

(19) 日本国特許庁 (JP)

(12) 特 許 公 報 (B2)

(11) 特許番号

特許第4137084号
(P4137084)

(45) 発行日 平成20年8月20日 (2008. 8. 20)

(24) 登録日 平成20年6月13日 (2008. 6. 13)

(51) Int. Cl.	F I
H04N 1/387 (2006.01)	H04N 1/387
G06T 1/00 (2006.01)	G06T 1/00 500B
G06F 3/12 (2006.01)	G06F 3/12 K
G06F 21/24 (2006.01)	G06F 12/14 560C

請求項の数 19 外国語出願 (全 46 頁)

(21) 出願番号	特願2005-123918 (P2005-123918)	(73) 特許権者	000001007
(22) 出願日	平成17年4月21日 (2005. 4. 21)		キヤノン株式会社
(65) 公開番号	特開2006-14280 (P2006-14280A)		東京都大田区下丸子3丁目30番2号
(43) 公開日	平成18年1月12日 (2006. 1. 12)	(74) 代理人	100076428
審査請求日	平成17年4月21日 (2005. 4. 21)		弁理士 大塚 康德
(31) 優先権主張番号	2004902153	(74) 代理人	100112508
(32) 優先日	平成16年4月21日 (2004. 4. 21)		弁理士 高柳 司郎
(33) 優先権主張国	オーストラリア (AU)	(74) 代理人	100115071
			弁理士 大塚 康弘
		(74) 代理人	100116894
			弁理士 木村 秀二

最終頁に続く

(54) 【発明の名称】 不正顕示機能付文書処理するための方法、及び、不正顕示機能付文書の妥当性検証を行うための方法

(57) 【特許請求の範囲】

【請求項1】

不正顕示機能付文書処理するためのコンピュータシステムの各手段による方法であって、

(a) 分解手段により、記録されるべきN値レベル画像に関して、前記画像の少なくとも1つの画素をN個の可能な値を有する主成分に分解する工程と、

(b) 選択手段により、少なくとも1つの所定のパターンのうちの、前記主成分の値に対応する所定のパターンからパターン要素を選択する工程であって、該所定のパターンはそのパターン要素がそれぞれ位置に対応づけられたシーケンスであり、前記画像内の前記少なくとも1つの画素の位置に対応する該パターン要素を選択する工程と、

(c) 形成手段により、前記少なくとも1つの画素に対して選択された前記パターン要素を転送媒体上に記録して不正顕示機能付文書を形成する工程と、

(d) 抽出手段により、前記少なくとも1つの画素に対して検索パターン要素を不正顕示機能付文書から抽出する工程と、

(e) 判定手段により、(d i) 前記検索パターン要素から抽出された主成分と、(d i i) 前記不正顕示機能付文書上の前記少なくとも1つの画素の位置と、に対応するパターン要素を判定する工程と、

(f) 比較手段により、前記検索パターン要素と判定された前記パターン要素とを比較する工程と

を有することを特徴とする方法。

10

20

【請求項 2】

前記形成する工程においては、前記パターン要素を前記転送媒体上に印刷することにより、該パターン要素を該転送媒体上に記録し、

前記抽出する工程においては、前記不正顕示機能付文書を走査して、該不正顕示機能付文書上に印刷された前記検索パターン要素を抽出する

ことを特徴とする請求項 1 に記載の方法。

【請求項 3】

宣言手段により、前記検索パターン要素が判定された前記パターン要素と一致しない場合、前記記録文書の前記画素の前記主成分が改竄されたと宣言する工程をさらに有することを特徴とする請求項 1 に記載の方法。

【請求項 4】

前記少なくとも 1 つの所定のパターンは、前記 N 個の可能な値にそれぞれ対応する N 個の暗号フィールドであることを特徴とする請求項 1 に記載の方法。

【請求項 5】

(g) 前記分解する工程 (a) が、

(g a) 前記 N 個の暗号フィールドのそれぞれについて、パターン要素を生成する工程と、

(g b) 前記 N 個の暗号フィールドの各パターン要素を、各暗号フィールドについて、それぞれ前記 N 値レベル画像の各画素位置に対応づけて、前記暗号フィールドを位置決めする工程と、

(g c) 前記主成分値に対応する前記暗号フィールドを選択する工程と、

(g d) 前記選択された暗号フィールドから、前記画像内の前記少なくとも 1 つの画素の前記位置に対応する前記パターン要素を選択する工程とを有し、

(i) 前記記録する工程の後であって前記判定する工程の前に、前記方法が、

(i a) 前記 N 個の暗号フィールドを生成する工程と、

(i b) 記録された前記画素の前記位置が設定可能となるように、前記記録されるべき N 値レベル画像を使用して、前記暗号フィールドを位置決めする工程とをさらに有することを特徴とする請求項 4 に記載の方法。

【請求項 6】

前記位置決めする工程 (i b) においては、前記暗号フィールドを前記記録される N 値レベル画像とブロック相関付けすることによって、前記暗号フィールドを位置決めすることを特徴とする請求項 5 に記載の方法。

【請求項 7】

前記記録する工程は、位置決めマークを前記転送媒体上に記録することを更に有し、前記位置決めマークは、少なくとも 2 つの登録マークを有することを特徴とする請求項 5 に記載の方法。

【請求項 8】

前記位置決めマークは、少なくとも 1 つの線形波形関数を有することを特徴とする請求項 5 に記載の方法。

【請求項 9】

不正顕示機能付文書処理するための コンピュータシステムの各手段による方法であって、

(a) 分解手段により、記録されるべき N 値レベル画像に関して、前記画像の少なくとも 1 つの画素を、N 個の可能な値を有する主成分と、並びに (a i) 前記主成分及び (a i i) 前記画像内の前記少なくとも 1 つの画素の位置に依存する、対応するランダム化副成分と、に分解する工程と、

(b) 形成手段により、前記少なくとも 1 つの画素に対する前記主成分及び前記ランダム化副成分を転送媒体上に記録して不正顕示機能付文書を形成する工程と、

(c) 抽出手段により、前記少なくとも 1 つの画素に対する前記主成分を不正顕示機能付文書から抽出する工程と、

10

20

30

40

50

(d) 判定手段により、(d i) 前記抽出主成分と、(d i i) 前記不正顕示機能付文書上の前記少なくとも1つの画素の位置とに依存する、前記対応するランダム化副成分を判定する工程と、

(e) 測定手段により、前記少なくとも1つの画素について印刷された前記ランダム化副成分を前記不正顕示機能付文書から測定する工程と、

(f) 宣言手段により、測定された前記印刷ランダム化副成分が判定された前記ランダム化副成分と一致しない場合、前記不正顕示機能付文書の前記画素が改竄されたと宣言する工程と

を有することを特徴とする方法。

【請求項10】

不正顕示機能付文書の妥当性検証を行うためのコンピュータシステムの各手段による方法であって、

(a) 抽出手段により、検索パターン要素を、不正顕示機能付文書内の位置から抽出する工程と、

(b) 選択手段により、少なくとも1つの所定のパターンのうちの、前記検索パターン要素の特性に対応する所定のパターンからパターン要素を選択する工程であって、該所定のパターンはそのパターン要素がそれぞれ位置に対応づけられたシーケンスであり、前記位置に対応する該パターン要素を選択する工程と、

(c) 比較手段により、前記検索パターン要素と選択された前記パターン要素とを比較する工程と

を有することを特徴とする方法。

【請求項11】

確定手段により、前記検索パターン要素が、選択された前記パターン要素と一致しない場合、前記不正顕示機能付文書内の前記位置における特性が改竄されたと確定する工程をさらに有することを特徴とする請求項10に記載の方法。

【請求項12】

前記特性が、前記不正顕示機能付文書の人間の読み手には可視であることを特徴とする請求項10に記載の方法。

【請求項13】

前記少なくとも1つの所定のパターンは、前記不正顕示機能付文書に記録された画像の画素値が取り得る値にそれぞれ対応するN個の暗号フィールドであることを特徴とする請求項10に記載の方法。

【請求項14】

前記選択される前に、

(e) 生成手段により、前記N個の暗号フィールドのそれぞれについて、パターン要素を生成する工程と、

(f) 位置決め手段により、前記検索パターン要素の前記位置と暗号フィールド位置との関連付けが可能となるように、前記N個の暗号フィールドの各パターン要素を、各暗号フィールドについて、それぞれ前記記録された画像の各画素位置に対応づけて、前記暗号フィールドを位置決めする工程と

をさらに有することを特徴とする請求項13に記載の方法。

【請求項15】

位置決めマークが前記文書上に記録され、前記位置決めマークは、少なくとも2つの登録マークを有することを特徴とする請求項14に記載の方法。

【請求項16】

前記位置決めマークは、少なくとも1つの線形波形関数を有することを特徴とする請求項14に記載の方法。

【請求項17】

前記位置決めする工程(f)においては、前記暗号フィールドを前記記録された画像とブロック相関付けすることによって、前記暗号フィールドを位置決めすることを特徴とす

10

20

30

40

50

る請求項 14 に記載の方法。

【請求項 18】

不正顕示機能付文書の妥当性検証を行うためのコンピュータシステムの各手段による方法であって、

(a) 抽出手段により、不正顕示機能付文書に含まれる少なくとも 1 つの記録画素に対して、N 個の可能な値を有する主成分を前記不正顕示機能付文書から抽出する工程と、

(b) 判定手段により、少なくとも 1 つの所定のパターンのうちの、前記抽出主成分に対応する所定のパターンからパターン要素を選択し、該パターン要素に対応して予め定められたランダム化副成分を判定する工程であって、該所定のパターンはそのパターン要素がそれぞれ位置に対応づけられたシーケンスであり、前記少なくとも 1 つの記録画素の位置に対応する該パターン要素に対応して予め定められた対応するランダム化副成分を判定する工程と、

(c) 測定手段により、前記少なくとも 1 つの画素に対応して前記不正顕示機能付文書上に記録されているランダム化副成分を、前記不正顕示機能付文書から測定する工程と、

(d) 比較手段により、測定された前記ランダム化副成分と判定された前記ランダム化副成分とを比較する工程と

を有することを特徴とする方法。

【請求項 19】

確定手段により、測定された前記記録ランダム化副成分が判定された前記ランダム化副成分と一致しない場合、前記不正顕示機能付文書の前記記録画素が改竄されたと確定する工程をさらに有することを特徴とする請求項 18 に記載の方法。

【発明の詳細な説明】

【技術分野】

【0001】

本発明は、記録文書の作成及び処理に関し、特に、不正顕示機能付文書の作成及び不正顕示機能付文書の改竄の検知に関する。説明を容易にし、且つ説明の一貫性を維持するために、まず、印刷文書に関する説明を行う。しかしながら、開示された方法は、情報が記録された他の形態の文書にも同様に適用できる。

【0002】

[背景]

最初に印刷文書を作成した時期から、その印刷文書がある不正な方法で改変されていないことを保証することは、多くの場合において望ましい。例えば、ある日時に同意され、署名された契約は、その後不正に改変されている可能性がある。このような改変を詳細に検知できることは、望ましい。同様に、小切手及び通貨代替物を含む様々な種類の有価証券は、不正に改変され易い価値を記録している。不正な改変に対する検知は、いずれの場合においても望ましい。このような検知が自動的に行われ、この検知により改変の正確な特徴を明らかにすることは、更に望ましい。文書に対する不正な改竄を検知することに加えて、このような文書が、不正な改変を可視的に防止できることは望ましい。

【0003】

文書に対する不正な改変の防止及び検知には、様々な方法が、提案され、使用されてきた。

【0004】

高品質カラスキャナ及びプリンタが市販される以前の使用方法の一つは、その時期では再現が困難であった特殊なフォントを使用して、又は特殊な陰影を施して重要情報（金額等）を印刷する方法であった。しかしながら、現代のプリンタ及びスキャナを使用すれば、このような技法に対しての攻撃が容易となった。

【0005】

改変検知の公知の一方法では、文書のページの一部分に印刷された 2 次元バーコードを使用して、署名領域等のいくつかの他の部分の表現を符号化する（暗号的に行われる可能性がある）。この 2 次元バーコードは、復号できる。オペレータは、生成された画像と、類

10

20

30

40

50

似性確認を意図した領域とを比較できる。

【0006】

関連研究の中心は、印刷／走査サイクルが施されていないデジタル画像の改竄の検知である。多くの「フラジャイル (fragile) 透かし」技法は、この研究分野において知られる。しかしながら、印刷文書が、ノイズ、ローテーション／スケーリング／トランスレーション (RST)、再サンプリング及び局所変形 (印刷／走査サイクルにおいて発生する) の導入に対する耐久力に乏しいため、これらの改竄検知技法は、一般に、印刷文書の改竄検知には適用できない。これらの改竄検知技法のうちのいくつかでは、画像の画素の最下位ビットの全て又はいくつかを、各画素内に残るビットのチェックサム等の形態で置換することにより演算を行う。

10

【0007】

また、多くの「セミフラジャイル (semi-fragile) 透かし」システムは、既に説明された。これらのセミフラジャイル透かしシステムは、相互相関を使用して、画像部分の簡易埋め込みシフトコピーの存在を検知するシステムを含む。別の技法は、透かしを画像ブロック内に埋め込み、その後、これらの埋め込まれた透かしの検知強度を比較することにより、改変されたブロックが存在するか否かを認識する方法である。これらのセミフラジャイル透かしシステムでは、透かしの検知能力が改善されると、位置推定能力が小さくなる傾向がある。また、それらの位置推定能力が改善されると、これらのセミフラジャイル透かしシステムは、よりノイズ及び他の変形に対する感受性が高くなるため、印刷文書の局所変化の検知に使用できない。

20

【0008】

他の技法では、特殊な素材を利用して、文書改変を困難にする。このような技法は、ラミネートに対する損傷が明らかな印刷表面を被覆する複数のラミネートを含む。しかしながら、特殊な素材の利用により、文書作成は複雑化するため、特殊な素材の利用は、普通紙用途に適用できない。また、特殊な素材には、自動検知を施すことができない。

【0009】

多くの既存の技法における追加的な欠点は、暗号セキュリティが脆弱であることである。多くの場合、一旦、採用されるべき暗号アルゴリズムが識別されると、このアルゴリズムは、直接識別された方法を攻撃するための破壊方法となる。

【0010】

本技法の別の共通の欠点は、ページの広い領域にわたるか、又は認証されるべき画像領域に完全に分離された領域にもわたる改変検知情報の分布である (上記のバーコード法と同様)。認証されるべき画像領域から離れた領域内の文書の偶発的な汚れが存在する場合、この改変検知情報の分布が問題となる。これらの改竄検知技法の多くは、文書全体の領域の認証に使用できないため、文書は、これら技法を含めるために特殊なデザインが施される必要がある。

30

【0011】

更なる種類の技法では、文書のオリジナル非改変形態に関する情報を、認証処理へ独立して転送する方法を使用する。この方法は、独立した知識を有する人物への電話呼び出しと同様に単純であり、安全保証位置内の文書の完全なコピーを維持するために拡張されてもよい。このような技法は、この技法がこのような独立情報の処理及び格納を必要とするため、多くの実施上の不都合な点を有する。

40

【特許文献1】米国特許第6, 457, 651号明細書

【特許文献2】米国特許第6, 366, 696号明細書

【特許文献3】米国特許第5, 291, 243号明細書

【特許文献4】米国特許第6, 167, 147号明細書

【特許文献5】米国特許第5, 509, 692号明細書

【0012】

[要約]

本発明の目的は、既存の構成の1つ以上の欠点をほぼ解決するか、あるいは、少なくとも

50

も改善することである。

【0013】

本発明は、印刷を所望する情報の処理形態（「ソース」情報と呼ばれる）を印刷文書に印刷する（記録情報に印刷された形態が使用される場合）ことにより、上述の問題の解決方法を探る構成、一般に、「改竄防止方法」と呼ばれるを開示する。上述の処理手順では、印刷され、可視摂動されたソース情報形態を作成する。摂動は、人間又は機械手段（例えば、ビデオ検知及びビデオ処理を使用して）が、印刷文書からソース情報を読み取ることを可能とするために、印刷摂動情報が、ソース情報に関して十分な忠実度を保持することである。しかしながら、「摂動」がソース情報への空間的な手掛かりであるため、ソース情報は、印刷文書の各領域における摂動の詳細を確立する。

10

【0014】

説明を容易にし、説明の一貫性を維持するために、まず、印刷文書への開示された改竄防止方法の用途に関する説明を行う。しかしながら、開示された方法は、情報が記録された文書の他の形態にも同様に適用できる。従って、例えば、改竄防止方法は、情報が光学的に記録された撮影フィルム（銀塩等）を有する文書に適用できる。

【0015】

摂動情報を形成するためのソース情報の処理では、暗号的に安全な鍵を使用する。一般に、この鍵の知識を使用しない印刷文書への改竄では、改竄領域内に「正確な」摂動要素を発生させることはない。印刷文書の改竄状態を認証するために、最初に、印刷文書の認証者は、目視により、あるいはビデオ処理を使用して、摂動ソース情報を抽出する。次に、ユーザは、ユーザの暗号コードの知識を使用して、文書上の摂動を再現する。改竄が行われた領域において、改竄情報と関連付けられた摂動は、この再現によって発生する。しかしながら、改竄者が、正確な摂動を正確に作成することが暗号的に妨げられたため、これらの摂動は、予め規定された信頼水準に対して正確ではない。

20

【0016】

改竄防止方法は、本来、不正顕示機能付文書を作成するために使用された暗号フィールド（の再生）を使用して精位置決めが施されるべき不正顕示機能付文書を必要とする。フィールドは、フィールドが機密（この場合、鍵）に基づくという意味で暗号的である。フィールドは、フィールドの断片が知られている場合においても、鍵の知識を使用せずにフィールドを完全に生成するためには実際的ではないという性質を有する。一構成によると、不正顕示機能付文書が暗号フィールドに関して変形されなかった場合、単純な登録ポイントは、不正顕示機能付文書内に組み込むことができる。これらの登録ポイントは、不正顕示機能付文書と妥当性検証に使用された暗号フィールドとの間の精位置決めを得るために使用できる。実現の観点から、図2に関して説明されるように、不正顕示機能付文書105が走査された場合、登録ポイントは、スキャナ2218（図1を参照）により検出できる。粗位置決め工程は、任意である。多くの用途において、特に、改竄が文書の小さな領域内で検知される場合、他の粗位置決め方法は、使用できる。いくつかの例においては、手動粗位置決めさえも利用できる。別の構成において、手動粗位置決めは、走査／印刷サイクルにより引き起こされた文書変形に対してよりロバストである。分散「粗」位置決め情報及び分散「精」位置決め情報は、不正顕示機能付文書内に埋め込まれ、その後、不正顕示機能付文書の妥当性検証時に、位置決めを実現するために使用される。

30

40

【0017】

本発明の一態様によれば、不正顕示機能付文書処理するためのコンピュータシステムの各手段による方法であって、

（a）分解手段により、記録されるべきN値レベル画像に関して、前記画像の少なくとも1つの画素をN個の可能な値を有する主成分に分解する工程と、

（b）選択手段により、少なくとも1つの所定のパターンのうちの、前記主成分の値に対応する所定のパターンからパターン要素を選択する工程であって、該所定のパターンはそのパターン要素がそれぞれ位置に対応づけられたシーケンスであり、前記画像内の前記少なくとも1つの画素の位置に対応する該パターン要素を選択する工程と、

50

(c) 形成手段により、前記少なくとも1つの画素に対して選択された前記パターン要素を転送媒体上に記録して不正顕示機能付文書を形成する工程と、

(d) 抽出手段により、前記少なくとも1つの画素に対して検索パターン要素を不正顕示機能付文書から抽出する工程と、

(e) 判定手段により、(d i) 前記検索パターン要素から抽出された主成分と、(d i i) 前記不正顕示機能付文書上の前記少なくとも1つの画素の位置と、に対応するパターン要素を判定する工程と、

(f) 比較手段により、前記検索パターン要素と判定された前記パターン要素とを比較する工程と

を有することを特徴とする方法を提供する。

10

【0018】

本発明の別の態様によれば、不正顕示機能付文書処理するためのコンピュータシステムの各手段による方法であって、

(a) 分解手段により、記録されるべきN値レベル画像に関して、前記画像の少なくとも1つの画素を、N個の可能な値を有する主成分と、並びに(a i) 前記主成分及び(a i i) 前記画像内の前記少なくとも1つの画素の位置に依存する、対応するランダム化副成分と、に分解する工程と、

(b) 形成手段により、前記少なくとも1つの画素に対する前記主成分及び前記ランダム化副成分を転送媒体上に記録して不正顕示機能付文書を形成する工程と、

(c) 抽出手段により、前記少なくとも1つの画素に対する前記主成分を不正顕示機能付文書から抽出する工程と、

20

(d) 判定手段により、(d i) 前記抽出主成分と、(d i i) 前記不正顕示機能付文書上の前記少なくとも1つの画素の位置とに依存する、前記対応するランダム化副成分を判定する工程と、

(e) 測定手段により、前記少なくとも1つの画素について印刷された前記ランダム化副成分を前記不正顕示機能付文書から測定する工程と、

(f) 宣言手段により、測定された前記印刷ランダム化副成分が判定された前記ランダム化副成分と一致しない場合、前記不正顕示機能付文書の画素が改竄されたと宣言する工程と

を有することを特徴とする方法を提供する。

30

【0021】

本発明のさらに別の態様によれば、不正顕示機能付文書の妥当性検証を行うためのコンピュータシステムの各手段による方法であって、

(a) 抽出手段により、検索パターン要素を、不正顕示機能付文書内の位置から抽出する工程と、

(b) 選択手段により、少なくとも1つの所定のパターンのうちの、前記検索パターン要素の特性に対応する所定のパターンからパターン要素を選択する工程であって、該所定のパターンはそのパターン要素がそれぞれ位置に対応づけられたシーケンスであり、前記位置に対応する該パターン要素を選択する工程と、

(c) 比較手段により、前記検索パターン要素と選択された前記パターン要素とを比較する工程と

40

を有することを特徴とする方法を提供する。

【0022】

本発明のさらに別の態様によれば、不正顕示機能付文書の妥当性検証を行うためのコンピュータシステムの各手段による方法であって、

(a) 抽出手段により、不正顕示機能付文書に含まれる少なくとも1つの記録画素に対して、N個の可能な値を有する主成分を前記不正顕示機能付文書から抽出する工程と、

(b) 判定手段により、少なくとも1つの所定のパターンのうちの、前記抽出主成分に対応する所定のパターンからパターン要素を選択し、該パターン要素に対応して予め定められたランダム化副成分を判定する工程であって、該所定のパターンはそのパターン要素

50

がそれぞれ位置に対応づけられたシーケンスであり、前記少なくとも1つの記録画素の位置に対応する該パターン要素に対応して予め定められた対応するランダム化副成分を判定する工程と、

(c) 測定手段により、前記少なくとも1つの画素に対応して前記不正顕示機能付文書上に記録されているランダム化副成分を、前記不正顕示機能付文書から測定する工程と、

(d) 比較手段により、測定された前記ランダム化副成分と判定された前記ランダム化副成分とを比較する工程と

を有することを特徴とする方法を提供する。

【0031】

本発明の他の態様もまた開示される。

【0032】

[最良の形態を含む詳細な説明]

本発明は、1つ以上の添付の図面のステップ及び／又は特徴と関連させて説明される。1つ以上の添付の図面において、同一符号で示すステップ及び／又は特徴は、別途特定されない限り、同一の1つ以上の機能又は動作を表す。

【0033】

尚、「背景技術」及び従来技術の構成に関連する以上の記載は、それぞれ刊行物及び／又は実施を通して公知技術を形成する複数の文献又は装置の記載に関する。当該記載は、これらの文献や装置が多少なりとも当該技術分野における周知技術の一部を形成するものとして本発明者又は出願人が説明したものと解釈するべきではない。

【0034】

開示された「改竄防止方法」により、モノクロのオリジナル文書を特定セキュリティマーキングにより印刷する（又は、再印刷する）ことが可能となる。この説明は、2値レベル（例えば、モノクロ）文書に関するが、開示された改竄防止方法は、例えば、黒ソース情報、グレーソース情報及び白ソース情報を使用した多値レベル文書に利用できる。あるいは、改竄防止方法では、ディザ法又は網点を使用して、黒画素及び白画素で階調を表現してもよい。生成された「不正顕示機能付」文書は、人間により直接に認識及び読み取りが行われ、走査及び解析を施すことにより、改竄（改変等）が行われたか否かを検知できる。読み手にとっての印刷文書上での可視事象とオリジナル文書上での可視事象との間の局所化された詳細な差異は、例えば、ノイズ、退色、物理的変形、及び印刷／走査処理により導入される多くの変化等の印刷文書に対する微小な損傷でさえも明らかにできる。不正顕示機能付文書に適用される妥当性検証処理は、オリジナルのソース情報の知識を必要としない。差異は、局所化された詳細な状態で明らかにされるので、明らかにされた差異を見る人物は、汚れ又は偶発的なペンマーク等の些細な変化から金額の変化等の重要な変化までを容易に識別できる。妥当性検証処理は、予め規定された信頼水準までは、「中継者」攻撃に対して、暗号的に安全である。中継者攻撃は、鍵を所有していない場合における悪意のある介入による攻撃を説明するために使用される暗号法用語である。

【0035】

妥当性検証解析は、物質的な（印刷された）不正顕示機能付文書及び共通秘密鍵へのアクセスのみに必要である。好適な構成において、この共通秘密鍵は、システムの暗号安全管理を疑問視することなく、多くの文書に対して同一であってもよい。特に、本発明の方法では、同一の鍵でマーキングした異なるページの情報に基づく攻撃を受け易くなることはない。

【0036】

次のいくつかの部分の説明では、コンピュータメモリ内のデータの演算アルゴリズム及び演算記号表現を、明示的又は黙示的に提示する。これらのアルゴリズムの説明及び表現は、データ処理の当業者の業務の実質内容を最も効果的に他の当業者に受け渡すために、データ処理の当業者により使用される方法である。ここで、一般に、アルゴリズムは、所望の結果を導出する工程の自己矛盾のないシーケンスであると考えられる。この工程は、物理量の物理的処理を必要とする工程である。これらの量は、必ずしも必要ではないが、

10

20

30

40

50

通常、格納、転送、結合、比較及び他の操作を施すことが可能な電気信号又は磁気信号の形態をとる。主に慣用的な理由により、ビット、値、要素、記号、文字、用語、数等として、これらの信号を示すことが好都合な場合があることが判明している。

【0037】

しかしながら、上記の用語及び類似の用語は、適切な物理量と関連付けられるべきであり、これらの物理量に適用される好都合な表現に過ぎないことを理解すべきである。特に説明はしないが、次の説明から明らかなように、本明細書を通して、「走査」、「算出」、「判定」、「交換」、「生成」、「初期化」、「出力」等の用語を使用する説明が、コンピュータシステム又は類似の電子装置の動作及び処理に関連することは理解できる。コンピュータシステム又は類似の電子装置は、レジスタ内及びコンピュータシステムのメモリ内の物理（電子）量として表現されたデータを処理し、このデータをコンピュータシステムのメモリ内、レジスタ内又は他の情報記憶装置内、情報送信装置内又は情報表示装置内の物理量として同様に表現される他のデータに変換する。

10

【0038】

また、本明細書は、本発明の方法を実施する装置を開示する。このような装置は、要求される目的に応じて特別に構築されてもよい。あるいは、このような装置は、汎用コンピュータ又はコンピュータ内に格納されたコンピュータプログラムにより選択的に実行又は再構成される他の装置を具備してもよい。この説明において提示された複数のアルゴリズム及び表示は、本質的に、いずれかの特定コンピュータ又は他の装置と関連付けられていない。様々な汎用機械は、この説明の教示に従ったプログラムと共に使用されてもよい。あるいは、必要な方法工程を実行するためのより特殊化された装置の構築が、適切である。従来の汎用コンピュータの構造は、以下の説明から明らかとなる。

20

【0039】

また、開示された構成は、暗黙のうちに、1つ以上のコンピュータプログラムモジュールを開示する。この開示において、当業者には明らかなように、ここで説明する方法の個々の工程は、1つ以上のコンピュータコードモジュールにより実行される。1つ以上のコンピュータプログラムが、任意の特定プログラミング言語及びその特定プログラミング言語の実現に限定されることは、意図されていない。様々なプログラミング言語及びプログラミング言語のコーディングが、この説明に含まれる本開示の教示を実現するために使用できることは、理解できる。更に、コンピュータプログラムは、任意の特定制御フローに限定されることは、意図されていない。そのため、多くの他のコンピュータプログラムの変形が存在する。この変形では、開示された構成の趣旨の範囲を逸脱せずに、異なる制御フローを使用できる。更に、コンピュータプログラムの1つ以上のステップは、連続的ではなく、並行に実行されてもよい。

30

【0040】

このようなコンピュータプログラムは、任意の1つ以上のコンピュータ可読媒体内に格納されてもよい。コンピュータ可読媒体は、磁気ディスク、光ディスク、メモリチップ又は1つ以上の汎用コンピュータとインタフェースで連結するのに適切な他の記憶装置等の記憶装置を含む。また、コンピュータ可読媒体は、インターネットシステムで例証される1つ以上のハードワイヤード媒体、又はGSM移動式電話システムで例証される無線媒体を含んでもよい。コンピュータプログラムモジュールは、汎用コンピュータ等内に読み込まれ、実行されることにより、好適な方法の工程を実現する装置において、効果的に得られる。

40

【0041】

図1は、説明される改竄防止構成が実現可能な汎用コンピュータを概略的に示すブロック図である。改竄防止方法は、図1に示すような汎用コンピュータシステム2200を使用して実現されることが好ましい。この場合、図3、図4、図6、図7、図12～図15、図17、図18の処理は、コンピュータシステム2200内で実行する改竄防止アプリケーションプログラム等のソフトウェアとして実現されてもよい。特に、改竄防止方法の工程は、コンピュータにより実行される改竄防止アプリケーションソフトウェアの命令に

50

より実行される。命令は、各々が1つ以上の特定タスクを実行する1つ以上のコードモジュールとして構成されてもよい。また、改竄防止アプリケーションソフトウェアは、2つの個別の区分に分割されてもよい。この個別の区分において、第1の区分は、改竄防止方法を実行し、第2の区分は、第1の区分とユーザとの間のユーザインタフェースを管理する。改竄防止アプリケーションソフトウェアは、例えば、以下に説明する記憶装置を含むコンピュータ可読媒体内に格納されてもよい。改竄防止アプリケーションソフトウェアは、コンピュータ可読媒体からコンピュータ内に読み込まれ、コンピュータにより実行される。このようなソフトウェア又はコンピュータプログラムが記録されたコンピュータ可読媒体は、コンピュータプログラムプロダクトである。コンピュータ内のコンピュータプログラムプロダクトの使用は、改竄防止に有用な装置に対して有効である。

10

【0042】

コンピュータシステム2200は、コンピュータモジュール2201と、キーボード2202、マウス2203及びスキャナ2218等の入力装置と、プリンタ2215、表示装置2214及びスピーカ2217を含む出力装置とにより構成される。変調器—復調器(モデム)トランシーバ装置2216は、例えば、電話回線2221又は他の機能媒体を介して接続可能な通信ネットワーク2220との通信のために、コンピュータモジュール2201により使用される。モデム2216は、インターネットへのアクセス、及びローカルエリアネットワーク(LAN)又は広域ネットワーク(WAN)等の他のネットワークシステムへのアクセスの獲得のために使用できる。また、モデム2216は、いくつかの実現例において、コンピュータモジュール2201に内蔵されてもよい。

20

【0043】

コンピュータモジュール2201は、通常、少なくとも1つのプロセッサユニット2205及びメモリユニット2206を含む。メモリユニット2206は、例えば、半導体ランダムアクセスメモリ(RAM)及び半導体読み取り専用メモリ(ROM)から構成される。また、モジュール2201は、多数の入出力(I/O)インタフェースを含む。多数の入出力(I/O)インタフェースは、ビデオ表示装置2214及びスピーカ2217に接続されるオーディオ/ビデオインタフェース2207と、キーボード2202、マウス2203及び任意のジョイスティック(不図示)用のI/Oインタフェース2213と、モデム2216、スキャナ2218及びプリンタ2215用のインタフェース2208とを含む。いくつかの実現例において、モデム2216は、インタフェース2208内等のコンピュータモジュール2201に内蔵されてもよい。記憶装置2209は、コンピュータモジュール2201内に設けられ、通常、ハードディスクドライブ2210と、フロッピディスクドライブ2211とを含む。更に、コンピュータモジュール2201は、磁気テープドライブ(不図示)を使用してもよい。CD-ROMドライブ2212は、通常、不揮発性データの供給源として設けられる。

30

【0044】

コンピュータモジュール2201の構成要素2205から構成要素2213は、通常、関連技術の当業者に知られるコンピュータシステム2200の従来の動作モードが得られるように、相互接続バス2204を介して通信を行う。上述の構成を実現可能なコンピュータの例は、複数のIBM-PCと、IBM-PCの互換機と、Sun Sparcstations又はSun Sparcstationsから派生した類似のコンピュータシステムとを含む。

40

【0045】

通常、改竄防止アプリケーションプログラムは、ハードディスクドライブ2210上に常駐する。改竄防止アプリケーションプログラムは、プロセッサ2205により、ハードディスクドライブ2210の作動時に読み取られ、制御される。プログラム及びネットワーク2220から取り込まれた任意のデータの間合格納は、半導体メモリ2206を使用して実現されてもよく、ハードディスクドライブ2210との協働により行われてもよい。いくつかの例において、改竄防止アプリケーションプログラムは、それぞれ、破線2224で示すように、CD-ROM2225上で、又は破線2223で示すように、フロッ

50

ピディスク 2 2 2 2 上で符号化され、且つ対応するドライブ 2 2 1 2 又はドライブ 2 2 1 1 を介して読み取られた状態でユーザに提供されてもよい。あるいは、改竄防止プログラムは、モデム装置 2 2 1 6 を介してネットワーク 2 2 2 0 からユーザにより読み取られてもよい。更に、改竄防止アプリケーションソフトウェアは、他のコンピュータ可読媒体からコンピュータシステム 2 2 0 0 内に読み込み可能である。本明細書で用いられる「コンピュータ可読媒体」とは、実行及び／又は処理のために、命令及び／又はデータを、コンピュータシステム 2 2 0 0 へ提供することに関わる任意の記憶媒体又は送信媒体である。記憶媒体の例には、フロッピディスク、磁気テープ、C D - R O M、ハードディスクドライブ、R O M 又は集積回路、光磁気ディスク、又は P C M C I A カード等のコンピュータ可読カードが含まれる。これらの装置は、コンピュータモジュール 2 2 0 1 の内部又は外部のいずれに設けられてもよい。送信媒体の例は、無線送信チャネル又は赤外線送信チャネルと、別のコンピュータ又はネットワーク装置へのネットワーク接続回路と、ウェブサイト等に記録された電子メール送信及び情報を含むインターネット又はイントラネットとを含む。

10

【0046】

改竄防止技法の好適な構成は、コンピュータシステム 2 2 0 0 のような汎用コンピュータシステム上で実行される 1 つ以上のソフトウェアモジュールとして実現される。しかしながら、改竄防止技法は、複合機等の埋め込み型システムの改竄防止アプリケーションソフトウェアモジュールとして実現されてもよい。また、改竄防止技法は、特定用途向け集積回路又は F P G A (Field Programmable Gate Array) 等の固定論理又はプログラマブル固体論理回路により実現されてもよい。

20

【0047】

図 2 は、開示された改竄防止システムの機能ブロック図の一例を示す図である。図 2 は、不正顕示機能付文書 1 0 5 及び不正顕示機能付文書 1 0 5 ' を作成する作成サブシステム 1 2 6 と、不正顕示機能付文書 1 0 5 及び不正顕示機能付文書 1 0 5 ' が改竄されたか否かを検知する(妥当性検証を行う)妥当性検証サブシステム 1 2 7 とを有する。

【0048】

不正顕示機能付文書 1 0 5 を作成する作成サブシステム 1 2 6 を考えると、選択モジュール 1 0 4 は、走査ベースの 2 値レベルソース信号 1 1 7 の値に応じて、2 つの同期させた暗号信号 1 1 5 及び暗号信号 1 1 6 のうちの 1 つから選択する。信号 1 1 7 は、印刷されるべきソース情報であり、2 値レベルソース画像 1 0 1 から導出される。それぞれ、暗号信号 1 1 5 は、暗号信号供給源 1 0 2 により生成されたストリーム暗号であり、暗号信号 1 1 6 は、暗号信号供給源 1 0 3 により生成されたストリーム暗号である。暗号信号供給源 1 0 2 は、鍵生成モジュール 1 3 4 からの矢印 1 3 5 で示すように、秘密鍵ベース情報を受け取る。暗号信号供給源 1 0 3 は、鍵生成モジュール 1 3 4 からの矢印 1 3 6 で示すように、秘密鍵ベース情報を受け取る。鍵生成モジュール 1 3 4、暗号信号供給源 1 0 2 及び暗号信号供給源 1 0 3 の動作は、図 6 に関して更に説明される。ソース文書 1 0 1 が紙文書の形態である場合、スキャナ 2 2 1 8 (図 1 を参照)を使用して、信号 1 1 7 を紙文書 1 0 1 から発生させることができる。ソース文書が電子文書形式(Adobe PDF 等)である場合、信号 1 1 7 をラスタ画像プロセッサ(R I P)から発生させることができる。R I P は、電子文書を、信号 1 1 7 を形成する画素に変換する。あるいは、ソース画像 1 0 1 が、メモリ(不図示)内にデジタル画像形態で格納された場合、信号 1 1 7 は、走査ベース方式でメモリから読み出すことができる。

30

40

【0049】

ソース信号 1 1 7 を使用して、暗号信号 1 1 5 と暗号信号 1 1 6 との間からいずれかの信号を選択することにより、それぞれのルックアップテーブル 1 3 0 及びルックアップテーブル 1 3 1 と関連させて変調された合成暗号信号 1 1 8 を形成する。変調された合成暗号信号 1 1 8 は、ソース情報 1 0 1 の可視摂動バージョンである。本例において、ソース画像 1 0 1 は、黒画素及び白画素で合成された 2 値レベル画像である。一構成例によると、合成信号 1 1 8 は、「暗」画素及び「明」画素で合成された多値レベル画像を表現する

50

。そのため、一例において、「暗」画素は、黒並びに完全な純色の赤、緑及び青のうちの1色であってもよい。「明」画素は、白、シアン、マゼンダ及びイエロのうちの1色であってもよい。

【0050】

そのため、ソース画像101が2値レベルである本例において、2つの各暗号信号115及び暗号信号116は、それぞれのルックアップテーブル130及びルックアップテーブル131を介して、非暗号であり且つ相互に識別可能な主成分を有する信号と関連付けられる。信号115及び信号116のうちの他方と関連付けられた主成分は、常時、視覚的に暗い。一方、信号115及び信号116のうちの他方と関連付けられた主成分は、常時、視覚的に明るい。更に、2つの各暗号信号115及び暗号信号116は、それぞれのルックアップテーブル130及びルックアップテーブル131を介して、暗号副成分（例えば、色変化の形態をとる）と関連付けられる。

10

【0051】

「非暗号」は、相互に識別可能な複数の主成分が、暗号を考慮せずに互いに区別できることを意味する。

【0052】

多値レベル（N段階の異なる色調を有するN値レベル）文書において、N個の暗号供給源102、・・・、103が使用される。N個の各暗号供給源は、それぞれのルックアップテーブルを介して、暗号信号と関連付けられる。この暗号信号は、非暗号であり、且つ相互に識別可能なN個の主成分、及びN個の暗号副成分を有する。

20

【0053】

図2の2値レベル文書の場合に戻ると、合成暗号信号118は、組み合わせモジュール114内で組み合わせ処理が実行される。生成された合成されたコンポジット信号122は、記録モジュール（図1のプリンタ2215等）により転送媒体上に記録され、本例においては、印刷された不正顕示機能付文書105を形成する。転送媒体は、通常、印刷文書を形成するために使用される紙である。この場合、転送媒体を印刷媒体と呼ぶ。転送媒体の別の例は、銀塩フィルムである。また、合成されたコンポジット信号のデジタル転送も、可能である。

【0054】

多くの場合、この説明における「文書」という用語は、合成されたコンポジット信号122がプリンタ（図1のプリンタ2215等）により印刷される印刷（転送）媒体を有する印刷文書のコンテキストにおいて使用されるが、文書という用語は、より一般的な意味を有する。従って、文書という用語は、合成されたコンポジット信号122が適切な光学処理及び／又は光学装置を使用して記録された銀塩フィルム（転送）媒体を有する記録文書等にも適用できる。

30

【0055】

更に別の構成において、マーキング処理及び認証処理は、複数のデジタル文書画像の準備、格納、転送及び認証において使用されてもよい。この構成において、開示された改竄防止方法を内蔵するコンピュータアプリケーションは、まず、マーキング処理をデジタル文書画像に適用する。このデジタル文書画像は、走査処理の一部として作成された。しかしながら、このデジタル文書画像は、デジタル手段のみにより作成してもよい。その後、アーカイブ、送信、再符号化（異なるデジタル画像標準への変換等）、再サンプリング（画像スケーリング中に作成する）、及び圧縮又は再圧縮（ベースラインJPEG圧縮等の所謂「非可逆」圧縮を含む）のうちの1つ以上の処理が、文書画像に対して実行される。これらの動作のうちの1つ以上の動作の後、コンピュータアプリケーションは、開示された認証処理、及び第2のコンピュータアプリケーションを使用して表示された結果を使用して、生成された画像を認証してもよい。上述のマーキング処理及び認証処理の使用は、画像変換により画像のデジタルビットパターン又は画像の符号化に重要な変化を施す場合においても、画像の出現に対して有効な可視変化を施さない画像変換に対してロバストである。

40

50

【0056】

合成されたコンポジット信号122を構築する暗号信号115及び暗号信号116と関連付けられた主成分は、オリジナルのソース画像101を読み取り可能とした場合と同様の方法によって、人間又は機械が不正顕示機能付文書105を読み取ることを可能とする。ソース画像101内の情報に対する追加としての副摂動成分は、不正顕示機能付文書105内で可視であるが、この摂動が微小なため、人間（又は機械）の読み手又は読取り装置では認識されない。そのため、不正顕示機能付文書105は、ソース画像101から可視摂動が行なわれるが、ソース画像101と明確に等価である。換言すれば、印刷媒体上に印刷された場合に摂動されたソース情報は、人間又は機械により読み取り可能な状態である。

10

【0057】

妥当性検証サブシステム127における位置決め処理のロバストさを改善するために、粗位置決め提供源111からの任意の視覚的に微弱な粗位置決め信号128は、組み合わせモジュール114により変調された合成暗号信号118上に重畳される。位置決めが（a）手動登録マーク方法又は（b）精位置決め処理のみのいずれかに依存するため、粗位置決め信号は、任意である。十分な計算資源が利用可能な場合、精位置決め処理のみを使用して位置決めを実現することができる。尚、この方法では、検索を行う必要がある。開示された精位置決め処理は、手動粗位置決め方法又は別の粗位置決め方法を使用して十分に実行される。更に、複数の異なる不正顕示機能付文書105…、105'からの合成信号120の試験により、暗号信号115及び暗号信号116の潜在的な回復を防止するために、暗号信号115及び暗号信号116を生成する秘密鍵（図6のステップ2501を参照）は、2つの要素から作成される。第1の要素は、複数の文書105、…、105'のために固定される。この第1の要素は、文書105、…、105'の任意の1つに適用されるような妥当性検証サブシステム127により実行される妥当性検証処理に必要とされる。第2の要素は、ソルト生成器112からの「ソルト」値129と呼ばれる。ソルト値は、各文書105、…、105'（図6のステップ2508及びステップ2501を参照）に対して固有である。ソルト値の使用は、暗号法分野において公知の技法である。ソルト値129は、組み合わせモジュール114により各不正顕示機能付文書105、…、105'の変調された合成暗号信号118内にわずかに埋め込まれる。また、ソルト値129は、矢印142で示すように、鍵生成モジュール134に提供される。ソルト値129は、妥当性検証処理中に粗位置決め／ソルト回復モジュール113により再び回復できる。そのため、妥当性検証サブシステム127による不正顕示機能付文書105の妥当性検証処理は、秘密鍵及びソルト値129の（共通の）第1の要素を必要とする。ソルト値129は、秘密鍵の第2の要素と同様に、不正顕示機能付文書105に対して固有である。不正顕示機能付文書105'の妥当性検証処理は、秘密鍵及びソルト値の（共通の）第1の要素を必要とする。ソルト値は、秘密鍵の第2の要素と同様に、不正顕示機能付文書105'に対して固有である。

20

30

【0058】

秘密鍵の共通の第1の要素140は、管理手段（例えば、オペレータに手動で妥当性検証サブシステム127に入力させるために渡された密封封筒内の第1の要素を提供する）等により妥当性検証サブシステム127に提供される。要素140は、矢印141で示すように、暗号信号供給源102'及び暗号信号供給源103'に提供される。各不正顕示機能付文書105からの妥当性検証サブシステム127は、秘密鍵の第2の文書固有要素を抽出できる。

40

【0059】

改竄検知（妥当性検証とも呼ばれる）のために使用された妥当性検証サブシステム127に戻ると、走査ベース不正顕示信号120は、図1のスキヤナ2218を使用して、作成サブシステム126により作成した不正顕示機能付文書105を走査することにより導出される。信号120は、主成分（オリジナル情報117を反映すると仮定される）及び副成分（選択モジュール104の制御下において、暗号信号115及び暗号信号116に

50

より導入されると仮定される)を含む。粗位置決め／ソルト回復モジュール113は、不正顕示機能付文書105の粗位置決めを実行し、「粗位置決め」走査ベース不正顕示機能付文書121を作成する。また、ソルトモジュール113は、信号120からソルト値を抽出し、矢印139で示すように、暗号信号供給源102'及び暗号信号供給源103'にソルト値を提供する。精位置決めモジュール106は、粗位置決め信号121の色成分と、同期させた暗号信号115'及び暗号信号116'、並びにルックアップテーブル134からの色138及びルックアップテーブル135からの色137を組み合わせる(すなわち、平均化する)ことにより作成された信号とを相関させる。尚、色137と色138とは、関連付けられている。図4に関してより詳細に説明するように、上記の組み合わせられた暗号信号115'及び暗号信号116'、並びに色137及び色138は、暗号信号115'及び暗号信号116'のカラー画像バージョンを形成する。

10

【0060】

信号115'は、暗号信号供給源102'からの暗号信号であり、信号116'は、暗号信号供給源103'からの暗号信号である。暗号信号供給源102'及び暗号信号供給源103'は、通常、暗号信号供給源102及び暗号信号供給源103から物理的に離間されているが、同一である。精位置決めモジュール106により実行された相関付けにより、粗位置決め不正顕示信号121と暗号信号115'及び暗号信号116'との間の精スケール同期(すなわち、位置決め)は、不正顕示機能付文書105内を人間又は機械が読み取り可能な強力な主成分と独立して実現される。この位置決めは、「精位置決め」走査ベース不正顕示信号123を形成する。

20

【0061】

その後、妥当性検証サブシステム127における妥当性検証処理では、閾化モジュール107を使用して、精位置決め不正顕示信号123内に存在する複数の暗号信号の複数の主成分を識別することにより、2値レベル信号119を形成する。2値レベル信号119は、(オリジナル)2値レベル信号117と仮定される。ソース信号117がN値レベルである場合、仮定文書信号119は、N値レベル信号である。ソース信号117が2値レベルソースの本例では、文書信号119は、2値レベルである。次に、比較モジュール108において、123で示す信号と同一の信号である精位置決め不正顕示信号124は、選択モジュール109の制御下で、第1の暗号信号115'と関連付けられたルックアップテーブル134からの値、又は第2の暗号信号116'と関連付けられたルックアップ

30

テーブル135からの値のいずれかの値と比較される。選択モジュール109は、対応する走査位置の信号119の2値レベルの値に従って切り替えられる。選択モジュール109は、対応する走査位置の信号119の2値レベルの値に従って変調された合成暗号信号125を出力する。不正顕示機能付文書105からの信号119の副成分と、対応する変調された合成暗号信号125からの副成分とが一定の許容範囲内で一致しない複数の走査位置(画素位置と呼ばれる)は、妥当性検証信号モジュール110により(例えば、改変の導入を介して)改竄されたことが明らかにされる。

【0062】

＜不正顕示機能付文書形成方法の詳細な説明＞

本実施例において、2値レベルソース画像101からの2値レベル信号供給源117は、デジタル形式の白黒文書画像を表現する。この(ソース)画像101は、ラスタ化処理(RIP)提供元、走査提供元又は他の等価の提供元の出力として発信できる。不正顕示機能付文書105を作成するために、このソース画像101の導出を紙転送媒体上にマーキングすることにより、ソース画像101は、不正顕示機能付文書105となる。妥当性検証サブシステム127により実行される妥当性検証(すなわち、改竄検知)処理は、媒体(文書105に対して使用される)がオリジナルのソース画像101の各サンプルに対する3つ以上の識別可能な値を支持する必要がある。従って、オリジナルのソース画像101の解像度を、このような処理が実現されるように設定する必要がある。

40

【0063】

不正顕示機能付文書105は、必要な情報を保持可能にするため、十分に高度な解像度

50

を有する必要がある。例えば、プリンタがハーフトーン装置である場合、不正顕示機能付文書105は、装置画素の収集を利用して複数の識別可能な値を得る。

【0064】

実現可能な空間解像度は、印刷技術と共に変化する。電子写真（レーザ）印刷技術及び熱インクジェット技術を含む多くの現代印刷技術に対して、オリジナルのソース画像101の解像度は、約200DPIである。多くの場合において、より高度な解像度は、実現可能である。ソース画像101に対する解像度が低下すると共に、解像度は、徐々によりロバストになる（すなわち、印刷処理及び走査処理に固有の誤り及び劣化の許容度が高くなる）。しかしながら、解像度の品質は、明らかに低い。

【0065】

暗号信号供給源102からの暗号信号115及び暗号信号供給源103からの暗号信号116は、ストリーム暗号から生成された2次元暗号フィールドから導出される。上述の構成において、暗号信号115及び暗号信号116は、52ビット鍵を有するRC4ストリーム暗号のマスタ・インスタンスーションを使用して生成される。暗号信号115及び暗号信号116は、まず、単一のマスタRC4ストリームから、暗号信号（115等）へ交互バイトを指向させ、且つ次に他の暗号信号（116等）へ指向させることにより生成される。他のストリーム暗号又は擬似ランダムシーケンス生成器は、異なる鍵長さで、交互に利用できる。別の技法の例は、一对の最大期間の線形フィードバックシフトレジスタを使用して、暗号信号115及び暗号信号116を生成することである。この例は、図6に関連してより詳細に説明する。

【0066】

図3は、図2のシステムを使用して、開示された改竄防止方法に係る不正顕示機能付文書を作成する方法ステップのフローチャートとして、プロセス2300を示す。プロセス2300は、ステップ2301で開始する。ステップ2301では、ソース画像101からの次の画素を読み取る。その後、判断ステップ2302では、上記の画素値を判定する。この説明のバルクが2値レベルである場合、ステップ2301において読み取られた画素は、2つの可能な値のうちの1つを有する。しかしながら、一般に、ソース画像101は、N段階のレベルを有することが可能である。そのため、一般に、判断ステップ2302では、ステップ2301において読み取られた画素が、複数のN値のうちの1つの値を有することが可能であることを考慮すると、その画素は、そのうちのどの値を有するかを判定する。ステップ2302において、画素値がBに等しいと判定された場合、プロセス2300は、矢印Bに従って、ステップ2303へ進む。ステップ2303では、（a）画素値に従って暗号フィールドBを選択し、（b）次に、当該画素の位置に依存する上記の暗号フィールドから値を選択し、且つ（c）最後に、多値レベル画素値を判定するために、暗号フィールドBから選択された値を使用してルックアップテーブルBを索引することにより、多値レベル画素値を判定する。続くステップ2311では、この画素値を格納する。その後、プロセス2300は、判断（検査）ステップ2304へ進む。ステップ2304では、ソース画像101内で更なる画素が使用できるか否かが判定される。更なる画素が使用できる場合、プロセス2300は、矢印YESに従って、ステップ2301へ戻る。

【0067】

判断（検査）ステップ2302へ戻ると、画素が値Aを有すると判定された場合、プロセス2300は、矢印Aに従って、ステップ2305へ進む。ステップ2305は、ステップ2303と同様に機能する。その後、プロセス2300は、ステップ2311へ進む。

【0068】

判断ステップ2302へ戻ると、画素が値Cを有すると判定された場合、プロセス2300は、破線矢印Cに従って処理ブロック（不図示）へ進む。処理ブロックは、ブロック2303及びブロック2305と等価である。ソース文書101がN段階のレベルを有する一般的な場合において、判断ステップ2302では、N通りの判断のうちの1つを行う

10

20

30

40

50

ことができる。

【0069】

判断ステップ2304へ戻ると、更なる画素が使用できない場合、プロセス2300は、矢印N Oに従って、ステップ2307へ進む。ステップ2307では、多値レベル画素データと粗位置決めマーク及びソルト値とを組み合わせる。その後、ステップ2308では、合成されたコンポジット信号を印刷媒体上に印刷する。ステップ2308の結果、破線矢印2309で示すように、不正顕示機能付文書105が得られる（図2を参照）。

【0070】

図4は、図3の不正顕示機能付文書が改竄されたか否かを判定する方法ステップのフローチャートとして、プロセス2400を示す。プロセス2400は、ステップ2430で開始する。ステップ2430では、不正顕示機能付文書105を走査する。その後、ステップ2401では、粗位置決めマークを回復する。その後、ステップ2402では、回復された粗位置決めマークを使用して暗号フィールドに対して不正顕示機能付文書105の粗位置決めを行う。続くステップ2422では、文書105からソルト値を回復する。その後、ステップ2403では、不正顕示機能付文書105と暗号フィールドとの間の精位置決めを行う。精位置決めステップ2403は、3つのサブプロセスを有する。第1のサブプロセス2403Aでは、図15に関してより詳細に説明するように、ブロック相関付けを行うことにより、置換マップを形成する。第2のサブプロセス2403Bでは、図17に関してより詳細に説明するように、置換マップに関して補間を行う。第3のサブプロセス2403Cでは、図18に関してより詳細に説明するように、ワーピングを行うことにより、精位置決め文書を形成する。

【0071】

次のステップ2404では、走査対象の不正顕示機能付文書105の次の画素を読み取る。その後、判断（検査）ステップ2405では、2値レベルソース画像101に対して、画素の主成分が値A又は値Bを有するか否かを検査する。図3に関して説明された場合と同様に、ソース画像101がN段階のレベルを有する場合、判断ステップ2405は、N回の判断ブランチを有する。

【0072】

本例において、画素の主成分が値Aを有する場合、プロセス2400は、矢印Aで示すように、ステップ2407へ進む。ステップ2407では、上記の画素位置の仮定副成分を判定する。この判定は、当該画素位置の暗号フィールドAを考慮し、且つこの暗号フィールド値を使用して関連ルックアップテーブル（図2の130及び131を参照）を索引することにより行われる。この判定により、仮定副成分が生成される。その後、ステップ2417では、印刷文書105から当該画素位置の実際の副成分値を読み取る。続く判断ステップ2409では、ステップ2407からの仮定副成分値が、ある許容度の範囲内でステップ2417からの実際の読み取り副成分値に等しいか否かが確認される。仮定副成分値が実際の副成分値と等しくない場合、プロセス2400は、矢印N Oに従って、ステップ2415へ進む。ステップ2415では、上記の画素位置において改竄が行われたことを宣言する。

【0073】

判断ステップ2405へ戻ると、画素の主成分が値Bを有すると判定された場合、プロセス2400は、矢印Bに従って、ステップ2411へ進む。ステップ2411は、ステップ2407と同様に、すなわち、当該画素位置の仮定副成分を判定するために、当該画素位置の暗号フィールドBを参照し、且つ暗号フィールド値の使用により図2からの関連ルックアップテーブル130又はルックアップテーブル131を索引することによって機能する。その後、プロセス2400は、ステップ2417へ進む。

【0074】

判断ステップ2409へ戻ると、ステップ2407及びステップ2408からの仮定副成分が、受け入れ可能な許容範囲まで、ステップ2417の印刷文書からの実際の読み取り副成分に等しい場合、プロセス2400は、矢印Y E Sに従って、ステップ2413へ

進む。ステップ2413では、関心画素位置において改竄が検知されなかったことを宣言する。その後、プロセスは、矢印2414に従って、ステップ2404へ進む。プロセス2400は、ステップ2415からもステップ2404へ進む。

【0075】

＜2次元暗号フィールドの生成＞

図5は、2次元暗号フィールド（2次元暗号フィールドとも呼ばれる）の生成を表す図である。図5は、ストリーム暗号から2次元暗号フィールド306及び2次元暗号フィールド307を生成するための2つの方法を示す。暗号フィールドの生成は、図6に関して説明するプロセス2500に従って、暗号信号供給源102及び暗号信号供給源103（図2を参照）により作成サブシステム126において、並びに暗号信号供給源102'及び暗号信号供給源103'により妥当性検証サブシステム127において行われる。

10

【0076】

妥当性検証処理において暗号鍵データを使用するため、暗号フィールドを再生できるように、ストリーム暗号を2次元暗号フィールドに変換することが望ましい。特に、オリジナルのソース画像101の走査線の長さに依存することを回避することが望ましい。例えば、ストリーム暗号が、ラスト順に単純に暗号フィールドに変換された場合、この走査線の長さへの依存は、引き起こされる。また、暗号フィールド306及び暗号フィールド307は、ラスト順に生成されることが望ましい。暗号フィールド306及び暗号フィールド307は、ソース画像101の公称中心位置に対して生成される。この公称中心位置は、通常、画像101の空間的中心付近に位置決めされるが、必ずしも空間的中心付近ではない。

20

【0077】

図5の暗号フィールド306を考慮すると、鍵K1（すなわち、鍵301）は、2つの暗号信号供給源（図2の暗号信号供給源102又は暗号信号供給源103）のうちの1つによる利用のために生成された第1の52ビットシーケンスである。ストリーム暗号の次の52ビットセグメントは、以前に生成された鍵（K1等）上における鍵位置（K2等）、及び以前に生成された鍵（K1等）下における鍵位置（K3等）に、交互に割り当てられる。このようにして、最初の52ビットシーケンス鍵の中心スパイン（Spine）308は、生成される。スパイン308は、垂直方向の任意の所望の長さを有する。これらの各52ビット鍵K1、K2、...、は、生成されるべき暗号フィールド306の水平走査線（走査線305等）と関連付けられる。

30

【0078】

暗号フィールド306の任意の特定走査線（走査線305等）を生成するために、第2のRC4暗号生成器は、その特定走査線と関連付けられた鍵を使用して初期化される。従って、例えば、302で示される鍵K4は、走査線305に関して使用される。連続多値ビット「S」値は、第2のRC4暗号生成器から生成される。連続多値ビット「S」値は、その走査線上の以前に生成された「S」値の右の（S41等における）「S」値及び次の左の（S42等における）「S」値と交互に関連付けられる。各多値ビット「S」値は、暗号フィールド306内に値（S42等）を形成する。マスタ暗号ストリームとの同期を維持するために、信号供給源102及び信号供給源103と関連付けられた2つの暗号フィールド306及び暗号フィールド306'（後者は不図示）は、同時に生成される。

40

【0079】

スパイン308は、暗号フィールド306及び暗号フィールド306'を形成するために使用される。しかしながら、スパイン308は、暗号フィールド自体の一部を形成するものではない。暗号フィールド306及び暗号フィールド306'は、「S」値のみにより構成される。スパイン308（すなわち、「K」値）は、52ビット鍵で構成される。「S」値（暗号フィールドを形成する）は、本例において2ビット値である。

【0080】

暗号フィールドを発生させる他の方法は、可能である。符号307は、別の暗号フィールドを示す。別の暗号フィールドにおいて、符号303は、ラストグリッド304を埋め

50

込む別の渦巻ベース構成の開始を指示する。この構成 307 は、単一のストリーム暗号エンジンのみを必要とする点で有用であるが、いくつかの実現例においては特殊バッファリングを必要とする。

【0081】

暗号フィールド 306 及び暗号フィールド 307 の絶対サイズは、必ずしもソース文書 101 の大きさと同一ではないが、暗号フィールドの S 値は、ソース画像 101 の画素と「合同」であるとする。この合同において、ソース画像 101 の各画素と、暗号信号供給源 102 及び暗号信号供給源 103 により出力された暗号フィールドの対応する S 値との間に固有の 1 : 1 対応が成立するようにする。改竄防止方法を行うために、妥当性検証サブシステム 127 により行われた位置決めは、この合同を再確立する。

10

【0082】

図 6 は、図 5 の暗号フィールドのうちの 1 つを生成する方法ステップのフローチャートとして、プロセス 2500 を示す。プロセス 2500 は、図 2 に関して説明されたように、鍵生成モジュール 134 及び暗号信号供給源 A（すなわち、暗号信号供給源 102）により実現される。鍵生成モジュール 134 へ戻ると、図 6 の第 1 のステップ 2508 では、ソルト値が生成される。ステップ 2508 の破線アウトラインで示すように、ステップ 2508 は、任意のステップである。その後、ステップ 2501 では、ステップ 2508 のオプションが選択された場合、ソルト値を使用して 52 ビット秘密鍵を生成する。続くステップ 2502 では、RC4 暗号ストリームを生成する。次のステップ 2503 では、矢印 135 で示すように、連続する 52 ビットバイトの暗号ストリームを、暗号信号供給源 102 等の連続する暗号信号供給源に割り当てる。矢印 136 は、交互の 52 ビットバイトが信号供給源 103 へ指向されることを示す。

20

【0083】

信号供給源 102 において、第 1 のプロセスステップ 2504 では、図 5 に関して説明されたように、鍵生成モジュール 134 から受け取られた連続する 52 ビットバイトを、暗号フィールドのスパイン位置に割り当てる。その後、ステップ 2505 では、スパイン位置ごとに、関連走査線に対して RC4 ストリーム暗号を生成する。次のステップ 2506 では、走査線ストリーム暗号ごとに、連続する 2 ビットバイトを走査線上の連続する画素位置に割り当てる。その後、ステップ 2507 では、2 ビット暗号フィールド値が出力される。

30

【0084】

＜オリジナル画像と暗号フィールドとの結合＞

尚、図 2 に戻り、特に、選択モジュール 104 の動作に関して、選択動作（図 3 の対応するステップ 2302、ステップ 2303 及びステップ 2305 を参照）として、まず、暗号供給源 102 及び暗号供給源 103 からの 2 つの暗号フィールド、並びにソース画像 101 からのオリジナル画像は、暗号フィールド及びオリジナル画像の公称中心位置上に位置決めされる。選択段階（図 3 のプロセス 2312 に対応）において、位置決め位置の選択は、公称である。しかしながら、選択された位置決め位置は、不正顕示機能付文書 105 内へロックされ且つ符号化された状態となり、妥当性検証サブシステム 127 による回復処理（図 4 を参照）における位置決めのベースを形成する。

40

【0085】

好適な構成において、暗号信号供給源 102 及び暗号信号供給源 103（図 2 を参照）により生成された 2 つの各 2 次元暗号フィールド（暗号フィールド 306（図 5 を参照）等）内の各値は、2 ビット精度を有する。そのため、説明される例において、ソース情報 117 は、1 ビット精度を有する 2 値レベルである。一方、不正顕示機能付文書 105 は、各々が 2 ビット精度を有する 2 組の 4 値レベルを有する。2 組の 4 値レベルは、各ソース文書画素の対応する印刷形態に対して合計 8 つの可能な状態を与える。暗号信号（図 2 の暗号信号 115 及び暗号信号 116 等）が各入力画素（図 2 のソース画像 101 からの信号 117 において）に関するもので、各暗号信号に対する状態（すなわち、この例では振幅解像度）の数は、変化する。好適な構成は、4 つの状態（そのため、2 ビットである）

50

を使用するが、2つ以上のいずれの状態の数であっても効果的である。

【0086】

偽造者が、画素値を黒から白へ、又は白から黒へ変化させる場合、暗号値115及び暗号値116に対して使用する状態の数の選択は、不正顕示機能付文書105上の印刷画素の副信号の正しい値を「推測」する偽造者の能力に影響を及ぼす。本例における2ビットの選択が、偽造者が75%の時間を誤って推測する可能性があることを意味するので、その選択は、画素集合が小さい場合においても、偽造の強力な指示を提供できる。

【0087】

多値レベル（すなわち、1画素当たり2ビット以上を有する）不正顕示機能付画像組み合わせ信号122（図2を参照）は、関連暗号信号供給源102及び関連暗号信号供給源103により出力された対応する暗号フィールドからの関連暗号信号値115又は関連暗号信号値116を使用して、それぞれのルックアップテーブル130及びルックアップテーブル131を索引することにより、オリジナルのソース画像101の画素ごとに生成される。好適な構成において、不正顕示機能付文書105を印刷するために使用された出力装置は、プリンタ2215である。本例では、プリンタ2215は、カラープリンタである。不正顕示機能付文書105上の多値レベル画像は、本実施例において、24ビットRGB画像である。

【0088】

図7は、暗号信号供給源102及び暗号信号供給源103、並びに信号供給源102及び信号供給源103のそれぞれのルックアップテーブル130及びルックアップテーブル131（図2を参照）に関連して、選択モジュール104が動作する方法の特定例406を示す図である。プロセス406では、ソース情報117内の2値レベル画素値を、変調された合成暗号信号118（図2を参照）内の多値レベル画素値に変換する。矢印2315（図3を参照）は、ステップ401へリードする。ステップ401では、オリジナルのソース画像101の画素を考慮する。考慮中の画素が黒である場合、プロセス406は、矢印「Yes」に従って、ステップ402へ進む。ステップ402では、B（黒）暗号フィールドより、考慮中の画素と関連付けられた暗号フィールド内の位置から2ビット値を選択する。しかしながら、画素が白である場合、プロセス406は、矢印「No」に従って、ステップ403へ進む。ステップ403では、W（白）暗号フィールドより、考慮中の画素と関連付けられた位置から2ビット値を選択する。ステップ401～ステップ403は、それぞれの暗号供給源102（図2を参照）からの暗号信号115と、暗号供給源103（図2を参照）からの暗号信号116との間の選択を行う選択モジュール104により実行される。

【0089】

考慮中の画素が黒である場合、ステップ402において暗号フィールド「B」から選択された2ビット暗号値を使用して、差分ルックアップテーブル404を索引する。ルックアップテーブル404内の画素は、全て、黒又は何らかの暗色のいずれかである。好適な構成において、この画素には、黒並びに完全な純色の赤、緑及び青が使用される。考慮中の画素が白である場合、ステップ403において暗号フィールド「W」から選択された暗号値を使用して、差分ルックアップテーブル405を索引する。ルックアップテーブル405内の画素は、全て、白又は何らかの明色のいずれかである。好適な構成において、この画素には、白、シアン、マゼンダ及びイエロが使用される。これらの色が使用されるのは、人間の目又は自動ビデオ抽出技法の使用のいずれによっても、視覚的な相互識別が容易であるためである。この色選択の結果、ロバストな妥当性検証システム127が得られる。しかしながら、この色選択では、他の色が使用されてもよい。ルックアップテーブル404及びルックアップテーブル405は、図2のルックアップテーブル130及びルックアップテーブル131の特定例である。

【0090】

例えば、ステップ402において、B暗号フィールドから暗号値「10」が発生した場合、この値「10」は、「10」における（RGB）ルックアップテーブル404を索引

10

20

30

40

50

する。これにより、赤（R）チャンネルがFF（16進法において）であり、緑（G）チャンネルが00であり、且つ青（B）チャンネルが00である出力が得られる。この出力は、赤の出力に等しい。

【0091】

ステップ401～ステップ405では、ステップ2311（図3を参照）において格納された多値レベル画素値を発生させる。その後、プロセス406は、矢印2314（図3を参照）に従って、処理を進める。

【0092】

また、非色ベース方式も使用できる。例えば、完全なグレースケール方式において、不正顕示機能付文書に対して印刷及び走査が行われた後、大多数の場合に異なる階調間を識別可能であれば、この異なる階調を使用できる。別の使用可能な方法は、各ソース文書画素に対応するセル内の2値レベル（通常、黒及び白）装置画素の1組の小パターンである。小パターンのうちの1つは、暗号フィールドの各状態を示す。

10

【0093】

図8は、2値レベル画像701（図2のソース画像101と関連付けられた2値レベル画像等）の多値レベル画像705（不正顕示機能付文書105と関連付けられた多値レベル画像等）への変換の描画表現を示す図である。オリジナル画像701（図2のソース画像101の特定例）は、画素単位ベースで選択モジュール704（図2の選択モジュール104の特定例）を制御するために使用される。

【0094】

20

選択モジュール704は、画像701からの画素値706により制御された1画素ベースで、2つの暗号フィールド由来カラーグリッド702及び暗号フィールド由来カラーグリッド703の色オプションから選択する。カラーグリッドは、次のようにして生成される。「黒」色グリッド702内の画素位置707に対する画素値は、「黒」暗号フィールド（不図示）内の上記の画素位置707に対する対応する暗号値を使用して判定される。黒暗号フィールドは、対応する暗号供給源102により生成された暗号フィールド115の特定例である。黒暗号フィールドからの上記の暗号値は、図7のテーブル404と同様に、対応するルックアップテーブル（不図示）内に多値レベル色値を索引するために使用される。「白」色グリッド703内の画素位置707'に対する画素値は、「白」暗号フィールド（不図示）内の上記の画素位置に対する対応する暗号値を使用して判定される。これにより、図7のテーブル405と同様に、対応するルックアップテーブル（不図示）内に多値レベル色値を索引する。

30

【0095】

オリジナル画像701内の画素位置708における画素値が白であるため、選択モジュール704は、不正顕示機能付画像705内の画素位置708'において挿入されるべきカラーグリッド703内の画素位置707'の色値を選択する。

【0096】

複数の画素709は、改竄検知に関して図19に関連させて説明される。

【0097】

<粗位置決めマーク>

40

図9は、粗位置決めに使用された2次元線形波形関数の2値レベル表現を示す図である。図2の妥当性検証サブシステム127において使用された精位置決めモジュール106により行われた精位置決めを支援するために、図9の波形関数を使用した粗位置決めマークは、粗位置決め提供元111及び組み合わせモジュール114により合成暗号信号118内に組み込まれる。これにより、不正顕示機能付文書105（図2を参照）上に印刷された多値レベル画像を形成する。好適な構成において、図9に示す関数を使用した微弱な粗位置決めパターン画像は、組み合わせモジュール114により、変調された合成暗号信号118（図2を参照）と混合される。この画像混合は、変調された合成暗号信号118内の各画素値の1つ以上のカラーチャンネルに適切な値を加算することにより、あるいは、カラーチャンネルから適切な値を減算することにより、行われる。加算量は、非常に小さい

50

ため、妥当性検証処理 1 2 7 において閾化モジュール 1 0 7 により行われる複数の色間の識別に影響を与えない。位置決めパターンは、図 9 に示す複数の 1 次元スケール不変関数の特定構成から形成される。1 次元スケール不変関数は、フーリエ法を使用して効率的に検出できる。選択された 1 次元スケール不変関数の特定構成は、関数の対称軸が、アフィン変換下において不変である一定長さ比を有する線セグメントを規定する点で交差するように選択される。アフィン変換は、図 1 2 に関して、特に、ステップ 1 7 9 0 に関して、更に説明される。

【0098】

位置決めパターン画像は、図 9 に示すように、4 つの 1 次元スケール不変パターンの重ね合わせである。1 次元スケール不変パターンは、横方向に延在して図 2 のソース画像 1 0 1 を被覆する。単一の 1 次元スケール不変パターンは、数学的に次式により表される。

$$f(x) = \cos(\gamma \log|x - x_0|) \quad (1)$$

ここで、 γ は、パターン振動速度を特定する定数であり（パターン振動の高速化と共に、距離 5 0 1 は短縮される）、 x_0 は、パターンに対する対称線 5 0 2 を特定する。

【0099】

図 1 0 は、図 9 に示した線形波形関数のグラフィック表現を示す図である。尚、横方向に延在した 1 次元スケール不変パターンは、2 つのパラメータ、すなわち、パターン半径 r 及びパターン角度 α により特定される。このようなパターンの 2 次元関数形態（図 9 に示す）は、数学的に次式により表される。

$$f(x, y) = \cos(\gamma \log|x \cos \alpha + y \sin \alpha - r|) \quad (2)$$

ここで、 r （図 9 の半径 5 0 3 を参照）は、パターン半径であり、 α （図 9 の角度 5 0 4 を参照）は、パターン角度である。

【0100】

所望の位置決めパターン（図 2 の信号 1 2 8 において）を形成するために重ね合わせられた 4 つの 1 次元スケール不変パターンは、1 次元スケール不変パターンに、相互に関連した特定の空間的構成（図 1 1 を参照）を与える r パラメータ値及び α パラメータ値を有する。特定の空間的構成は、位置決めパターン 1 2 8 が組み込まれた不正顕示機能付文書 1 0 5 の位置決めを判定する際に好都合である。この空間的構成は、図 1 1 において表現される。

【0101】

図 1 1 は、配列検出の際に使用された複数の線形波形関数に基づく対称軸の構成を示す図である。図 1 4 に関して更に説明されるように、これらの対称軸を確立するパラメータの組は、特に、対称軸が、アフィン変換下において不変である一定長さ比（比 1 1 0 1 : 1 1 0 2 により例証される）を有する線セグメントを規定するように選択される。

【0102】

好適な構成において、オリジナルのソース画像 1 0 1 は、幅（ x ）寸法及び高さ（ y ）寸法の両方において、少なくとも 1, 0 2 4 画素の最小画素寸法を有する。しかしながら、最小画素寸法は、いずれか又は両方の寸法において、より大きくてもよい。この最小画素寸法は、以下の式において、 N_{min} とする。一般に、ソース画像 1 0 1 は、幅 N 画素及び高さ M 画素の寸法を有する。この場合、 $M \geq N_{min}$ 且つ $N \geq N_{min}$ である。位置決めマーク 1 2 8 を形成するために使用された 4 通りのパターンに対するパターンパラメータ r 値及びパターンパラメータ α 値は、次式により表される。

$$\begin{aligned}
 r_1 &= P_d, \alpha_1 = \frac{9}{16} 2\pi \\
 r_2 &= P_d, \alpha_2 = \frac{13}{16} 2\pi \\
 r_3 &= P_d, \alpha_3 = \frac{3}{16} 2\pi \\
 r_4 &= \frac{P_d}{\sqrt{2}}, \alpha_4 = \frac{15}{16} 2\pi
 \end{aligned}
 \tag{3}$$

10

ここで、

$$P_d = N_{min} / (2 + \sqrt{2}) \tag{4}$$

である。

【 0 1 0 3 】

また、ナイキスト半径 R_{NYQ} も、特定される。ナイキスト半径は、パターン対称軸に基づく画素数である。この場合、パターン周波数は、画像のナイキスト周波数に等しい。対称軸から第 1 の可視波形までの距離は、ナイキスト周波数を表す。

20

【 0 1 0 4 】

j 番目のパターンに対して、パラメータ r_j 及びパラメータ α_j を使用すると、中間量 D_j 、 X_j 、 Y_j 及び R_j は、

$$\begin{aligned}
 D_j &= \cos\left(\frac{\pi}{2} \text{frac}\left(4\left(\alpha_j + \frac{1}{8}\right)\right) - \frac{\pi}{4}\right) \\
 X_j &= \left\lfloor \frac{N}{2} \right\rfloor + r_j \cos \alpha_j \\
 Y_j &= \left\lfloor \frac{N}{2} \right\rfloor + r_j \sin \alpha_j \\
 R_j &= -(X_j \cos \alpha_j + Y_j \sin \alpha_j) / D_j
 \end{aligned}
 \tag{5}$$

30

のように事前に算出される。

【 0 1 0 5 】

オフセット (x, y) における画素に対する j 番目のパターンの「影響」 $P_j(x, y)$ は、

$$\begin{aligned}
 &\text{if } (|R_j| > R_{NYQ}) \\
 &\quad P_j(x, y) = \cos(\pi R_{NYQ} \log(|R_j|)) \\
 &\text{else} \\
 &\quad P_j(x, y) = 0
 \end{aligned}
 \tag{6}$$

40

により与えられる。

【 0 1 0 6 】

改竄防止方法を効果的に実行可能とした状態で、ソース画像 1 0 1 が受け入れ不可能な程度まで変形されることを防止するために、パターン影響を使用して、位置決め信号 1 2 8 及びソルト信号 1 2 9 を適切にスケーリングする。

【 0 1 0 7 】

< ディクショナリ攻撃防止のためのソルト値加算 >

50

図2へ戻ると、同一の暗号鍵（図6のステップ2501により生成された鍵等）が2ページ以上の不正隠示機能付文書105を生成するために使用された場合、暗号信号供給源102及び暗号信号供給源103により生成された暗号フィールド115及び暗号フィールド116は、文書105の異なるページから明領域及び暗領域を採取することにより潜在的に発見できる。この可能性を防止するために、好適な構成では、ソルト生成器112により提供されるソルト値を採用する。ソルトは、ディクショナリ攻撃を防止するための暗号法の分野において知られる技法である。ソルト技法は、このように、不正隠示機能付文書105の異なる2ページ上の暗号ストリームの類似性に基づいた攻撃を防止する場合においても使用できる。

【0108】

好適な構成において、例えば、図6のステップ2501により生成された鍵は、不正隠示機能付文書105の生成器（すなわち、作成サブシステム126のユーザ）及び不正隠示機能付文書105の妥当性検証者（すなわち、妥当性検証サブシステム127のユーザ）によく知られていることが望ましい。しかしながら、不正隠示機能付文書105の2ページに対する暗号ストリームの類似性に基づいた攻撃を防止するために、不正隠示機能付文書105の各ページに対して異なる鍵を使用する必要がある。これらの両方の目的を達成するために、好適な実施の形態では、鍵を2つの要素で形成する。例えば、40ビットの長さの鍵の第1の要素は、作成サブシステム126及び妥当性検証サブシステム127の両方によく知られる。この第1の要素は、不正隠示機能付文書105の各ページに対して同一である。鍵の残る要素、すなわち、この例では12ビット長さのソルトは、不正隠示機能付文書105の各ページに対して異なる。このソルトは、不正隠示機能付文書105の各ページに対して暗号的に（すなわち、「乱」数を効果的に使用して）生成される。ソルト値は、暗号化されない状態で関連ページ内に埋め込まれる。図6のステップ2501により生成された実際の52ビット鍵は、固定40ビットと12ビットソルトとの接続結果である。この実際の52ビット鍵は、作成サブシステム126の各信号115及び信号116、並びに妥当性検証サブシステム127の各信号115'及び信号116'に対して使用されたものである。

【0109】

暗号的に（ランダムに）生成された12ソルトビットは、2つの6ビット部分 S_a 及び6ビット部分 S_r に分割される。それぞれ、6ビット部分 S_a は、図9に示すスケール不変パターンと類似する第5のスケール不変パターンの角度を表し、6ビット部分 S_r は、図11に示すスケール不変パターンと類似する第5のスケール不変パターンの位置を表す。 S_a 及び S_r の両方には、64個の異なる値を仮定できる。特定角度及び特定位置を有するこの第5のスケール不変パターンが、信号118内に埋め込まれることにより、作成サブシステム126の不正隠示機能付文書105は、形成される。妥当性検証サブシステム127は、この第5のスケール不変パターンを抽出することにより、パターンの関連角度及び関連位置を判定する。この角度及び位置は、2つの6ビットソルト値部分を確立する。第5のスケール不変パターンは、特に、他の4つのパターンに対して説明した方法と同様の方法で埋め込まれるが、振動定数 γ が異なる場合を除く。

$if(|R_s| > R_{N\gamma Q})$

$$P_5(x, y) = \cos\left(\frac{\pi}{2} R_{N\gamma Q} \log(|R_s|)\right) \quad (7)$$

else

$$P_5(x, y) = 0$$

ここで、パラメータは、

10

20

30

40

$$r_s = s_r P_d / 64 \quad (8)$$

$$\alpha_s = 2s_a \pi / 64$$

により計算される。

【0110】

第5のスケール不変パターンの異なる振動定数の選択は、ソルト値と粗位置決めパターンとの間の検知空間におけるある程度の分離を引き起こす。干渉は、粗位置決めマークにおいて使用された角度に近似する特定角度を無効にすることにより、更に低減させることが可能である。

10

【0111】

＜粗位置決めとソルトパターンとの組み合わせ＞

図2の組み合わせモジュール114の機能へ戻ると、位置決めパターン及びソルトパターンにより引き起こされたネット影響は、次式の合計

$$P(x, y) = \sum_{i=1}^s P_i(x, y).$$

により判定される。

20

【0112】

この値は、-5から5までの範囲で変化する。次に、この値は、-15から15の範囲までスケールアップされ、組み合わせモジュール114により、変調された合成暗号信号118の各チャンネルに直接加算される。変調された合成暗号信号118は、多値レベルRGB画像であり、0...255の範囲まで結果をクランピングする。このスケーリング演算は、文書105内のオリジナルのソース情報101を過度に摂動させない状態で、粗位置決めマーク及びソルト値を文書105から抽出することを可能とする。

【0113】

＜マーキング処理の結果＞

図2の信号122における最終の多値レベル画像は、カラープリンタ2215を使用して不正顕示機能付文書105上に印刷される。カラープリンタ2215は、例えば、Canon I R C 3200電子写真複合機又はCanon i950熱インクジェットプリンタであってもよい。プリンタ解像度に対する200DPI画像のスケーリングは、単純な画素複製を使用して実現されることが好ましい。例えば、Canon I P C 3200は、600DPIの装置解像度を有する。このプリンタでは、最終の多値レベル画像の各200DPI画素は、Canon I P C 3200装置画素の3×3グループ内に複製される。

30

【0114】

組み合わせモジュール114により行われたマーキング処理の結果は、オリジナル2値レベルデジタル画像101の黒値及び白値に対応する明領域及び暗領域の効果により、人間が読み取り可能な印刷文書105である。このマーキングの例は、図8に示される。

40

【0115】

尚、図8へ戻ると、それぞれ、画素位置707'等の明領域及び画素位置707等の暗領域は、各々が副成分を含む。それぞれの副成分は、画素位置707'における単方向断面線、及び画素位置707における双方向断面線により示される。これらの副成分を生成する鍵が非存在中の副成分は、有用な情報を含まず、この副成分の偽造は、困難である。しかしながら、2つの副成分の存在間に正確な相関性は存在し、各画素の全体の暗度及び明度は、それぞれ、各画素における主成分を表現する。それぞれの主成分及び副成分の知識を有する検査者は、この相関性の存在又は不足を認証できる。偽造者が関連副成分を相応に変化させることはできないため、偽造者は、画素（すなわち、主成分に対する）を明

50

領域から暗領域へ（又は暗領域から明領域へ）適切に変化させることができる可能性は少ない。偽造者が、既定の画素位置における別の主成分に対する副成分の値を知らないため、偽造者は、相関性を維持することができない。

【0116】

<認証処理>

図2の妥当性検証サブシステム127へ戻ると、まず、カラスキャナ2218（図1を参照）により、認証されるべき不正顕示機能付文書105を走査することにより、24ビットRGB不正顕示信号120を発生させる。スキャナ2218の走査解像度は、オリジナル画像101の解像度より高いか、又は画像101の解像度に等しいことが要求される。好適な構成において、200DPIオリジナル画像101（図2を参照）の全体にわたり大きなマージンを提供する600DPIスキャナ2218は、使用される。

10

【0117】

<粗位置決め処理の概要>

図2の粗位置決め／ソルト回復モジュール113の動作へ戻ると、粗位置決めパターン（本実施例において、組み合わせモジュール114により、わずかに不正顕示機能付文書105の印刷前の信号118に加算された4つの位置決めマークを有する）に検出及び解析を施すことにより、走査文書120の方向を暗号フィールドと関連付けるアフィン変換を発生させる。

【0118】

図12は、図2の粗位置決め／ソルト回復モジュール113により行われた図4の粗位置決め処理2419を示す図である。走査不正顕示信号120の輝度チャネルの形態の走査文書は、ステップ1710において、まず、幅及び高さの最小値が256画素から511画素の範囲内になるように調整されるまで、生成された画像が、連続半減処理により、リサイズされる。半減処理は、信号120の形態の画像を低域フィルタで畳み込み、且つ畳み込みの結果を間引くことにより行われてもよい。

20

【0119】

次に、生成されたりサイズ画像は、ステップ1720において、2次元高速フーリエ変換（FFT）が施される。この結果は、ステップ1730において、準極周波数空間中に再サンプリングされる。ステップ1730では、バイキュービック補間を使用してFFTを極グリッド上に再サンプリングすることにより、ステップ11720から2次元FFTの極変換を直接使用できる。この方法は、演算が単純な一方で、検知に悪影響を及ぼす可能性のあるアーテファクトを発生させる。ステップ1730において使用された好適な準極方法は、図13に関して説明される。

30

【0120】

ステップ1720においてFFTを計算する前に、画像縁部に近接する画像値（強度）は、まず、減衰されることが好ましい。この減衰は、画像値が、画像縁部に向かうと共に徐々に且つスムーズにゼロにフェードするように行われる。ステップ1730では、水平列が、ステップ1720で得られた2次元FFTにおける半径スライスに対応する複素画像を作成する。角度スペーシング及び半径スケールリングは、一定である必要はない。

【0121】

ステップ1750において、ステップ1740により与えられた1次元基底関数の1次元フーリエ変換は、実行される。ステップ1740により与えられた基底関数は、数学的に次式により表される。

40

$$f(x) = \cos(\gamma \log|x - x_0|) + i \sin(\gamma \log|x - x_0|) \quad (9)$$

この式は、式（1）の複素バージョンである。そのため、 γ は、パターン振動速度を特定する定数であり、 x_0 は、パターンに対する対称点を特定する。あるいは、ステップ1740の基底関数は、数学的に変換できる。すなわち、式（9）のフーリエ変換の解析解導出後、この解を使用することにより、フーリエ変換1750を直接発生させることができる

50

。

【0122】

次に、ステップ1750から得られた基底関数の変換は、ステップ1760において、画素単位で、全ての角度値に対する水平列（2次元FFTの半径線を表現する）に沿ったステップ1730の出力値の複素共役で乗算される。その後、生成された複素画素値は、ステップ1760により、複素画素値が大きくとも単位大きさを有するように基準化される。次に、ステップ1770では、水平列に沿ったステップ1760の出力の1次元逆高速フーリエ変換（IFFT）を判定する。

【0123】

ステップ1770の結果、図2の走査文書信号120内の1次元基底関数（すなわち、4つの位置決めマーク）の方向及びスケールに対応する画像の大きさにピークを有する複素画像が得られる。これらのピークは、ピーク検出処理1780（図14に関してより詳細に説明される）を使用して検出される。最後に、ステップ1790において、ステップ1780で検出されたピークの位置を使用して、図2の信号120における走査文書を、図2の暗号フィールド115'及び暗号フィールド116'のデジタル形態と関連付けるアフィンパラメータを判定する。

【0124】

ステップ1790において、交点のアフィン変換に最小二乗適合度を与える4つのピークの結合に対応するアフィン変換は、図2の信号120における走査文書の方向を図2の暗号フィールド115'及び暗号フィールド116'の方向と関連付けるアフィン変換として選択される。最小二乗適合度の詳細は、後述される。

【0125】

次に、図4のステップ2402において、アフィン変換が使用され、バイキュービック補間を使用して走査文書が変換される。走査文書の変換により、粗位置決め走査文書を表す信号121（図2を参照）が形成される。この文書は、本例において、約600DPIの解像度を有する。

【0126】

＜準極マッピング処理の詳細＞

前述の構成において、粗位置決めに対する不変パターンマッチングを行う好適な方法では、チャープZ変換を使用してステップ1720により行われるフーリエ変換の準極変換（図12のステップ1730を参照）を提供する。チャープZ変換は、信号のフーリエ変換のスケールリング部分を計算するための方法である。

【0127】

図13は、図12のステップ1730をより詳細に示す図である。図13は、フーリエ変換の準極マッピングを算出するための準極変換を行うプロセスである。ステップ1810において、図12のステップ1720により出力された大きさ（X，Y）を有するリサイズ画像1801は、2つのコピーI1（符号1802により示される）及びコピーI2（符号1803により示される）として複製される。ステップ1820において、第1のコピーI1を、幅 $W = 2 * MAX(X, Y)$ までX方向にゼロでパディングすることにより、大きさ（W，Y）の画像1804を得る。パディングは、コピーI1の列オフセット

$\lfloor X/2 \rfloor$

が、パッド画像1804の列オフセット

$\lfloor W/2 \rfloor$

に対応するように行われる。

【0128】

ステップ1830において、第2のコピーI2を、高さWまでY方向にゼロでパディングすることにより、画像1805を形成する。ステップ1840において、画像1805を90°回転させることにより、大きさ（W，X）の画像1806が得られる。パディン

グは、コピー 12 の行オフセット

$\lfloor Y/2 \rfloor$

が、パッド画像 1806 の行オフセット

$\lfloor W/2 \rfloor$

に対応するように行われる。

【0129】

ステップ 1850 及びステップ 1860 において、画像 1804 及び画像 1806 を、
各行の 1 次元フーリエ変換計算により変換することにより、それぞれ、画像 1804 の変
換画像 1807 及び画像 1806 の変換画像 1808 を形成する。 10

【0130】

ステップ 1870 及びステップ 1880 において、画像 1807 及び画像 1808 を、
各列の個別のチャープ Z 変換計算により変換することにより、それぞれ、画像 1807 の
変換画像 1809 及び画像 1808 の変換画像 1811 を形成する。

【0131】

ステップ 1870 及びステップ 1880 により行われた各チャープ変換を行うことによ
り、それぞれのステップ 1870 及びステップ 1880 の列の範囲内の位置

$\lfloor Y/2 \rfloor$ 及び $\lfloor X/2 \rfloor$

20

における各列の中心位置を保存する。

【0132】

ステップ 1870 及びステップ 1880 における各列 に対するスケーリング係数は、

$$m_z = \lfloor W/2 \rfloor / (z - \lfloor W/2 \rfloor) \quad (10)$$

であり、各スケール係数 m_z は、垂直フリップに対応する

$$z < \lfloor W/2 \rfloor,$$

30

である場合、負の数となる。また、

$$z = \lfloor W/2 \rfloor,$$

である場合、スケーリング係数は規定されない。この場合、中心画素位置は、列全体にわ
たり複製される。

【0133】

不正顕示機能付文書 105 からの正方形画像を仮定すると、変換画像 1809 及び変換
画像 1811 は、リサイズされ、ウィンドウ化され、且つ変換画像 1809 及び変換画像
1811 を有する入力画像のフーリエ変換の準極変換を表現する。変換画像 1809 は、
[$-\pi/4$. . $\pi/4$] の範囲内の角度を有し、変換画像 1811 は、[$\pi/4$. . 3
 $\pi/4$] の範囲内の角度を有する。不正顕示機能付文書 105 からの画像が矩形である場
合、角度の範囲は、[$-\text{atan2}(Y, X)$. . $\text{atan2}(Y, X)$] 及び [$\text{atan2}(Y, X)$. . $\pi - \text{atan2}(Y, X)$] から変化する。準極変換の各行が、正半
径及び負半径を含むため、各行は、全て [0 . . 2π] ラジアン の範囲内の角度を有する
。 40

【0134】

ステップ 1890 において、画像 1812 の上部に画像 1809 の画素を複製し、且つ
画像 1812 の下部に画像 1811 の画素を複製することにより、2 つの入力画像 180
9 及び入力画像 1811 を結合して、(W, Y+X) 寸法の画像 1812 を形成する。 50

【0135】

＜ピーク検出処理の詳細＞

図14は、図12のピーク検出処理1780の一例を示す流れ図である。図12のステップ1770の結果、図2の走査文書信号120内の1次元基底関数（すなわち、4つの位置決めマーク）の方向及びスケールに対応する画像の大きさにピークを有する複素画像は、得られる。そのため、ピーク検出ステップ1780への入力は、上記の複素画像である相関画像1610で示される。複素画像において、P個の最大ピーク（好適な構成において、Pは64である）の位置の決定が所望される。換言すれば、P個の最大ピークは、相関画像の大きさのP個の最大局所極大である。

【0136】

ピークは、多数のピークが相互に近接集合したノイズのある領域において発生する。一定の閾半径内の最大ピークのみを考慮することにより、10個の画素のデフォルトの閾半径が選択されることが好ましい。ステップ1620において、相関画像1610は、走査され、画素値の大きさが画素値の全ての隣接値より大きい点のリストが、構築される。次のステップ1630において、このピークのリストは、画素値の大きさ順にソートされる。次のステップ1640において、ソートリストの各ピークは、大きさの降順に考慮され、半径距離閾値内のリスト上のソート後の任意のピークは、ピークリストから排除される。次のステップ1650において、ステップ1640で発生したピークのソートリストは、切り捨てられ、長さリストPとなる。

【0137】

上記の切り捨てリストは、高精度で決定可能なP個のピークの位置を含む。ステップ1660において、ループ入力により、同様にP個の各ピークを取り入れる。次のステップ1670において、考慮中のピークの位置にセンタリングされた27画素単位の領域は、FFTに入力され、その後、係数27により、ピークに焦点を合わせてズームするチャープZ変換に入力される。チャープZ変換は、任意のスペーシングでの離散フーリエ変換（DFT又は逆DFT）の計算を可能にする。チャープZ変換は、例えば、DFTを離散周期的畳み込みとして表現することにより行われる。このような畳み込みが、複数のFFTを使用して実現可能であるため、全体の計算には、FFT速度を利用できる。スペーシングの適切な選択により、チャープZ変換は、例えば、DFTを選択領域全体にわたり精密にサンプリングする（すなわち、ズームする）ことが可能な補間技法となる。

【0138】

最大の大きさを有する27画素単位の画像は、次のステップ1680において判定され、このピークのサブ画素位置は、双放物適合を使用して判定される。このサブ画素精度ピーク位置は、ピーク検出ステップ1780の出力である。

【0139】

＜粗位置決めを判定するための検出ピークの使用＞

その後、図14のステップ1780（図12も参照）から出力されたピークは、図12のステップ1790により、4つのピークの各可能な結合を順次選択し、且つ次の解析を行うことにより、更に処理される。これにより、4つのピークの結合のうちのこの解析の条件を最も満足する経路を保持する。

【0140】

各ピーク s_i 及びピーク β_i の半径及び角度は、図13の準極マップ1812内の各ピークのオフセット（ x , y ）から計算される。

【0141】

1813の準極座標（ x , y ）から極座標（ s , β ）へのこの変換は、次式により計算される。

【0142】

入力画像1812は、大きさ（ W , $X+Y$ ）画素の画像であり、次のパラメータ

$$\begin{aligned} Y_2 &= \lfloor Y/2 \rfloor \\ X_2 &= \lfloor X/2 \rfloor \\ W_2 &= \lfloor W/2 \rfloor \end{aligned} \quad (11)$$

が設定される。

【 0 1 4 3 】

もし、 $y < Y$ である場合は、

$$\begin{aligned} y_s &= y - Y_2 \\ x_s &= x - W_2 \\ \beta &= \pi/2 - \tan^{-1} \frac{Y_2}{y_s} \\ s &= \frac{x_s Y_2}{\sqrt{Y_2^2 + y_s^2}} \end{aligned} \quad (12)$$

あるいは、 $y \geq Y$ である場合は、

$$\begin{aligned} y_s &= x - W_2 \\ x_s &= y - X_2 \\ \beta &= \pi - \tan^{-1} \frac{X_2}{x_s} \\ s &= \frac{y_s X_2}{\sqrt{X_2^2 + x_s^2}} \end{aligned} \quad (13)$$

ここで、 Y_2 、 X_2 、 W_2 、 y_s 及び x_s は、中間値である。

【 0 1 4 4 】

線形変換パラメータ (a_{11} 、 a_{12} 、 a_{21} 、 a_{22} 、 x_0 、 y_0) により説明されるアフィン変換は、4つの選択ピークから判定される。線形変換パラメータは、1次元基底関数のパラメータ r_i 及びパラメータ α_i の最初の組 (式 (3) からの組であり、便宜上式 (14) で再生される) を、パラメータ s_i 及びパラメータ β_i にマッピングする。位置決めマークが埋め込まれた不正顕示機能付文書 105 において使用された1次元基底関数パラメータの予め規定された組は、式 (3) から次式により再生される。

$$\begin{aligned} r_1 &= P_d, \alpha_1 = \frac{9}{16} 2\pi \\ r_2 &= P_d, \alpha_2 = \frac{13}{16} 2\pi \\ r_3 &= P_d, \alpha_3 = \frac{3}{16} 2\pi \\ r_4 &= \frac{P_d}{\sqrt{2}}, \alpha_4 = \frac{15}{16} 2\pi \end{aligned} \quad (14)$$

この場合、

$$P_d = N/(2 + \sqrt{2}) \quad (15)$$

である。ここで、 $N = 1024$ である。

【 0 1 4 5 】

10

20

30

40

50

このパラメータの組は、パラメータの組が表現する1次元基底関数の対称軸が、アフィン変換下において不変である一定長さ比を有する線セグメントを規定する点で交差するように、特定の方法で選択されている。

【0146】

4つのピークの結合が満足すべき第1の条件は、4つのピークが、正確な長さ比（例えば、図11の1101：1102を参照）を有する線セグメントの組を生成することである。4つのピークが、正しい長さ比を有する線セグメントの組を生成しなかった場合、ピーク結合が、アフィン変換により変形された4つのオリジナルベースパターンに対応せず、この結合は、破棄される。

【0147】

前述したように、ピークの半径座標 s_i 及び角度座標 β_i は、不正顕示機能付文書内に埋め込まれた1次元スケール不変パターンの中の1つの対称軸を表す。これらの線パラメータにおける変化を直接通して画像に適用されたアフィン変換が判定されるのではなく、アフィン変換は、4つの選択ピークにより特定された4つの対称軸の交点から判定される。2つの対称線 $\{s_k, \beta_k\}$ の軸と対称線 $\{s_m, \beta_m\}$ の軸との交点は、 (x_{km}, y_{km}) でラベル付けされ、次の行列式(16)

$$\begin{pmatrix} x_{km} \\ y_{km} \end{pmatrix} = \frac{1}{\sin(\beta_k - \beta_m)} \begin{pmatrix} \sin \beta_k & -\sin \beta_m \\ \cos \beta_k & \cos \beta_m \end{pmatrix} \begin{pmatrix} s_m \\ s_k \end{pmatrix}. \quad (16)$$

により与えられる。

【0148】

線が平行である場合、交点は存在しないため、 $\sin(\beta_k - \beta_m) \neq 0$ の制約が課される。実施状況において、 $\sin^2(\beta_k - \beta_m) \geq 0.25$ であれば、良好な交点位置を確保するためには十分である。線のパラメータ式は、原点を通るその線の垂直二等分線に対してその線上の任意の点の線形距離を特定する。4つの相互に平行でない線の現在の場合において、各線は、線の長さ（例えば、図11の線3に対する点1103～点1105を参照）に沿って3つの交点を有し、交点間隔比（図11の線3に対する1101：1102）は、アフィン変形に対して不変の状態を維持する。m番目の線が交差するk番目の線に沿った距離 λ_{km} は、次式

$$\lambda_{km} = \frac{s_k \cos(\beta_k - \beta_m) - s_m}{\sin(\beta_k - \beta_m)}. \quad (17)$$

により与えられる。

【0149】

次に、上記の式(17)は、 $k \neq m$ である全ての組み合わせ λ_{km} に対して列挙され、線に沿った位置を含む表(18)は、次式

$$\begin{bmatrix} - & \lambda_{12} & \lambda_{13} & \lambda_{14} \\ \lambda_{21} & - & \lambda_{12} & \lambda_{24} \\ \lambda_{31} & \lambda_{32} & - & \lambda_{34} \\ \lambda_{41} & \lambda_{42} & \lambda_{43} & - \end{bmatrix} \quad (18)$$

により生成される。

【0150】

次に、表(18)のパラメータは、大きさ順に次式により表される。

$\{\lambda_{km}\}_{\max} > \{\lambda_{km}\}_{\text{mid}} > \{\lambda_{km}\}_{\min}$ (各線kの $m = 1 \rightarrow 4$) である。これにより、次の式(19)

10

20

30

40

50

$$R_k' = \min \left[\frac{\{\lambda_{km}\}_{\max} - \{\lambda_{km}\}_{\text{mid}}}{\{\lambda_{km}\}_{\text{mid}} - \{\lambda_{km}\}_{\min}}, \frac{\{\lambda_{km}\}_{\text{mid}} - \{\lambda_{km}\}_{\min}}{\{\lambda_{km}\}_{\max} - \{\lambda_{km}\}_{\text{mid}}} \right] \leq 1 \quad (19)$$

【0151】

に示すように、長さ比 R_k' を求める。

【0152】

この式により、4つの対称軸から、4つの比が生成される。また、4つの比は、1次元基底関数パラメータ r_i 及び1次元基底関数パラメータ α_i の最初の組から生成されてもよい。これらの（最初の）比が R_k として示される場合、4つのピークの選択された組に対する比測定における誤りは、次式

$$E_{\text{ratio}} = \sqrt{\sum_{k=1}^4 (R_k'/R_k - 1)^2}. \quad (20)$$

により規定される。

【0153】

この誤りが0.1を超える場合、このピークの組は、破棄される。誤りが0.1未満である場合、線形最小二乗適合モデルを適用することにより、最適アフィン変換を判定する。最適アフィン変換は、4つの選択ピークにより生成された対称軸の交点の組を、埋め込みパターンの対称軸の交点の最初の組へマッピングし直す。最適アフィン変換を求める方法は、後述される。

【0154】

<ソルト値の抽出>

図4へ戻ると、一旦、粗位置決めマークが回復され、且つステップ2401及びステップ2402に従って粗位置決めが行われた場合、次に、ステップ2422においてソルトは、回復される。ソルトパターンに対応するピークは、粗位置決めマークに対して上述した方法と同様の方法を使用して回復される。ソルト振動定数 γ を有するベースパターンの最有力検出候補のピークを使用して、検出ピークの角度及び半径から2つの6ビット値は、回復される。これらの値が結合されることにより、12ビットソルト値は、形成される。

【0155】

<暗号フィールド及び合成暗号位置決め画像の再生>

図4の精位置決めステップ2403に先行して、図2の妥当性検証サブシステム127の暗号フィールドを再生する必要がある。この再生は、図5及び図6に関して説明した方法と同様の方法で、オリジナル鍵（図6のステップ2501を参照）を使用して行われる。オリジナル鍵は、オペレータにより入力されるか、妥当性検証サブシステム127にとって既知であるか、あるいは、作成サブシステム126から、又は他の手段により転送されてもよい。オリジナル鍵（図6のステップ2501により使用された）は、前述した方法と同様の方法により、ソルト値（図6のステップ2508から）と組み合わせられる。その後、暗号フィールドは、信号供給源102及び信号供給源103に関して説明した方法と同様の方法で、図2の暗号信号供給源102'及び暗号信号供給源103'により生成される。図1の粗位置決め／ソルト回復モジュール113により実行された粗位置決めステップ2401及び粗位置決めステップ2402（図4を参照）により判定されたように、信号供給源102'及び信号供給源103'により生成された暗号フィールド空間領域は、粗位置決め走査文書121の等価領域に制限できる。

【0156】

次に、信号供給源102'及び信号供給源103'により生成された暗号フィールドのカラー画像バージョンは、精位置決めモジュール106内で作成される。図7に関して説

10

20

30

40

50

明した方法と同様の方法で、これらの各カラー画像バージョン（図7に関して暗号フィールド由来カラーグリッドと呼ぶ）は、各画素における2ビット暗号値に、カラーlookupアップテーブル134及びlookupアップテーブル135内の索引付けをすることにより作成される。その後、各暗号フィールドの各生成カラー画像バージョンを、画素複製により各寸法の係数3でアップスケーリングすることにより、600DPI画像（走査文書120と同一の解像度）を形成する。600DPI画像は、暗号フィールドの「原寸」カラー画像バージョンを形成する。最後に、暗号フィールドの合成カラー画像バージョンは、暗号フィールドの2つのカラー画像バージョンを平均化することにより生成される。

【0157】

＜ブロックベースマッチングによる精位置決め＞

10

図15は、図4の精位置決め処理2403における置換マップを形成するために使用されたブロックベース相関付け副処理2403Aを示す図である。ブロックベース相関付け処理2403Aでは、ワープ（すなわち、故意の事前細粒変形）を表現する置換マップDを生成する。ワープは、図2の信号121における粗位置決め走査文書の画素を、カラー暗号フィールドのそれぞれの画素位置にマッピングするために必要とされる。不正顕示信号120を発生させるために、印刷／走査動作が、不正顕示機能付文書105の印刷の際にプリンタ2215により実行され、且つ文書105の走査の際にスキャナ2218により実行されたため、ワーピングでは、粗位置決め走査文書において行われた変形を考慮する。このワーピングは、粗位置決め文書121、暗号フィールド115'及び暗号フィールド116'の精位置決めの一部を構成する。

20

【0158】

ブロックベース相関付け処理2403Aでは、入力として、（a）図2の信号121における粗位置決め走査文書（図15の画像1である2010で示される）及び（b）暗号フィールドの合成カラー画像バージョン（画像2である2020で示される）を受け取る。粗位置決め走査文書は、幅N画素及び高さM画素を有し、合成カラー画像バージョンも、幅N画素及び高さM画素を有する。画像1（すなわち、2010）は、図4の粗位置決めステップ2419の結果121であるため、2つの画像2010及び画像2020は、相互の数画素の範囲内に大まかに位置決めされる。

【0159】

ブロックベース相関付け処理2403Aは、ブロックの大きさQ及び段差の大きさPの選択を含む。これらの大きさは、変更可能である。ブロックの大きさQを増大させると、より大きい空間領域（及びより多くの計算時間）にわたりQを平均化する代償として、より高度な測定精度が得られる。段差の大きさPを減少させると、計算時間は増大するが、より大きな空間ディテールが得られる。考慮中の例では、 $Q=256$ 、且つ $P=32$ である。これは、高さ256画素及び幅256画素を有し、且つ水平方向及び垂直方向に増分32画素で画像2010及び画像2020に沿って段差付けされているブロックを表す。

30

【0160】

図16は、相関付けのためのブロックの選択を示し、ブロック相関付け処理2403Aにおけるブロックの大きさ及び段差の大きさを示す図である。相関ブロック2100は、画像1（すなわち、2010）上に示される。ブロック2100は、水平寸法「Q」及び垂直寸法「Q」を有する。ブロック2100は、水平方向に増分「P」（2101で示す）で、垂直方向に増分「P」（2102で示す）で段差付けが施されている。

40

【0161】

図15へ戻ると、ステップ2080におけるブロックベース相関付け処理2403Aの出力は、置換マップ「D」である。置換マップDは、次の式（21）により規定された寸法を有するラスタ画像である。

$$D_x = \lfloor (N + Q - 1) / P \rfloor$$

by (21)

$$D_y = \lfloor (M + Q - 1) / P \rfloor$$

ここで、 D_x は水平寸法であり、 D_y は垂直寸法であり、 N は画像 2 0 1 0 の幅画素であり、 M は画像 2 0 1 0 の高さ画素であり、 Q は選択ブロックの大きさである。

【0 1 6 2】

要素数は、 $D_x * D_y$ である。 P は、固定である。置換マップ D の各要素は、置換ベクトル及び信頼度推定を有する。置換マップ D 内の各置換ベクトル及び信頼度推定は、ブロック相関付けの結果である。

10

【0 1 6 3】

画像 2 0 1 0 及び画像 2 0 2 0 の処理は、画像 2 0 1 0 及び画像 2 0 2 0 からの全ての相関ブロック B_p 及び相関ブロック B_q にわたるステップ 2 0 3 0 のループの入力により開始する。この場合、それぞれ、相関ブロックのサブスクリプト「 p 」は、 $[0 \dots D_x - 1]$ の範囲内において、サブスクリプト「 q 」は、 $[0 \dots D_y - 1]$ の範囲内で変化する。画像 2 0 1 0 からのブロック B_m と画像 2 0 2 0 からのブロック B_n との既定の対に対して、置換マップ D における画素 (i, j) を考えると、各々のブロック B_m 及びブロック B_n は、次の式 (2 2) で表現される画素 (i, j) の画素オフセットにおいてこれらのブロックの左上の画素を有する。

20

$$(\lfloor N/2 \rfloor + (i - \lfloor D_x/2 \rfloor)P - \lfloor Q/2 \rfloor, \lfloor M/2 \rfloor + (j - \lfloor D_y/2 \rfloor)P - \lfloor Q/2 \rfloor) \quad (22)$$

ここで、式 (2 2) 内の最初の項は、水平方向のオフセットを表し、2 番目の項は、垂直方向のオフセットを表す。

【0 1 6 4】

次のステップ 2 0 4 0 において、それぞれ、全体の選択ブロック B_m が画像 2 0 1 0 の範囲内に、選択ブロック B_n が画像 2 0 2 0 の範囲内に存在するか否かが確認される。全体のブロックがそれぞれの画像の範囲内に存在しない場合、置換マップ D 内の画素 (i, j) に対する信頼度推定は、0 に設定され、ループは、継続される。しかしながら、全体のブロック B_m が画像 2 0 1 0 の範囲内に、全体のブロック B_n が画像 2 0 2 0 の範囲内に存在する場合、次のステップ 2 0 5 0 では、(RGB) ブロック B_m 及び (RGB) ブロック B_n の Yuv カラー空間バージョンを生成する。その後、ステップ 2 0 5 0 では、 u を対応する Yuv ブロックからの実数要素として、 v を対応する Yuv ブロックからの虚数要素として取り扱うことにより、それぞれ、ブロック B_m からの新規の複素画像 B''_m 及び B_n からの新規の複素画像 B''_n を形成する。 u 値及び v 値に基づいた新規のブロック B''_m 及び新規のブロック B''_n は、Yuv カラー空間の主に Y 要素に閉じ込められた主成分の効果を低減する。ステップ 2 0 5 0 では、更に、ウィンドウ関数で新規のブロック B''_m 及び新規のブロック B''_n を乗算することにより、それぞれのウィンドウ化ブロック B'_m 及びウィンドウ化ブロック B'_n を形成する。上述の構成では、垂直方向に二乗されたハニングウィンドウおよび水平方向に二乗されたハニングウィンドウを使用する。次のステップ 2 0 6 0 では、2 つのウィンドウ化ブロック B'_m 及びウィンドウ化ブロック B'_n に対して位相相関付けを行う。

30

40

【0 1 6 5】

相関付けステップは、以下の相相関付けを使用して行われる。相相関付けにおいて、ブロック B'_m の FFT は、ブロック B'_n の FFT の複素共役で乗算され、 $B^{p h n}_{m n}$ で示されるこの乗算結果は、基準化されて単位大きさの最大値を有ようになる。基準化された結果は、 $B^{p h n}_{m n}$ で示される。その後、ステップ 2 0 5 0 では、 $B^{p h n}_{m n}$ に逆 FFT を適用して、「 C 」で示す相関ブロックを形成する。

50

【0166】

相関ブロックCは、（本実施例では）複素値の $Q \times Q$ 寸法のラスタアレイである。その後、複素値は、ピーク検出ステップ2070に入力される。ステップ2070は、図12のピーク検出ステップ1780の動作に類似する。ステップ2070では、ブロックCの中心に対する相関ブロックCの最大ピークの位置をサブ画素精度で判定する。ステップ2080において、ブロックCの中心に対するこのサブ画素精度位置は、相関付け結果の信頼度推定として、ピーク高さの平方根に沿った位置（ i, j ）における置換マップD内に格納される。ループ2030は、未処理のブロックが存在しなくなるまで継続される。

【0167】

次に、図17に関して説明されるように、補間処理2403Bでは、図15のブロック相関付け副処理2403Aから出力された置換マップDを使用して、変形マップD'を形成する。変形マップD'は、粗位置決め走査文書121内の各画素を、暗号フィールドの座標空間内の画素と関連付ける。変形マップD'のいくつかの部分は、粗登録文書121内の画素を、暗号フィールド境界線の外側の画素にマッピングしてもよい。この動作の理由は、撮影装置が、文書全体を撮影しなかったためである。

【0168】

図17は、変形マップD'を形成するために、置換マップDを補間するための補間処理2403Bを示す図である。補間処理2403Bでは、ステップ1910において、図15のステップ2080において格納された置換マップDを受け取る。次のステップ1920では、置換マップDを使用して、置換マップDに最適な線形変換パラメータ（ $b_{11}, b_{12}, b_{21}, b_{22}, \Delta x, \Delta y$ ）の組を判定する。

【0169】

暗号フィールド内の任意の点（ x_{ij}, y_{ij} ）（尚、このような点の x, y の位置は、文書121内の画素とは対照的に、位置上の変形を受けなかった）は、次の数学的関係に係る置換マップD内の対応する画素（ i, j ）

$$(x_{ij}, y_{ij}) = ([N/2] + (i - [D_x/2])P, [M/2] + (j - [D_y/2])P). \quad (23)$$

にマッピングされる。

【0170】

次の演算を実行することによって、置換マップを使用して暗号フィールド点を置換し、対応する置換暗号フィールド点座標

$$(\hat{x}_{ij}, \hat{y}_{ij})$$

を生成する。

$$(\hat{x}_{ij}, \hat{y}_{ij}) = (x_{ij}, y_{ij}) - D(i, j), \quad (24)$$

ここで、 $D(i, j)$ は、考慮中の画素（ i, j ）に対する置換マップDの置換ベクトル部分である。

【0171】

非変形点（ x_{ij}, y_{ij} ）に割り当てられた線形変換パラメータ（ $b_{11}, b_{12}, b_{21}, b_{22}, \Delta x, \Delta y$ ）は、次式により、アフィン変換点

$$(\tilde{x}_{ij}, \tilde{y}_{ij})$$

$$\begin{pmatrix} \tilde{x}_{ij} \\ \tilde{y}_{ij} \end{pmatrix} = \begin{pmatrix} b_{11} & b_{21} \\ b_{12} & b_{22} \end{pmatrix} \begin{pmatrix} x_{ij} \\ y_{ij} \end{pmatrix} + \begin{pmatrix} \Delta x \\ \Delta y \end{pmatrix}. \quad (25)$$

10

20

30

40

50

を生成する。

【0172】

最適アフィン変換は、置換座標

$$(\hat{x}_{ij}, \hat{y}_{ij})$$

の間の誤りの最小化により判定され、アフィン変換点

$$(\tilde{x}_{ij}, \tilde{y}_{ij})$$

は、アフィン変換パラメータを変化させることにより判定される。最小化すべき誤り関数は、次式

10

$$E = \sum_{n=1}^N (\hat{x}_n - \tilde{x}_n)^2 + (\hat{y}_n - \tilde{y}_n)^2 \quad (26)$$

により規定されたユークリッドノルム測度Eである。

【0173】

最小化の解は、次式により与えられる。

$$\begin{pmatrix} b_{11} \\ b_{12} \\ \Delta x \end{pmatrix} = \mathbf{M}^{-1} \begin{pmatrix} \sum \hat{x}_n x_n \\ \sum \hat{x}_n y_n \\ \sum \hat{x}_n \end{pmatrix} \quad (27)$$

20

$$\begin{pmatrix} b_{21} \\ b_{22} \\ \Delta y \end{pmatrix} = \mathbf{M}^{-1} \begin{pmatrix} \sum \hat{y}_n x_n \\ \sum \hat{y}_n y_n \\ \sum \hat{y}_n \end{pmatrix}$$

この場合、

$$\mathbf{M} = \begin{pmatrix} S_{xx} & S_{xy} & S_x \\ S_{xy} & S_{yy} & S_y \\ S_x & S_y & S \end{pmatrix} = \begin{pmatrix} \sum x_n x_n & \sum x_n y_n & \sum x_n \\ \sum y_n x_n & \sum y_n y_n & \sum y_n \\ \sum x_n & \sum y_n & \sum 1 \end{pmatrix} \quad (28)$$

30

$$\mathbf{M}^{-1} = \frac{1}{|\mathbf{M}|} \begin{pmatrix} -S_y S_y + SS_{yy} & -SS_{xy} + S_x S_y & S_{xy} S_y - S_x S_{yy} \\ -SS_{xy} + S_x S_y & -S_x S_x + SS_{xx} & S_x S_{xy} - S_{xx} S_y \\ S_{xy} S_y - S_x S_{yy} & S_x S_{xy} - S_{xx} S_y & -S_{xy} S_{xy} + S_{xx} S_{yy} \end{pmatrix} \quad (29)$$

且つ

40

$$|\mathbf{M}| = \det \mathbf{M} = -S S_{xy} S_{xy} + 2S_x S_{xy} S_y - S_{xx} S_y S_y - S_x S_x S_{yy} + SS_{xx} S_{yy} \quad (30)$$

である。ここで、合計は、置換マップD内の置換ベクトル上のゼロでない信頼度推定を使用して、置換画素全体にわたって実行される。

【0174】

次のステップ1930では、次式

$$D(i, j) \rightarrow D(i, j) - \begin{pmatrix} b_{11} & b_{21} \\ b_{12} & b_{22} \end{pmatrix} \begin{pmatrix} x_{ij} \\ y_{ij} \end{pmatrix} - \begin{pmatrix} \Delta x \\ \Delta y \end{pmatrix}. \quad (31)$$

により各置換マップ画素を置換することにより、置換マップから最適線形変換を排除する。

【0175】

その後、次のステップ1940では、最適線形変換を、バイキュービック補間を使用して排除した後、置換マップを $D_x \times P \times D_y \times P$ 寸法の置換マップに補間する。置換マップが、バイキュービック補間カーネルの隣接部分内に信頼度ゼロを有する画素を有する場合、補間ステップにおいて、複雑化が発生する可能性がある。複雑化が発生した場合、信頼度ゼロを有する画素自体を、画素の信頼値により重み付けされた隣接画素の平均を使用して、推定値で置換する。隣接画素が、正の信頼度を有していない場合、画素値を判定するために、アルゴリズム発展領域は、使用される。次に、補間置換画素は、置換マップ内の置換画素に沿った正の信頼度を有する画素を使用するバイキュービック補間を使用して計算される。

10

【0176】

次のステップ1950では、次式により、以前に排除された最適線形変換を補間置換マップ D' に再び適用する。

$$D'(i, j) \rightarrow D'(i, j) + \begin{pmatrix} b_{11} & b_{21} \\ b_{12} & b_{22} \end{pmatrix} \begin{pmatrix} x_{ij} \\ y_{ij} \end{pmatrix} + \begin{pmatrix} \Delta x \\ \Delta y \end{pmatrix} \quad (32)$$

20

ここで、

$$(x_{ij}, y_{ij}) = ([N/2] + (i/P - [D_x/2])P, [M/2] + (j/P - [D_y/2])P). \quad (33)$$

である。

【0177】

$D'(i, j)$ は、変形マップであり、補間処理2403Bのステップ1950からの出力を形成する。

30

【0178】

<精位置決めに対する画像ワーピング>

図18は、図17のステップ1950の変形マップ D' から精位置決め文書を形成するために使用されたワーピング処理2403Cを示す図である。画像ワーピング処理2403Cでは、入力として、走査文書121と、図12のステップ1790において粗登録処理により生成されたアフィン変換パラメータと、図17のステップ1950の変形マップ D' とを使用し、出力として、カラー暗号フィールドに精密に登録された走査文書のワーピング形態（精位置決め走査文書と呼ぶ）を使用する。画像ワーピング処理2403Cにおける第1のステップ2601では、変形マップ D' を、暗号フィールド内の画素と走査文書121内の画素とを関連付ける関連マップ D'_c に修正する。この修正は、次式を実行することによって、粗登録ステップ（図12のステップ1790）において判定されたアフィン変換を、変形マップ D' に戻り加算することにより行われる。

40

$$D'(i, j) \rightarrow D'(i, j) + \begin{pmatrix} a_{11} & a_{21} \\ a_{12} & a_{22} \end{pmatrix} \begin{pmatrix} x_{ij} \\ y_{ij} \end{pmatrix} + \begin{pmatrix} x_0 \\ y_0 \end{pmatrix}. \quad (34)$$

ここで、 $(a_{11}, a_{12}, a_{21}, a_{22}, x_0, y_0)$ は、粗登録ステップにおいて判定されたアフィン変換パラメータである。

【0179】

50

その後、更にステップ2601において、暗号フィールド内の画素に対応する走査文書121内の画素は、(a) 関連マップD'cを使用して、走査文書121内の各画素に対して、暗号フィールド内の画素位置に対応する走査文書121上のサブ画素位置を判定し、且つ(b) バイキュービック補間を使用して、その位置における走査文書121を補間することにより、識別される。

【0180】

次のステップ2602では、粗位置決め走査文書121と同一の大きさを有する空画像I^eを形成する。その後、ステップ2603では、上記の空画像I^e内の次の画素を読み取る。次の判断ステップ2304では、I^e内の全ての画素が処理されたか否かが検定される。I^e内の全ての画素が処理された場合、プロセス2403Cは、図4の矢印2423である矢印YESに従って進み、2423(図4を参照)で精位置決め文書を出力する。これに対して、I^e内に未処理の画素が残存する場合、プロセス2403Cは、ステップ2304から「NO」に従って、ステップ2606へ進む。

10

【0181】

ステップ2606において、空画像I^e内の考慮中の画素に対して、(x, y)座標は、関連マップD'c内の対応する画素から取り出される。その後、ステップ2607では、この(x, y)座標を使用して、バイキュービック補間により、粗位置決め走査文書121の対応する「真の」画素値を計算する。次のステップ2608では、当該画素に関してワープ(真の)画素値をI^e内に書き込むことにより、精位置決め走査文書を形成する。その後、プロセス2403Cは、矢印2609によりステップ2603へ戻る。尚、I^eは、特に、赤強度成分、緑強度成分及び青強度成分のようないくつかの成分を含む。

20

【0182】

600DPIの精位置決め走査文書I^e及びカラー画像暗号フィールドは、各ブロックの中央画素をサンプリングすることにより、200DPIに減少する。この減少により、200DPI画素間のいくつかの混色値を有する画素を、回避する。

【0183】

＜精位置決め走査文書の認証＞

図19は、改竄検知の一例を示す図である。画素801は、(図2の信号123又は信号124における)精位置決め走査文書812の一部を形成する。4つの画素802は、図8の不正顕示機能付文書705に示す比較可能なオリジナル画素709から変化した。そのため、非認証人物は、図8の文字「EF」を図19の「FE」に変化させるために、2対の画素802を変化させた。

30

【0184】

最初の工程として、矢印813で示すように、精位置決め走査文書812に対して、各画素の輝度値を考慮する閾化モジュール107内で閾値演算が施される。輝度が50%未満の画素は、黒として分類され、残る画素は、白として分類される。オリジナルのソース画像(不図示)として仮定された画像804は、閾値演算の結果として作成される。

【0185】

文書802の最初の符号化の際に使用された次のカラー画像バージョン暗号フィールド805は、精位置決め走査文書812を被覆するために、十分な領域内に再生される。この再生は、図6のステップ2501からのオリジナル鍵を使用して行われる。オリジナル鍵は、オペレータにより入力されるか、妥当性検証サブシステム127にとって既知であるか、あるいは、作成サブシステム126から、又は他の手段により転送されてもよい。オリジナル鍵は、図6のステップ2508からのソルト値と組み合わせられる。

40

【0186】

次に、選択モジュール109は、閾化画像804内の各画素の値814を使用して選択を制御する。この制御814下において、選択モジュール109は、1つのカラー画像バージョン暗号フィールド又は他のカラー画像バージョン暗号フィールドから画素値816又は画素値815を選択することにより、基準画像807を作成する。この基準画像の作成は、符号化処理において使用された処理と等価の処理である。比較モジュール108内

50

では、基準画像内のこのような各選択画素（画素807等）に対して、選択画素（本例では、画素807）と位置決め走査画像（この場合、画素801）の対応する画素との比較が行われる。画素807の色の副成分及び画素801の色の副成分が、要求された許容範囲内で一致しない場合、画素は、画素の元の状態から改竄されたとして規定される。一構成例によると、画素の色成分のうちの任意の成分が、線形RGBカラー空間内で測定された既定の色に対して通常の補正值25%を越える差異を有する場合、画素は、「一致」状態を満足できなかったとみなされる。各色に対する通常の補正值は、サンプル色のサンプル色パッチ走査により、又は、推定値のみに基づいて判定できる。閾化画像に沿ったこの情報は、新規の認証画像809を構築するために使用される。説明された例において、マゼンダ以外の全ての画素が、閾化画像に係る黒又は白のいずれかである状態で、マゼンダの複数の画素810は、再生される。

10

【0187】

改竄された画素は、改竄されたポイントにおいて、適切なランダムフィールド（副成分を含む）と偶然にも同一色を有することにより、明らかにされない可能性がある。この状態は、画素が白から黒に変化したにもかかわらず、認証画像内で改変としてフラグされていない場合を示す画素811で示される。上述の構成において、通常、25%までの画素の改変は、検知できない可能性がある。このことは、暗号フィールドが2ビット精度を使用している事実から導出される。検出された画素の75%が、通常、ユーザに対して改変の発生及び特徴を警告するためには十分である。従って、大きな領域（例えば、52ビット鍵内のビット数を超える画素を有する領域）にわたって、検出不可能な不正改変方法を施すことの困難性は、鍵空間の大きさにほぼ比例する。

20

【0188】

最終認証画像809は、通常、オペレータによる試験のためにカラープリンタ上に印刷される。しかしながら、認証画像809は、改変画素の数又は改変画素の稠密領域の存在に基づいた自動解析も施されてもよい。

【0189】

改変画素を明らかにすることが、固有に且つ精密にスケーリングされるため、それを示すように、オリジナル文書708の画素スケールを発生させる。また、改変画素を明らかにすることは、オリジナル文書708を感知できないため、疑わしい文書812及びこれらの改変を明らかにするためのオリジナル鍵のみを必要とする。

30

【0190】

説明された方法の実質的な利点は、文書812の副次部分の改変を明らかにすることが、文書812の残る部分と無関係であることである。尚、粗位置決め情報及びソルト情報は、高度な冗長を実現するために、空間領域内及び周波数領域内の情報の非常な広域分散に対して十分な信号強度を提供する技法を使用して、文書内に組み込まれる。これは、文書812の残る部分と関連することなく、これらの信号が、文書812の任意の副次部分から回復できることを意味する。上述の構成において、文書の任意の25%の領域からのこれらの信号の回復は、容易に実現できる。尚、精位置決め工程及び認証工程は、局所的処理及び不可視部分に対する高度なロバストさも提供する。従って、システム全体は、柔軟性が高く（特殊な構成を有していない任意の文書の全領域に適用可能である）、且つ部分的な転送又は偶発的文書損害に対してロバストな認証方法を提供する。

40

【0191】

＜プリンタドライバにおけるマーキング処理の使用＞

改竄防止方法は、マイクロソフトのウィンドウズ（登録商標）ベースコンピュータ等の汎用コンピュータ上のプリンタドライバの一部として内蔵していてもよい。この構成において、プリンタドライバの特性には、改竄防止方法を可能とするためにオペレータが選択できるユーザインタフェースエレメントと、鍵（又はパスワード）の入力が可能な第2のユーザインタフェースエレメントとが設けられている。この構成の一変形例において、プリンタドライバは、応用データを印刷待ち画像に変化させるラスタ化処理を含む。この段階において、印刷待ち画像は、改竄防止方法で説明したように、プリンタドライバにより

50

修正され、生成された画像は、プリンタ装置に送信される。

【0192】

第2の変形例において、改竄防止方法は、プリンタ装置内で実行される。この方法は、改竄防止方法が、高周波データを印刷データ内に導入するので、利便性が高い。プリンタへのデータ転送処理、又はプリンタの内部処理が、画像圧縮を採用する場合、この高周波データが存在するため、画像圧縮への効果は少ない。しかしながら、プリンタ装置へのデータ転送後、改竄防止方法が実行された場合、プリンタ装置は、圧縮及び解凍の終了後に、後段の処理において高周波データを加算できる。

【0193】

＜複合機におけるマーキング及び認証の使用＞

10

改竄防止方法の別の構成では、Canon IR C3200等の複合機の能力として、改竄防止方法を採用する。この構成において、複合機は、セキュリティコピー動作の一部として改竄防止方法を採用可能とするユーザインタフェースエレメントを提供する。プリンタドライバの場合、第2のユーザインタフェースが、鍵入力を可能とする。この実現されたオプションを使用してコピーされた文書が走査され、上述のように、デジタル走査画像がマーキングされ、且つこの生成されたデジタル画像が印刷されることにより、セキュリティコピー動作を提供できる。また、同一の多機能装置又は別の多機能装置は、認証特徴を採用する。この認証特徴も、ユーザインタフェースエレメント及び第2の鍵入力エレメントにより実現できる。このオプションの範囲下においてコピーされた文書は、上述の認証処理が施される。印刷文書は、非改変領域の黒及び白が再現される状態で、マゼンダ（又は他の強調表示色）が明らかにされた改変領域を有する認証処理結果である。

20

【0194】

＜スキャナを使用した文書の認証＞

改竄防止方法の別の構成では、USBインタフェースを介してマイクロソフトのウィンドウズ（登録商標）を稼動し、且つ改竄防止処理を採用したソフトウェアアプリケーションを稼動している汎用コンピュータに接続されたCanon CanoScan 8000F等のスキャナ装置が使用される。この構成において、ソフトウェアアプリケーションは、TWINスキャナドライバを使用して、オペレータにより提供された紙文書から文書画像を得る。各文書画像は、改竄防止方法に従って解析される。妥当性検証結果は、オペレータによる検査のために、コンピュータ画面上に表示される。

30

【0195】

＜枚葉紙スキャナを使用した大容量文書の認証＞

改竄防止方法の別の構成では、Canon DR-5080C等のデスクトップ型高速枚葉スキャナが使用される。この構成において、大容量文書は、オペレータが介入することなく走査される。妥当性検証処理が、走査処理と同期して使用されることにより、改変された文書は、発見される。この構成において、妥当性検証処理の結果であるデジタル画像は、改変画素の閾値を越える画素を含む複数の小さなパッチに対して試験される。パッチの大きさ及び閾値は、オペレータによる設定が可能である。また、文書の異なる領域における異なる閾値及びパッチを設定すること、並びに文書が形態認識システムにより識別されたこれらの領域を有することも可能である。

40

【0196】

〔産業上の利用可能性〕

上述したように、上記の構成が、文書処理産業に適用できることは、明らかである。

【0197】

先の説明は、本発明のいくつかの実施の形態のみを説明したが、本発明の趣旨の範囲を逸脱せずに、本発明の変形及び／又は変更を行うことができる。実施の形態は、例証するものであって、限定するものではない。

【図面の簡単な説明】

【0198】

【図1】 上述の改竄防止構成が実施可能な汎用コンピュータを概略的に示すブロック図で

50

ある。

【図 2】開示された改竄防止システムの機能ブロック図の一例を示す図である。

【図 3】図 2 のシステムを使用して、不正顕示機能付文書を作成するプロセスを示す図である。

【図 4】図 2 のシステムを使用して、図 3 からの不正顕示機能付文書の妥当性検証、すなわち、文書が改竄されたか否かを判定するプロセスを示す図である。

【図 5】ストリーム暗号から 2 次元暗号フィールドを生成する 2 つの方法を表す図である。

【図 6】図 5 の暗号フィールドを生成するプロセスを示す図である。

【図 7】2 値レベルソース画素を多値レベル不正顕示機能付画素に変換するために使用された図 2 の選択処理の一例を示す図である。

10

【図 8】多値レベル画像に変換されるべき 2 値レベル画像の描画例を示す図である。

【図 9】粗位置決めで使用された 2 次元線形波形関数の 2 値レベル表現を示す図である。

【図 10】図 9 の線形波形関数のグラフィック表現を示す図である。

【図 11】不正顕示機能付文書の粗位置決めにおいて使用された位置決めマークを形成するために使用された 4 つの線形波形関数の予め規定された組からの対称軸の一例を示す図である。

【図 12】図 4 の粗位置決め処理をより詳細に示す図である。

【図 13】図 12 の準極変換処理をより詳細に示す図である。

【図 14】図 12 のピーク検出処理をより詳細に示す図である。

20

【図 15】図 4 の精位置決め処理における置換マップを形成するために使用されたブロックベース相関付け副処理を示す図である。

【図 16】図 15 のブロック相関付け処理におけるブロックの大きさ及び段差の大きさを示す図である。

【図 17】図 15 の置換マップから変形マップを形成するために使用された補間副処理を示す図である。

【図 18】図 17 の置換マップから精位置決め文書を形成するために使用されたワーピング処理を示す図である。

【図 19】改竄検知の一例を示す図である。

【図 1】

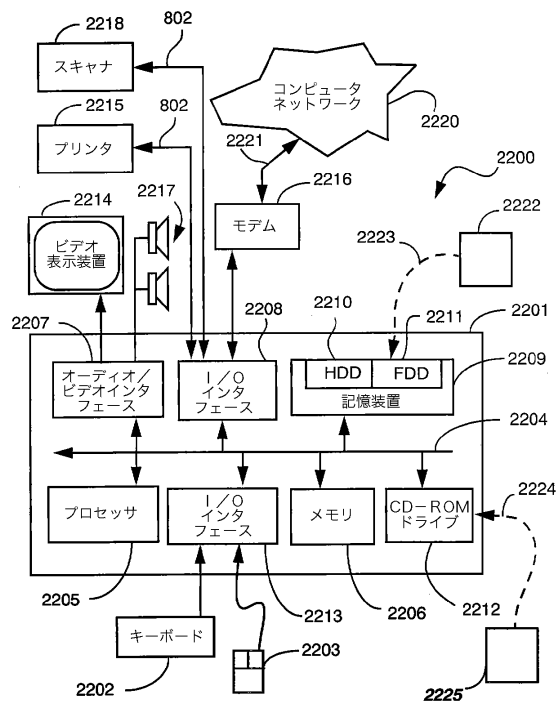


Fig. 1

【図 2】

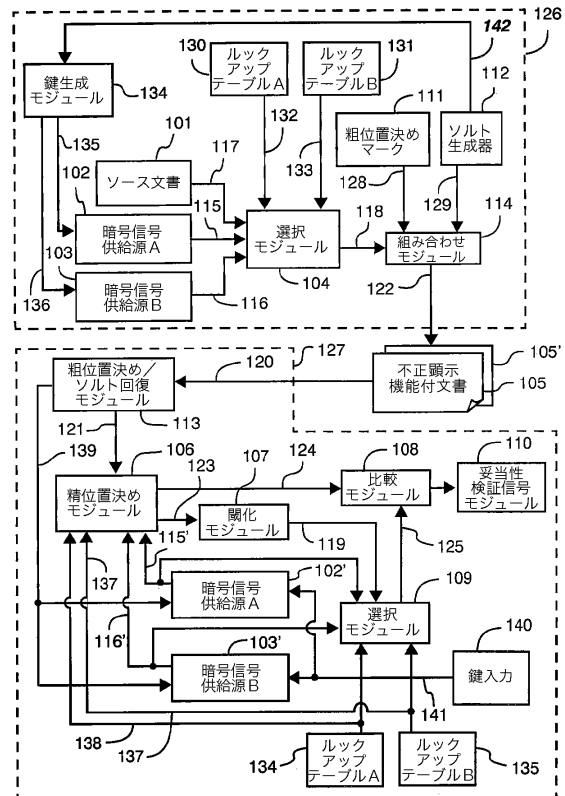


Fig. 2

【図 3】

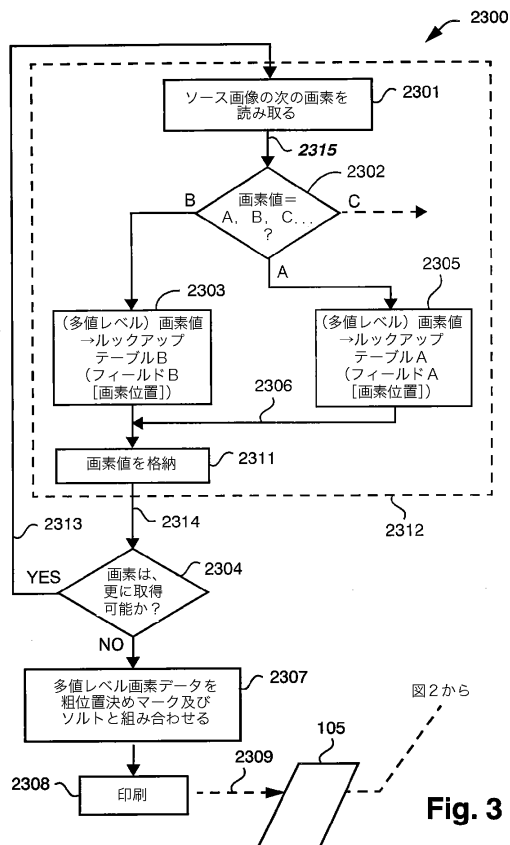


Fig. 3

【図 4】

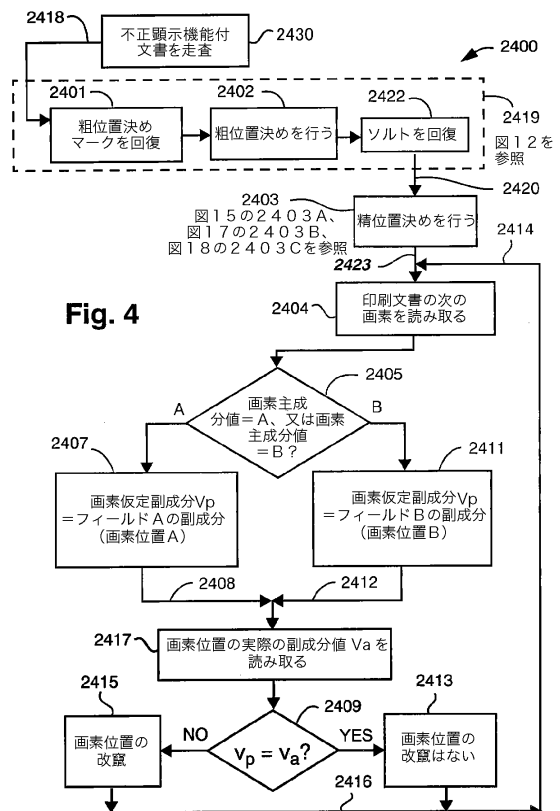


Fig. 4

【図 5】

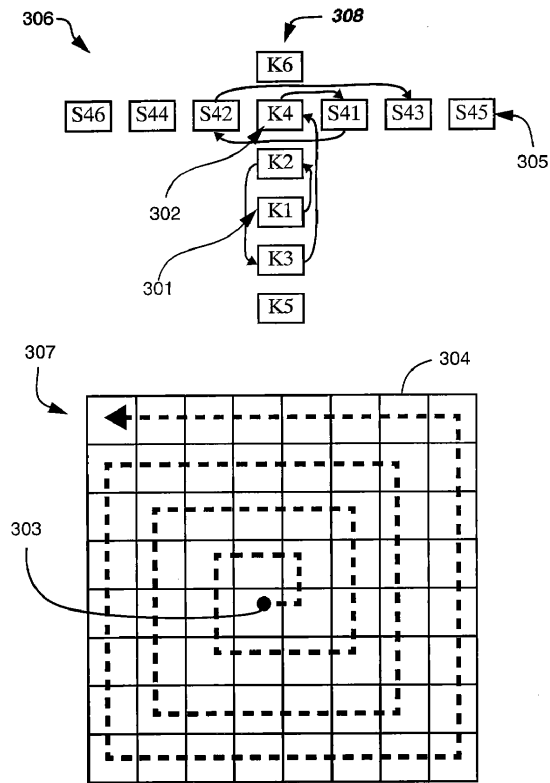


Fig. 5

【図 6】

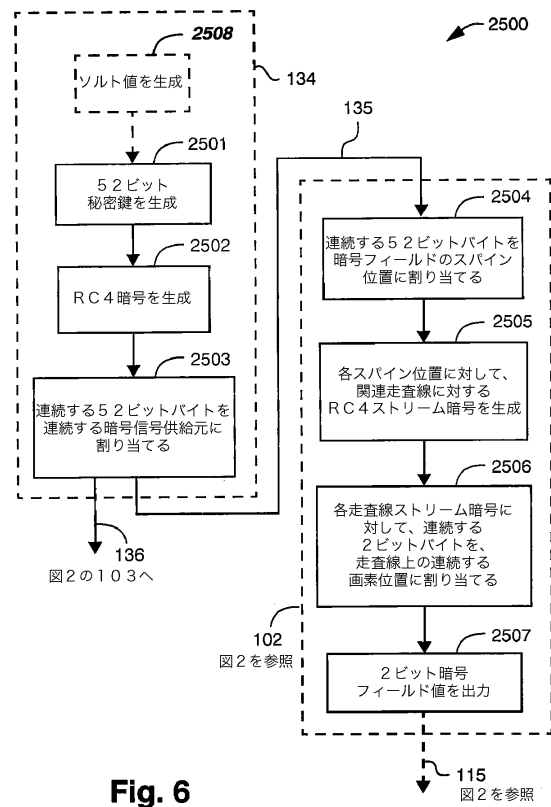


Fig. 6

【図 7】

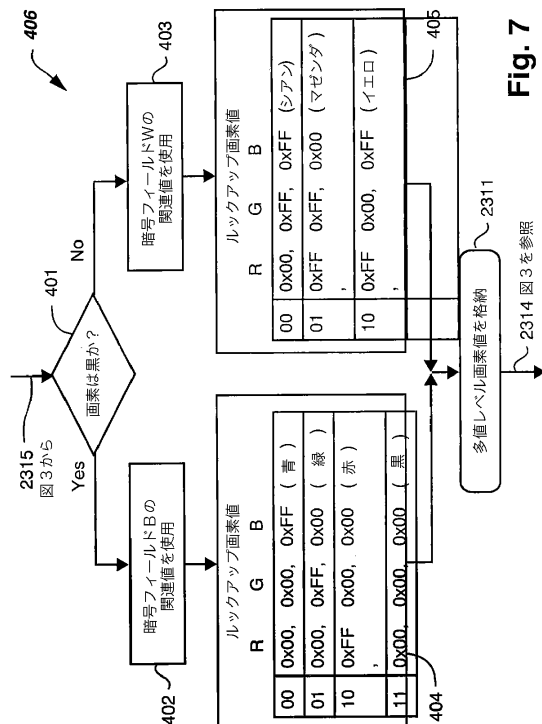


Fig. 7

【図 8】

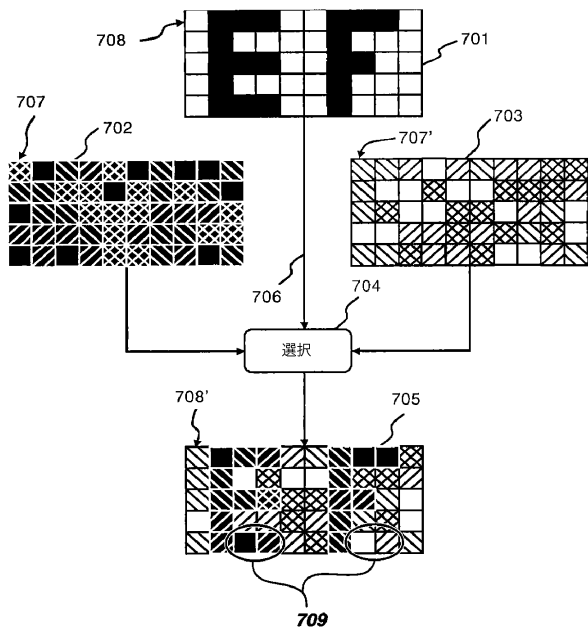


Fig. 8

【図 9】

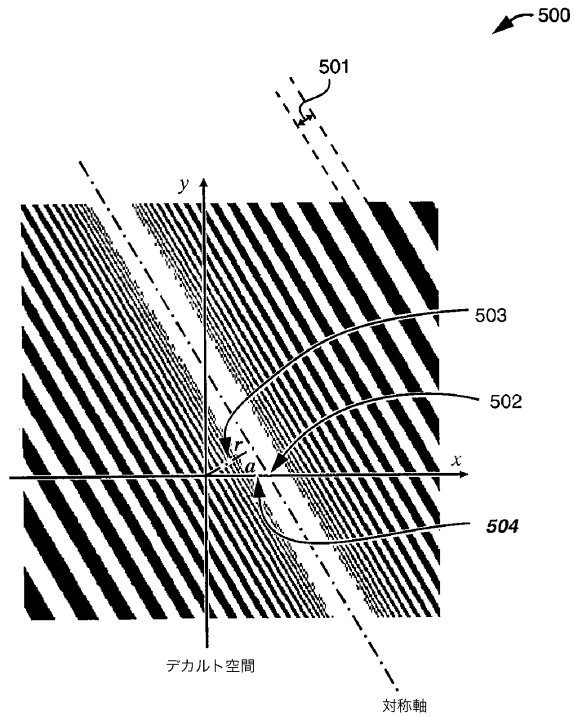


Fig. 9

【図 10】

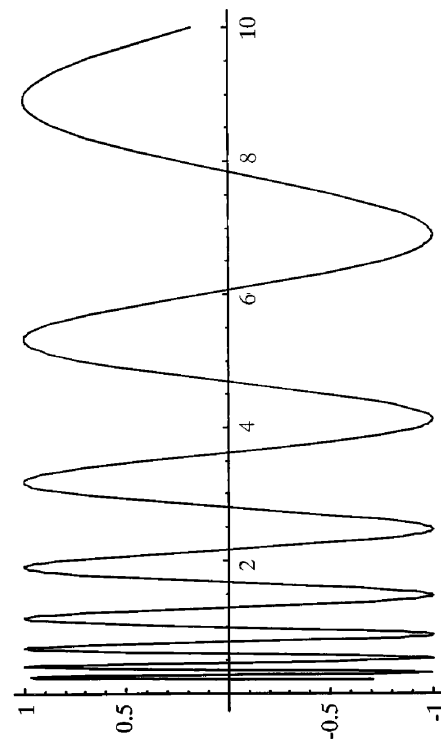


Fig. 10

【図 11】

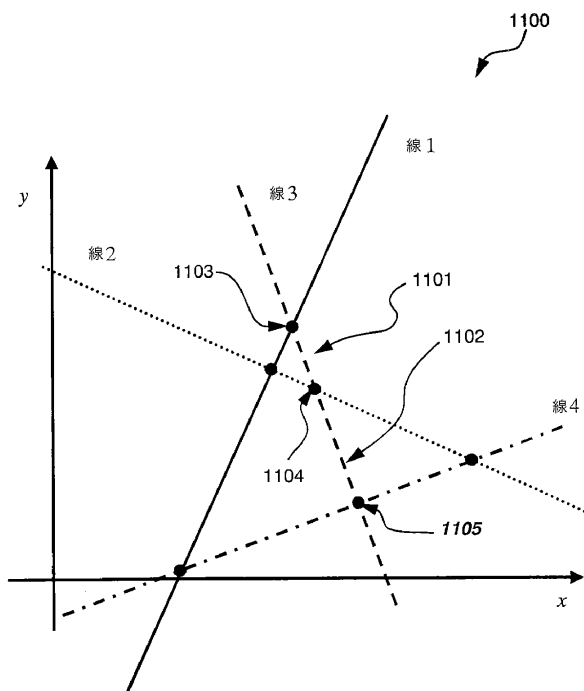


Fig. 11

【図 12】

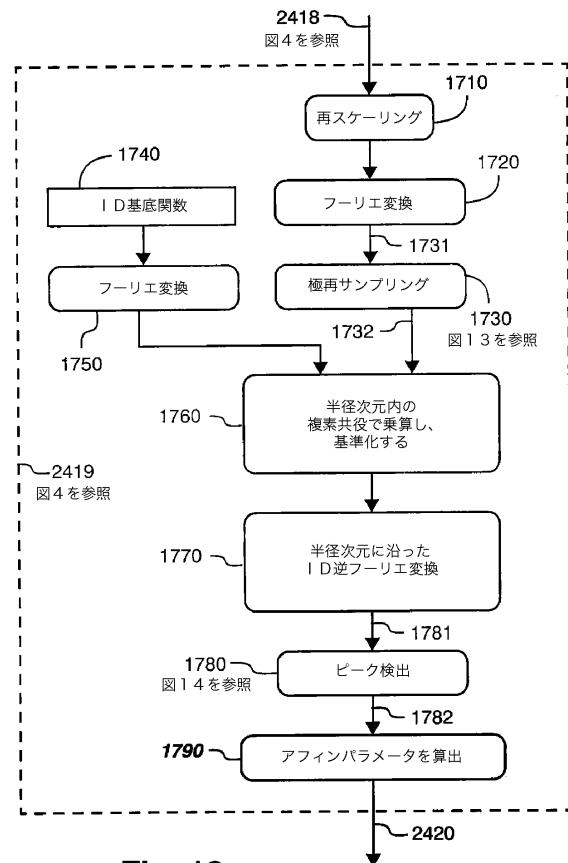


Fig. 12

【図 13】

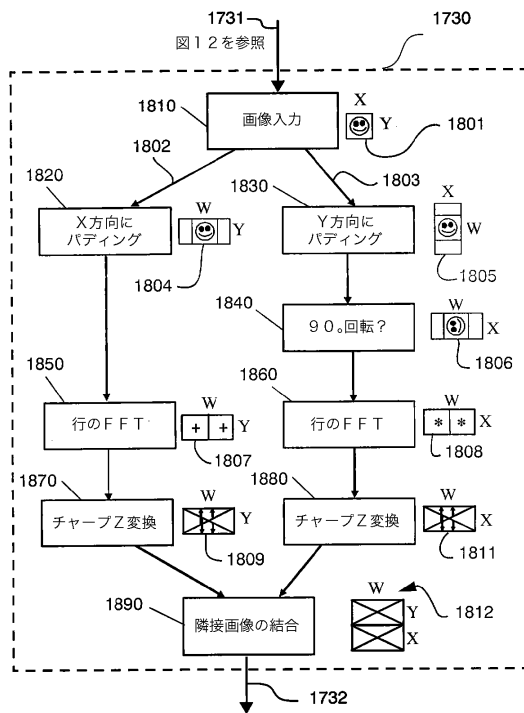


Fig. 13

【図 14】

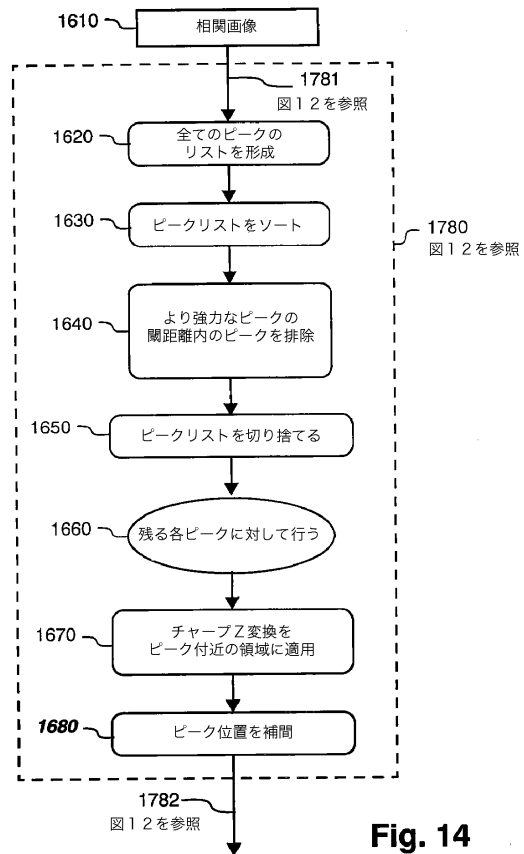


Fig. 14

【図 15】

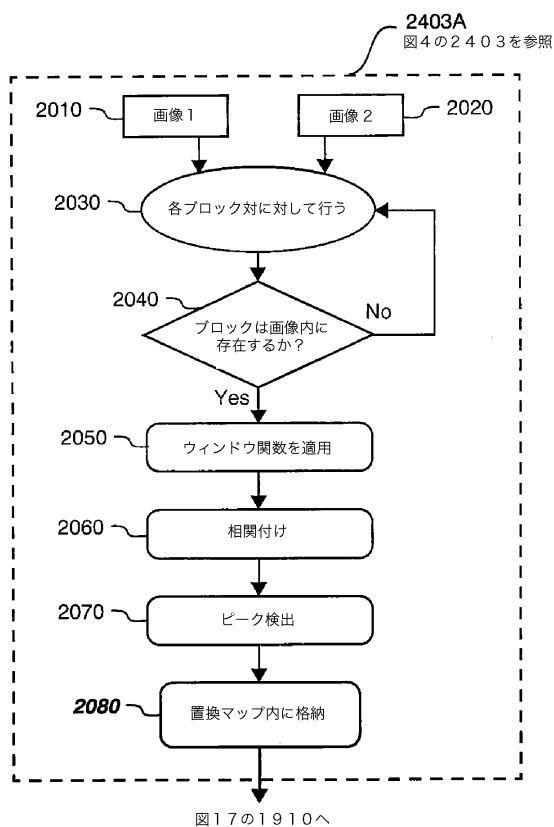


Fig. 15

【図 16】

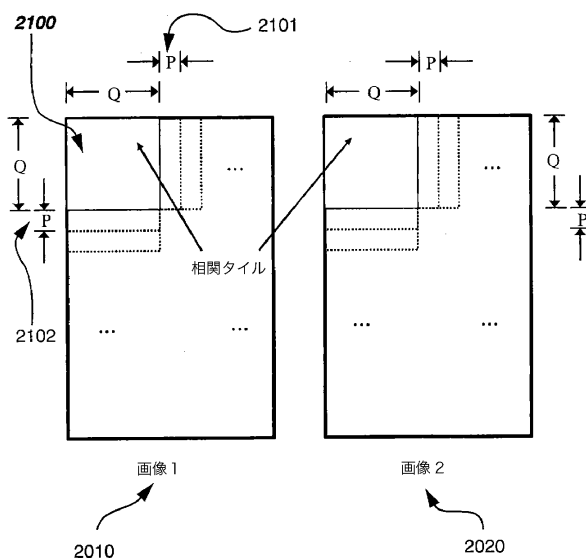


Fig. 16

【図 17】

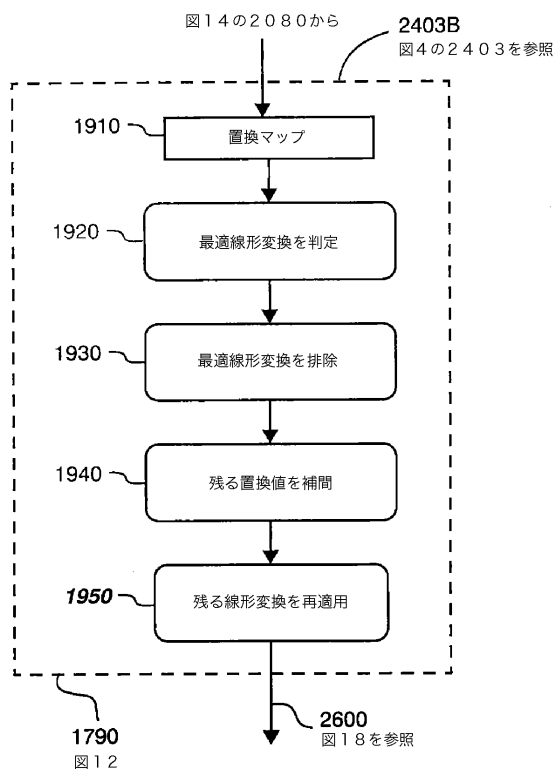


Fig. 17

【図 18】

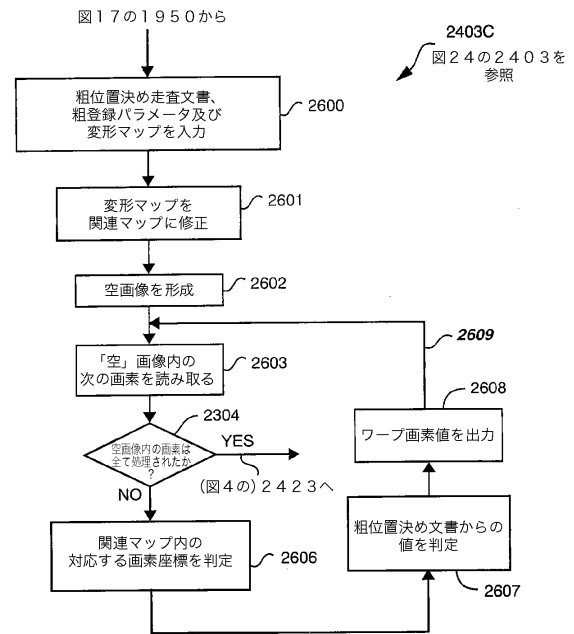


Fig. 18

【図 19】

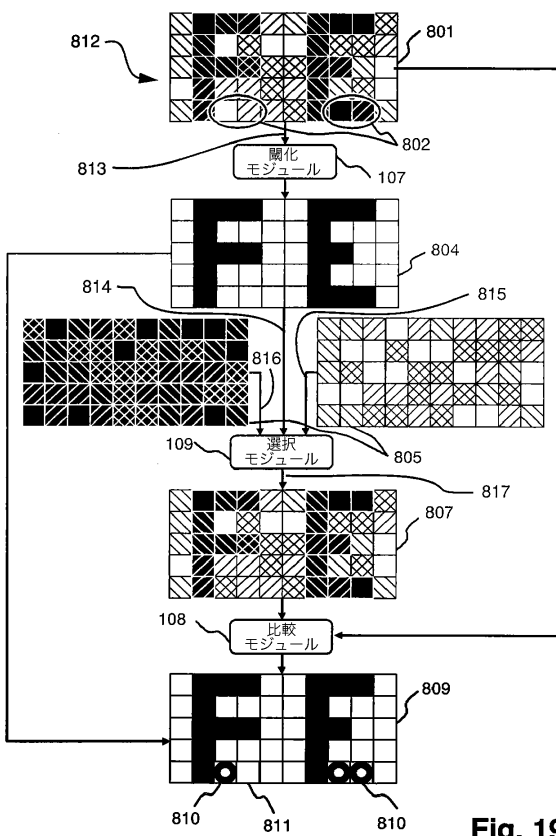


Fig. 19

フロントページの続き

- (72)発明者 ティモシー メリック ロング
オーストラリア国 2113 ニュー サウス ウェールズ州, ノース ライド, トーマス ホル
ト ドライブ 1 キヤノン インフォメーション システムズ リサーチ オーストラリア プ
ロプライエタリー リミテッド内
- (72)発明者 ピーター アレイン フレッチャー
オーストラリア国 2113 ニュー サウス ウェールズ州, ノース ライド, トーマス ホル
ト ドライブ 1 キヤノン インフォメーション システムズ リサーチ オーストラリア プ
ロプライエタリー リミテッド内
- (72)発明者 ステファン ジェームス ハーディー
オーストラリア国 2113 ニュー サウス ウェールズ州, ノース ライド, トーマス ホル
ト ドライブ 1 キヤノン インフォメーション システムズ リサーチ オーストラリア プ
ロプライエタリー リミテッド内

審査官 橋爪 正樹

(56)参考文献 特開2001-148775 (JP, A)

(58)調査した分野(Int.Cl., DB名)

H04N 1/38- 1/393

G06T 1/00