(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号

特許第4837091号
(P4837091)

(45)発行日　平成23年12月14日(2011.12.14)　(24)登録日　平成23年10月7日(2011.10.7)

(51)Int.Cl.		F I		
G06T 1/00	(2006.01)	G06T	1/00	400H
H04N 5/225	(2006.01)	H04N	5/225	C
G08B 25/00	(2006.01)	G08B	25/00	510M
G08B 25/04	(2006.01)	G08B	25/04	G
		G08B	25/04	J

請求項の数 4　(全 16 頁)

(21)出願番号　特願2009-507383 (P2009-507383)
(86)(22)出願日　平成19年3月29日 (2007.3.29)
(86)国際出願番号　PCT/JP2007/056986
(87)国際公開番号　WO2008/120395
(87)国際公開日　平成20年10月9日 (2008.10.9)
審査請求日　平成21年7月15日 (2009.7.15)

(73)特許権者　000005223
富士通株式会社
神奈川県川崎市中原区上小田中４丁目１番１号
(74)代理人　100101856
弁理士　赤澤　日出夫
(72)発明者　青木　隆浩
神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内
(72)発明者　▲浜▼　壮一
神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内
(72)発明者　福田　充昭
神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内

最終頁に続く

(54)【発明の名称】撮影装置、および撮影方法、ならびに撮影プログラム

(57)【特許請求の範囲】

【請求項１】

所定の撮影領域を撮影することができるカメラから撮影画像を取得し、該取得された撮影画像を監視画像又は認証画像のいずれかに用いる撮影装置であって、

前記カメラの撮影範囲に被写体の生体認識を行うことができる生体特徴部分が含まれるか否かを判断する被写体検出部と、

認証画像取得指示を受け付けると前記撮影画像を認証画像として処理するとともに、前記認証画像取得指示が無い場合において、前記被写体検出部により前記生体特徴部分が含まれると判断されない場合は、前記撮影画像を監視画像として処理する一方、前記被写体検出部により前記生体特徴部分が含まれると判断される場合は、前記カメラによる撮影を停止する制御部と

を備える撮影装置。

【請求項２】

請求項１に記載の撮影装置において、

前記被写体検出部は、前記被写体と前記カメラとの距離を測定する距離測定部と、前記距離測定部により測定された距離が所定の値よりも小さい場合に、前記撮影画像に前記被写体が含まれると判断する判断部とを備えることを特徴とする撮影装置。

【請求項３】

所定の撮影領域を撮影するカメラから撮影画像を取得し、該取得された撮影画像を監視画像又は認証画像のいずれかに用いる撮影方法であって、

前記カメラの撮影範囲に被写体の生体認識を行うことができる生体特徴部分が含まれるか否かを判断する被写体検出ステップと、
認証画像取得指示を受け付けると前記撮影画像を認証画像として処理するとともに、前記認証画像取得指示が無い場合において、前記被写体検出ステップにより前記生体特徴部分が含まれると判断されない場合は、前記撮影画像を監視画像として処理する一方、前記被写体検出ステップにより前記生体特徴部分が含まれると判断される場合は、前記カメラによる撮影を停止する制御ステップと
を備える撮影方法。
【請求項４】
所定の撮影領域を撮影することができるカメラから撮影画像を取得し、該取得された撮影画像を監視画像又は認証画像のいずれかに用いる撮影方法をコンピュータに実行させる撮影プログラムであって、
前記カメラの撮影範囲に被写体の生体認識を行うことができる生体特徴部分が含まれるか否かを判断する被写体検出ステップと、
認証画像取得指示を受け付けると前記撮影画像を認証画像として処理するとともに、前記認証画像取得指示が無い場合において、前記被写体検出ステップにより前記生体特徴部分が含まれると判断されない場合は、前記撮影画像を監視画像として処理する一方、前記被写体検出ステップにより前記生体特徴部分が含まれると判断される場合は、前記カメラによる撮影を停止する制御ステップと
をコンピュータに実行させる撮影プログラム。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、生体認証画像を撮影するカメラを監視カメラとして使用し、生体認証に有効な生体特徴を含まない画像を監視画像として出力することにより、生体特徴を含む画像の流出を防ぐと共に生体認証における不正行為を監視する撮影装置、および撮影方法、ならびに撮影プログラムに関するものである。
【背景技術】
【０００２】
近年、セキュリティシステムにおいて、生体認証は金融機関のＡＴＭやマンションの入退室管理等で利用されているが、生体認証装置やその周辺の装置に対して様々な不正が行なわれる可能性がある。例えば、顔認証において、顔認証装置の登録者以外の人間が登録者の顔写真を顔認証装置のカメラに見せることで認証を行おうとする不正認証行為が行われる可能性がある。また、入退室管理において、生体認証装置の非登録者が登録者である人に続いてドアに入ってしまうような可能性がある。また、認証に生体認証を用いているＡＴＭにおいても、暗証番号が覗き見される可能性がある。このような不正行為を防ぐために、生体認証と監視カメラを組み合わせた技術が知られている。
【０００３】
このような生体認証と監視カメラを組み合わせたセキュリティシステムとして、集合住宅の入館者を撮像する監視カメラと顔画像を検出する画像検出部と居住者の顔が予め登録されているデータベースを持ち、監視カメラに写った顔画像がデータベース内の顔画像と照合されるによって入館者が居住者かどうかを認証し、不審者を通報する不審者通報システムが知られている（例えば特許文献１参照）。
【０００４】
また、本発明の関連ある従来技術として、指紋識別器の光学系で指紋画像のみを撮像するのではなく、人物画像も撮像できるようにすることでセキュリティ性を高める指紋識別器の光学系を利用した人物像撮像が知られている（例えば、特許文献２参照）。
【特許文献１】特開２００６-１２００８４号公報
【特許文献２】特開平６－３０９４４７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、生体認証装置が撮影した画像をそのまま出力してしまうと、生体特徴が流出するおそれがある。認証に用いられる生体特徴情報の流出は、悪意を持つ第三者のみでなく、監視画像を目にすることができる内部の人間によって行なわれる可能性がある。例えば、内部の人間によってなされる生体特徴の流失の可能性としては監視画像を見ている警備員が監視画像を記録してしまうこと、システムを管理するシステムエンジニア等が生体認証装置に記録されている監視画像を容易に取り出せてしまうことなどが考えられる。
【０００６】
また、生体特徴は暗証番号と異なり、変えることができないため、生体特徴情報が一旦流出してしまうと、その後の生体認証によるセキュリティは保証されない。
【０００７】
本発明は上述した問題点を解決するためになされたものであり、生体認証画像を撮影するカメラを監視カメラとして使用するとともに、生体認証に有効な生体特徴を含まない画像を監視画像として管理することにより、生体特徴を含む画像の流出を防ぐと共に生体認証における不正行為を監視する撮影装置、および撮影方法、ならびに撮影プログラム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】
【０００８】
上述した課題を解決するため、本発明は、所定の撮影領域を撮影することができるカメラから撮影画像を取得し、該取得された撮影画像を監視画像又は認証画像のいずれかに用いる撮影装置であって、前記カメラの撮影範囲に被写体の生体認識を行うことができる生体特徴部分が含まれるか否かを判断する被写体検出部と、認証画像取得指示を受け付けると前記撮影画像を認証画像として処理するとともに、前記認証画像取得指示が無い場合において、前記被写体検出部により前記生体特徴部分が含まれると判断されない場合は、前記撮影画像を監視画像として処理する一方、前記被写体検出部により前記生体特徴部分が含まれると判断される場合は、前記カメラによる撮影を停止する制御部とを備える撮影装置。
【０００９】
また、本発明の撮影装置において、前記被写体検出部は、前記被写体と前記カメラとの距離を測定する距離測定部と、前記距離測定部により測定された距離が所定の値よりも小さい場合に、前記撮影画像に前記被写体が含まれると判断する判断部とを備えることを特徴とする。
【００１０】
また、撮影領域全体を照明して撮影を行い得られた第１撮影画像と、前記撮影領域全体と共に、前記撮影領域全体よりも狭い前記カメラ近傍領域を照明して撮影を行い得られた第２撮影画像との差分画像を取得する差分画像取得部と、前記差分画像における輝度が所定値以上である領域を抽出し、前記第１撮影画像又は前記第２撮影画像から、前記輝度が所定値以上である領域の撮像物を除去して監視画像を得る監視画像取得部とを備える。
【００１１】
また、本発明は、所定の撮影領域を撮影することができるカメラから撮影画像を取得し、該取得された撮影画像を監視画像又は認証画像のいずれかに用いる撮影装置であって、所定のタイミングにおいて撮影を行って得られた撮影画像を登録された生体特徴と比較する比較部と、前記比較部の比較結果に基づいて、前記撮影画像が前記登録された生体特徴に一致しないと判断された場合、前記撮影画像を監視画像として処理すると共に、前記比較部の比較結果に基づいて、前記撮影画像が前記登録された生体特徴に一致すると判断された場合、前記撮影画像を監視画像として処理しない監視画像選択処理部とを備える。
【００１２】
また、本発明は、所定の撮影領域を撮影するカメラから撮影画像を取得し、該取得され

た撮影画像を監視画像又は認証画像のいずれかに用いる撮影方法であって、前記カメラの撮影範囲に被写体の生体認識を行うことができる生体特徴部分が含まれるか否かを判断する被写体検出ステップと、認証画像取得指示を受け付けると前記撮影画像を認証画像として処理するとともに、前記認証画像取得指示が無い場合において、前記被写体検出ステップにより前記生体特徴部分が含まれると判断されない場合は、前記撮影画像を監視画像として処理する一方、前記被写体検出ステップにより前記生体特徴部分が含まれると判断される場合は、前記カメラによる撮影を停止する制御ステップとを備える。

【００１３】

また、本発明は、所定の撮影領域を撮影することができるカメラから撮影画像を取得し、該取得された撮影画像を監視画像又は認証画像のいずれかに用いる撮影方法であって、前記撮影領域全体を照明し前記カメラにより撮影を行う第１撮影ステップと、前記撮影領域全体の照明と共に、前記撮影領域全体よりも狭い前記カメラ近傍領域を照明し、前記カメラにより撮影を行う第２撮影ステップと、前記第１撮影ステップにより得られた第１撮影画像と、前記第２撮影ステップにより得られた前記第２撮影画像との差分画像を取得する差分画像取得ステップと、前記差分画像における輝度が所定値以上である領域を抽出し、前記第１撮影画像又は前記第２撮影画像から前記輝度が所定値以上である領域の撮像物を除去して監視画像を得る監視画像取得ステップとを備える。

【００１４】

また、本発明は、所定の撮影領域を撮影することができるカメラから撮影画像を取得し、該取得された撮影画像を監視画像又は認証画像のいずれかに用いる撮影方法であって、所定のタイミングにおいて撮影を行って得られた撮影画像を登録された生体特徴と比較する比較ステップと、前記比較ステップの比較結果に基づいて、前記撮影画像が前記登録された生体特徴に一致しないと判断された場合、前記撮影画像を監視画像として処理すると共に、前記比較部の比較結果に基づいて、前記撮影画像が前記登録された生体特徴に一致すると判断された場合、前記撮影画像を監視画像として処理しない監視画像選択処理ステップとを備える。

【００１５】

また、本発明は、所定の撮影領域を撮影することができるカメラから撮影画像を取得し、該取得された撮影画像を監視画像又は認証画像のいずれかに用いる撮影方法をコンピュータに実行させる撮影プログラムであって、前記カメラの撮影範囲に被写体の生体認識を行うことができる生体特徴部分が含まれるか否かを判断する被写体検出ステップと、認証画像取得指示を受け付けると前記撮影画像を認証画像として処理するとともに、前記認証画像取得指示が無い場合において、前記被写体検出ステップにより前記生体特徴部分が含まれると判断されない場合は、前記撮影画像を監視画像として処理する一方、前記被写体検出ステップにより前記生体特徴部分が含まれると判断される場合は、前記カメラによる撮影を停止する制御ステップとをコンピュータに実行させる。

【００１６】

また、本発明は、所定の撮影領域を撮影することができるカメラから撮影画像を取得し、該取得された撮影画像を監視画像又は認証画像のいずれかに用いる撮影方法をコンピュータに実行させる撮影プログラムであって、前記撮影領域全体を照明し前記カメラにより撮影を行う第１撮影ステップと、前記撮影領域全体の照明と共に、前記撮影領域全体よりも狭い前記カメラ近傍領域を照明し、前記カメラにより撮影を行う第２撮影ステップと、前記第１撮影ステップにより得られた第１撮影画像と、前記第２撮影ステップにより得られた前記第２撮影画像との差分画像を取得する差分画像取得ステップと、前記差分画像における輝度が所定値以上である領域を抽出し、前記第１撮影画像又は前記第２撮影画像から前記輝度が所定値以上である領域の撮像物を除去して監視画像を得る監視画像取得ステップとをコンピュータに実行させる。

【００１７】

また、本発明は、所定の撮影領域を撮影することができるカメラから撮影画像を取得し、該取得された撮影画像を監視画像又は認証画像のいずれかに用いる撮影方法をコンピュ

ータに実行させる撮影プログラムであって、所定のタイミングにおいて撮影を行って得られた撮影画像を登録された生体特徴と比較する比較ステップと、前記比較ステップの比較結果に基づいて、前記撮影画像が前記登録された生体特徴に一致しないと判断された場合、前記撮影画像を監視画像として処理すると共に、前記比較部の比較結果に基づいて、前記撮影画像が前記登録された生体特徴に一致すると判断された場合、前記撮影画像を監視画像として処理しない監視画像選択処理ステップとをコンピュータに実行させる。

【図面の簡単な説明】

【００１８】

【図１】実施の形態１の全体構成の一例を示すブロック図である。

【図２】実施の形態１の認証装置が適用されるオートロックを示す図である。

【図３】実施の形態１の認証装置の操作部の一例を示す図である。

【図４】実施の形態１の全体動作を示すフローチャート（その１）である。

【図５】実施の形態１の全体動作を示すフローチャート（その２）である。

【図６】実施の形態１における監視画像取得タイミングを示す図である。

【図７】実施の形態１における監視画像適合チェック処理を示す図である。

【図８】実施の形態１における制御部の監視画像取得処理を示すフローチャートである。

【図９】実施の形態２の認証装置によるＡＴＭを示す図である。

【図１０】実施の形態２の認証装置による作用を示す図である。

【図１１】実施の形態２の全体構成の一例を示すブロック図である。

【図１２】実施の形態２の監視画像の撮影方法を示す図（その１）である。

【図１３】実施の形態２の監視画像の取得方法を示す図（その２）である。

【図１４】実施の形態２の監視画像生成動作を示すフローチャートである。

【図１５】実施の形態３の全体構成の一例を示す図である。

【図１６】実施の形態３における監視画像出力選択の動作を示すフローチャートである。

【発明を実施するための最良の形態】

【００１９】

以下、本発明の実施の形態について本発明の撮影装置を適用した認証装置について図面を参照しつつ説明する。

実施の形態１.

【００２０】

図１は実施の形態１の全体構成の一例を示すブロック図である。

【００２１】

実施の形態１における認証装置１０は、撮影装置（本発明の撮影装置）１０Ａと認証処理装置１０Ｂとから構成され、認証結果に基づいてドアを開閉制御するドア制御部３０を駆動する。

【００２２】

撮影装置１０Ａは、キー入力部１０１、撮影部１０８、制御部１０５、メモリ部１０６、通信部１０７を備える。ここで制御部１０５は本発明の制御部に対応している。また、撮影部１０８は照明部１０２、カメラ１０３、距離センサ１０４を備える。

【００２３】

認証処理装置１０Ｂは認証処理制御部２０１、記録部２０２、認証処理部２０３、通信部２０４を備える。なお、認証処理装置１０Ｂは撮影装置１０Ａとは別の場所、例えば管理センタなどに設置されていることが望ましい。

【００２４】

照明部１０２はカメラ１０３が撮影する被写体を照らす。なお、照明部１０２はＬＥＤ、白熱灯など認証の為の撮影に適したものを便宜備えるものとする。

【００２５】

本実施の形態では、カメラ１０３で撮像される画像は、認証画像または監視画像として用いられる。なお、カメラ１０３はＣＣＤであってもＣＭＯＳであっても構わない。

【００２６】

距離センサ１０４は赤外線を投射し、被写体までの距離を測る。なお、測定方法は被写体までの距離が測定できるものであれば他の手段であっても構わない。この距離センサは本発明の被写体検出部に対応している。

【００２７】

制御部１０５は、後述するように撮影部１０８の制御を行う。また、制御部１０５は取得したＩＤと、カメラ１０３で撮影した画像のうち監視画像をメモリ部１０６に格納させる。また、認証結果に基づいてドア制御部３０にドアを開けるよう指示を出す。

【００２８】

情報提示部１０９は認証を行う利用者に対して情報を提示する。なお、この情報は視覚情報によって提示されても、音声によって提示されても構わない。

【００２９】

通信部１０７は認証処理装置１０Ｂの通信部２０４とデータの送受信を行い、認証結果に基づいてドア制御部３０に制御部１０５からの指示を送信する。また、通信部１０７は通信部２０４にデータを送信する際、データを暗号化する。なお、通信部１０７と通信部２０４、ドア制御部３０とを接続するネットワークはデータの送受信が行えるものであればＴＣＰ／ＩＰ、ＵＳＢ、ＬＡＮ、無線ＬＡＮのいずれであっても構わない。

【００３０】

認証処理装置１０Ｂの通信部２０４は撮影装置１０Ａの通信部１０７とデータの送受信を行う。また、通信部２０４は通信部１０７からデータを受信する際、データを復号化する。

【００３１】

認証処理装置１０Ｂの記録部２０２は生体特徴画像、ＩＤを対応付けて記録する。また、認証が行われた時間、認証の結果、監視画像もＩＤと対応付けて記録する。

【００３２】

認証処理装置１０Ｂの認証処理部２０３は認証処理制御部２０１から撮影装置１０Ａから受信した生体特徴画像（認証画像）を取得し、記録部２０２内に登録された生体特徴画像（登録画像）との比較処理をする。なお、この認証画像と登録画像との比較処理においては、認証処理部２０３はそれぞれの画像から、認証画像と登録画像が同一の生体特徴を有しているか否かの判断基準とするための情報（例えば特徴点）を抽出し、この生体特徴情報を用いて処理を行なうものとする。

【００３３】

認証処理制御部２０１は通信部２０４を通じて撮影装置１０ＡからＩＤ及び画像データを受信する。また、ＩＤを引数として記録部２０２から該当する登録画像を取得し、認証処理部２０３に認証画像との比較処理を行わせる。

【００３４】

図２は、本実施の形態の認証装置が適用される一例としての認証装置によるオートロックを示す図である。このオートロックはサーバルームやマンションルームの入り口等のセキュリティが要求される部屋の入り口に設けられ、認証装置１０（又は撮影装置１０Ａ）と、認証装置１０の認証結果によりドアＤを開閉するドア制御部３０を備える。

【００３５】

なお、図２に示す認証装置１０はスタンドアローンの形態として構築されても、撮影操作部と認証処理部とが通信回線で接続されるシステムとして構築されていてもよい。実施の形態１の認証装置は不審者の侵入を防ぐために、認証装置１０により、事前にシステムに登録された登録者の認証がなされると、ドア制御部３０にドアのロックを解除させる。なお、実施の形態１において、生体認証は静脈認証を想定しているが、実施の形態１の構成及び動作は他の生体特徴画像に基づく認証においても有効である。

【００３６】

図３は撮影装置１０Ａの概観構成の一例を示す図である。この撮影装置１０Ａは登録者が操作を行って例えばＩＤを入力するキー入力部１０１と、撮影画像を取得するカメラを有する撮影部１０８と、情報を提示する情報提示部１０９とを備えている。

【００３７】
次に、実施の形態１の全体動作について図４及び図５のフローチャートを用いて説明する。
【００３８】
まず、撮影装置１０Ａの制御部１０５はキー入力部１０１でＩＤが入力されたか否かを判断する（Ｓ１０１）。
【００３９】
ＩＤが入力された場合（Ｓ１０１，ＹＥＳ）、制御部１０５は通信部１０７を介して、入力されたＩＤ（入力ＩＤ）と共に認証要求を認証処理装置１０Ｂへ送信し（Ｓ１０２）、またカメラ１０３には監視画像を撮影させ取得する（Ｓ１０３）。
【００４０】
次に、認証処理装置１０Ｂの認証処理制御部２０１は、通信部２０４を介して受信した入力ＩＤが記録部２０２に記録されているＩＤ（登録ＩＤ）のいずれかと一致するか否かを判断する（Ｓ１０４）。
【００４１】
ステップＳ１０４の判断において、入力ＩＤと登録ＩＤが一致した場合（Ｓ１０４，ＹＥＳ）、認証処理制御部２０１は制御部１０５に認証画像要求を送信し、認証画像要求を受信した制御部１０５はカメラ１０３に認証画像を撮影させ、認証画像を取得する（Ｓ１０６）。
【００４２】
次に、制御部１０５は認証画像を通信部１０７に暗号化させ（Ｓ１０７）、通信部１０７は認証処理装置１０Ｂの通信部２０４に認証画像を送信する（Ｓ１０８）。この動作は本発明の制御ステップの動作の一部である。
【００４３】
認証画像を受信した通信部２０４は暗号化された認証画像を復号化し、通信部２０４から認証画像を取得した認証処理制御部２０１は、認証処理部２０３に入力ＩＤに対応する登録画像２０２との比較処理をさせ、認証処理制御部２０１は撮影装置１０Ａの制御部１０５に認証結果を送信する（Ｓ１０９）。なお、この認証結果は認証画像と登録画像が一致するか否か（ＯＫまたはＮＧ）を示す情報である。
【００４４】
認証結果を受信した制御部１０５は認証結果がＯＫか否かを判断し（Ｓ１１０）、認証結果がＯＫである場合（Ｓ１１０，ＹＥＳ）、制御部１０５は通信部１０７を介してドア制御部３０にドアを開けさせ（Ｓ１１７）、カメラ１０３に再び監視画像を撮影させ、監視画像を取得する（Ｓ１１２）。
【００４５】
そして、さらに認証処理制御部２０１は制御部１０５に監視画像要求を送信し（Ｓ１１３）、監視画像要求を受信した制御部１０５は通信部１０７に監視画像を暗号化させ（Ｓ１１４）、認証処理装置１０Ｂの通信部２０４へ送信させる（Ｓ１１５）。
【００４６】
監視画像を受信した通信部２０４は暗号化された監視画像を復号化し、通信部２０４から監視画像を取得した認証処理制御部２０１は、記録部２０２に認証が行われた時間、認証の結果、監視画像をＩＤと対応付けて格納させる（Ｓ１１８）。
【００４７】
また、ステップＳ１１０の判断において、認証結果がＮＧである場合（Ｓ１１０，ＮＯ）、制御部１０５は情報提示部１０９に認証エラーを提示させ（Ｓ１１１）、カメラ１０３に再び監視画像を撮影させ、監視画像を取得する（Ｓ１１２）。
【００４８】
また、図４におけるステップＳ１０４の判断において、入力ＩＤと登録ＩＤが一致しなかった場合（Ｓ１０４，ＮＯ）、認証処理制御部２０１は制御部１０５に不正ＩＤ通知を送信し（Ｓ１０５）、不正ＩＤ通知を受信した制御部１０５は情報提示部１０９にＩＤエ

ラーを提示させる（Ｓ１１６）。

【００４９】

なお、ステップＳ１０７とステップＳ１１４における暗号化の暗号アルゴリズムについて、認証画像は監視画像よりも高いセキュリティを求められるため、例えば、通信部１０７が監視画像をセキュリティよりも処理速度優先の暗号化アルゴリズムで暗号化し、認証画像を処理速度よりもセキュリティ重視の暗号化アルゴリズムで暗号化することにより、信頼性と処理速度を両立することができる。

【００５０】

次に、撮影装置１０Ａの制御部が監視画像を取得するタイミングについて、図６を用いて説明する。

【００５１】

制御部１０５はキー入力部１０１にキー入力がなされた時点でカメラ１０８に監視画像（１）を取得させ、認証処理後に再び監視画像（２）を取得させる。また、制御部１０５によって取得された監視画像は認証処理装置１０Ｂに送信されるまでメモリ部１０６に一時格納される。

【００５２】

次に、撮影装置１０Ａの制御部１０５の監視画像撮影適合チェック処理について図７を用いて説明する。

【００５３】

撮影部１０８の距離センサ１０４は監視画像取得の際、被写体までの距離を測定し、距離が所定の値よりも大きい場合は、制御部１０５はカメラ１０３による撮影画像を監視用画像として扱うよう処理する。一方、距離が所定の値よりも小さい場合は、制御部１０５はカメラ１０３による監視用画像の撮影を停止させる。実施の形態１において、生体認証は細い線状の生体特徴である手の静脈によってなされる。手の静脈が一定の距離以上離れて撮影された画像は認証には使用できない為、距離による監視画像適合チェックがなされることで、認証に有効な生体特徴が監視画像として撮影されることがない。

【００５４】

次に、図４に示したステップＳ１０３及び図５に示したステップＳ１１２における制御部１０５の監視画像取得動作（本発明の制御ステップの一部）について図８を用いて説明する。

【００５５】

まず、制御部１０５は距離センサ１０４に被写体までの距離（Ｄ）を測定させ（被写体検出ステップ）、その値を取得し（Ｓ２０１）、Ｄが予め設定された閾値以下である場合（Ｓ２０２，ＮＯ）、撮影画像（監視画像）に生体特徴部分が含まれると判断し、制御部１０５は監視画像取得処理を終了する。一方、Ｄが予め設定された閾値より大きい場合（Ｓ２０２，ＹＥＳ）、制御部１０５はカメラ１０３に撮影を続行させ、監視画像を取得する（Ｓ２０３）。

【００５６】

なお、図８の動作において、カメラ１０３による監視画像の撮影は、撮影条件として、認証画像の撮影よりも長い露出時間で撮影する。監視画像の露出時間を認証画像の露出時間よりも長くすることによって、カメラ１０３の絞り値を上げることができ、鮮明な監視画像を得ることができる。また、監視画像の被写体よりも認証画像の被写体の方が照明部１０２に近いため、生体特徴が映ったとしても、露出オーバーにより生体特徴部分は白トビを起こす。よって、監視画像に認証可能な生体特徴が映ることはない。

【００５７】

また、ステップＳ１０３での監視画像取得処理において、認証処理が開始されるまで制御部１０５が一定の間隔で監視画像を取得しても良いし、ステップＳ１１２での監視画像取得処理において、制御部１０５が所定の時間内に一定の間隔で監視画像を取得しても構わない。

【００５８】

以上の構成、動作によって、実施の形態１の認証監視システムは認証画像と監視画像を同じカメラで撮影し、なおかつ認証画像の漏洩を防ぐことができる。

【００５９】

実施の形態２.

以下、本発明の撮影装置を認証装置によるＡＴＭに適用した実施の形態２について説明する。図９は実施の形態２の認証装置によるＡＴＭを示す図である。

【００６０】

実施の形態１では認証装置によるオートロックを想定していたが、実施の形態２では認証装置によるＡＴＭを想定している。新たに設けられたＩＣカード読み取り部１１０は、口座情報などと共に生体特徴情報が保存されたキャッシュカードを読み取る。また、実施の形態２におけるキー入力部１０１は例えばタッチパネルであっても構わない。また、実施の形態２の撮影装置１０Ａには、距離センサ１０４は備えられておらず、実施の形態２の撮影装置１０Ａは照明部１０２の照明の有無に基づく撮影画像の輝度差を利用することにより、生体特徴が撮影された領域を除去し、生体特徴を含む監視画像が流失することを防ぐようにしたものである。

【００６１】

なお、実施の形態２によれば、例えば、図１０に示すように、銀行のＡＴＭにおいて、生体認証を行う撮影装置１０Ａ（撮影部１０８）が生体認証を行わない時に監視カメラとして機能することにより、例えば暗証番号を覗き見るためのカメラＣがＡＴＭ近くに備え付けられるなどの不正行為を監視することによって、そのような不正行為を未然に防ぐことができる。

【００６２】

図１１は実施の形態２の全体構成の一例を示すブロック図である。図１１において、図３と同一符号は図３に示された対象と同一又は相当物を示しており、実施の形態１と機能が変わらない部分についてはここでの説明を省略する。

【００６３】

実施の形態１の全体構成と異なるのは実施の形態１の撮影装置１０Ａと認証処理装置１０Ｂとが一つの筐体内に認証装置１０として備えられていること、認証装置１０（撮影装置１０Ａ）内に距離センサ１０４が備えられていないこと、ＩＣカード読み取り部１１０及び監視画像生成部１１１が新たに設けられていること、記録部２０２に相当するデータベース４０が設けられていることである。また、実施の形態２において、予め保存されている生体特徴情報である登録画像はＩＣカード読み取り部１１０によって読み取られるキャッシュカード内に保存されている為、データベース４０は登録画像を保持していない。また、監視画像は監視画像生成部１１１によって、不正行為が行なわれていないかを監視する監視ルームへ送信される為、データベース４０は監視画像も保持しておらず、認証が行われた時間、認証の結果、ＩＤ、そしてキャッシュカードの暗証番号を対応付けて記録している。また、認証装置１０の外部に外部照明１１４が新たに設けられている。この外部照明１１４は例えば室内照明である。なお、照明部１０２と波長が異なる光を発するものであればより好ましい。

【００６４】

なお、監視画像生成部１１１から出力される監視画像は、映像であってもよく、その際、監視画像生成部１１１が映像データを非可逆圧縮しても構わない。また、監視画像生成部１１１の映像出力方式はデジタル出力であってもアナログ出力であっても構わない。

【００６５】

次に実施の形態１と異なる実施の形態２の動作について説明する。

【００６６】

実施の形態２では認証処理部２０３が認証装置１０内に備えられているため、制御部１０５は実施の形態１の認証処理制御部２０１の通信部２０４以外の動作をも行う。また、制御部１０５が認証処理部２０３に認証処理を行わせる際、制御部１０５が登録画像をキャッシュカードから取得し、認証画像と登録画像が同一の生体特徴を有しているか否かの

判断基準とするための情報（例えば特徴点）を抽出し、この生体特徴情報を用いて処理を行なう動作、及び制御部１０５がキャッシュカードの暗証番号をデータベース４０に格納された暗証番号と照合する動作が実施の形態１の動作と異なる。また、距離センサ１０４が備えられておらず、新たに監視画像生成部１１１が設けられたことにより、監視画像に認証画像が含まれてしまうことを防ぐための動作が実施の形態１と異なっている。

【００６７】

図１２及び図１３は実施の形態２の認証画像及び監視画像の撮影方法を示す図である。

【００６８】

実施の形態２では、図１２に示すように、例えばＡＴＭが設置された部屋に備え付けられた外部照明１１４の光の下で、認証装置１０の照明部１０２の光の有無により生じる撮影画像の輝度の差を利用して、監視画像生成部１１１は撮影画像から被写体を削除する処理を行い、監視画像を得る。監視画像生成部１１１は照明部１０２が被写体を照らしている状態（照明ＯＮ）、及び被写体を照らしていない状態（照明ＯＦＦ）、それぞれの状態の被写体をカメラ１０３に撮影させる。

【００６９】

そして、図１３に示すように、監視画像生成部１１１は照明ＯＮ画像及び照明ＯＦＦ画像の同じ座標における輝度値を比較し、照明ＯＮ画像と照明ＯＦＦ画像とで輝度が同じ領域を抽出し、監視画像とすることで認証可能な生体特徴が映っていない監視画像を得ることができる。なお、監視画像生成部１１１は本発明の差分画像取得部及び監視画像取得部を構成している。

【００７０】

なお、ＡＴＭが設置された部屋に外部照明がない場合は、認証装置１０の外部、または認証装置１０の近くに外部照明１１４を設けても構わない。

【００７１】

図１４は実施の形態２の監視画像生成部の動作を示すフローチャートである。

【００７２】

まず、監視画像生成部１１１は照明ＯＮ画像と照明ＯＦＦ画像を取得し（Ｓ３０１）。取得する座標を示す変数Ｘ及びＹに０を代入し、それぞれ初期化し（Ｓ３０２）、照明ＯＮ画像ピクセル（Ｘ，Ｙ）の輝度値Ｖ１及び照明ＯＦＦ画像ピクセル（Ｘ，Ｙ）の輝度値Ｖ２をそれぞれ取得する（Ｓ３０３）。そして監視画像生成部１１１はＶ１からＶ２を差し引いた差分画像を生成取得し（差分画像生成ステップ）、この差分画像において、輝度値が所定の閾値より大きいか否かを判断する（Ｓ３０４）。

【００７３】

ステップＳ３０４の判断において、Ｖ１からＶ２を差し引いた値が所定の閾値より大きい（又は所定の閾値以上である）場合（Ｓ３０４，ＹＥＳ）、監視画像生成部１１１は監視画像ピクセル（Ｘ，Ｙ）の輝度を０にし（Ｓ３０６）、ＸにＸ＋１を代入し（Ｓ３０７）、Ｘが監視画像の横サイズのピクセル数以上であるか否かを判断する（Ｓ３０８）。

【００７４】

ステップＳ３０８の判断において、Ｘが監視画像の横サイズのピクセル数以上である場合（Ｓ３０８，ＹＥＳ）、監視画像生成部１１１はＸに０を代入し、ＹにＹ＋１を代入し（Ｓ３０９）、Ｙが監視画像の縦サイズのピクセル数以上であるか否かを判断する（Ｓ３１０）。

【００７５】

ステップＳ３１０の判断において、Ｙが監視画像の縦サイズのピクセル数以上である場合（Ｓ３１０，ＹＥＳ）、監視画像生成部１１１は処理を終了する。

【００７６】

一方、Ｙが監視画像の縦サイズのピクセル数より小さい場合（Ｓ３１０，ＮＯ）、監視画像生成部１１１は、再び照明ＯＮ画像ピクセル（Ｘ，Ｙ）の輝度値Ｖ１及び照明ＯＦＦ画像ピクセル（Ｘ，Ｙ）の輝度値Ｖ２をそれぞれ取得する（Ｓ３０３）。

【００７７】

また、ステップＳ３０８の判断において、Ｘが監視画像の横サイズのピクセル数より小さい場合（Ｓ３０８，ＮＯ）、監視画像生成部１１１は、再び照明ＯＮ画像ピクセル（Ｘ，Ｙ）の輝度値Ｖ１及び照明ＯＦＦ画像ピクセル（Ｘ，Ｙ）の輝度値Ｖ２をそれぞれ取得する（Ｓ３０３）。

【００７８】

また、ステップＳ３０４の判断において、Ｖ１からＶ２を差し引いた値が所定の閾値以下である場合（Ｓ３０４，ＮＯ）、監視画像生成部１１１は監視画像ピクセル（Ｘ，Ｙ）の輝度をＶ２にし（Ｓ３０５）、ＸにＸ＋１を代入する（Ｓ３０７）。

【００７９】

なお、この処理におけるステップＳ３０６の動作により、監視画像に映った認証特徴部分は黒く塗りつぶされる。また、ステップＳ３０５の動作により、監視画像に映った認証特徴部分以外の部分の輝度は処理前と同じ状態で維持される。また、ステップＳ３０７～ステップＳ３１０の動作により、監視画像の全てのピクセルにおいて、輝度＝０の代入、または輝度＝Ｖ２の代入がなされることにより、認証に利用可能な認証特徴部分は全て黒く塗りつぶされる。また、監視画像生成部１１１が映像を出力する場合、この処理は映像の全てのフレームに対して行われる。

【００８０】

以上の動作により実施の形態２の監視画像生成部１１１は認証特徴を流出することなく、監視画像または監視映像を出力することができる。

【００８１】

実施の形態３．

以下、本発明の撮影装置を認証装置に適用した実施の形態３について説明する。図１５は実施の形態３の全体構成の一例を示す図である。

【００８２】

実施の形態３における認証装置１０は、ＩＣカード読み取り部１１０、キー入力部１０１、監視画像出力部１１３が備えられていないこと、認証開始スイッチ１１２、監視画像出力部１１３が新たに設けられていることが実施の形態２の認証装置１０と異なる。実施の形態３では、生体認証のみで認証を行なう１：Ｎ認証によってＩＤ、暗証番号などを使用せずに個人の認証を行なう。よって、暗証番号やＩＤを入力するキー入力部１０１が監視装置１０に備わっていないので、認証開始スイッチ１１２が押されることによって、生体認証が開始される。なお、生体認証が静脈認証によって行なわれる場合は、認証開始スイッチ１１２は被撮影者が指先で押せる位置に配置され、生体認証が顔認証によって行なわれる場合には、認証開始スイッチ１１２は被撮影者の足元に配置される。

【００８３】

なお、データベース４０には認証が行われた時間、認証の結果、予め保存された生体特徴画像である登録画像が格納されている。また、監視画像出力部１１３は監視画像を監視ルームへ送信する。

【００８４】

次に、実施の形態３の動作を説明する。

【００８５】

実施の形態３の認証装置１０では、認証処理部２０３が監視画像として撮影された画像に認証特徴が含まれていないか否かを確認する。制御部１０５は認証開始スイッチ１１２が押されていなくても、カメラ１０３に一定時間間隔おきに画像を撮影させ、撮影画像を取得し、取得した画像を認証処理部２０３に送信し、認証処理部２０３はデータベース４０を参照して、登録された全登録画像と撮影された全撮影画像との照合を行い、最も生体特徴が一致している登録画像との類似度を返す。なお、この認証画像と全登録画像との照合においては、認証処理部２０３はそれぞれの画像から、認証画像と登録画像が同一の生体特徴を有しているか否かの判断基準とするための情報（例えば特徴点）を抽出し、この生体特徴情報を用いて比較処理を行ない、類似度を算出するものとする。

【００８６】

この類似度は登録画像と一致しているほど高く、一致していないほど低いスコアである。つまり、このスコアが低い撮影画像は、監視画像として使用されても不正な照合に利用される可能性が低い。以下、監視画像取得の動作を説明する。なお、実施の形態３における制御部１０５は、本発明の監視画像選択処理部を構成している。また認証処理部２０３は本発明の比較部を構成している。

【００８７】

図１６は実施の形態３における監視画像取得の動作を示すフローチャートである。

【００８８】

まず、制御部１０５は認証開始スイッチ１１２が押されたか否かを判断する（Ｓ４０１）。

【００８９】

ステップＳ４０１の判断において、認証開始スイッチ４０１が押された場合（Ｓ４０１，ＹＥＳ）、制御部１０５はカメラ１０３に被写体を撮影させ、画像を取得し（Ｓ４０７）、認証処理部２０３にデータベース４０内の登録画像との照合処理をさせ（Ｓ４０８）、認証処理部２０３は照合の結果算出された最大類似度スコアが閾値以上であるか否かを判断する（Ｓ４０９）。

【００９０】

ステップＳ４０９の判断において、最大類似度スコアが閾値以上である場合（Ｓ４０９，ＹＥＳ）、認証処理部２０３は撮影画像が登録画像と一致すると判断し、照合ＯＫという結果を制御部１０５に返す（Ｓ４１０）。

【００９１】

一方、最大類似度スコアが閾値より小さい場合（Ｓ４０９，ＮＯ）、認証処理部２０３は撮影画像が登録画像と一致しないと判断し、照合ＮＧという結果を制御部１０５に返す（Ｓ４１１）。

【００９２】

また、ステップＳ４０１の判断において、認証開始スイッチが押されていない場合（Ｓ４０１，ＮＯ）、制御部１０５は前回の監視画像取得から一定時間が経過している否かを判断する（Ｓ４０２）。

【００９３】

ステップＳ４０２の判断において、前回の監視画像取得から一定時間が経過している場合（Ｓ４０２，ＹＥＳ）、制御部１０５はカメラ１０３に被写体を撮影させ、画像を取得し（Ｓ４０３）、認証処理部２０３にデータベース４０内の登録画像との照合処理をさせ（Ｓ４０４）、認証処理部２０３は照合の結果算出された最大類似度スコアが閾値以上であるか否かを判断する（Ｓ４０５：比較ステップ）。

【００９４】

ステップＳ４０５の判断において、最大類似度スコアが閾値以上である場合（Ｓ４０５，ＹＥＳ）、認証処理部２０３は処理を終了する。

【００９５】

一方、最大類似度スコアが閾値より小さい場合（Ｓ４０５，ＮＯ）、認証処理部２０３の認証結果に基づき制御部１０５は撮影画像を監視画像として監視画像出力部１１３へ撮影画像を送信する（Ｓ４０６：監視画像選択処理ステップ）。

【００９６】

なお、ステップＳ４０２の判断において、前回の監視画像取得から一定時間が経過していない場合（Ｓ４０２，ＮＯ）、制御部１０５は再び認証開始スイッチ１１２が押されたか否かを判断する（Ｓ４０１）。

【００９７】

以上の動作によって、認証装置１０は生体認証に有効な生体特徴を含まない監視画像を出力することができる。

【００９８】

なお、本実施の形態で図示したフローチャートやステップに示された各動作をコンピュ

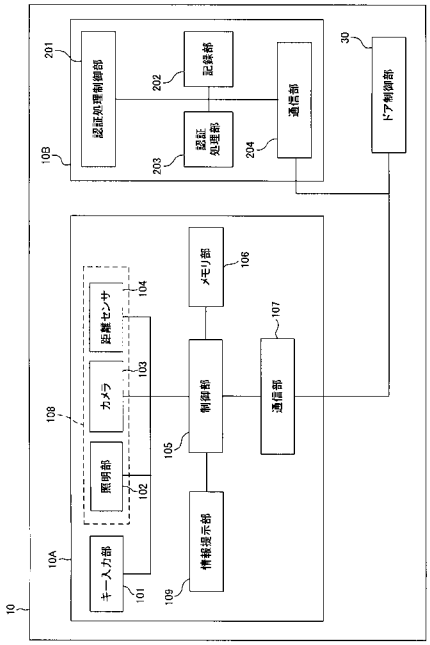
ータにより実行させるプログラムを提供することにより、本発明の撮影プログラムを提供することができる。これらプログラムはコンピュータにより読取可能な媒体に記録されてコンピュータにより実行させることができる。コンピュータは、パーソナルコンピュータのようなホスト装置、試験装置のコントローラ、記憶装置のＭＰＵやＣＰＵのようなコントローラなどを含む。ここで、コンピュータにより読取可能な媒体としては、ＣＤ－ＲＯＭやフレキシブルディスク、ＤＶＤディスク、光磁気ディスク、ＩＣカード等の可搬型記憶媒体や、コンピュータプログラムを保持するデータベース、或いは、他のコンピュータ並びにそのデータベースや、更に回線上の伝送媒体をも含むものである。

【産業上の利用可能性】

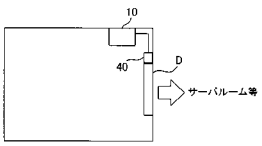
【００９９】

以上説明したように、本発明によれば、生体認証画像を撮影するカメラを防犯カメラとして使用し、生体認証に有効な生体特徴を含まない監視画像を出力することにより、生体特徴の流出を防ぐと共に生体認証における不正行為を監視することが可能になる。

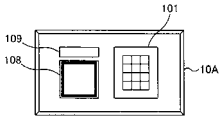
【図１】



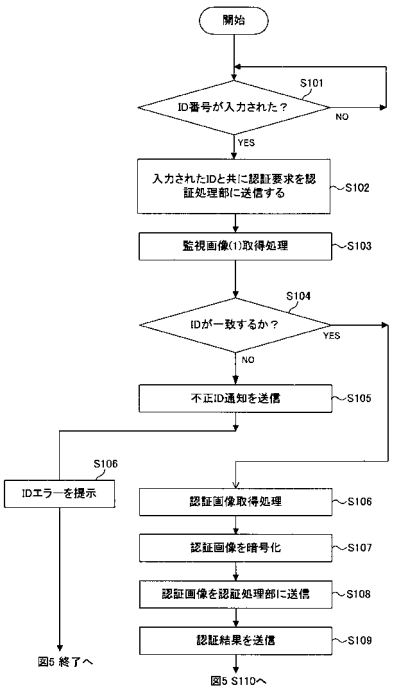
【図２】



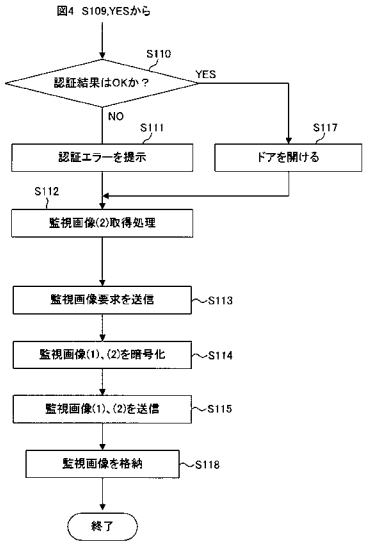
【図３】



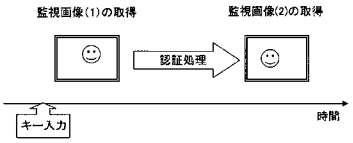
【図４】



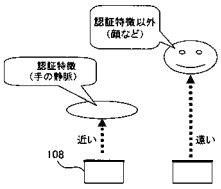
【図５】



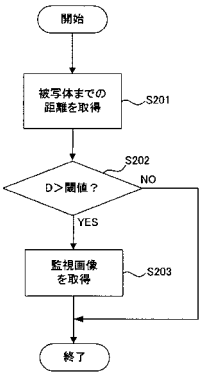
【図６】



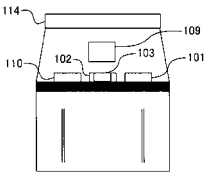
【図７】



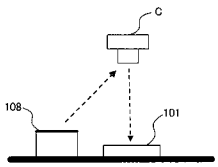
【図８】



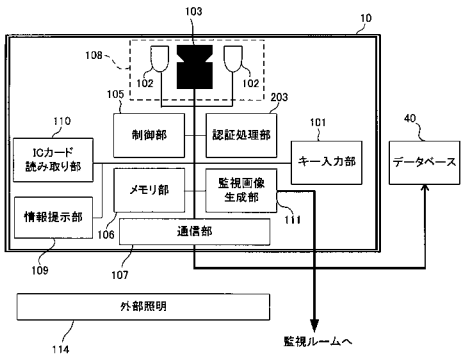
【図９】



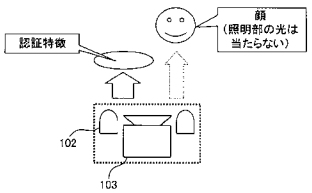
【図１０】



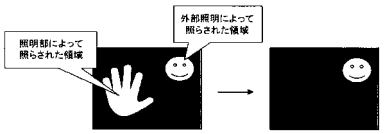
【図１１】



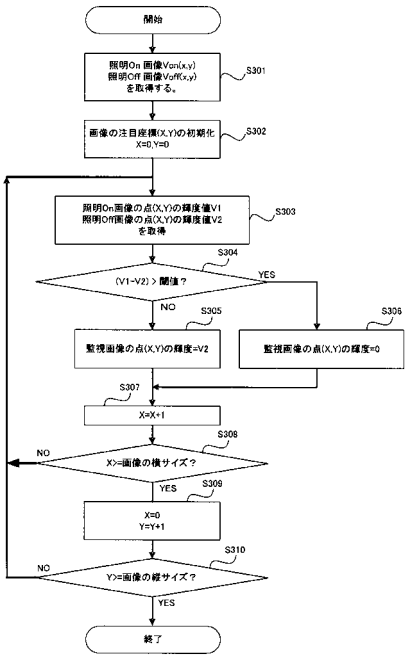
【図１２】



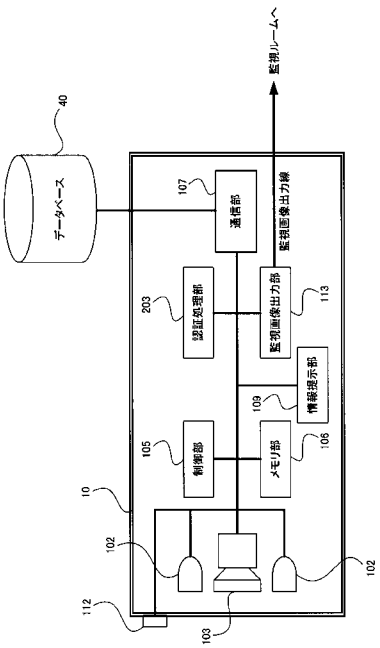
【図１３】



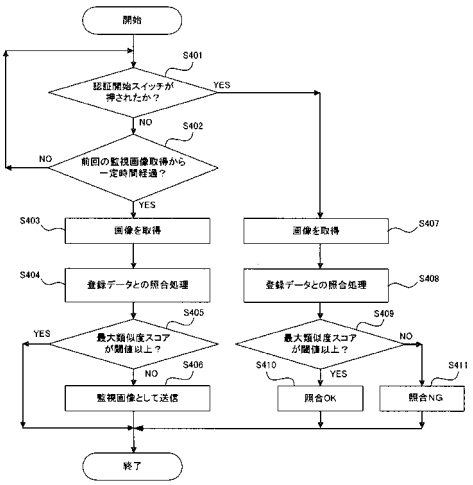
【図１４】



【図１５】


監視ルームへ
40
データベース
107
通信部
監視画像出力線
203
認証処理部
監視画像出力部
113
情報提示部
109
105
制御部
メモリ部
106
10
102
102
112
103

【図１６】


開始
S401
認証開始スイッチが押されたか？
YES
NO
S402
前回の監視画像取得から一定時間経過？
NO
YES
S403
画像を取得
S404
登録データとの照合処理
S405
最大類似度スコアが閾値以上？
YES
NO
S406
監視画像として送信
S407
画像を取得
S408
登録データとの照合処理
S409
最大類似度スコアが閾値以上？
NO
YES
S410
照合OK
S411
照合NG
終了

フロントページの続き

審査官　▲広▼島　明芳

(56)参考文献　特開２００６－１２００８４（ＪＰ，Ａ）
特開２００５－２４２７６６（ＪＰ，Ａ）
特開２００４－２９７５１８（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
G06T　1/00
H04N　5/225
G08B　25/00　- 25/04