

(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2016-118910

(P2016-118910A)

(43) 公開日 平成28年6月30日 (2016. 6. 30)

(51) Int. Cl.		F I				テーマコード (参考)
G06T	7/00	(2006.01)	G06T	7/00	570	5B043
G06F	3/041	(2006.01)	G06F	3/041	595	5B087
G06F	3/0346	(2013.01)	G06F	3/033	422	

審査請求 未請求 請求項の数 9 O L (全 20 頁)

(21) 出願番号 特願2014-257756 (P2014-257756)
 (22) 出願日 平成26年12月19日 (2014. 12. 19)

(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 園分 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 渡邊 睦
 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

最終頁に続く

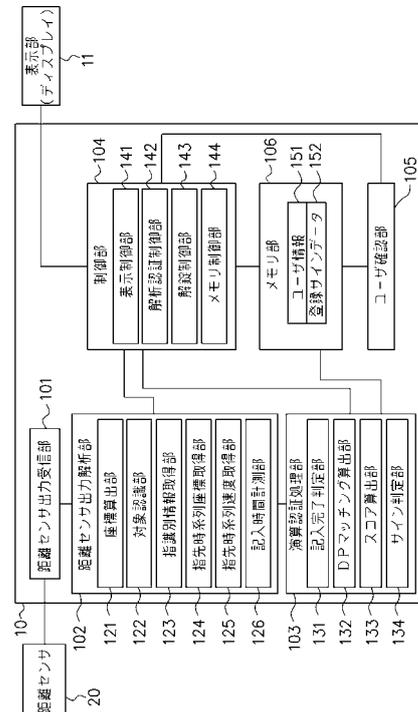
(54) 【発明の名称】 認証処理装置及び認証処理方法、認証情報登録装置及び認証情報登録方法

(57) 【要約】

【課題】 覗き見等によるサインの漏洩を無くすし、また認証センサ等に触れることなく、非常に高いセキュリティ性を確保した個人認証を可能とすることを課題とする。

【解決手段】 距離センサ20は三次元空間内の手と手指の三次元座標をフレームごとに検出する。指識別情報取得部123は、手の手指を識別して指識別情報を生成する。演算認証処理部103は、指識別情報と、認証対象者の手指の指先が三次元空間内を移動した際に距離センサ20が検出した三次元座標情報とに基づいて、認証対象者が手指の指先により三次元空間内に記入した空中サインデータを算出し、その空中サインデータと登録サインデータとを比較して認証判定を行う。

【選択図】 図8



【特許請求の範囲】**【請求項 1】**

三次元空間内における検出対象物の三次元座標を所定の時間周期ごとに検出する座標検出手段と、

前記三次元空間内の前記検出対象物が認証対象者の手であるとき、前記手の手指を識別して指識別情報を生成する指識別手段と、

前記指識別手段による前記指識別情報と、前記認証対象者の前記手指の指先が前記三次元空間内を移動した際に前記座標検出手段にて前記所定の時間周期ごとに検出された三次元座標情報とに基づいて、前記認証対象者が前記手指の指先により前記三次元空間内に記入したサインのデータを算出する演算手段と、

前記演算手段により算出された前記サインのデータと予め登録されている登録サインのデータとを比較して認証判定を行う認証判定手段とを有することを特徴とする認証処理装置。

10

【請求項 2】

前記指識別手段は、前記手の各手指のうち何れか一本の手指のみが伸ばされて他の各手指が折り曲げられているとき、前記伸ばされた手指を個別に識別した指識別情報を生成し、

前記演算手段は、前記サインを構成している複数のパーツごとに、前記指識別手段により前記個別に識別された前記手指の指識別情報と、前記手指の指先が前記三次元空間内を移動した際の前記三次元座標情報とに基づいて、前記サインのデータを算出し、

前記認証判定手段は、登録サインを構成している複数のパーツごとに個別の指識別情報と三次元座標情報とに基づいて予め算出されて登録されている前記登録サインのデータと、前記演算手段により算出された前記サインのデータとを比較して前記認証判定を行うことを特徴とする請求項 1 記載の認証処理装置。

20

【請求項 3】

三次元空間内における検出対象物の三次元座標を所定の時間周期ごとに検出する座標検出手段と、

前記三次元空間内の前記検出対象物が登録対象者の手であるとき、前記手の手指を識別して指識別情報を生成する指識別手段と、

前記指識別手段による前記指識別情報と、前記登録対象者の前記手指の指先が前記三次元空間内を移動した際に前記座標検出手段にて前記所定の時間周期ごとに検出された三次元座標情報とに基づいて、前記登録対象者が前記手指の指先により前記三次元空間内に記入したサインのデータを算出する演算手段と、

前記演算手段により算出された前記サインのデータを、登録サインのデータとして登録する登録手段とを有することを特徴とする認証情報登録装置。

30

【請求項 4】

前記指識別手段は、前記手の各手指のうち何れか一本の手指のみが伸ばされて他の各手指が折り曲げられているとき、前記伸ばされた手指を個別に識別した指識別情報を生成し、

前記演算手段は、前記サインを構成している複数のパーツごとに、前記指識別手段により前記個別に識別された前記手指の指識別情報と、前記手指の指先が前記三次元空間内を移動した際の前記三次元座標情報とに基づいて、前記サインのデータを算出することを特徴とする請求項 3 記載の認証情報登録装置。

40

【請求項 5】

前記登録手段は、複数の登録対象者ごとに個別に前記算出がなされた登録サインのデータを、前記登録対象者ごとに対応させて前記登録することを特徴とする請求項 3 又は 4 記載の認証情報登録装置。

【請求項 6】

前記登録手段は、複数の登録対象場所ごとに、それぞれ異なる前記サインのデータを対

50

応させて前記登録することを特徴とする請求項 3 乃至 5 のうち何れか 1 項に記載の認証情報登録装置。

【請求項 7】

前記登録手段は、前記登録対象場所ごとに要求されるセキュリティレベルに応じて、前記登録対象場所ごとに前記異なるサインのデータを対応させて登録することを特徴とする請求項 6 記載の認証情報登録装置。

【請求項 8】

認証処理装置が実行する認証処理方法であって、
三次元空間内における検出対象物の三次元座標を所定の時間周期ごとに検出する座標検出ステップと、

前記三次元空間内の前記検出対象物が認証対象者の手であるとき、前記手の手指を識別して指識別情報を生成する指識別ステップと、

前記指識別ステップによる前記指識別情報と、前記認証対象者の前記手指の指先が前記三次元空間内を移動した際に前記座標検出ステップにて前記所定の時間周期ごとに検出された三次元座標情報とに基づいて、前記認証対象者が前記手指の指先により前記三次元空間内に記入したサインのデータを算出する演算ステップと、

前記演算ステップにより算出された前記サインのデータと予め登録されている登録サインのデータとを比較して認証判定を行う認証判定ステップと
を含むことを特徴とする認証処理方法。

【請求項 9】

認証情報登録装置が実行する認証情報登録方法であって、
三次元空間内における検出対象物の三次元座標を所定の時間周期ごとに検出する座標検出ステップと、

前記三次元空間内の前記検出対象物が登録対象者の手であるとき、前記手の手指を識別して指識別情報を生成する指識別ステップと、

前記指識別ステップによる前記指識別情報と、前記登録対象者の前記手指の指先が前記三次元空間内を移動した際に前記座標検出ステップにて前記所定の時間周期ごとに検出された三次元座標情報とに基づいて、前記登録対象者が前記手指の指先により前記三次元空間内に記入したサインのデータを算出する演算ステップと、

前記演算ステップにより算出された前記サインのデータを登録サインのデータとして登録する登録ステップと
を含むことを特徴とする認証情報登録方法。

【発明の詳細な説明】

【技術分野】

【0001】

本発明は、認証対象者の個人認証を行う認証処理装置及び認証処理方法、個人認証に使用する情報を登録する認証情報登録装置及び認証情報登録方法に関するものである。

【背景技術】

【0002】

従来より、クレジットカードなどを使用した際にはサイン（署名）の記入が求められることが多い。サインは、ペンなどを用いて伝票等の所定欄に氏名を書くことにより行われている。クレジットカードの管理会社等は、伝票等に記入されたサインを基に、そのクレジットカードを使用した者（認証対象者）が正当な使用者であるかを確認する。なお、伝票等の紙面上にサインを記入する代わりに、例えばクレジットカードの管理会社等とオンライン接続されているタブレット端末等を使用し、そのタブレット端末等のタッチセンサ画面上にサインすることでオンライン個人認証が行われる場合もある。

【0003】

また例えば、特許文献 1 には、ステレオカメラから得られる手指の軌跡と、3次元加速度センサから得られる手指動作の加速度データとに基づく、空中での署名動作により個人認証を行う認証装置が開示されている。

10

20

30

40

50

【先行技術文献】

【特許文献】

【0004】

【特許文献1】特開2009-9280号公報

【発明の概要】

【発明が解決しようとする課題】

【0005】

ところで、伝票等に記入されたサインを用いる個人認証は、クレジットカードの管理会社等による確認作業が必要であり、その場で認証対象者が正当な者であることを確認することが難しい。また、伝票等に記入されたサインは、覗き見られる虞があり、その伝票等が盗まれてしまう虞もある。一方、前述したタブレット端末等のタッチセンサ画面上へのサインによるオンライン個人認証ならば、その場で個人認証を行うことはできるが、サインを記入している際に覗き見られてしまう虞がある。このように、従来のサイン記入による個人認証は、覗き見等によるサインの漏洩に対して、セキュリティ性が高いとは言い難い。

10

【0006】

これに対し、近年は、例えば指紋や手の静脈模様、虹彩などに基づくバイオメトリクス情報を利用した個人認証を用いることで、高いセキュリティ性を確保した個人認証が行われるケースも増えてきている。

【0007】

20

しかしながら、バイオメトリクス情報による認証は、セキュリティ性が高く安全、安心ではあるが、指紋センサや静脈センサ、虹彩センサのような特殊な認証用センサが必要になり、その導入コストはかなりの高額となる。

【0008】

また例えば指紋を用いた場合において、例えば表面が非常に滑らかな金属やガラス等を指先で触れたような時に、それらガラス等の表面に皮脂による指紋パターンが残ってしまうこともあり、その指紋パターンが盗まれることも考えられる。また、手の静脈模様についても、例えば赤外線カメラなどにより撮影されることで静脈パターンが盗まれてしまう虞がある。

【0009】

30

さらに、指紋等の生体情報は、各人に対して唯一の情報であって代替ができない情報であるため、例えばその情報が何らかの方法で盗まれてしまうと、新たに認証情報を登録し直すようなことが非常に難しくなるという問題もある。

【0010】

その他にも、指紋を認証に使用する場合は、予め指紋採取が行なわれることになるが、指紋採取に対して抵抗感を抱く人も多い。バイオメトリクス情報として指紋や手の静脈などの情報を用いる場合、認証対象者は、認証機器が備えている認証用センサ上に手指や手掌を接触させなければならない。しかしながら、不特定多数の人が触れた認証用センサに触れることに対して嫌悪感を抱く人が少なくなかない。

【0011】

40

本発明はこのような問題点に鑑みてなされたものであり、覗き見等によるサインの漏洩を無くすことができ、また認証用センサ等に触れることなく、非常に高いセキュリティ性を確保した個人認証を可能とする認証処理装置及び認証処理方法、個人認証に使用する情報を登録する認証情報登録装置及び認証情報登録方法を提供することを目的とする。

【課題を解決するための手段】

【0012】

本発明の認証処理装置は、三次元空間内における検出対象物の三次元座標を所定の時間周期ごとに検出する座標検出手段と、前記三次元空間内の前記検出対象物が認証対象者の手であるとき、前記手の手指を識別して指識別情報を生成する指識別手段と、前記指識別手段による前記指識別情報と、前記認証対象者の前記手指の指先が前記三次元空間内を移

50

動した際に前記座標検出手段にて前記所定の時間周期ごとに検出された三次元座標情報とに基づいて、前記認証対象者が前記手指の指先により前記三次元空間内に記入したサインのデータを算出する演算手段と、前記演算手段により算出された前記サインのデータと予め登録されている登録サインのデータとを比較して認証判定を行う認証判定手段とを有することを特徴とする。

【0013】

本発明の認証情報登録装置は、三次元空間内における検出対象物の三次元座標を所定の時間周期ごとに検出する座標検出手段と、前記三次元空間内の前記検出対象物が登録対象者の手であるとき、前記手の手指を識別して指識別情報を生成する指識別手段と、前記指識別手段による前記指識別情報と、前記登録対象者の前記手指の指先が前記三次元空間内を移動した際に前記座標検出手段にて前記所定の時間周期ごとに検出された三次元座標情報とに基づいて、前記登録対象者が前記手指の指先により前記三次元空間内に記入したサインのデータを算出する演算手段と、前記演算手段により算出された前記サインのデータを、登録サインのデータとして登録する登録手段とを有することを特徴とする。

10

【0014】

本発明の認証処理方法は、認証処理装置が実行する認証処理方法であって、三次元空間内における検出対象物の三次元座標を所定の時間周期ごとに検出する座標検出ステップと、前記三次元空間内の前記検出対象物が認証対象者の手であるとき、前記手の手指を識別して指識別情報を生成する指識別ステップと、前記指識別ステップによる前記指識別情報と、前記認証対象者の前記手指の指先が前記三次元空間内を移動した際に前記座標検出ステップにて前記所定の時間周期ごとに検出された三次元座標情報とに基づいて、前記認証対象者が前記手指の指先により前記三次元空間内に記入したサインのデータを算出する演算ステップと、前記演算ステップにより算出された前記サインのデータと予め登録されている登録サインのデータとを比較して認証判定を行う認証判定ステップとを含むことを特徴とする。

20

【0015】

本発明の認証処理方法は、認証情報登録装置が実行する認証情報登録方法であって、三次元空間内における検出対象物の三次元座標を所定の時間周期ごとに検出する座標検出ステップと、前記三次元空間内の前記検出対象物が登録対象者の手であるとき、前記手の手指を識別して指識別情報を生成する指識別ステップと、前記指識別ステップによる前記指識別情報と、前記登録対象者の前記手指の指先が前記三次元空間内を移動した際に前記座標検出ステップにて前記所定の時間周期ごとに検出された三次元座標情報とに基づいて、前記登録対象者が前記手指の指先により前記三次元空間内に記入したサインのデータを算出する演算ステップと、前記演算ステップにより算出された前記サインのデータを登録サインのデータとして登録する登録ステップとを含むことを特徴とする。

30

【発明の効果】

【0016】

本発明によれば、覗き見等によるサインの漏洩を無くすことができ、また認証センサ等に触れることなく、非常に高いセキュリティ性を確保した個人認証が可能となる。

40

【図面の簡単な説明】

【0017】

【図1】実施形態の認証処理装置の概観の一例を示す図である。

【図2】異なる手指で空中サインの記入が行われる一例の説明に用いる図である。

【図3】空中サインとして使用される記号、重ね字等の説明に用いる図である。

【図4】登録サインの変更の説明に用いる図である。

【図5】セキュリティレベルに応じた空中サインの一例を示す図である。

【図6】空中サインを登録する際の類似度の説明に用いる図である。

【図7】登録サインに対する空中サインの類似度に応じて登録ユーザの認証が行われることの説明に用いる図である。

【図8】本実施形態の情報処理装置の構成を示す図である。

50

【図 9】本実施形態の情報処理装置において認証処理が行われる際の制御フローチャートである。

【図 10】距離センサのセンサ面上の赤外線 LED と赤外線カメラの配置例を示す図である。

【図 11】距離センサの有効範囲の説明に用いる図である。

【図 12】距離センサのセンサ面上の三次元空間の座標説明に用いる図である。

【図 13】検出対象物である手をモデル化して説明する図である。

【図 14】登録ユーザ本人の空中サインと他人による空中サインの時系列座標データとスコアポイントの説明に用いる図である。

【図 15】登録ユーザ本人の空中サインと他人による空中サインの時系列速度データとスコアポイントの説明に用いる図である。

10

【図 16】時系列速度データ上に、記入時間の差に相当するフレーム数の差を表して記入時間の説明に用いる図である。

【図 17】三つの登録サインデータと登録ユーザでない他人による空中サインデータとの間の座標、速度、記入時間の各データと類似度の値を示す図である。

【図 18】本実施形態の認証処理装置が適用されて、サーバによりセキュリティ管理がなされるシステムの概略的な構成例を示す図である。

【発明を実施するための形態】

【0018】

図 1 は、本発明の実施形態の認証処理装置 1 の概観の一例を示す図である。図 1 に示すように、本実施形態に係る認証処理装置 1 は、座標検出手段と指識別手段と演算手段と認証判定手段の機能を実現するための構成の一例である情報処理装置 10 と、座標検出手段の機能を実現するための構成の一例である距離センサ 20 とを有して構成されている。情報処理装置 10 と距離センサ 20 は、信号ケーブル若しくは無線により接続されている。また、図 1 に示すように、情報処理装置 10 にはディスプレイ 11 が併設されている。

20

【0019】

距離センサ 20 は、三次元空間内における検出対象物の三次元座標を所定の時間周期ごとに検出するための座標検出手段の機能の一部を担っている。座標検出手段は、距離センサ 20 と情報処理装置 10 内の後述する座標算出部 121 により構成されている。距離センサ 20 の詳細は後述する。また、ディスプレイ 11 は、認証対象者 2 の個人認証が行われる際に、その認証対象者 2 に対するユーザインターフェイス画面を表示する。情報処理装置 10 は、三次元空間内に仮想二次元平面を設定する。また、情報処理装置 10 は、仮想二次元平面の三次元空間内で、認証対象者 2 が例えば手指 31 を用いて個人認証のためのサインを記入（以下、空中サインと呼ぶ。）したときに、その空中サインを記入している手指 31 が親指から小指までの何れの手指であるかを識別する。さらに、情報処理装置 10 は、その識別した手指 31 の指先が三次元空間内で動いた際の移動軌跡と移動時間及び移動速度を解析する。情報処理装置 10 は、それら手指を識別した指識別情報と移動軌跡と移動時間及び移動速度を表す各情報とに基づいて、空中サインデータを算出する。そして、情報処理装置 10 は、算出した空中サインデータと、予め登録されている正規ユーザの登録サインデータとを比較して、認証対象者 2 の個人認証を行う。仮想二次元平面の三次元空間内に記入される空中サインの詳細については後述する。空中サインデータと登録サインデータとの比較処理の詳細、登録サインデータの登録処理の詳細、情報処理装置 10 の構成の詳細についても後述する。

30

40

【0020】

ここで、図 2 には、一例として、仮想ノートエリア 40 の三次元空間内に、漢字の二文字で構成された空中サインが記入された例を示す。この図 2 の例の場合、先ず人差し指 31 (F1) を用いて、空中サインを構成する「島」の文字からなるパーツ 50 が記入され、続いて親指 31 (F0) を用いて、空中サインを構成する「中」の文字からなるパーツ 51 が記入されている。情報処理装置 10 は、パーツ 50 の記入に使用された手指 31 (F1) の識別情報及び三次元空間内でその手指 31 (F1) の指先が動いた移動軌跡と移

50

動時間及び移動速度を表す情報と、パーツ 5 1 の記入に使用された手指 3 1 (F 0) の指識別情報及び三次元空間内でその手指 3 1 (F 0) の指先が動いた移動軌跡と移動時間及び移動速度を表す情報とに基づいて、空中サインデータを算出する。そして、情報処理装置 1 0 は、空中サインデータと、予め登録されている登録サインデータとを比較して、認証対象者 2 の個人認証を行う。

【 0 0 2 1 】

図 2 には漢字二文字で構成される空中サインが記入された例を挙げたが、本実施形態における空中サインは、文字のみに限定されず、例えば図 3 (a) や図 3 (b) に示すような記号であってもよい。記号が空中サインに用いられる場合、その記号は図 3 (a) に示すように一本の手指のみで記入されてもよいし、図 3 (b) に示すようにその記号を構成する各線のパーツがそれぞれ別の手指を用いて記入されてもよい。なお、図 3 (b) において、それぞれ太さが異なる各パーツは、そのパーツを記入した手指が異なっていることを表している。また図 2 の例では、空中サインの構成パーツである各文字等を横方向に並べて記入しているが、各文字は縦方向に並べられてもよいし、斜め方向に並べられてもよい。また、空中サインの構成パーツである各文字等は、例えば図 3 (c) や図 3 (d) のように各文字が重ねられてもよい。なお、図 3 (c) は空中サインの構成パーツである「畠」と「中」の漢字二文字が重ねられて記入された例を示しており、図 3 (d) は空中サインの構成パーツである「I」, 「S」, 「S」, 「E」, 「I」のローマ字五文字が重ねられて記入された例を示している。図 3 (c) と図 3 (d) においても、それぞれ太さが異なる各文字は、その文字を記入した手指が異なっていることを表している。その他にも、空中サインとして使用可能な文字は筆記体など様々な書体であってもよく、空中サインは文字や記号以外の任意の図形が用いられてもよい。

10

20

【 0 0 2 2 】

また、空中サインによる認証の際に使用される登録サインデータは、登録変更により任意に変更可能である。すなわち、登録サインデータは、一例として、図 4 (a) に示すような「畠」と「中」の各文字が構成パーツとなされた登録サインを、図 4 (b) に示すように「一」と「成」の各文字や他の記号等のパーツで構成されたサインへ変更することが可能となされている。さらに、登録サインは、本実施形態の認証処理装置 1 を使用するシステムにおいて要求されるセキュリティレベルに応じて設定することができる。例えばセキュリティレベルが低い設定でよい場合には、例えば図 5 (a) に示すように手指が変更されずに簡単な記号を記入するサインを使用し、より高いセキュリティレベルを設定する場合には例えば図 5 (b) に示すように手指が変更されずに漢字等の複雑な複数の文字を記入するサインを使用することができる。さらに高いセキュリティレベルを設定する場合には、例えば図 5 (c) に示すようにそれぞれ異なる手指が用いられて漢字のような複雑な複数の文字を記入するサインを使用し、それよりも更に高いセキュリティレベルを設定する場合には、例えば図 5 (d) に示すようにそれぞれ異なる手指が用いられて複数の文字を重ねて記入するようなサインを使用することができる。言い換えると、本実施形態の場合、使用される手指や文字等の組み合わせの複雑さに応じて、様々なセキュリティレベルが設定可能となっている。セキュリティレベルは、例えば入出部屋などの登録対象場所ごとに要求されるセキュリティの度合いに応じて設定することができ、また、認証対象者ごとに設定されてもよい。

30

40

【 0 0 2 3 】

また本実施形態において、登録サインデータは、仮想ノートエリア 4 0 の三次元空間内において、登録対象者であるユーザ (以下、登録ユーザとする) が予め任意に決めた文字等を、同じく登録ユーザが予め任意に決めた手指を任意に変更しながら記入した際の空中サインから、前述同様に指認識と移動軌跡と移動時間及び移動速度の解析により得られて登録されたデータとなされている。また、本実施形態の場合、登録サインデータは、一例として、図 6 に示すように、登録ユーザが予め決めた文字等を予め決めた手指を用いて複数回記入した空中サインのデータのうち、類似度 $S L (1)$, $S L (2)$, $S L (3)$ がそれぞれ類似度閾値 $S L t$ よりも高い三つのデータ $s i g n _ a$, $s i g n _ b$, $s i g$

50

n__cを用いている。なお、三つのデータs i g n __ a , s i g n __ b , s i g n __ cのうち、何れかのデータの類似度S Lが類似度閾値S L tよりも低かった場合、登録ユーザに対して空中サインの再記入を求め、その再記入による空中サインのデータの類似度S Lが類似度閾値S L tより高くなった場合、その再記入によるデータを用いて、類似度S Lが低かったデータを上書きする。

【0024】

そして、本実施形態において、認証対象者2による空中サインデータと、登録サインデータの比較の際には、図7に示すように、認証対象者2による空中サインデータs i g n __ d a t a __ dと、三つの登録サインデータs i g n __ a , s i g n __ b , s i g n __ cとの間でそれぞれ類似度を計算する。それら空中サインデータs i g n __ d a t a __ dと、三つの登録サインデータs i g n __ a , s i g n __ b , s i g n __ cとの間でそれぞれ算出された類似度S Lが、類似度閾値S L tよりも高くなった数が二つ以上ある場合、認証対象者2は、登録サインデータの登録ユーザであると認証される。一方、それら空中サインデータs i g n __ d a t a __ dと、三つの登録サインデータs i g n __ a , s i g n __ b , s i g n __ cとの間でそれぞれ算出された類似度S Lが、類似度閾値S L t以下となった数が二つ以上ある場合、認証対象者2は、登録サインデータの登録ユーザでないと判定される。

【0025】

以下、情報処理装置10の構成と情報処理装置10にて行われる処理の詳細について説明する。図8には、情報処理装置10の構成を示す。図8の示した各構成は、本実施形態の情報処理装置10においてプログラムに基づいて行われる各処理や制御、実際のハードウェア構成をそれぞれ機能ごとに分けた機能ブロックとして表したものである。なお、図8には距離センサ20も描かれている。また、図8において、表示部(ディスプレイ11)は、情報処理装置10の外部に設けられていてもよい。メモリ部106内に記憶されている各種情報は、外部の記憶装置に格納されていてもよい。

【0026】

図9には、空中サインにより認証対象者2の個人認証を行う際の情報処理装置10の処理及び制御の流れをフローチャートにより示している。以下、図8の各構成の動作及び処理と制御について、図9のフローチャートを参照しながら説明する。

【0027】

まず、認証対象者2の個人認証が行われる際、制御部104の解析認証制御部142は、ステップS1の処理として、メモリ制御部144を通じて、メモリ部106のユーザ情報格納部151に格納されているユーザ情報を読み出してユーザ確認部105へ送る。そして、解析認証制御部142は、ユーザ確認部105を制御して、ユーザ確認部105にユーザ確認のための判定を行わせる。このときのユーザ確認部105は、認証対象者2が、予め登録されている複数ユーザのうちの一人名であるか否かを判定するユーザ確認処理を行う。ここで、予め登録されているユーザが一人のみである場合、ユーザ確認のための判定処理は省略されてもよい。予め登録されているユーザが複数である場合、例えば登録サインデータとは別に予め登録されているパスワード等を用いたユーザ確認や、予め各ユーザに配布している認証用カード等を用いたユーザ確認、或いは、各ユーザの生体情報等を用いたユーザ確認等を行うことができる。これらユーザ確認のための処理は既存の処理と同じであるため、その詳細な説明は省略する。なお、空中サインデータを用いた個人認証が行われる場合、情報処理装置10は、例えば認証対象者2に対してどのような手順で個人認証が行われるかを案内するナビゲートメッセージ等をディスプレイ11の画面上に表示したり、図示しないスピーカ等からナビゲート音声を出力したりしてもよい。

【0028】

ステップS1において、ユーザ確認部105にて認証対象者2が登録ユーザでないと判定されると、解析認証制御部142は、ステップS11の処理として、認証否定(NG)処理を行う。解析認証制御部142は、ステップS11の認証NG処理として、例えばそれ以前の処理で取得された情報を全てクリアした後、処理をステップS10へ進める。ス

10

20

30

40

50

ステップ S 1 0 の処理へ進むと、制御部 1 0 4 の表示制御部 1 4 1 は、ディスプレイ 1 1 の画面上に認証 N G 等の表示を行う。なお認証 N G の通知は音声により行われてもよい。

【 0 0 2 9 】

一方、ステップ S 1 において認証対象者 2 が登録ユーザであると判定された場合、解析認証制御部 1 4 2 は、ステップ S 2 の処理として、まず、距離センサ 2 0 から供給される信号に基づいて、当該距離センサ 2 0 のセンサ面 2 0 F の上空の三次元空間に、仮想二次元平面の一例である仮想ノートエリア 4 0 を設定する。さらに、解析認証制御部 1 4 2 は、ステップ S 2 において、距離センサ出力解析部 1 0 2 で行われる解析結果を基に、検出対象物として手 3 0 が前記仮想ノートエリア 4 0 の三次元空間内に存在しているか判断する。なお、仮想ノートエリア 4 0 は、三次元空間内に仮想的に設定されるものであり、認証対象者 2 や他の第三者が実際に見ることの出来るものではない。

10

【 0 0 3 0 】

ここで、距離センサ出力解析部 1 0 2 で行われる処理の詳細を述べる前に、距離センサ 2 0 の構成と当該距離センサ 2 0 から得られる信号について説明する。距離センサ 2 0 は、図 1 0 に示すように、センサ面 2 0 F の側に、例えば三つの赤外線 LED 2 2 L , 2 2 C , 2 2 R と、二つの赤外線カメラ 2 1 L , 2 1 R が配されて構成されている。赤外線 LED 2 2 L , 2 2 C , 2 2 R から出射された赤外光は、当該距離センサ 2 0 のセンサ面 2 0 F 側に何らかの検出対象物が存在していた場合、その検出対象物により反射されて、赤外線カメラ 2 1 L , 2 1 R へ入射する。赤外線カメラ 2 1 L , 2 1 R は、それぞれ撮像光学系と撮像素子を備えており、検出対象物にて反射された赤外光からなる光像を、所定の時間周期ごとに撮像する。なお、本実施形態の場合、所定の時間周期は、一例として 2 9 0 f p s (フレーム / 秒) のフレームレートとなされている。

20

【 0 0 3 1 】

なお、距離センサ 2 0 において、赤外線 LED 2 2 L , 2 2 C , 2 2 R から出射された赤外光が検出対象物で反射されて赤外線カメラ 2 1 L , 2 1 R が受光できる有効範囲は、例えば図 1 1 に示すように、センサ面 2 0 F 上での赤外線カメラ 2 1 L , 2 1 R の中間点 2 0 C から、例えば 2 5 m m ~ 6 0 0 m m までの距離範囲 D R 内で且つ広がり角 が 1 5 0 度の逆ピラミッド状の範囲となされている。上述した距離センサ 2 0 は、赤外線カメラ 2 1 L , 2 1 R の撮像信号を、情報処理装置 1 0 へ出力する。

【 0 0 3 2 】

距離センサ 2 0 から出力された撮像信号は、本実施形態の情報処理装置 1 0 の距離センサ出力受信部 1 0 1 により受信される。距離センサ出力受信部 1 0 1 は、距離センサ 2 0 と情報処理装置 1 0 との間を接続する信号ケーブル或いは無線等の通信方式に応じた受信部となっている。当該距離センサ出力受信部 1 0 1 にて受信された撮像信号は、距離センサ出力解析部 1 0 2 へ送られる。

30

【 0 0 3 3 】

距離センサ出力解析部 1 0 2 は、例えば、座標算出部 1 2 1 と対象認識部 1 2 2 と指識別情報取得部 1 2 3 と指先時系列座標取得部 1 2 4 と指先時系列速度取得部 1 2 5 と記入時間計測部 1 2 6 とを有して構成されている。座標算出部 1 2 1 は、距離センサ 2 0 の二つの赤外線カメラ 2 1 L , 2 1 R からの撮像信号の画像解析を行うことにより、図 1 1 及び図 1 2 に示すように、距離センサ 2 0 の前記有効範囲内の X 軸、Y 軸、Z 軸で表される三次元空間における検出対象物 (本実施形態の場合は手 3 0 及び各手指 3 1) の三次元座標を算出する。なお、距離センサ 2 0 から供給される撮像信号は前述のように 2 9 0 f p s のフレームレートの信号となされているため、座標算出部 1 2 1 は、フレームごとに手 3 0 及び手指 3 1 の三次元座標を算出する。なお、座標算出部 1 2 1 は、検出対象物が複数存在する場合であっても、或いは、一つの検出対象物内にそれぞれ異なる動きをする複数の部位が存在する場合であっても、それらについてそれぞれの三次元座標を算出する。

40

【 0 0 3 4 】

ここで、検出対象物である手 3 0 は、手掌と 5 本の手指 3 1 からなる物体、すなわち一つの検出対象物内にそれぞれ異なる動きをする複数の部位が存在する物体である。したが

50

って、座標算出部 1 2 1 は、手 3 0 を構成している手掌及び 5 本的手指 3 1 の三次元座標を算出する。座標算出部 1 2 1 にて算出されたフレームごとの三次元座標情報は、対象認識部 1 2 2 へ送られる。

【 0 0 3 5 】

対象認識部 1 2 2 は、前記フレームごとの撮像信号と三次元座標情報を基に、前記検出対象物がどのようなものであるかを認識する。ここで、距離センサ 2 0 の赤外線カメラにより、手掌及び 5 本的手指 3 1 からなる手 3 0 が撮像されている場合、対象認識部 1 2 2 は、前記撮像信号と前記座標算出部 1 2 1 でフレームごとに算出された三次元座標とから、前記検出対象物が手 3 0 であることを認識する。また、対象認識部 1 2 2 は、検出対象物である手 3 0 を構成する各部位、すなわち手掌と 5 本的手指 3 1、それら 5 本的手指 3 1 の指先、5 本的手指 3 1 の屈曲部である各関節等を認識する。このように、対象認識部 1 2 2 は、検出対象物が手 3 0 であることを認識すると、その対象認識結果と当該手掌と 5 本的手指 3 1 からなる手 3 0 の座標情報を解析認証制御部 1 4 2 へ送る。

【 0 0 3 6 】

以下、対象認識部 1 2 2 において、検出対象物が人の手 3 0 であること及び当該手 3 0 を構成する手掌と 5 本的手指 3 1 をどのように認識するかについて、図 1 3 を参照しながら説明する。なお、以下の説明は概念説明であり、本発明はこの例に限定されるものではない。

【 0 0 3 7 】

対象認識部 1 2 2 は、距離センサ 2 0 の赤外線カメラ 2 1 L, 2 1 R により人の手 3 0 が撮像された場合、その撮像信号と前記座標算出部 1 2 1 でフレームごとに算出された三次元座標とから、検出対象物は他の部位よりも広い面積を有する部位（手掌に相当する部位）と、その広い部位から伸びて且つそれぞれが個別に屈曲可能な 5 本の部位（5 本的手指に相当する部位）とからなることを認識する。

【 0 0 3 8 】

図 1 3 は、検出対象物として認識された手をモデル化して説明するための図である。図 1 3 の例では、検出対象物として認識された手掌部位を掌オブジェクト P としてモデル化し、5 本的手指部位をそれぞれ指オブジェクト F 0 ~ F 4 としてモデル化して表している。なお、指オブジェクト F 0 は親指に対応しており、以下同様、指オブジェクト F 1 は人差し指、指オブジェクト F 2 は中指、指オブジェクト F 3 は薬指、指オブジェクト F 4 は小指にそれぞれ対応している。また、図 1 3 の例では、各手指の関節を関節オブジェクト F 0 j ~ F 4 j としてモデル化し、各手指の指先を指先オブジェクト F 0 t ~ F 4 t としてモデル化し、それら各関節オブジェクトの間或いは指先オブジェクトから隣の関節オブジェクトまでの間をボーンオブジェクトとしてモデル化して表している。対象認識部 1 2 2 は、図 1 3 に示すようにモデル化できる各部位を有した検出対象物が三次元空間内に存在していることを認識し、さらにそれら各部位の三次元空間内における配置関係から、当該検出対象物が人の手であると認識する。

【 0 0 3 9 】

そして、制御部 1 0 4 の解析認証制御部 1 4 2 は、対象認識部 1 2 2 から、検出対象物として人の手 3 0 の認識結果を受け取ると、図 9 のステップ S 2 において、前記仮想ノートエリア 4 0 の三次元空間内で人の手 3 0 を検出したと判断し、処理をステップ S 3 へ進める。ステップ S 3 へ処理を進めると、解析認証制御部 1 4 2 は、距離センサ出力解析部 1 0 2 の指識別情報取得部 1 2 3 に対して、手 3 0 の各手指 3 1 を識別するための指識別情報を生成させる。

【 0 0 4 0 】

このときの指識別情報取得部 1 2 3 は、対象認識部 1 2 2 が認識した手 3 0 の各部位のうち、例えば図 1 3 の指オブジェクト F 0 ~ F 4 のようにモデル化できる各部位を、親指から小指までの手指部位としてそれぞれ個別に識別する。したがって、指識別情報取得部 1 2 3 は、手 3 0 から例えば一本だけ手指 3 1 が伸ばされ、他の四本的手指 3 1 が握られていた（折り曲げられていた）場合、その一本だけ伸ばされた手指 3 1 が、親指から小指

までの五本の手指のうちの何れの手指であることを識別可能である。また、指識別情報取得部 1 2 3 は、手 3 0 から伸ばされた手指 3 1 が変更されたか否かをも識別可能となされている。一例として、手 3 0 から伸ばされていた人差し指が折り曲げられた後、手 3 0 から別の手指（例えば親指）が出されたような場合には、手 3 0 から伸ばされた手指が切り替わったこと、さらにその切り替わった手指が親指であることをも識別可能である。そして、指識別情報取得部 1 2 3 は、上述のようにして手指 3 1 を認識した結果を表す指識別情報を生成して、演算認証処理部 1 0 3 へ送る。

【 0 0 4 1 】

次に、解析認証制御部 1 4 2 は、図 9 のステップ S 4 へ処理を進め、指先時系列座標取得部 1 2 4 を制御して、仮想ノートエリア 4 0 の三次元空間内で指先が移動した際の移動軌跡を表す時系列座標データを取得させる。すなわち、指先時系列座標取得部 1 2 4 は、前記指識別情報取得部 1 2 3 が識別した各手指部位のうち、例えば図 1 3 の指先オブジェクト F 0 t ~ F 4 t のようにモデル化できる指先部位が、仮想ノートエリア 4 0 の三次元空間内を移動した際の時系列座標データを取得する。したがって、指先時系列座標取得部 1 2 4 は、手 3 0 から例えば一本だけ手指 3 1 が伸ばされ、他の四本の手指 3 1 が折り曲げられていた場合には、その一本だけ伸ばされた手指 3 1 の指先が移動した際の時系列座標データを取得する。また、指先時系列座標取得部 1 2 4 は、手 3 0 から伸ばされた手指 3 1 が変更された場合には、その変更された手指 3 1 の指先が移動した際の時系列座標データをも取得する。なお、時系列座標データは、前述した距離センサ 2 0 が検出するフレームごとに対応した時系列の情報である。指先時系列座標取得部 1 2 4 にて取得された各指先部位の時系列座標データは、演算認証処理部 1 0 3 へ送られる。

10

20

【 0 0 4 2 】

また、解析認証制御部 1 4 2 は、図 9 のステップ S 4 の処理として、指先時系列速度取得部 1 2 5 を制御して、仮想ノートエリア 4 0 の三次元空間内で指先が移動した際の移動速度を表す時系列速度データを取得させる。すなわち、指先時系列速度取得部 1 2 5 は、前記指識別情報取得部 1 2 3 が識別した各手指部位のうち、図 1 3 の指先オブジェクト F 0 t ~ F 4 t でモデル化された指先部位が、仮想ノートエリア 4 0 の三次元空間内を移動した際の時系列速度データを取得する。したがって、指先時系列速度取得部 1 2 5 は、手 3 0 から例えば一本だけ手指 3 1 が伸ばされ、他の四本の手指 3 1 が折り曲げられていた場合には、その一本だけ伸ばされた手指 3 1 の指先が移動した際の時系列速度データを取得する。また、指先時系列速度取得部 1 2 5 は、手 3 0 から伸ばされた手指 3 1 が変更された場合には、その変更された手指 3 1 の指先が移動した際の時系列座標データをも取得する。時系列速度データは、前述した距離センサ 2 0 が検出するフレームごとに対応した時系列の情報である。指先時系列速度取得部 1 2 5 にて取得された各指先部位の時系列速度データ、演算認証処理部 1 0 3 へ送られる。

30

【 0 0 4 3 】

また、解析認証制御部 1 4 2 は、図 9 のステップ S 4 の処理として、記入時間計測部 1 2 6 を制御して、仮想ノートエリア 4 0 の三次元空間内で指先が移動して空中サインを記入していた時間を計測させる。すなわち、記入時間計測部 1 2 6 は、前記指識別情報取得部 1 2 3 が識別した各手指部位のうち、図 1 3 の指先オブジェクト F 0 t ~ F 4 t でモデル化された各指先部位が、仮想ノートエリア 4 0 の三次元空間内を移動していた時間を計測する。前述同様に、記入時間計測部 1 2 6 は、手 3 0 から一本だけ手指 3 1 が伸ばされている場合や、その手指 3 1 が別の手指 3 1 に変更された場合にも、時間を計測する。記入時間計測部 1 2 6 が計測した記入時間データは、演算認証処理部 1 0 3 へ送られる。

40

【 0 0 4 4 】

演算認証処理部 1 0 3 は、空中サインに用いられている手指の指識別情報と時系列座標データと時系列速度データと記入時間データとに基づいて空中サインデータを算出する演算手段と、その算出された空中サインデータと登録サインデータとを比較して認証判定を行う認証判定手段としての機能を含んでいる。

【 0 0 4 5 】

50

解析認証制御部 142 は、図 9 のステップ S5 へ処理を進め、演算認証処理部 103 の記入完了判定部 131 を制御して、空中サインの記入が完了したか判定させる。すなわち、記入完了判定部 131 は、前述した記入時間データと時系列座標データ、時系列速度データを参照して、仮想ノートエリア 40 の三次元空間内で指先の移動が止まり、その指先が予め決められた所定時間以上静止した場合に、空中サインの記入が完了したと判定する。記入完了判定部 131 は、空中サインの記入が完了したと判定した場合、記入完了通知を制御部 104 の解析認証制御部 142 へ送る。解析認証制御部 142 は、記入完了判定部 131 から記入完了通知が送られてこない間はステップ S3 へ処理を戻し、ステップ S3 とステップ S4 の処理を続けさせる。したがって、例えば前述のように手指 31 が変更されて空中サインのための記入が行われている場合も、ステップ S5 において空中サインの記入が完了するまでは、ステップ S3 とステップ S4 の処理は続けられることになる。解析認証制御部 142 は、空中サインの記入完了通知を受けると、ステップ S6 へ処理を進める。

10

【0046】

ステップ S6 の処理に進むと、解析認証制御部 142 は、メモリ制御部 144 を介してメモリ部 106 の登録サインデータ格納部 152 から登録サインデータを読み出させて、演算認証処理部 103 の DP マatching 算出部 132 へ送る。そして、解析認証制御部 142 は、DP マatching 算出部 132 を制御して、DP (Dynamic Programming: 動的計画法) マatching によるパターンマatching を行わせる。この場合の DP マatching 算出部 132 は、前述の時系列座標データと時系列速度データと指識別情報を含む空中サインデータと、登録サインデータ格納部 152 に格納されていた時系列座標データと時系列速度データと指識別情報を含む登録サインデータとを、DP マatching を用いたパターンマatching により比較して、それら空中サインデータと登録サインデータの二つの時系列パターン間の最適マatching を算出する。なおこのとき、時系列パターンの過適合への対処として、式 (1) に示すように、最適経路の移動回数 $Path_all$ のうち、ギャップとなる経路数 $Path_gap$ の割合を、最適距離 D_dp に乗じたものを、時系列パターン間の距離 D とする。

20

【0047】

$$D = (Path_gap / Path_all) D_dp \quad \dots \text{式 (1)}$$

30

【0048】

次に、解析認証制御部 142 は、ステップ S7 の処理として、演算認証処理部 103 のスコア算出部 133 を制御して、DP マatching により算出されたパターン間の距離 D をスコア化させる。この場合のスコア算出部 133 は、DP マatching により算出されたパターン間の距離 D を、所定のスコア変換パラメータ Cp を用いた式 (2) の演算によりスコア化する。なお、スコア化を行うのは、パターン間の距離のみによる分布と比較した場合、スコアによる分布を用いた方が、登録ユーザ本人による空中サインの時系列パターンを、誤って認証拒否してしまう可能性を低くすることができるためである。記入時間データについては、後述する図 16 に示すように、記入時間の差に相当するフレーム数の差を距離 D とし、その後、式 (2) によりスコア化する。

40

【0049】

$$SC = \exp(-D^2 / 2 Cp^2) \quad \dots \text{式 (2)}$$

【0050】

次に、解析認証制御部 142 は、ステップ S8 の処理として、サイン判定部 134 を制御して、空中サインデータと登録サインデータ的一致判定を行わせる。この場合のサイン判定部 134 は、スコアの総積を類似度 SL とし、その類似度 SL と類似度閾値 SLt とを比較する。すなわち、サイン判定部 134 は、スコア算出部 133 によりそれぞれスコア化された x 座標データ ($score_point_x$)、 y 座標データ ($score_point_y$)、 x 軸方向の速度データ ($score_velocity_x$)、 y 軸方向の速度データ ($score_velocity_y$)、記入時間データ ($score_length$)、指識別情報 ($score_finger$) を用いた式 (3)

50

の演算により類似度 S_L を算出し、その類似度 S_L を類似度閾値 S_{L_t} と比較する。

【0051】

$$S_L = (\text{score_point_x}) \times (\text{score_point_y}) \times (\text{score_velocity_x}) \\ \times (\text{score_velocity_y}) \times (\text{score_length}) \times (\text{score_finger}) \quad \dots \text{式(3)}$$

【0052】

そして、前述した三つの登録サインデータのうち二つ以上に対して、類似度 S_L が類似度閾値 S_{L_t} 以下であるとき、サイン判定部 134 は、空中サインデータが登録サインデータと一致しないことを示す通知を解析認証制御部 142 へ送る。この通知を受けると、解析認証制御部 142 は、前述したステップ S11 のように、認証否定 (NG) 処理を行う。

【0053】

一方、前述した三つの登録サインデータのうち二つ以上に対して、類似度 S_L が類似度閾値 S_{L_t} より大きいとき場合、サイン判定部 134 は、空中サインデータが登録サインデータと略々一致していること示す通知を解析認証制御部 142 へ送る。この通知を受けて解析認証制御部 142 は、ステップ S9 へ処理を進める。ステップ S9 に進むと、解析認証制御部 142 は認証 OK とし、このときの表示制御部 141 は、ディスプレイ 11 の画面上に認証 OK 等の表示を行う。なお、認証 OK の通知は音声により行われてもよい。

【0054】

なお、本実施形態の認証処理装置 1 が例えば入室時の認証を行うための装置であり、認証結果に応じて図示しない電気錠の開閉を制御する場合、解錠制御部 143 は、ステップ S10 において、解析認証制御部 142 による認証結果に基づいて電気錠の開閉を制御する。すなわち、認証対象者が正規の登録ユーザである場合、解錠制御部 143 は、ステップ S10 において、電気錠を開制御して当該認証対象者 2 の入室を可能にする。このステップ S10 の後、制御部 104 は、図 9 のフローチャートの処理を終了する。

【0055】

図 14 には、予め決めた登録サインデータにおける指先移動軌跡の時系列座標データと、登録ユーザ本人による空中サインデータにおける指先移動軌跡の時系列座標データと、他人による空中サインデータにおける指先移動軌跡の時系列座標データの一例を示している。図 15 には、登録サインデータにおける指先移動速度の時系列速度データと、登録ユーザ本人による空中サインデータにおける指先移動速度の時系列速度データと、他人による空中サインデータにおける指先移動速度の時系列速度データの一例を示している。また、図 16 には、図 15 の時系列速度データ上に、記入時間の差に相当するフレーム数の差を表した例を示している。これら図 14 から図 16 の例によれば、登録ユーザ本人による空中サインデータと登録サインデータとの間のスコアポイント (score_point) は「1」に近い値となる一方で、他人による空中サインデータと登録サインデータとの間のスコアポイントは「0」に近い値となる。また、図 17 には、登録サインデータとなされている三つのデータ $sign_a$, $sign_b$, $sign_c$ と、登録ユーザではない他人による空中サインデータと間の具体的な座標、速度、記入時間の各データと類似度の値を示している。これら図 14 ~ 図 17 から判るように、本実施形態によれば、登録ユーザ本人による空中サインの時系列パターンを、他人によるものとして誤って認証拒否してしまう可能性は非常に低く、また、他人を誤って認証してしまうこともない。また、本実施形態によれば、複数人の登録ユーザ本人が例えば 2 週間ごとに空中サインを行って個人認証の経日変化を観察した場合も、全員を登録ユーザ本人であると認証可能となっている。

【0056】

また、前述の説明では、認証対象者となっているユーザの個人認証が行われる例を主に説明したが、本実施形態の情報処理装置 10 は、登録対象者のユーザがサインを登録する際にも使用可能である。前述のような登録サインデータは、一例として、予め図 8 の情報処理装置 10 において前述同様にして作成したサインデータを、メモリ部 106 の登録サインデータ格納部 152 に格納したものであってもよいし、別の情報処理装置 10 を用い

10

20

30

40

50

て作成されたものであってもよい。すなわち、本実施形態の情報処理装置 10 は、空中サインデータを登録サインデータとして登録する認証情報登録装置としての機能も備えている。また、制御部 104 は、空中サインデータを登録サインデータとして登録する登録手段としての機能も備えている。なお、登録サインデータは、メモリ部 106 だけでなく、他の様々な記録媒体に記録されてもよい。そして、登録サインデータは、複数の登録対象者ごとに設定されてもよく、また、セキュリティレベルに応じて設定されてもよい。

【0057】

以上説明したように、本実施形態によれば、三次元空間上に仮想的に配置した仮想ノートエリア 40 内において、例えば手指を変更しながら空中サインが行われ、その空中サインデータと登録サインデータとを比較して個人認証が行われるため、覗き見等によるサインの漏洩を無くすることができ、また認証用センサ等に触れることなく、非常に高いセキュリティ性を確保した個人認証が可能となっている。特に、本実施形態の場合、手指を替えながら空中サインが行われるため、空中サインが覗き見されたとしても、他の者がその空中サイン時の記入軌跡を再現することは不可能である。さらに、本実施形態の場合、照明環境によらずに空中サインによる認証が可能である。また、本実施形態によれば、必要とされるセキュリティレベルに応じた設定が可能である。

10

【0058】

< その他の実施形態 >

本実施形態の認証処理装置 1 は、例えば銀行 ATM や研究所等のような高度なセキュリティ管理が必要とされるシステムに適用可能である。図 18 には、本実施形態の個人認証が適用され、サーバによりセキュリティ管理がなされるシステムの概略的な構成例を示している。

20

【0059】

図 18 のセキュリティシステムにおいて、サーバ 300 は、大別してシステム情報蓄積部 301、システム制御部 302、ネットワーク I/F 部 303 を有して構成されている。ネットワーク I/F 部 303 は、ネットワーク 304 を介して、サーバ 300 によりセキュリティ管理がなされる端末 310 との間で通信可能となされている。各端末 310 には前述した距離センサ 20 が併設されている。システム制御部 302 は、このセキュリティシステム全体を制御し、また、ネットワーク 304 を通じて接続されている端末 310 との間で送受信される情報の管理等を行う。

30

【0060】

サーバ 300 内のシステム情報蓄積部 301 は、システム全体を管理するための様々な情報とともに、このセキュリティシステムに登録されている全てのユーザの前記ユーザ情報と全ユーザの登録サインデータとを蓄積している。このセキュリティシステムの場合、各端末 310 は、全ユーザの登録サインデータ等を内部に保持しておらず、認証対象者 2 の個人認証が行われる際に当該認証に必要な情報のみを、ネットワーク 304 を介してサーバ 300 から取得する。そして端末 310 は、距離センサ 20 の出力信号に対して前述の距離センサ出力解析部 102 と同様の解析のみを行い、サーバ 300 は、その解析情報を用いて前述の演算認証処理部 103 及び解析認証制御部 142 と同様にして認証対象者 2 の個人認証を行う。そして、認証対象者が正規の登録ユーザであると判定したとき、サーバ 300 は、その認証対象者 2 に対して、例えば銀行 ATM を使用した入出金等の操作を許可したり、室内への出入りを許可（解錠等）したりする。

40

【0061】

なお、前述した情報処理装置 10 のように端末 310 が個人認証まで行う場合、前述のステップ S1 にて認証対象者 2 が登録ユーザであると確認できたとき、当該端末 310 は、サーバ 300 に蓄積されている全ての登録ユーザの登録サインデータの中で、ステップ S1 で確認したユーザ用に登録されている登録サインデータのみをサーバ 300 から受け取る。そして、認証対象者 2 が正規の登録ユーザであると端末 310 で判定されたとき、サーバ 300 は、その認証対象者 2 に対して、例えば銀行 ATM を使用した入出金等の操作や室内への出入りを許可（解錠等）する。

50

【 0 0 6 2 】

その他、本発明は、以下の処理を実行することによっても実現される。すなわち、上述した実施形態の機能を実現するソフトウェア（プログラム）を、ネットワーク又は各種記録媒体を介してシステム或いは装置に供給し、そのシステム或いは装置のコンピュータ（又はCPUやMPU等）がプログラムを読み出して実行する処理である。このプログラム及び当該プログラムを記憶したコンピュータ読み取り可能な記録媒体は、本発明に含まれる。

【 0 0 6 3 】

なお、上述した本発明の実施形態は、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。すなわち、本発明はその技術思想、又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。

10

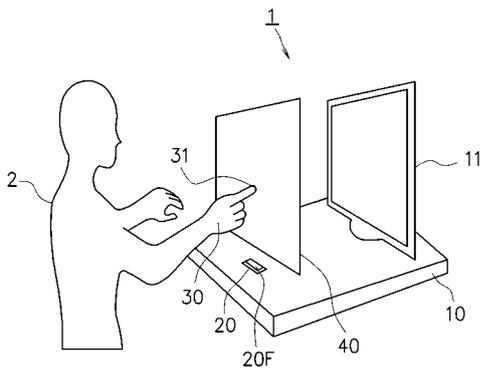
【 符号の説明 】

【 0 0 6 4 】

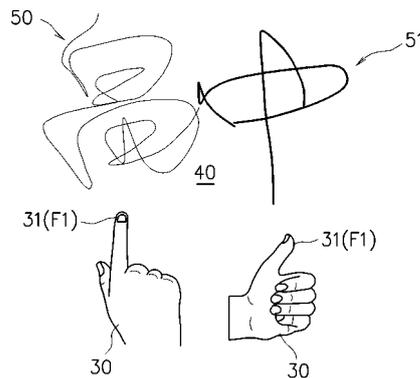
1：認証処理装置、10：情報処理装置、11：ディスプレイ、20：距離センサ、20F：センサ面、30：手、31：手指、40：仮想ノートエリア、101：距離センサ出力受信部、102：距離センサ出力解析部、103：演算認証処理部、104：制御部、105：ユーザ確認部、106：メモリ部、121：座標算出部、122：対象認識部、123：指識別情報取得部、124：指先時系列座標取得部、125：指先時系列速度取得部、126：記入時間計測部、131：記入完了判定部、132：DPマッチング算出部、133：スコア算出部、134：サイン判定部、141：表示制御部、142：解析認証制御部、143：解錠制御部、144：メモリ制御部、151：ユーザ情報格納部、152：登録サインデータ格納部

20

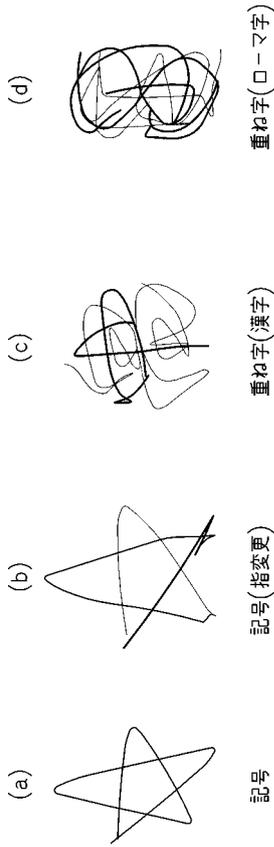
【 図 1 】



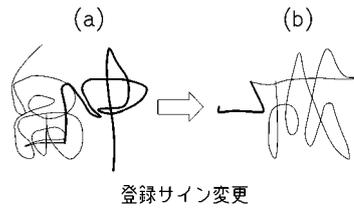
【 図 2 】



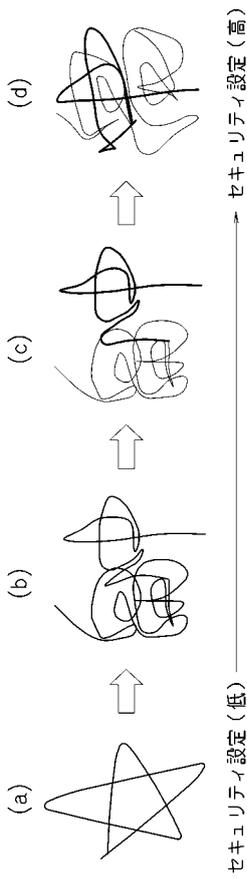
【 図 3 】



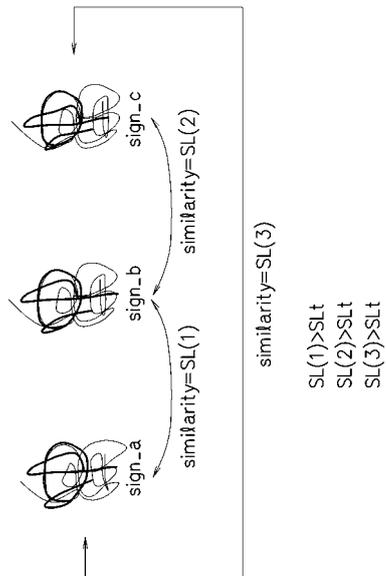
【 図 4 】



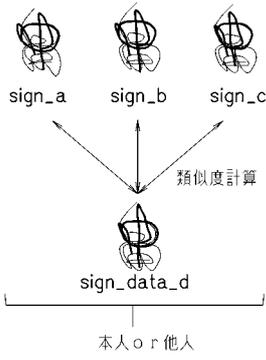
【 図 5 】



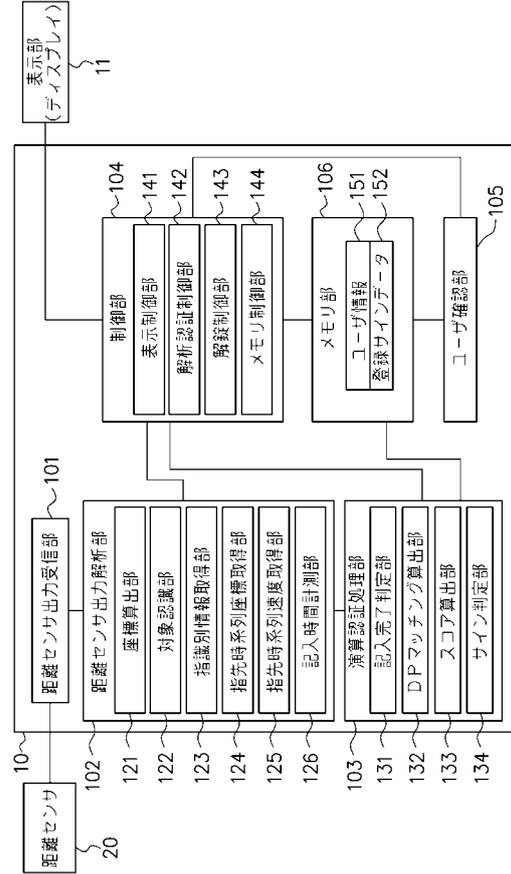
【 図 6 】



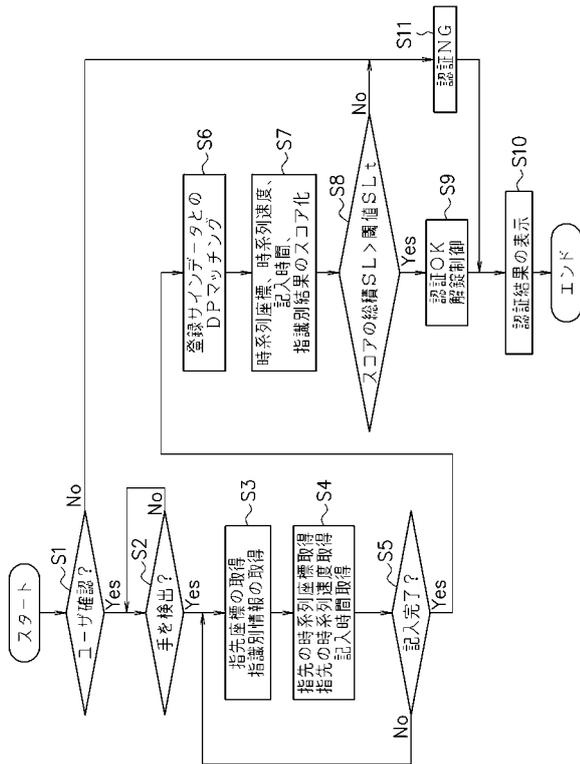
【 図 7 】



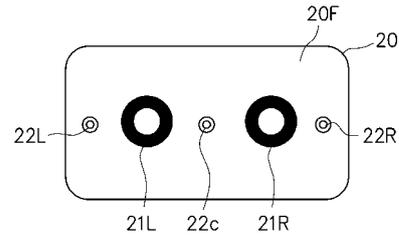
【 図 8 】



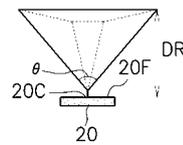
【 図 9 】



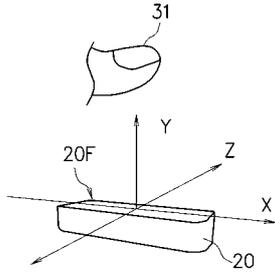
【 図 10 】



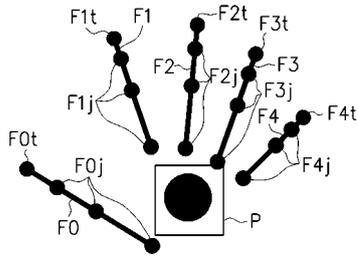
【 図 11 】



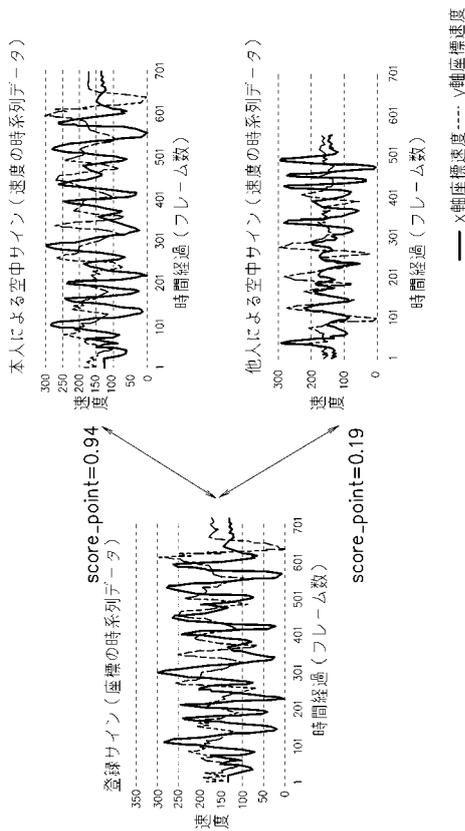
【図 1 2】



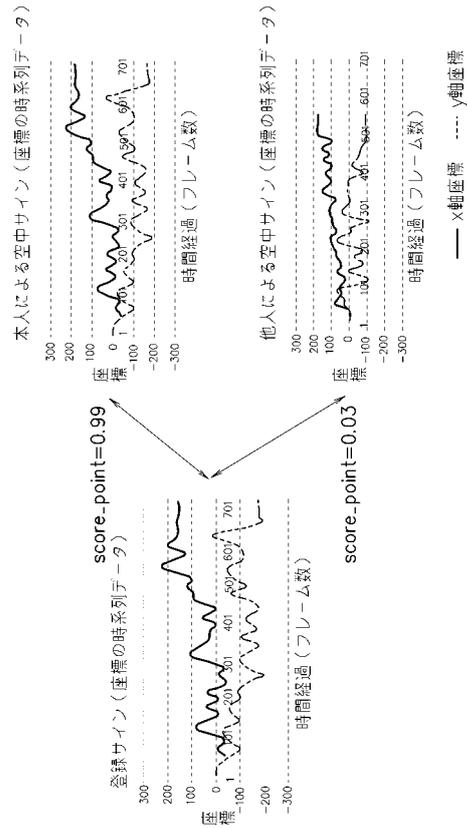
【図 1 3】



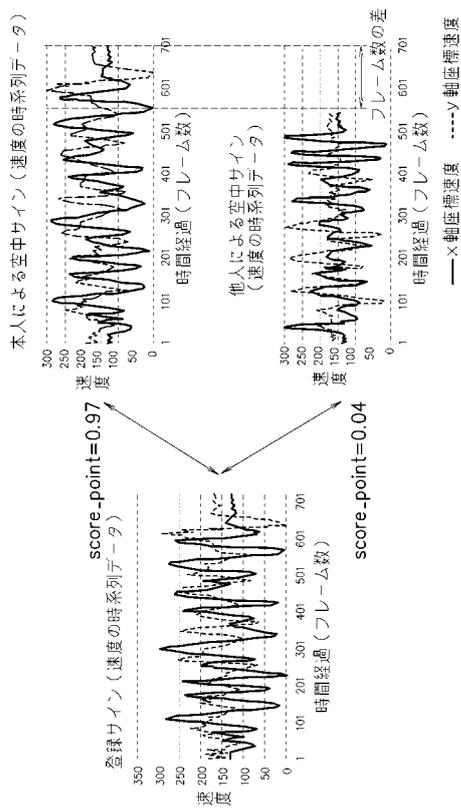
【図 1 5】



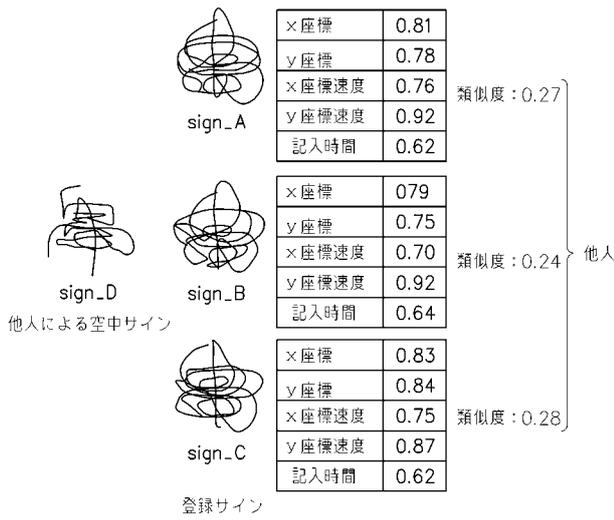
【図 1 4】



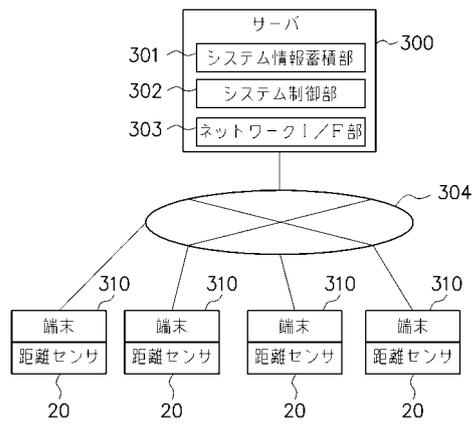
【図 1 6】



【 図 1 7 】



【 図 1 8 】



フロントページの続き

(72)発明者 畠中 一成

鹿児島県鹿児島市郡元一丁目2番24号 国立大学法人 鹿児島大学内

Fターム(参考) 5B043 AA01 AA09 BA06 CA03 CA10 DA05 FA03 FA07 FA08 FA09

GA05 GA13

5B087 AA07 AA09 AB02 BC12 BC13 BC16 BC32 DD03