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

特許第6934231号
(P6934231)

(45)発行日　令和3年9月15日(2021.9.15)　(24)登録日　令和3年8月25日(2021.8.25)

(51)Int.Cl.		F I		
G06Q 50/26	(2012.01)	G06Q	50/26	300
G06T 7/00	(2017.01)	G06T	7/00	350C
G06F 21/64	(2013.01)	G06T	7/00	610Z
		G06F	21/64	

請求項の数 24　(全 32 頁)

(21)出願番号　特願2019-541677(P2019-541677)
(86)(22)出願日　平成29年10月13日(2017.10.13)
(65)公表番号　特表2019-534526(P2019-534526A)
(43)公表日　令和1年11月28日(2019.11.28)
(86)国際出願番号　PCT/US2017/056516
(87)国際公開番号　WO2018/071768
(87)国際公開日　平成30年4月19日(2018.4.19)
審査請求日　令和2年10月9日(2020.10.9)
(31)優先権主張番号　62/408,531
(32)優先日　平成28年10月14日(2016.10.14)
(33)優先権主張国・地域又は機関
米国(US)

早期審査対象出願

(73)特許権者　519135574
アイディー　メトリクス　グループ　インコーポレイテッド
アメリカ合衆国　０３１０１　ニューハンプシャー州　マンチェスター　ローウェル　ストリート　６２　スイート　４
(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

最終頁に続く

(54)【発明の名称】身分証明書の改ざん検出方法

(57)【特許請求の範囲】
【請求項１】
画像化された物理的信用証明書の電子的または物理的改ざんを検出するための、コンピュータによって実行される方法であって、1つまたは複数のプロセッサを使用して実行され、以下の工程:
識別データを含む1つまたは複数の高価値領域を有する物理的信用証明書を表す、画素配列を含むデジタル画像を受け取る工程;
所定の改ざんシグネチャに関して前記デジタル画像の前記高価値領域の画素レベルの解析を行うように構成された改ざん検出器で、前記デジタル画像を処理し、前記デジタル画像の固有の特性に対応する出力を生成する工程;および
前記改ざん検出器からの前記出力に基づいて、前記デジタル画像が電子的に改ざんされているかどうかを判定する工程
を含む、前記方法であって、
前記改ざん検出器が、訓練データセットを適用する機械学習アルゴリズムによって訓練された予測モデルを含み、
前記訓練データセットが、
複数の固有の画素特徴の組合せを含む、第1の改ざんされていないデジタル画像のセットと、
前記改ざんされていないデジタル画像のうちの1つまたは複数の電子的に改ざんされた派生物を含む、第2のデジタル画像のセットと

を含み、
前記第1のセットの前記改ざんされていないデジタル画像の各々が前記訓練データセットにおいて第1の共通ラベルを割り当てられており、前記第2のセットの前記改ざんされたデジタル画像の各々が前記訓練データセットにおいて第2の共通ラベルを割り当てられており、前記第2のラベルが前記第1のラベルとは異なる、
前記方法。
【請求項２】
前記画素レベルの解析が、
物理的および/または電子的改ざんの証拠となる1つまたは複数の画素特徴と、
改ざんされていない画像取込みおよび処理操作の証拠となる、1つまたは複数の無害な画素特徴と
を含む、複数の固有の画素特徴の組合せの検査を含む、
請求項1記載の方法。
【請求項３】
前記受け取られるデジタル画像の高価値領域が人物情報（biographical）テキストを含み、前記改ざん検出器の前記所定の改ざんシグネチャが人物情報の継ぎ合わせまたは他の改変を含む、請求項1記載の方法。
【請求項４】
前記受け取られるデジタル画像の高価値領域がバイオメトリックデータを含み、前記改ざん検出器の前記所定の改ざんシグネチャが写真の継ぎ合わせまたは他の改変を含む、請求項1記載の方法。
【請求項５】
前記受け取られるデジタル画像の高価値領域が機械可読領域（MRZ）を含み、前記改ざん検出器の前記所定の改ざんシグネチャがMRZの継ぎ合わせまたは他の改変を含む、請求項1記載の方法。
【請求項６】
前記改ざん検出器の前記所定の改ざんシグネチャが1つまたは複数の前記高価値領域の画像のぼけまたはオクルージョンを含む、請求項1記載の方法。
【請求項７】
前記固有の画素特徴の組合せが、
物理的および/または電子的改ざんの証拠となる1つまたは複数の画素特徴と、
改ざんされていない画像取込みおよび処理操作の証拠となる、1つまたは複数の無害な画素特徴と
を含む、請求項1記載の方法。
【請求項８】
前記第1の改ざんされていないデジタル画像のセットが、異なる密度のセキュリティ特徴または異なるレイアウトデザインのうち少なくとも一つを有する異なる形式の個人の身元信用証明書を表す複数の画像を含む、請求項1記載の方法。
【請求項９】
前記第1の改ざんされていないデジタル画像のセットが、以下のうち少なくとも一つを含む、請求項1記載の方法：
異なる照明条件の下で取り込まれた複数の画像、
異なる撮像装置で取り込まれた複数の画像、
同じ物理的信用証明書を表す一連のデジタル画像であって、前記一連のデジタル画像の各々が、異なる回転の度合いで方向決めされている、前記一連のデジタル画像、
ランダムに縮尺変更された複数の画像、または、
ランダムに導入されたデジタルノイズを含む複数の画像。
【請求項１０】
前記第2の電子的に改ざんされた画像のセットが、前記第1のセットの改ざんされていない各画像の前記画素配列の1つまたは複数の部分を改変することによって導出され、前記

改変が前記改ざん検出器の前記改ざんシグネチャに基づいて決定される、請求項1記載の方法。

【請求項１１】

前記第2の改ざんされた画像のセットが、物理的信用証明書を物理的改ざん方法を用いて手動で改変し、続いて物理的に改変された信用証明書を電子的に画像化することによって導出され、前記第2の物理的に改変された改ざんされた画像のセットが、前記物理的改ざんをマスクするために画素レベルでさらに改変される、請求項1記載の方法。

【請求項１２】

前記第2の改ざんされた画像のセットが、摩耗、損傷、デザインの欠陥、または意図的な物理的改変のうち少なくとも一つを含む物理的使用特性を有する物理的信用証明書から導出される、請求項1記載の方法。

【請求項１３】

前記第2の改ざんされた画像のセットが、元のデジタル画像化イベントからの照明、焦点面に対する角度、スキュー、回転、ぼけを有する元の未補正画像から導出される、請求項1記載の方法。

【請求項１４】

前記第2の改ざんされた画像のセットが、エンハンスメントされた補正画像から導出される、請求項1記載の方法。

【請求項１５】

前記訓練データセットの複数のデジタル画像が、改変された主成分を有する画素配列を含む、請求項1記載の方法。

【請求項１６】

前記予測モデルが確率的分類器を含み、前記出力が前記デジタル画像の分類および確度を含み、前記デジタル画像が改ざんされているかどうかを判定することが、前記確度を所定の閾値と比較することを含む、請求項1記載の方法。

【請求項１７】

前記予測モデルが、多層ノードベースアーキテクチャを有する畳み込みニューラルネットワーク分類器を含み、前記分類器が、マルチクラスデータ層を含む出力層を有する、請求項1記載の方法。

【請求項１８】

前記画素配列を解析することが、

関心領域を前記画素配列のサブセットとして識別することと、

前記関心領域のために調整および訓練された、前記識別された関心領域のみに関する改ざん検出アルゴリズムを実施することと

を含む、請求項1記載の方法。

【請求項１９】

前記画素配列を解析することが、

関心領域を前記画素配列のサブセットとして識別することと、

前記識別された関心領域に関して、異なる改ざんシグネチャに基づく複数の改ざん検出器を実施することと

を含み、

デジタル画像が改ざんされているかどうかを判定することが、前記複数の改ざん検出器からのそれぞれの出力に複数の独立した閾値を適用することを含む、

請求項1記載の方法。

【請求項２０】

前記画素配列を解析することが、

複数の関心領域を前記画素配列のサブセットとして識別することと、

前記関心領域の各々に関して、1つまたは複数の異なる改ざん検出アルゴリズムの組合せを実施することと

を含む、請求項1記載の方法。

【請求項２１】
デジタル画像が改ざんされているかどうかを判定することが、
各関心領域について、複数の改ざん確率を決定するために前記1つまたは複数の改ざん検出器からのそれぞれの改ざん出力に複数の独立した閾値を適用することと、
各関心領域について、領域レベルの改ざん確率を決定するために前記複数の改ざん確率を集計することと、
文書レベルの改ざん確率を決定するために前記複数の領域の前記領域レベルの改ざん確率を集計することと
を含む、請求項1記載の方法。
【請求項２２】
前記受け取られるデジタル画像によって表された前記物理的信用証明書が1つまたは複数の物理的に埋め込まれたセキュリティ特徴を含み、前記改ざん検出器が、前記表された物理的信用証明書に埋め込まれた前記セキュリティ特徴に依存しない前記画素レベルの解析を行うようにさらに構成される、請求項1記載の方法。
【請求項２３】
1つまたは複数のプロセッサによって実行されると、画像化された物理的信用証明書の電子的または物理的改ざんを検出するための操作を前記1つまたは複数のプロセッサに行わせる命令が格納されている、前記1つまたは複数のプロセッサに結合された非一時的コンピュータ可読記憶媒体であって、前記操作が、
識別データを含む1つまたは複数の高価値領域を有する物理的信用証明書を表す、画素配列を含むデジタル画像を受け取ること;
所定の改ざんシグネチャに関して前記デジタル画像の前記高価値領域の画素レベルの解析を行うように構成された改ざん検出器で、前記デジタル画像を処理し、前記デジタル画像の固有の特性に対応する出力を生成すること;および
前記改ざん検出器からの前記出力に基づいて、前記デジタル画像が電子的に改ざんされているかどうかを判定すること
を含む、非一時的コンピュータ可読記憶媒体であって、
前記改ざん検出器が、訓練データセットを適用する機械学習アルゴリズムによって訓練された予測モデルを含み、
前記訓練データセットが、
複数の固有の画素特徴の組合せを含む、第1の改ざんされていないデジタル画像のセットと、
前記改ざんされていないデジタル画像のうちの1つまたは複数の電子的に改ざんされた派生物を含む、第2のデジタル画像のセットと
を含み、
前記第1のセットの前記改ざんされていないデジタル画像の各々が前記訓練データセットにおいて第1の共通ラベルを割り当てられており、前記第2のセットの前記改ざんされたデジタル画像の各々が前記訓練データセットにおいて第2の共通ラベルを割り当てられており、前記第2のラベルが前記第1のラベルとは異なる、
前記非一時的コンピュータ可読記憶媒体。
【請求項２４】
コンピューティングデバイスと、
前記コンピューティングデバイスによって実行されると、画像化された物理的信用証明書の電子的または物理的改ざんを検出するための操作を前記コンピューティングデバイスに行わせる命令が格納されている、前記コンピューティングデバイスに結合されたコンピュータ可読記憶装置であって、前記操作が、
識別データを含む1つまたは複数の高価値領域を有する物理的信用証明書を表す、画素配列を含むデジタル画像を受け取ること;
所定の改ざんシグネチャに関して前記デジタル画像の前記高価値領域の画素レベルの解析を行うように構成された改ざん検出器で、前記デジタル画像を処理し、前記デジタル

画像の固有の特性に対応する出力を生成すること;および
　前記改ざん検出器からの前記出力に基づいて、前記デジタル画像が電子的に改ざんされているかどうかを判定すること
を含む、コンピュータ可読記憶装置と
を含む、システムであって、
前記改ざん検出器が、訓練データセットを適用する機械学習アルゴリズムによって訓練された予測モデルを含み、
前記訓練データセットが、
複数の固有の画素特徴の組合せを含む、第1の改ざんされていないデジタル画像のセットと、
前記改ざんされていないデジタル画像のうちの1つまたは複数の電子的に改ざんされた派生物を含む、第2のデジタル画像のセットと
を含み、
前記第1のセットの前記改ざんされていないデジタル画像の各々が前記訓練データセットにおいて第1の共通ラベルを割り当てられており、前記第2のセットの前記改ざんされたデジタル画像の各々が前記訓練データセットにおいて第2の共通ラベルを割り当てられており、前記第2のラベルが前記第1のラベルとは異なる、
前記システム。

【発明の詳細な説明】

【技術分野】

【０００１】

関連出願の相互参照

本出願は、その全体が参照により本明細書に組み入れられる、2016年10月14日に出願された、「Tamper Detection For Identification Documents」という名称の米国特許出願第62/408531号の米国特許法第119条（ｅ）による恩典を主張する。

【０００２】

技術分野

本明細書は一般に、改ざんされた身分証明書を検出するためのシステムおよび方法に関する。

【背景技術】

【０００３】

背景

物理的な身分証明書の使用は、何十年にもわたって様々な業界で広く浸透している。さらに、近年では、身分証明書のデジタル画像がセキュアな電子取引を行うためにますます使用されるようになっている。画像化された身分証明書を認証するための現在の技術は、基になっている文書に物理的に埋め込まれた特定のセキュリティ特徴を精査するように構成されたシステムを含む。これらのセキュリティ特徴は、意図的に、複製がきわめて困難であるようにされているので、文書の偽造コピーを作成しようとする試みを事実上食い止める。現在使用されている多くのセキュリティ特徴には、複雑な印刷パターン、電子透かし、マイクロプリントテキスト、固有のエンブレムまたはロゴ、ホログラムなどが含まれる。これらの画像化された身分証明書を処理するための従来の認証技術は、電子透かしから情報を系統的に復号すること、および/またはテキストマッチング技術もしくはパターンマッチング技術を用いて1つもしくは複数の他のセキュリティ特徴の正当性を検証することによって行われる。

【発明の概要】

【０００４】

概要

本明細書では、改ざんされた身分証明書をデジタル画像に基づいて検出するための技術について説明する。より具体的には、本明細書に記載されるある特定の態様は、デジタル画像に固有であり、かつ、例えば、抽出されたテキスト（光学式文字認識によって識別さ

れたテキストなど）または他の符号化データ（セキュリティ特徴または機械可読領域において符号化されたデータなど）と関連付けられていない、1つまたは複数の様相に基づいて、身分証明書の電子的または物理的改ざんを検出するための技術を含む。そのような様相は、物理的および/または電子的改ざんの証拠となる画素特徴、ならびに、環境、取込装置、信用証明書の摩耗、照明の影響、ハードウェア/ソフトウェア量子化、および/またはデジタル圧縮の影響を含むがこれらに限定されない特定の無害な画素特徴を含む。いくつかの例では、これらの改ざん検出技術は、1つまたは複数の特定の関心領域、例えば身分証明書の高価値識別領域に適用される。

【０００５】

身分証明書のデジタル画像は、本開示で論じられるように、電子取引での使用に適した物理的信用証明書のデジタル画像である。「電子取引」という用語は、物理的なまたは画像化された身分証明書の所有者と1または複数の第三者との間の、コンピュータによって促進される任意の交換を広く指す。電子取引は、対面して、またはコンピュータネットワークを介して遠隔で、行うことができる。電子取引の中には通貨の交換を含むものもあるし、含まないものもある。セキュアな電子取引を行うのに適した身分証明書には、個人の識別情報、雇用もしくは職業上の信用証明書もしくは証明書、または他の高価値の身元提示文書、例えば運転免許証もしくはパスポートが含まれ得るが、これに限定されない。さらに、いくつかの実施態様では、適切な身分証明書には、いわゆる「ブリーダ書類」（出生証明書、結婚証明書、社会保障文書、ならびに公共料金請求書、サービス請求書、および他の生活データ相関文書など）が含まれ得る。「身分証明書」および「物理的信用証明書」という用語は、識別データを含む身元の証明、確認、または認証のために設計された任意の文書を指す場合に本開示全体を通して区別なく使用され得る。「識別データ」は、以下の1つまたは複数を含み得る:身分証明写真、人物情報（生年月日、識別シリアル番号、社会保障番号、物理的な郵送先住所もしくは電子的なメールアドレス、身長、目の色、性別など）および/または1つもしくは複数の機械可読領域（MRZ）（バーコードもしくはQコードなど）。いくつかの実施態様では、識別データは、ID写真に加えて、指紋、掌形、網膜パターン、虹彩パターン、筆跡パターン、および/または他の物理的な形態学的識別特性などの他のバイオメトリック情報をさらに含み得る。この識別データを含む画像化された身分証明書の領域は、電子取引において文書の所有者を識別する際に重要であるため、本開示全体を通してこれらを一般に「高価値領域」と呼ぶ。

【０００６】

本開示の1つまたは複数の態様は、画像化された身分証明書を認証するための従来の技術が、実施することが困難であり、失敗しやすく、かつ/または重大なセキュリティ脆弱性を抱えているという認識の結果として得られたものである。一例として、セキュリティ特徴に依拠した認証技術は、それらが物理的身分証明書に対する改変を必要とするため、大規模に実施することが困難であり得る。これは各所有者に信用証明書を再発行することを意味する。これらの改変は、大量の物理的信用証明書、例えばパスポートおよび運転免許証の全体に広まるまでに長い時間を要する可能性がある。というのも、ユーザがこれらの証明書をあまり頻繁に交換しない傾向があるからである。よって、例えば、各文書に符号化データを埋め込むことを必要とする電子透かしシステムを完全に実施するのには何年もかかることになり得る。これらの従来の認証技術にはまた、失敗しやすい可能性もある。というのも、復号化および/またはテキスト/パターン認識ルーチンが、身分証明書を非常に特別な照明条件および/または位置合わせの向きで画像化することを必要とするからである。適切に画像を取り込むためにユーザはしばしば何回も試みる必要がある。さらに重要なことに、従来のセキュリティ特徴は偽造の成功を阻止または防止するのに有効ではあり得るが、真正に発行された物理的身分証明書が電子的にまたは手動で改ざんされているかどうかを検出するのには役に立たない。例えば、本物の身分証明書の所有者は、電子取引において所有者を識別するのに重要な特定の高価値領域（写真、バイオメトリック、人物情報（biography）、MRZなど）を差し替えるまたは変更することによってその文書を改ざんすることができる。

【０００７】
この種の改ざんは多くの場合（例えば、セキュリティ特徴が身分証明書の高価値領域に重なっていない場合には）埋め込まれたセキュリティ特徴に影響を与えずに成し遂げることができ、よって、従来の認証技術によって検出されず、文書所有者が、自分の身元を秘匿するために重要な情報を隠ぺいまたは完全に差し替えることを許すことになる。さらに、市販の画像編集ソフトウェアを使用して、高価値領域を含む身分証明書の非セキュリティ特徴の様相を操作することは比較的簡単である。当然ながら、身分証明書を改ざんしようとする試みは、その種類および洗練度が様々に異なる傾向がある。低い洗練度では、テクスチャまたはフォントを一致させようと試みることなく身分証明書の全領域が（電子的または物理的に）変更または差し替えられ得る。他の試みはより洗練されたものであり得る。例えば、偽造者が特殊なソフトウェアを利用して、背景、セキュリティ特徴などを細部にわたって再現しようと試みる場合もある。さらに別の例として、偽造者が、継ぎ合わせまたは改ざん済みのもののプリントアウトまたはスクリーンショットの新しいライブ写真を撮影することによって画像の改変部分を均質化しようとする場合もある。これらおよび無数の他の改ざん技術を使用して、従来の認証方法を効果的に弱体化させることが可能である。

【０００８】
したがって、本開示の態様は、画像化された身分証明書の正当性を検証するためにセキュリティ特徴のみに頼らない当分野における根本的なパラダイムシフトを提供することによって、従来の認証技術に伴う上記およびその他の問題を解決することを目的とする。特に、本開示は、画像化された身分証明書の特定の高価値領域内およびその周りの固有の画像特性を検証するための技術に関する。以下の考察に鑑みて明らかになるように、本開示の従来と異なる技術は、セキュリティ特徴が所定のパターンまたは符号化データに基づいて精査されない限り、それらのセキュリティ特徴にはどちらかといえば依存しない。さらに、特定の種類の身分証明書では、埋め込まれたセキュリティ特徴が部分的にまたは完全に高価値関心領域に重なっていてもよいことを理解されたい。そのような重なりが存在しない場合には、本明細書に記載される技術は、文書の完全性の唯一の保証としての機能を果たし得る。重なっている場合には、本開示の技術は、それらのセキュリティ特徴が文書に本来備わったものであり、改変された高価値領域（複数可）上に偽造されたものでも、全く同じ種類の別の文書から盗用されたものでもないことを保証することによって、それらのセキュリティ特徴に付加価値を与える。

【０００９】
一般に、本明細書に記載される主題の1つの革新的な局面は、1つまたは複数の高価値領域を有する物理的信用証明書を表す、画素配列を含むデジタル画像を受け取る動作と、所定の改ざんシグネチャに関してデジタル画像の高価値領域の画素レベルの解析を行うように構成された改ざん検出器で、デジタル画像を処理し、デジタル画像の固有の特性に対応する出力を生成する動作と、改ざん検出器からの出力に基づいて、デジタル画像が電子的に改ざんされているかどうかを判定する動作とを含む方法において具体化することができる。

【００１０】
この局面の他の態様は、本方法の動作を行うように各々構成された、対応するコンピュータシステム、装置、および1つまたは複数のコンピュータ記憶装置上に記録されたコンピュータプログラムを含む。1つまたは複数のコンピュータのシステムが特定の操作または動作を行うように構成されるとは、作動中にシステムにそれらの操作または動作を行わせるソフトウェア、ファームウェア、ハードウェア、またはそれらの組合せがシステムにインストールされていることを意味する。1つまたは複数のコンピュータプログラムが特定の操作または動作を行うように構成されるとは、データ処理装置によって実行されるとそれらの操作または動作を装置に行わせる命令を、1つまたは複数のプログラムが含むことを意味する。

【００１１】

上記およびその他の態様は、単独でまたは組み合わせて、以下の特徴のうちの1つまたは複数を各々任意で含むことができる。特に、一態様は、以下のすべての特徴を組み合わせて含む。さらに、いくつかの例では、画素レベルの解析は、複数の固有の画素特徴の組合せの検査を含む。いくつかの例では、固有の画素特徴の組合せは、物理的および/または電子的改ざんの証拠となる1つまたは複数の画素特徴と、環境、取込装置、信用証明書の摩耗、照明の影響、ハードウェア/ソフトウェア量子化、および/またはデジタル圧縮の影響を含む、1つまたは複数の無害な画素特徴とを含む。

【００１２】

いくつかの例では、受け取られるデジタル画像の高価値領域は人物情報テキストを含み、改ざん検出器の所定の改ざんシグネチャは人物情報の継ぎ合わせまたは他の改変を含む。いくつかの例では、受け取られるデジタル画像の高価値領域はバイオメトリックデータを含み、改ざん検出器の所定の改ざんシグネチャは写真の継ぎ合わせまたは他の改変を含む。いくつかの例では、バイオメトリックデータは身分証明写真を含む。いくつかの例では、受け取られるデジタル画像の高価値領域は機械可読領域（MRZ）を含み、改ざん検出器の所定の改ざんシグネチャはMRZの継ぎ合わせまたは他の改変を含む。いくつかの例では、改ざん検出器の所定の改ざんシグネチャは、1つまたは複数の高価値領域の画像のぼけまたはオクルージョンを含む。

【００１３】

いくつかの例では、改ざん検出器は、訓練データセットを適用する機械学習アルゴリズムによって訓練された予測モデルを含む。いくつかの例では、訓練データセットは、第1の改ざんされていないデジタル画像のセットと、1つまたは複数の改ざんされていないデジタル画像の電子的に改ざんされた派生物を含む、第2のデジタル画像のセットとを含む。第1のセットの改ざんされていないデジタル画像の各々は、訓練データセットにおいて第1の共通ラベルを割り当てられており、第2のセットの改ざんされたデジタル画像の各々は、訓練データセットにおいて第2の共通ラベルを割り当てられており、第2のラベルは第1のラベルとは異なる。

【００１４】

いくつかの例では、第1の改ざんされていないデジタル画像のセットは、複数の固有の画素特徴の組合せの検査を誘導するために選択される。いくつかの例では、固有の画素特徴の組合せは、物理的および/または電子的改ざんの証拠となる1つまたは複数の画素特徴と、環境、取込装置、信用証明書の摩耗、照明の影響、ハードウェア/ソフトウェア量子化、および/またはデジタル圧縮の影響を含む、1つまたは複数の無害な画素特徴とを含む。いくつかの例では、第1の改ざんされていないデジタル画像のセットは、異なる形式の個人の身元信用証明書を表す複数の画像を含む。いくつかの例では、異なる形式の個人の身元信用証明書は、異なる密度のセキュリティ特徴を含む。いくつかの例では、異なる形式の個人の身元信用証明書は、異なるレイアウトデザインを含む。いくつかの例では、第1の改ざんされていないデジタル画像のセットは、異なる照明条件の下で取り込まれた複数の画像を含む。いくつかの例では、第1の改ざんされていないデジタル画像のセットは、異なる撮像装置で取り込まれた複数の画像を含む。いくつかの例では、第1の改ざんされていないデジタル画像のセットは、同じ物理的信用証明書を表す一連のデジタル画像を含み、一連のデジタル画像の各々は、異なる回転の度合いで方向決めされている。いくつかの例では、第1の改ざんされていないデジタル画像のセットは、ランダムに縮尺変更された複数の画像を含む。いくつかの例では、第1の改ざんされていないデジタル画像のセットは、ランダムに導入されたデジタルノイズを含む複数の画像を含む。いくつかの例では、第2の電子的に改ざんされた画像のセットは、第1のセットの改ざんされていない各画像の画素配列の1つまたは複数の部分を自動的に改変することによって導出され、改変は改ざん検出器の改ざんシグネチャに基づいて決定される。いくつかの例では、第2の改ざんされた画像のセットは、物理的改ざん方法を用いて物理的信用証明書を手動で改変し、続いて物理的に改変された信用証明書を電子的に画像化することによって導出される。いくつかの例では、第2の物理的に改変された改ざんされた画像のセットは、物理的改ざん

をマスクするためにデジタル編集ツールを用いて画素レベルでさらに改変される。いくつかの例では、第2の改ざんされた画像のセットは、物理的使用特性が視覚的に顕著である物理的信用証明書上に手動でまたは自動的に生成された物理的または改ざんから導出される。いくつかの例では、視覚的に顕著な使用特性は、摩耗、損傷、デザインの欠陥、または意図的な物理的改変を含む。いくつかの例では、第2の改ざんされた画像のセットは、元のデジタル画像化イベントからの特有の照明、焦点面に対する角度、スキュー、回転、ぼけを有する元の未補正画像から導出される。いくつかの例では、第2の改ざんされた画像のセットは、改ざん前に、縦方向または横方向の、エッジにおいて0度または90度に向いた文書印刷の向きと一致するよう傾けられ、スキューが適正な縦横比に補正され、ぼけおよび照明およびその他の影響が補正およびエンハンスメントされた、エンハンスメントされた補正画像から導出される。

【００１５】

いくつかの例では、訓練データセットの複数のデジタル画像は、改変された主成分を有する画素配列を含む。いくつかの例では、予測モデルは確率的分類器を含み、出力はデジタル画像の分類および確度を含む。いくつかの例では、デジタル画像が改ざんされているかどうかを判定することは、確度を所定の閾値と比較することを含む。

【００１６】

いくつかの例では、予測モデルは、多層ノードベースアーキテクチャを有する畳み込みニューラルネットワーク分類器を含み、分類器の出力層はマルチクラスデータ層を含む。

【００１７】

いくつかの例では、画素配列を解析することは、関心領域を画素配列のサブセットとして識別する動作と、当該関心領域のために調整および訓練された、識別された関心領域のみに関する改ざん検出アルゴリズムを実施する動作とを含む。いくつかの例では、画素配列を解析することは、関心領域を画素配列のサブセットとして識別する動作と、識別された関心領域に関して、異なる改ざんシグネチャに基づく複数の改ざん検出器を実施する動作とを含む。いくつかの例では、デジタル画像が改ざんされているかどうかを判定することは、複数の改ざん検出器からのそれぞれの出力に複数の独立した閾値を適用することを含む。いくつかの例では、画素配列を解析することは、複数の関心領域を画素配列のサブセットとして識別する動作と、関心領域の各々に関して、1つまたは複数の異なる改ざん検出アルゴリズムの独特な組合せを実施する動作とを含む。いくつかの例では、デジタル画像が改ざんされているかどうかを判定することは、各関心領域について、複数の改ざん確率を決定するために、1つまたは複数の改ざん検出器からのそれぞれの改ざん出力に複数の独立した閾値を適用する動作と、各関心領域について、領域レベルの改ざん確率を決定するために複数の改ざん確率を集計する動作と、文書レベルの改ざん確率を決定するために複数の領域の領域レベルの改ざん確率を集計する動作とを含む。

【００１８】

いくつかの例では、受け取られるデジタル画像によって表された物理的信用証明書は、1つまたは複数の物理的に埋め込まれたセキュリティ特徴を含み、改ざん検出器は、表された物理的信用証明書に埋め込まれたセキュリティ特徴に依存しない画素レベルの解析を行うようにさらに構成される。

【００１９】

［本発明１００１］

画像化された物理的信用証明書の電子的または物理的改ざんを検出するためのコンピュータ実装方法であって、1つまたは複数のプロセッサを使用して実行され、以下の工程:

1つまたは複数の高価値領域を有する物理的信用証明書を表す、画素配列を含むデジタル画像を受け取る工程;

所定の改ざんシグネチャに関して前記デジタル画像の前記高価値領域の画素レベルの解析を行うように構成された改ざん検出器で、前記デジタル画像を処理し、前記デジタル画像の固有の特性に対応する出力を生成する工程;および

前記改ざん検出器からの前記出力に基づいて、前記デジタル画像が電子的に改ざんされ

ているかどうかを判定する工程
を含む、コンピュータ実装方法。
［本発明１００２］
1つまたは複数のプロセッサによって実行されると、画像化された物理的信用証明書の電子的または物理的改ざんを検出するための操作を前記1つまたは複数のプロセッサに行わせる命令が格納されている、前記1つまたは複数のプロセッサに結合された非一時的コンピュータ可読記憶媒体であって、前記操作が、
1つまたは複数の高価値領域を有する物理的信用証明書を表す、画素配列を含むデジタル画像を受け取ること;
所定の改ざんシグネチャに関して前記デジタル画像の前記高価値領域の画素レベルの解析を行うように構成された改ざん検出器で、前記デジタル画像を処理し、前記デジタル画像の固有の特性に対応する出力を生成すること;および
前記改ざん検出器からの前記出力に基づいて、前記デジタル画像が電子的に改ざんされているかどうかを判定すること
を含む、非一時的コンピュータ可読記憶媒体。
［本発明１００３］
コンピューティングデバイスと、
前記コンピューティングデバイスによって実行されると、画像化された物理的信用証明書の電子的または物理的改ざんを検出するための操作を前記コンピューティングデバイスに行わせる命令が格納されている、前記コンピューティングデバイスに結合されたコンピュータ可読記憶装置であって、前記操作が、
1つまたは複数の高価値領域を有する物理的信用証明書を表す、画素配列を含むデジタル画像を受け取ること;
所定の改ざんシグネチャに関して前記デジタル画像の前記高価値領域の画素レベルの解析を行うように構成された改ざん検出器で、前記デジタル画像を処理し、前記デジタル画像の固有の特性に対応する出力を生成すること;および
前記改ざん検出器からの前記出力に基づいて、前記デジタル画像が電子的に改ざんされているかどうかを判定すること
を含む、コンピュータ可読記憶装置と
を含む、システム。
［本発明１００４］
前記画素レベルの解析が複数の固有の画素特徴の組合せの検査を含む、前記本発明のいずれか一つの方法、記憶媒体、またはシステム。
［本発明１００５］
前記固有の画素特徴の組合せが、
物理的および/または電子的改ざんの証拠となる1つまたは複数の画素特徴と、
環境、取込装置、信用証明書の摩耗、照明の影響、ハードウェア/ソフトウェア量子化、および/またはデジタル圧縮の影響を含む、1つまたは複数の無害な画素特徴と
を含む、本発明1004の方法、記憶媒体、またはシステム。
［本発明１００６］
前記受け取られるデジタル画像の高価値領域が人物情報（biographical）テキストを含み、前記改ざん検出器の前記所定の改ざんシグネチャが人物情報の継ぎ合わせまたは他の改変を含む、前記本発明のいずれか一つの方法、記憶媒体、またはシステム。
［本発明１００７］
前記受け取られるデジタル画像の高価値領域がバイオメトリックデータを含み、前記改ざん検出器の前記所定の改ざんシグネチャが写真の継ぎ合わせまたは他の改変を含む、前記本発明のいずれか一つの方法、記憶媒体、またはシステム。
［本発明１００８］
前記バイオメトリックデータが身分証明写真を含む、本発明1007の方法、記憶媒体、またはシステム。

［本発明１００９］
前記受け取られるデジタル画像の高価値領域が機械可読領域（MRZ）を含み、前記改ざん検出器の前記所定の改ざんシグネチャがMRZの継ぎ合わせまたは他の改変を含む、前記本発明のいずれか一つの方法、記憶媒体、またはシステム。
［本発明１０１０］
前記改ざん検出器の前記所定の改ざんシグネチャが1つまたは複数の前記高価値領域の画像のぼけまたはオクルージョンを含む、前記本発明のいずれか一つの方法、記憶媒体、またはシステム。
［本発明１０１１］
前記改ざん検出器が、訓練データセットを適用する機械学習アルゴリズムによって訓練された予測モデルを含む、前記本発明のいずれか一つの方法、記憶媒体、またはシステム。
［本発明１０１２］
前記訓練データセットが、
第1の改ざんされていないデジタル画像のセットと、
前記改ざんされていないデジタル画像のうちの1つまたは複数の電子的に改ざんされた派生物を含む、第2のデジタル画像のセットと
を含み、
前記第1のセットの前記改ざんされていないデジタル画像の各々が前記訓練データセットにおいて第1の共通ラベルを割り当てられており、前記第2のセットの前記改ざんされたデジタル画像の各々が前記訓練データセットにおいて第2の共通ラベルを割り当てられており、前記第2のラベルが前記第1のラベルとは異なる、本発明1011の方法、記憶媒体、またはシステム。
［本発明１０１３］
前記第1の改ざんされていないデジタル画像のセットが、複数の固有の画素特徴の組合せの検査を誘導するために選択される、本発明1012の方法、記憶媒体、またはシステム。
［本発明１０１４］
前記固有の画素特徴の組合せが、
物理的および/または電子的改ざんの証拠となる1つまたは複数の画素特徴と、
環境、取込装置、信用証明書の摩耗、照明の影響、ハードウェア/ソフトウェア量子化、および/またはデジタル圧縮の影響を含む、1つまたは複数の無害な画素特徴と
を含む、本発明1012または本発明1013の方法、記憶媒体、またはシステム。
［本発明１０１５］
前記第1の改ざんされていないデジタル画像のセットが、異なる形式の個人の身元信用証明書を表す複数の画像を含む、本発明1012～1014のいずれか一つの方法、記憶媒体、またはシステム。
［本発明１０１６］
前記異なる形式の個人の身元信用証明書が異なる密度のセキュリティ特徴を含む、本発明1015の方法、記憶媒体、またはシステム。
［本発明１０１７］
前記異なる形式の個人の身元信用証明書が異なるレイアウトデザインを含む、本発明1015または本発明1016の方法、記憶媒体、またはシステム。
［本発明１０１８］
前記第1の改ざんされていないデジタル画像のセットが、異なる照明条件の下で取り込まれた複数の画像を含む、本発明1012～1017のいずれか一つの方法、記憶媒体、またはシステム。
［本発明１０１９］
前記第1の改ざんされていないデジタル画像のセットが、異なる撮像装置で取り込まれた複数の画像を含む、本発明1012～1018のいずれか一つの方法、記憶媒体、またはシステム。

［本発明１０２０］
前記第1の改ざんされていないデジタル画像のセットが、同じ物理的信用証明書を表す一連のデジタル画像を含み、前記一連のデジタル画像の各々が、異なる回転の度合いで方向決めされている、本発明1012～1019のいずれか一つの方法、記憶媒体、またはシステム。
［本発明１０２１］
前記第1の改ざんされていないデジタル画像のセットが、ランダムに縮尺変更された複数の画像を含む、本発明1012～1020のいずれか一つの方法、記憶媒体、またはシステム。
［本発明１０２２］
前記第1の改ざんされていないデジタル画像のセットが、ランダムに導入されたデジタルノイズを含む複数の画像を含む、本発明1012～1021のいずれか一つの方法、記憶媒体、またはシステム。
［本発明１０２３］
前記第2の電子的に改ざんされた画像のセットが、前記第1のセットの改ざんされていない各画像の前記画素配列の1つまたは複数の部分を自動的に改変することによって導出され、前記改変が前記改ざん検出器の前記改ざんシグネチャに基づいて決定される、本発明1012～1022のいずれか一つの方法、記憶媒体、またはシステム。
［本発明１０２４］
前記第2の改ざんされた画像のセットが、前記第1のセットの改ざんされていない各画像の前記画素配列の1つまたは複数の部分をデジタル編集ツールを介して手動で改変することによって導出され、前記改変が前記改ざん検出器の改ざん関心領域に基づいて決定される、本発明1012～1023のいずれか一つの方法、記憶媒体、またはシステム。
［本発明１０２５］
前記第2の改ざんされた画像のセットが、物理的信用証明書を物理的改ざん方法を用いて手動で改変し、続いて物理的に改変された信用証明書を電子的に画像化することによって導出される、本発明1012～1024のいずれか一つの方法、記憶媒体、またはシステム。
［本発明１０２６］
前記第2の物理的に改変された改ざんされた画像のセットが、前記物理的改ざんをマスクするためにデジタル編集ツールを用いて画素レベルでさらに改変される、本発明1025の方法、記憶媒体、またはシステム。
［本発明１０２７］
前記第2の改ざんされた画像のセットが、物理的使用特性が視覚的に顕著である物理的信用証明書上に手動でまたは自動的に生成された物理的または改ざんから導出される、本発明1012～1026のいずれか一つの方法、記憶媒体、またはシステム。
［本発明１０２８］
前記視覚的に顕著な使用特性が、摩耗、損傷、デザインの欠陥、または意図的な物理的改変を含む、本発明1027の方法、記憶媒体、またはシステム。
［本発明１０２９］
前記第2の改ざんされた画像のセットが、元のデジタル画像化イベントからの特有の照明、焦点面に対する角度、スキュー、回転、ぼけを有する元の未補正画像から導出される、本発明1012～1028のいずれか一つの方法、記憶媒体、またはシステム。
［本発明１０３０］
前記第2の改ざんされた画像のセットが、改ざん前に、縦方向または横方向の、エッジにおいて0度または90度に向いた文書印刷の向きと一致するよう傾けられ、スキューが適正な縦横比に補正され、ぼけおよび照明およびその他の影響が補正およびエンハンスメントされた、エンハンスメントされた補正画像から導出される、本発明1012～1029のいずれか一つの方法、記憶媒体、またはシステム。
［本発明１０３１］
前記訓練データセットの複数のデジタル画像が、改変された主成分を有する画素配列を含む、本発明1011～1030のいずれか一つの方法、記憶媒体、またはシステム。

［本発明１０３２］
前記予測モデルが確率的分類器を含み、前記出力が前記デジタル画像の分類および確度を含む、本発明1011～1031のいずれか一つの方法、記憶媒体、またはシステム。
［本発明１０３３］
前記デジタル画像が改ざんされているかどうかを判定することが、前記確度を所定の閾値と比較することを含む、本発明1032の方法、記憶媒体、またはシステム。
［本発明１０３４］
前記予測モデルが、多層ノードベースアーキテクチャを有する畳み込みニューラルネットワーク分類器を含み、前記分類器の出力層がマルチクラスデータ層を含む、本発明1011～1033のいずれか一つの方法、記憶媒体、またはシステム。
［本発明１０３５］
前記画素配列を解析することが、
関心領域を前記画素配列のサブセットとして識別することと、
前記関心領域のために調整および訓練された、前記識別された関心領域のみに関する改ざん検出アルゴリズムを実施することと
を含む、前記本発明のいずれか一つの方法、記憶媒体、またはシステム。
［本発明１０３６］
前記画素配列を解析することが、
関心領域を前記画素配列のサブセットとして識別することと、
前記識別された関心領域に関して、異なる改ざんシグネチャに基づく複数の改ざん検出器を実施することと
を含む、前記本発明のいずれか一つの方法、記憶媒体、またはシステム。
［本発明１０３７］
デジタル画像が改ざんされているかどうかを判定することが、前記複数の改ざん検出器からのそれぞれの出力に複数の独立した閾値を適用することを含む、本発明1036の方法、記憶媒体、またはシステム。
［本発明１０３８］
前記画素配列を解析することが、
複数の関心領域を前記画素配列のサブセットとして識別することと、
前記関心領域の各々に関して、1つまたは複数の異なる改ざん検出アルゴリズムの独特な組合せを実施することと
を含む、前記本発明のいずれか一つの方法、記憶媒体、またはシステム。
［本発明１０３９］
デジタル画像が改ざんされているかどうかを判定することが、
各関心領域について、複数の改ざん確率を決定するために前記1つまたは複数の改ざん検出器からのそれぞれの改ざん出力に複数の独立した閾値を適用することと、
各関心領域について、領域レベルの改ざん確率を決定するために前記複数の改ざん確率を集計することと、
文書レベルの改ざん確率を決定するために前記複数の領域の前記領域レベルの改ざん確率を集計することと
を含む、本発明1038の方法、記憶媒体、またはシステム。
［本発明１０４０］
前記受け取られるデジタル画像によって表された前記物理的信用証明書が1つまたは複数の物理的に埋め込まれたセキュリティ特徴を含み、前記改ざん検出器が、前記表された物理的信用証明書に埋め込まれた前記セキュリティ特徴に依存しない前記画素レベルの解析を行うようにさらに構成される、前記本発明のいずれか一つの方法、記憶媒体、またはシステム。
本明細書の主題の1つまたは複数の態様の詳細は、添付の図面および以下の説明に記載されている。主題の他の特徴、局面、および利点は、それらの説明、図面、および特許請求の範囲を読めば明らかになるであろう。

【図面の簡単な説明】
【００２０】
【図１】画像分類器を生成するための例示的なシステムの図である。
【図２】画像分類器を訓練するための例示的なプロセスの流れ図である。
【図３】訓練画像を生成するための例示的なプロセスの流れ図である。
【図４】画像分類器を生成するための訓練フェーズを示すプロセス図である。
【図５】画像分類器を評価するための試験フェーズを示すプロセス図である。
【図６Ａ】図6A～6Fは、州の運転免許証の加工されていないデジタル画像および改ざんされたデジタル画像の説明図である。
【図６Ｂ】図6A～6Fは、州の運転免許証の加工されていないデジタル画像および改ざんされたデジタル画像の説明図である。
【図６Ｃ】図6A～6Fは、州の運転免許証の加工されていないデジタル画像および改ざんされたデジタル画像の説明図である。
【図６Ｄ】図6A～6Fは、州の運転免許証の加工されていないデジタル画像および改ざんされたデジタル画像の説明図である。
【図６Ｅ】図6A～6Fは、州の運転免許証の加工されていないデジタル画像および改ざんされたデジタル画像の説明図である。
【図６Ｆ】図6A～6Fは、州の運転免許証の加工されていないデジタル画像および改ざんされたデジタル画像の説明図である。
【図７Ａ】図7A～7Fは、自国のパスポートの加工されていないデジタル画像および改ざんされたデジタル画像の説明図である。
【図７Ｂ】図7A～7Fは、自国のパスポートの加工されていないデジタル画像および改ざんされたデジタル画像の説明図である。
【図７Ｃ】図7A～7Fは、自国のパスポートの加工されていないデジタル画像および改ざんされたデジタル画像の説明図である。
【図７Ｄ】図7A～7Fは、自国のパスポートの加工されていないデジタル画像および改ざんされたデジタル画像の説明図である。
【図７Ｅ】図7A～7Fは、自国のパスポートの加工されていないデジタル画像および改ざんされたデジタル画像の説明図である。
【図７Ｆ】図7A～7Fは、自国のパスポートの加工されていないデジタル画像および改ざんされたデジタル画像の説明図である。
【図８】画像化された身分証明書が改ざんされているかどうかを示す出力を提供するための例示的なシステムの図である。
【図９】画像化された身分証明書が改ざんされているかどうかを示す出力を提供するための例示的なプロセスの流れ図である。
【図１０Ａ】デジタル画像によって表された改ざんされた身分証明書と改ざんされていない身分証明書とを比較した図である。
【図１０Ｂ】デジタル画像化された身分証明書の様々な固有層を示す図である。
【００２１】
様々な図面中の同様の符番および名称は、同様の要素を示し得る。
【発明を実施するための形態】
【００２２】
詳細な説明
本開示の1つまたは複数の態様は、電子取引を行うために画像化されている改ざんされた身分証明書を検出するためのシステムおよび方法を含む。特に、ある特定の態様は、デジタル画像の固有の特性に対応する出力を生成するために改ざん検出器で物理的身分証明書のデジタル画像を処理することを含み得る。改ざん検出器は、所定の電子的および/または物理的改ざんシグネチャに関してデジタル画像の画素レベルの解析を行い得る。「画素レベルの解析」という用語は、デジタル画像中の個々の画素、または小さい画素グループのコンピュータ実装検査を指す。例えば、画素レベルの解析は、物理的および/または

電子的改ざんの証拠となるある特定の画素特徴、ならびに、環境、取込装置、信用証明書の摩耗、照明の影響、ハードウェア/ソフトウェア量子化、および/またはデジタル圧縮の影響を含むがこれらに限定されない特定の無害な画素特徴を検査し得る。これらの局面については以下で詳細に論じる。「改ざんシグネチャ」という用語は、改ざん検出器が検出するように構成されている特定の種類（複数可）の電子的または物理的改ざん、例えば画像継ぎ合わせ、MRZ継ぎ合わせ、人物情報継ぎ合わせ、および/またはぼかし/オクルージョンを指す。いくつかの例では、改ざん検出器は、表された物理的信用証明書に埋め込まれた特定のセキュリティ特徴に実質的に依存しない画素レベルの解析を行うように構成される。すなわち、改ざん検出器は、（例えば、セキュリティ特徴が身分証明書の特定の高価値領域に重なっている場合には）セキュリティ特徴を表す画像の画素を検査する場合もあるが、それらを検証するためにいかなる特定の復号化またはパターンマッチングルーチンも実施しない場合もある。

【００２３】

いくつかの態様では、改ざん検出器は訓練された画像分類器を含む。画像分類器は一般に、既定のラベルに従って画像を分類するために使用される。画像分類器は、画像に適合するかまたは部分的に適合する既定のラベルを識別し、次いで、識別されたラベルを画像と関連付けることができる。例えば、椅子に座っている猫の画像は、「猫」、「椅子」、またはその両方とラベル付けされ得る。いくつかの画像分類器では、画像は、画像コンテンツの広いカテゴリ、例えば動物または人間に従って、ラベル付けされ得る。他の画像分類器では、画像は狭いカテゴリ、例えばペルシャ猫またはベンガル猫に従って、ラベル付けされ得る。本開示のある特定の態様は、身分証明書の高価値領域が改ざんされているかどうかを判定するように特に構成された画像分類器の構築を含む。例えば、画像分類器は、デジタル画像化された身分証明書の画素レベルの解析から得られるいくつかの固有の特徴に基づいて、文書化された身分証明書の画像を「改ざんされた」または「改ざんされていない」としてラベル付けし得る。画像分類器は、訓練画像の集合から抽出された1つまたは複数の特徴に基づいて訓練することができる。訓練画像は、改ざんされたかまたは改ざんされていないかのどちらかであり、そのようにラベル付けされた様々な画像化された身分証明書の代表例である。本開示全体を通して論じるように、訓練画像の選択/作成およびラベル付けは、基となっている身分証明書に含まれる高価値領域データに関するこれらの画像内の固有の特徴の1つまたは複数の様相に基づいて、分類器アーキテクチャにおけるある特定の重みを最適化および/または強化するように、特に設計される。

【００２４】

いくつかの例では、訓練データを処理し、本明細書に記載される技術を可能にするための適切な画像分類器を構築するために、機械学習システムが使用され得る。これらの機械学習システムは、無数の独特な訓練例を受け取って処理することができ、各例は、物理的信用証明書内に埋め込まれたセキュリティ特徴とは切り離された別個の固有の特徴の特異な組合せを具体化する。画像分類器を開発するときには、例えばニューラルネットワークを含む様々なアーキテクチャが使用され得る。本明細書に記載されるいくつかの実施態様では、畳み込みニューラルネットワーク（「CNN」）または深層畳み込みニューラルネットワーク（「DCNN」）が使用され得る。

【００２５】

図1は、画像分類器106を生成するための例示的なシステム100の図である。画像分類器106は、識別データの特定の高価値領域と関連付けられた固有の特徴に基づいて、物理的信用証明書の改ざんされたデジタル画像と改ざんされていないデジタル画像とを区別するように適切に構成され得る。図示されているように、システム100は、訓練画像102の集合を受け取る分類器生成器104を含む。分類器生成器104は、訓練画像102を利用して画像分類器106を生成する。訓練画像102の集合は、「改ざんされた」とラベル付けされたポジティブなデジタル画像のグループと、「改ざんされていない」とラベル付けされたネガティブなデジタル画像のグループとを含む。ポジティブなおよびネガティブな（改ざんされたおよび改ざんされていない）デジタル画像には、人間のユーザが手動でラベル付けするか、

または訓練データ生成システムによって自動的にラベル付けすることができる。訓練画像102の集合を開発するための具体的な技術については、図6A～図7Fに関連して以下でより詳細に説明する。

【００２６】

この例では、分類器生成器104は、特徴抽出エンジン108、特徴インスタンス110、および分類器訓練エンジン112を含む。特徴抽出エンジン108は、受け取った訓練画像102から固有の特徴（例えば固有の画素特徴）を抽出する。いくつかの例では、特徴抽出エンジン108は、CNN（例えば、多様な画像の大規模な集合から生成された事前訓練済みCNN）を含み得る。いくつかの異なる種類の特徴が、物理的信用証明書のデジタル画像を示すものとして抽出される。例えば、抽出される特徴は、テキスト情報、写真のエッジ、写真のパターンなどを含むことができる。受け取った訓練画像102内の各デジタル画像からの抽出された特徴は、特徴インスタンス110の集合を形成する。これらの抽出された特徴は、分類器訓練エンジン112によって画像分類器を訓練するために使用される。すべての特徴が分類器訓練エンジン112に提供される必要はない。代わりに、特定の分類器用途、例えば訓練される画像分類器106の意図する改ざんシグネチャに応じて、特徴の異なる組合せを使用することができる。

【００２７】

いくつかの例では、抽出された固有の画素特徴は、画像取込照明に関する1つまたは複数の様相を含み得る。照明の様相は、異なる光源の構成（複数または単一）、光色/波長応答、入射角などによる画像化の影響を含み得る。いくつかの例では、抽出された画素特徴は、選択された画像取込装置に関する1つまたは複数の様相を含み得る。画像取込装置に関する様相は、異なる種類のイメージセンサ（電荷結合素子（CCD）、相補型金属酸化膜半導体（CMOS）、N型金属酸化膜半導体（NMOS）など）の使用による影響（ピクシレーション/解像度、ノイズ、製造欠陥など）を含み得る。いくつかの例では、抽出された画素特徴は、光学的レンズ作用に関する1つまたは複数の様相を含み得る。光学的レンズ作用の様相は、固定/可変焦点距離、魚眼、ならびに他の光学的レンズ作用の歪み（例えばレンズの損傷/汚れ）などの影響を含み得る。いくつかの例では、抽出された画素特徴は、特定の画像化環境に関する1つまたは複数の様相を含み得る。画像化環境の様相は、様々な背景および/または前景にわたる異なるイメージセンサによる色/強度/色相応答を含み得る。画像化環境の様相はまた、物理的/電子的推定を伴う複数/単一の焦点/焦点面、目標焦点面の二等分、および焦点面における前景/背景の影響を含み得る。いくつかの例では、抽出された画素特徴は、ハードウェアおよび/またはソフトウェア量子化に関する1つまたは複数の様相を含み得る。量子化の様相は、連続物理空間からの量子化空間における色空間レンダリング、様々な画像化ライブラリによる量子化および推定、ならびに圧縮画像フォーマットによるさらなる量子化/圧縮によって生み出される画像化の影響を含み得る。いくつかの例では、抽出された画素特徴は、カラーバランシング、画像エンハンスメント、ヒストグラム平坦化、複数の色空間/応答などといった、ソフトウェアで実施される自動の画像化後エンハンスメントに関する1つまたは複数の様相を含み得る。いくつかの例では、抽出された画素特徴は、フィルタ、変換などといった手動の画像化後改変に関する1つまたは複数の様相を含み得る。

【００２８】

抽出された固有の画素特徴に関する様々な様相について、図10Aおよび図10Bの考察によってさらに例示する。図10Aには、3つの画像、すなわち、第1の運転免許証の第1の改ざんされていない画像1000a、第2の運転免許証の第2の改ざんされていない画像1000b、および第1の画像1000aの写真および人物情報の領域を第2の画像1000bの対応する領域で差し替えるまたは「継ぎ合わせる」ことによって改ざんされている第3の画像1000cが示されている。図10Bには、第3の画像1000cの階層化された図が示されている。

【００２９】

図10Bの例では、「レイヤ0」（1002）は、正規の製造業者によって作成された元の完全な文書を表している。この層は、基となる身分証明書を、すべての可視光セキュリティ特

徴、高価値領域（バイオメトリック、人物情報、MRZなど）と共に、それが完全に画像化されたように含む。「レイヤ1」（1004）は、経時的に蓄積する可能性がある汚れおよび損傷を表している。これは、例えば、ラミネートの品質、使用、摩損などを含み得る。この層はまた、反射率（光沢または穿孔の度合いなど）および損傷（摩損、擦れ、亀裂、日光曝露による退色または汚れなど）を含む、信用証明書のラミネートまたは外面自体も表し得る。この層はまた、切断、穿孔、または表面へのステッカもしくはその他の製造後の材料の貼付（例えば、住所ステッカの交換、期限切れおよび交換に起因する機関による穿孔、データを偽るための意図的な物理的改ざん）を含む信用証明書の意図的な物理的改変も表し得る。一般に、この層は基となる文書の1つまたは複数の物理的様相に対応する。

【００３０】

「レイヤ2」（1006）は、画像取込みイベント中の照明および環境の影響を表している。照明の影響は、光源の数、光の強度および角度の度合い（例えば、光源に近づくほど明るく、離れるほど暗い）、色変化するセキュリティ特徴/ホログラムなどの光学的可変デバイス（「OVD」）の存在、光の色/色相/強度の度合いなどに関連し得る。環境の影響は、画像化された文書と背景との間のコントラスト、および他の同様の様相に関連し得る。「レイヤ3」（1008）はレンズ作用の影響および焦点距離を表している。例えば、魚眼は、文書がレンズに近すぎるか、またはレンズに対して斜めに位置決めされた場合に発生し得る。画像取込み時の向きにおけるこれらの不完全性はまた、焦点距離に関して問題を引き起こす可能性があり、その結果、レンズに対してより遠いまたはより近い文書の部分が部分的にぼやけることになる。一般に、この層は、画像取込みの条件に基づいて焦点が合うかまたは焦点が合わない可能性のある領域に対応する。「レイヤ4」（1010）は、CCDの色/照明応答、シャッタスピード（露出時間など）といった露出に関する影響を表している。一般に、この層は、画像取込み時の露出の不完全性が原因で「色あせた」のように見える領域に対応する。「レイヤ5」（1012）は、CCD（または他のイメージセンサ）に関する影響、例えば製造品質を表している。低品質のイメージセンサには、画像の一部を、濁った、ノイズが多い、色あせた、またはその他の欠陥があるように見せる傾向がある。この層はまた、波長高調波によるピクセル化およびモアレ色空間効果をもたらす、コンピュータ画面とイメージセンサとの間の走査速度およびリフレッシュ速度の差を捕捉し得る。一般に、この層は、不完全なイメージセンサおよびセンサと画面との間の物理的波長高調波によって典型的に引き起こされる欠陥の全体的な均一性に対応する。

【００３１】

「レイヤ6」（1014）は、ハードウェアおよび/またはソフトウェア量子化に関する影響を表している。当業者には理解されるように、量子化の目的は、現実世界の様相（例えば、色、影、光など）を画素に効果的に変換することである。図10Bには、「レイヤ6」（1014）の画像における量子化の影響の一例が示されており、画像の左側と右側との間にピクシレーションの著しい差が生じている。一般に、この層は、画像取込み時に発生し得る広範囲のピクシレーションに対応する。「レイヤ7」（1016）は、ソフトウェア画像エンハンスメントおよび圧縮による影響を表している。これらの様相は通常、利用可能なカラーパレットおよび深度（例えば、8ビットカラーまたは24ビットカラー）への再量子化に関連する。エンハンスメントは、ヒストグラム平坦化、および暗い領域を強調し、明るい領域を和らげる他のフィルタまたは効果も含み得る。エンハンスメントに続いて圧縮が行われる場合もあり、圧縮では、再度再量子化を行ってスペースを節約し、画素数を減らし、深度を減らすことなどができる。一般に、この層は、取込み後の処理によるより高いピクシレーションレベルを示す画素のグループに相当する。

【００３２】

上述した7つの層は、画像分類器（ならびに他の種類の改ざん検出器）によって認識され、加工されていないまたは改ざんされていない画像化身分証明書と関連付けられたものとして識別され得る、例示的な固有の画素特徴を表している。すなわち、上述した固有の特徴は、通常の従来の画像取込みおよび処理操作によって導入される傾向があり、したがって無害である。他方、「レイヤ8」（1018）は、前の7つの層の他の無害な固有の特徴と

区別することができる、改ざんされた画像（すなわち図10Aの画像1000c）の様相を表している。この第8の層に特有の固有の特徴は、物理的または電子的に改ざんされている身分証明書と関連付けられている。本開示の様々な態様は、無害である固有の画素特徴と改ざん攻撃の証拠となる画素特徴とを識別し区別するように構成された画像分類器を訓練し適用するための技術を対象とする。

【００３３】

図1に戻って、任意の適切な種類の画像分類器を訓練して、物理的信用証明書のデジタル画像を分類するために使用することができる。例えば、画像分類器106は、CNN、サポートベクトルマシン、またはベイズ分類器であり得る。いずれにしても、分類器訓練エンジン112が画像分類器106を訓練することは、各入力特徴に適用するためのそれぞれの重みを学習する機械学習プロセスを含む。典型的には、画像分類器は、入力特徴ごとに重みを漸進的に発展させる反復プロセスを使用して訓練される。すなわち、画像分類器は、プロセスが最適な重みを見つけようと試みるに従って繰り返し改変される、各特徴に割り当てられたデフォルトのまたは初期の重みを含み得る。学習された特徴重みに基づき、生成された画像分類器106によって物理的信用証明書の入力デジタル画像を採点することができる。いくつかの実施態様では、物理的信用証明書の各入力デジタル画像は、画像分類器106によって、改ざんされている確率として0.0～1.0の尺度で採点される。いくつかの実施態様では、物理的信用証明書のデジタル画像ごとの出力分類器スコアは、画像化された物理的信用証明書が（電子的または物理的に）改ざんされているか、それとも改ざんされていないかを判定するために、閾値確率と比較される。いくつかの例では、複数の画像分類器からのスコアを組み合わせて集計スコアを生成することができ、または各分類器のそれぞれのスコアが個々に順次に評価されてもよい。

【００３４】

いくつかの実施態様では、訓練後、得られたサンプル画像グループを使用して画像分類器106を評価することができる。サンプル画像は訓練画像とは異なり、公知の改ざんされたラベル/改ざんされていないラベルを有する。訓練画像102と同様に、サンプル画像グループは、ポジティブな/改ざんされたデジタル画像とネガティブな/改ざんされていないデジタル画像の両方を含み得る。サンプル画像グループの各デジタル画像は、画像分類器106によって採点される。上記のように、スコアは、物理的信用証明書のデジタル画像が改ざんされているかまたは改ざんされていない可能性を示す。スコアは、画像分類器106の精度を評価するために公知のラベルと比較される。画像分類器106の出力が公知のラベルと実質的に一致しない場合には、分類器106を調整するか、または新しい訓練画像セットで訓練することができる。さらに、いくつかの例では、試験フェーズにおける画像分類器106の出力と公知のラベルとの間の差異が、分類結果にラベル付けするために使用される採点閾値に影響を及ぼし得る（例えば、所与のデータセットのスコア応答に対応する特定の動作閾値を選択することができる）。

【００３５】

図2は、画像分類器を訓練するための例示的なプロセス200の流れ図である。プロセス200、および本明細書に記載される他のすべてのプロセスは、本開示の1つまたは複数の態様に従ってプログラムされた、1つまたは複数の場所に位置する、1台または複数のコンピュータのシステムによって行うことができる。例えば、図1の分類器生成器104はプロセス200を行うことができる。

【００３６】

プロセス200によれば、システムは訓練画像の集合を取得する（202）。訓練画像の集合は、システムによって生成することもでき、または別のソースから取得することもできる。訓練画像（例えば訓練画像102）は、改ざんされたものとしてラベル付けされたポジティブなデジタル画像例と、改ざんされていないまたは加工されていないものとしてラベル付けされたネガティブなデジタル画像例とを含む。システムは訓練画像から特徴を抽出する（204）。上述したように、特徴抽出器（例えば特徴抽出器エンジン108）は、受け取った訓練画像から1つまたは複数の固有の画素特徴を抽出することができる。システムは、

抽出された特徴インスタンスを使用して、抽出された特徴を変数として有する画像分類器を訓練する（206）。画像分類器の訓練は、入力デジタル画像を改ざんされたまたは改ざんされていないとして正しくラベル付けする可能性を最大にする最適な重みをそれぞれの特徴に割り当てる。システムは画像分類器を評価する（208）。特に、画像分類器は、公知のサンプル画像のグループに適用される。画像分類器の出力は、デジタル画像の公知のラベルと比較される。結果として、画像分類器を検証することができる。次いで画像分類器を、より大きなデジタル画像の集合に適用することができ、改ざんされている画像化された物理的信用証明書を検出するために使用することができる。

【００３７】

図3は、画像分類器を訓練するために使用することができる訓練画像の集合を生成する（例えば、プロセス200の工程202）ための例示的なプロセス300の流れ図である。プロセス300によれば、システムは、物理的信用証明書の改ざんされていないデジタル画像を取得する（302）。物理的信用証明書の改ざんされていないデジタル画像は、編集されたり、継ぎ合わされたり、またはそれ以外に意図的に改ざんされていないデジタル画像である（ただし、改ざんされていない画像を、様々な照明条件、環境の影響などを模倣するように改変することはできる）。より具体的には、改ざんされていない画像の集合は、特定の固有の画素特徴の識別、抽出、および重み最適化を誘導するように特に選択される。例えば、選択される固有の画素特徴は、民生（COT）の撮像装置によって生成されたデジタル画像の様々な様相に関連し得る。よって、上述したように、改ざんされていない画像は、画像取込照明、画像取込装置、光学レンズ作用、画像化環境、ハードウェアおよび/もしくはソフトウェア量子化、または自動もしくは手動の画像化後エンハンスメント、のうちの1つまたは複数を含む固有の特徴の組合せの検査を実現するように選択され得る。本開示の様々な態様は、そのような固有の特徴の選択された組合せがデジタル画像の一意の「指紋」を含むという認識から派生したものである。確かに、特定の高価値領域に関して各画像化身分証明書の指紋を識別し精査するように分類器を訓練することにより、改ざん検出において驚くほど正確な結果が得られることが分かっている。

【００３８】

いくつかの例では、適切な改ざんされていない画像に含まれ得るのは、米国の様々な州および諸外国の運転免許証のデジタル画像、様々な国のパスポートのデジタル画像、または様々な政府の部局および機関の政府発行身分証明書のデジタル画像を、物理的信用証明書の改ざんされていないデジタル画像とすることができる。加えて、改ざんされていないデジタル画像は、特定の物理的信用証明書の様々なバージョンのデジタル画像を含む。例えば、1990年代、2000年代、および2010年代に発行されたカリフォルニア州の運転免許証のデジタル画像を、改ざんされていないデジタル画像とすることができる。さらに、物理的信用証明書の改ざんされていないデジタル画像は、様々な状況下で得られる特定の物理的信用証明書のデジタル画像を含み得る。例えば、様々な照明条件下で撮影された、または様々な画像取込装置（例えば、ポイントアンドシュートカメラ、携帯電話カメラなど）を使用して撮影された特定の運転免許証のデジタル画像。様々な照明条件に影響を与える因子の例には、色、温度、光の強度、および入射光の方向が含まれる。いくつかの例では、改ざんされていないデジタル画像は、摩耗、損傷、デザインの欠陥、または意図的な物理的改変などの視覚的に顕著な物理的使用特性を提示し得る。さらに、いくつかの例では、改ざんされていないデジタル画像は、元の画像化イベントに対して「未補正」であり得る。よって、改ざんされていない画像は、照明、焦点面に対する角度、スキュー、回転、およびぼけに関する欠陥を含み得る。いくつかの他の例では、改ざんされていない画像は、そのような欠陥を補正するためにシステムによって自動的に処理され得る。当然ながら、特定の固有の画素特徴の検査を誘導するために適切な改ざんされていない画像の集合を提供するための他の多数の操作も、本開示の範囲内で企図されている。

【００３９】

さらに図3を参照すると、システムは、改ざんされていないデジタル画像に基づいて第1の改ざんされた画像のセットを生成する（304）。いくつかの実施態様では、第1の改ざん

されたデジタル画像のセットは、人間のユーザが手動で生成するか、またはシステムによって自動的に生成することができる。例えば、第1の改ざんされたデジタル画像のセットは、（i）物理的信用証明書のデジタル画像内の元の写真を別の写真で差し替えること（「写真継ぎ合わせ」）、（ii）物理的信用証明書のデジタル画像内の元の人物情報を別の人物情報で差し替えること（「人物情報継ぎ合わせ」）、（iii）物理的信用証明書のデジタル画像内の元のMRZを別のMRZで差し替えること（「MRZ継ぎ合わせ」）、および/または（iv）物理的信用証明書のデジタル画像内の写真、人物情報、またはMRZを覆い隠すかまたはぼかすこと、によって生成され得る。物理的信用証明書の改ざんされていないデジタル画像に基づいて物理的信用証明書の第1の改ざんされたデジタル画像のセットを生成する例について、図6A～図7Fに関連して以下で説明する。

【００４０】

システムは、任意で、物理的信用証明書の第2の改ざんされた画像のセットを取得してもよい（306）。システムは第2の改ざんされた画像のセットを、元の改ざんされていない画像以外のソース（例えば、改ざんされた画像のリポジトリ）から取得することができる。例えば、第2の改ざんされた画像のセットは、システムのテスト中または実際の使用中に誤ってラベル付けされた画像（またはその変形物）を含むことがある。いずれにしても、システムは、第1および（任意で）第2の改ざんされた画像のセットに「改ざんされた」とラベル付けする（308）。加えて、システムは、物理的信用証明書の改ざんされていないデジタル画像を「改ざんされていない」とラベル付けする（308）。システムはまた、第1および第2の改ざんされた画像のセットと、改ざんされていない画像を増やしてもよい（310）。デジタル画像を増やすと、有利には、訓練画像の集合が増加し、さらに多様化され、画像分類器の性能レベルが向上する。いくつかの例では、システムは、デジタル画像全体、またはデジタル画像の特定の部分だけを増やすことができる。加えて、システムは、デジタル画像の異なる部分に対して異なる増大技術を適用することもできる。

【００４１】

システムは、改ざんされていないデジタル画像/改ざんされたデジタル画像を増やすために様々な技術を使用することができる。いくつかの実施態様では、システムは、デジタル画像をサイズ変更することによってデジタル画像を増やすことができる。例えば、システムはデジタル画像のサイズを拡大または縮小することができる。いくつかの実施態様では、システムはデジタル画像を回転させることによってデジタル画像を増やすことができる。例えば、システムはデジタル画像を90度、180度、または270度回転させることができる（当然ながら、他の回転の度合い、例えば5度、120度、260度も使用され得る）。いくつかの実施態様では、システムは、デジタル画像にノイズ、例えばランダムガウスノイズを付加することによってデジタル画像を増やすことができる。いくつかの実施態様では、システムは、測光的特徴を変更することによってデジタル画像を増やすことができる。例えば、システムはデジタル画像の色を変えることができる。さらにまた、いくつかの実施態様では、システムは、異なる色深度および画像チャネルアーキテクチャ（1チャネル、3チャネル、4チャネルなど）への再量子化、様々な画像圧縮フォーマットを使用した圧縮、ならびに/または様々な他のフィルタリング効果を介してデジタル画像を増やすことができる。

【００４２】

システムは次いで、増やしたデジタル画像に基づいて訓練画像の集合を生成する（312）。システムによって生成された訓練画像は、2つのデジタル画像のグループを含み、あるデジタル画像のグループは改ざんされたとラベル付けされ、別のデジタル画像のグループは改ざんされていないとラベル付けされる。訓練画像は、画像分類器を訓練するための分類器生成器、例えば図1の分類器生成器104に提供されることができる。

【００４３】

図4に、上述したプロセス200およびプロセス300に従って画像分類器を生成するための訓練フェーズを示す例示的なプロセス図を示す。図4に示すように、訓練フェーズは、加工されていないまたは「改ざんされていない画像」を受け取ることから開始する。改ざん

されていない画像は、次いで、図6A～図7Fを参照して後述するように、手動でまたは自動的に改ざんされる。改ざんされた画像と改ざんされていない画像はしかるべくラベル付けされ、次いで（必要ならば）サイズ変更および増大によって処理される。増やした訓練画像は次いで、訓練された画像分類器を生成するためのCNNに提供される。図5に、画像分類器を評価するための試験フェーズ（例えば、プロセス200の工程200）を例示するプロセス図を示す。図5に示すように、試験フェーズは、システムに試験画像を提示し、その試験画像を訓練されたCNN画像分類器を用いて処理することによって実施される。分類器は改ざん確率を出力し、改ざん確率は、改ざん警報が発せられるかどうかを決定するために所定の閾値と比較される。改ざんされた/改ざんされていないという分類は検証され、誤ってラベル付けされた画像があれば訓練データセットに追加される。

【００４４】

図6A～図7Fは、改ざんされていない画像化身分証明書および改ざんされた画像化身分証明書の様々な例を表している。特に、デジタル画像600aおよび700aは、高価値領域、すなわち、写真602、702、人物情報データ604、704、およびMRZ606、706を含む、改ざんされていない身分証明書の例である。デジタル画像600b～fおよび700b～fは、特定の高価値領域が改ざんされている身分証明書の例である。デジタル画像600a～fは州の運転免許証に対応しており、デジタル画像700a～fはパスポートに対応している。

【００４５】

上記のように、改ざんされたデジタル画像600b～fおよび700b～fは、改ざんされていないデジタル画像600aおよび700aから導出され得る。第1の例として、改ざんされたデジタル画像600bおよび700bは、写真602、702を新しい別の写真602'、702'で差し替えることによって生成することができる。第2の例として、改ざんされたデジタル画像600cおよび700cは、元の人物情報604、704を新しい別の人物情報604'、704'で差し替えることによって生成することができる。第3の例として、改ざんされたデジタル画像600dおよび700dは、元のMRZ606、706を新しい別のMRZ606'、706'で差し替えることによって生成することができる。第4の例として、改ざんされたデジタル画像600eおよび700eは、画像化された身分証明書の1つまたは複数の高価値領域を覆い隠すことによって生成することができる。例えば、画像600eにおいて、写真602''および人物情報604''は、それらの領域の部分を黒く塗りつぶすことによって覆い隠されている。同様に、画像700eでは、人物情報704''およびMRZ706''が黒く塗りつぶされることによって覆い隠されている。当然ながら、高価値領域の目視検査を妨害する他の様々な種類の画像オクルージョンもまた本開示の範囲内に含まれる。第5の例として、改ざんされたデジタル画像600fおよび700fは、画像化された身分証明書の1つまたは複数の高価値領域をぼかすことによって生成することができる。画像600fでは、人物情報604'''がぼやけている。画像700fでは、写真702'''、人物情報704'''、およびMRZ706'''の3つの高価値領域すべてがぼやけている。

【００４６】

いくつかの例では、写真、人物情報、およびMRZの継ぎ合わせ（例えば、デジタル画像の一部の差替え）、オクルージョン、およびぼかしを、訓練データセットの一部を生成するためにシステムが自動的に行うことができる。例えば、システムは、顔検出器、テキスト検出器、または他の適切な画像解析技術を利用して、特定の画像化された身分証明書上の高価値領域を識別し得る。識別された領域は次いで、上述したように選択的に改ざんされ得る。いくつかの例では、高価値領域の特定の部分だけが改ざんされ得る。例えば、顔検出器は、写真の特定の選択的部分、例えば、目、髪、鼻または口を識別するように構成され得る。別の例として、テキスト検出器は、特定の人物情報、例えば、運転免許証番号、生年月日、または文書弁別子を識別するように構成され得る。いくつかの例では、複数の改ざんされた画像を、共通の改ざんされていない画像から導出することができる。例えば、継ぎ合わせ、オクルージョン、およびぼかしのための異なる技術を使用して、異なる種類の改ざんされた画像を作成することができる。いくつかの実施態様では、異なる継ぎ合わせ技術により、ソフトなエッジ、ハードなエッジ、またはギザギザのエッジを得ることができる。様々な継ぎ合わせ技術はまた、勾配領域ステッチングおよび/またはバラン

ス調整も含み得る。同様に、様々なぼけの度合い、ならびに/または異なるサイズ、形状、および色のオクルージョンを使用して、複数の改ざんされた画像が導出されてもよい。いくつかの異なる種類の改ざんされた画像を自動的に生成することは、それが訓練データセットのサイズを増大させるので有利である。この利点は、画像が改ざんされた身分証明書に対応しているかどうかの判定を容易にするためにCNNが使用される場合に増幅される。というのも、これらの種類の分類器は訓練例の増加と共に向上し続けるからである。さらに、自動的に生成された改ざんされた画像は、改ざんに際して様々な洗練度を模倣することによって訓練データをさらに多様化する。例えば、継ぎ合わせの初歩的な試みではギザギザのエッジを生み出し得るが、より洗練された試みでは滑らかなエッジを生み出し得る。

【００４７】

図8は、画像化された身分証明書が改ざんされているかどうかを示す出力を提供するための例示的なシステム800の図である。システム800は、インターネット、イントラネット、または他の任意の適切な有線もしくは無線のクライアント・サーバ環境において実装することができる。システム800は、以下で説明するシステム、構成要素、および技術を実装することができる例示的なアーキテクチャを提供する。

【００４８】

図示のように、ユーザ802は、ユーザ機器804を介して改ざん検出システム814と対話することができる。例えば、ユーザ機器804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）、例えばインターネットを介して改ざん検出システム814に結合された、コンピュータ、カメラ、スキャナ、ビデオレコーダ、またはモバイル機器、例えば、携帯電話もしくはタブレットを含み得る。いくつかの実施態様では、改ざん検出システム814とユーザ機器804を1台の機械とすることができる。例えば、ユーザ802は、ユーザ機器804にコンピュータプログラムまたはアプリケーションをインストールすることができる。ユーザ機器804は一般に、ランダムアクセスメモリ（RAM）806およびプロセッサ808を含む。

【００４９】

ユーザ802は、改ざん検出システム814内の改ざん検出エンジン830に物理的信用証明書のデジタル画像810を提示することができる。この例では、物理的信用証明書のデジタル画像810はネットワークを介して改ざん検出システム814に送信される。改ざん検出システム814は、例えば、ネットワークを介して互いに結合されている1つまたは複数の場所にある1台または複数のコンピュータ上で走るコンピュータプログラムとして実装することができる。

【００５０】

改ざん検出システム814は、改ざん検出エンジン830を含む。改ざん検出エンジン830は、物理的信用証明書の訓練画像を使用して訓練された画像分類器を含む。いくつかの実施態様では、改ざん検出エンジン830は、図1に関連して上述した分類器生成器104によって訓練された画像分類器106を含むことができる。改ざん検出エンジン830は、物理的信用証明書のデジタル画像810を受け取り、画素レベルの画像解析技術を使用してデジタル画像810を解析する。改ざん検出エンジン830は、画素配列を含むデジタル画像810に対して画素レベルの解析を行うことができる。改ざん検出エンジン830は、デジタル画像810から固有の画素特徴を抽出し、抽出された特徴に基づいてデジタル画像810が改ざんされているかそれとも改ざんされていないかを判定する。改ざん検出エンジン830は、デジタル画像810が改ざんされているかそれとも改ざんされていないかに関する判定に基づいて、改ざん指摘出力828を生成する。

【００５１】

改ざん検出システム814によって生成された改ざん指摘出力828は、ユーザ802に提示するためにユーザ機器804に提供される。いくつかの実施態様では、改ざん指摘出力828は、ユーザ802を認証する際に使用するためにサーバシステム824に提供される。例えば、サーバシステム824は、金融機関のサーバシステムとすることができる。サーバシステム824は

、改ざん指摘出力828を使用してユーザ802が特定の口座の所有者であると認証することができる。加えて、サーバシステム824は、雇用主のサーバシステムとすることもできる。サーバシステム824は、改ざん指摘出力828を使用してユーザ802が雇用主の従業員であると認証することができる。さらに、サーバシステム824は、ホテルのサーバシステムとすることもできる。サーバシステム824は、改ざん指摘出力828を使用してユーザ802がホテルに滞在している客であると認証することができる。様々な他の種類の電子取引も本開示の範囲内で想定される。多くの実施態様では、改ざん指摘出力は、最終的にユーザを認証するためにさらに別の処理技法と組み合わされ得ることに留意されたい。すなわち、「加工されていない」または「改ざんされていない」という改ざん指摘出力は、画像化された信用証明書の1つまたは複数の高価値領域に含まれるデータが本物であり改ざんされていないことをシステムに知らせることができる。この保証により、システムは、高価値領域から情報を抽出し処理して、従来の認証技術および手法に従ってユーザを認証することができる。

【００５２】

図8に関して、いくつかの実施態様では、改ざん検出エンジン830は複数の画像分類器を含むことができる。例えば、改ざん検出エンジン830は、物理的信用証明書のデジタル画像が改ざんされているかそれとも改ざんされていないかをデジタル画像の身分証明写真領域に基づいて判定する第1の画像分類器を含むことができる。第1の画像分類器は、図6Bおよび図7Bに関連して上述した訓練画像を使用して訓練することができる。改ざん検出エンジン830は、物理的信用証明書のデジタル画像が改ざんされているかそれとも改ざんされていないかをデジタル画像の人物情報領域に基づいて判定する第2の画像分類器をさらに含むことができる。第2の画像分類器は、図6Cおよび図7Cに関連して上述した訓練画像を使用して訓練することができる。改ざん検出エンジン830は、物理的信用証明書のデジタル画像が改ざんされているかそれとも改ざんされていないかをデジタル画像内のMRZに基づいて判定する第3の画像分類器をさらに含むことができる。第3の画像分類器は、図6Dおよび図7Dに関連して上述した訓練画像を使用して訓練することができる。改ざん検出エンジン830は、物理的信用証明書のデジタル画像が改ざんされているかそれとも改ざんされていないかを、デジタル画像の身分証明写真領域、人物情報領域、MRZ、またはバイオメトリック情報のオクルージョンまたはぼけに基づいて判定する第4の画像分類器をさらに含むことができる。第4の画像分類器は、図6E～6Fおよび図7E～7Fに関連して上述した訓練画像を使用して訓練することができる。

【００５３】

いくつかの実施態様では、改ざん検出エンジン830は、複数の画像分類器のうちの1つまたは複数を順次に適用することができる。複数の分類器からの出力を、1つまたは複数の閾値に独立して適用すること、または組み合わされた出力を生成するために集約することができる。例えば、改ざん検出エンジン830は、デジタル画像810に第1の画像分類器および第3の画像分類器を順次に適用することができる。改ざん検出エンジン830は、第1の画像分類器と第3の画像分類器のどちらかがデジタル画像810は改ざんされていると判定した場合に、改ざんされたとする改ざん指摘出力828を生成するように構成することができる。いくつかの実施態様では、改ざん検出エンジン830は、物理的信用証明書の種類に基づいて画像分類器の様々な組合せを適用することができる。すなわち、異なる種類の信用証明書/身分証明書は、異なる画像分類器による解析を必要とする異なる高価値領域を有し得る。さらに、いくつかの実施態様では、改ざん検出エンジン830は、物理的信用証明書のデジタル画像が表しているのが物理的信用証明書の表面かそれとも裏面かに関する決定に基づいて、画像分類器の様々な組合せを適用することができる。第1の例として、改ざん検出エンジン830は、図7A～7Fに示されているパスポートの表面の画像に対して、広範な高価値領域のセットが存在していることから、第1、第2、第3、および第4の画像分類器を適用するように構成され得る。第2の例として、改ざん検出エンジン830は、MRZを裏面にのみ含む図6A～6Cおよび図6E～6Fに示されている運転免許証の表面の画像に対して第1、第2、および第4の画像分類器を使用するように構成され得る。

【００５４】
図9は、画像化された身分証明書が改ざんされているかどうかを示す出力を提供するための例示的なプロセス900の流れ図である。いくつかの例では、図8に関連して説明した改ざん検出システム830はプロセス900を行うことができる。プロセス900によれば、システムは物理的信用証明書のデジタル画像を受け取る（902）。システムは、ユーザ機器から物理的信用証明書のデジタル画像を受け取る。システムは、受け取った物理的信用証明書のデジタル画像が改ざんされているかそれとも改ざんされていないかを判定する（904）。システムは物理的信用証明書のデジタル画像を受け取り、画像解析技術を使用してデジタル画像を解析する。システムは、画素配列を含むデジタル画像に対して画素レベルの解析を行うことができる。システムは、デジタル画像から固有の特徴を抽出し、抽出された特徴に基づいてデジタル画像が改ざんされているかそれとも改ざんされていないかを判定する。システムは、デジタル画像が改ざんされているかそれとも改ざんされていないかについての判定に基づいて改ざん指摘出力を生成する。システムは、改ざん指摘出力を提供する（906）。いくつかの実施態様では、システムによって生成された改ざん指摘出力は、ユーザに提示するためにユーザ機器に提供される。いくつかの実施態様では、改ざん指摘出力は、ユーザを認証するために第三者のサーバシステムに提供される。

【００５５】
本明細書では、「エンジン」という用語は、1つまたは複数の特定の機能を果たすことができるソフトウェアベースのシステムまたはサブシステムを指すために広く使用される。一般に、エンジンは、1つまたは複数の場所にある1台または複数のコンピュータにインストールされた1つまたは複数のソフトウェアモジュールまたはコンポーネントとして実装されることになる。場合によっては、1台または複数のコンピュータが特定のエンジン専用とされる。場合によっては、複数のエンジンを同じ1台または複数のコンピュータにインストールして実行することもできる。

【００５６】
一般に、本明細書に記載される主題および機能的動作の態様は、本明細書で開示された構造およびそれらの構造的均等物を含む、デジタル電子回路として、有形に具体化されたコンピュータソフトウェアもしくはファームウェアとして、コンピュータハードウェアとして、またはそれらのうちの1つもしくは複数の組合せとして実装することができる。本明細書に記載される主題の態様は、1つまたは複数のコンピュータプログラム、すなわち、データ処理装置が実行するための、またはデータ処理装置の動作を制御するように有形の非一時的記憶媒体上で符号化されたコンピュータプログラム命令の1つまたは複数のモジュールとして実装することができる。コンピュータ記憶媒体は、機械可読記憶装置、機械可読記憶基板、ランダムアクセスもしくはシリアルアクセスのメモリデバイス、またはそれらのうちの1つまたは複数の組合せとすることができる。代替として、または加えて、プログラム命令は、データ処理装置が実行するための適切な受信側装置に送信するための情報を符号化するように生成される、人為的に生成された伝播信号（例えば、機械で生成された電気信号、光信号、または電磁信号）上で符号化することもできる。

【００５７】
「データ処理装置」という用語は、データ処理ハードウェアを指し、例えば、プログラマブルプロセッサ、コンピュータ、または複数のプロセッサもしくはコンピュータを含む、データを処理するためのあらゆる種類の装置、デバイス、および機械を包含する。装置はまた、FPGA（フィールド・プログラマブル・ゲート・アレイ）やASIC（特定用途向け集積回路）などの専用論理回路とすることもでき、またはそれらをさらに含むこともできる。装置は、任意で、ハードウェアに加えて、コンピュータプログラムのための実行環境を生成するコード、例えば、プロセッサファームウェアを構成するコード、プロトコルスタック、データベース管理システム、オペレーティングシステム、またはそれらのうちの1つもしくは複数の組合せ含むこともできる。

【００５８】
コンピュータプログラムは、プログラム、ソフトウェア、ソフトウェアアプリケーショ

ン、アプリ、モジュール、ソフトウェアモジュール、スクリプト、またはコードとも呼ばれ、コンパイル言語もしくはインタプリタ言語、または宣言型言語もしくは手続き型言語を含む任意の形式のプログラミング言語で書くことができ、スタンドアロンプログラムとしてやモジュール、コンポーネント、サブルーチン、またはコンピューティング環境で用いるのに適したその他のユニットとしての形式を含む任意の形式で配置することができる。プログラムは、ファイルシステム内のファイルに対応し得るが、そうである必要はない。プログラムは、他のプログラムもしくはデータを保持するファイルの一部、例えば、マークアップ言語文書に格納された1つもしくは複数のスクリプトに、問題のプログラムに専用の単一ファイルに、または複数の連携したファイル、例えば、1つもしくは複数のモジュール、サブプログラム、もしくはコードの一部を格納するファイルに格納することができる。コンピュータプログラムは、1台のコンピュータ上で、または1箇所に位置するかもしくは複数のサイトに分散され、データ通信ネットワークによって相互接続された複数のコンピュータ上で実行されるように配置することができる。

【００５９】

本明細書に記載されるプロセスおよび論理フローは、入力データに作用して出力を生成することによって機能を果たす1つまたは複数のコンピュータプログラムを実行する1台または複数のプログラマブルコンピュータによって実行することができる。プロセスおよび論理フローはまた、例えばFPGAやASICなどの専用論理回路によって、または専用論理回路と1台もしくは複数のプログラムされたコンピュータとの組合せによっても実行することができる。

【００６０】

コンピュータプログラムの実行に適したコンピュータは、汎用もしくは専用のマイクロプロセッサもしくはその両方、または任意の他の種類の中央処理装置に基づくものとすることができる。一般に、中央処理装置は、読取り専用メモリまたはランダムアクセスメモリまたはその両方から命令およびデータを受け取ることになる。コンピュータの必須要素は、命令を遂行または実行するための中央処理装置と、命令およびデータを格納するための1つまたは複数のメモリデバイスとである。中央処理装置およびメモリは、専用論理回路によって補うか、または専用論理回路に組み込むこともできる。一般に、コンピュータはまた、データを格納するための1台または複数の大容量記憶装置、例えば、磁気、光磁気ディスクや光ディスクを含むか、または大容量記憶装置との間でデータの受信もしくは送信もしくはその両方を行うように動作可能に結合されることになる。しかし、コンピュータにはそのような装置がなくてもよい。さらに、コンピュータは、別の機器、例えば、いくつか例を挙げると、携帯電話、携帯情報端末（PDA）、モバイルオーディオやビデオプレーヤ、ゲームコンソール、全地球測位システム（GPS）受信機、または携帯用記憶デバイス、例えば、ユニバーサル・シリアル・バス（USB）フラッシュ・ドライブに組み込むこともできる。

【００６１】

コンピュータプログラム命令およびデータを格納するのに適したコンピュータ可読媒体には、あらゆる形の不揮発性メモリ、媒体およびメモリデバイスが含まれ、これには、例えば、EPROM、EEPROM、フラッシュ・メモリ・デバイスなどの半導体メモリデバイス、内蔵ハードディスクやリムーバブルディスクなどの磁気ディスク、光磁気ディスク、CD-ROMおよびDVD-ROMディスクが含まれる。

【００６２】

ユーザとの対話を提供するために、本明細書に記載される主題の態様を、ユーザに情報を表示するためのCRT（陰極線管）やLCD（液晶ディスプレイ）モニタなどの表示装置と、ユーザがコンピュータに入力を提供するためのキーボードおよびマウスやトラックボールなどのポインティングデバイスとを備えるコンピュータ上で実装することができる。ユーザとの対話を提供するために、他の種類のデバイスもまた使用することができる。例えば、ユーザに提供されるフィードバックは、任意の形態の感覚フィードバック、例えば、視覚フィードバック、聴覚フィードバック、または触覚フィードバックとすることができ、

ユーザからの入力は、音響入力、音声入力、または触覚入力を含む、任意の形態で受け取ることができる。加えて、コンピュータは、ユーザが使用する機器との間でデジタル画像を送受信することによって、例えば、ウェブブラウザから受信した要求に応答してユーザの機器のウェブブラウザにウェブページを送信することによってユーザと対話することもできる。

【００６３】

本明細書に記載される主題の態様は、データサーバなどのバックエンドコンポーネントを含むコンピュータシステム、またはアプリケーションサーバなどのミドルウェアコンポーネントを含むコンピュータシステム、またはユーザが本明細書に記載される主題の実施態様と対話するためのグラフィカル・ユーザ・インターフェースやウェブブラウザやアプリを有するクライアントコンピュータなどのフロントエンドコンポーネントを含むコンピューティングシステム、または1つもしくは複数のそのようなバックエンドコンポーネント、ミドルウェアコンポーネントもしくはフロントエンドコンポーネントの任意の組合せにおいて実装することができる。システムの構成要素は、任意の形態のデジタルデータ通信またはデジタルデータ通信の媒体、例えば、通信ネットワークによって相互接続することができる。通信ネットワークの例には、ローカル・エリア・ネットワーク（LAN）および広域ネットワーク（WAN）、例えばインターネットが含まれる。

【００６４】

コンピューティングシステムは、クライアントとサーバとを含むことができる。クライアントとサーバとは、一般に相互にリモートであり、通常、通信ネットワークを介して対話する。クライアントとサーバの関係は、それぞれのコンピュータ上で動作する、互いにクライアント/サーバ関係を有するコンピュータプログラムによって生じる。いくつかの態様では、サーバは、例えばクライアントとして動作するユーザ機器と対話するユーザにデータを表示し、ユーザからユーザ入力を受け取るために、ユーザ機器にデータ、例えばHTMLページを送信する。ユーザ機器で生成されたデータ、例えばユーザ対話の結果を、サーバにおいて機器から受信することができる。

【００６５】

本明細書には多くの具体的な実装詳細が含まれているが、これらの詳細は、発明または特許請求され得るものの範囲に対する限定と解釈されるべきではなく、むしろ、個々の発明の個々の態様に特有の特徴の記述と解釈されるべきである。本明細書に別々の態様の文脈において記載されている特定の特徴を、単一の態様において組み合わせて実施することもできる。逆に、単一の態様の文脈で記載されている様々な特徴を、複数の態様において別々に、または任意の適切な部分組合せとして実施することもできる。さらに、各特徴は、上記では、特定の組合せとして動作するものとして記述されており、そうしたものとして当初請求されている場合もあるが、請求される組合せの中からの1つまたは複数の特徴を、場合によっては、その組合せの中から削除することもでき、請求される組合せは、部分的組合せまたは部分的組合せの変形も対象とし得る。

【００６６】

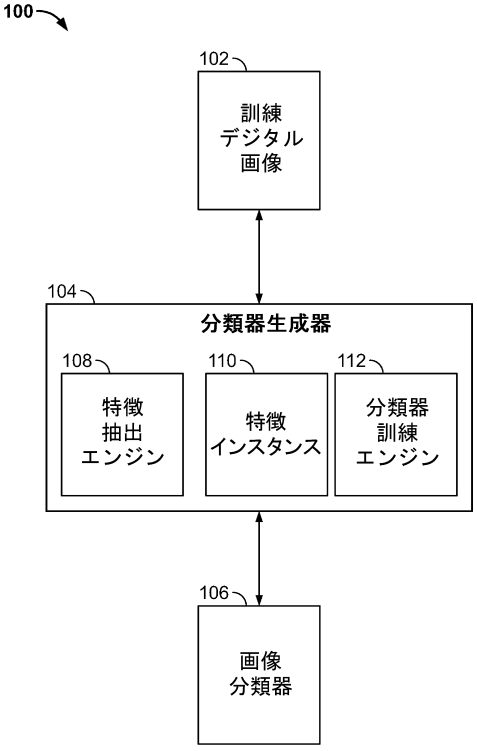
同様に、各動作は図面において特定の順序で示されているが、これは、所望の結果を達成するために、そうした動作が図示の特定の順序で、もしくは順番に行われること、またはすべての図示の動作が行われることを必要とするものとして理解されるべきではない。ある特定の状況では、マルチタスク処理および並列処理が有利な場合もある。さらに、上述した態様における様々なシステムモジュールおよびコンポーネントの分離は、そうした分離をすべての態様において必要とするものとして理解されるべきではなく、前述のプログラムコンポーネントおよびシステムは、一般に、単一のソフトウェア製品に統合することもでき、複数のソフトウェア製品にパッケージ化することもできることを理解されたい。

【００６７】

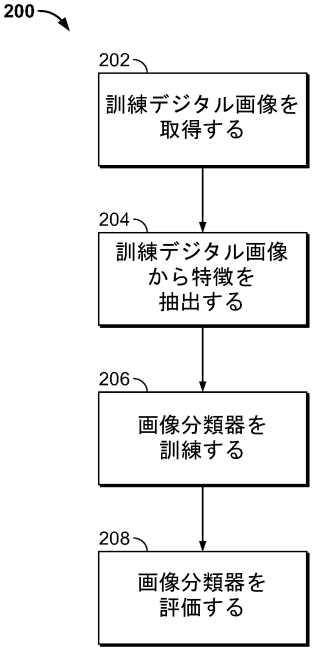
本主題の特定の態様について説明した。添付の特許請求の範囲内には他の態様が含まれる。例えば、特許請求の範囲に記載されている動作を、異なる順序で実行し、しかも所望

の結果を達成することができる。一例として、添付の図に示されているプロセスは、所望の結果を達成するために、必ずしも、図示の特定の順序、または順番を必要としない。場合によっては、マルチタスク処理および並列処理が有利であり得る。

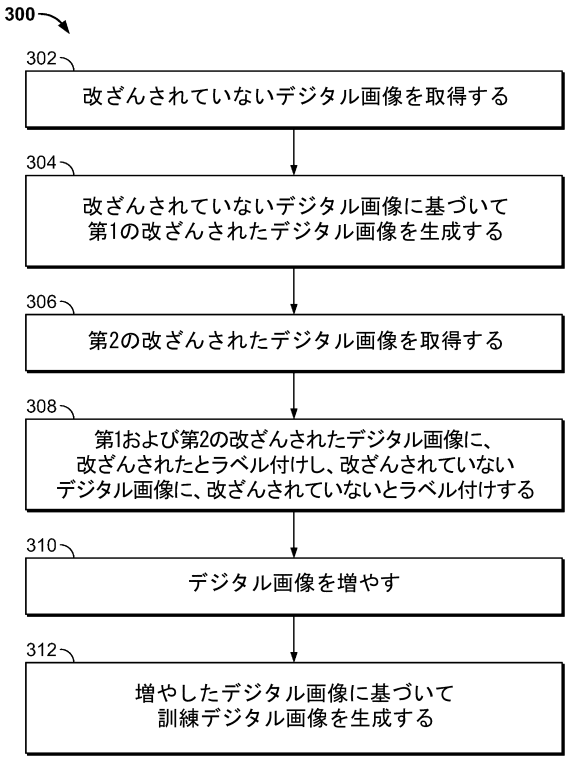
【図１】



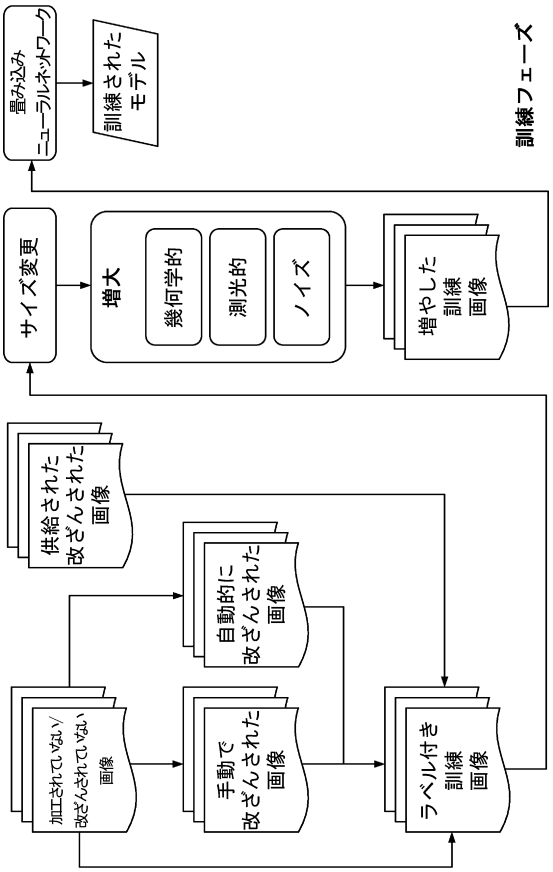
【図２】



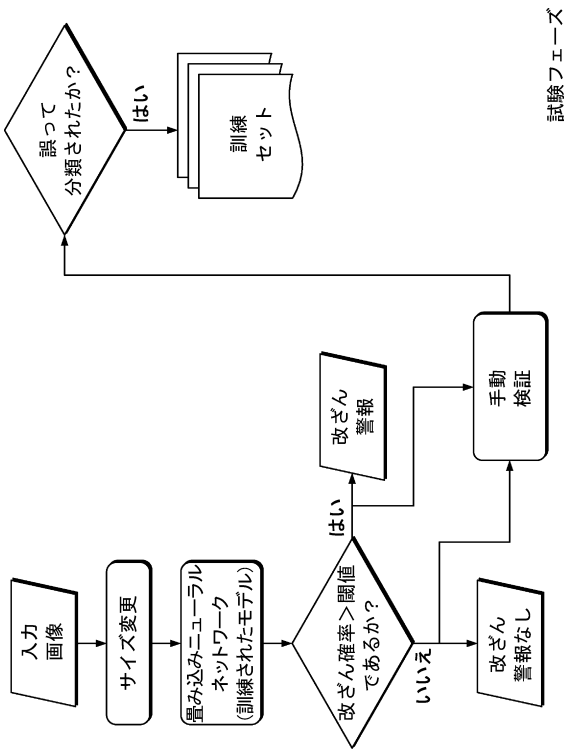
【図３】



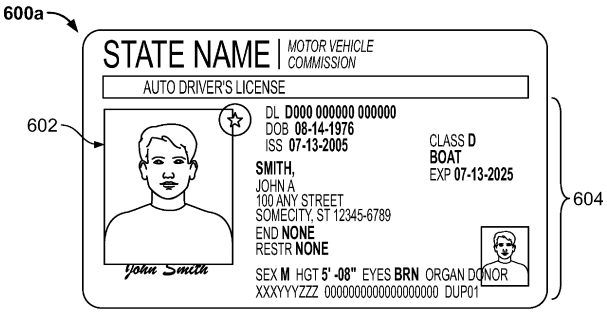
【図４】



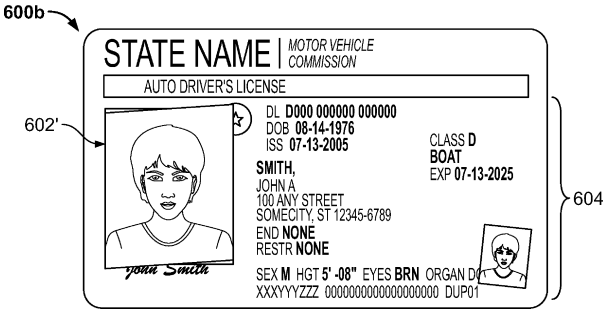
【図５】



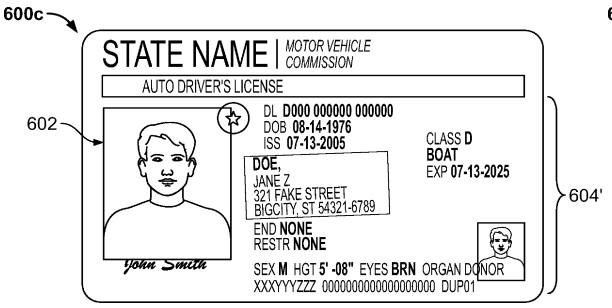
【図６Ａ】



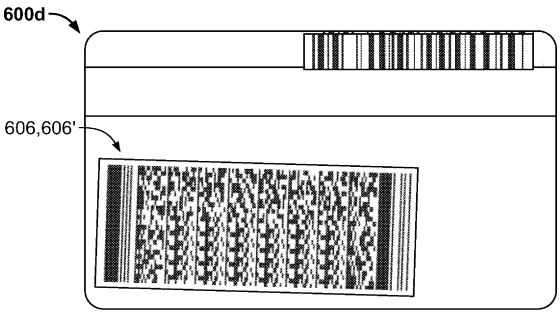
【図６Ｂ】



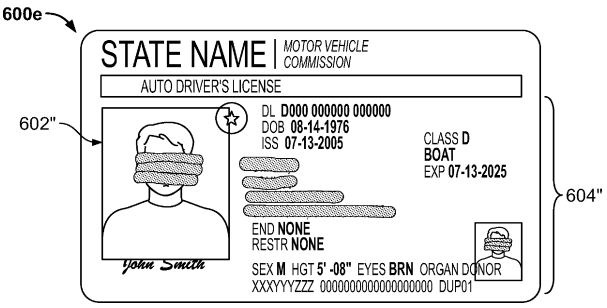
【図６Ｃ】



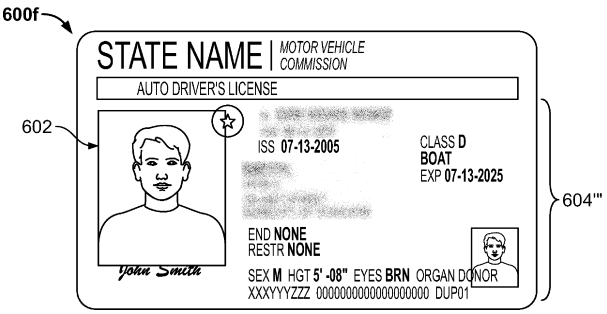
【図６Ｄ】



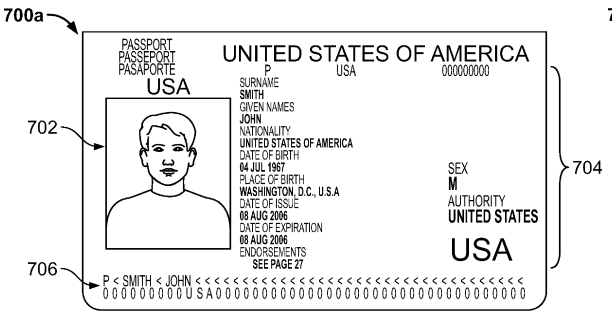
【図６Ｅ】



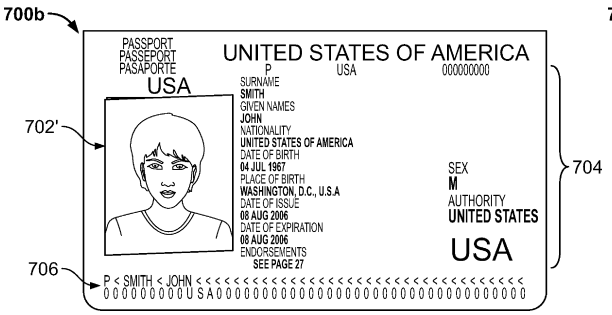
【図６Ｆ】



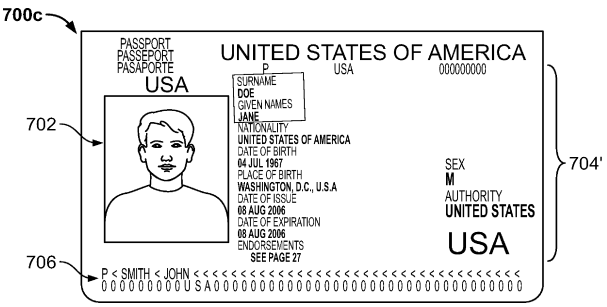
【図７Ａ】



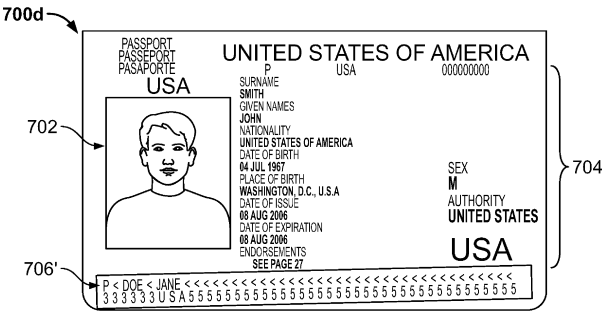
【図７Ｂ】



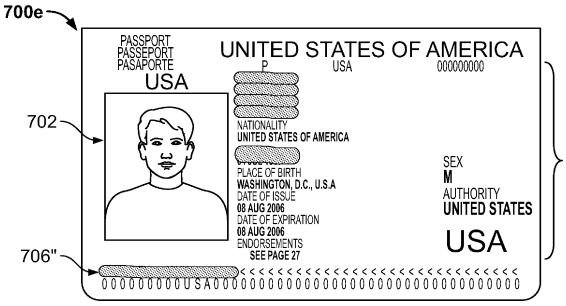
【図７Ｃ】



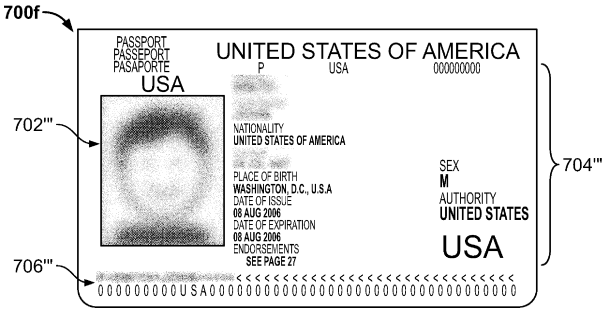
【図７Ｄ】



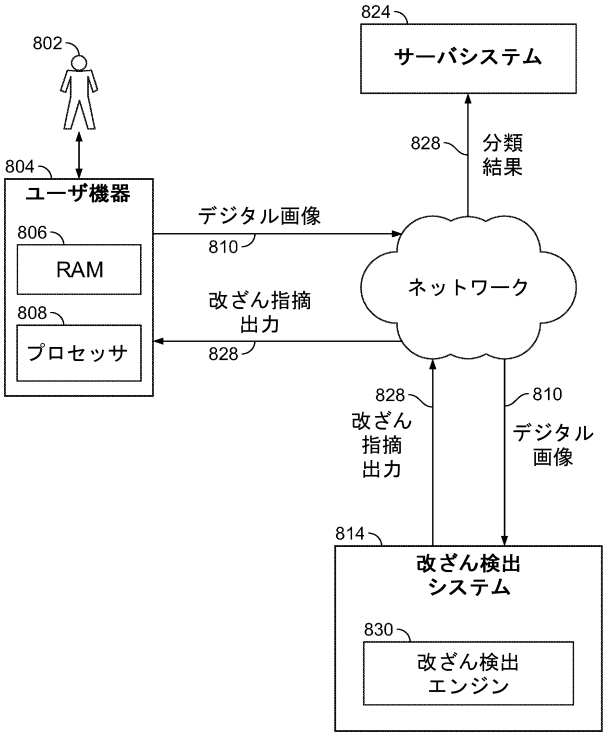
【図７Ｅ】



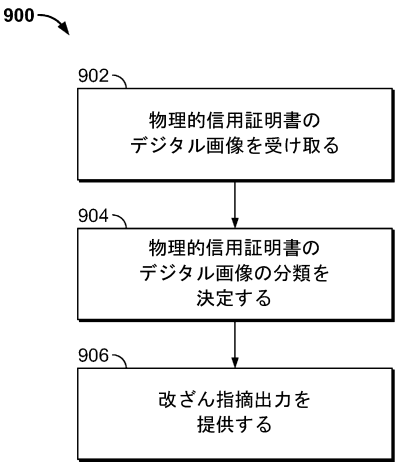
【図７Ｆ】



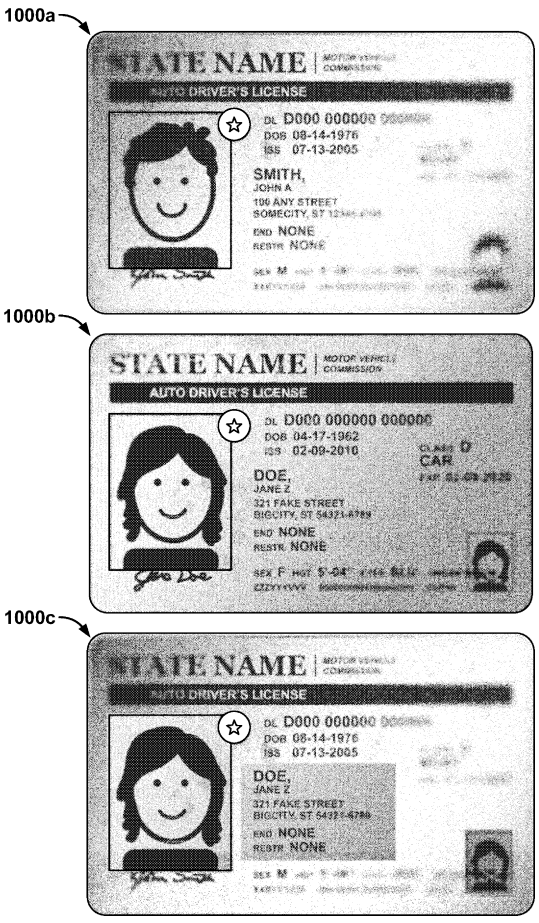
【図８】



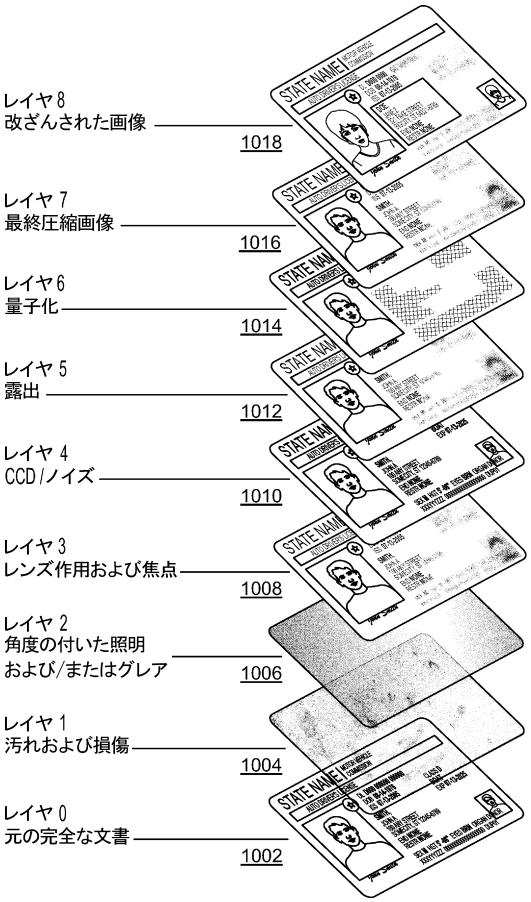
【図９】



【図１０Ａ】



【図１０Ｂ】


レイヤ 8
改ざんされた画像
1018
レイヤ 7
最終圧縮画像
1016
レイヤ 6
量子化
1014
レイヤ 5
露出
1012
レイヤ 4
CCD/ノイズ
1010
レイヤ 3
レンズ作用および焦点
1008
レイヤ 2
角度の付いた照明
および/またはグレア
1006
レイヤ 1
汚れおよび損傷
1004
レイヤ 0
元の完全な文書
1002

フロントページの続き

(74)代理人 100142929
弁理士 井上 隆一
(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 100205707
弁理士 小寺 秀紀
(74)代理人 100114340
弁理士 大関 雅人
(74)代理人 100121072
弁理士 川本 和弥
(72)発明者 ヒューバー ジュニアー リチャード オースティン
アメリカ合衆国 ０７０８６ ニュージャージー州 ウィーホーケン スターリング アベニュー ５０
(72)発明者 マリック サトヤ プラカシュ
アメリカ合衆国 ９２１３０ カリフォルニア州 サンディエゴ ファロン サークル ３７７９
(72)発明者 フラグ マシュー ウィリアム
アメリカ合衆国 ９２１０９ カリフォルニア州 サンディエゴ ツアーマリン ストリート １０２４
(72)発明者 シンハル コウスタブ
インド ５６００８７ バンガロール カダビーサナハリ アウター リング ロード ビサイド クローマ ビルディング ロード プラナーバ ギター ビー５５１１

審査官 千葉 久博

(56)参考文献 特開２００６－３１３５３４（ＪＰ，Ａ）
米国特許出願公開第２０１４／０１８０９８１（ＵＳ，Ａ１）
米国特許出願公開第２００５／０２４２５６８（ＵＳ，Ａ１）
国際公開第２０１６／０６４４２８（WO，Ａ１）
国際公開第２００９／０６５１５１（WO，Ａ１）
Marco Fontani, 外３名, "The watchful forensic analyst: Multi-clue information fusion with background knowledge", 2013 IEEE Internatinal Workshop on Information Forensics and Security(WIFS), ２０１３年１１月１８日, p.120-125

(58)調査した分野(Int.Cl., ＤＢ名)
Ｇ０６Ｑ ５０／２６
Ｇ０６Ｆ ２１／６４
Ｇ０６Ｔ ７／００