(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2009-64344
(P2009-64344A)
(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	510B	5B043
G06T	1/00	(2006.01)	G06T	1/00	500A	5B057

審査請求 未請求　請求項の数 5　OL　（全 12 頁）

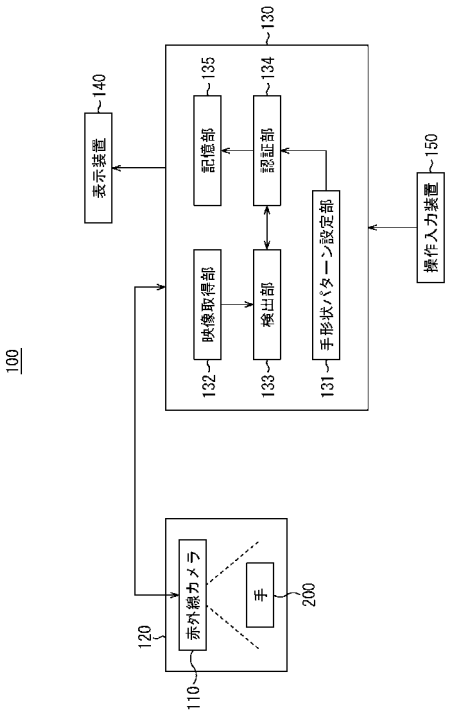
(21)出願番号　特願2007-233169 (P2007-233169)
(22)出願日　平成19年9月7日 (2007.9.7)

(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　大野　敬弘
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】セキュリティ認証システム及びセキュリティ認証方法

(57)【要約】
【課題】セキュリティ認証システムを導入し易くすると共に、非接触で、且つ、セキュリティ性の確保を実現できるようにする。
【解決手段】セキュリティ認証システム１００において、手２００の撮影を行う赤外線カメラ１１０と、赤外線カメラ１１０において撮影される手２００の１又は複数の手形状からなる手形状パターンをセキュリティキーとして認証処理を行う認証部１３４を備えるようにする。このように、赤外線カメラ１１０を用いた手２００の撮影による認証を行うことにより、その導入コストが安価なものとなってセキュリティ認証システムの導入がし易くなると共に、非接触で、且つ、セキュリティ性の確保が実現できる。
【選択図】図２



【特許請求の範囲】
【請求項１】
手の撮影を行う赤外線カメラと、
前記赤外線カメラにおいて撮影される手の１又は複数の手形状からなる手形状パターンをセキュリティキーとして認証処理を行う認証部と
を有することを特徴とするセキュリティ認証システム。
【請求項２】
前記手形状パターンの設定を行う手形状パターン設定部と、
前記赤外線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手形状を検出する検出部と
を更に有し、
前記認証部は、前記手形状パターン設定部で設定された前記手形状パターンの手形状と、前記検出部で検出された手形状との照合の結果に基づいて、前記認証処理を行うことを特徴とする請求項１に記載のセキュリティ認証システム。
【請求項３】
前記手形状パターンが複数の手形状から構成されている場合、
前記認証部は、前記手形状パターンの各手形状ごとに、順次、前記検出部で検出された手形状との照合を行って、前記認証処理を行うことを特徴とする請求項２に記載のセキュリティ認証システム。
【請求項４】
前記赤外線カメラは、暗箱内に設置されており、当該暗箱内に挿入された手の撮影を行うことを特徴とする請求項１乃至３のいずれか１項に記載のセキュリティ認証システム。
【請求項５】
手の撮影を行う赤外線カメラを有するセキュリティ認証システムにおけるセキュリティ認証方法であって、
前記赤外線カメラにおいて撮影される手の１又は複数の手形状からなる手形状パターンをセキュリティキーとして認証処理を行うことを特徴とするセキュリティ認証方法。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、セキュリティの認証を行うセキュリティ認証システム及びセキュリティ認証方法に関するものである。
【背景技術】
【０００２】
現在、銀行の現金自動預け払い機（ＡＴＭ：Automated Teller Machine）などでは、セキュリティキーとして暗証番号が用いられ、例えば、４桁の数字が利用されている。その一方で、カードの偽造や暗証番号入力時の盗撮などによる犯罪は、後を絶たないのが現状である。
【０００３】
このような背景のもと、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バイオメトリック情報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）。
【０００４】
【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】
【０００５】
しかしながら、上述したバイオメトリック情報をセキュリティキーとするセキュリティ認証システムでは、その導入コストがかなりの高額となり、容易に導入することが難しい

という問題があった。

【０００６】

また、上述したバイオメトリック情報をセキュリティキーとするセキュリティ認証システムでは、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。

【０００７】

本発明は上述の問題点に鑑みてなされたものであり、セキュリティ認証システムを導入し易くすると共に、非接触で、且つ、セキュリティ性の確保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】

【０００８】

本発明のセキュリティ認証システムは、手の撮影を行う赤外線カメラと、前記赤外線カメラにおいて撮影される手の１又は複数の手形状からなる手形状パターンをセキュリティキーとして認証処理を行う認証部とを有する。

【０００９】

本発明のセキュリティ認証方法は、手の撮影を行う赤外線カメラを有するセキュリティ認証システムにおけるセキュリティ認証方法であって、前記赤外線カメラにおいて撮影される手の１又は複数の手形状からなる手形状パターンをセキュリティキーとして認証処理を行う。

【発明の効果】

【００１０】

本発明によれば、セキュリティ認証システムが導入し易くなると共に、非接触で、且つ、セキュリティ性の確保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】

【００１１】

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。

【００１２】

図１は、本発明の実施形態に係るセキュリティ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、セキュリティ認証システム１００は、赤外線カメラ１１０と、暗箱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。

【００１３】

赤外線カメラ１１０は、黒色の暗箱１２０内に設置されており、情報処理装置１３０による制御に基づいて、当該暗箱１２０内に挿入された手２００の撮影を行うものである。ここで、赤外線カメラ１１０は、例えば、暗箱１２０の第１の面１２１に備え付けられている。また、暗箱１２０には、例えば、第２の面１２２に、認証を行う人間の手２００を挿入するための挿入口１２２ａが設けられている。

【００１４】

情報処理装置１３０は、セキュリティ認証システム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、赤外線カメラ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セキュリティ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、手形状パターン設定部１３１、映像取得部１３２、検出部１３３、認証部１３４、及び、記憶部１３５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１３１～１３４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１３５が備えられるものとする。
【００１９】
手形状パターン設定部１３１は、手の１又は複数の手形状からなる手形状パターンを設定する処理を行う。具体的に、手形状パターン設定部１３１は、操作者から操作入力装置１５０を介して入力された手形状パターンに係る情報に基づいて、手形状パターンを設定する処理を行う。
【００２０】
映像取得部１３２は、赤外線カメラ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１３２は、赤外線カメラ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。
【００２１】
検出部１３３は、映像取得部１３２で取得した手２００の映像に基づいて当該手２００の手形状を検出する処理を行う。本実施形態では、検出部１３３は、まず、映像取得部１３２で取得した映像中に手２００が存在するか否かを検出し、当該映像中に手２００が存在する場合に、続いて、当該手２００の手形状を検出する。以下に、検出部１３３による手形状の検出処理について、詳しく説明する。
【００２２】
図３は、検出部１３３による手形状の検出処理を説明するための図である。
図３において、図３（ａ）は、暗箱１２０内で赤外線カメラ１１０により撮影された手２００の映像の一例を示す写真である。この図３（ａ）に示す映像は、映像取得部１３２において取得される。また、図３（ｂ）は、例えば、図３（ａ）に示す映像をデジタル的に処理し、且つ、手２００の部分をピックアップしたピックアップ映像を示している。
【００２３】
検出部１３３は、赤外線カメラ１１０により撮影され、映像取得部１３２で取得した映像に対して、手（指）の開き・閉じ状態や、何本の指が出ているか、どの指が出ているかなどを認識判定することにより、手２００の手形状の検出処理を行う。図３に示す例では、検出部１３３は、手（指）は開いており、３本の指が出ており、具体的に、親指（１）、人差し指（２）及び小指（５）が出ていると認識判定をして、手２００の手形状を検出する。
【００２４】
認証部１３４は、赤外線カメラ１１０において撮影される手２００の１又は複数の手形状からなる手形状パターンをセキュリティキーとして認証処理を行う。具体的に、認証部１３４は、手形状パターン設定部１３１で設定された手形状パターンの手形状と、検出部１３３で検出された手形状との照合の結果に基づいて、認証処理を行う。また、認証部１３４は、手形状パターン設定部１３１で設定された手形状パターンが複数の手形状から構成されている場合、当該手形状パターンの各手形状ごとに、順次、検出部１３３で検出された手形状との照合を行って、認証処理を行う。そして、認証部１３４は、認証処理の結果を認証処理結果情報として、記憶部１３５に記憶する。
【００２５】
その後、必要に応じて、情報処理装置１３０は、記憶部１３５に記憶されている認証処理結果情報を表示装置１４０に表示する。また、情報処理装置１３０は、必要に応じて、

例えば、記憶部１３５に記憶されている認証処理結果情報を、ネットワーク（不図示）を介して外部装置に送信する。

【００２６】

次に、セキュリティ認証システム１００におけるセキュリティ認証方法の処理手順について説明する。

【００２７】

図４は、本発明の実施形態に係るセキュリティ認証システムにおけるセキュリティ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４に示すフローチャートにおいては、赤外線カメラ１１０による撮影が継続的に行われており、映像取得部１３２は、赤外線カメラ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。

【００２８】

まず、セキュリティ管理者（操作者）から操作入力装置１５０を介して情報処理装置１３０に手形状パターンに係る情報が入力されると、図４のステップＳ１において、手形状パターン設定部１３１は、入力された手形状パターンに係る情報に基づいて、セキュリティキーとなる手形状パターンを設定する処理を行う。以下に、手形状パターン設定部１３１による手形状パターンの設定処理について、詳しく説明する。

【００２９】

図５は、手形状パターン設定部１３１による手形状パターンの設定処理を説明するための図である。

図５に示す例では、セキュリティ管理者（操作者）から、第１段階の認証処理に用いる手形状を「パー」、第２段階の認証処理に用いる手形状を「グー」、第３段階の認証処理に用いる手形状を「チョキ」、第４段階の認証処理に用いる手形状を「グー」とする合計４つの手形状からなる手形状パターンに係る情報が入力され、手形状パターン設定部１３１において当該手形状パターンが設定された場合を示している。この際、手形状パターン設定部１３１は、第１段階の認証処理に用いる手形状～第４段階の認証処理に用いる手形状に対して、それぞれ、認証処理を行う順番を示す手形状番号１～４を設定する。

【００３０】

具体的に、ステップＳ１において、手形状パターン設定部１３１は、図５に示すような手形状パターンの設定処理を行うと共に、当該手形状パターンの手形状の数Ｎを設定する。例えば、図５に示す例では、手形状の数Ｎとして４が設定される。

【００３１】

なお、図５に示す例では、４つの手形状からなる手形状の変化を表す手形状パターンが示されているが、本実施形態においては、必ずしも４つの手形状からなる必要は無い。例えば、２つや３つの手形状からなるもの、更には、５つ以上の手形状からなるもの、或いは、１つの手形状からなるものであっても適用可能である。

【００３２】

続いて、ステップＳ２において、認証部１３４は、検出部１３３が映像取得部１３２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、検出部１３３が映像取得部１３２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１３３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Ｓ２で待機する。

【００３３】

一方、ステップＳ２の判断の結果、検出部１３３が映像取得部１３２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、ステップＳ３に進む。ステップＳ３に進むと、認証部１３４は、暗箱１２０内に、認証を行う人間の手２００が挿入されたと判断し、認証処理を開始する。

【００３４】

認証処理が開始されると、まず、ステップＳ４において、認証部１３４は、ステップＳ１でセキュリティキーとして設定された手形状パターンの手形状のうち、認証対象の手形状番号を示す変数ｎを１に設定する。これにより認証対象の手形状番号ｎが設定される。

ここでは、例えば、図５に示す例では、手形状番号１の「パー」の手形状が認証対象の手形状として設定されることになる。

【００３５】

続いて、ステップＳ５において、検出部１３３は、手２００の手形状を検出する。この際、検出部１３３は、上述したように、手（指）の開き・閉じ状態や、何本の指が出ているか、どの指が出ているかなどを認識判定することにより、手２００の手形状の検出処理を行う。

【００３６】

続いて、ステップＳ６において、認証部１３４は、ステップＳ５で検出された手２００の手形状が、ステップＳ１で設定された手形状パターンにおける手形状番号ｎの手形状と合致するか否かを判断する。この判断の結果、ステップＳ５で検出された手２００の手形状が手形状パターンにおける手形状番号ｎの手形状と合致する場合には、ステップＳ７に進む。

【００３７】

ステップＳ７に進むと、認証部１３４は、認証対象の手形状番号を示す変数ｎが、ステップＳ１で設定された手形状パターンの手形状の数Ｎより小さいか否かを判断する。この判断の結果、認証対象の手形状番号を示す変数ｎがステップＳ１で設定された手形状パターンの手形状の数Ｎより小さい場合には、ステップＳ１で設定された手形状パターンの全ての手形状については認証処理が行われていないと判断し、ステップＳ８に進む。

【００３８】

ステップＳ８に進むと、認証部１３４は、認証対象の手形状番号を示す変数ｎに１を加算して、認証対象の手形状番号を示す変数ｎを変更する。続いて、ステップＳ９において、検出部１３３は、映像取得部１３２で取得した映像中の手２００の手形状が変化したか否かを判断する。この判断の結果、映像取得部１３２で取得した映像中の手２００の手形状が変化していない場合には、映像中の手２００の手形状が変化するまで、ステップＳ９で待機する。

【００３９】

一方、ステップＳ９の判断の結果、映像取得部１３２で取得した映像中の手２００の手形状が変化した場合には、ステップＳ５に戻る。そして、変更した手形状番号ｎに対して、ステップＳ５以降の処理を再度行う。即ち、図４のフローチャートでは、ステップＳ５～ステップＳ９の処理は、最大で、ステップＳ１で設定された手形状パターンの手形状の数（Ｎ）分、繰り返し行われることになる。

【００４０】

また、ステップＳ６の判断の結果、ステップＳ５で検出された手２００の手形状が手形状パターンにおける手形状番号ｎの手形状と合致しない場合には、ステップＳ１０に進む。ステップＳ１０に進むと、認証部１３４は、手形状が合致しなかったことから、認証ＮＧとする処理を行う。その後、認証部１３４は、認証ＮＧの結果を認証処理結果情報として、記憶部１３５に記憶する。

【００４１】

また、ステップＳ７の判断の結果、認証対象の手形状番号を示す変数ｎがステップＳ１で設定された手形状パターンの手形状の数Ｎより小さくない（即ち、以上である）場合には、ステップＳ１で設定された手形状パターンの全ての手形状について認証処理を行ったと判断し、ステップＳ１１に進む。ステップＳ１１に進むと、認証部１３４は、ステップＳ１で設定された手形状パターンの全ての手形状と合致したことから、認証ＯＫとする処理を行う。その後、認証部１３４は、認証ＯＫの結果を認証処理結果情報として、記憶部１３５に記憶する。

【００４２】

ステップＳ１０の処理が終了した場合、或いは、ステップＳ１１の処理が終了した場合には、ステップＳ１２に進む。ステップＳ１２に進むと、情報処理装置１３０は、記憶部１３５に記憶されている認証処理結果情報を表示装置１４０に表示する。これにより、ス

テップＳ１０で認証ＮＧとされた場合には、表示装置１４０に認証ＮＧである旨の表示がなされ、ステップＳ１１で認証ＯＫとされた場合には、表示装置１４０に認証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、記憶部１３５に記憶されている認証処理結果情報を、ネットワーク（不図示）を介して外部装置に送信する。

【００４３】

以上のステップＳ１～ステップＳ１２の処理を経ることにより、手形状パターン設定部１３１で設定された手形状パターンをセキュリティキーとする認証処理が行われる。

【００４４】

なお、本実施形態においては、手形状パターン設定部１３１でセキュリティキーである手形状パターンを設定する際に、セキュリティ管理者（操作者）から入力された手形状パターンに係る情報に基づいて行う形態を示したが、以下に示す形態であっても適用可能である。

【００４５】

例えば、図６に示す複数の手形状パターン（手形状パターン番号１、２、３、・・・）を、予め、情報処理装置１３０内の記憶部（例えば、記憶部１３５）に記憶させておく。そして、記憶部に予め記憶されている図６の複数の手形状パターンを表示装置１４０に表示し、表示された複数の手形状パターンの中からセキュリティ管理者（操作者）が操作入力装置１５０を用いて選択した手形状パターンを、手形状パターン設定部１３１でセキュリティキーとして設定を行う。このように構成すれば、セキュリティ管理者（操作者）の情報処理装置１３０に対する手形状パターンに係る情報の入力の負荷を軽減させることができる。

【００４６】

また、図６に示す例では、図５に示す例に倣って、４つの手形状からなる手形状パターンが示されているが、本実施形態においては、必ずしも４つの手形状からなる必要は無く、例えば、２つや３つの手形状からなるもの、更には、５つ以上の手形状からなるもの、或いは、１つの手形状からなるものであっても適用可能である。

【００４７】

次に、本発明の実施形態に係るセキュリティ認証システム１００における作用・効果を、従来例であるバイオメトリック認証システム（具体例として、指紋認証システム）と比較しながら説明する。

【００４８】

図７は、本発明の実施形態に係るセキュリティ認証システムの従来例に対する作用・効果の一例を示す図である。

【００４９】

まず、認証システムの導入コストについては、従来例である指紋認証システムでは、特殊な入力センサが必要で高価であるのに対し、本発明のセキュリティ認証システム１００では、赤外線カメラ１１０を用いているため安価である。

【００５０】

また、盗難・偽造については、従来例である指紋認証システムでは、指紋の偽造が可能であるのに対し、本発明のセキュリティ認証システム１００では、手２００を暗箱１２０内に挿入した撮影であるため、例えば、隠しカメラでは、盗撮が不可能である。

【００５１】

また、盗難の場合の対処については、従来例である指紋認証システムでは、指紋は唯一のため、盗難の場合、代替が不可能であるのに対し、本発明のセキュリティ認証システム１００では、セキュリティキーである手形状パターンの手形状の組み合わせは多数あるため、容易に手形状パターンを変更できる。

【００５２】

また、使用における抵抗感については、従来例である指紋認証システムでは、手（指）を入力センサに対して接触させる必要があるため嫌悪感を与える場合があることや、指紋

の採取に抵抗感がある場合などがあるのに対し、本発明のセキュリティ認証システム１００では、手２００の撮影のため、非接触で、抵抗感がない等の利点がある。

【００５３】

即ち、本発明のセキュリティ認証システム１００の主な特徴は、暗箱１２０内に赤外線カメラ１１０を設置し、暗箱１２０の中に手２００を入れて、セキュリティキー（たとえば、パー、グー、チョキ、グーの手形状）を入力すれば、他人から覗かれない、また、小型隠しカメラなどの盗撮も不可能であるという点である。また、本発明のセキュリティ認証システム１００では、暗箱１２０を用意せずとも、照明条件が十分で無い環境においてもセキュリティキーの入力が可能である。

【００５４】

つまり、本発明のセキュリティ認証システム１００の優位性としては、

１．セキュリティキーが第三者に盗撮などで盗まれないこと

２．手の状態、即ち手形状（手が開いている、どの指が出ているなど）をセキュリティキーとして用いることで、その組み合わせは無数にあること

３．非接触であること

４．例えば、マンションなどの入室キー入力において、真っ暗な環境（十分な照明が無い場所）でも、キー入力可能なこと

などが挙げられる。

【００５５】

前述した本実施形態に係るセキュリティ認証システム１００の情報処理装置１３０における図２の各機能構成、並びに当該セキュリティ認証システム１００におけるセキュリティ認証方法を示す図４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。

【００５６】

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。

【００５７】

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セキュリティ認証システム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セキュリティ認証システム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セキュリティ認証システム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。

【００５８】

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。

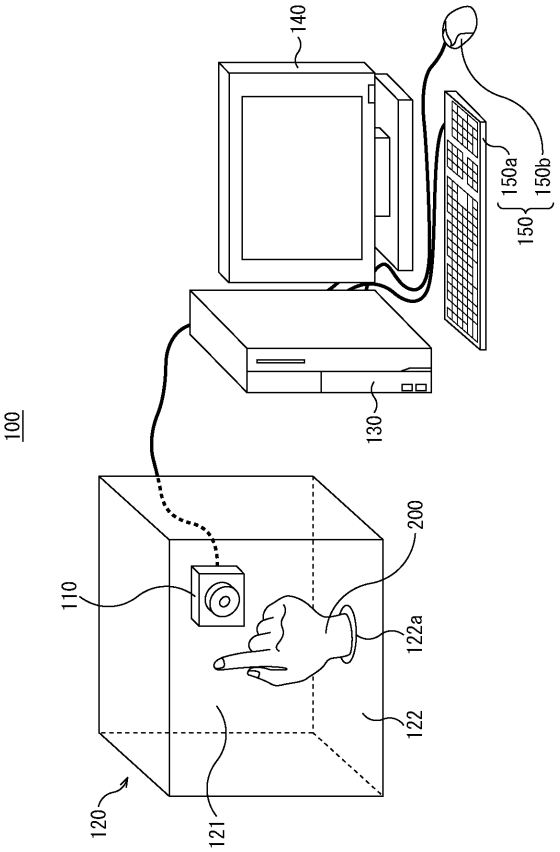
【図面の簡単な説明】

【００５９】

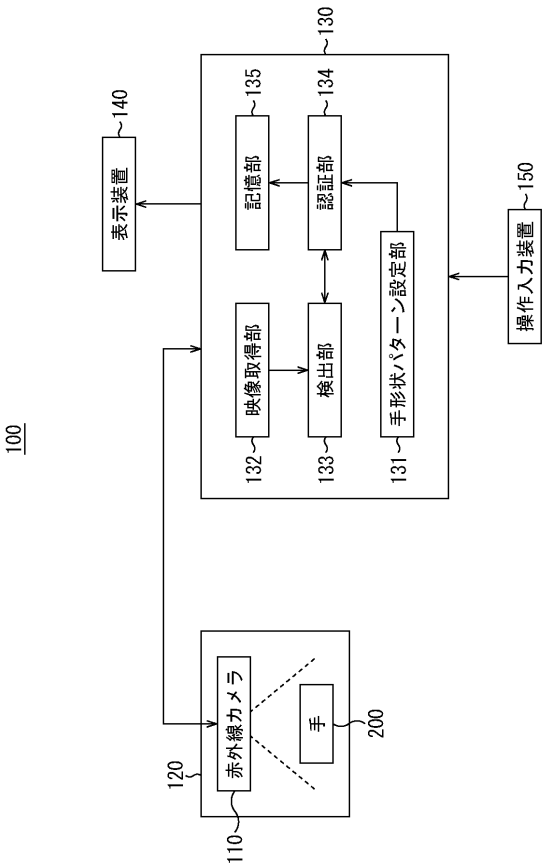
【図１】本発明の実施形態に係るセキュリティ認証システムの外観の一例を示す模式図で

ある。
【図２】本発明の実施形態に係るセキュリティ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】検出部による手形状の検出処理を説明するための図である。
【図４】本発明の実施形態に係るセキュリティ認証システムにおけるセキュリティ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。
【図５】手形状パターン設定部による手形状パターンの設定処理を説明するための図である。
【図６】予め記憶部に記憶されている複数の手形状パターンの一例を示す図である。
【図７】本発明の実施形態に係るセキュリティ認証システムの従来例に対する作用・効果の一例を示す図である。
【符号の説明】
【００６０】
１００　セキュリティ認証システム
１１０　赤外線カメラ
１２０　暗箱
１３０　情報処理装置
１３１　手形状パターン設定部
１３２　映像取得部
１３３　検出部
１３４　認証部
１３５　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　手

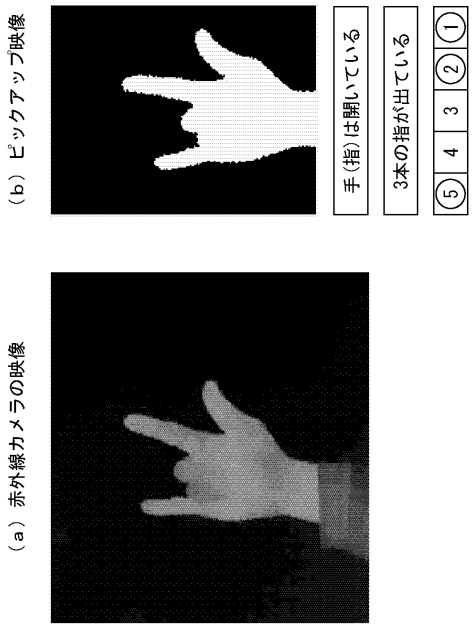
【図１】


100
140
150a
150b
150
130
200
110
122a
122
120
121

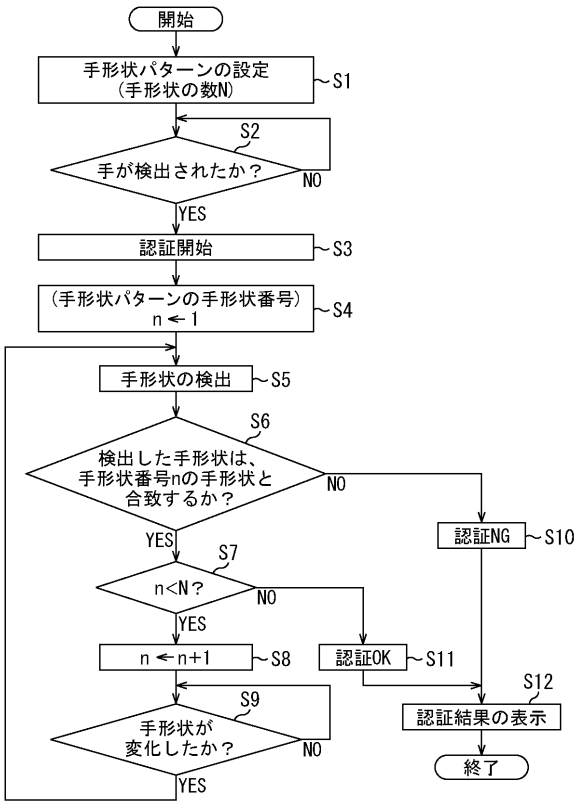
【図２】


100
130
140
表示装置
135
記憶部
134
認証部
150
操作入力装置
映像取得部
検出部
手形状パターン設定部
132
133
131
120
赤外線カメラ
手
200
110

【図３】


（ｂ）ピックアップ映像
手（指）は開いている
3本の指が出ている
①
②
3
4
⑤
（ａ）赤外線カメラの映像

【図４】


開始
手形状パターンの設定
（手形状の数N）
S1
S2
手が検出されたか？
NO
YES
認証開始
S3
（手形状パターンの手形状番号）
n←1
S4
手形状の検出
S5
S6
検出した手形状は、
手形状番号nの手形状と
合致するか？
NO
YES
認証NG
S10
S7
n<N？
NO
YES
n←n+1
S8
認証OK
S11
S12
S9
手形状が
変化したか？
NO
YES
認証結果の表示
終了

【図５】

手形状番号(n)	1	2	3	4
手形状パターン	パー	グー	チョキ	グー

【図６】

手形状パターン番号 ＼ 手形状番号(n)	1	2	3	4
1	パー	グー	チョキ	グー
2	グー	パー	チョキ	パー
3	チョキ	グー	パー	グー
・ ・ ・	・ ・ ・	・ ・ ・	・ ・ ・	・ ・ ・

【図７】

	本発明	従来例 （バイオメトリック認証（指紋認証））
導入コスト	・赤外線カメラは安価である	・特殊な入力センサが必要で、高価である
盗難・偽造	・暗箱内での提示のため、 隠しカメラでは、盗撮が 不可能である	・指紋は偽造が可能である
盗難の場合の対処	・手形状パターンの変更ができる （手形状パターンの組み合わせ は、多数ある）	・指紋は唯一のため、盗難の場合、 代替が不可能である
使用における抵抗感	・非接触で、抵抗感がない	・接触型で、嫌悪感を抱く人がいる ・指紋採取に抵抗感がある

フロントページの続き

Ｆターム(参考) 5B043 AA09 BA03 DA05 FA07 GA05 GA11 HA02
5B057 CA02 CA08 CA12 CA16 DA12 DC08 DC09 DC33