

(19) 日本国特許庁 (JP)

再公表特許(A1)

(11) 国際公開番号

W02012/144105

発行日 平成26年7月28日 (2014. 7. 28)

(43) 国際公開日 平成24年10月26日 (2012. 10. 26)

(51) Int.Cl.	F I	テーマコード (参考)
G 0 6 F 21/32 (2013.01)	G O 6 F 21/20 1 3 2	5 B O 4 3
G 0 6 T 7/00 (2006.01)	G O 6 T 7/00 5 1 O B	

審査請求 有 予備審査請求 未請求 (全 28 頁)

出願番号	特願2013-510846 (P2013-510846)	(71) 出願人	000005108 株式会社日立製作所 東京都千代田区丸の内一丁目6番6号
(21) 国際出願番号	PCT/JP2011/078025	(74) 代理人	110001689 青稜特許業務法人
(22) 国際出願日	平成23年12月5日 (2011. 12. 5)	(72) 発明者	加賀 陽介 日本国東京都千代田区丸の内一丁目6番6号 株式会社日立製作所内
(31) 優先権主張番号	特願2011-92622 (P2011-92622)	(72) 発明者	高田 治 日本国東京都千代田区丸の内一丁目6番6号 株式会社日立製作所内
(32) 優先日	平成23年4月19日 (2011. 4. 19)	(72) 発明者	磯部 義明 日本国東京都千代田区丸の内一丁目6番6号 株式会社日立製作所内
(33) 優先権主張国	日本国 (JP)		

最終頁に続く

(54) 【発明の名称】 生体認証システム

(57) 【要約】

認証時に利用者から取得した生体情報を登録し、次回以降の認証精度を向上させる。この際、既存の登録生体情報の一部が大きな誤差を含んでいた場合でも、高精度な認証を実現する。過去の認証時に利用者から取得した複数の生体情報と、当該生体情報間の類似度に基づいて評価した各生体情報の信頼度を保持し、利用者の認証時には、利用者の生体情報と複数の登録生体情報間の類似度を算出し、各登録生体情報に対応する類似度と信頼度に基づいて、利用者が本人である確率を示す本人確率を算出し、当該本人確率が所定のしきい値を超えたか否かによって利用者が本人であるか否かを判定することで高精度な認証を実現し、利用者が本人であると判定された際には、利用者から取得した生体情報を登録生体情報として追加登録して次回以降の認証で用いる。

図7

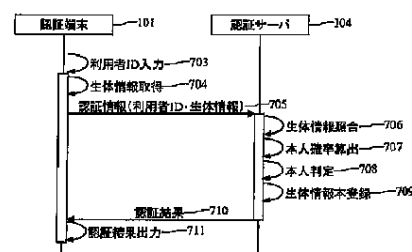


FIG. 7:

101 Authentication terminal
104 Authentication server
703 User ID input
704 Biometric information acquisition
705 Authentication information (user ID, biometric information)
706 Biometric information comparison
707 Identity likelihood computation
708 Identity assessment
709 Actual biometric information registration
710 Authentication result
711 Authentication result output

【特許請求の範囲】**【請求項 1】**

利用者の生体情報を取得する入力装置と、当該入力装置に接続されたプロセッサと、記憶装置と、を備える生体認証システムであって、

前記記憶装置には、

過去に前記利用者を認証した際の前記利用者の生体情報である複数の登録生体情報と、前記複数の登録生体情報の間の誤差を示す信頼度とが格納され、

前記プロセッサは、前記利用者の認証時に、

前記入力装置から入力された前記利用者の生体情報である入力生体情報を受け取り、

前記入力生体情報と前記複数の登録生体情報の各々との間の第 1 の類似度を算出し、

前記第 1 の類似度と前記信頼度に基づいて、前記利用者が本人である確率を示す本人確率を算出し、

前記本人確率が所定の認証しきい値を超えた場合には、前記利用者が本人であると認証し、

前記利用者が本人であると判定された場合は、前記入力生体情報を前記登録生体情報に追加して前記記憶装置に登録する

ことを特徴とする生体認証システム。

【請求項 2】

請求項 1 に記載した生体認証システムであって、

前記プロセッサは、

前記登録生体情報の信頼度を算出する際に、

前記登録生体情報の各々の間の第 2 の類似度を算出し、

当該類似度に基づき前記登録生体情報に含まれる誤差を見積もる

ことを特徴とする生体認証システム。

【請求項 3】

請求項 2 に記載した生体認証システムであって、

前記プロセッサは、前記利用者の登録生体情報の各々について前記第 2 の類似度の平均値を前記誤差として求めることを特徴とする生体認証システム。

【請求項 4】

請求項 1 に記載した生体認証システムであって、

前記記憶装置はさらに、他の利用者の登録生体情報を記憶し、

前記プロセッサは、

前記利用者の登録生体情報の信頼度および類似度に関する第 1 の尤度比と、

前記他の利用者の登録生体情報の信頼度および類似度に関する第 2 の尤度比と

を推定して前記記憶装置に格納し、

前記第 1 の尤度比と前記第 2 の尤度比を用いて前記本人確率を算出する

ことを特徴とする生体認証システム。

【請求項 5】

請求項 1 に記載した生体認証システムであって、

認証端末をさらに備え、

前記プロセッサは、

前記利用者の認証結果を前記認証端末に出力し、

前記認証結果を受け入れることを示す第 1 の情報、または、生体情報以外の身分事項に基づく審査結果を示す第 2 の情報を前記認証端末から受け取り、

前記第 1 の情報を受け取った場合には前記認証結果を、前記第 2 の情報を受け取った場合には前記審査結果を、最終的な認証結果とし、

前記最終的な認証結果により、認証が成功した場合には、前記入力生体情報を前記複数の登録生体情報に追加して登録する

ことを特徴とする生体認証システム。

【請求項 6】

請求項 5 に記載した生体認証システムであって、

前記記憶装置はさらにブラックリストを格納し、前記ブラックリストには利用者の生体情報が格納され、

前記プロセッサは、

前記利用者から、前記利用者の第 1 の生体情報と前記第 1 の生体情報とは異なる前記利用者の第 2 の生体情報を受け取り、

前記第 1 の生体情報に基づいて本人であることを認証し、

前記第 2 の生体情報と前記ブラックリスト内に格納されている生体情報とに基づいて前記利用者が前記ブラックリストに含まれる利用者であることを認証し、

前記利用者が前記ブラックリストに登録された要注意人物ではないと判明した場合は、

前記第 1 の生体情報を

前記複数の登録生体情報に追加して登録することを特徴とする生体認証システム。

【請求項 7】

請求項 1 に記載した生体認証システムであって、

生体情報の登録数に上限を設け、

閾値を超える生体情報が登録された際には、各登録生体情報の登録日時、登録情報間の類似度、各登録生体情報の品質を示す値、等に基づき保持する生体情報を選択し、

それ以外の生体情報を削除することを特徴とする生体認証システム。

【請求項 8】

請求項 1 に記載した生体認証システムであって、

利用者の認証に成功した際に、利用者から取得した生体情報を一旦仮登録し、

その後バッチ処理にて各仮登録生体情報に対する信頼度を算出し、

仮登録生体情報とその信頼度を本登録することを特徴とする生体認証システム。

【発明の詳細な説明】

【技術分野】

【0001】

本発明は、生体認証技術に関し、特に複数の登録生体情報に基づき生体認証を行う技術に関する。

【背景技術】

【0002】

生体認証システムは、指紋、静脈、虹彩、顔、音声、筆跡等の生体情報に基づき個人認証を行う。一般に、生体認証システムでは、まず利用者の生体情報を取得して予め登録しておき、認証時に取得した利用者の生体情報（以降、「認証生体情報」という）と予め登録しておいた生体情報（以降、「登録生体情報」という）との類似度が一定のしきい値を超えるか否かで本人認証を実現する。ここで、当該生体認証システムにおいて、登録生体情報と本人から取得した認証生体情報との類似度が、しきい値より低い値となった場合、本人が認証されない事象（以降、「本人拒否」という）が発生し、システムの利便性低下に繋がる。この本人拒否が発生する確率（以降、「本人拒否率」という）は、利用者の生体情報に経年変化が起きた場合や、生体情報を取得する際の周辺環境（気温、湿度、照明環境等）が変化して生体情報に誤差が生じた場合等に高くなる。

【0003】

この問題を解決するためには、経年変化後の生体情報や、様々な周辺環境において取得した生体情報を複数登録しておき、その生体情報を認証に用いる方式が考えられる。

【0004】

特許文献 1 では、認証時に利用者から取得した生体情報を登録し、次回以降の認証に用いる生体認証システムが開示されている。当該生体認証システムは、認証生体情報と登録生体情報の類似度に一定の範囲を設定し、その範囲に含まれる認証生体情報を追加登録する。次回以降の認証では、追加登録された生体情報を含む複数の登録生体情報に基づき、認証を行う。

10

20

30

40

50

【0005】

非特許文献1では、複数種類の生体情報（例えば、指紋と顔等）を取得してそれらを事前に取得した生体情報と照合し、得られた類似度の融合判定を行うことで本人確認を行う生体認証方式が開示されている。当該生体認証方式は、各類似度から尤度比を算出し、得られた尤度比に対する検定を行うことで本人であるか否かを判定する。

【0006】

特許文献1では、認証生体情報と複数の登録生体情報の類似度に基づき、認証対象者が事前登録した人物と同一か否かを判定する。当該判定方式には、全ての類似度の平均値から判定する方式、最も大きい（あるいは、小さい）数値の類似度から判定する方式、数値の大きい上位いくつかの類似度から判定する方式等を適用することができる。

10

【先行技術文献】

【特許文献】

【0007】

【特許文献1】特開2006-127236号公報

【非特許文献1】K. Nandakumar, S. C. Dass, A. K. Jain, 「Likelihood Ratio Based Biometric Score Fusion」、Pattern Analysis and Machine Intelligence、IEEE、vol30、pp342-347、2008

【発明の概要】

【発明が解決しようとする課題】

20

【0008】

しかしながら、これらの判定方式は、登録生体情報の一つ（あるいは、複数）に大きな誤差が含まれている場合は、十分な認証精度を達成できない可能性がある。

【0009】

そこで、本発明は、登録生体情報の一部に、生体情報の経年変化、周辺環境の変化、生体情報取得時のノイズ等に起因する誤差を含むものがある場合でも、高精度な認証を行うことを目的とする。

【課題を解決するための手段】

【0010】

代表的な一例は、利用者の生体情報を取得する入力装置と、当該入力装置に接続されたプロセッサと、記憶装置と、を備える生体認証システムであって、前記記憶装置には、過去に前記利用者を認証した際の前記利用者の生体情報である複数の登録生体情報と、前記複数の登録生体情報の間の誤差を示す信頼度とが格納され、前記プロセッサは、前記利用者の認証時に、前記入力装置から入力された前記利用者の生体情報である入力生体情報を受け取り、前記入力生体情報と前記複数の登録生体情報の各々との間の第1の類似度を算出し、前記第1の類似度と前記信頼度に基づいて、前記利用者が本人である確率を示す本人確率を算出し、前記本人確率が所定の認証しきい値を超えた場合には、前記利用者が本人であると認証し、前記利用者が本人であると判定された場合は、前記入力生体情報を前記登録生体情報に追加して前記記憶装置に登録することを特徴とする生体認証システムを提供する。

30

40

【発明の効果】

【0011】

本発明の一実施形態によれば、認証用に取得した生体情報を複数登録しその生体情報を次回以降の認証に用いる際に、登録生体情報の一部に大きな誤差を含むものが存在している場合でも、認証精度を落とすことなく高精度な認証を実現することができる。

【図面の簡単な説明】

【0012】

【図1】本発明の第一の実施形態の、認証端末、認証サーバのシステム構成を示す図である。

【図2】本発明の第一の実施形態の、登録生体情報格納部の中に蓄積される情報を示した

50

図である。

【図 3】本発明の第一の実施形態の、仮登録生体情報格納部の中に蓄積される情報を示した図である。

【図 4】本発明の第一の実施形態の、尤度比配列格納部の中に保存する情報を示した図である。

【図 5】本発明の第一の実施形態の、認証しきい値格納部の中に保存する情報を示した図である。

【図 6】本発明の第一の実施形態において、認証端末を利用者が操作し、生体情報の登録をバッチ処理にて行う場合の手順を示す図である。

【図 7】本発明の第一の実施形態において、認証端末を利用者が操作し、生体情報の登録をリアルタイム処理にて行う場合の手順を示す図である。

【図 8】本発明の第二の実施形態において、認証端末をオペレータが操作し、生体情報の登録をバッチ処理にて行う場合の手順を示す図である。

【図 9】本発明の第二の実施形態において、認証端末をオペレータが操作し、生体情報の登録をリアルタイム処理にて行う場合の手順を示す図である。

【図 10】本発明の第三の実施形態において、認証端末をオペレータが操作し、生体情報の登録をバッチ処理にて行う場合の手順を示す図である。

【図 11】本発明の第三の実施形態において、認証端末をオペレータが操作し、生体情報の登録をリアルタイム処理にて行う場合の手順を示す図である。

【図 12】本発明の第一の実施形態において、生体情報照合の手順を示す図である。

【図 13】本発明の第一の実施形態において、本人確率算出の手順を示す図である。

【図 14】本発明の第一の実施形態において、本人判定の手順を示す図である。

【図 15】本発明の第一の実施形態において、生体情報仮登録の手順を示す図である。

【図 16】本発明の第一の実施形態において、生体情報本登録の手順を示す図である。

【図 17】本発明の第一の実施形態の生体認証システムにおける認証端末、認証サーバのハードウェア構成を示すブロック図である。

【図 18】本発明の第三の実施形態の、ブラックリストの中に蓄積される情報を示した図である。

【発明を実施するための形態】

【0013】

特許文献 1、非特許文献 2 の判定方式は、登録生体情報の一つ（あるいは、複数）に大きな誤差が含まれている場合は、十分な認証精度を達成できない可能性がある。例えば、全ての類似度の平均値から判定する方式、または最も小さな数値の類似度から判定する方式では、登録生体情報の一つ（あるいは、複数）に大きな誤差が含まれていた場合は、本人拒否率が高くなる。また、最も大きい数値の類似度から判定する方式は、大きな誤差が含まれた登録生体情報と、他人の生体情報が類似していた際に、他人を本人と誤って判定してしまう確率（以降、「他人受入率」という）が高くなる。数値の大きい上位いくつかの類似度から判定する方式では、用いる類似度の個数というパラメータによって認証精度が変化するが、当該パラメータとして適切な値は生体認証システムの運用環境（利用者の慣れ、認証毎の周辺環境変化等）によって異なるので、常に高い認証精度で運用することは困難であると考えられる。

【0014】

また、非特許文献 1 では、各類似度に対する尤度比を算出して、得られた尤度比を用いて融合判定を行うことで、認証対象者が事前登録した人物と同一か否かを判定する（以降、「尤度比検定方式」という）。尤度比検定方式を用いることで、本人の生体情報同士を照合した際の類似度が従う分布（以降、「本人分布」という）と他人の生体情報同士を照合した際の類似度が従う分布（以降、「他人分布」という）が既知である場合に、一定の他人受入率の制約の下で本人拒否率を最小化することが可能となる。

【0015】

しかしながら、登録生体情報の一つ（あるいは、複数）に大きな誤差が含まれていた場

10

20

30

40

50

合には、誤差を含む登録生体情報と本人の生体情報との類似度分布が、予め学習により求めた本人分布と異なり、認証精度が低下する問題が発生する。

【0016】

＜第一の実施形態＞

第一の実施形態は、利用者自身が操作する認証端末と認証サーバを用いて、予め登録された複数の生体情報（以降、「登録生体情報」という）に対して、生体情報に含まれる誤差を示す信頼度を付与しておき、利用者の認証を行う際には、利用者から取得した生体情報（以降、「認証生体情報」という）と複数の登録生体情報との類似度、および各登録生体情報に対する信頼度に基づき、利用者が事前に登録した人物と同一人物である確率（以降、「本人確率」という）を算出することで本人か否かの判定を行い、認証が成功した際には認証生体情報を認証サーバへ自動で登録するシステムである。

10

【0017】

以下、図面を参照して、詳細に説明する。

【0018】

図1は、本発明の第一の実施形態の、認証端末、および認証サーバのシステム構成を示す図である。

【0019】

この図において、符号101は認証端末、符号102は認証情報取得部、符号103は認証結果表示部、符号104は認証サーバ、符号105は生体情報照合部、符号106は生体情報選択部、符号107は生体情報登録部、符号108は信頼度算出部、符号109は信頼度登録部、符号110は本人確率算出部、符号111は登録生体情報格納部、符号112は仮登録生体情報格納部、符号113は尤度比配列格納部、符号114は認証しきい値格納部である。

20

【0020】

認証端末101は例えば入退室管理システムにおける端末、PCログインシステムにおけるPC、出入国管理システムにおける審査端末や自動化ゲート等に相当し、認証対象である利用者自身、または端末を担当しているオペレータが操作する端末である。認証端末101は、認証情報取得部102、認証結果表示部103を含んで構成されており、認証サーバ104と接続されている。

【0021】

認証情報取得部102は、利用者から利用者IDと生体情報を取得する。生体情報は、指紋、静脈、虹彩、顔、音声、筆跡等、個人を特定することが可能な行動的あるいは身体的特徴である。

30

【0022】

認証結果表示部103は認証結果を、認証端末101を操作している利用者、またはオペレータに対して表示する。

【0023】

認証サーバ104は、例えば入退室管理システムやPCログインシステム、出入国管理システムにおいて、生体情報の管理・照合を行うサーバである。認証サーバ104は、生体情報照合部105、生体情報選択部106、生体情報登録部107、信頼度算出部108、信頼度登録部109、本人確率算出部110、登録生体情報格納部111、仮登録生体情報格納部112、尤度比配列格納部113、認証しきい値格納部114を含んで構成されており、認証端末101と接続されている。

40

【0024】

生体情報照合部105は、二つの生体情報を照合し、生体情報間の類似度、または非類似度を算出する。当該類似度、または非類似度は、例えば0～100のように一定の範囲を持つ数値で表される、生体情報がどの程度類似しているかを表す指標である。当該類似度、または非類似度は、例えば指紋認証の場合、二つの指紋画像における特徴点の位置・方向に基づいて画像間の類似性を評価することで求められる。また、画像マッチングに基づく指静脈認証では、例えば二つの指静脈パターンを重ね合わせ、一致する画素の数に基

50

づいてパターン間の類似性を評価することで求められる。

【0025】

生体情報選択部106は、複数の生体情報から登録する生体情報を選択する。生体情報の選択に用いる基準としては、生体情報間の類似度、生体情報の登録日時、生体情報の品質等を適用することが可能である。

【0026】

生体情報登録部107は、生体情報を利用者IDと紐付けて登録生体情報格納部111に登録する。

【0027】

信頼度算出部108は、登録生体情報に対する信頼度を算出する。信頼度は、各登録生体情報が、どの程度誤差を含んでいるかを示す値であり、当該信頼度を考慮して本人判定を行うことで、登録生体情報に誤差が含まれていた場合でも高精度な判定が可能となる。当該信頼度算出には、生体情報間の類似度、生体情報の登録日時、生体情報の品質等を用いることが可能である。例えば、信頼度算出の対象とする登録生体情報と、同一の生体から取得されたその他の登録生体情報との類似度(M-1個)の平均値は、対象とする登録生体情報に含まれる誤差に依存するため、対象とする登録生体情報の信頼度として用いることができる。なお、平均値に代わり、対象とする登録生体情報と、同一の生体情報から取得されたその他の登録生体情報との類似度から、統計的手法を用いて登録生体情報に含まれる誤差を推定し、それを信頼度としても良い。

【0028】

信頼度登録部109は、信頼度算出部108で算出した信頼度を登録生体情報格納部111へ登録する。

【0029】

本人確率算出部110は、生体情報間の類似度と各生体情報に対する信頼度に基づき、利用者に対する本人確率を算出する。

【0030】

登録生体情報格納部111は、利用者ID、生体情報、信頼度を格納する。

【0031】

仮登録生体情報格納部112は、登録生体情報格納部111に格納される前の利用者IDと生体情報を格納する。仮登録生体情報格納部112に格納された情報は、その後バッチ処理にて登録生体情報格納部111へ登録される。

【0032】

尤度比配列格納部113は、生体情報の信頼度および生体情報間の類似度に対応する尤度比を格納する。信頼度 r 、類似度 s に対応する尤度比 $L(r, s)$ は、 $L(r, s) = G(r, s) / I(r, s)$ と表される。ここで、 $G(r, s)$ は信頼度 r 、類似度 s のときの本人分布の値、 $I(r, s)$ は信頼度 r 、類似度 s のときの他人分布の値を示す。本人分布 $G(r, s)$ 、他人分布 $I(r, s)$ は、事前に生体情報を収集し、当該生体情報が従う分布を学習することで得られる。この学習は、具体的には、本人同士および他人同士の生体情報の組に対して信頼度 r 、類似度 s を算出し、2次元の頻度分布を取得する。この頻度分布に対して、正規分布に代表される分布関数を用いたパラメトリック推定や、カーネル密度推定に代表されるノンパラメトリック推定等による分布推定を行うことで、本人分布 $G(r, s)$ および他人分布 $I(r, s)$ を求める。

【0033】

認証しきい値格納部114は、本人確率に対する認証しきい値を格納する。認証しきい値は、本人確率に基づき認証対象者が本人であるか否かを判定する時に用いられ、本人確率が認証しきい値以上である時は本人であると判定し、本人確率が認証しきい値未満である時は他人であると判定する。認証しきい値は、事前に生体情報を収集し、精度要件を満たす認証しきい値を算出することで決定される。また、認証しきい値は、要求される精度要件によって適切な値が変わるため、精度要件とそれに対応する認証しきい値を予め決定して保持しておく。ここでは、精度要件として、他人を誤って本人と判定してしまう確率

10

20

30

40

50

(以降、「他人受入率」という)を用いる。

【0034】

図1の各部の詳細については、図2～図5の図面を参照して説明する。

【0035】

図2は、本発明の第一の実施形態の、登録生体情報格納部111の中に蓄積される情報を示した図である。

【0036】

「利用者ID」201は各利用者に割り当てられた固有のIDであり、例えば英数字により構成される。行204は「利用者ID」が「0001」であるものに関する記述であり、行205は「利用者ID」が「0001」であるものに関する記述であり、行206は「利用者ID」が「0002」であるものに関する記述である。

10

【0037】

「登録生体情報」202には、利用者から取得した登録生体情報が記載される。例えば行204の「登録生体情報」202には、「利用者ID」が「0001」である利用者が1回目に利用した際に取得した生体情報が格納されている。

【0038】

「信頼度」203には、利用者IDがiの利用者が、j回目の利用時に取得した生体情報に対する信頼度 $R(i, j)$ が記載される。信頼度は、ある一定の範囲の数値で表され、対応する登録生体情報がどの程度の誤差を含んでいるかを示す値であり、前記信頼度算出部108にて算出が行われる。

20

【0039】

図3は、本発明の第一の実施形態の、仮登録生体情報格納部112の中に蓄積される情報を示した図である。本実施形態では、生体情報を登録する方法にはバッチ処理とリアルタイム処理の二つがあり、仮登録生体情報格納部112は、バッチ処理で登録を行う際にバッチ適用前の情報を格納するために用いられる。

【0040】

「利用者ID」301は各利用者に割り当てられた固有のIDであり、例えば英数字により構成される。行303は「利用者ID」が「0001」であるものに関する記述であり、行304は「利用者ID」が「0001」であるものに関する記述であり、行305は「利用者ID」が「0002」であるものに関する記述である。

30

【0041】

「仮登録生体情報」302には、利用者から取得した仮登録生体情報が記載される。例えば、行303の「仮登録生体情報」302は、利用者IDが「0001」である利用者が3回目に利用した際に取得した生体情報を格納している。

【0042】

図4は、本発明の第一の実施形態の、尤度比配列格納部113の中に保存する情報を示した図である。本実施形態では、事前に学習した本人分布 $G(r, s)$ 、他人分布 $I(r, s)$ に基づき、信頼度 r 、類似度 s のときの尤度比 $L(r, s)$ を算出し、得られた尤度比を尤度比配列格納部113に格納する。この尤度比に基づき本人確率を算出し、認証対象者が本人であるか否かを判定することで、個人認証が実現する。

40

【0043】

「信頼度」401には、登録生体情報の信頼度 r (例えば、10、20、...)が記載される。

【0044】

「類似度」402には、生体情報間の類似度 s が取りうる値(例えば、0～100)が記載される。

【0045】

「尤度比」403には、信頼度 r 、類似度 s のときの尤度比 $L(r, s)$ が格納される。当該尤度比 $L(r, s)$ は、予め学習用に収集した生体情報に基づき算出し、システムの運用開始前に「尤度比」403に書き込んでおく。

50

【0046】

図5は、本発明の第一の実施形態の、認証しきい値格納部114の中に保存する情報を示した図である。

【0047】

「精度要件(FAR)」501は認証の精度に対する要件であり、行503は「精度要件(FAR)」が「0.001」であるものに関する記述であり、行504は「精度要件(FAR)」が「0.0001」であるものに関する記述であり、行505は「精度要件(FAR)」が「0.00001」であるものに関する記述である。

「認証しきい値」502には、本人確率に対して適用する認証しきい値が記載される。

【0048】

「精度要件(FAR)」501は認証の精度に対するセキュリティ要件である。例えば、誤って他人を受け入れる確率を1000回に1回程度(すなわち、 $FAR = 0.001$)に抑えたい場合は、行503に従って認証しきい値を「 $T(0.001)$ 」に設定する。この場合、本人確率が「 $T(0.001)$ 」を上回った時に認証成功となり、下回った場合に認証失敗となる。

【0049】

図6、図7は、本発明の第一の実施形態において、利用者の認証、および生体情報の登録を行う手順を示す図である。本発明における第一の実施形態では、認証対象者である利用者自身が認証端末101を操作する。また、生体情報の登録を行う方法には、バッチ処理とリアルタイム処理の二つがあり、図6ではバッチ処理により生体情報を登録する場合の手順、図7ではリアルタイム処理により生体情報を登録する場合の手順を示す。さらに、図6、図7の処理の詳細な手順は、図12～図16に示されている。

【0050】

図6は、本発明の第一の実施形態において、認証端末を利用者が操作し、生体情報の登録をバッチ処理にて行う場合の手順を示す図である。

【0051】

最初に、認証端末101は利用者IDを取得する処理603を行う。利用者IDを取得する方法には、数字キーにより手入力を行う方法、磁気カードやICカードからIDを取得する方法、紙に印字された文字列をスキャナで読み取る方法、等が適用可能である。

【0052】

次に、認証端末101は生体情報を取得する処理604を行う。生体情報の取得では、認証情報取得部102に含まれる、指紋や静脈、虹彩、筆跡等を読み取る専用装置、顔を撮影するカメラ、音声を取得するマイク等を用いる。次に、認証端末101は、認証情報(利用者ID・生体情報)605を認証サーバ104へ送信する。次に、認証サーバ104は生体情報を照合する処理606を行う。処理606では、利用者の生体情報(1件)と複数の登録生体情報(N件)との照合を行い、N個の類似度(または、非類似度)を算出する。処理606の具体的な処理手順を図12に示す。次に、認証サーバ104は本人確率を算出する処理607を行う。処理607の中で、認証サーバ104は利用者から取得した生体情報と登録生体情報との類似度、および登録生体情報の信頼度に基づき、本人確率算出を行う。生体情報間の類似度は、処理606にて算出された、生体情報がどの程度類似しているかを示す指標であり、類似度が大きい場合、二つの生体情報は同一人物から取得されたものであると判断できる。登録生体情報の信頼度は、以前に利用者が認証を行った際に、生体情報本登録612にて事前に算出されており、登録生体情報がどの程度誤差を含んでいるかを示している。処理607の具体的な処理手順を図13に示す。次に、認証サーバ104は本人であるか否かを判定する処理608を行う。処理608では、生体情報間の類似度と各登録生体情報の信頼度から尤度比を算出し、その尤度比を統合することで本人確率算出を行い、得られた本人確率に対して認証しきい値を適用することで利用者が本人であるか否かの判定を行う。この際、本実施形態では、登録生体情報の信頼度を尤度比算出に含め、登録生体情報に含まれる誤差を考慮した本人確率算出を行う。これにより、生体情報間の類似度のみから本人判定を行う方式に比べ、登録生体情報の一部

10

20

30

40

50

が大きな誤差を含んでいた場合でも、高精度な認証が可能となる。処理 608 の具体的な処理手順を図 14 に示す。次に、認証サーバ 104 は生体情報を仮登録する処理 609 を行う。処理 609 の具体的な処理手順を図 15 に示す。次に、認証サーバ 104 は、認証結果 610 を認証端末 101 へ送信する。認証結果 610 には、利用者の認証が成功したか否かを示す情報が含まれている。次に、認証端末 101 は認証結果を出力する処理 611 を行う。処理 611 では、認証結果表示部 105 を用いて利用者へ認証結果を伝える。

【0053】

利用者 ID 取得処理 603 から認証結果出力処理 611 までの認証処理を繰り返すことで、生体情報仮登録 609 が複数回実行され、複数の生体情報が仮登録生体情報格納部 112 へ蓄積される。その後、本実施形態では、バッチ処理として生体情報本登録 612 を行う。処理 612 の具体的な手順を図 16 に示す。これにより、複数の生体情報が登録され、次回以降の認証で活用される。

【0054】

このように生体情報仮登録 609 を複数回実行し、その後生体情報本登録 612 を行う方式（以降、「生体情報一括登録方式」という）では、利用者の認証時に、認証に必要な処理（処理 606～処理 608）と生体情報仮登録 609 を行う。生体情報仮登録 609 は、比較的計算機負荷が低いため、生体情報一括登録方式採用によりパフォーマンスを落とすことなく、迅速な認証処理を行うことが可能である。従って、単位時間当たりの認証回数が多い大規模生体認証システムでは生体情報一括登録方式を採用することが望ましい。生体情報一括登録方式では、認証時に各登録生体情報間の類似度算出、および信頼度算出を行わず、生体情報本登録 612 にてバッチ処理として行う。

【0055】

第一の実施形態における処理の詳細な手順を図 12～図 16 に示す。以下、図面を参照して、詳細に説明する。

【0056】

図 12 は、本発明の第一の実施形態において、生体情報照合の手順を示す図である。

【0057】

ステップ 1201 は、利用者 ID に基づき、登録生体情報格納部 114 に格納されている登録生体情報 202 を読み出す処理である。登録生体情報格納部 114 には複数の登録生体情報を格納することが可能であるため、ここで読み出す登録生体情報は、一つ、または複数である。

【0058】

ステップ 1202 は認証端末 101 から受信した生体情報と、ステップ 1201 にて読み出した N 件の登録生体情報をそれぞれ照合する処理である。この処理により、N 件の登録生体情報に対して、N 件の類似度が算出される。

【0059】

図 13 は、本発明の第一の実施形態において、本人確率算出の手順を示す図である。

【0060】

ステップ 1301 は利用者 ID に基づき、登録生体情報格納部 114 に格納されている各登録生体情報に対する信頼度 203 を読み出す処理である。登録生体情報格納部 114 には複数の登録生体情報を格納することが可能であるため、ここで読み出す信頼度 203 は、一つ、または複数である。

【0061】

ステップ 1302 はステップ 1301 で読み出した各登録生体情報の信頼度 r と、ステップ 1202 で算出した類似度 s に基づき、尤度比配列格納部 113 から尤度比 $L(r, s)$ を読み出す処理である。

【0062】

ステップ 1303 は、ステップ 1302 で求めた尤度比を統合して、本人確率を算出する処理である。具体的には、各登録生体情報に対する尤度比同士を掛け合わせて登録生体情報全体に対する尤度比 L' を求め、ベイズの定理に基づき事後確率 $P' = (L' \times P)$

／ $(L' \times P + 1 - P)$ を算出する。ただし、 P は本人に対する事前確率であり、利用者本人が認証を試みる確率を予め代入しておく。当該事前確率は、予め全ての利用者と同じ値（例えば0.5）を付与しておいても良い。なお、利用者が認証を行う確率に差がある場合には、その確率に応じて利用者毎に異なる事前確率を割り当てても良い。ステップ1303は、得られた事後確率 P' を本人確率として出力する。

【0063】

ここで、各尤度比 L は各登録生体情報に対応する信頼度と類似度に基づき算出される。各尤度比 L は、信頼度が高い（つまり、登録生体情報に含まれる誤差が小さい）ときに大きな値をとり、信頼度が低い（つまり、登録生体情報に含まれる誤差が大きい）ときに小さな値をとる。これにより、誤差が小さいと判定された登録生体情報を重視した判定が行われ、登録生体情報の一部が大きな誤差を含む場合でも、その影響は小さくなり、高精度な認証が可能となる。

10

【0064】

なお、本人判定を行う方式には、上記尤度比を用いた方式に限らず、様々な方式を採用することができる。例えば、SVM、Boostingに代表される機械学習手法において、各登録生体情報の信頼度を考慮して最終的な出力値を得ることで、同様の効果を得ることが可能となる。

【0065】

図14は、本発明の第一の実施形態において、本人判定の手順を示す図である。ステップ1401は、ステップ1304にて算出した本人確率に対して、認証しきい値502を適用する処理である。

20

【0066】

ステップ1402は、本人確率が認証しきい値502より大きいかな否かを判定する処理である。もし本人確率が認証しきい値502より大きければ、ステップ1403へ進む。もし本人確率が認証しきい値502より小さければ、ステップ1404へ進む。

【0067】

ステップ1403は認証結果に認証成功を示す情報を代入する処理である。

【0068】

ステップ1404は認証結果に認証失敗を示す情報を代入する処理である。

【0069】

30

図15は、本発明の第一の実施形態において、生体情報仮登録の手順を示す図である。

【0070】

ステップ1501は利用者ID取得処理603で取得した利用者IDと生体情報取得処理604で取得した生体情報を、仮登録生体情報格納部112へ登録する処理である。登録された生体情報は、次回以降の認証にはまだ用いられず、図16に示す生体情報本登録が行われた際に、登録生体情報格納部111へ登録される。

【0071】

図16は、本発明の第一の実施形態において、生体情報本登録の手順を示す図である。

【0072】

ステップ1601は認証端末101から受信した利用者ID・生体情報、および仮登録生体情報格納部112に記録された利用者ID・生体情報を、登録生体情報格納部111に登録する処理である。この際、既に利用者IDに紐付いた生体情報が登録生体情報格納部111に存在する場合は、既存の生体情報は残したまま生体情報を追加登録する。なお、追加登録を繰り返して登録生体情報を増加させて行くと、必要な記憶容量や生体情報の照合に要する時間が比例して増加していくため、生体情報の登録数には上限を設けることもできる。生体情報の登録数を上限以下に保つためには、登録数が上限を超えた際に生体情報を選択・削除する必要がある。この削除する生体情報の選択は、生体情報選択部106において、生体情報登録日時、生体情報間の類似度、生体情報の品質を示す値、等に基づいて行われる。例えば、最も登録日時の古い生体情報、他の生体情報との類似度の最大値（または最小値）・平均値・中央値・上位（または下位）数件の平均値等が最大（また

40

50

は最小)となる生体情報、品質を示す値が最も低い生体情報、等を選択し、削除することで、生体情報の登録数を上限以下に保つことが可能となる。

【0073】

なお、生体情報を削除した場合、認証に用いる情報が少なくなり、次回以降の認証精度が低下する恐れがある。この精度低下を防ぐためには、例えば各登録生体情報に対する重みを設けて、生体情報の削除時に当該生体情報に類似する生体情報に対する重みを増加させる方法が考えられる。認証時には、この重みを考慮して本人確率を求めることで、生体情報削除による認証精度低下を抑えることが可能となる。

【0074】

ステップ1602は、利用者IDが等しい登録生体情報について、全ての組み合わせを照合し、類似度を取得する処理である。例えば、ある利用者IDに対応する登録生体情報がN件登録されている場合は、登録生体情報同士の照合は $(N-1) \times N$ 回行われ、 $(N-1) \times N$ 個の類似度が得られる。

【0075】

ステップ1603は登録生体情報間の類似度に基づき、各登録生体情報の信頼度を算出する処理である。信頼度は、各登録生体情報が、どの程度誤差を含んでいるかを示す値であり、当該信頼度を考慮して本人判定を行うことで、登録生体情報に誤差が含まれていた場合でも高精度な判定が可能となる。当該信頼度としては、例えば対象とする登録生体情報とその他の登録生体情報との類似度 $(N-1)$ 個の平均値を採用することができる。なお、当該信頼度は、対象とする登録生体情報とその他の登録生体情報との類似度 $(M-1)$ 個の最小値、平均値、中央値、最大値、上位(または下位)数件の平均値等、および、生体情報を登録してからの経過時間、生体情報の品質を示す値、のうち、1つまたは複数を用いて算出することもできる。

【0076】

ステップ1604はステップ1603で算出した信頼度を登録生体情報格納部111の信頼度203へ登録する処理である。

【0077】

図17は、第一の実施形態の生体認証システムにおける認証端末、認証サーバのハードウェア構成を示すブロック図である。

【0078】

この図において、符号1701はCPU(Central Processing Unit)、符号1702はメモリ、符号1703はHDD(Hard Disk Drive)、符号1704は入力装置、符号1705は出力装置、符号1706は通信装置である。

【0079】

CPU1701は認証サーバ104の生体情報照合部105、生体情報選択部106、生体情報登録部107、信頼度算出部108、信頼度登録部109、本人確率算出部110に対応するプログラムを実行する。メモリ1702は認証サーバ104の生体情報照合部105、生体情報選択部106、生体情報登録部107、信頼度算出部108、信頼度登録部109、本人確率算出部110に対応するプログラムを格納する。これらのプログラムをCPU1701が実行することで、各々の処理が実現する。HDD1703は認証サーバ104における登録生体情報格納部111、仮登録生体情報格納部112、尤度比配列格納部113、認証しきい値格納部114に相当する。各部が格納するデータは、HDD1703上のデータとして蓄積される。入力装置1704は認証端末101における生体情報取得部102に相当する。生体情報取得部102では、利用者から指紋、静脈、虹彩、音声、筆跡等の生体情報を取得する。出力装置1705は認証端末101の認証結果表示部103に相当する。認証結果表示部103では、例えばディスプレイ等を通して認証端末101を操作している利用者、またはオペレータに対して、認証結果を伝える。通信装置1706は認証端末101と認証サーバ104の間で、認証情報や認証結果を送受信する際に用いられる。

10

20

30

40

50

【0080】

図7は、本発明の第一の実施形態において、認証端末を利用者が操作し、生体情報の登録をリアルタイム処理にて行う場合の手順を示す図である。

【0081】

最初に、認証端末101は利用者IDを入力処理703を行う。利用者IDを取得する方法には、数字キーにより手入力を行う方法、磁気カードやICカードからIDを取得する方法、紙に印字された番号をスキャナで読み取る方法、等が適用可能である。次に、認証端末101は生体情報を取得する処理704を行う。生体情報の取得では、認証情報取得部102に含まれる、指紋や静脈、虹彩、筆跡等を読み取る専用装置、顔を撮影するカメラ、音声を取得するマイク等を用いる。次に、認証端末101は、認証情報（利用者ID・生体情報）705を認証サーバ104へ送信する。次に、認証サーバ104は生体情報を照合する処理706を行う。処理706の具体的な処理手順を、図12に示す。次に、認証サーバ104は本人確率を算出する処理707を行う。処理707の具体的な処理手順を、図13に示す。次に、認証サーバ104は本人を判定する処理708を行う。処理708の具体的な処理手順を、図14に示す。次に、認証サーバ104は生体情報本登録する処理709を行う。処理709の具体的な手順は、図16に示す。次に、認証サーバ104は、認証結果710を認証端末101へ送信する。認証結果710には、利用者の認証が成功したか否かを示す情報が含まれている。最後に、認証端末101は認証結果を出力する処理711を行う。処理711では、認証結果表示部103を用いて利用者へ認証結果を伝える。

【0082】

このように認証時に生体情報本登録709を行う方式（以降、「生体情報逐次登録方式」という）では、利用者の認証時に本人判定に必要な処理（処理706～処理708）と生体情報本登録709を行う。生体情報本登録709は、比較的計算機負荷が高いため、生体情報逐次登録方式の大規模生体認証システムへの適用は困難である。しかしながら、生体情報逐次登録方式では認証時に即座に生体情報を本登録するため、バッチ処理を待たずに認証精度の向上を行うことが可能となる。従って、単位時間当たりの認証回数が少なく、同一人物が短時間に何度も認証を行うような生体認証システムでは効果が大きいと考えられる。

【0083】

以上の本発明の第一の実施形態によれば、複数の登録生体情報の一部に大きな誤差が含まれていた場合でも、高精度な本人確認を行うことができる。

【0084】

<第二の実施形態>

第二の実施形態は、オペレータが操作する認証端末と認証サーバを用いて、利用者から取得した生体情報（以降、認証生体情報）を認証サーバへ自動で登録し、登録された複数の生体情報（以降、登録生体情報）に対して、登録生体情報間の類似度に基づく信頼度を付与し、利用者の認証時には認証生体情報と複数の登録生体情報との類似度と各登録生体情報に対する信頼度に基づき本人確率を算出することで本人か否かの判定を行うシステムである。ただし、認証端末は操作するオペレータから利用者の身分事項に関する確認結果を受理することができる。例えば、認証サーバにおける生体情報照合に失敗し、生体情報に基づく本人確認が行えなかった場合は、当該確認結果を受理することで本人確認が完了したとする。

【0085】

以下、図面を参照して、第二の実施形態を詳細に説明する。

【0086】

図8は、本発明の第二の実施形態において、認証端末をオペレータが操作し、生体情報の登録をバッチ処理にて行う場合の手順を示す図である。

【0087】

最初に、認証端末101は利用者IDを入力する処理803を行う。利用者IDを取得

する方法には、第一の実施形態と同様に、数字キーにより手入力を行う方法、磁気カードやICカードからIDを取得する方法、紙に印字された番号をスキャナで読み取る方法、等が適用可能である。次に、認証端末101は生体情報を取得する処理804を行う。生体情報の取得でも、第一の実施形態と同様に、認証情報取得部102に含まれる、指紋や静脈、虹彩、筆跡等を読み取る専用装置、顔を撮影するカメラ、音声を取得するマイク等を用いる。次に、認証端末101は、認証情報（利用者ID・生体情報）805を認証サーバ104へ送信する。次に、認証サーバ104は生体情報を照合する処理806を行う。処理806の具体的な処理手順を、図12に示す。次に、認証サーバ104は本人確率を算出する処理807を行う。処理807の具体的な処理手順を、図13に示す。次に、認証サーバ104は本人であるか否かの判定をする処理808を行う。処理808の具体的な処理手順を、図14に示す。次に、認証サーバ104は、認証結果809を認証端末101へ送信する。認証結果809には、利用者の認証が成功したか否かを示す情報が含まれている。次に、認証端末101は認証結果を出力する処理810を行い、出力装置1705を通してオペレータへ利用者の認証が成功したか否かを提示する。次に、認証端末101は認証結果の確認結果を受け付ける処理811を行う。

【0088】

当該確認結果には、利用者の認証結果に応じて、4つの種類が考えられる。利用者の認証が成功した場合は、認証結果を受け入れて利用者を本人と認める確認結果と、認証結果に反して利用者を本人と認めない確認結果を選択することができる。利用者に関する生体情報以外の身分事項（例えば、身分証明書等）に問題が無い場合は、前者を選択することで、最終的な本人確認が成功とみなされ、利用者から取得した生体情報の追加登録を行うことが可能となる。一方で、利用者に関する生体情報以外の身分事項に問題があり、利用者を本人と認めることができない場合は、後者を選択することで本人確認を失敗とし、生体情報の追加登録を中止することが可能となる。

【0089】

また、利用者の認証が失敗した場合は、認証結果に反して利用者を本人と認める確認結果と、認証結果を受け入れて本人と認めない確認結果を選択することができる。利用者に関する生体情報以外の身分事項から本人確認が行えた場合には、前者を選択することで、最終的な本人確認が成功とみなされ、利用者から取得した生体情報の追加登録を行うことが可能となる。一方で、利用者に関する生体情報以外の身分事項を用いても本人確認を行うことが困難であった場合には、後者を選択することで、本人確認を失敗とし、生体情報の追加登録を行わないことが可能となる。

【0090】

次に、認証端末101は、上記の確認結果812を認証サーバ104へ送信する。確認結果812に、本人確認成功を示す情報が含まれていた場合は、認証サーバ104は生体情報仮登録処理813を実行する。処理813の具体的な手順を、図15で示す。一方、確認結果812に本人確認失敗を示す情報が含まれていた場合には、その後の生体情報仮登録処理813を行わずに、処理を終了する。

【0091】

利用者ID入力803から生体情報仮登録813までの認証処理を繰り返すことで、生体情報仮登録813が複数回実行される。その後、本実施形態では、バッチ処理として生体情報本登録814を行う。処理814の具体的な手順を、図16に示す。これにより、利用者の生体情報が複数登録される。

【0092】

本実施例では、生体情報に基づく認証結果が認証端末101へ送信された後、オペレータの確認結果を受け付けることができる。これにより、既存の登録生体情報と利用者から取得した生体情報との類似度が低く、正規の利用者が認証に失敗した場合でも、認証端末101のオペレータによる生体情報以外の身分事項に基づく本人確認結果を、認証サーバ106へ送信することが可能となる。これにより、認証サーバ106は生体情報に基づく本人確認に失敗した場合でも、生体情報の追加登録を行うことができる。

【0093】

図9は、本発明の第二の実施形態において、認証端末をオペレータが操作し、生体情報の登録をリアルタイム処理にて行う場合の手順を示す図である。

【0094】

最初に、認証端末101は利用者IDを入力処理903を行う。利用者IDを取得する方法には、数字キーにより手入力を行う方法、磁気カードやICカードからIDを取得する方法、紙に印字された番号をスキャナで読み取る方法、等が適用可能である。次に、認証端末101は生体情報を取得する処理904を行う。処理904では、認証情報取得部102に含まれる、指紋や静脈、虹彩、筆跡等を読み取る専用装置、顔を撮影するカメラ、音声を取得するマイク等を用いる。次に、認証端末101は、認証情報（利用者ID・生体情報）905を認証サーバ104へ送信する。次に、認証サーバ104は生体情報を照合する処理906を行う。処理906の具体的な処理手順を、図12で示す。次に、認証サーバ104は本人確率を算出する処理907を行う。処理907の具体的な処理手順を、図13で示す。次に、認証サーバ104は本人を判定する処理908を行う。処理908の具体的な処理手順を、図14で示す。次に、認証サーバ104は、認証結果909を認証端末101へ送信する。認証結果909には、利用者の認証が成功したか否かを示す情報が含まれている。次に、認証端末101は認証結果を出力する処理910を行い、出力装置1705を通してオペレータへ利用者の認証が成功したか否かを提示する。次に、認証端末101は認証結果の確認結果を受け付ける処理911を行う。次に、認証端末101は、確認結果912を認証サーバ104へ送信する。最後に、認証サーバ104は生体情報本登録する処理913を行う。処理913の具体的な処理手順を、図16で示す。

【0095】

以上の手順により、本実施形態では、認証時に取得した生体情報を追加登録し、複数の登録生体情報を用いて認証を行う生体認証システムにおいて、登録生体情報の一部に大きな誤差が含まれていた場合でも、高精度な認証を行うことが可能である。また、正規の利用者が生体認証に失敗した場合は、オペレータによる審査結果を受け付けることで生体情報の追加登録を行い、次回以降の認証精度を向上させることが可能である。

<第三の実施形態>

第三の実施形態は、オペレータが操作する認証端末と認証サーバを用いて、利用者から第一生体情報と第二生体情報の2種類の生体情報を取得し、第一生体情報を用いた本人確認と第二生体情報を用いたブラックリスト照合を活用することで効率的な審査を行うシステムである。第一生体情報は、指紋、静脈、虹彩、顔、音声、筆跡等の生体情報であり、第二生体情報は、第一生体情報とは異なる種類の生体情報である。例えば、第一生体情報として静脈、第二生体情報として指紋を採用することが可能である。また、ブラックリスト照合は、犯罪者等の要注意人物から取得した生体情報をブラックリストとして蓄積し、利用者の生体情報と照合を行うことで、利用者が要注意人物か否かを判定するものである。ブラックリストの一例を、図18に示す。「利用者ID」1801は各利用者に割り当てられた固有のIDであり、例えば英数字により構成される。「身分情報」1802は利用者の身分に関する情報であり、例えば氏名、国籍、性別、生年月日等を含む。「生体情報」1803は利用者の生体情報であり、利用者から取得した登録第二生体情報を格納する。このブラックリストは、認証サーバ104のHDD1703、または、認証サーバ104が参照可能な別のサーバにおけるHDD1703に保存されている。本実施形態は、入国審査に代表される、生体認証を活用したブラックリスト照合を行っているシステムに適用可能である。

【0096】

本人確認は、第二の実施形態と同様に、以前認証を行った際に登録した生体情報に基づき本人であるか否かを判定することで実現する。この際、本人確認用の生体情報データベースには、ブラックリストに登録されていない利用者のみを登録することで、第一生体情報に基づく本人確認により利用者がブラックリストに登録されていないことを保証するこ

とが可能となる。

【0097】

一方、ブラックリスト照合は、ブラックリストに含まれる第二生体情報と利用者から取得した第二生体情報との照合を行うことで実現する。ブラックリスト照合の結果一致する生体情報が無ければ、利用者は要注意人物ではないと判断され、審査を通過することができる。

【0098】

以下、図面を参照して、第三の実施形態を詳細に説明する。

【0099】

図10は本発明の第三の実施形態において、認証端末をオペレータが操作し、利用者に対するブラックリスト照合を含む審査を行う場合の手順を示す図である。

10

【0100】

最初に、認証端末101は利用者IDを入力処理1003を行う。利用者IDを取得する方法には、第一の実施形態と同様に、数字キーにより手入力を行う方法、磁気カードやICカードからIDを取得する方法、紙に印字された番号をスキャナで読み取る方法、等が適用可能である。特に、入国審査を適用対象とした場合は、旅券に印字されている旅券番号を読み取ることで、渡航者を一意に定めることが可能となる。

【0101】

次に、認証端末101は第一生体情報と第二生体情報を取得する処理1004を行う。生体情報の取得では、第一の実施形態と同様に、認証情報取得部102に含まれる、指紋や静脈、虹彩等を読み取る専用装置、顔を撮影するカメラ、等を用いる。ただし、本実施形態では第一生体情報と第二生体情報の2種類を取得する必要がある。2種類の生体情報を取得する方法には、第一生体情報（例えば、静脈）を取得する装置と第二生体情報（例えば、指紋）を取得する装置を併用する方法、および第一生体情報と第二生体情報を一度に取得する装置を活用する方法、が適用可能である。

20

【0102】

次に、認証端末101は、認証情報（利用者ID・第一生体情報）1005を認証サーバ104へ送信する。次に、認証サーバ104は生体情報照合（第一生体情報）する処理1006を行う。処理1006の具体的な処理手順を、図12に示す。処理1006の内容は、第一の実施形態における処理606と同様である。

30

【0103】

次に、認証サーバ104は本人確率を算出する処理1007を行う。処理1007の具体的な処理手順を、図13に示す。処理1007の内容は、第一の実施形態における処理607と同様である。

【0104】

次に、認証サーバ104は本人を判定する処理1008を行う。処理1008の具体的な処理手順を、図14に示す。処理1008の内容は、第一の実施形態における処理608と同様である。

【0105】

次に、認証サーバ104は、第一照合結果1009を認証端末101へ送信する。第一照合結果1009には、利用者の認証が成功したか否かを示す情報が含まれている。

40

【0106】

次に、認証端末101は第一照合結果を出力する処理1010を行い、出力装置1705を通してオペレータへ利用者の認証が成功したか否かを提示する。本実施形態は、利用者がブラックリストに登録された要注意人物であるか否かを判定することを目的としている。このため、第一照合結果1009において、認証が成功したことを示す情報が含まれている場合には、下記の処理1011～処理1014においてブラックリスト照合を行わなくても良い。一方で、第一照合結果1009において、認証失敗、または登録生体情報が存在しないことを示す情報が含まれていた場合には、下記の処理1011～処理1014でブラックリスト照合を行い、利用者が要注意人物か否かを判定する必要がある。

50

【0107】

次に、認証端末101は、認証情報（第二生体情報）1011を認証サーバ104へ送信する。

【0108】

次に、認証サーバ104は第二生体情報に基づくブラックリスト照合を行う処理1012を行う。処理1012では、複数の要注意人物から事前に取得した第二生体情報と、利用者から取得した生体情報を照合することで、利用者が要注意人物であるか否かを判定する。

【0109】

次に、認証サーバ104は、第二照合結果1013を認証端末101へ送信する。第二照合結果1013には、利用者が要注意人物と判定されたか否かを示す情報が含まれている。

10

【0110】

次に、認証端末101は第二照合結果を出力する処理1014を行い、出力装置1705を通してオペレータへ利用者が要注意人物であるか否かを提示する。

【0111】

次に、認証端末101はオペレータの確認結果を受け付ける処理1015を行う。確認結果には、第一生体情報を登録するか否かを示す情報が含まれている。利用者が要注意人物ではない場合は、第一生体情報を登録することで次回以降にブラックリスト照合を必要としないスムーズな審査を実現することができる。一方、利用者が要注意人物である場合は、第一生体情報を登録せず、審査を完了する。ここでオペレータは、第二照合結果1013において利用者が要注意人物であると判定された場合でも、利用者の生体情報以外の身分事項に基づく審査で利用者が要注意人物ではないと確認されれば、第一生体情報登録を実行することができる。これは、利用者の第二生体情報と要注意人物の第二生体情報が類似している場合、要注意人物以外の利用者が要注意人物と誤判定される可能性があるためである。このように、要注意人物と類似する第二生体情報を持つ利用者は、第二生体情報に基づくブラックリスト照合を行う度に要注意人物と誤判定されて利便性が低下する危険性があるが、第一生体情報を登録することでブラックリスト照合を不要とし、利便性の確保を行うことが可能となる。

20

【0112】

次に、認証端末101は、確認結果1016を認証サーバ104へ送信する。

30

【0113】

ここで、認証サーバ104は、確認結果1016に含まれる情報に応じて処理を分岐する。確認結果1016に第一生体情報登録を行うとの情報が含まれている場合は、処理1017～処理1018を行う。確認結果1016に第一生体情報登録を行わないとの情報が含まれている場合には、ここで処理を終了する。

【0114】

処理1017では、第一生体情報の仮登録を行う。処理1017の具体的な処理手順を、図15で示す。処理1003～処理1017を繰り返すことで、複数の第一生体情報が仮登録生体情報格納部115に蓄積する。

40

【0115】

最後に、認証サーバ104は第一生体情報を登録する処理1018を行う。処理1018の具体的な処理手順を、図16に示す。処理1003～処理1017を繰り返すことで蓄積した第一生体情報の登録が完了する。

【0116】

図11は、本発明の第三の形態において、認証端末をオペレータが操作し、利用者に対するブラックリスト照合を含む審査を行う場合の手順を示す図である。処理1103～処理1116は図10と同様であるが、その後の生体情報本登録（第一生体情報）1117を実行するタイミングが図10と異なる。図10では生体情報仮登録（第一生体情報）1017を繰り返すことで仮登録生体情報格納部115へ生体情報を蓄積した後、生体情報

50

本登録（第一生体情報）1018にてバッチ処理で生体情報を登録生体情報格納部114に本登録する。この生体情報仮登録を伴う方式では、認証時の計算負荷が低い、仮登録生体情報を蓄積するためのテーブルが必要となり、DBの容量が増加する。一方、図11では、生体情報の仮登録は行わず、リアルタイムで生体情報本登録（第一生体情報）1117を行い、登録生体情報格納部114へ生体情報を登録する。このリアルタイムに生体情報本登録を行う方式では、認証時の計算負荷が高い、仮登録生体情報を蓄積するテーブルが不要となり、必要なDB容量が小さくなる。

【0117】

以上により、第二生体情報に基づくブラックリスト照合を含む審査を行う生体認証システムにおいて、第一生体情報を複数登録し、本人確認に活用することが可能となる。本実施形態を用いることで、ブラックリスト内の生体情報と一致しない利用者は、第一生体情報に基づく本人確認によりスムーズな審査を行うことが可能となる。また、要注意人物と第二生体情報が類似する利用者は、生体情報以外の身分事項に基づく審査で要注意人物ではないと確認されれば、第一生体情報を登録し、次回以降ブラックリスト照合の誤判別なしに審査を受けることが可能となる。

10

【符号の説明】

【0118】

101…認証端末
 102…認証情報取得部
 103…認証結果表示部
 104…認証サーバ
 105…生体情報照合部
 106…生体情報選択部
 107…生体情報登録部
 108…信頼度算出部
 109…信頼度登録部
 110…本人確率算出部
 111…登録生体情報格納部
 112…仮登録生体情報格納部
 113…尤度比配列格納部
 114…認証しきい値格納部
 201…利用者ID
 202…登録生体情報
 203…信頼度
 301…利用者ID
 302…仮登録生体情報
 401…信頼度
 402…類似度
 403…尤度比
 501…精度要件（FAR）
 502…認証しきい値
 603…利用者ID取得
 604…生体情報取得
 605…認証情報（利用者ID・生体情報）
 606…生体情報照合
 607…本人確率算出
 608…本人判定
 609…生体情報仮登録
 610…認証結果
 611…認証結果出力

20

30

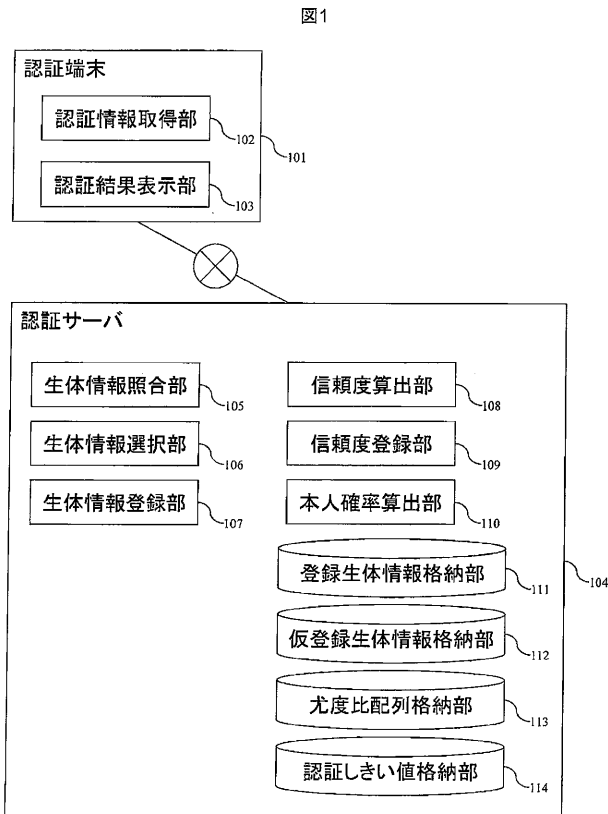
40

50

6 1 2 … 生体情報本登録	
7 0 3 … 利用者 I D 入力	
7 0 4 … 生体情報取得	
7 0 5 … 認証情報（利用者 I D ・ 生体情報）	
7 0 6 … 生体情報照合	
7 0 7 … 本人確率算出	
7 0 8 … 本人判定	
7 0 9 … 生体情報本登録	
7 1 0 … 認証結果	
7 1 1 … 認証結果出力	10
8 0 3 … 利用者 I D 入力	
8 0 4 … 生体情報取得	
8 0 5 … 認証情報（利用者 I D ・ 生体情報）	
8 0 6 … 生体情報照合	
8 0 7 … 本人確率算出	
8 0 8 … 本人判定	
8 0 9 … 認証結果	
8 1 0 … 認証結果出力	
8 1 1 … 確認結果入力	
8 1 2 … 確認結果	20
8 1 3 … 生体情報仮登録	
8 1 4 … 生体情報本登録	
9 0 3 … 利用者 I D 入力	
9 0 4 … 生体情報取得	
9 0 5 … 認証情報（利用者 I D ・ 生体情報）	
9 0 6 … 生体情報照合	
9 0 7 … 本人確率算出	
9 0 8 … 本人判定	
9 0 9 … 認証結果	
9 1 0 … 認証結果出力	30
9 1 1 … 確認結果入力	
9 1 2 … 確認結果	
9 1 3 … 生体情報本登録	
1 0 0 3 … 利用者 I D 入力	
1 0 0 4 … 第一・第二生体情報取得	
1 0 0 5 … 認証情報（利用者 I D ・ 第一生体情報）	
1 0 0 6 … 生体情報照合（第一生体情報）	
1 0 0 7 … 本人確率算出	
1 0 0 8 … 本人判定	
1 0 0 9 … 第一照合結果	40
1 0 1 0 … 第一照合結果出力	
1 0 1 1 … 認証情報（利用者 I D ・ 第二生体情報）	
1 0 1 2 … 生体情報照合（第二生体情報）	
1 0 1 3 … 第二照合結果	
1 0 1 4 … 第二照合結果出力	
1 0 1 5 … 確認結果入力	
1 0 1 6 … 確認結果	
1 0 1 7 … 生体情報仮登録（第一生体情報）	
1 0 1 8 … 生体情報本登録（第一生体情報）	
1 1 0 3 … 利用者 I D 入力	50

1 1 0 4	… 第一・第二生体情報取得	
1 1 0 5	… 認証情報（利用者 I D・第一生体情報）	
1 1 0 6	… 生体情報照合（第一生体情報）	
1 1 0 7	… 本人確率算出	
1 1 0 8	… 本人判定	
1 1 0 9	… 第一照合結果	
1 1 1 0	… 第一照合結果出力	
1 1 1 1	… 認証情報（利用者 I D・第二生体情報）	
1 1 1 2	… 生体情報照合（第二生体情報）	
1 1 1 3	… 第二照合結果	10
1 1 1 4	… 第二照合結果出力	
1 1 1 5	… 確認結果入力	
1 1 1 6	… 確認結果	
1 1 1 7	… 生体情報本登録（第一生体情報）	
1 2 0 1	… 利用者 I Dに基づき登録生体情報(N件)を参照する処理	
1 2 0 2	… 受信した生体情報と、N件の登録生体情報を照合する処理	
1 2 0 3	… N件の類似度を算出する処理	
1 3 0 1	… 利用者 I Dに基づき、各登録生体情報に対する信頼度を読み出しする処理	
1 3 0 2	… 登録生体情報の信頼度と類似度に基づき、尤度比を読み出しする処理	
1 3 0 3	… 各登録生体情報に対応する尤度比を統合して、本人確率を算出する処理	20
1 4 0 1	… 本人確率に対して、予め設定した認証しきい値を適用する処理	
1 4 0 2	… 本人確率>認証しきい値かどうか調べる処理	
1 4 0 3	… 認証結果に認証成功を代入する処理	
1 4 0 4	… 認証結果に認証失敗を代入する処理	
1 5 0 1	… 利用者 I Dと利用者から取得した生体情報を、仮登録生体情報格納部へ登録する処理	
1 6 0 1	… 利用者 I Dと生体情報を、登録生体情報格納部に登録する処理	
1 6 0 2	… 利用者 I Dが等しい登録生体情報同士を照合し、類似度を取得する処理	
1 6 0 3	… 登録生体情報間の類似度に基づき、各登録生体情報の信頼度を算出する処理	
1 6 0 4	… 信頼度を登録生体情報格納部へ登録する処理	30
1 7 0 1	… C P U (C e n t r a l P r o c e s s i n g U n i t)	
1 7 0 2	… メモリ	
1 7 0 3	… H D D (H a r d D i s k D r i v e)	
1 7 0 4	… 入力装置	
1 7 0 5	… 出力装置	
1 7 0 6	… 通信装置	
1 8 0 1	… 利用者 I D	
1 8 0 2	… 身分情報	
1 8 0 3	… 生体情報	

【図 1】



【図 2】

図2

利用者ID	登録生体情報	信頼度
0001	1回目の利用時に取得した生体情報	R(0001,1)
0001	2回目の利用時に取得した生体情報	R(0001,2)
0002	1回目の利用時に取得した生体情報	R(0002,1)
...	...	...

【図 3】

図3

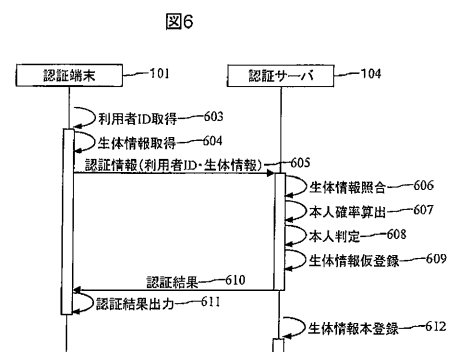
利用者ID	仮登録生体情報
0001	3回目の利用時に取得した生体情報
0001	4回目の利用時に取得した生体情報
0002	3回目の利用時に取得した生体情報
...	...

【図 4】

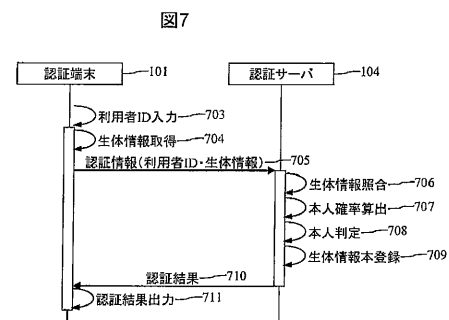
図4

信頼度	類似度	尤度比
10	0	L(10,0)
	1	L(10,1)
	...	...
	100	L(10,100)
20	0	L(20,0)
	1	L(20,1)
	...	...
	100	L(20,100)
...	...	...

【図 6】



【図 7】



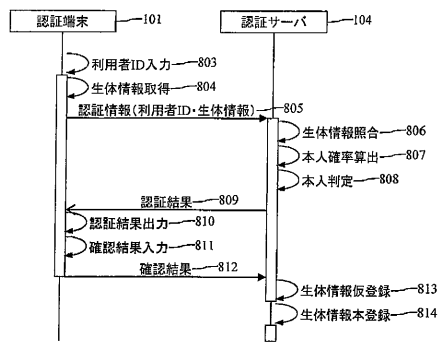
【図 5】

図5

精度要件(FAR)	認証しきい値
0.001	T(0.001)
0.0001	T(0.0001)
0.00001	T(0.00001)
...	...

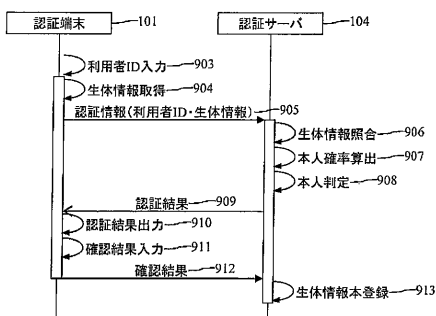
【図 8】

図8



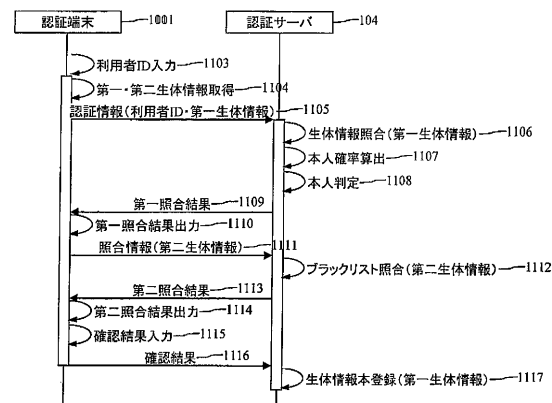
【図 9】

図9



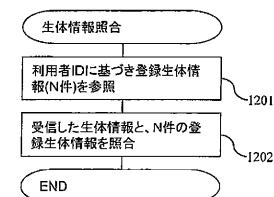
【図 1 1】

図11



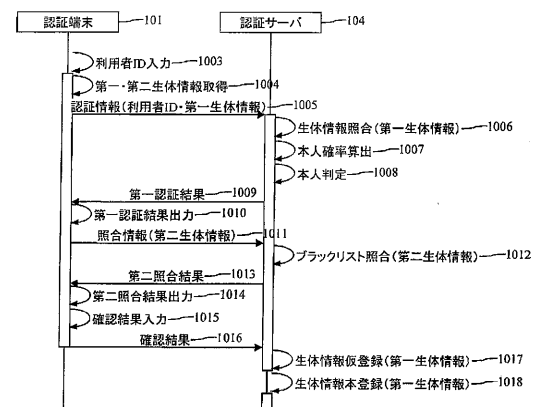
【図 1 2】

図12



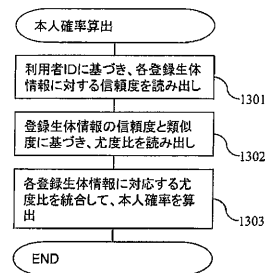
【図 1 0】

図10



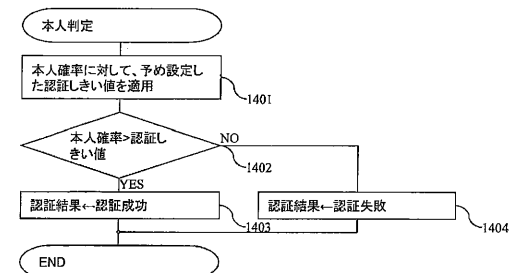
【図 1 3】

図13

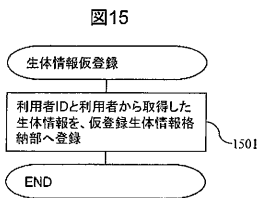


【図 1 4】

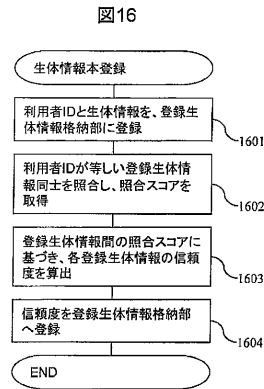
図14



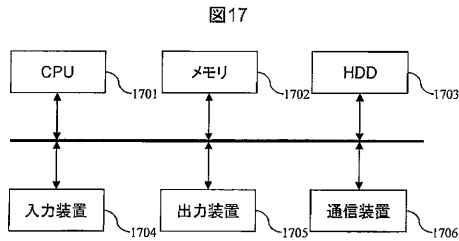
【図 1 5】



【図 1 6】



【図 1 7】



【図 1 8】

図18

1801			1802		1803	
利用者ID	身分情報	生体情報				
0001	氏名、国籍等	登録第二生体情報				
0001	氏名、国籍等	登録第二生体情報				
0002	氏名、国籍等	登録第二生体情報				
...	...	...				

【国際調査報告】

INTERNATIONAL SEARCH REPORT		International application No. PCT/JP2011/078025
A. CLASSIFICATION OF SUBJECT MATTER G06F21/20(2006.01)i, G06T7/00(2006.01)i According to International Patent Classification (IPC) or to both national classification and IPC		
B. FIELDS SEARCHED Minimum documentation searched (classification system followed by classification symbols) G06F21/20, G06T7/00 Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched Jitsuyo Shinan Koho 1922-1996 Jitsuyo Shinan Toroku Koho 1996-2011 Kokai Jitsuyo Shinan Koho 1971-2011 Toroku Jitsuyo Shinan Koho 1994-2011 Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)		
C. DOCUMENTS CONSIDERED TO BE RELEVANT		
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	JP 2004-342073 A (NEC Corp.), 02 December 2004 (02.12.2004), paragraphs [0018] to [0023] & US 2004/0255128 A1 & EP 1471458 A2 & DE 602004016910 D & CN 1540573 A	1-8
Y	JP 2003-44858 A (Matsushita Electric Industrial Co., Ltd.), 14 February 2003 (14.02.2003), paragraphs [0017] to [0035] (Family: none)	1-8
☒ Further documents are listed in the continuation of Box C. ☐ See patent family annex.		
* Special categories of cited documents: "A" document defining the general state of the art which is not considered to be of particular relevance "E" earlier application or patent but published on or after the international filing date "L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified) "O" document referring to an oral disclosure, use, exhibition or other means "P" document published prior to the international filing date but later than the priority date claimed "T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention "X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone "Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art "&" document member of the same patent family		
Date of the actual completion of the international search 14 December, 2011 (14.12.11)		Date of mailing of the international search report 27 December, 2011 (27.12.11)
Name and mailing address of the ISA/ Japanese Patent Office		Authorized officer
Facsimile No.		Telephone No.

INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2011/078025

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	JP 2005-50328 A (Trek 2000 International Ltd.), 24 February 2005 (24.02.2005), paragraph [0054] & US 2003/0005337 A1 & US 2008/0049984 A1 & EP 2000937 A2 & WO 2003/003278 A1 & WO 2003/003282 A1	5, 6
Y	JP 2006-260482 A (Fujitsu Ltd.), 28 September 2006 (28.09.2006), abstract & US 2006/0212717 A1	6

国際調査報告		国際出願番号 PCT/J P 2 0 1 1 / 0 7 8 0 2 5	
A. 発明の属する分野の分類 (国際特許分類 (IPC)) Int.Cl. G06F21/20 (2006.01)i, G06T7/00 (2006.01)i			
B. 調査を行った分野 調査を行った最小限資料 (国際特許分類 (IPC)) Int.Cl. G06F21/20, G06T7/00			
最小限資料以外の資料で調査を行った分野に含まれるもの 日本国実用新案公報 1922-1996年 日本国公開実用新案公報 1971-2011年 日本国実用新案登録公報 1996-2011年 日本国登録実用新案公報 1994-2011年			
国際調査で使用した電子データベース (データベースの名称、調査に使用した用語)			
C. 関連すると認められる文献			
引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求項の番号	
Y	JP 2004-342073 A (日本電気株式会社) 2004.12.02, 段落【0018】 - 【0023】等 & US 2004/0255128 A1 & EP 1471458 A2 & DE 602004016910 D & CN 1540573 A	1-8	
Y	JP 2003-44858 A (松下電器産業株式会社) 2003.02.14, 段落【0017】 - 【0035】等 (ファミリーなし)	1-8	
Y	JP 2005-50328 A (トレック・2000・インターナショナル・リミテッド) 2005.02.24, 段落【0054】等 & US 2003/0005337 A1 & US 2008/0049984 A1 & EP 2000937 A2 & WO 2003/003278 A1 & WO 2003/003282 A1	5、6	
☒ C欄の続きにも文献が列挙されている。 ☐ パテントファミリーに関する別紙を参照。			
* 引用文献のカテゴリー 「A」特に関連のある文献ではなく、一般的技術水準を示すもの 「E」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの 「L」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献 (理由を付す) 「O」口頭による開示、使用、展示等に言及する文献 「P」国際出願日前で、かつ優先権の主張の基礎となる出願日の後に公表された文献 「T」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの 「X」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの 「Y」特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの 「&」同一パテントファミリー文献			
国際調査を完了した日 14.12.2011		国際調査報告の発送日 27.12.2011	
国際調査機関の名称及びあて先 日本国特許庁 (ISA/J P) 郵便番号100-8915 東京都千代田区霞が関三丁目4番3号		特許庁審査官 (権限のある職員) 児玉 崇晶 電話番号 03-3581-1101 内線 3546	5 S 3651

国際調査報告		国際出願番号 PCT/J P 2 0 1 1 / 0 7 8 0 2 5
C (続き) . 関連すると認められる文献		
引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求項の番号
Y	JP 2006-260482 A (富士通株式会社) 2006.09.28, 要約等 & US 2006/0212717 A1	6

フロントページの続き

(81)指定国 AP(BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, SZ, TZ, UG, ZM, ZW), EA(AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), EP(AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OA(BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG), AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN

Fターム(参考) 5B043 AA02 AA04 AA09 BA02 BA03 BA04 BA06 BA07 CA09 EA06
EA07 EA08 FA02 FA07 FA08 GA05 GA18

(注) この公表は、国際事務局(WIPO)により国際公開された公報を基に作成したものである。なおこの公表に係る日本語特許出願(日本語実用新案登録出願)の国際公開の効果は、特許法第184条の10第1項(実用新案法第48条の13第2項)により生ずるものであり、本掲載とは関係ありません。