

明 細 書

発明の名称：画像情報検証装置

技術分野

[0001] 本発明は、画像情報の検証及びそれに基づく認証技術に関する。

背景技術

[0002] 身分証明書はＩＣカードやプラスチックカードなどの券面に顔写真や名前等の属性情報を印刷し、発行されるケースが一般的であるが、スマートフォン等のモバイル機器が普及している昨今、カード状の身分証明書ではなく、常に携帯しているモバイル機器で身分証明を行いたいという要求がある。

[0003] 身分証明書をモバイル機器にて実装する場合、顔写真や名前等の属性情報を電子化し、身分を証明する際、そのデータをモバイル機器のディスプレイに表示して提示し、目視によって身分証明書の正当性を検証する方法や、通信を介してそのデータを検証する機器に送付して、検証する側の機器にて身分証明書データの正当性を機械的に検証する方法などが考えられる。しかし、後者の場合、モバイル機器には身分証明書のデータ以外にも様々なデータが格納されている場合が多く、誤って不必要なデータを検証する側の機器に送付してしまうようなケースも考えられる。それ故、前者の様にディスプレイに身分証明書の画像を表示して提示するだけで、身分証明できる仕組みが望まれる。

[0004] しかしながら従来のカード状の身分証明書の券面印刷と異なり、電子化された身分証明書データの場合、顔写真を別の顔写真に張り替えることは容易であり、また、張り替えられた画像データを表示されても、張り替えられた痕跡を検知することは困難である。

[0005] そこで、顔写真と顔写真のデータを埋め込んだ二次元コードの画像を身分証明書とし、身分を証明する際、二次元コードから顔写真を復元して、元々の顔写真と比較することにより真贋判定をする技術が提案されている（特許文献１）。

先行技術文献

特許文献

[0006] 特許文献1：特開2005-141626号公報

発明の概要

発明が解決しようとする課題

[0007] しかしながら従来技術においては、二次元コードに顔写真データそのものを埋め込んでいる為、二次元コードが大きくなるという課題があった。通常、身分証明書に用いる程度の大きさの顔写真データでも、数キロバイトから数十キロバイトのデータ量となり、例えそのデータを圧縮したとしても、顔写真データを二次元コードに埋め込んで二次元コードリーダが認識できる解像度にした場合、顔写真データのデータ量によっては、二次元コードが例えばA4サイズの半分程度まで大きくなってしまい、その二次元コードはスマートフォンのディスプレイには表示しきれないという課題があった。

[0008] また逆にスマートフォンのディスプレイに表示できる程度の大きさの二次元コードに顔写真データを埋め込もうとすると、顔写真データのデータ量を削減する必要がある為、顔写真が荒い画像となり、その荒い画像からでは顔写真の正当性を確認するのが難しくなるという課題があった。

課題を解決するための手段

[0009] 上記課題を解決するために、バイオメトリクス認証で用いる技術を応用し、顔写真データから顔写真を一意に識別できる特徴値（「目、鼻、口端などの顔の特徴点位置」や「顔を特徴付ける目の部分だけ切り取った画像」などを抽出し、その特徴値を二次元コードに埋め込む。

[0010] そして、顔写真、二次元コードをスマートフォンのディスプレイに同一画面として表示させ当該画像（身分証明書として利用可能）を検証する際は、デジタルカメラ、WEBカメラ、スキャナー等の撮影機器で、ディスプレイに表示された画像を読み取り、表示された画像の中の二次元コードから電子署名の検証をし、二次元コードが正当な物であることを判断する。

[0011] 更に別の発明では、外部のカメラ等で撮影した顔画像と、正当なものと検証された顔写真とからカメラの被写体を認証する。

発明の効果

[0012] 本発明の特徴は、顔写真データを二次元コードに埋め込むのに比べて小さなデータ量で、画像（身分証明書として利用可能）の正当性を検証することができる。

図面の簡単な説明

[0013] [図1]本実施形態1のシステム構成例を示す図である。

[図2]本実施形態1および2における発行装置、検証装置およびスマートフォンのハードウェア構成例を示す図である。

[図3]本実施形態1および2におけるデジタル身分証明書の発行処理手順を示すシーケンス図である。

[図4]本実施形態1におけるデジタル身分証明書の検証処理手順を示すシーケンス図である。

[図5]本実施形態1における検証装置での検証結果を表示した図である。

[図6]本実施形態2のシステム構成例を示す図（図1との差分）である。

[図7]本実施形態2におけるデジタル身分証明書の検証処理手順およびデジタル身分証明書の保有者の認証処理手順を示すシーケンス図である。

[図8]本実施形態2における検証装置での認証結果を表示した図（図5との差分）である。

発明を実施するための形態

実施例 1

[0014] ーシステム構成ー

以下に本発明の実施形態1について図面を用いて詳細に説明する。

[0015] 図1は、本実施形態1におけるデジタル身分証明書システム1の全体構成例を示す図である。この図では、全体構成と共に、デジタル身分証明書システム1を構成する各コンピュータの機能構成例についても示している。図1

に示すデジタル身分証明書システム１は、発行装置１０がスマートフォン３０向けにデジタル身分証明書（画像データ）３０１を発行し、検証装置２０はスマートフォン３０のディスプレイに表示されたデジタル身分証明書３０１の画像を読み込み、その画像から提示されたデジタル身分証明書３０１の真贋判定をするシステムである。

[0016] 図１に示すように、発行装置１０は、電子署名を生成する署名鍵ＳＫ１０４と検証装置２０との共通鍵Ｋ１０５を管理しており、顔写真のデータから特徴値を抽出する特徴値抽出機能１０６と、データの暗号化及び電子署名生成処理をする暗号処理機能１０３と、二次元コードを生成する二次元コード生成機能１０２と、顔写真データ３０２と名前等の属性情報３０３と二次元コード３０４からデジタル身分証明書（画像データ）３０１を成型する身分証明書成型機能１０１から構成できる。また、検証装置２０は画像撮影機器２１と繋がっており、検証装置２０は、電子署名を検証する検証鍵ＰＫ２０４と発行装置１０との共通鍵Ｋ２０５を管理しており、スマートフォン３０のディスプレイに表示されたデジタル身分証明書３０１の画像を読み取るデータ読取機能２０１と、前記読み取った画像から二次元コード部分３０４を取り出して二次元コードをデコードする二次元コード読取機能２０２と、データの復号化及び電子署名検証処理をする暗号処理機能２０３と、前記読み取ったデジタル身分証明書３０１の画像から名前等の属性情報３０３の文字を認識する文字認識機能２０６と、二次元コードに埋め込まれている特徴値と前記読み取ったデジタル身分証明書３０１の画像に含まれている顔写真画像３０２とを比較検証するマッチング機能２０７と、検証結果に応じて画面表示を行ったり、入退室管理のゲートの開閉指示を行ったりする検証結果処理機能２０８から構成できる。また、スマートフォン３０は、ネットワークまたは媒体渡し等で入手した該当デジタル身分証明書（画像データ）３０１をインストールして格納し、必要に応じて前記デジタル身分証明書３０１をディスプレイに表示させる機能を有する。

[0017] このような機能を有する発行装置１０、検証装置２０、スマートフォン３

0は、図2に例示するように一般的な情報処理装置40により実現できる。例えば、発行装置10の特徴値抽出機能106や暗号処理機能103や二次元コード生成機能102や身分証明書成型機能101や、検証装置20のデータ読取機能201や二次元コード読取機能202や暗号処理機能203や文字認識機能206やマッチング機能207や検証結果処理機能208は、CPU (CENTRAL PROCESSING UNIT) 等のCPU405により実行されるコンピュータプログラムとして実現できる。こうしたコンピュータプログラムは、例えば、ハードディスクなどの記憶装置404に予め格納・保持するか、或いはネットワークから配布を受け、メモリー403上に展開して利用することができる。

[0018] また、本デジタル身分証明書システム1を利用する利用者からの指示は、入力を受け付けるキーボードやマウス、タッチパネルなどの入力装置401にて入力され、また、その指示による処理結果は、液晶表示装置や有機EL (ELECTRO LUMINESCENCE) ディスプレイなどの出力装置402にて出力される。

[0019] 発行装置10、検証装置20、スマートフォン30のこれらの装置は、バスなどの内部通信線（以下、バスという）406で連結された情報処理装置40上に構成することができる。

[0020] また、検証装置20と繋がっている画像撮影機器21は、デジタルカメラ、WEBカメラ、スキャナー等の機器にて実現される。

[0021] ー処理手順例ー

以下、本実施形態1における手順について図に基づき説明する。以下で説明する各種動作は、デジタル身分証明書システム1を構成する各装置が、それぞれメモリー等に読み出して実行するプログラムによって実現される。

[0022] 図3は、本実施形態におけるデジタル身分証明書301の発行処理手順を示すシーケンス図である。

[0023] 発行装置10にデジタル身分証明書301の保有者となる人物の顔写真データ302を入力し、発行装置10は、特徴値抽出機能106より、その顔

写真データ 302 から、顔写真を一意に識別できる比較的小さなデータ量である特徴値（「目、鼻、口端などの顔の特徴点位置」や「目の部分だけ切り取った画像」など）を抽出する（ステップ S101）。そして発行装置 10 は、暗号処理機能 103 より、前記特徴値を検証装置 20 との共通鍵 K105 で暗号化する（ステップ S102）。また、発行装置 10 にデジタル身分証明書 301 の保有者となる人物の名前等の属性情報 303 を入力し、発行装置 10 は、その属性情報 303 を前記暗号化特徴値と連結する（ステップ S103）。次に発行装置 10 は、暗号化特徴値と属性情報 303 を連結したデータに対して、発行装置 10 の署名鍵 SK104 で電子署名値を計算し、暗号化特徴値と属性情報 303 を連結したデータに付与する（ステップ S104）。そして、二次元コード生成機能 102 より、連結した暗号化特徴値と属性情報 303 と電子署名データを入力として二次元コード 304 を生成する。即ち前記連結データの二次元コードエンコード化を行う（ステップ S105）。そして、発行装置 10 は、身分証明書成型機能 101 より、顔写真データ 302、属性情報 303、二次元コード 304 をスマートフォンのディスプレイに同時に表示できるように配置・成型し（ステップ S106）、デジタル身分証明書（画像データ）301 として外部出力する（ステップ S107）。

[0024] スマートフォン 30 は、ネットワークまたは媒体渡し等で前記デジタル身分証明書（画像データ）301 を取得し（ステップ S108）、前記デジタル身分証明書（画像データ）301 をスマートフォン 30 の記憶装置 404 に保管する（ステップ S109）。

[0025] 図 4 は、本実施形態 1 におけるデジタル身分証明書の検証処理手順を示すシーケンス図である。

[0026] スマートフォン 30 は、ステップ S109 で保管したデジタル身分証明書（画像データ）301 をスマートフォン 30 のディスプレイに表示し、画像撮影機器 21 に提示する（ステップ S200）。

[0027] 画像撮影機器 21 は、スマートフォン 30 のディスプレイに表示された画

像を撮影し（ステップS201）、検証装置20は画像撮影機器21が撮影した画面画像を画像撮影機器21から取得する（ステップS202）。そして検証装置20は二次元コード読取機能202より、ステップS202で取得した画面画像から二次元コードを読み取り、二次元コードをデコードする（ステップS203）。デコードされたデータは、暗号化特徴値、属性情報、電子署名値からなっており、それらのデータから暗号処理機能203を用いて電子署名の検証を行う（ステップS204）。署名検証に失敗した場合、エラー処理として例えば図5の左上の図の様に、検証装置20のディスプレイにデジタル身分証明書301の二次元コード304の部分に不正があって、署名検証に失敗した旨を表示する（ステップS205）。

[0028] 署名検証に成功した場合、ステップS202で取得した画面画像から文字認識機能206を用いて属性情報303に関する文字を認識し、ステップS203でデコードした属性情報と比較検証する（ステップS206）。両者の情報が一致しない場合、エラー処理として例えば図5の右上の図の様に、検証装置20のディスプレイにデジタル身分証明書301の属性情報303の部分に不正があり、属性情報が詐称されている旨と正しい属性情報を表示する（ステップS207）。

[0029] 属性情報が一致した場合、暗号処理機能203より、ステップS203でデコードした暗号化特徴値を共通鍵K205で復号し（ステップS208）、復号された特徴値とステップS202で取得した画面画像の顔写真部分とをマッチング機能207を用いて比較検証し、その特徴値がその顔写真から抽出されたデータであるかどうかを検証する（ステップS209）。マッチング機能207は顔写真と特徴値の相関関係を数値として表し、顔写真と特徴値とのマッチング率が閾値以下である場合、エラー処理として例えば図5の左下の図の様に、検証装置20のディスプレイにデジタル身分証明書301の顔写真302の部分に不正あり、顔写真が偽造されている旨を表示する（ステップS210）。

[0030] 顔写真と特徴値とのマッチング率が閾値以上である場合、真正結果処理と

して例えば図5の右下の図の様に、検証装置20のディスプレイにデジタル身分証明書301が正しいものである旨を表示する（ステップS210）。

実施例 2

[0031] 以下に本発明の実施形態2について図面を用いて詳細に説明する。実施形態2は実施形態1に追加する形で実施される。

[0032] 図6は、本実施形態2におけるデジタル身分証明書システム2の全体構成例を示す図（図1との差分）である。実施形態2では、検証装置20は人物撮影機器22とも繋がっており、顔写真302と人物撮影機器22で撮影された映像・画像からバイオメトリクス認証で用いられている顔認証機能209を介して、デジタル身分証明書301を提示した者が正しい保有者であるかどうかを検証するシステムである。検証装置と繋がっている人物撮影機器22は、デジタルカメラ、WEBカメラ等の機器にて実現される。

[0033] 尚、実施形態2では実施形態1と同様にデジタル身分証明書301が発行される。

[0034] 図7は、本実施形態2におけるデジタル身分証明書の検証処理手順およびデジタル身分証明書の保有者の認証処理手順を示すシーケンス図である。ステップS210までは実施形態1と同様の処理である。

[0035] 人物撮影機器22はデジタル身分証明書301を提示した人物を撮影し（ステップS301）、検証装置20は、人物撮影機器22からステップS301で撮影した人物画像を取得する（ステップS302）。そして検証装置20は、ステップS209で真正と判断された顔写真データとステップS301で取得した人物画像データとを顔認証機能209を用いて比較検証し、デジタル身分証明書301を提示した者が正しい保有者であるかどうかを検証する（ステップS303）。顔認証機能209は顔写真と人物画像の相関関係を数値として表し、顔写真と人物画像とのマッチング率が閾値以下である場合、エラー処理として例えば図8の上図の様に、検証装置20のディスプレイにデジタル身分証明書301の顔写真302とデジタル身分証明書301を提示した人物の顔とが一致していない旨を表示する（ステップS30

4)。

[0036] 顔写真と人物画像とのマッチング率が閾値以上である場合、真正結果処理として例えば図8の下図の様に、検証装置20のディスプレイにデジタル身分証明書301が真正で、デジタル身分証明書301を提示した人物の顔とが一致している旨を表示する(ステップS305)。

符号の説明

- [0037] 1 デジタル身分証明書システム
2 デジタル身分証明書システム
10 発行装置
20 検証装置
21 画像撮影機器
22 人物撮影機器
30 スマートフォン
40 情報処理装置
101 身分証明書成型機能
102 二次元コード生成機能
103 暗号処理機能
104 署名鍵SK
105 共通鍵K
106 特徴値抽出機能
201 データ読取機能
202 二次元コード読取機能
203 暗号処理機能
204 検証鍵PK
205 共通鍵K
206 文字認識機能
207 マッチング機能
208 検証結果処理機能

- 209 顔認証機能
- 301 デジタル身分証明書
- 302 顔写真
- 303 属性情報
- 304 二次元コード
- 401 入力装置
- 402 出力装置
- 403 メモリー
- 404 記憶装置
- 405 CPU (CENTRAL PROCESSING UNIT)
- 406 バス

請求の範囲

- [請求項1] 画像を読み取り、当該画像から識別子画像と顔画像とを抽出する抽出部と、
- 前記識別子画像に含まれる電子署名から、当該識別子画像を検証する識別子画像検証部、
- 前記顔画像から抽出した第一の特徴値情報と、前記識別子画像に含まれる第二の特徴値情報と、を比較し前記画像情報の真正性を検証する画像検証部と、
- を備えることを特徴とする画像情報検証装置。
- [請求項2] 請求項1に記載の画像情報検証装置において、
- 前記抽出部は更に、前記画像から前記顔画像に関する属性情報画像を抽出し、
- 前記画像検証部は、更に、前記識別子画像に含まれる属性情報と、前記抽出した属性情報画像と、を比較し前記画像情報の真正性を検証することを特徴とする画像情報検証装置。
- [請求項3] 請求項2に記載の画像情報検証装置において、
- 前記第一の特徴値及び第二の特徴値とは、顔の特徴点位置に関する情報であることを特徴とする画像情報検証装置。
- [請求項4] 請求項3に記載の画像情報検証装置において、
- 更に、前記検証の結果を表示する表示部を備えることを特徴とする画像情報検証装置。
- [請求項5] 請求項4に記載の画像情報検証装置と、撮影装置と、を備える認証システムであって、
- 前記画像情報検証装置は、更に、前記撮影装置にて撮影された撮影画像と、前記顔画像と、を比較し当該撮影装置にて撮影された対象を認証する認証部を備えることを特徴とする認証システム。
- [請求項6] 請求項5に記載の認証システムにおいて、
- 前記認証部は、特徴値を用いて前記撮影画像と前記顔画像の比較を

することを特徴とする認証システム。

[請求項7] 請求項6に記載の認証システムにおいて、
更に、前記対象の認証の結果に応じた処理を行うゲートを備えることを特徴とする認証システム。

[請求項8] 請求項7に記載の認証システムにおいて、
前記識別子画像は、前記第二の特徴値を公開鍵で暗号化して作成されることを特徴とする認証システム。

[請求項9] 画像を読み取る画像読み取りステップと、
前記画像から識別子画像と顔画像とを抽出する抽出ステップと、
前記識別子画像に含まれる電子署名から、当該識別子画像を検証する識別子画像検証ステップと、
前記顔画像から抽出した第一の特徴値情報と、前記識別子画像に含まれる第二の特徴値情報と、を比較し前記画像情報の真正性を検証する画像検証ステップと、
を備えることを特徴とする画像情報検証方法。

[請求項10] 画像を読み取る画像読み取りステップと、
前記画像から識別子画像と顔画像とを抽出する抽出ステップと、
前記識別子画像に含まれる電子署名から、当該識別子画像を検証する識別子画像検証ステップと、
前記顔画像から抽出した第一の特徴値情報と、前記識別子画像に含まれる第二の特徴値情報と、を比較し前記画像情報の真正性を検証する画像検証ステップと、
撮影装置にて撮影された撮影画像と、前記顔画像と、を比較し当該撮影装置にて撮影された対象を認証する認証ステップと、
を備えることを特徴とする認証方法。