(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2009-64352
(P2009-64352A)
(43)公開日　平成21年3月26日(2009.3.26)

(51)Int.Cl.		F I			テーマコード（参考）
G06T 7/00	(2006.01)	G06T	7/00	570	5B043
G06F 21/20	(2006.01)	G06F	15/00	330F	5B285
H04L 9/32	(2006.01)	G06T	7/00	510B	5J104
		H04L	9/00	673D	

審査請求 未請求　請求項の数 6　ＯＬ　（全 14 頁）

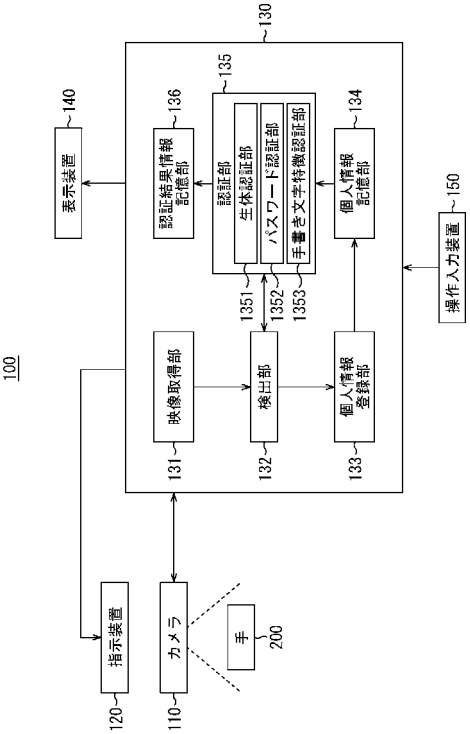
(21)出願番号　特願2007-233253 (P2007-233253)
(22)出願日　平成19年9月7日 (2007.9.7)

(71)出願人　504258527
国立大学法人　鹿児島大学
鹿児島県鹿児島市郡元一丁目２１番２４号
(74)代理人　100090273
弁理士　國分　孝悦
(72)発明者　佐藤　公則
鹿児島県鹿児島市郡元一丁目２１番２４号
国立大学法人　鹿児島大学内
(72)発明者　鹿嶋　雅之
鹿児島県鹿児島市郡元一丁目２１番２４号
国立大学法人　鹿児島大学内
(72)発明者　崎田　隆行
鹿児島県鹿児島市郡元一丁目２１番２４号
国立大学法人　鹿児島大学内

最終頁に続く

(54)【発明の名称】個人認証システム及び個人認証方法

(57)【要約】
【課題】個人認証を行う際に、非接触で、且つ、従来よりもセキュリティ性の向上を実現できるようにする。
【解決手段】個人認証を行う個人認証システム１００において、手２００の撮影を行うカメラ１１０と、カメラ１１０において撮影された手２００の映像を取得する映像取得部１３１と、映像取得部１３１で取得した手２００の映像に基づいて、当該手２００の生体情報、及び、当該手２００の指で描かれた手書き文字による手書き文字情報を検出する検出部１３２と、検出部１３２で検出された手２００の生体情報を用いて生体認証を行う生体認証部１３５１と、生体認証部１３５１による生体認証の結果に応じて、検出部１３２で検出された手書き文字情報を用いてパスワード認証を行うパスワード認証部１３５２を有するようにする。
【選択図】図２



【特許請求の範囲】
【請求項１】
手の撮影を行うカメラと、
前記カメラにおいて撮影された手の映像を取得する映像取得部と、
前記映像取得部で取得した手の映像に基づいて、当該手の生体情報、及び、当該手の指で描かれた手書き文字による手書き文字情報を検出する検出部と、
前記手の生体情報を用いて生体認証を行う生体認証部と、
前記生体認証部による生体認証の結果に応じて、前記手書き文字情報を用いてパスワード認証を行うパスワード認証部と
を有することを特徴とする個人認証システム。
【請求項２】
前記検出部は、前記手書き文字に係る特徴を示す手書き文字特徴情報を更に検出するものであり、
前記パスワード認証部によるパスワード認証の結果に応じて、前記手書き文字特徴情報を用いて手書き文字特徴認証を行う手書き文字特徴認証部を更に有することを特徴とする請求項１に記載の個人認証システム。
【請求項３】
認証対象者の手の生体情報、当該認証対象者におけるパスワード情報、及び、当該認証対象者が前記パスワード情報を手書き文字とした際の特徴を示す手書き文字特徴情報を、認証対象者ごとに個人情報として予め登録する処理を行う個人情報登録部を更に有し、
前記生体認証部は、前記個人情報登録部により認証対象者ごとに登録された手の生体情報と、前記検出部で検出された手の生体情報との照合の結果に基づいて、前記生体認証を行い、
前記パスワード認証部は、前記個人情報登録部により登録され、前記生体認証部により認定された認証対象者における前記パスワード情報と、前記検出部で検出された手書き文字情報との照合の結果に基づいて、前記パスワード認証を行い、
前記手書き文字特徴認証部は、前記個人情報登録部により登録され、前記生体認証部により認定された認証対象者における手書き文字特徴情報と、前記検出部で検出された手書き文字特徴情報との照合の結果に基づいて、前記手書き文字特徴認証を行うことを特徴とする請求項２に記載の個人認証システム。
【請求項４】
前記パスワード情報を要求する指示を行う指示装置を更に有し、
前記手書き文字情報は、前記指示装置により前記パスワード情報を要求する指示が行われた後に、前記検出部で検出された前記手書き文字による情報であることを特徴とする請求項３に記載の個人認証システム。
【請求項５】
前記手書き文字特徴情報は、前記手書き文字の形、前記手書き文字の筆順、及び、前記手書き文字のスピードの３つの情報を含むことを特徴とする請求項２乃至４のいずれか１項に記載の個人認証システム。
【請求項６】
手の撮影を行うカメラを備えた個人認証システムにおける個人認証方法であって、
前記カメラにおいて撮影された手の映像を取得する映像取得ステップと、
前記映像取得ステップで取得された手の映像に基づいて、当該手の生体情報、及び、当該手の指で描かれた手書き文字による手書き文字情報を検出する検出ステップと、
前記手の生体情報を用いて生体認証を行う生体認証ステップと、
前記生体認証ステップによる生体認証の結果に応じて、前記手書き文字情報を用いてパスワード認証を行うパスワード認証ステップと
を有することを特徴とする個人認証方法。
【発明の詳細な説明】
【技術分野】

【０００１】
本発明は、個人認証を行う個人認証システム及び個人認証方法に関するものである。
【背景技術】
【０００２】
近時では、セキュリティ向上の観点から、セキュリティキーとして、手の指紋や静脈パターンなどの生体的特徴を用いた認証が提案されて実現されている（例えば、下記の特許文献１及び特許文献２参照）。
【０００３】
【特許文献１】特開２００２－４９９１３号公報
【特許文献２】特開２００７－１１５０７２号公報
【発明の開示】
【発明が解決しようとする課題】
【０００４】
これまで、手の指紋や静脈パターンなどの生体的特徴を用いた個人認証システムは、生体的特徴の複製の困難さなどから、極めて堅牢であると考えられてきた。しかしながら、人工指の研究など、手の指紋などによる生体認証の脆弱性を示唆する例も挙げられている。このため、一度、生体的特徴の複製技術が確立し、生体的特徴が漏洩してしまうと、セキュリティ性の確保が困難になるという問題があった。
【０００５】
また、上述した手の指紋や静脈パターンなどの生体的特徴を用いた個人認証システムでは、認証を行う際に、手などを入力センサに対して接触させる必要がある。これは、入力センサに不特定多数の人が接触することになり、例えば、潔癖症の人には、嫌悪感を与えるという問題があった。
【０００６】
本発明は上述の問題点に鑑みてなされたものであり、個人認証を行う際に、非接触で、且つ、従来よりもセキュリティ性の向上を実現できるようにすることを目的とする。
【課題を解決するための手段】
【０００７】
本発明の個人認証システムは、手の撮影を行うカメラと、前記カメラにおいて撮影された手の映像を取得する映像取得部と、前記映像取得部で取得した手の映像に基づいて、当該手の生体情報、及び、当該手の指で描かれた手書き文字による手書き文字情報を検出する検出部と、前記手の生体情報を用いて生体認証を行う生体認証部と、前記生体認証部による生体認証の結果に応じて、前記手書き文字情報を用いてパスワード認証を行うパスワード認証部とを有する。
【０００８】
本発明の個人認証方法は、手の撮影を行うカメラを備えた個人認証システムにおける個人認証方法であって、前記カメラにおいて撮影された手の映像を取得する映像取得ステップと、前記映像取得ステップで取得された手の映像に基づいて、当該手の生体情報、及び、当該手の指で描かれた手書き文字による手書き文字情報を検出する検出ステップと、前記手の生体情報を用いて生体認証を行う生体認証ステップと、前記生体認証ステップによる生体認証の結果に応じて、前記手書き文字情報を用いてパスワード認証を行うパスワード認証ステップとを有する。
【発明の効果】
【０００９】
本発明によれば、個人認証を行う際に、非接触で、且つ、従来よりもセキュリティ性の向上を実現することができる。
【発明を実施するための最良の形態】
【００１０】
以下に、本発明を実施するための最良の形態について説明する。
【００１１】

図１は、本発明の実施形態に係る個人認証システムの外観の一例を示す模式図である。

図１に示すように、個人認証システム１００は、カメラ１１０と、指示装置１２０と、情報処理装置１３０と、表示装置１４０と、操作入力装置１５０を有して構成されている。

【００１２】

カメラ１１０は、情報処理装置１３０による制御に基づいて、個人認証を行う認証対象者の手２００の撮影を行うものである。

【００１３】

指示装置１２０は、情報処理装置１３０による制御に基づいて、認証対象者に対して各種の要求を指示するものである。ここで、指示装置１２０は、例えば、認証対象者に対する各種の要求に係る指示を文字等で表示する表示装置、若しくは、認証対象者に対する各種の要求に係る指示を音声として出力する音声出力装置、又は、これらを組み合わせた装置から構成されている。

【００１４】

情報処理装置１３０は、個人認証システム１００における動作を統括的に制御するものである。

【００１５】

表示装置１４０は、情報処理装置１３０による制御に基づいて、カメラ１１０で撮影された映像を表示したり、各種の情報を表示したりする。

【００１６】

操作入力装置１５０は、例えばセキュリティ管理者や認証対象者等の操作者が情報処理装置１３０に対して情報の入力を行う際に操作されるものである。この操作入力装置１５０は、例えば、キーボード１５０ａや、ポインティング・デバイスであるマウス１５０ｂを具備して構成されている。

【００１７】

図２は、本発明の実施形態に係る個人認証システムの機能構成の一例を示す模式図である。ここで、図２において、図１と同様の構成については、同じ符号を付しており、その詳細な説明は省略する。

【００１８】

情報処理装置１３０は、映像取得部１３１、検出部１３２、個人情報登録部１３３、個人情報記憶部１３４、認証部１３５、及び、認証結果情報記憶部１３６の各機能構成を有している。本実施形態においては、例えば、情報処理装置１３０のＣＰＵ及びＲＯＭ内に記録されるプログラムから、上述した各部１３１～１３３及び１３５が構成され、例えば、情報処理装置１３０のＲＡＭに、上述した記憶部１３４及び１３６が備えられるものとする。

【００１９】

映像取得部１３１は、カメラ１１０において撮影された映像を取得する処理を行う。特に、本実施形態では、映像取得部１３１は、カメラ１１０において撮影された手２００の映像を取得する処理を行う。

【００２０】

検出部１３２は、映像取得部１３１で取得した手２００の映像に基づいて、当該手２００の生体情報、及び、当該手２００の指で描かれた手書き文字による手書き文字情報、並びに、当該手書き文字に係る特徴を示す手書き文字特徴情報を検出する処理を行う。

【００２１】

個人情報登録部１３３は、認証対象者の手の生体情報、当該認証対象者におけるパスワード情報、及び、当該認証対象者が前記パスワード情報を手書き文字とした際の特徴を示す手書き文字特徴情報を、認証対象者ごとに個人情報として予め個人情報記憶部１３４に記憶して登録する処理を行う。例えば、個人情報登録部１３３は、操作入力装置１５０から予め入力された認証対象者におけるパスワード情報を取得すると共に、検出部１３２で予め検出された当該認証対象者の手の生体情報、及び、当該認証対象者の手の指で描かれ

た手書き文字に係る特徴を示す手書き文字特徴情報を取得して、取得した情報を個人情報として個人情報記憶部１３４に登録する処理を行う。

【００２２】

図３は、個人情報登録部１３３により個人情報記憶部１３４に登録された個人情報の一例を示す模式図である。

図３では、登録された認証対象者の順番等に応じてＩＤ番号が１、２、３、・・・と付されている。また、図３には、認証対象者ごとに個人情報として、当該認証対象者の手の生体情報、当該認証対象者におけるパスワード情報、及び、当該認証対象者の手の指で描かれた手書き文字特徴情報が示されている。

【００２３】

ここで、図３に示す例では、手の生体情報として、手の形及び指の形などが示されており、また、手書き文字特徴情報として、手書き文字の形、手書き文字の筆順（書き順）、及び、手書き文字のスピードが示されている。また、図３に示す例では、ＩＤ番号が１の認証対象者におけるパスワード情報として「佐藤」が示されており、ＩＤ番号が２の認証対象者におけるパスワード情報として「鹿嶋」が示されており、ＩＤ番号が３の認証対象者におけるパスワード情報として「崎田」が示されている。

【００２４】

認証部１３５は、個人情報登録部１３３により個人情報記憶部１３４に登録された個人情報と、検出部１３２で検出された各種の情報とを照合することにより、各種の認証処理を行う。具体的に、認証部１３５は、生体認証を行う生体認証部１３５１と、パスワード認証を行うパスワード認証部１３５２と、手書き文字特徴認証を行う手書き文字特徴認証部１３５３の各機能構成を有している。

【００２５】

図４は、認証部１３５における生体認証部１３５１、パスワード認証部１３５２、及び手書き文字特徴認証部１３５３の各認証処理の一例を示すイメージ図である。

図４には、具体的に、図４（ａ）に生体認証部１３５１による生体認証処理の一例が示され、図４（ｂ）にパスワード認証部１３５２によるパスワード認証処理の一例が示され、図４（ｃ）に手書き文字特徴認証部１３５３による手書き文字特徴認証処理の一例が示されている。

【００２６】

まず、生体認証部１３５１は、検出部１３２で検出された手の生体情報を用いて生体認証を行う。

具体的には、図４（ａ）に示すように、カメラ１１０において手２００（手２００の甲）の撮影が行われ、検出部１３２で手２００の生体情報が検出されると、生体認証部１３５１は、個人情報登録部１３３により認証対象者ごとに個人情報記憶部１３４に登録された図３に示す手の生体情報と、検出部１３２で検出された手の生体情報との照合の結果に基づいて、生体認証を行う。この際、個人情報記憶部１３４に登録された手の生体情報の中に、検出部１３２で検出された手の生体情報と合致すると判定できるものがある場合には、生体認証がＯＫであると判断される。そして、この場合、検出部１３２で検出された手の生体情報と合致すると判定された個人情報記憶部１３４の手の生体情報におけるＩＤ番号が抽出され、ＩＤ番号が決定される。

【００２７】

続いて、パスワード認証部１３５２は、生体認証部１３５１による生体認証の結果に応じて、検出部１３２で検出された手書き文字情報を用いてパスワード認証を行う。

具体的には、図４（ｂ）に示すように、認証対象者に対して、例えば「あなたの名前を漢字で入力してください。」とのパスワード情報を要求する指示が指示装置１２０から行われた後に、検出部１３２で手書き文字情報が検出されると、パスワード認証部１３５２は、個人情報登録部１３３により登録され、生体認証部１３５１により認定された（即ち、決定されたＩＤ番号の）認証対象者における図３に示すパスワード情報と、検出部１３２で検出された手書き文字情報との照合の結果に基づいて、パスワード認証を行う。この

際、図４（ｂ）に示す例では、検出部１３２で「崎田」の手書き文字情報が検出されており、生体認証部１３５１で認定された認証対象者のＩＤ番号が３である場合には、図３に示すパスワード情報から、パスワード認証がＯＫであると判断される。

【００２８】

続いて、手書き文字特徴認証部１３５３は、パスワード認証部１３５２によるパスワード認証の結果に応じて、検出部１３２で検出された手書き文字特徴情報を用いて手書き文字特徴認証を行う。

具体的には、図４（ｃ）に示すように、検出部１３２で手書き文字特徴情報が検出されると、手書き文字特徴認証部１３５３は、個人情報登録部１３３により登録され、生体認証部１３５１により認定された（即ち、決定されたＩＤ番号の）認証対象者における図３に示す手書き文字特徴情報と、検出部１３２で検出された手書き文字特徴情報との照合の結果に基づいて、手書き文字特徴認証を行う。この際、本実施形態の手書き文字特徴認証においては、図４（ｃ）に示すように、手書き文字特徴情報である手書き文字の形、手書き文字の筆順、及び、手書き文字のスピードの各要素を統合した判断に基づく認証が行われる。そして、手書き文字特徴認証部１３５３は、照合の結果、手書き文字特徴情報が合致したと判断した場合には、手書き文字特徴認証がＯＫであると判断する。

【００２９】

そして、認証部１３５は、各認証部１３５１～１３５３により行われた認証結果を認証結果情報として、認証結果情報記憶部１３６に記憶する。

【００３０】

その後、必要に応じて、情報処理装置１３０は、認証結果情報記憶部１３６に記憶されている認証結果情報を表示装置１４０に表示し、また、当該認証結果情報を指示装置１２０から報知する。また、情報処理装置１３０は、必要に応じて、例えば、認証結果情報記憶部１３６に記憶されている認証結果情報を、ネットワーク（不図示）を介して外部装置に送信する。

【００３１】

次に、個人認証システム１００における個人認証方法の処理手順について説明する。

以下には、まず、個人認証システム１００における個人認証を行う前に予め行われる個人情報登録部１３３による個人情報登録処理について説明する。

【００３２】

図５は、本発明の実施形態に係る個人認証システムの個人情報登録部１３３による個人情報登録処理の処理手順の一例を示すフローチャートである。

【００３３】

個人認証システム１００において個人情報登録処理モードとなり、例えば、認証対象者（或いはセキュリティ管理者）から操作入力装置１５０を介して情報処理装置１３０に認証対象者のパスワード情報が入力されると、ステップＳ１０１において、個人情報登録部１３３は、入力されたパスワード情報を設定する。ここで、認証対象者が自己のパスワード情報を人力する場合には、操作入力装置１５０は、認証対象者の近傍に設けられているものとし、また、セキュリティ管理者が認証対象者のパスワード情報を人力する場合には、セキュリティ管理者が認証対象者からパスワード情報を得て入力を行うものとする。なお、本実施形態では、パスワード情報が操作入力装置１５０を介して入力される形態を示すが、例えば、指示装置１２０からパスワード情報を手書き文字で入力する旨の指示を行い、その後、検出部１３２で検出された手書き文字情報をパスワード情報として設定する形態であっても適用可能である。

【００３４】

続いて、指示装置１２０から手の生体情報を設定する旨の指示を行い、その後、検出部１３２で手の生体情報が検出されると、ステップＳ１０２において、個人情報登録部１３３は、検出部１３２で検出された手の生体情報を設定する。

【００３５】

続いて、指示装置１２０からパスワード情報を手書き文字で入力し手書き文字特徴情報

を設定する旨の指示を行い、その後、検出部１３２で手書き文字特徴情報が検出されると、ステップＳ１０３において、個人情報登録部１３３は、検出部１３２で検出された手書き文字特徴情報を設定する。

【００３６】

続いて、ステップＳ１０４において、個人情報登録部１３３は、ステップＳ１０１～Ｓ１０３で設定したパスワード情報、手の生体情報及び手書き文字特徴情報を、当該認証対象者における個人情報として、個人情報記憶部１３４に登録する。これにより、例えば、図３に示すような個人情報が、登録された認証対象者の順番等に応じてＩＤ番号が付されて認証対象者ごとに登録される。

【００３７】

図６は、本発明の実施形態に係る個人認証システムにおける個人認証方法の処理手順の一例を示すフローチャートである。なお、図６に示すフローチャートにおいては、カメラ１１０による撮影が継続的に行われており、映像取得部１３１は、カメラ１１０において撮影された映像を継続的に取得しているものとする。

【００３８】

まず、ステップＳ２０１において、検出部１３２は、映像取得部１３１で取得した映像中に手２００が存在することを検出したか否かを判断する。この判断の結果、映像取得部１３１で取得した映像中に手２００が存在することを検出していない（即ち、映像中に手２００が存在しないことを検出している）場合には、検出部１３２が映像中に手２００が存在することを検出するまで、ステップＳ２０１で待機する。

【００３９】

一方、ステップＳ２０１の判断の結果、映像取得部１３１で取得した映像中に手２００が存在することを検出した場合には、情報処理装置１３０による制御に基づいて指示装置１２０から手２００の生体情報を取得するための撮影を行う旨の指示を行い、その後、ステップＳ２０２に進む。

【００４０】

ステップＳ２０２に進むと、検出部１３２は、図４（ａ）に示すようにしてカメラ１１０で撮影され、映像取得部１３１で取得された手２００（手２００の甲）の映像に基づいて、手２００の生体情報を検出する。ここで、本実施形態では、手２００の生体情報として、図３に示すように、手の形及び指の形などが検出されることになる。

【００４１】

続いて、ステップＳ２０３において、認証部１３５における生体認証部１３５１は、個人情報記憶部１３４に登録されている図３に示す手の生体情報と、ステップＳ２０２で検出された手２００の生体情報との照合を行い、生体認証がＯＫであるか否かを判断する。具体的に、ステップＳ２０３では、個人情報記憶部１３４に登録された手の生体情報の中に、ステップＳ２０２で検出された手２００の生体情報と合致すると判定できるものがあるか否かを判断し、合致すると判定できるものがある場合には、生体認証がＯＫであると判断される。換言すれば、ステップＳ２０３では、現在、個人認証を行っている認証対象者が、予め個人情報記憶部１３４に登録されている登録者であるか否かが判断される。

【００４２】

ステップＳ２０３の判断の結果、生体認証がＮＧである（即ち、現在、個人認証を行っている認証対象者が登録者でない）場合には、個人認証システム１００は、個人情報登録処理モードに移行する。そして、この場合、指示装置１２０から、生体認証がＮＧであり個人情報登録処理モードに移行する旨の指示がなされ、図５に示すフローチャートの処理が行われることになる。

【００４３】

一方、ステップＳ２０３の判断の結果、生体認証がＯＫである（即ち、現在、個人認証を行っている認証対象者が登録者である）場合には、ステップＳ２０４に進む。ステップＳ２０４に進むと、認証部１３５は、ステップＳ２０３において、検出部１３２で検出された手２００の生体情報と合致すると判定された個人情報記憶部１３４の手の生体情報に

おけるＩＤ番号を抽出し、認証対象の個人情報におけるＩＤ番号を決定する。

【００４４】

続いて、ステップＳ２０５において、情報処理装置１３０は、認証対象者に対して、指示装置１２０からパスワード情報を要求する指示を行う。本実施形態では、例えば、図４（ｂ）に示すように、「あなたの名前を漢字で入力してください。」とのパスワード情報を要求する指示を行う。

【００４５】

続いて、ステップＳ２０６において、検出部１３２は、カメラ１１０において撮影され、映像取得部１３１で取得された手２００の映像から、手２００の指先点の検出を行う。具体的に、図４（ｂ）に示す例では、手２００の人差し指における指先点の検出が行われる。

【００４６】

続いて、ステップＳ２０７において、検出部１３２は、ステップＳ２０６で検出した手２００の指（図４（ｂ）に示す例では人差し指）で描かれた手書き文字による手書き文字情報を検出する。

【００４７】

続いて、ステップＳ２０８において、認証部１３５におけるパスワード認証部１３５２は、ステップＳ２０４で決定されたＩＤ番号の認証対象者における図３に示すパスワード情報と、ステップＳ２０７で検出された手書き文字情報との照合を行い、パスワード認証がＯＫであるか否かを判断する。具体的に、ステップＳ２０８では、ステップＳ２０４で決定されたＩＤ番号の認証対象者における図３に示すパスワード情報と、ステップＳ２０７で検出された手書き文字情報とが合致すれば、パスワード認証がＯＫと判断される。

【００４８】

ステップＳ２０８の判断の結果、パスワード認証がＯＫである場合には、ステップＳ２０９に進む。ステップＳ２０９に進むと、検出部１３２は、ステップＳ２０６で検出した手２００の指（図４（ｂ）に示す例では人差し指）で描かれた手書き文字に係る特徴を示す手書き文字特徴情報を検出する。ここで、本実施形態では、手書き文字特徴情報として、図３及び図４（ｃ）に示すように、手書き文字の形、手書き文字の筆順、及び、手書き文字のスピードなどが検出されることになる。

【００４９】

続いて、ステップＳ２１０において、認証部１３５における手書き文字特徴認証部１３５３は、ステップＳ２０４で決定されたＩＤ番号の認証対象者における図３に示す手書き文字特徴情報と、ステップＳ２０９で検出された手書き文字特徴情報との照合を行い、手書き文字特徴認証がＯＫであるか否かを判断する。具体的に、ステップＳ２１０では、ステップＳ２０４で決定されたＩＤ番号の認証対象者における図３に示す手書き文字特徴情報と、ステップＳ２０９で検出された手書き文字特徴情報とが合致したと判断された場合には、手書き文字特徴認証がＯＫと判断される。このステップＳ２１０における手書き文字特徴認証において、署名動作の認証（行動様式による認証）がなされることになる。

【００５０】

ステップＳ２１０の判断の結果、手書き文字特徴認証がＯＫである場合には、ステップＳ２１１に進む。ステップＳ２１１に進むと、認証部１３５は、ステップＳ２０３の生体認証部１３５１による生体認証、ステップＳ２０８のパスワード認証部１３５２によるパスワード認証、及び、ステップＳ２１０の手書き文字特徴認証部１３５３による手書き文字特徴認証の全ての認証がＯＫとなったことから、当該認証対象者における個人認証をＯＫとする処理を行う。その後、認証部１３５は、個人認証ＯＫの結果を認証結果情報として、認証結果情報記憶部１３６に記憶する。

【００５１】

一方、ステップＳ２０８でパスワード認証がＮＧであると判断された場合、或いは、ステップＳ２１０で手書き文字特徴認証がＮＧであると判断された場合には、ステップＳ２１２に進む。ステップＳ２１２に進むと、認証部１３５は、ステップＳ２０８のパスワー

ド認証部１３５２によるパスワード認証、又は、ステップＳ２１０の手書き文字特徴認証部１３５３による手書き文字特徴認証がＮＧとなったことから、当該認証対象者における個人認証をＮＧとする処理を行う。その後、認証部１３５は、個人認証ＮＧの結果を認証結果情報として、認証結果情報記憶部１３６に記憶する。

【００５２】

ステップＳ２１１の処理が終了した場合、或いは、ステップＳ２１２の処理が終了した場合には、ステップＳ２１３に進む。ステップＳ２１３に進むと、情報処理装置１３０は、認証結果情報記憶部１３６に記憶されている認証結果情報を表示装置１４０に表示する。これにより、ステップＳ２１２で個人認証ＮＧとされた場合には、表示装置１４０に個人認証ＮＧである旨の表示がなされ、ステップＳ２１１で個人認証ＯＫとされた場合には、表示装置１４０に個人認証ＯＫである旨の表示がなされる。また、情報処理装置１３０は、必要に応じて、例えば、認証結果情報記憶部１３６に記憶されている認証結果情報を、指示装置１２０から当該認証対象者に報知したり、ネットワーク（不図示）を介して外部装置に送信したりする。

【００５３】

以上のステップＳ２０１～ステップＳ２１３の処理を経ることにより、生体認証、パスワード認証、及び、手書き文字特徴認証による段階的な個人認証処理が行われる。

【００５４】

なお、本実施形態では、手の生体情報として、図３に示すように、手の形や指の形などの例を示したが、さらに、例えば、手の大きさや長さ、指の大きさや長さ、手の色、爪の形、指の太さなどを適用することも可能である。

【００５５】

また、本実施形態では、手書き文字特徴情報として、手書き文字の形、手書き文字の筆順、及び、手書き文字のスピードの３つの特徴情報を適用した例を示している。この点、本実施形態の手書き文字特徴認証においては、この３つの特徴情報の全てが合致しているか否かを判断し、この３つの特徴情報の全てが合致している場合に、手書き文字特徴認証がＯＫと判断される。これは、例えば、手書き文字のスピードが合致せずに登録されたものよりもゆっくり書かれた場合に、手書き文字の形を似せて書くことも可能であり、このような場合であっても、手書き文字特徴認証ＮＧと判断できるようにするためである。

【００５６】

以上説明したように、本実施形態の個人認証システム１００では、カメラ１１０において撮影され、映像取得部１３１で取得された手２００の映像に基づいて、検出部１３２で当該手２００の生体情報、及び、当該手２００の指で描かれた手書き文字による手書き文字情報を検出し、検出部１３２で検出された手２００の生体情報を用いて生体認証部１３５１で生体認証を行い、また、生体認証部１３５１による生体認証の結果に応じて、検出部１３２で検出された手書き文字情報を用いてパスワード認証部１３５２でパスワード認証を行うようにしている。即ち、本実施形態の個人認証システム１００では、手２００の生体情報をキーとし、当該個人認証システム１００が指示するパスワードの指先署名による手書き文字情報に基づいて、個人認証を行うようにしている。

かかる構成によれば、個人認証を行う際に、手２００の映像に基づいて認証処理を行うため、非接触で個人認証を行うことができ、且つ、仮に、手２００の生体情報が漏洩した場合であっても手書き文字情報を用いたパスワード認証を併せて行っているため、従来よりもセキュリティ性の向上を実現することができる。

【００５７】

また、本実施形態の個人認証システム１００では、更に、検出部１３２において、手２００の指で描かれた手書き文字に係る特徴を示す手書き文字特徴情報を検出し、パスワード認証部１３５２によるパスワード認証の結果に応じて、検出部１３２で検出された手書き文字特徴情報を用いて手書き文字特徴認証部１３５３で手書き文字特徴認証を行うようにしている。

かかる構成によれば、個人認証を行う際に、手２００の生体情報による生体認証及び手

書き文字情報によるパスワード認証に加えて、更に、手書き文字特徴情報による手書き文字特徴認証を行うようにしたので、セキュリティ性の更なる向上を実現することができる。

【００５８】

上述したように、本実施形態の個人認証システム１００は、手２００の生体情報による生体認証に加えて、手２００の指先署名による対話型の認証システムを提供するものである。即ち、本実施形態の個人認証システム１００は、カメラ１１０から得られた手及び指の映像を入力デバイスとすることによって、生体認証、当該個人認証システム１００から指示されたパスワードによるパスワード認証、及び、手書き文字の形や筆順、スピードなどの署名時の特徴（行動様式）による手書き文字特徴認証を効果的に複合し、堅牢な認証システムを提供することが可能となる。また、本実施形態の個人認証システム１００は、複合型の複雑な認証システムであるが、対話型（即ち、指示装置１２０から認証対象者に対してその都度指示を行う）の認証システムであるため、認証対象者は、複合型の複雑な認証システムであることを意識すること無く利用することができ、認証対象者の負担をより軽減させた認証システムを提供することが可能となる。また、不正認証対象者の生体情報や行動様式等に関する情報が収集可能であり、これにより、不正認証対象者の監視及び発見が容易となる。また、本実施形態の個人認証システム１００では、生体認証がＯＫとなった際に（Ｓ２０３／ＹＥＳ）、ＩＤ番号を決定する処理を行うため（Ｓ２０４）、認証対象者は、別途、氏名やＩＤカード等を呈示する必要がない。また、本実施形態の個人認証システム１００では、生体認証、パスワード認証、及び、手書き文字特徴認証を段階的に行うことにより、万が一、生体情報やパスワード情報の漏洩に対しても、より安全な認証を行うことが可能である。

【００５９】

前述した本実施形態に係る個人認証システム１００の情報処理装置１３０における図２の各機能構成、並びに当該個人認証システム１００における処理手順を示す図５及び図６の各ステップは、コンピュータのＲＡＭやＲＯＭなどに記憶されたプログラムが動作することによって実現できる。このプログラム及び当該プログラムを記録したコンピュータ読み取り可能な記憶媒体は本発明に含まれる。

【００６０】

具体的に、前記プログラムは、例えばＣＤ－ＲＯＭのような記憶媒体に記録し、或いは各種伝送媒体を介し、コンピュータに提供される。前記プログラムを記録する記憶媒体としては、ＣＤ－ＲＯＭ以外に、フレキシブルディスク、ハードディスク、磁気テープ、光磁気ディスク、不揮発性メモリカード等を用いることができる。他方、前記プログラムの伝送媒体としては、プログラム情報を搬送波として伝搬させて供給するためのコンピュータネットワーク（ＬＡＮ、インターネットの等のＷＡＮ、無線通信ネットワーク等）システムにおける通信媒体を用いることができる。また、この際の通信媒体としては、光ファイバ等の有線回線や無線回線などが挙げられる。

【００６１】

また、本発明は、コンピュータが供給されたプログラムを実行することにより本実施形態に係る個人認証システム１００の機能が実現される態様に限られない。そのプログラムがコンピュータにおいて稼働しているＯＳ（オペレーティングシステム）或いは他のアプリケーションソフト等と共同して本実施形態に係る個人認証システム１００の機能が実現される場合も、かかるプログラムは本発明に含まれる。また、供給されたプログラムの処理の全て、或いは一部がコンピュータの機能拡張ボードや機能拡張ユニットにより行われて本実施形態に係る個人認証システム１００の機能が実現される場合も、かかるプログラムは本発明に含まれる。

【００６２】

また、前述した本実施形態は、何れも本発明を実施するにあたっての具体化の例を示したものに過ぎず、これらによって本発明の技術的範囲が限定的に解釈されてはならないものである。即ち、本発明はその技術思想、またはその主要な特徴から逸脱することなく、

様々な形で実施することができる。

【図面の簡単な説明】

【００６３】

【図１】本発明の実施形態に係る個人認証システムの外観の一例を示す模式図である。

【図２】本発明の実施形態に係る個人認証システムの機能構成の一例を示す模式図である。

【図３】個人情報登録部により個人情報記憶部に登録された個人情報の一例を示す模式図である。

【図４】認証部における生体認証部、パスワード認証部、及び手書き文字特徴認証部の各認証処理の一例を示すイメージ図である。

【図５】本発明の実施形態に係る個人認証システムの個人情報登録部による個人情報登録処理の処理手順の一例を示すフローチャートである。

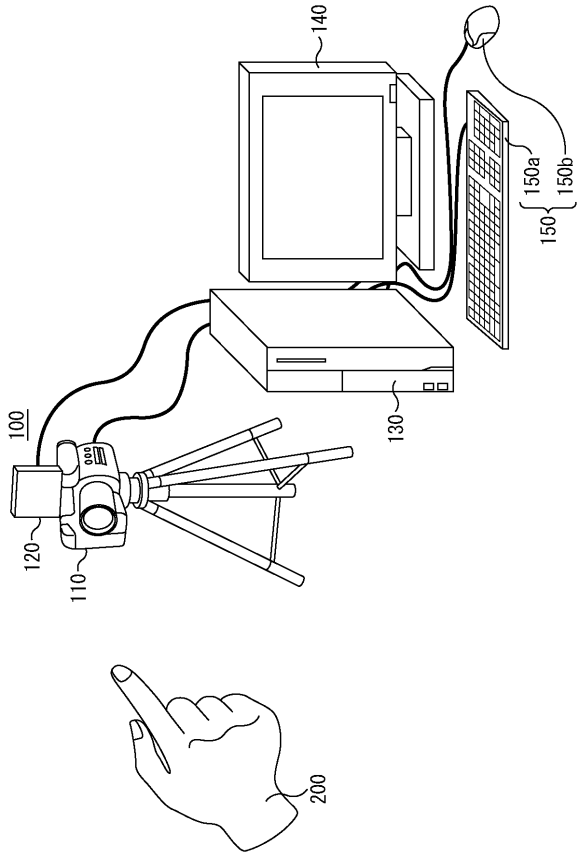
【図６】本発明の実施形態に係る個人認証システムにおける個人認証方法の処理手順の一例を示すフローチャートである。

【符号の説明】

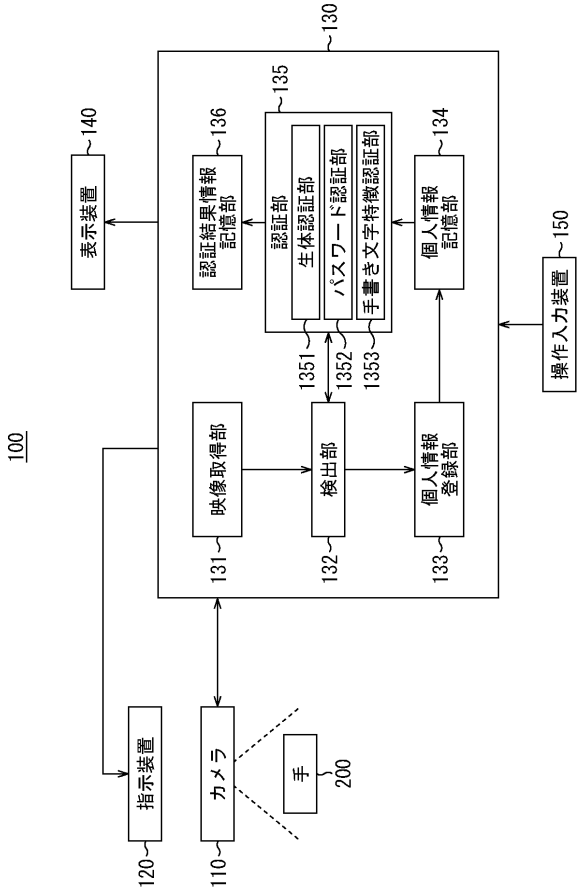
【００６４】

１００　個人認証システム
１１０　カメラ
１２０　指示装置
１３０　情報処理装置
１３１　映像取得部
１３２　検出部
１３３　個人情報登録部
１３４　個人情報記憶部
１３５　認証部
１３５１　生体認証部
１３５２　パスワード認証部
１３５３　手書き文字特徴認証部
１３６　認証結果情報記憶部
１４０　表示装置
１５０　操作入力装置
１５０ａ　キーボード
１５０ｂ　マウス
２００　認証対象者の手

【図１】



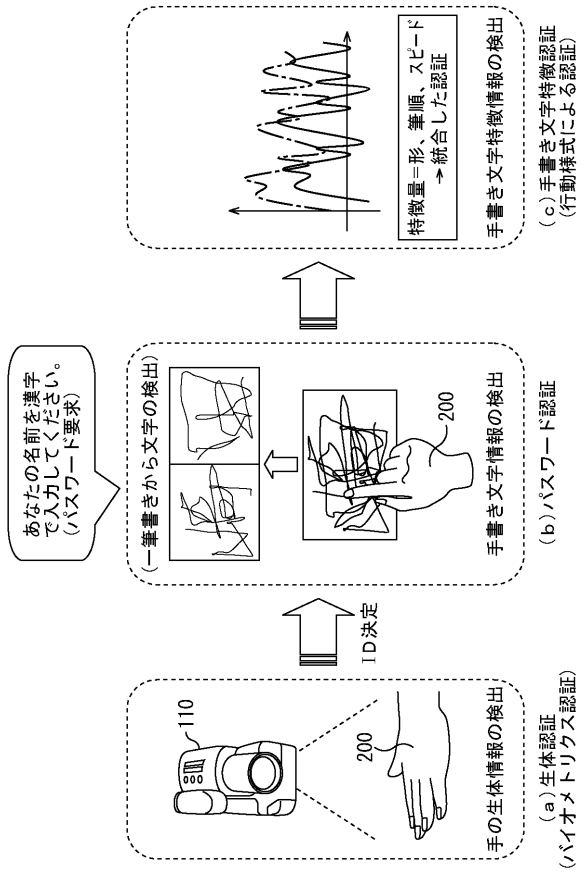
【図２】



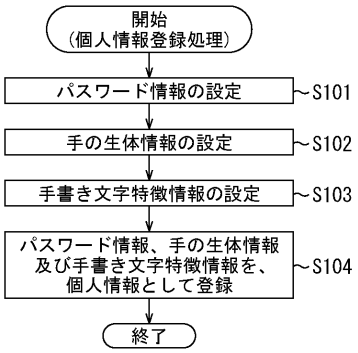
【図３】

個人情報 / ＩＤ番号	手の生体情報	パスワード情報	手書き文字特徴情報
1	(手の形)・・・ (指の形)・・・ ・・・	佐藤	(形)・・・ (筆順)・・・ (スピード)・・・
2	(手の形)・・・ (指の形)・・・ ・・・	鹿嶋	(形)・・・ (筆順)・・・ (スピード)・・・
3	(手の形)・・・ (指の形)・・・ ・・・	崎田	(形)・・・ (筆順)・・・ (スピード)・・・
・・・	・・・	・・・	・・・

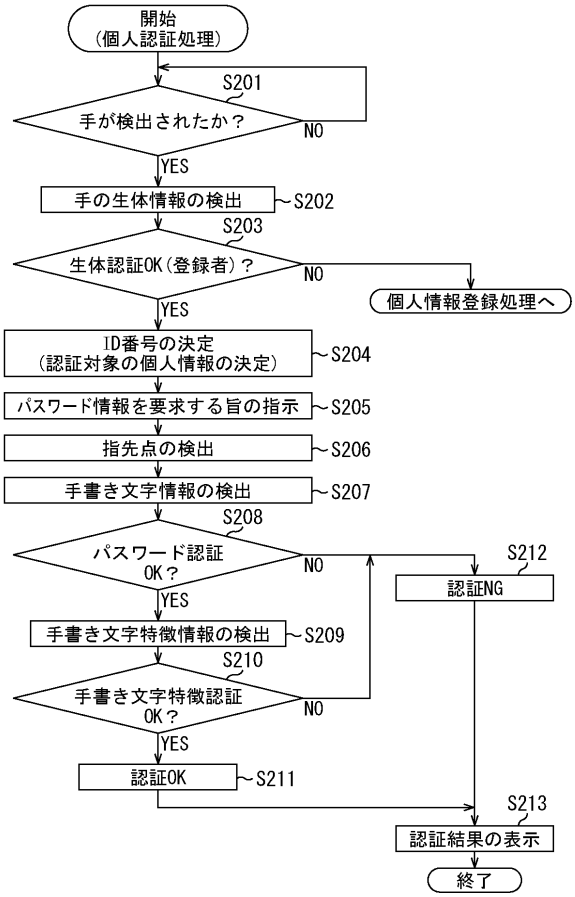
【図４】



【図５】


開始
(個人情報登録処理)
パスワード情報の設定
S101
手の生体情報の設定
S102
手書き文字特徴情報の設定
S103
パスワード情報、手の生体情報
及び手書き文字特徴情報を、
個人情報として登録
S104
終了

【図６】


開始
(個人認証処理)
S201
手が検出されたか？
NO
YES
手の生体情報の検出
S202
S203
生体認証OK(登録者)？
NO
個人情報登録処理へ
YES
ID番号の決定
(認証対象の個人情報の決定)
S204
パスワード情報を要求する旨の指示
S205
指先点の検出
S206
手書き文字情報の検出
S207
S208
パスワード認証
OK？
NO
S212
認証NG
YES
手書き文字特徴情報の検出
S209
S210
手書き文字特徴認証
OK？
NO
YES
認証OK
S211
S213
認証結果の表示
終了

フロントページの続き

Ｆターム(参考) 5B043 AA09 BA03 BA06 DA05 GA02 GA13
5B285 AA01 BA01 CB12 CB24 CB26 CB56 CB63 CB74
5J104 AA07 KA01 KA04 KA16 NA05 NA27 NA38