな変更を加えることは困難ではないであろう。他方、透かしが非常にロバストであると、透かしは改変箇所を検出、追跡調査するのに有用になる。

【００２８】

改変箇所の位置を突き止めるために透かしを使用するため、透かしがあると予想される

場所とその透かしベクトルを知っていさえすればよい。技法は、透かしが特定のコンテンツを有することを必要としないため、透かしベクトルは単一のビットでありさえすればよい。検出器がいったん透かしの場所と透かしベクトルを知ると、検出器は、オリジナルの透かしの透かしベクトルwのレプリカである透かしベクトルw’を使用し、w’を疑わしいコンテンツの中の透かしw”と比較できる。w’とw”の相違点は、疑わしいコンテンツのソースとであるデジタル文書またはアナログ形式が修正されているかどうか、及び修正されている場合には、どの部分が修正されたのかを示してよい。

【００２９】

さらに詳細には、検出器はデジタル文書またはアナログ形式のそれぞれの下位区分（ここではブロックと呼ばれる）の中の透かしベクトルw”を、ベクトルw’と比較する。前記比較は、文書または形式の各ブロックが正しい透かし情報を保持しているかどうかを示す。デジタル文書では、改変箇所がない場合には、大部分のブロックが正しい透かし情報を含むであろう。アナログ形式を用いると、印刷と走査のプロセスが透かしを劣化させ、結果的に全てのブロックが正しい透かし情報を保持するわけではない（例えば、約20％から40％のエラーがある場合がある）。これらの印刷エラーと走査エラーは、一般的にはランダムな性質であるため、多かれ少なかれ均一にアナログ形式で分布されると予想できる。したがって、画像が局所的に改変され、それにより改変された領域でその透かしを失った場合、透かし検出器は、それが透かしが入れられていない領域に応答するのと同じように改変された領域に応答するであろう。こうすることで、透かし検出器は改変箇所を検出する。前記技法は、画像のそれぞれの領域での透かしの強度を示すためにも使用できる。

【００３０】

改変箇所または透かし強度を検出するために使用されるレプリカ透かしベクトルは任意のソースから出現してよい。例はオリジナル画像、無事に読み取られた疑わしいコンテンツからの透かしベクトル、あるいはメッセージから新たに作成された透かしベクトルを含む。適応埋め込み及び検出は改変箇所を検出する効果を高めるために使用されてよい。例えば、変更に対する特殊な保護を必要とするコンテンツの領域は、コンテンツの他の領域よりさらに大きな強度の透かしを受け取ってよく、これらの領域での透かしの前記さらに大きな強度は、透かしが前述されたように分析されると考慮に入れられてよい。言うまでもなく、画像の各領域での透かしの強度を示すために使用されるような技法は、適応埋め込み及び検出のためのマスクの設計に役立てるために利用されてもよい。

【００３１】

統計、信号処理、またはパターン認識により着想されるさまざまな技法が、間違った情報を保持する（あるいはまったく情報を保持しない）異常に多数のブロックを含む領域を自動的に検出するために適用できる。例えば、パターン認識から着想される1つの技法は、間違ったブロックのつながりを突き止め、閾値より高いそれらのつながりを抽出することである。別の技法は、P個より多い間違ったブロックがあるかどうかを、アナログ形式のサイズNxNの全ての領域で判断することであろう。信号処理からの別の技法は、正しいブロックに正の値を、間違ったブロックに負の値を割り当て、次に結果として生じる行列を低域濾波することである。値が閾値未満である濾波された行列の領域は改変されたとして検出される。最後に、改変されていない画像、及び改変されている画像の領域を特徴付け、ユーザの期待に相対して検出パラメータ（例えば、改変された領域の最小サイズ、偽警報/拒絶の確率等）を決定するための全ての手法で統計を適用することができる。ユーザに、間違ったブロックと正しいブロックのある画像を別々の色で表示し、データの人間による解釈を可能にすることもできる。

【００３２】

図5は、透かし強度に対する改変の影響を示し、改変された領域を示す図式方法の例も提供する。ここでは、画像501は、それが、画像501の中の顔に透かしが入れられたように透かしが入れられなかった別の顔と顔を置き換えることにより透かしを入れられた後に修正された。修正の結果は画像502である。画像502が画像501と比較されると、画像502の顔の領域は画像501の顔の領域より暗いことが分かるであろう。これは、同様に、画像502の

顔領域が画像501の顔領域のブロックよりはるかに弱く透かしを入れられていることを示している。画像502の顔領域の弱い透かしは言うまでもなく修正の直接的な結果である。多くの弱いブロックを持つ領域を強調表示するフィルタが適用されると、結果として修正された領域505が明確に際立つ画像503が生じる。

【００３３】

技法の拡張

・1つより多くの改変領域を検出すること。

・最も意味論的に重要な領域（例えばID写真の目）に改変の検出を集中するために外部モジュール（例えば顔認識）を使用すること。

・走査可変を無効にするために物理文書を複数回走査すること。

透かしが判読できない場合、改変箇所検出はその判読不能の理由を解析するために使用されてよい。

【００３４】

可視認証パターン

前記実現の後に本発明につながる実現が続いた。つまり、透かしの単なる存在がアナログ形式の真正性を判断するために使用されている時、透かしはコンテントのないパターンとして使用されている。パターンにコンテンツがないため、それが目に見えない必要はなくなった。代わりに、それは可視要素として文書に追加できる。以下では、認証のために使用される可視パターンは可視認証パターンつまりVAPと呼ばれる。VAPは可視であるため、それは透かしよりはるかに検出しやすい。しかしながら、目に見えない透かしの認証機能の全てを実行することは依然として可能であり、加えてそれは文書の消費者に文書の真正性が保護されていることを知らせる。

【００３５】

専門用語

詳細な説明においては、デジタル表現とアナログ形式の関係性を明確にするために以下の専門用語が使用されるであろう。

【００３６】

オブジェクトのデジタル表現は、前記オブジェクトがデジタル処理システムに記憶され、デジタル処理システムにより処理される前記オブジェクトの形式である。オブジェクトは、構成要素として、文書、画像、音声、ビデオまたはデジタル表現を作成できる任意の他の媒体であってよい、あるいはそれらを含んでよい。

【００３７】

デジタル表現のアナログ形式は、デジタル表現がディスプレイ、プリンタまたはラウドスピーカなどのアナログ装置に出力されると生じるオブジェクトまたは構成要素の形式である。

【００３８】

アナログ形式のデジタル記録は、前記アナログ形式から作られるデジタル表現である。デジタル記録が作られる方法は、媒体に依存する。例えば、文書または画像の場合、デジタル記録は文書または画像のアナログ形式から作られる画像をデジタル化することにより実行される。

【００３９】

オリジナルデジタル表現は、そうすることが許可された誰かによって作成されるまたはコピーされるデジタル表現である。オリジナルアナログ形式は、オリジナルデジタル表現から作られるものである。

【００４０】

オリジナルではないデジタル表現は、アナログ形式を許可なくデジタルで記録することにより作成されるものである。オリジナルではないアナログ形式は、オリジナルではないデジタル表現から、あるいはアナログ形式を写真複写することにより作成される。

【００４１】

用語のさらに普通の意味での文書、ラベル、パッケージ、及びそれら自体が刻み込まれ

ているオブジェクトを含む文書には、印刷プロセスにより作成される任意のアナログ形式の特殊な意味が与えられる。妥当な類推が及ぶ範囲まで、文書について言われる以下の全てが他の媒体にも当てはめられてよい。例えば、音声アナログ形式は、VAPの音声同等物である可聴認識パターンを含んでよい。

【００４２】

可視認証パターンを生成する：図1

可視認証パターンのパラドックスは、パターンは目に見える一方、偽造容疑者は、本物ではない文書をそれが認証するようにパターンを修正することができてはならないという点である。好ましい態様では、この目的は、パターンをノイズが多くすることにより達成される。つまり、パターンを構成するピクセルの値の大部分が明らかに無作為に決定される。パターンにノイズがあるため、パターンオリジナルデジタル表現にアクセスせずに、パターンのデジタル表現を構成するピクセルがどの値を有さなければならないのかということは不可能である。他方、VAPのオリジナルデジタル表現を得ると、文書からのVAPのデジタル記録をVAPのオリジナルのデジタル表現と比較し、VAPのオリジナルのデジタル表現に関して記録されたVAPがどのようにして改変されたのかを突き止め、相違点から、問題の文書がどのように改変されたのかを判断することができる。以下でさらに詳細に分かるように、検出できる改変は、オリジナルではない文書を作成する際に含まれるもの、及び文書中の情報を改変する際に含まれるものを含む。

【００４３】

図1は、可視認識パターンを生成し、文書中にそれを挿入する1つの方法を示している。以下の3つの段階がある。

・101に図示されるパターンのデジタル表現を作成する。

・107に図示される認証パターンに目に見えるロゴまたは説明文を追加するオプションの工程。

・113に図示される文書中に認証パターンを挿入すること。

パターン105のオリジナルデジタル表現は、パターンのピクセルが強力な無作為成分を含む値を有すると思われる結果を生じさせる方法で作成できる。パターン105のデジタル表現はグレースケールパターンであってよい、あるいはそれは着色されたピクセルを利用してよい。パターンを生成するためにキーを利用することは特に有用である。キー103は、パターンの中のピクセルに与えられる値のシーケンスを作成する擬似乱数生成プログラムのためのシードとして使用される。キーの使用は以下に詳述される。パターン105のオリジナルデータ表現は、パターン105を含む文書を走査することにより作成されるデジタル表現でパターンの位置を突き止める際に役立つ構成要素も含んでよい。パターン105では、黒い境界線106がこの機能を果たす。

【００４４】

目に見えるロゴまたは説明文109は、パターンを構成するピクセルの値の一部だけしか無作為に求められる必要がないため、パターン105のノイジネスを危うくすることなくパターン111のオリジナルデジタル表現を作成するために、パターン105のオリジナルデジタル表現に加えることができる。このようにして、ロゴまたは説明文は、ロゴまたは説明文を表示させる一方でそれらのランダム性を保つようにロゴまたは説明文を作成するピクセルの値を操作することによりパターン105の上に重ねることができる。例えば、パターン105がグレースケールパターンである場合、説明文またはロゴは、説明文またはロゴのピクセルをそれらのオリジナルのランダム値を基準にして均一にさらに暗くする、またはさらに明るくすることによって作成できる。前記技法は、それがパターン105のノイジネスを保つという点を除き、画像に可視透かしを追加することに類似している。

【００４５】

パターン111のオリジナルデジタル表現がいったん作成されると、それは113に示されるように文書115のオリジナルデジタル表現に挿入される。文書117がオリジナルデジタル表現115から印刷されるとき、文書117は印刷された可視認証パターン119を含む。言うまでもなく、文書は、すでにその上に印刷物を有する基板の上にも印刷されてよい。このよう

にして、パターン119は事前に印刷された基板に追加されてよい。

【００４６】

文書を認証するために可視認証パターンを使用する：図2及び図3

印刷されたVAP 119を含む文書が認証されるとき、以下が起こる。

・印刷されたVAP 119が文書で検出される。

・検出された印刷済みVAP119のデジタル記録が作成される。

・印刷済みVAPのデジタル記録がVAPのオリジナルデジタル表現と比較される。

・比較に基づき真正性が決定される。

印刷されたVAPのデジタル記録がVAPのオリジナルデジタル表現に比較される方法は、実行される認証の種類に依存する。さらに、指定される文書の認証は、デジタル記録とオリジナルデジタル表現の間で行われる複数の異なる種類の比較も必要とする可能性がある。例えば、小切手の金額フィールドでの可視認証パターンのデジタル記録は、第1にオリジナルデータ表現と比較され、小切手が偽造品かどうかが判断され、第2に金額フィールドの金額が改変されているかどうかが判断される。

【００４７】

図2は、好ましい態様で印刷されたVAPを検出し、VAPのデジタル記録を作成することを示している。両方とも、メディアセックテクノロジーズ（MediaSec Technologies）から入手可能な「スキャンリード（Scanread）」アプリケーションプログラムを使用して行われる。文書の一部を検出し、そのデジタル記録を作成する他のアプリケーションも利用されてよい。スキャンリード201は黒い境界線106を使用して、印刷文書117における可視認証パターン119の存在を検出してから、可視認証パターン119のデジタル記録203を作成する。図3は、VAP 119のデジタル記録203及びオリジナルデジタル表現111を使用して真正性を判断するプログラムの一般的なフローチャート301を示している。VAPのオリジナルデジタル表現111はそれ自体オリジナル、オリジナルのコピー、最初のオリジナルデジタル表現とまったく同じように作成される新しいオリジナルデジタル表現111であってよい。これらの方法のどれかにより取得されるオリジナルデジタル表現は、言うまでもなく正確に同等であり、どの方法が使用されるのかは、VAPのオリジナルデジタル表現の保管の費用、ネットワーク全体でVAPのオリジナルデジタル表現を送信する費用、及びそれが必要されるたびにオリジナルデジタル表現を作成する費用などの実現の問題点の問題である。

【００４８】

303で開始して、デジタル記録203とオリジナルデジタル表現111の特徴は305で比較される。どの特徴が比較され、それらがどのように比較されるのかは実行される認証の種類に依存する。デジタル記録203とオリジナルデジタル表現111の相違点が閾値（307）を超える場合には、認証の問題があり、分岐309が取られる。閾値も実行されている認証の種類に依存する。分岐309では、311で、問題の存在が、認証を実行しているアプリケーションプログラムに示される。それが有用である場合、プログラムは比較（315）についての情報も提供してよい。また、情報の種類及びそれがどのように提供されるのかはやはり認証の種類に依存する。例えば、金額フィールドの金額が改変されたと思われる場合、プログラムは、オリジナルデジタル表現のピクセルのどれが可視認証パターンのデジタル記録で改変されたと思われるのかを示す画像を表示してよい。差異が閾値を超えない場合、分岐317が取られる。そこで、認証の問題が検出されなかったという事実が、認証を行っているアプリケーションプログラムに示される。分岐とプログラムの両方とも321で終了する。

【００４９】

オリジナルではない文書からオリジナル文書を区別するために可視認証パターンを使用する：図4、図5

文書を認証するために可視認証パターンを使用できる1つの方法とは、文書がオリジナルであるか、つまりオリジナルデジタル表現から印刷されたかどうか、あるいはオリジナルでないのか、つまり文書から写真複写されたかまたはオリジナルではないデジタル表現から印刷された、つまり文書の許可されていないデジタル記録から作成されたデジタル表

現であるかどうかを判断することによる。可視認証パターンをこのようにして使用できる理由とは、印刷プロセス、デジタル記録プロセスまたは写真複写プロセス文書がいかに正確であるのかに関係なく、文書をそのデジタル表現から印刷し、そのデジタル記録から文書のデジタル表現を作成すること、あるいは文書を写真複写することが常に可視認証パターンの情報の損失を生じさせるためである。結果として、文書がオリジナルであるのか、あるいはオリジナルではないのかに関係なく文書から可視認証パターンを記録することにより作成されるデジタル表現と可視認証パターンのオリジナルデジタル表現を比較することにより判断できる。オリジナル文書のケースでは、可視認証パターンは一度印刷され、デジタルで一度記録される。オリジナルではない文書のケースでは、可視認証パターンは、オリジナルではない文書の作成元のオリジナル文書を作成するために、一度、印刷され、デジタルで記録され、次にオリジナルではない文書がどのように作成されたのかに応じて、写真複写されるか、または再び印刷されデジタル記録され、オリジナルではない文書の可視認証パターンの中では、オリジナル文書の可視認証パターンにおいてよりかなりの量の情報が失われる結果となる。

【００５０】

基本的な技法は、図4に詳細に示されている。401では、可視認証パターンを使用する認証がオリジナル文書とどのように連動するのかが示されている。文書のオリジナルデジタル表現403はオリジナル可視認証パターン（ovap）405を含む。次に、オリジナルデジタル表現403はオリジナルアナログ形式409を作成するために407で印刷される。印刷動作により、アナログ形式409のオリジナルアナログ可視認証パターン（oavap）411にloss 1が生じる。認証符号421がアナログ形式409を認証すると、それはoavap 411のデジタル記録を作成し、loss 2を生じさせる。記録はroavap 415のように見える。認証符号421は、次にコンパレータ417を利用し、ovap 406をroavap 415と比較する。それらの差異がloss 1とloss 2の合計である。それは、それ以外の損傷を受けていないroavap 415がovap 405と比較され、そのサイズの差異が、アナログ形式409が実際にオリジナルアナログ形式であるという信頼できる表示であるときに当てはまるであろう。

【００５１】

420では、認証がどのようにしてオリジナルではない文書と連動するのかが分かる。オリジナル文書とオリジナルではない文書の相違点は、オリジナルではない文書が文書のオリジナルデジタル表現403から直接的にではなく、代わりにオリジナル文書409をデジタルで記録すること（422）により作成された文書のオリジナルではないデジタル表現423から印刷されているという点である。デジタル記録の結果として、デジタル表現423の中のオリジナルではない可視認証パターン425は、図4にloss3として表示される情報の追加の損失を被っている。オリジナルではないアナログ形式429がデジタル表現423から印刷されるとき（427）、loss 4として示される別の損失がオリジナルではないアナログ視覚認証パターン431で発生する。オリジナルではないアナログ形式429は前述したように認証符号421により認証され、noavap 431から生成されるrnoavap 435がovap 405と比較されるとき、loss 3とloss 4の影響が、ovap 405とroavap 415の間にあったよりさらに大きな差異としてovap 405とrnovap 435の間に出現するであろう。オリジナルではないアナログ形式429のnovap 431は常に追加のloss 3とloss 4を受けるため、前記さらに大きな差異はオリジナルではない文書の信頼できるインジケータである。

【００５２】

オリジナルではないアナログ形式429は、言うまでもなくオリジナルではないデジタル表現423を作成するためにオリジナルアナログ形式（422）を記録してから、オリジナルではないアナログ形式429を作成するためにデジタル表現423を印刷する（427）プロセスによってだけではなく、写真複写プロセスによっても作成できる。オリジナルアナログ形式409の画像を獲得してから、前記画像からオリジナルではないアナログ形式429を印刷するプロセスにより、損失3と4の追加損失のような追加損失が生じ、結果的にこのようにして生じたrnoavap 435は依然としてroavap 425よりovap 405に類似していないであろう。

【００５３】

言うまでもなく、オリジナルではないデジタル表現423がそれ自体オリジナルではないデジタル表現から作成される場合、rnovap435はそのオリジナルではないデジタル表現の写真複写または印刷及びデジタル記録の結果生じる追加の損失も含むであろう。loss 1とloss 2が固定値であるならば、検出器が、文書がオリジナルであるのか、それともオリジナルではないのかを常に正しく判断できるのは明らかである。しかしながら、一般的にはそれぞれの損失に何らかの変動が発生する。例えば、いくつかのオリジナルは他よりさらに優れた品質（忠実度）をもって印刷できるであろう。検出に対する統計的な手法が利用される必要があると思われる。

【００５４】

オリジナル文書とオリジナルではない文書を区別するための技法の好ましい態様の詳細：図6及び図7

認証技法は、その信頼性と同程度に良好であるにすぎない。検出エラーの確率を最小限に抑えるキーは、文書から記録された視覚認証パターンが、前記視覚認証パターンのオリジナルデジタル表現とどの程度「異なる」のかを測定するための方法である。選ばれた測定方法は、オリジナルではない文書を作成するプロセスにより影響を及ぼされるVAPの特性に基づいていなければならず、オリジナルではない文書からオリジナルを明確に区別しなければならない。

【００５５】

我々の手法は、フィルタとして、さらに詳細には低域フィルタとして写真複写プロセス、記録プロセス及び印刷プロセスを考慮することである。したがって、高周波は、印刷プロセスと記録プロセスにより低周波よりさらに減衰され、各記録と印刷工程または写真複写工程でさらに多くの情報を失うであろう。記録プロセス及び印刷プロセスまたは写真複写プロセスがほぼ全てのエネルギーを保存する低周波の場合、オリジナルではない文書のVAPは、オリジナル文書のVAPより大幅に多い情報を持つ可能性がある。非常に高い周波数も、VAPでのこれらの周波数でのエネルギーの大部分はVAPが最初に印刷されたときに失われてしまうため、役立たない可能性がある。その結果として、オリジナル文書のVAPさえそれらの周波数からほとんど情報を含んでいない。したがって、検出器によって使用される周波数の適切な選択及び/または重みづけを行わなければならない。文書がオリジナルであるのか、あるいはオリジナルではないのかを判断するための閾値の選択だけではなく、比較のための周波数の選択も、通常、オリジナル文書からVAPでの比較ソフトウェアを訓練することにより行われる。

【００５６】

ここでは、前述した技法が特殊な視覚認証パターンを必要としないことが指摘されなければならない。代わりに、文書全体またはその一部がパターンとして使用できる。しかしながら、多くの文書には、文書がオリジナルであるのか、あるいはコピーであるのかを判断するために必要なエネルギーレベルでの情報が含まれないため、適切なエネルギーレベルでの情報を含む視覚認証パターンを使用するほうがよい。以下においては、このような視覚認証パターンはコピー検出パターン、つまりCDPと呼ばれる。CDPの情報は適切な周波数で分散される。好ましい態様においては、CDPのオリジナルデジタル表現はキーにより擬似ランダムに作成され、その結果キーにアクセスできるプログラムが常にCDPのオリジナルデジタル表現の新しいコピーを作成できる。このキーは秘密に保たれる、あるいは信頼を受けた関係者だけに明らかにされる。コピー検出パターンは、保護される文書の上に挿入される、あるいは印刷される。好ましい態様においては、文書からのコピー検出パターンの分析は、文書のCDPをデジタル記録し、CDPのオリジナルデジタル表現の新しいコピーを作成するためにキーを使用し、記録されたCDPをCDPのオリジナルデジタル表現と比較することにより行われる。他の態様においては、記録されたCDPはCDPのオリジナルデジタル表現の既存のコピーと単に比較されるだけでよい。

【００５７】

技法で使用されるアルゴリズム

本項では、（1）CDPのオリジナルデジタル表現を作成する、（2）CDPを検出し、文書か

ら抽出する、（3）CDPのオリジナルデジタル表現を記録されたCDPと比較する、及び（4）CDPがオリジナルであるのか、それともオリジナルではないのかを判断するために称されるアルゴリズムについて説明する。CDPがアルゴリズムに比較される（4）方法、及びCDPがオリジナルであるのか、それともオリジナルではないのかを決定するための閾値は、トレーニングデータを収集するためにアルゴリズム（3）が使用されるトレーニングプロセスにより求められる。

【００５８】

CDPのオリジナルデジタル表現を作成する

関数make_patternは、オリジナル文書の作成元のデジタル表現のソースで識別されてよいコピー検出パターンのデジタル表現（pattern_img）を作成するために使用される。make_patternは、ノイズのあるグレースケールまたはカラーパターンを作成する。文書中のその検出を容易にするためにパターンに黒い境界線を追加してもよい。CDPは任意でロゴも表示してよい。ロゴは通常、最低の周波数バンドに影響を及ぼすため、その検出に対する影響は制限される。典型的な値はパラメータの説明に示される。

pattern_img=make_pattern(type, height, width, key, filename, border, logo_img, logo_weight)

【００５９】

パターン生成のためのパラメータ

以下を必要とした。

1.Type（型）：「randn」（ガウス分布N（0,1）、「rand」（蓋然性が等しい分布）、「randint」（二進＋1または-1分散）またはMD5、SHAアルゴリズム（0から255の整数）などの生成された乱数値の型。次に、乱数値はグレースケールまたはカラーイメージを作るために使用される。

2.Height（高さ）：ピクセル単位のパターンの高さ（例えば、104）

3.Width（幅）：ピクセル単位のパターンの幅（例えば、304）

4.Key（キー）：乱数生成プログラムのためのシードとして使用される整数値の秘密鍵またはパスワード

オプション：

5.Filename（ファイル名）：パターン画像が保存されるファイルの名称

6.Registration mark（見当合わせマーク）：（例えば、パターン画像の両側に加えられる黒い境界線、パターン画像の４つの角で点を追加する）

7.Logo_img：自動的にパターン画像の寸法に増減される背景ロゴとして使用される画像

8.Logo_weight：パターン画像に重ねられるロゴ画像のエネルギーを荷重するための0と1の間の値（例えば0.2）

【００６０】

パターン生成アルゴリズムの使用例

1.特定のドメイン内でパターンを生成（例えば、DCT輝度またはカラーRGBモードでの空間）：

pattern= generate_pattern(type, height, width, key))

1.工程1のドメインが空間ではない（例えば逆DCT）場合に空間領域にパターンを変形:

pattern_img=transform(pattern))

3.必要とされる場合、ピクセル値pを整数値0＜p＜225に切り上げる。

4.ロゴをパターンに結合する。例えば以下の関数を混合;

pattern_img=(1-logo_weight)*pattern_img+logo_weight*logo_img

5.見当合わせマーク（例えば黒い境界線）を追加する。

6.画像をダンプする。

パターン画像は、赤、青、緑、または前記工程1と2に説明したように生成できるYUVなどの複数の成分/チャネルから構成されてよい。

【００６１】

CDPをロゴまたは背景画像と結合するためには、多様な混合関数を採用できる。例えば

、CDPがバーコード（画像）とマージされるとき、CDPはバーコードの黒の領域だけを置換し、白い領域はそのまま残す。

【００６２】

パターン画像の（円、楕円などの）任意の形状が生成できる。簡略な手法は、「1」と「0」から構成される二次元アレイにより表現される任意の形状を画定する「形状マスク」を使用することである。「形状マスク」を矩形のパターン画像に適用することにより、任意の形状を生成できる。

【００６３】

VAPを検出し、文書から抽出する

この実施では、認証されている文書のデジタル記録が作成され、VAP上の黒い境界線がデジタル記録内でVAPの位置を突き止めるために使用される。黒い境界線は、容易に検出可能である遷移領域での輝度の強力な変動を生じさせる。VAPの場所を突き止めるための他の技法も使用されてよい（文書内の卵形の既存の特徴、黒い点等）。いったんVAPが検出されると、デジタル表現が、VAPのオリジナルデジタル表現に匹敵するそれから作られる。デジタル表現は記録されたVAPである。

【００６４】

VAPのオリジナルデジタル表現及び記録されたVAPは、記録されたVAPがVAPのオリジナルデジタル表現からどの程度「近い」のかを示す指数を測定する以下の関数を使用して比較される。VAPのオリジナルデジタル表現は、検出器のメモリ内に記憶することができる、あるいは検出器が、オリジナルデジタル表現及び関数make_pattern（..）を生成するために使用されるパラメータを使用できる場合に生成し直すことができる。ロゴは通常パターンの特性にわずかにだけ影響を及ぼすため、パターンをロゴと結合するときに使用されるオプションのパラメータは必要とされない可能性がある。比較を行うための関数は、Results（結果）を返すanalyze_patternであり、実際に適用されるシナリオに応じて異なるパラメータを取ってよい。

Results = analyze_pattern(type, height, width, key, ..., test,_img)

あるいは

Results = analyze_pattern(orig_img, test,_img)

パラメータ及び出力：

1.type、height、width及びkey：これらは、説明されているように、パターン生成のためである。

2.text_img：文書から抽出されるテストパターン画像

3.orig_img：パターンのオリジナルデジタル表現

4.Results：分析の全ての結果を含む。例えば、それは、画像のさまざまな要素、例えば、さまざまな周波数、さまざまな領域、さまざまなカラーチャネル等のために計算された相関関係または統計のさまざまな基準を含んでよい。

【００６５】

以下の例は、オリジナルデジタルパターンが生成し直されるアルゴリズム及びアルゴリズムに必要とされるサブファンクションを示す。

1.（オプション）テストCDPから黒い境界線を取り除く。

2.テストパターン画像を、それが最初に生成されたドメイン、例えば8x8ブロックDCTに変形する。

test_pattern=transform(test_img))

3.オリジナルCDPを生成し直す。

pattern=make_pattern(type, height, width, key)

4.（オプション）後述されるように、テストCDPをオリジナルCDPと局所的に同期させる。（オプション）オリジナルCDPとのより優れた相関関係を生じさせるために、（鋭くするなどの）一定の画像フィルタをテストCDPに適用する。

5.必要とされる場合、オリジナルCDPとテストCDPを、比較が行われるドメイン（例えば、8x8のブロックDCT）に変換する。比較が1つより多くのドメイン、例えば空間領域と周波

数領域の両方で行うことができることに留意する。
6.オリジナルCDPとテストCDPの類似性の複数の計算値を変形されたドメイン内のチャネルごとに計算する。例えば、パターンが生成され、カラーRGBドメインに記録され、分析が8x8ブロックDCTドメインで行われる。従って、2つのパターンを比較できる192通りの（つまり8x8x3）の組み合わせがあるため、類似性の192の測定を実行できる。類似性基準自体が、破壊されている可能性があるテストCDPの領域を排除するために、例えば、値を捨て、より高い相関関係がある値だけを保つことによるなど複数の方法で計算できる。
7.テストCDPの「品質」つまりオリジナルCDPに対する「近似」を測定するために、テストCDP全ての類似性基準または他のイメージ特徴に基づいた基準を収集し、結合する。組み合わせ関数は、例えば、オリジナルCDPとテストCDPとのさらに優れた弁別手段である特徴にさらに重みつまり重要性を割り当てることによって類似性の程度を結合する関数である場合がある。

【００６６】

すでに前述したように、重複プロセスは常にオリジナルCDPを劣化させ、一般的には、近似または品質の異なる程度がアナログ形式から記録されるCDPの場合より低くなると予想される。しかしながら統計学的な変動のために、さまざまな程度の適切な選択及び結合は、テストCDPがオリジナルアナログ形式から記録されているのか、あるいはオリジナルではないアナログ形式から記録されているのかを判断する上でより効果的である場合がある。

【００６７】

図6は、（603に図示されている）周波数の30のバンドのために、オリジナルCDPと、認証されている文書からのテストCDPの周波数のエネルギー間の（605に示される）相関関係を示している。予想されるように、エネルギー間の相関関係は、コピープロセスでほとんど情報が失われない低周波バンドで最高であり、ただ1回の印刷動作だけで情報の大部分が失われてしまう高周波バンドで最低である。相関関係が、それらが平均してオリジナルア文書からのCDPのためとなるより、中間周波数バンドで実質的に低くなる場合、CDPはオリジナルではなく、したがって文書も認証されていない。これは、このようにして認証されている文書がオリジナルではないことを示す図6のプロットに当てはまる。

【００６８】

相関関係値がそれだけでは文書がオリジナルアナログ形式であるのか、あるいはオリジナルではないアナログ形式であるのかを判断するためには十分ではないとき、他の画像特徴も考慮できる。オリジナルCDPとテストCDPの間の相関関係値を生成するために使用できる追加の画像特徴は以下を含む。

-カラーヒストグラム、
-端縁、線、及び外形、
-（フーリエドメイン及びウェーブレットドメインなどの）他のドメインの周波数、
-輝きとコントラスト。

【００６９】

CDPがオリジナルからであるか、あるいはオリジナルではない文書からであるかを検出する

関数detect_patternは、analyze_patternによって返される結果を分析し、CDPがオリジナル文書からであるのか、あるいはオリジナルではない文書からであるのかを示す値Outputを返す。

output=detect_pattern (Results, Parameters))

Results：スカラー値またはベクトルであり、関数analyze_patternの出力である。
Parameters：応用例の要件及びそれが検出を実行する条件に依存することがある、検出関数の動作を調整するために必要とされる値。
Output：さまざまな出力値が考えられる。その最も簡略な形式では、Outputは3つの値、つまりORIGINAL、NON-ORIGINALまたはPROCESSING-ERRORを取ってよい。最後の出力は、パターンがひどく記録されるときに発生する可能性がある。Outputはさらに詳細な情報を返

してよく、例えばNON-ORIGINALは、オリジナルではない文書からのテストパターンがどのようにして生成されたのか（例えば、重複、写真複写、再生等）を示すことがある。Outputはさらに品質つまり近似の指数も提供できる。

【００７０】

ここに簡略な検出関数のアルゴリズムの一例がある。

1.スカラー値Sを取得するために、analyze_patternによって結合される多様なResults値を結合する。これを行う1つの方法は、返されるResultsを合計することによりSを生成することであろう。

2.S＞T1である場合、出力はORIGINALである。それ以外の場合、S＞T2であると、出力はNON_ORIGINALであり、それ以外の場合出力はPROCESSING ERRORである。

【００７１】

ここでは、T1とT2は、通常T1＞T2で、トレーニングプロセスを介して通常取得される2つのスカラーパラメータである。

【００７２】

文書からのCDPのオリジナルCDPとの局所的な再同期

文書から記録されるCDPをオリジナルCDPと比較するためには、記録されるCDPはオリジナルCDPと同期されなければならない。これを行う1つの方法は、オリジナルを同期するために、記録されているCDPの同期点、例えば黒の境界線601を使用することである。いったんCDPが同期されると、それらの間の比較はピクセル単位またはブロック単位で実行される。

【００７３】

文書に、あるいは文書からのCDPのデジタル記録にCDPを印刷する際にエラーがあったとき、CDPはこの方法によって完全に同期することはできない。例えば、オリジナルCDPと文書から記録されたCDPの間に1ピクセル未満のシフトがある可能性がある。さらに、シフトはパターンに沿って変化してよい。いくつかのケースでは、記録されたCDPの上部はオリジナルCDPに比較して下方にシフトされてよく、下部は上方にシフトされてよい（あるいは、逆もまた同様であるのは言うまでもない）。これらのシフトは気付くのが難しく、一貫して発生せず、記録パターンで局所的に変化する可能性がある。それらは、プリンタ内のわずかな不安定さによって引き起こされるが、記録装置内の同様の不安定さによっても生じることがある。

【００７４】

これらの予測不可能なサブピクセルのシフトが検出器の性能を下げることがある。これらの不良位置合わせのために、オリジナル文書からのいくつかのCDPが、オリジナルではない文書からであるとして検出されてよい。オリジナル文書からのこれらの「病的な」CDPを処理する、及び一般的には、CDP検出の安定性を改善する1つの方法は、局所的な不良位置合わせを補正するためにCDPを局所的に再同期することである。局所的な再同期を実行する複数の方法があるが、一般的な考えでは、局所的な再同期のために記録されたCDP自体を使用する。

【００７５】

局所的な再同期を実行する1つの方法は、オリジナルCDPをブロック（重複しないブロックが好ましいが、ブロックが重複することもある）に分割し、記録されたCDPのどのブロックがオリジナルCDPの指定ブロックに最も近似した一致をするかを見つけることである。不良位置合わせがない場合には、前記指定ブロックに最も厳密に一致した記録されたCDPのブロックが、指定ブロックがオリジナルCDPで有していた記録されたCPD内の同じ位置にあるであろう。例えば、オリジナルCDPの開始位置（80、80）及び終了位置（89、89）の10x10ブロックの最良の一致は、記録されたCDPの対応するブロック（80、80）から（89、89）となるであろう。しかしながら、不良位置合わせがある場合、最良の一致はブロック（81、80）から（90、89）となるであろう（1ピクセル右へのシフト）。それが当てはまる場合には、記録されたパターンは、位置（80、80）から（89、89）に1ピクセル左にシフトされたブロック（81、80）から（90、89）を有するであろう。同じデータが、「局

所的に再同期された」CDPを生成するために記録されたCDP内の各ブロックに適用できる。

【００７６】

局所的な再同期は、2～3のパラメータと関数を必要とする。第1に、我々はオリジナルCDPの各ブロックと記録されたCDPの同じ寸法のブロックの間の距離の基準を定めなければならない。この目的の便利な基準は標準相関係数である。オリジナルCDPが分割されるブロックの寸法を確かめることも必要である。通常、寸法8x8または16x16のブロックが使用できるが、一般的には、サイズNxMのブロックが使用できる。前述したように、ブロックは重複することがあり、そのケースでは連続ブロック間の重複量を定める必要がある。設定する別のパラメータは検索範囲または検索分野である。つまり、一致する位置から開始し、アルゴリズムはどのように一致するブロックを探すべきか。これは、パラメータnで設定され、オリジナルCDPの位置（x、y）で開始するブロックの場合、位置（x＋/-i,y＋/-i）、0＜i＜nの全てのブロックがテストされる。

【００７７】

局所的な再同期を行う前にデジタルCDPと記録されたCDPを拡大縮小することも可能である。これによりさらに細かいグレイン一致が可能になる。例えば、2つのCDPを2で拡大縮小することによって、半分のピクセルシフトを回復できる。そして最後に同期アルゴリズムは、追加の改善が見つけられなくなるまで再同期されたCDPで繰り返し適用することができる。

【００７８】

いったん再同期が実行されると、再同期された記録済みのCDPとオリジナルCDPの間の類似性/距離の任意の測定が実行できる。おそらくトレーニングセットに基づいたパラメータを用いて単純な相関関係、つまり局所周波数分析を実行できる。しかしながら、通常はCDP全体で一定の量の平均を生成するこれらの測定は、一定の応用例で発生することがある走査されたCDPに対する何らかの局所的な損傷に対して必ずしもロバストではない可能性がある。例えば、CDPの1つの領域がひどく印刷されたか、あるいはキズ、書き込みまたは水によって損傷を受けた可能性があるケースもある。他のケースでは、走査装置は走査されたCDPに歪みを差し込んだ可能性がある。その問題は、文書が正しく挿入されていないときに通常フィードスルー装置で発生する。CDPをこれらの種類の歪みに対してよりロバストにするために、類似性のさらにロバストな基準が使用されてよい。1つのこのような基準が中央値局所相関係数であり、相関係数はCDPのブロックごとに計算され、全ての局所相関係数の中央値が計算される。ここでは、平均の代わりに中央値を計算することにより、検出器は局所的な改変に対して著しくよりロバストになる。CDPのかなりの量の破壊された領域に対処するため、破壊されていないと仮定できる20％にすぎない最良局所相関係数の平均を計算することもできる。1つの実施では、この計算する手順は、この種の「片寄った」平均がそれぞれの周波数チャネルに別個に適用され、任意でさまざまなカラーチャネルに適用されるという点である。言うまでもなく、前記同期技法はCDPとだけではなく、オリジナル可視認証パターンと同期される必要のある任意の記録された可視認証パターンと共に適用できる。

【００７９】

CDPの応用例

CDPは、それがオリジナル文書をオリジナルではない文書から区別するために有効であるあらゆる状況で使用できる。CDPは、CDPのデジタル記録がCDPのオリジナルデジタル表現に匹敵するように十分な忠実度でCDPを印刷する任意のプロセスによって印刷されてよい。パターンは、特定の写真複写技法、走査技法、または印刷技法によって作成されるオリジナルではない文書を検出するように特に適応されてよい。

CDPの特定の使用は、以下を含む。

1.ブランド品保護のためのパッケージ上にCDPを印刷する。

2.コピー検出のために小切手及び紙幣にCDPを印刷する。

3.証明書、契約書及び文書がオリジナルであるのかあるいはコピーであるのかを検証するための同等物を含む重要書類の上にCDPを印刷する。

4.ホログラムの上にCDPを印刷する。
5.航空機/自動車部品または製薬などの貴重品のラベルにCDPを印刷する。
【００８０】
さらに一般的には、CDPは、文書にどのプロセスが適用されたのかを判断できることが望ましい応用例で使用されてよい。パターンは言うまでもなく、対象となるプロセスを最もよく検出するために必要に応じて変えられてよい。
【００８１】
CDPは、以下の応用例にも使用できる。
1.印刷品質のベンチマーキング
CDPを読み取るとき、CDPのデジタル記録の品質指数が計算される。この品質指数は、印刷品質、用紙/基板の品質、またはデジタル化/走査（装置））品質に関して変化するであろう。CDP品質指数は一定の印刷プロセス、一定の基板または一定のスキャナを定量化するために使用できる。
2.品質管理
同じ傾向で、CDP読取装置は自動品質管理のための印刷製作プロセスで使用できる。手動検査に優るCDPの優位点とは、それが自動化され、客観的且つ精密な品質の基準を示すという点である。
3.追跡
CDPは、プリンタ、用紙、カメラ、及び使用と摩耗に関連付けられた構造と特性を有している。原則的に、CDPを分析すると、文書の一般的な「履歴」、つまりそれがどのようにして印刷されたのか、それがどの程度の「消耗」を被っているのかを突き止めることができる。
【００８２】
文書中の改変箇所を検出するために可視認証パターンを使用する：図10
一定のクラスの文書は、印刷後常に「修正される」。これの1つの共通の例は、小切手が作成されるときに記入される空のフィールドと共に印刷される小切手である。これらのクラスの全てに属する文書にまつわる問題点は、記入済みのフィールドに掲載されている内容が後に改変される可能性があるという点である。したがって、小切手自体は本物であったとしても、空のフィールドに書き込まれた内容の意味的な価値が変更される可能性がある。例えば、小切手の受取人は、出納係が気付くが困難な方法で（例えば「百」から「九百」に）自分に宛てられた小切手の金額を修正できる。
【００８３】
偽造者は実際に偽造文書を作成するわけではないため、この種の問題は解決するのが困難である。代わりに、彼らは本物の文書の意味論的な価値を改変する。前記問題は、書き込まれた本物の文書がすでに法律上の修正を含んでいるという事実によりさらに困難になる。問題は、文書に対する法律上の修正が、後の法律的な修正とどのようにして区別されるべきかということである。
【００８４】
この問題に対する解決策の1つは、犯罪科学的な調査である。出納係が小切手が修正されているのではないかと疑う場合、彼はそれを追加の調査のために別の権威者に持ち込むことができる。しかしながら、この作業は手作業で、高価で時間がかかり、それをあらゆる文書または小切手に組織的に適用することが可能ではないことは明らかである。多くの場合、偽造者は、最初に書かれたものの一部を消去することにより小切手を偽造する。例えば、金額を「二百」から「九百」に修正するために、偽造者はおそらく「二」を消去し、それを「九」に修正するであろう。手書きのものを消去するために、偽造者の多くの場合化学製品を使用する。別の可能性は、小切手からオリジナルの金額を擦り取り、背景を塗り直し、次に新しい金額を書き込むことである。
【００８５】
可視検証パターンは、これらの不法な修正を検出するために使用できる。一般的な考えでは、不法な修正の検出を希望することがある文書の領域のそれぞれにVAPを印刷するこ

とである。法律上の修正は、次にVAPの上に書き込むことによりなされる。正確で、一意且つコピー不可能なVAP構造は後に修正を検出するため、及び修正が受け入れられるかどうかを判断するために使用できる。考え方は、VAP上に書き込むことと、VAP上に書き込まれた何かを消去することの両方によりVAPに検出可能な修正を生じさせるということである。VAP上に書き込むと、VAPの書き込みを擦り取る、あるいはVAPに化学的な消去剤を塗布するのと同様にパターンが破壊される。このようにして使用されるVAPは、以下で修正検出パターン、つまりMDPと呼ばれる。

【００８６】

MDPが、不法な修正を検出するためにどのように使用されてよいのかは、以下のように要約できる。

・許可されていない修正から保護する必要のある文書のそれぞれの領域にMDPを挿入する。

・文書の真正性を検証するとき、最初に文書の中にMDPのそれぞれの画像を記録する。

・記録されたMDPごとに、記録されたMDPをMDPのオリジナルのデジタル表現と比較し、MDPが損傷を受けた領域を検出する。

【００８７】

記録されたMDPの、MDPのオリジナルデジタル表現との比較の結果は多くの方法で使用できる。

・意思決定者に強調表示された損傷を受けた領域との比較の結果を表示する。これは、書き込みを含む領域と消去された領域の両方を示す。

・意思決定者に強調表示された書き込まれていない損傷を受けた領域との比較の結果を表示する。

・損傷を受けた領域のサイズを、書き込みがなされている領域のサイズと比較し、差異が閾値を上回る場合、フィールドを修正されたとして処理する。

【００８８】

図10は、MDPが修正を検出するためにどのように使用できるのかを示す。1001では、文書のための金額フィールドで使用されるMDP1002が示されている。前述したようにMDP1002は黒の境界線106で囲まれている。1003で示されているように、金額250はMDP1002の中に書き込まれている。1005では、偽造者が、2の「尾部」を消去し、ループを追加し、それを数9にすることにより金額＄250を金額＄950にどのようにして修正したのかが分かる。消去を隠蔽するために、偽造者はMDPのパターンを模倣した。模倣は1005でも目に見えるが、図示されていたにしても、急がされている出納係を通り抜けるほど十分によくできており、技能のある偽造者は容易に模倣をさらに改善することができる。

【００８９】

偽造者にとっての問題は、消去がMDPを破壊したという点である。MDPを走査し、それを局所的に分析することによって、高い精度で、MDPのどの部分がオリジナルから変化したのかを検出することができる。消去は、テキストもオリジナルパターンも含まない領域をMDPの中で見つけ出すことにより検出できる。これは1009に示されている。テキスト領域は、通常それらは色が均一であり、MDPよりさらに濃いために見つけ出すのが容易である。その場合消去された領域を見つけ出すために行う必要があるのは、テキストを含まない記録されたMDPの領域を、MDPのオリジナルデジタル表現と比較することである。消去された領域は、1011に示されるように、オリジナルデジタル表現に一致しない記録されたMDPの部分として現れる。好ましい態様においては、このような一致しない部分は赤で表示される。

【００９０】

文書の改変箇所を検出するためにMDPを使用するためのアルゴリズムに関して、もう少し詳説する。

・MDPを生成すること。MDPは、VAPが生成される任意の方法で生成されてよいが、そのときピクセル値はMDPをさらに明るくするために増加される（そうしない場合、MDP上に書き込まれるテキストはMDPから容易に区別できないであろう）。

・見当合わせマーク（例えば黒い境界線または角のマーク）を使用し、記録されたMDPを文書から抽出する。
・テキスト領域を検出する。低域フィルターが記録されたMDPに適用され、閾値の値のピクセルは、テキスト及び法律上の修正の一部であると見なされる。
・MDPの修正を検出する。局所的な再同期が適用されてから、相関関係計数がMDPのブロックごとに計算される。1009に図示されるように、テキストの領域と法律上の修正の領域が改変されたのを確認できる。
・画像1001から（1003で）法律上の修正を除外することにより、不法な修正を検出するためにいくつかのアルゴリズムを適用できる。1つの考えられる方法は、最初に、（局所的な相関関係を基準点とすることにより）領域を修正済みまたは未修正に分類し、次に個々のまたは重要ではない修正された領域を削除するノイズ処理アルゴリズムまたは低域フィルターを適用する。領域検出アルゴリズムは、重要な修正済みの領域を検出するためにも適用できる。結果は1009に表示されている。つまり、（テキストに対する）許可された修正が緑で表示される一方、許可されていない修正は赤で表示されている。
・許可されていない修正の量に応じて、任意でMDPが属する文書の真正性に関して決定を下すことができる。

【００９１】

VAPの実施詳細

文書中のVAPの形式

VAPを使用して、アナログ形式における改変を検出するために必要とされる全ては、アナログ形式には、役目を果たすパターンを有する領域、及びアナログ形式から記録されるようなパターンと比較できるパターンのオリジナルデジタル表現がある可能性があるという点である。したがって、技法のためにアナログ形式の既存のパターンを使用することが可能なケースもあるであろう。しかしながら、さらに通常は、VAPは新しいアナログ形式の意匠の一部として含まれるであろう。VAPをアナログ形式に隠す必要がないことは言うまでもなく、実際にいくつかのケースではその存在が、カスタマに対し、違法なアナログ形式を検出できることを安心させるために広告されることがある。他方、VAPは任意の形状を有することができるため、アナログ形式の他の特徴に容易に組み込むことができる。図11は、2つの例を示している。1101では、そのバーがVAPを構成しているバーコードが示されている。1103にはVAPを含むロゴがある。言うまでもなく、文書中に1つより多くのVAPがある可能性があり、1つより多くのVAPが場所を共用してよい。これは、パターンの全ての重みが総計して1になるように重みを付けた値を各パターンに与えることにより実行できる。例えば、

Final_pattern = a*pattern1+(1-a)*pattern2,　0<a<1の場合

複数のパターンの1つの応用例は、それぞれの関係者が契約書に署名をするときに、あるいはそれ以外の場合交渉の中の段階を終了するときに、独自のパターンを追加する契約書の認証であろう。

【００９２】

1つの文書で複数の場所に、通常は、複数の関係者が他の関係者のCDPを検証できることなく（その結果、それらを複製できずに）自らのCDPを検証できるようにするためにさまざまなキーを用いて生成されるいくつかのCDPを挿入することも可能である。さまざまな関係者がCDPを検証できるようにするために、さまざまなキー（それぞれのキーが、CDPの空間領域または周波数領域を制御できる）を使用してCDPを生成することも可能である。このようにして、ある関係者が自分のキーをリリースする場合、このキーはCDPの正確な重複を生成するには十分ではなく（全てのキーが必要である）、セキュリティが危険にさらされることはない。これは「共用される秘密」という概念に類似している。

【００９３】

VAPの見当合わせ

好ましい態様は、VAPの見当合わせとして黒いボックス106を利用する。しかしながら、他の多くの見当合わせ技法が可能である。例えば、OCRだけではなく、フレーム、バーコ

ードまたはVAPの位置を突き止めるためにすでにパッケージ上に表示されている類似物などの可視パターンを使用できるであろう。UVマークまたは2002年11月4日に出願された親特許出願の米国特許出願第10/287,206号、J.Zhaoら、Apparatus and methods for improving detection of watermarks in content that has undergone a lossy transformationに説明されるあらゆる技法も使用できる。また、記録されたVAPのフーリエ-メリン変換を生成し、それをVAPのオリジナルデジタル表現と一致させることもできるであろう。

【００９４】

いくつかの応用例の場合、VAPのデジタル記録の向きが正しいかどうか、あるいはそれが読み取る前に逆さま（180度の回転）に反転される必要があるかどうかを知ることは困難である。一度にVAPを分析しなければならなくてもよいようにするために、そして分析がうまく行かない場合にはそれを反対の垂直向きで回転し、それを再び分析するために、対称的なVAPを設計することが可能である。つまり、下部は上部を映し出す鏡である。その結果、VAPは、その垂直向きに無関係に分析できる。

【００９５】

VAPのパターンの特性

パターンはグレイスケールパターンであるか、あるいはそれは着色されたパターンである場合がある。後者のケースでは、RGBとYUVなどのさまざまなカラーチャネルを利用できる。パターンは、例えば空間領域、ウェーブレットドメイン、DFTドメインまたはDCTドメインなどの多様な周波数領域でも生成できる。

【００９６】

VAPの生成

VAPのノイジネス、つまりランダムな性質は、偽造者及び捏造者がそれに対処するのを困難にするものである。ランダムまたは擬似ランダムなパターンを生成できる任意の技法はVAPを生成するために役に立つ。好ましい態様においては、生成は、値にとって一意である乱数のシーケンスを生成する擬似乱数生成プログラムに値を与えることで行われる。したがって、値は、パターンの新しいコピーを作成するために使用されてよいキーとしての役割を果たす。さまざまな態様においてさまざまな擬似乱数生成プログラムが使用されてよく、生成される乱数の確率論的な頻度の値はさまざまな確率分布から取ることができる。分析が実行されるVAPの場所を決定するためには、キーも使用できる。以下の他の情報を伝搬するためにVAPを使用することの説明で説明されるように、キーはこのような他の情報を含むことがある。パターンを設計するために使用されるキーが他の関係者に明らかにされない応用例もある。そのケースでは、例えば、非対称鍵または公開鍵-私有鍵の組などのキーを分配する有効な方法が使用されてよい。

【００９７】

パターンは、ロゴをパターンに追加する、あるいは反対にするかのどちらかによりロゴと組み合わされてよい。ロゴは、他の役割を果たす（2Dバーコード、透かしが入れられた画像等）画像を含む既存の画像または文書である場合がある。ロゴがVAPのオリジナルデジタル表現と記録されたVAPを比較することに最小限に干渉するように、フィルタリングなどのプロセスをパターンまたはロゴに適用することも可能である。

【００９８】

VAPの印刷

VAPにより提供される認証の品質は、VAPが文書上で印刷される忠実度に完全に依存している。認証エラーは、VAPの忠実度を保証するために印刷プロセスの最後に「品質管理」工程が加えられれば削減することができる。

1.それぞれの印刷されたVAPが、認証パターンが、それがオリジナルとして認識されるために必要とされる最小の品質を有しているかどうかを確認するために自動認証プロセスに渡される。

2.品質が最小品質を下回る場合には、警報が出され、認証パターンを含む文書/パッケージが印刷され直す。

3.このような検証は、印刷品質またはプリンタにより導入されるエラーについて「品質管

理」の役割も果たすことができる。

【００９９】

VAPの生成は、印刷技術に適応できる。例えば、レーザプリンタ印刷専用の2進ドットが使用される場合には、プリンタの可能性をよりよく使用するために2進ドットVAPが生成できる。また、VAPは、プリンタの色空間でさらに適切に生成され、印刷される可能性がある。一定のプリンタが特定のインク（例えばCMYK）を使用する場合、それはRGBドメインにおいてよりそのドメインでVAPを生成する方がより効果的である。VAPが2進ドットだけを生成できるレーザエングレーバを用いて金属に彫り込まれる場合、2進VAPを生成する方がより意味をなすであろう。

【０１００】

他の情報を伝搬するためにVAPを使用する

他の情報を伝搬するためにVAPを使用する3つの手法が以下に説明されている。つまり、情報を保持するためにVAPの一定の領域を確保することと、オリジナルVAPを生成するために使用されるキーを生成するために他の情報を使用することと、VAPに透かしを加えることである。透かしを加えることの不利な点とは、それによりオリジナルではないアナログ形式またはVAPの修正を検出するVAPの能力が削減される点である。

【０１０１】

情報を保持するためにVAPに領域を確保する

VAPの一定の領域（例えば8x8ブロック）は情報を保持するために確保できる。それらの領域では、VAPの構造/特性はその真正性を検証するために実際に使用されることはないが、数ビットの情報を記憶するために使用される。キーを有していないエンティティが、VAP内の領域が情報を記憶するため、あるいはVAPの真正性を突き止めるために実際に使用されるかどうかを判断することができないように、これらの領域はキーを使用して擬似ランダムに選択することができる。情報を保持するために使用される領域では、VAPの一定の構造/特性は、情報の一定のビップ値（「0」か「1」）に一致できる。このビットに依存した構造/特性は、言うまでもなくキーによって決定されるように変化することができる。確保された領域及びそれらが含む情報は、生成されるとおりにVAPの一部であることに注意する。したがって、それらは本物ではない文書を検出するためにVAPの能力を劣化させない。確保された領域の1つの用途とはVAPを生成するために使用されるキーを記憶することである。

【０１０２】

VAPのキーを生成するために情報を使用する

この説明は以下の用語を使用する。VAPはキーPを用いて生成、検出される。確保された領域に関して前述されたか、あるいは透かしに関して後述されるようにパターンの中にメッセージを埋め込むために別のキーSを使用することを希望する場合がある。メッセージMはキーSを使用してVAPに埋め込まれる。最後に、追加の情報Iが文書に可視に印刷される（シリアルナンバー、バーコード等）、あるいはパターンの中でまたはその外側で目に見えないようにUV符号化される、あるいは外部ソースから取得される可能性がある。

【０１０３】

固定パターンキー

1つの態様では、VAP生成キーは固定Pである。これは、通常、印刷技術がパッケージ/製品/文書ごとに動的にパターンを変更する能力を持たない、標準的なオフセット印刷技術に当てはまる。キーは前述されたように秘密に保つことができるか、あるいは他のセキュリティ機能に組み込まれてよい。例えば、それは文書上にUVインクで印刷できるであろう。固定パターンキーは、一般的にブランド品保護または文書保護のために使用できる。

【０１０４】

可変パターンキー。別の態様では、VAPのキーは秘密鍵Sおよび何らかの他の情報Iに依存している。この他の情報Iは（パターンの中またはその外側で）文書に表示されてよい、あるいは外部ソースから取得されてよい。文書からの情報は、例えばシリアルナンバー、テキスト、バーコード等である場合がある。外部ソースからの情報は、例えばVAPに関

連付けられ、VAPを含む文書が真正であるかどうかをチェックする人に知らされる値であってよい。パターンキーは、秘密鍵及び情報Iであるパラメータの任意の関数P＝ｆ（S,I）であってよい。単純な関数は2つのパラメータを連結する、つまり合計するためであるだろうが、2つのパラメータ等の組み合わせのハッシュ値などの他の多くの関数が考えられる。検出時に、印刷情報Iが適切な技術－バーコードリーダ、OCR等を用いて抽出される。次にパターンキーがP＝ｆ（S,I）として生成され、パターンが分析される。通常の用途は、デジタル印刷を用いるブランド保護を含む。

【０１０５】

VAP内の透かし

透かし技術を使用してVAPに可視、または非可視の透かしを埋め込むことが可能である。透かしは複数の役割を果たす。それは、前述されたように単一ビットだけを含む任意の情報を含むか、あるいはパターンの見当合わせを補助してよい。透かしは、VAPを生成するために使用されるキーを用いて、あるいはその読み取りが別のユーザまたはユーザのグループに制限されるように別のキーを用いて検出できる。後述される第3の可能性は、VAPを生成するために使用されるキーを引き出すために透かしにより搬送されるメッセージを使用することである。

【０１０６】

電子透かしがVAPの中に埋め込まれると、VAPはわずかに修正される。その結果として、同じVAPが真正性検証のために使用されると、その目的でのVAPの信頼性は下がる可能性がある。代替策として、電子透かしを、前述したような情報を記憶するために確保されるVAP内の領域に埋め込むことができる。

【０１０７】

透かし及びキー

別の態様においては、パターン生成キーPは秘密鍵S、及びコピー検出パターン内の電子透かしとして埋め込まれるメッセージMから引き出される。このケースではMは前述した可変パターンキーを生成するために使用される情報Iの代わりをする。あるとき、パターンキーPは秘密鍵Sとメッセージ M,g（M,S）の任意の関数となることがある。パターンは通常に生成され、次に透かしがパターンの中に差し込まれ、透かしはパラメータとして秘密鍵Sを使用してメッセージMを符号化する。検出時、最初に透かしメッセージMは秘密鍵Sを用いてパターンから読み出されなければならない。いったんMが既知になると、パターンキーP＝g（M,S）が引き出され、パターンが分析される。

【０１０８】

この応用例の枠組みでは、パッケージ上に印刷されているさらに多くの情報を抽出するためには補助的な技術は必要とされないであろう。しかしながら、本明細書に説明する原則の範囲内のいくつかの方法でパッケージに印刷される情報Iを使用することも可能である。例えば、秘密鍵Sは、パターンにメッセージを埋め込むために使用される透かしキーW つまりh（S,I）＝Wを生成するために情報Iと組み合わせて使用できる。次にパターンキーは前述されたのと同様に生成される、つまりP＝ｆ（M,W）＝ｆ（M,h（S,I））である。一般的には、VAPは、さまざまなレベルの検証を作成するために、透かし技術と他の読み取り技術（例えば、OCRまたはバーコードリーダ）と組み合わされてよい。

【０１０９】

VAPを比較する

記録されたVAPがVAPのオリジナルデジタル表現とどのように比較されるのかは、VAPがどのように生成されるのか、及びその目的は何かに依存する。いくつかの一般的に適用可能な変動は、文書にどのプロセスが適用されたのかに関してさらに多くのヒントを有するため、あるいはセキュリティ機能のために、一定の領域を独立して評価することを含む。前述したように、VAPは1つより多くの認証パターンを含み、さまざまなパターンはさまざまなグループによって分析されてよい。

【０１１０】

VAPが有意義に比較される前に、比較プログラムは、CDPについて前述したようにオリジ

ナル文書から記録されるVAPを用いて「訓練され」なければならない場合がある。トレーニングは、真正性が調べられている文書から記録されるVAPが本物であるかどうかを判断するための閾値を確立する。閾値の意味は、言うまでもなく、VAPが検出するために使用されている改変の種類に依存するであろう。オリジナル文書が印刷される方法が、VAP比較にどのように影響を及ぼすのかにおいて変化するたびに、再トレーニングが必要とされる。トレーニングは1枚の用紙の上で多くのVAPを印刷し、用紙を走査し、トレーニングソフトウェアに走査を提供することにより自動的に実行できる。

【０１１１】

別の態様では、その品質指数を測定するために、テストVAPのデジタル記録を対応するデジタル表現に比較する代わりに、別のVAP（通常は走査されたオリジナルVAP）のデジタル記録にデジタル記録を比較することができる。

【０１１２】

VAP分析が実行される環境

VAP分析を行うために必要とされるのは、記録されたVAPを生成するために文書からのVAPを記録できる装置、VAPのオリジナルデジタル表現のコピー、及び記録されたVAPをVAPのオリジナルデジタル表現と比較できるプロセッサである。レコーダ及びプロセッサは互いに対して局所的であるか、あるいはネットワークにより接続されてよい。ネットワークはローカルエリアネットワーク（LAN）または広域ネットワーク（WAN）のどちらかであってよい。局所的な環境の一例は、スキャナを有するPC内のプロセッサ、分析コードのコピー及びVAPのオリジナルデジタル表現のコピーである。VAPのオリジナルデジタル表現のコピーはキーを使用してダウンロードされるか、あるいは局所的に作成されてよい。分析結果はPCのディスプレイ装置に出力される。

【０１１３】

ネットワーク環境では、走査、分析及びVAPのオリジナルデジタル表現が任意の様式でネットワーク全体に分散されてよい。VAPのオリジナルデジタル表現のセキュリティを維持し、ローカルレベルで必要とされる装置を簡略化する分散は、走査がWANに接続される装置で実行される分散である。文書上のVAPが記録されたVAPを生成するために走査されると、記録されたVAPは、分析コードとVAPのオリジナルデジタル表現の両方ともが使用可能であるWANの中の場所に送信される。オリジナルデジタル表現は、要求に応じて記憶または再生されるかのどちらかでよい。分析はその場所で実行され、分析の結果だけがWANを介して走査のために使用された装置に返される。ネットワーク環境では、通常、記録されたVAPの中で搬送される、あるいは記録されたVAPと共に送信される情報は分析の中で使用するための情報を検索するために使用されてよい。例えば、文書はシリアルナンバーを含んでよく、シリアルナンバーは分析を行う場所に記録されたVAPと共に送信されてよい。VAPとシリアルナンバーの関連がある場合、シリアルナンバーは、記録されたVAPと比較する必要があるVAPのオリジナルデジタル表現のためのキー、またはVAP自体のオリジナルデジタル表現のコピーのどちらかを検索するためにネットワーク内の場所にあるデータベースにまたは他のどこかに適用できるであろう。前述したように、シリアルナンバーは、VAP内の可視透かしとして、VAPを含んだバーコード内で指定できる、文書からOCRできる、あるいは走査を行う人物によって入力することもできるであろう。

【０１１４】

VAPの画像を捕捉するためには、カメラ（ウェブカメラ、カムコーダ等）も使用できる。このケースでは、VAPデコーダは入力として1つの画像だけではなく、画像の不変のストリームも受け取る。複数の画像により提供される追加情報は、おそらく分析では非常に有効である場合がある。しかしながら、1つの画像を分析するために必要とされる時間は2つの連続画像の間の時間よりはるかに大きい場合があるので、画像のストリームの使用は最適化できる。例えば、正しい読み取りのための特性（優れた鮮明さ、ピクチャに完全に含まれているVAP）を有すると思われる画像がストリームから選択され、分析のために使用できる。

【０１１５】

他のセキュリティ技術とのVAPの組み合わせ

VAPは、アナログ形式をさらに安全にすることを目的とした他の技術と組み合わせることができる。例えば、VAPは電子透かしなどの情報非表示技法と、1-Dまたは2-Dバーコードなどの機械読み取り可能情報と、ホログラムと、またはアナログ形式に適用可能である任意の他の技術と共に使用できる。技術の間の関係性は多種多様である。一例として、2-Dバーコードは独立した情報、またはパターン分析に必要とされる秘密鍵を含むことができる、あるいは逆にVAPは2-Dバーコードを復号するために必要とされるキーを保持することができる、あるいは2-DバーコードがVAPを含むことができる。

【０１１６】

結論

前記発明の詳細な説明は、関連技術の当業者に対し、オブジェクトのアナログ形式がオリジナルアナログ形式なのか、あるいはオリジナルではないアナログ形式であるのかを判断するための発明者の技法、アナログ形式で真正性チェックを実行するためにVAPを使用するための発明者の技法、及びアナログ形式のメッセージを非表示にするためにVAPを使用するための発明者の技法を開示しており、さらに関連技術の当業者に対し、技法を実践するために発明者に現在既知である最前の形態を開示した。本明細書に開示されているもの以外の出願人の技法の多くの態様が可能であることは、当業者にとってはすぐに明らかになるであろう。例えば、VAPのサイズ、形状及びパターンは、VAPがともに使用されるアナログ形式の性質によって、及びVAPの目的によって決定される。VAPが追加情報をどのように伝搬するのか、及びその情報が何であるのかも、アナログ形式の性質、及びVAPの目的によって決定されるであろう。一般的には、VAPは、オリジナルアナログ形式が作成された後に行われる変更が検出されなければならない任意の状況で使用されてよい。本願は文書に印刷されたVAPを開示する一方、これらの印刷されたVAPの類似物は他の媒体のアナログ形式に置かれてよい。

【０１１７】

前記理由の全てから、発明の詳細な説明は全ての点において例示的であり、制限的ではないと見なされるべきであり、本明細書に開示されている発明の広さは発明の詳細な説明からではなく、むしろ特許法により許可される完全な広さをもって解釈される特許請求の範囲から決定されなければならない。

【図面の簡単な説明】

【０１１８】

【図１】可視認証パターン（VAP）がどのようにして生成され、文書に挿入されるのかの概要である。

【図２】VAPがどのようにして文書から記録されるのかを示す。

【図３】VAPがどのようにして認証で使用できるのかを概略で示すフローチャートである。

【図４】オリジナルアナログ形式とオリジナルではないアナログ形式の印刷及び認証の概要である。

【図５】透かし検出及び改変箇所検出のためのGUIを示す。

【図６】VAP、及びオリジナルではない文書から記録されたVAPのオリジナルデジタル表現における周波数のバンドのエネルギー間の相関関係を示すグラフである。

【図７】VAP及びオリジナルの文書から記録されるVAPのオリジナルデジタル表現における周波数のバンドのエネルギー間の相関関係を示すグラフである。

【図８】コンテントのない（contentless）透かしを画像の中に埋め込むためにどのようにしてメッセージベースのキーが使用できるのかを示す。

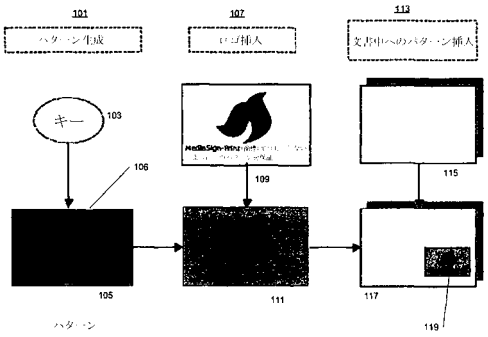
【図９】メッセージベースのキーを使用して透かしされたデジタル表現から特定のデジタル表現が引き出されるかどうかを判断するための技法を示す。

【図１０】文書の改変箇所を検出するためにVAPがどのようにして使用されてよいのかを示す。

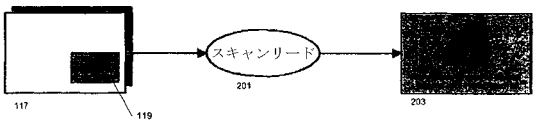
【図１１】VAPがどのようにしてバーコードまたはロゴの中に組み込まれてよいのかを示

す。

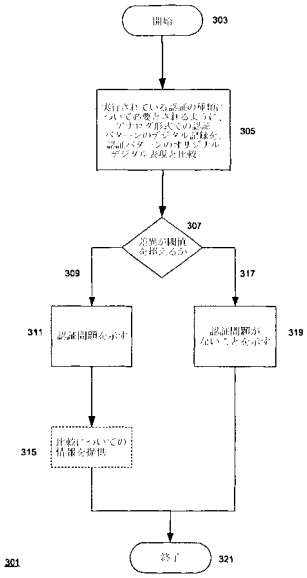
【図１】


101
パターン生成
107
ロゴ挿入
113
文書中へのパターン挿入
キー
103
106
109
115
105
111
117
119
パターン

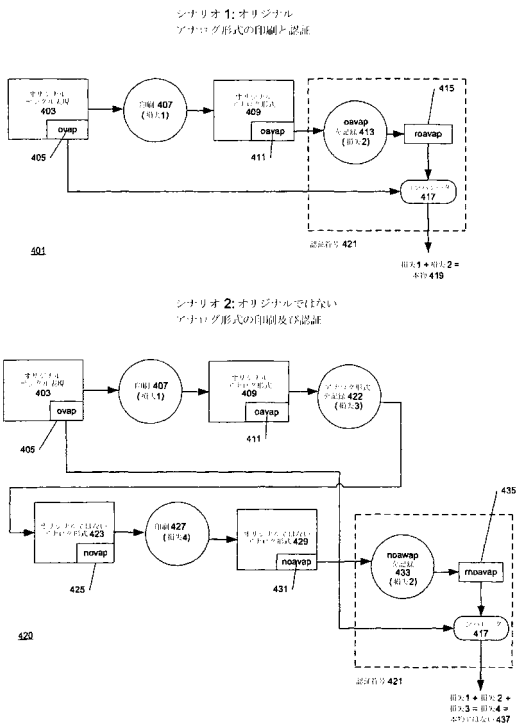
【図２】


スキャンリード
117
119
201
203

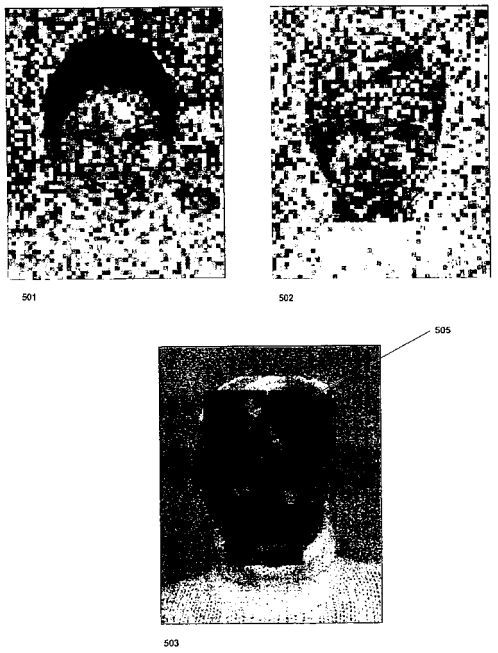
【図３】


開始
303
305
307
309
317
311
319
315
終了
321
301

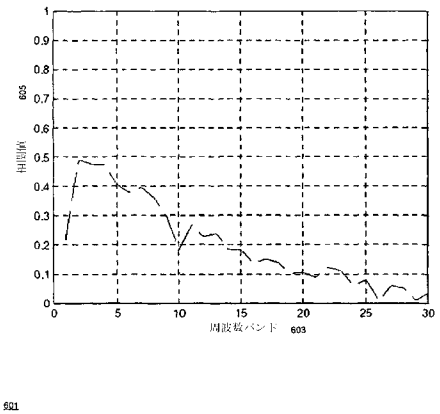
【図４】


シナリオ 1: オリジナル
アナログ形式の印刷と認証
403
ovap
405
印刷 407
(相関 1)
409
oavap
411
oavap
相関 413
(相関 2)
415
roavap
417
認証番号 421
相関 1 + 相関 2 =
本物 419
401
シナリオ 2: オリジナルではない
アナログ形式の印刷及び認証
403
ovap
405
印刷 407
(相関 1)
409
oavap
411
アナログ形式
相関 422
(相関 3)
アナログ形式
423
novap
425
印刷 427
(相関 4)
429
noavap
431
435
noavap
相関
433
(相関 2)
roavap
417
認証番号 421
相関 1 + 相関 2 +
相関 3 = 相関 4 =
本物ではない 437
420

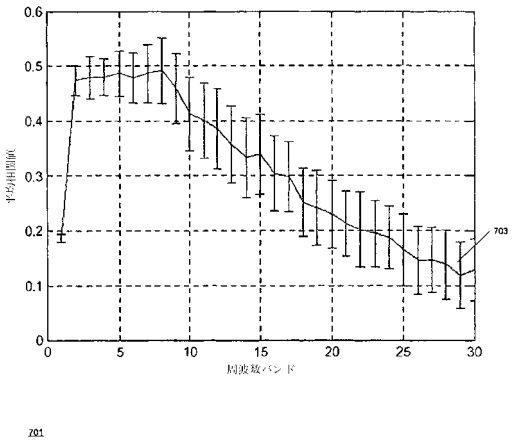
【図５】


501
502
505
503

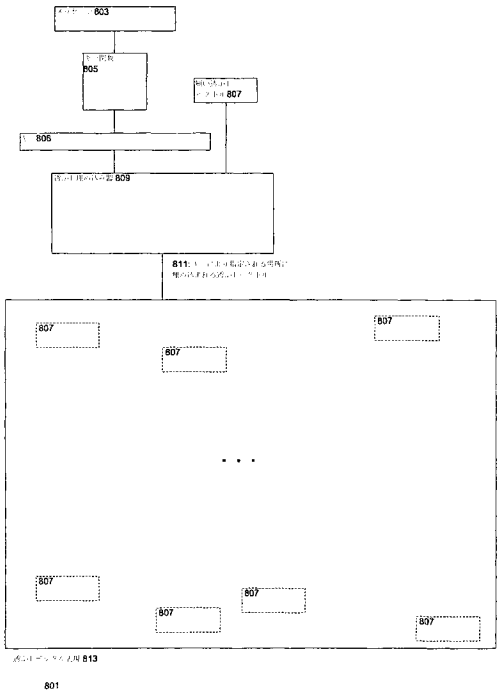
【図６】


605
相関値
周波数バンド
603
601

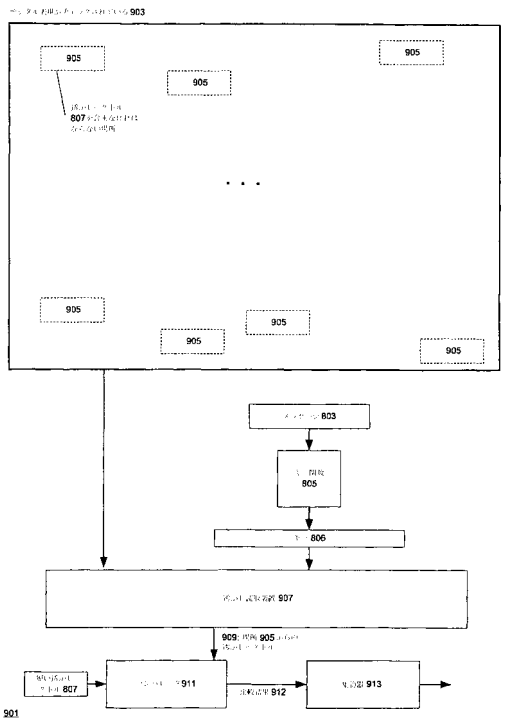
【図７】


平均相関値
周波数バンド
703
701

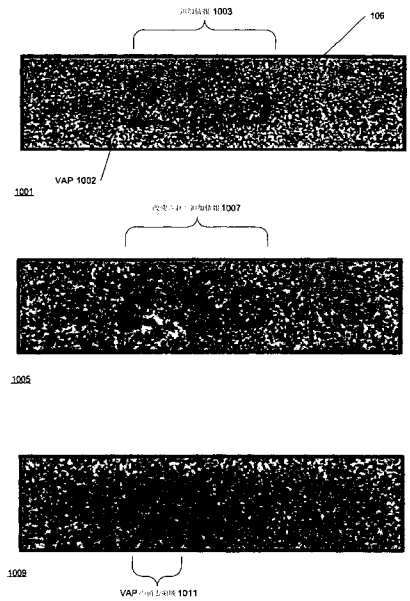
【図８】


803
805
807
806
809
811
807
807
807
807
807
807
807
813
801

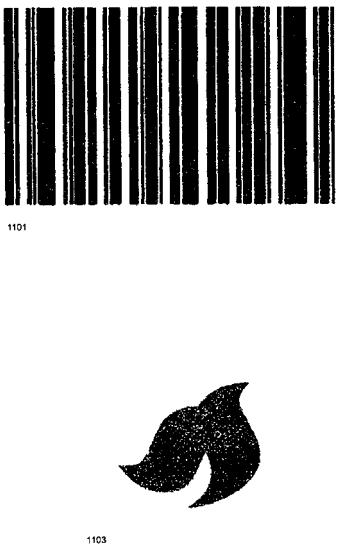
【図９】


903
905
905
905
905
905
905
905
803
805
806
907
909
911
912
913
807
901

【図１０】


1003
106
VAP 1002
1001
1007
1005
1009
1011

【図１１】


1101
1103

フロントページの続き

(74)代理人 100148699
弁理士 佐藤 利光
(74)代理人 100128048
弁理士 新見 浩一
(74)代理人 100129506
弁理士 小林 智彦
(74)代理人 100130845
弁理士 渡邉 伸一
(74)代理人 100114340
弁理士 大関 雅人
(74)代理人 100114889
弁理士 五十嵐 義弘
(74)代理人 100121072
弁理士 川本 和弥
(72)発明者 チャオ チアン
アメリカ合衆国 ロードアイランド州 ランフォード ニュー ロード １３０
(72)発明者 ピカード ジャスティン
アメリカ合衆国 ロードアイランド州 プロビデンス メイフラワー ストリート １６
(72)発明者 トーウィルス ニールス
アメリカ合衆国 ロードアイランド州 プロビデンス ＃２ ホープ ストリート ５４９

合議体
審判長 吉村 博之
審判官 古川 哲也
審判官 加藤 恵一

(56)参考文献 国際公開第０２／３１７５２（WO，Ａ１）
国際公開第００／５８９２８（WO，Ａ１）
国際公開第０１／１５３８２（WO，Ａ１）