

(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2021-24093

(P2021-24093A)

(43) 公開日 令和3年2月22日(2021.2.22)

(51) Int.Cl.	F I	テーマコード (参考)
B 4 1 J 29/38 (2006.01)	B 4 1 J 29/38 Z	2 C 0 6 1
B 4 1 J 29/00 (2006.01)	B 4 1 J 29/00 Z	2 H 2 7 0
G 0 3 G 21/00 (2006.01)	G 0 3 G 21/00 3 8 6	5 B 0 4 3
H 0 4 N 1/00 (2006.01)	H 0 4 N 1/00 3 5 0	5 C 0 6 2
G 0 6 T 7/00 (2017.01)	G 0 6 T 7/00 5 1 0 F	
審査請求 未請求 請求項の数 17 O L (全 20 頁)		

(21) 出願番号 特願2019-140820 (P2019-140820)
 (22) 出願日 令和1年7月31日 (2019.7.31)

(71) 出願人 000001007
 キヤノン株式会社
 東京都大田区下丸子3丁目30番2号
 (74) 代理人 100126240
 弁理士 阿部 琢磨
 (74) 代理人 100124442
 弁理士 黒岩 創吾
 (72) 発明者 田中 康智
 東京都大田区下丸子3丁目30番2号キヤ
 ノン株式会社内
 (72) 発明者 沼田 千堯
 東京都大田区下丸子3丁目30番2号キヤ
 ノン株式会社内
 Fターム(参考) 2C061 AP01 AP07 AQ06 CL08 CL10
 HJ07 HK23 HN15
 最終頁に続く

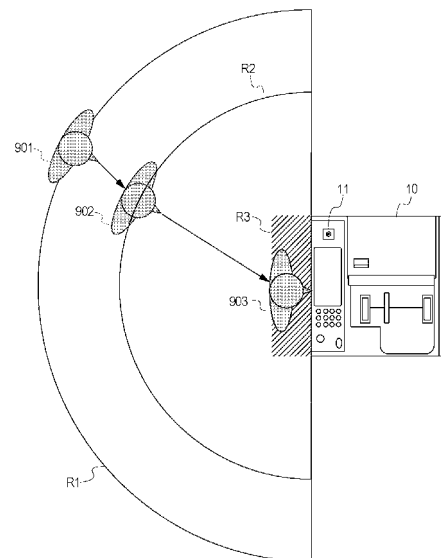
(54) 【発明の名称】 画像形成装置、画像形成装置の制御方法ならびにコンピュータプログラム

(57) 【要約】

【課題】 ユーザが画像形成装置の目の前に来る前にユーザ認証を完了させながら、認証されたユーザが画像形成装置の目の前に行く前にユーザに対応付けられた情報に基づく画面が表示されてしまうことを抑制することを目的とする。

【解決手段】 画像形成装置の前方の画像を撮像する撮像部と、画面を表示する表示部と、前記撮像部が撮像した画像からユーザの顔画像を取得する取得手段と、前記取得手段により取得されたユーザの前記顔画像を用いて前記画像形成装置が第1の距離よりも近くにいる前記ユーザを認証する認証手段と、前記認証手段により認証されたユーザを追尾する追尾手段と、前記追尾手段により追尾されたユーザが前記第1の距離よりも前記画像形成装置に近い第2の距離まで近づいたことに基づき、前記ユーザに対応する情報に基づく画面を前記表示部に表示させる制御手段と、を有することを特徴とする。

【選択図】 図9



【特許請求の範囲】**【請求項 1】**

画像形成装置の前方の画像を撮像する撮像部と、
画面を表示する表示部と、
前記撮像部が撮像した画像からユーザの顔画像を取得する取得手段と、
前記取得手段により取得されたユーザの前記顔画像を用いて前記画像形成装置が第 1 の距離よりも近くにいる前記ユーザを認証する認証手段と、
前記認証手段により認証されたユーザを追尾する追尾手段と、
前記追尾手段により追尾されたユーザが前記第 1 の距離よりも前記画像形成装置に近い第 2 の距離まで近づいたことに基づき、前記ユーザに対応する情報に基づく画面を前記表示部に表示させる制御手段と、を有することを特徴とする画像形成装置。 10

【請求項 2】

前記制御手段は、前記認証手段による認証が完了しても、前記追尾手段により追尾されたユーザが前記第 2 の距離まで近づくまで、前記認証されたユーザに対応する情報に基づく画面を表示しないことを特徴とする請求項 1 に記載の画像形成装置。

【請求項 3】

前記取得手段は、前記撮像部が撮像した第 1 の画像から顔画像を取得し、
前記認証手段は、前記取得手段が取得した前記顔画像に基づき認証を行い、
前記追尾手段は、前記第 1 の画像よりも後に前記撮像部により撮像された第 2 の画像において、前記認証手段により認証されたユーザを追尾することを特徴とする請求項 1 または 2 に記載の画像形成装置。 20

【請求項 4】

前記認証手段は、前記第 1 の画像から取得された顔画像を用いて認証を行い、前記第 2 の画像から取得された認証されたユーザに対応する顔画像を用いた認証を行わないことを特徴とする請求項 3 に記載の画像形成装置。

【請求項 5】

前記制御手段は、前記認証手段による認証の完了していないユーザが前記第 2 の距離まで近づいたことに応じて、前記ユーザを認証するための情報を入力する画面を前記表示部に表示することを特徴とする請求項 1 乃至 4 のいずれか一項に記載の画像形成装置。

【請求項 6】

前記認証手段は、前記取得手段により取得された所定の閾値よりも大きい顔画像を用いて認証を行うことを特徴とする請求項 1 乃至 5 のいずれか一項に記載の画像形成装置。 30

【請求項 7】

前記制御手段は、前記取得手段により取得された他の所定の閾値よりも大きい顔画像に基づき、前記認証手段により認証されたユーザに対応する情報に基づく画面を前記表示部に表示させることを特徴とする請求項 6 に記載の画像形成装置。

【請求項 8】

前記取得手段は、前記撮像部の撮像した画像から、第 1 の顔画像と第 2 の顔画像を取得し、
前記認証手段は、前記第 1 の顔画像と前記第 2 の顔画像をそれぞれ認証することを特徴とする請求項 1 乃至 7 のいずれか一項に記載の画像形成装置。 40

【請求項 9】

前記制御手段は、前記第 2 の距離よりも前記画像形成装置に近いユーザであって、前記画像形成装置に最も近い位置にいるユーザに対応する情報に基づく画面を前記表示部に表示させることを特徴とする請求項 1 乃至 7 のいずれか一項に記載の画像形成装置。

【請求項 10】

前記画像形成装置に最も近いユーザとは、前記取得手段により取得される顔画像の大きさが最も大きなユーザであることを特徴とする請求項 9 に記載の画像形成装置。

【請求項 11】

前記追尾手段により追尾されるユーザを識別するための識別情報と、前記追尾されてい 50

るユーザの前記認証手段による認証結果を対応づけて記憶する記憶手段をさらに有することを特徴とする請求項 1 乃至 10 のいずれか一項に記載の画像形成装置。

【請求項 12】

前記記憶手段は、前記認証手段による顔画像の認証に用いられるデータと、ユーザを識別する識別情報に対応づけて記憶し、

前記認証手段は、前記取得手段の取得した顔画像と前記記憶手段に記憶した前記データに基づき顔認証を行うことを特徴とする請求項 11 に記載の画像形成装置。

【請求項 13】

前記制御手段は、前記第 2 の距離まで近づいた第 1 のユーザに対応づけて記憶された表示言語の画面を前記表示部に表示させることを特徴とする請求項 1 乃至 12 のいずれか一項に記載の画像形成装置。

10

【請求項 14】

前記取得手段は、前記撮像部が撮像した画像から人の顔と特定された領域を含む多角形を顔画像として取得することを特徴とする請求項 1 乃至 13 のいずれか一項に記載の画像形成装置。

【請求項 15】

画像形成装置の前方の画像を撮像する撮像部と、

画面を表示するための表示部と、

前記撮像部が撮像した画像からユーザの顔画像を取得する取得手段と、

前記取得手段により取得されたユーザの前記顔画像であって、第 1 の距離よりも前記画像形成装置に近いユーザの前記顔画像を用いた認証結果を受信する受信手段と、

20

前記受信手段により前記認証結果が受信されたユーザを追尾する追尾手段と、

前記追尾手段により追尾されたユーザが前記画像形成装置から第 2 の距離まで近づいたことに基づき、前記ユーザに対応する情報に基づく画面を前記表示部に表示させる制御手段と、を有することを特徴とする画像形成装置。

【請求項 16】

画像形成装置の前方の画像を撮像する撮像部と、

画面を表示するための表示部と、を有する画像形成装置の制御方法において、

前記撮像部が撮像した画像からユーザの顔画像を取得する取得工程と、

前記取得工程において取得されたユーザの前記顔画像であって、第 1 の距離よりも前記画像形成装置に近いユーザの前記顔画像を用いて前記ユーザを認証する認証工程と、

30

前記認証工程において認証されたユーザを追尾する追尾工程と、

前記追尾工程において追尾されたユーザが前記第 1 の距離よりも前記画像形成装置に近い第 2 の距離まで近づいたことに基づき、前記ユーザに対応する情報に基づく画面を前記表示部に表示させる制御工程と、を有することを特徴とする画像形成装置の制御方法。

【請求項 17】

請求項 16 に記載の画像形成装置の制御方法をコンピュータが実現するためのコンピュータプログラム。

【発明の詳細な説明】

【技術分野】

40

【0001】

本発明は、画像形成装置、画像形成装置の制御方法ならびにコンピュータプログラムに関する。

【背景技術】

【0002】

コピーやプリントなどの機能を有する画像形成装置では、ユーザがユーザ ID やパスワードを入力し、入力されたユーザ ID、パスワードを使った認証処理を行うことが知られている。上記の画像形成装置では、ユーザ認証を行い、ユーザが画像形成装置にログインするとログインしたユーザのジョブを印刷するための画面や、ログインしたユーザ用にカスタマイズされた画面を表示する。ユーザ認証には、ユーザ ID やパスワードを使用した

50

認証に加え、ＩＣカードや顔認証など様々な認証方法が用いられている。

【０００３】

特許文献１にはカメラで撮像した画像を用いた顔認証による画像形成装置の認証処理が記載されている。顔認証によるユーザ認証にはある程度の時間を要するため、ユーザが画像形成装置の目の前に来てから、画像の撮像と認証処理をするとユーザは画像形成装置の前で認証処理が完了するまで画像形成装置を操作することができない。そこで、特許文献１に記載の画像形成装置では、ユーザがあらかじめ決められた領域内に入ってきたときに撮像した画像を用いて顔認証を行う。これによりユーザはユーザＩＤやパスワードの入力を行わなくてもユーザが画像形成装置の前に到達するときにはユーザ認証を完了することができる。

10

【先行技術文献】

【特許文献】

【０００４】

【特許文献１】特開２０１９－５７０３６号公報

【発明の概要】

【発明が解決しようとする課題】

【０００５】

特許文献１では、ユーザが画像形成装置の目の前に来たときにはユーザ認証が完了しているように、ユーザが画像形成装置からある程度離れた場所にいるタイミングでユーザ認証が開始される。そのため、ユーザ認証が開始されてから、実際にユーザが画像形成装置の目の前に到達するまでの間に時間差が生じる。このとき、ユーザ認証が完了したのち、すぐに画像形成装置が認証されたユーザに対応する情報を使った画面表示を行うとする。すると、認証されたユーザよりも先に他のユーザが画像形成装置の前に来てしまった場合に認証したユーザに対応する情報に基づく画面が他のユーザに見られてしまう可能性がある。

20

【０００６】

請求項１に記載の画像形成装置は、ユーザが画像形成装置の目の前に来る前にユーザ認証を完了させながら、認証されたユーザが画像形成装置の目の前に行く前にユーザに対応付けられた情報に基づく画面が表示されてしまうことを抑制することを目的とする。

【課題を解決するための手段】

30

【０００７】

本願請求項１に記載の画像形成装置は、画像形成装置の前方の画像を撮像する撮像部と、画面を表示する表示部と、前記撮像部が撮像した画像からユーザの顔画像を取得する取得手段と、前記取得手段により取得されたユーザの前記顔画像を用いて前記画像形成装置が第１の距離よりも近くににいる前記ユーザを認証する認証手段と、前記認証手段により認証されたユーザを追尾する追尾手段と、前記追尾手段により追尾されたユーザが前記第１の距離よりも前記画像形成装置に近い第２の距離まで近づいたことに基づき、前記ユーザに対応する情報に基づく画面を前記表示部に表示させる制御手段と、を有することを特徴とする。

【発明の効果】

40

【０００８】

本発明によれば、ユーザが画像形成装置の目の前に来る前にユーザ認証を完了させながら、認証されたユーザが画像形成装置の目の前に行く前にユーザに対応付けられた情報に基づく画面が表示されてしまうことを抑制することができる。

【図面の簡単な説明】

【０００９】

【図１】本実施例に係る、画像形成装置の外観の一例を示した図である。

【図２】本実施例に係る、画像形成装置のカメラユニット１１の撮像したカメラ画像による顔データの取得ができる領域、顔認証ができる領域を示す模式図である。

【図３】本実施例に係る、画像形成装置の側面図である。

50

【図４】本実施例に係る、画像形成装置の構成を示すハードウェアブロック図である。

【図５】本実施例に係る、カメラユニットが撮像するカメラ画像と、カメラ画像解析部４１０の解析を示す模式図である。

【図６】本実施例に係る。カメラ画像解析部４１０が顔データに基づき、ユーザのいる領域を推定する方法を示す模式図である。

【図７】表示部２０２に表示される画面の一例を示す図である。

【図８】本実施例に係る、顔認証処理を説明するためのフローチャートである。

【図９】本実施例において、ユーザが画像形成装置１０に近づいてきたときの画像形成装置１０の動作を説明するための模式図である。

【図１０】本実施例において、ユーザが画像形成装置１０の前を通りすぎたときの画像形成装置１０の動作を説明するための模式図である。

10

【図１１】本実施例において、複数のユーザが画像形成装置に近づいてきた場合の画像形成装置１０の動作を説明するための模式図である。

【発明を実施するための形態】

【００１０】

以下、本発明を実施するための形態について図面を用いて例示的に詳しく説明する。ただし、この実施の形態に記載されている構成要素はあくまで例示であり、この発明の範囲をそれらのみに限定する趣旨のものではない。

【００１１】

< 画像形成装置外観 >

20

図１は、本実施例の画像形成装置１０の外観図である。画像形成装置１０は、プリント機能、スキャナ機能、コピー機能、ＦＡＸ機能などの複数の機能を有している。画像形成装置１０は、カメラユニット１１を備え、カメラユニット１１は画像形成装置１０の前方に向けて取り付けられる。

【００１２】

カメラユニット１１は、画像形成装置１０の前方の画像を撮像する撮像部として機能する。カメラユニット１１は画像形成装置１０のメインコントローラによる制御で画像を撮像する。

【００１３】

画像形成装置１０は、画像形成装置１０に近づくユーザを、カメラユニット１１を用いて撮影し、顔認証を実施する。顔認証結果が所定の条件を満たす場合に画像形成装置に自動的にログインさせる。なお、以下の説明においては、カメラユニット１１が撮像した画像をカメラ画像と称する。

30

【００１４】

< 撮像範囲および人操作範囲 >

はじめに、図２、図３を用いて、カメラユニット１１を用いて顔画像の抽出や顔画像による顔認証を行うことができる領域について説明する。

【００１５】

図２は、画像形成装置１０のカメラユニット１１が撮像した画像から顔画像を抽出することができる領域、および、抽出した顔画像に基づく顔認証を行うことができる領域を示した図である。図２は、画像形成装置１０およびその周辺を、画像形成装置１０の高さ方向上側から見たものを示している。

40

【００１６】

図３は、画像形成装置１０のカメラユニット１１により撮像が可能な範囲および、認証に関わる範囲を説明するための側面図である。図３は、画像形成装置１０およびその周辺を、画像形成装置の側方から見たものを示している。なお、図３の人物Ｈは画像形成装置１０が認証するユーザである。

【００１７】

図２において、領域Ｒ１はカメラユニット１１が撮像した画像から顔画像を抽出することができる領域である。この領域Ｒ１は、画像形成装置１０を高さ方向上側から見た時に、

50

中心角が180度程度に設定された扇形を呈している。画像形成装置10はR1よりも内側にいるユーザについて顔画像を抽出することができる。

【0018】

領域R2はカメラユニット11が撮像した画像に含まれる顔画像を使った顔認証を行うことができる領域である。領域R2は、画像形成装置10を高さ方向から見たときに、中心核が180度設定された扇型であり、領域R1よりも小さい扇型を呈している。

【0019】

続いて、領域R3は、画像形成装置10を操作するユーザが検出される領域である。画像形成装置10の前方に形成され、高さ方向上側から見たときに、矩形を呈している。この例に置いて、この矩形範囲における幅方向の長さは、画像形成装置10の幅方向の長さと同じである。また、領域R3の全域は、領域R1およびR2の内側に位置する。また、領域R3は、ユーザが表示部202を確認および操作することが可能な範囲である。

【0020】

また、本実施例では、カメラユニット11が撮像した画像から抽出される顔画像に基づいて、ユーザが領域R1、R3、R2のいずれの領域にいるかを判定する。なお、人物Hがいずれの領域にいるかを判定する詳細な検出方法については図6を用いて後述する。

【0021】

なお、領域R1、R2の中心角については、180度以外であっても構わない。

【0022】

図3に示すように、カメラユニット11はユーザの顔画像を撮像できる向きになるよう、画像形成装置10の表示部横等に配置される。

【0023】

本実施例の画像形成装置10では、後述するように、この画像形成装置10に近づいてくる人物Hの顔をカメラユニット11で撮像して得たカメラ画像を用いて、画像形成装置10の使用を許可するための認証を行う。

【0024】

< 画像形成装置のブロック図 >

図4は、本発明に係る、画像形成装置10の構成を示すブロック図である。

【0025】

画像形成装置10は、画像形成装置10の動作を統括するコントローラ100、操作部200、スキャナ部400及びプリンタ部500を備えている。

【0026】

コントローラ100は操作部200、スキャナ部400及びプリンタ部500と通信可能である。コントローラ100はCPU110、RAM111、ROM112、入出力I/F114、及びLANコントローラ115を備え、それらはシステムバス116に接続されている。また、コントローラ100はHDD117、デバイスI/F118及び画像処理部119を備え、それらはシステムバス116に接続されている。さらに、コントローラ100はカメラ画像解析部410、認証部411、認証結果管理部412を備え、それらはシステムバス116に接続されている。

【0027】

CPU110は、ROM112に記憶された制御プログラム等に基づいて接続中の各種デバイスとのアクセスを統括的に制御すると共に、コントローラ100で実行される各種処理についても統括的に制御する。CPU110と操作部200およびカメラユニット11は入出力I/F114を介して通信を行う。また、CPU110とスキャナ部400、プリンタ部500はデバイスI/F118を介して通信を行う。RAM111はCPU110が動作するためのシステムワークメモリであり、画像データを一時記憶するためのメモリでもある。本実施例では、CPU110がカメラユニット11と通信し、カメラユニット11による画像の撮像を制御する。

【0028】

ROM112には、装置のブートプログラムなど各種プログラムが格納されている。

10

20

30

40

50

【 0 0 2 9 】

L A Nコントローラ 1 1 5 は L A Nに接続される図示しない P C (P e r s o n a l C o m p u t e r) や、外部の認証サーバ等の外部装置と情報の送受信を行う。

【 0 0 3 0 】

H D D 1 1 7 はハードディスクドライブでありシステムソフトウェアや画像データを格納する。

【 0 0 3 1 】

画像処理部 1 1 9 は原稿の読み取りや印刷に伴う画像処理を行うためのものであり、R A M 1 1 1 に記憶された画像データを読み出し、J P E G、J B I Gなどの圧縮または伸張および、色調整などの画像処理を行う。

10

【 0 0 3 2 】

操作部 2 0 0 はユーザが画像形成装置 1 0 を制御するためのものであり、画像形成装置 1 0 とユーザ間での情報の入出力を行う。また、操作部 2 0 0 は操作部 C P U 2 0 1、L C D や L E D 等で構成される表示部 2 0 2、及びタッチパネル、ハードウェアキー等で構成される入力部 2 0 3 を備える。さらに、操作部 2 0 0 は N F C リーダライタ、B l u e t o o t h (登録商標) モジュール等のユーザの持つ携帯端末とデータをやり取りするためのインターフェースを備えていてもよい。

【 0 0 3 3 】

スキャナ部 4 0 0 は原稿から光学的に画像を読み取り画像データを生成する画像入力デバイスである。

20

【 0 0 3 4 】

プリンタ部 5 0 0 は電子写真方式に従って記録媒体 (用紙) に画像を形成する画像出力デバイスである。

【 0 0 3 5 】

カメラユニット 1 1 は、先述したように画像形成装置 1 0 の前方の画像を撮像する機能を有している。画像形成装置 1 0 に近づくユーザを、カメラユニット 1 1 を用いて撮影する。

【 0 0 3 6 】

カメラ画像解析部 4 1 0 は、カメラユニット 1 1 で撮像したカメラ画像の解析を行うためのものモジュールである。カメラ画像解析部 4 1 0 は、カメラ画像に含まれる人物の顔の検出および、検出した人物の顔の追尾を行う機能を有する。またカメラ画像解析部 4 1 0 は、カメラ画像から抽出した人物の顔領域の画像を認証部 4 1 1 に送付する機能を有する。ここでカメラ画像に含まれる人物の顔領域を抽出した画像を以後「顔データ」と称する。ここで、カメラ画像解析部 4 1 0 における顔検出、顔追尾、および顔領域の切り出しに関して図 5 を用いて例示的に説明する。

30

【 0 0 3 7 】

図 5 は、本実施例に係るカメラ画像解析部 4 1 0 による、カメラ画像に含まれる人物の顔検出、顔追尾、および人物の顔領域を切り出す機能を説明するための説明図である。

【 0 0 3 8 】

図 5 において、A 1 はカメラユニット 1 1 が取得したカメラ画像である。カメラ画像内 A 1 には 2 人の人物 H 1 および H 2 が写っている。

40

【 0 0 3 9 】

カメラ画像解析部 4 1 0 はカメラユニット 1 1 からカメラ画像を受け取り、カメラ画像から人物の顔データ F 1、F 2 を抽出する。カメラ画像解析部 4 1 0 は後述する方法で抽出した顔画像を用いた顔認証が可能であるか否かを判定する。顔画像による顔認証が可能であると判定した場合、顔データを認証部 4 1 1 に送信する。

【 0 0 4 0 】

また、検出した 2 人の人物に各々を識別する I D 5 1 0 および 5 2 0 (以後、「追尾 I D」と称する) を割り当て、検出した人物の追尾を行う。本実施例において、人物の追尾とは、カメラユニット 1 1 から取得する複数のカメラ画像において、同じユーザを抽出す

50

る処理を指す。

【 0 0 4 1 】

ここで、顔検出、追尾機能に関しては、一般に、画像処理・画像解析および機械学習機能を持つライブラリとして、オープンソースのOpenCVが一般に知られており、これらのライブラリを利用することにより、カメラ画像解析部410の機能が実現される。

【 0 0 4 2 】

図4の画像形成装置10の構成を示すブロック図の説明に戻る。

【 0 0 4 3 】

認証部411は、カメラ画像解析部410が抽出した顔データを受信して顔認証を実施する。顔認証を終了したのち、認証結果をカメラ画像解析部410に返す。認証部411は複数のユーザの顔データを管理するための図示しない顔データ管理部を有する。顔データ管理部には、例えば表1のように複数のユーザの顔データを管理する顔データ管理テーブルが記憶されている。表1において、ユーザNoは認証部411が管理するユーザの通し番号である。ユーザIDは当該ユーザを識別するための識別情報である。パスワードはユーザが画像形成装置10にログインするときに使用するパスワードである。認証用顔データは認証部411が顔認証に利用する顔データのファイル名を示している。

【 0 0 4 4 】

【表1】

ユーザNo	ユーザID	パスワード	認証用顔データ
0	tanaka	xxxx	tanaka_facedata.jpg
1	yamada	yyyy	yamada_facedata.jpg
2	suzuki	zzzz	suzuki_facedata.jpg

【 0 0 4 5 】

認証部411は、カメラ画像解析部410から顔データと共に顔認証要求を受ける。認証部411は顔データを解析し、受信した顔データと顔データ管理部に記憶された認証用顔データを比較し、受信した顔データが記憶されたいずれのユーザの顔かを判定する。認証部411が該当する人物の顔データが顔データ管理部に登録されていたと判定すると、認証部411は当該人物のユーザIDと認証が完了したことを示す通知を顔認証結果として認証結果管理部412に送信する。受け取った顔データに対応する認証用顔データが顔データ管理部に登録されていなかった場合、認証部411は認証が失敗した旨を認証結果管理部412に送信する。

【 0 0 4 6 】

認証結果管理部412は、認証部411での認証により取得した認証結果を格納する。認証結果管理部412は、認証部411から受け取った認証結果を表2に示す認証結果テーブルに記憶する。

【 0 0 4 7 】

【表2】

追尾ID	ユーザID
0	yamada
1	suzuki
3	unknown

【 0 0 4 8 】

認証結果テーブルにおいて、追尾IDはカメラ画像解析部410が抽出した顔データに

対して割り当てる識別情報である。ユーザIDはカメラ画像解析部410が抽出した顔データに基づき認証部411により認証されたユーザのユーザIDである。認証部411による認証がなされていない場合、認証結果管理部412は、カメラ画像解析部410が割り当てた追尾IDと、認証が完了していないことを示す情報に対応づけて認証結果テーブルに登録する。たとえば、表3では認証されていないユーザを“unknown”として登録する。追尾ID3の顔データのユーザが画像形成装置10に近づけ認証されると、ユーザIDが“unknown”から認証されたユーザのユーザIDに更新される。認証部411による認証がなされていない場合とは、たとえば、ユーザが図2の領域R2の外側であって領域R1よりも内側にいる場合や、カメラ画像解析部410が抽出した顔データに対応するユーザが顔データ管理部に登録されていない場合などである。

10

【0049】

なお、本実施例では、画像形成装置10内部に認証部411を持つ構成として説明するが、認証部411はLANやインターネットを介して接続される装置外部の認証サーバであってもよい。

【0050】

ログイン処理部413は、認証部411により認証されたユーザが画像形成装置10にログインするための処理を実行する処理部である。ログイン処理部413は、HDD117に記憶されたログイン情報テーブルを読み出し、認証されたユーザに対応する表示画面を表示部202に表示する。

20

【0051】

以下に示す表3はログイン情報テーブルの一例を示す図である。

【0052】

【表3】

ユーザ番号	ユーザID	表示言語	トップ画面	コピーデフォルト設定	スキャンデフォルト設定	画面の色反転
0	tanaka	日本語	メニュー画面	白黒、倍率50%、2in1	—	0
1	yamada	英語	コピー画面	白黒	カラー、両面、300dpi*300dpi	0
2	suzuki	日本語	スキャン画面	—	—	1

【0053】

ユーザ番号は、認証部411により管理される顔認証データテーブルのユーザ番号と共通する番号が割り振られている。ユーザIDは、顔認証データテーブルと共通のユーザIDが記憶されている。表示言語は当該ユーザ番号、ユーザIDのユーザがログインしたときに表示部202の画面表示に用いられる言語である。たとえばユーザID“tanaka”のユーザがログインした場合、表示部202は日本語表記の画面を表示する。一方で、ユーザID“yamada”のユーザがログインした場合、表示部202は英語表記の画面を表示する。トップ画面はユーザがログイン後最初に表示される画面の情報である。メニュー画面は、図7(b)で示すような、機能選択画面であり、ログインした後や、ユーザが不図示のホームボタンを選択したときに表示される画面である。コピー画面は、図7(a)に示すようなコピー機能の設定画面である。コピー画面では、コピー機能に関する複数の設定項目の設定を行うことができる。スキャン画面は、ユーザが原稿をスキャンするスキャン機能の設定画面である。スキャン画面ではスキャン機能に関する複数の設定項目の設定を行うことができる。

30

40

【0054】

コピーデフォルト設定は、ユーザがログインしたのち図7(c)に示すコピー画面を初めて開くときのコピー画面の設定値である。ログイン情報テーブルには、コピーに関する設定項目のうち、画像形成装置10のデフォルト設定から異なる値に設定が変更されている設定項目の設定値が記憶されている。スキャンデフォルト設定は、ユーザが画像形成装置10にログインして最初にスキャン画面を表示するときに表示される設定値である。ここでは画像形成装置10のデフォルト値から変更されている設定値のみがログイン情報テ

50

ーブルに記憶されているとする。画面の色反転は、表示部 202 に表示される画面の色に関する設定値である。色反転機能は、画面内の白い領域を黒く表示し、画面内の黒い領域を白で表示する機能である。“0”は色反転しないことを示しており、“1”は色反転することを示している。なお、本実施例では、ログイン情報テーブルは、画像形成装置 10 の HDD 117 に記憶されているとしたが、画像形成装置 10 の他のメモリや、画像形成装置 10 とネットワークを介して接続されるサーバ内に記憶されるとしてもよい。

【0055】

また、本実施例では、カメラ画像からの人物の顔検出および、追尾機能を全て画像形成装置 10 内部のカメラ画像解析部 410 が行う構成として説明するが、一部の機能をカメラユニット 11 側に持つ構成であってもよい。

【0056】

< 画像形成装置と人物の距離に関する説明 >

次に、カメラユニット 11 が取得するカメラ画像から、ユーザが領域 R1、R3、R2 のいずれの領域にいるかを判定するための方法を説明する。

【0057】

図 6 (a) は、ユーザ H1 が画像形成装置 10 から D1 の位置にあり、ユーザ H2 が画像形成装置 10 から D2 の距離にいる場合を画像形成装置 10 の上方から見たときの図である。図のようにユーザ 602 はユーザ 601 よりも画像形成装置 10 の近くにいる。この時、カメラユニット 11 が撮像する画像は図 5 に示したようになる。

【0058】

図 6 (b) はカメラユニット 11 が撮像した画像から抽出されたユーザ H1 の顔データである。カメラ画像解析部 410 はユーザ H1 の顔の写っている領域を含む矩形を顔データとして抽出する。図 6 (c) はカメラユニット 11 が撮像した画像から抽出されたユーザ H2 の顔データである。カメラ画像解析部 410 は、ユーザ H2 の顔の写っている領域を含む矩形を顔データとして抽出する。顔データを取得する際には、カメラ画像のうち顔の写っている領域全体を含む多角形であればよい。図 6 (b)、図 6 (c) からわかるように、距離が近いユーザの方が顔データのサイズが大きくなる。画像形成装置 10 の CPU 110 はカメラ画像解析部 410 が抽出した顔データの高さや幅から顔データの面積を求める。CPU 110 は求めた面積とあらかじめ設定された閾値を比較することでユーザが領域 R1、R3、R2 のいずれの領域にいるかを判定する。

【0059】

もちろん画像形成装置 10 から人物までの距離の判断手法に関して、図 6 で説明した方法は一例であり、他の公知の方法により距離を検出することも可能である。例えば、超音波センサ等の物体までの距離が検出可能なセンサを使用した距離検出や、赤外アレイセンサ等を使用した距離検出方法を本実施例に用いることも可能である。

【0060】

< 表示部に表示される画面の説明 >

図 7 (a) ~ (b) は、画像形成装置 10 の表示部 202 に表示される画面の一例を示している。本実施例において、画像形成装置 10 は認証部 411 による顔認証処理において、認証用の顔データを登録していないと判断されたユーザにはパスワード認証を促す。

【0061】

図 7 (a) は、ユーザが画像形成装置 10 に接近し、認証部 411 による顔認証処理において、顔画像データが登録されていないと判断されたユーザに対し、パスワード認証を促す画面の一例を示している。領域 701 はユーザがユーザ ID を入力する領域である。ユーザは表 1 のユーザ ID を領域 701 に入力する。領域 702 はユーザがパスワードを入力する領域である。ユーザは表 1 に記載のパスワードを入力する。ユーザはユーザ ID とパスワードの入力を完了したのち「ログイン」703 を選択する。これにより認証部 411 による認証処理が行われる。この画面は、画像形成装置 10 に近づいたユーザの顔データによる認証が行えない場合や、表 1 にユーザ ID、パスワードが登録されているものの認証用顔データが登録されていない場合などに有効である。

【 0 0 6 2 】

図 7 (b) (c) は、ユーザが画像形成装置 1 0 に接近したユーザの顔データによる認証完了している場合や、図 7 (a) の画面において「ログイン」7 0 3 が選択されログイン処理がなされた場合に表示部 2 0 2 に表示される画面である。図 7 (b) は、ユーザ No : 0 のユーザがログインした場合に表示される画面である。図 7 (c) はユーザ No : 1 のユーザがログインした場合に表示される画面である。

【 0 0 6 3 】

ユーザの認証後に表示部 2 0 2 に表示される画面はユーザに対応するユーザ固有の機能選択画面である。領域 7 0 4 にはログインしたユーザのユーザ ID が表示され、領域 7 0 5 にはログインしたユーザのユーザ No が表示される。画像形成装置 1 0 において、ユーザは画面の表示に用いられる言語や、ログイン直後に表示される画面の種類や機能選択画面に表示されるボタンの数や種類をユーザごとにカスタマイズすることができる。たとえば、ユーザ ID : 1 のユーザがログインした場合には、ユーザが領域 R 3 内にいる、または、図 7 (a) で示す画面で「ログイン」7 0 3 を選択すると、図 7 (c) に示すように英語のコピー設定画面が表示される。このように、画像形成装置 1 0 はユーザごとに適した画面表示を行うことができる。

【 0 0 6 4 】

< 顔認証フロー >

次に、図 8 を用いて、本実施例における画像形成装置 1 0 の顔認証処理、および、ログイン時の画面表示の制御について説明する。図 8 は、いずれのユーザもログインしていない場合に画像形成装置 1 0 が実行する処理を示すフローチャートである。本処理は、ROM 1 1 2 に格納されている本処理に対応するプログラムを RAM 1 1 1 へ展開し、CPU 1 1 0 が当該プログラムを実行することにより、実現される。なお、図 8 に記載の処理は画像形成装置 1 0 の電源がオンになったのちに開始される。図 8 に記載の処理は、画像形成装置 1 0 の電源オン時に加え、ユーザが画像形成装置 1 0 からログアウトしたのちにも実行される。

【 0 0 6 5 】

CPU 1 1 0 はカメラユニット 1 1 に対してカメラ画像の取得要求を送信し、カメラユニット 1 1 が撮像したカメラ画像を取得する (S 8 0 1)。CPU 1 1 0 はカメラユニットにカメラ画像取得要求を送信する。カメラユニット 1 1 はカメラ画像取得要求に基づき画像を取得し、取得した画像を CPU 1 1 0 に送信する。

【 0 0 6 6 】

CPU 1 1 0 は S 8 0 1 で取得したカメラ画像内に顔データがあるか否かを判定する (S 8 0 2)。CPU 1 1 0 はカメラユニット 1 1 から取得した画像をカメラ画像解析部 4 1 0 に送信し、カメラ画像から顔データの抽出を指示する。カメラ画像解析部 4 1 0 はカメラ画像から顔データを抽出する。カメラ画像解析部 4 1 0 はカメラ画像から顔データを抽出したか否かを CPU 1 1 0 に返す。CPU 1 1 0 はカメラ画像解析部 4 1 0 からの情報に基づき、カメラ画像内に顔データがあるか否かを判定する。カメラ画像内に顔データがない場合、CPU 1 1 0 は認証部 4 1 1 が管理する認証結果テーブルをクリアし、S 8 0 1 に処理を戻す (S 8 0 3)。

【 0 0 6 7 】

CPU 1 1 0 はカメラ画像から顔データを一つ選択する (S 8 0 4)。そして、CPU 1 1 0 は選択した顔データの面積が閾値 TH 1 よりも大きいかなんかを判定する (S 8 0 5)。TH 1 は、ユーザが領域 R 2 にいるかなんかを判定するための閾値である。顔データの面積が TH 1 よりも大きい場合、CPU 1 1 0 は選択した顔データのユーザが領域 R 2 にいるとし、処理を S 8 0 9 に進める。顔データの面積が TH 1 よりも小さい場合、カメラ画像に含まれる顔データの大きさが小さく、顔認証を行うことができない。そこで、CPU 1 1 0 は S 8 0 6 以降の処理を実行する。

【 0 0 6 8 】

CPU 1 1 0 は認証結果管理部 4 1 2 の管理する認証結果テーブルを参照し、選択した

10

20

30

40

50

顔データのユーザに追尾IDが割り振られているか否かを判定する(S806)。追尾IDが割り振られている場合、CPU110はS808に処理を進める。追尾IDが割り振られていない場合、CPU110はカメラ画像解析部410を制御し、当該顔データに追尾IDを付与し、付与した追尾IDを認証結果管理部412に通知して認証結果テーブルに追尾IDを登録する(S807)。このとき、当該顔データを用いた認証が完了していないため、CPU110はユーザIDを“unknown”として認証結果テーブルにレコードを追加する。

【0069】

CPU110は、カメラ画像内にS804で選択したことの無い顔データが含まれているか否かを判定する(S808)。カメラ画像に含まれるすべての顔データを選択済みであれば、CPU110は処理をS801に戻す。カメラ画像内に選択していない顔データが含まれている場合、CPU110はS804に処理を進める。1枚のカメラ画像に対して2回目以降のS804の処理では、CPU110はこれまでに選択していない顔データを選択するものとする。

10

【0070】

CPU110は選択した顔データが認証済みの顔データであるか否かを判定する(S809)。CPU110は認証結果管理部412を制御し認証結果テーブルを参照する。CPU110は認証結果テーブルにおいて、選択した顔データに付与されている追尾IDに対応するユーザIDが“unknown”でなければ、当該顔データは認証済みの顔データであると判定する。選択した顔データが認証済みの顔データである場合、CPU110はS814に処理を進める。S809で認証済みのユーザの顔データか否かを判定することにより、認証済みのユーザの顔データを使った認証を複数回行ってしまふことを防ぐことができる。これにより画像形成装置10の処理負荷を減らし、カメラ画像に含まれる複数人の顔データの認証に必要な時間を短くすることができる。

20

【0071】

選択した顔データが認証済みの顔データでない場合、CPU110は顔データを用いてユーザ認証を行う(S810)。S810において、CPU110はカメラ画像解析部410を制御し、顔データを認証部411に送信させる。認証部411はカメラ画像解析部410から受信した顔データと顔データ管理テーブルの情報を用いて、顔認証を行う。顔認証が成功した場合、CPU110は認証部411から顔認証の結果として認証されたユーザのユーザIDを受け取る。顔認証が失敗した場合、CPU110は認証部411から顔認証が失敗した旨を示す通知を受け取る。

30

【0072】

CPU110は認証部411から受信した情報に基づき、顔認証が成功したか否かを判定する(S811)。認証が成功している場合、CPU110は認証結果管理部412を制御し、認証結果テーブルの当該顔データの追尾IDに対応するユーザIDを認証されたユーザのユーザIDで更新する(S812)。一方で、認証が失敗した場合、CPU110は認証結果管理部412を制御し、認証失敗を示す情報で認証結果テーブルの当該顔データの追尾IDに対応するユーザIDを更新する(S813)。例えば、認証が失敗した場合、CPU110は顔認証に用いた顔データの追尾IDに対応するユーザIDを“failure”とする。これにより、CPU110は認証結果テーブルを参照することで、認証処理済みであるが認証に失敗したユーザを識別することができる。

40

【0073】

CPU110は、カメラ画像内に一度も選択されていない顔データがあるか否かを判定する(S814)。一度も選択されていない顔データがある場合、CPU110は処理をS804に戻す。

【0074】

カメラ画像に含まれるすべての顔データを選択済みの場合、CPU110はS815に記載の処理を実行する。

【0075】

50

CPU110は、カメラ画像に含まれる顔データのなかに面積が閾値TH2よりも大きな顔データがあるか否かを判定する(S815)。閾値TH2は領域R3内にユーザがいるか否かを判定するための閾値である。カメラ画像に含まれる顔データのなかに面積がTH2よりも大きい顔データがある場合、CPU110は領域R3内にユーザがいると判定しS818に処理を進める。

【0076】

カメラ画像に含まれる顔データの面積がいずれもTH2よりも小さい場合、CPU110はこれまで追尾していた顔データあって、カメラ画像から抽出されなくなった顔データがあるか否かを判定する(S816)。CPU110はカメラ画像解析部410を制御し、これまでに追尾IDを付与した顔データであって、カメラ画像から抽出された顔データに含まれていない顔データがあるか否かを判定する。S816において、CPU110は、一度、領域R1の内側に入ったものの、画像形成装置10の近くを通りすぎたなど、画像形成装置10を操作することなく領域R1の外に出たユーザがいるか否かを判定する。

【0077】

追尾IDが付与されている顔データであって、カメラ画像から抽出されなくなった顔データがない場合、CPU110はS801に処理を戻す。追尾IDが付与されている顔データであって、カメラ画像から抽出されなくなった顔データがある場合、CPU110は抽出されなくなった顔データに対応する追尾IDのレコードを認証結果テーブルから削除し、S801に処理を戻す。

【0078】

S815において、カメラ画像に面積が最も大きな顔データがある場合、CPU110は面積が最も大きな顔データが認証の完了している顔データであるか否かを判定する(S818)。CPU110は、認証結果管理部412を制御し、顔データの面積が最も大きいと判定された顔データに付与された追尾IDに対応するユーザIDを取得する。CPU110は取得したユーザIDが“unknown”または“failure”のいずれでもない場合に認証が完了していると判定する。一方で取得したユーザIDが“unknown”または“failure”である場合、CPU110は認証が完了していないと判定する。

【0079】

認証が完了している場合、CPU110は最も面積の大きい顔データに付与された追尾IDに対応するユーザIDを用いてログイン処理を実行する(S819)。ここで画像形成装置10のログイン処理を説明する。画像形成装置10のHDD117には、表3に示すログイン情報テーブルが記憶されている。ログイン情報テーブルはユーザIDと当該ユーザIDを用いて画像形成装置10にログインがなされた場合に表示する画面の情報が対応づけて記憶されている。画面の情報とは、たとえば、画面表示に用いられる表示言語や、ログイン後最初に表示される画面の種類、画像形成装置10の実行する各機能のデフォルト設定の設定値などである。CPU110はログイン情報テーブルに記憶されたレコードから面積の最も大きい顔データに付与された追尾IDに対応するユーザIDのレコードを特定する。そして、CPU110は特定したレコードの設定情報に基づき画面を生成し、表示部202に表示させる。

【0080】

認証が完了していない場合、CPU110は表示部202に図7(b)に示すログイン画面を表示する(S820)。CPU110はログイン画面表示後、入力部203を介したユーザID、パスワードの入力を受け付ける。ユーザがユーザID、パスワードを入力し“ログイン”703を選択したことに従って、CPU110はログイン画面に入力されたユーザID、パスワードを認証部411に送信する。認証部411はCPU110から受け取ったユーザID、パスワードと、顔データテーブルを比較し、ユーザの認証処理を行う。認証が成功した場合、認証部411はユーザIDとユーザ認証が成功した旨をCPU110に返す。認証が失敗した場合、認証部411は認証が失敗した旨の通知をCPU110に返す。ログイン画面を表示することで、顔認証によるユーザ認証が完了する前に

10

20

30

40

50

ユーザが画像形成装置 10 の前に到達した場合や、顔データによる認証が失敗していた場合であってもユーザを画像形成装置 10 にログインさせることができる。本実施例では、ログイン画面で入力されたユーザ ID、パスワードを使った認証の際に、顔データを用いた認証と同じ情報を用いて認証を行うとした。顔認証時と異なる認証用のデータを使って認証を行ったり、入力されたユーザ ID、パスワードを外部のサーバに送信して外部サーバで認証を行うとしてもよい。また、S 820 では図 7 (b) に示すログイン画面を介してユーザ ID やパスワードを入力することで認証を行うとした。S 820 における認証は、画面を介して入力されたデータに基づく認証に限らず、IC カードによる認証や指紋等の生体情報を用いた認証であってもよい。

【0081】

CPU 110 は、入力されたユーザ ID、パスワードによるユーザ認証が成功したか否かを判定する (S 821)。CPU 110 は認証部 411 から受信した情報に基づき、認証が成功したか否かを判定する。

【0082】

認証が成功していない場合、CPU 110 は S 801 に処理を戻す。認証が成功している場合、CPU 110 は表 3 に示すログイン情報テーブルに基づきログイン処理を実行する (S 822)。CPU 110 はログイン情報テーブルから認証されたユーザのユーザ ID に対応するレコードを特定する。そして、CPU 110 は特定したレコードの設定情報に基づき画面を生成し、表示する。このようにすることで、画像形成装置 10 はログインしたユーザに適した画面を表示することができる。

【0083】

最後に図 9 ~ 図 11 を用いて、図 8 において説明した顔認証処理を実行した場合に画像形成装置がどのように動作するか模式図を用いて説明する。

【0084】

図 9 はユーザが画像形成装置 10 を使用するために、画像形成装置 10 に近づいてきた場合を示す図である。

【0085】

まず、ユーザが 901 まで来て領域 R1 に入ると、カメラ画像解析部 410 はカメラユニット 11 が撮像したカメラ画像からユーザの顔データを取得することができるようになる。しかし、まだこの段階ではカメラ画像から抽出された顔データの大きさが十分ではないため、顔認証処理は行われない。

【0086】

次にユーザが 902 まで来て領域 R2 に入ると、カメラ画像解析部 410 はカメラユニット 11 が撮像したカメラ画像から顔データを取得し、認証部 411 に認証させる。ユーザが領域 R3 に到達することでカメラ画像から取得された顔データの大きさが顔認証を行うのに十分な大きくなる。認証部 411 による認証が完了すると、カメラ画像解析部 410 は顔データに追尾 ID を割り振り、以降カメラユニット 11 が画像を撮像する度に当該顔データを追尾する。また、認証部 411 は認証が完了すると、認証結果を認証結果管理部 412 に登録する。

【0087】

次いで、ユーザが、903 の位置まで来て領域 R3 に到達すると、CPU 110 は 903 に到達したされるユーザの追尾 ID に対応するユーザ ID を用いて設定情報を取得し、ログイン後の画面を表示部 202 に表示する。ユーザが 902 から 903 まで移動している間に認証処理を完了させることで、ユーザが 903 に到達してからユーザを待たせることなくログイン後の画面を表示することができる。

【0088】

図 10 はユーザが画像形成装置 10 の前を横切ったときを示した模式図である。

【0089】

ユーザが 1001 の位置まで来て、領域 R1 に到達するとカメラ画像解析部 410 はカメラ画像からユーザの顔データの取得を開始する。図 9、同様この段階では顔データによ

10

20

30

40

50

る認証は開始されない。

【0090】

その後、ユーザが1002の位置まで移動し、領域R2に到達するとカメラ画像解析部410は撮像したカメラ画像から取得した顔データを認証部411に送る。認証部411はカメラ画像解析部410から取得した顔データに基づく認証を行う。認証部411は認証結果を認証結果管理部412に格納する。

【0091】

このまま、ユーザが領域R3まで行くことなく、位置1003に移動したとする。このとき、ユーザは領域R1の外に移動する。カメラ画像解析部410はカメラユニット11が取得したカメラ画像から追尾していたユーザの顔データが取得できなくなったことに従って、認証結果管理部412に記憶された認証結果を削除する。

10

【0092】

図11は、2人のユーザが領域R3の位置まで来たが、2人のうち一方のユーザが領域R3に入り、画像形成装置10を使用した場合である。

【0093】

まず、ユーザが1101の位置に来到、カメラ画像解析部410はカメラユニット11が取得したカメラ画像から1101にいるユーザの顔データを取得する。この時点では、いずれのユーザの顔認証もできない。カメラ画像解析部410は2人のユーザに追尾IDを付与する。認証結果管理部412はそれぞれの顔データに付与された追尾IDを認証結果テーブルに登録する。

20

【0094】

ユーザが1101から1102まで移動し、領域R2内に入ると、カメラユニット11が撮像するカメラ画像から取得される顔データに基づく認証が可能となる。

【0095】

カメラ画像解析部410は、顔データを認証部411に送る。認証部411はカメラ画像解析部410から取得した顔データを使って顔認証処理を行う。認証結果管理部412は、認証部による認証結果として得られたユーザのユーザIDを追尾IDと紐づけて認証結果テーブルに登録する。ここで、人物H1の顔認証結果が取得済となる。

【0096】

次いで、1102にいるユーザが領域R3に到達する前に、他のユーザが1104に来到とする。このとき、カメラ画像解析部410はカメラ画像から1104にいつユーザの顔データを取得できるようになる。カメラ画像解析部410は、取得した1104にいるユーザの顔データに追尾IDを付与し、認証結果管理部412に追尾IDを登録する。これにより1104にいるユーザの追尾が開始される。さらに、1104にいたユーザが1105まで移動し領域R2に入ると、カメラ画像解析部410はカメラ画像から取得した顔データを認証部411に送る。認証部411は取得した1105の位置にいるユーザの顔データを用いて顔認証を行う。認証結果管理部412は認証部411の認証結果を認証結果テーブルに登録する。これにより、1103にいるユーザと、1105にいるユーザの二人のユーザの認証が完了する。

30

【0097】

この段階では、位置1102、1105にいるユーザのいずれのユーザが画像形成装置10を使用するユーザであるかわからない。画像形成装置10はカメラ画像解析部410の顔データの追尾機能を使って、領域R3内まで移動したユーザを判定し、R3まで移動したユーザが画像形成装置10を使用するユーザであると判定する。

40

【0098】

1102にいたユーザが位置1103まで移動すると、カメラ画像解析部410はカメラユニットが解析したカメラ画像から取得される顔データに基づき、領域R3に入ったユーザが1102から追尾したユーザであると判定する。認証結果管理部412は、カメラ画像解析部410から領域R3に到達したユーザの顔データに付与された追尾IDを取得する。認証結果管理部412は、認証結果テーブルを参照し、カメラ画像解析部410か

50

ら取得した追尾ＩＤに対応するユーザＩＤを特定し、当該ユーザＩＤを使ったログイン処理を実行する。

【００９９】

画像形成装置１０が上記のように動作することで、ユーザの認証処理自体はユーザがＲ２に到達した時点で完了させておき、ユーザが領域Ｒ３に到達したときにはログイン処理のみを行えばよいようにすることができる。また、本実施例では領域Ｒ３に到達したユーザの追尾ＩＤに対応するユーザＩＤを用いてログイン処理を行う。カメラユニット１１が撮像したカメラ画像から複数のユーザの顔データが取得される場合でも、画像形成装置１０の前に来たユーザに対応する画面を表示部２０２に表示することができる。さらに、このようにすることで、カメラ画像から顔データが取得されるほかのユーザの画面が表示部２０２に表示されてしまうことを防ぐことができる。

10

【０１００】

以上、説明したように、本実施例によれば、カメラユニット１１が撮像したカメラ画像から取得された顔データを用いて顔認証が行われる装置において、ユーザが画像形成装置１０の前に来てから顔認証を行うよりも早く認証処理を行うことができる。また、カメラユニットが撮像したカメラ画像から複数のユーザの顔データが取得される場合であっても、画像形成装置１０を操作するユーザに対応する画面表示を行うことができる。

【０１０１】

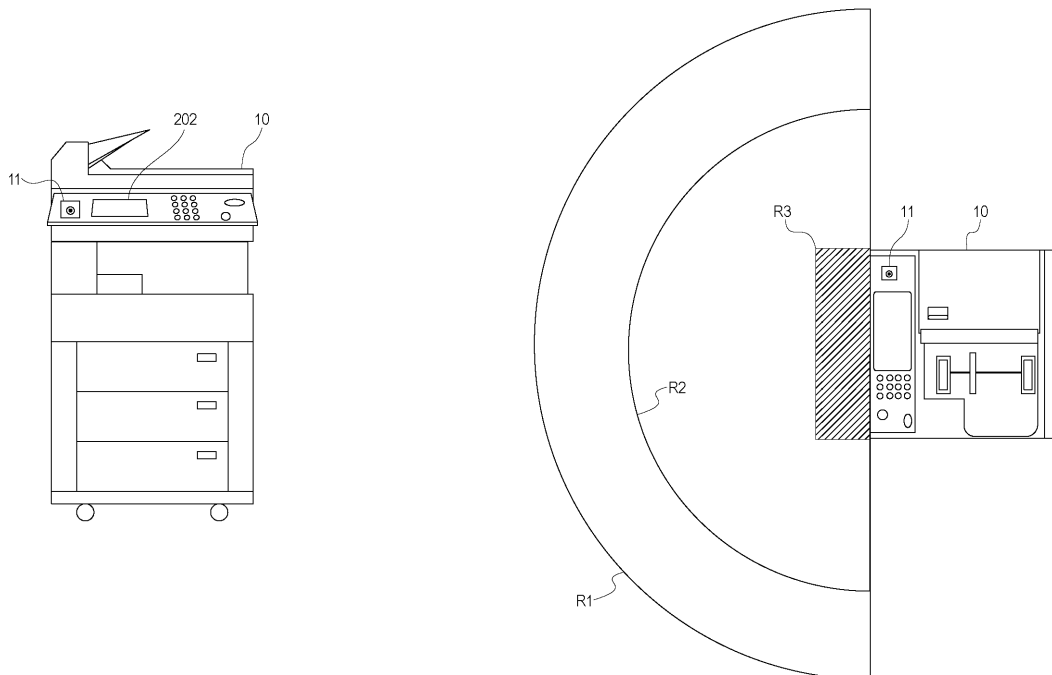
<その他の実施形態>

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。即ち、上述した実施例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憶媒体を介してシステム或いは装置に供給し、そのシステム又は装置のコンピュータ（又はＣＰＵやＭＰＵ等）がプログラムコードを読み出して実行する処理である。この場合、そのコンピュータプログラム、及び該コンピュータプログラムを記憶した記憶媒体は本発明を構成することになる。

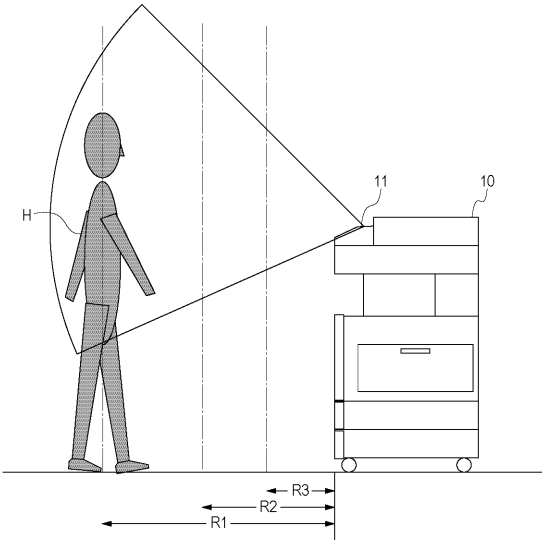
20

【図１】

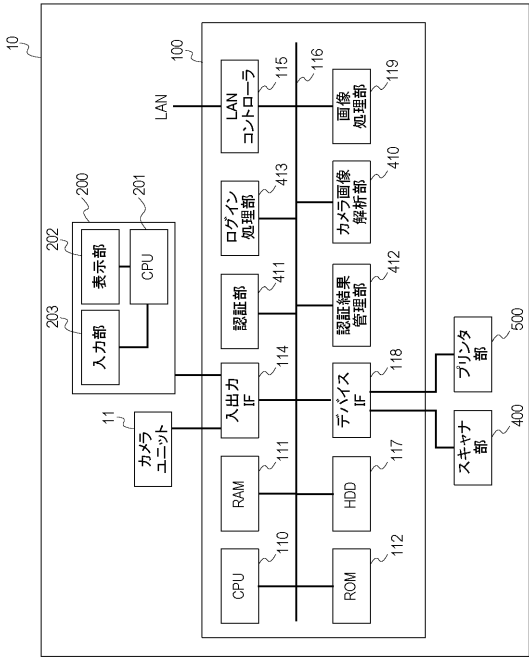
【図２】



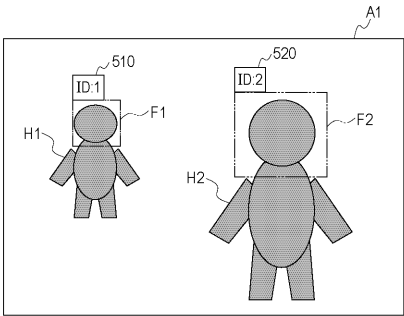
【 図 3 】



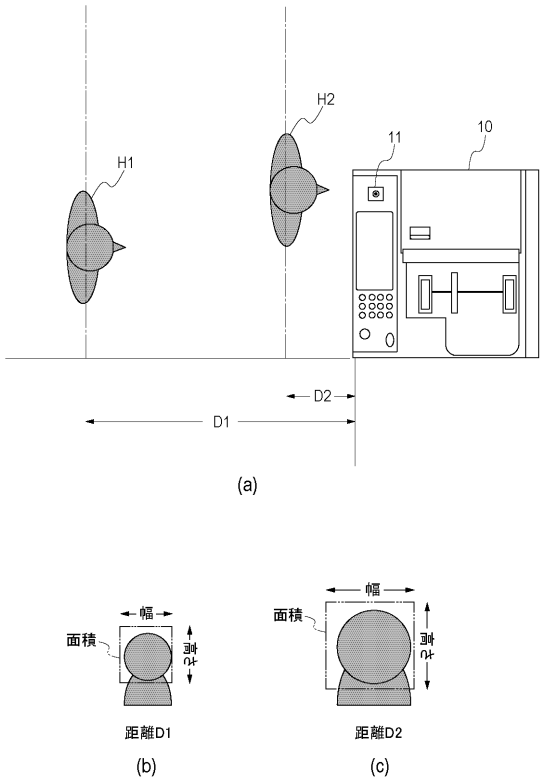
【 図 4 】



【 図 5 】



【 図 6 】



【図 7】

(a)

ユーザ名とパスワードを入力して
「ログイン」を押してください

ユーザID 701

パスワード 702

703

(b)

ようこそtanakaさん 704

705

ユーザNo: 0

(c)

Copy

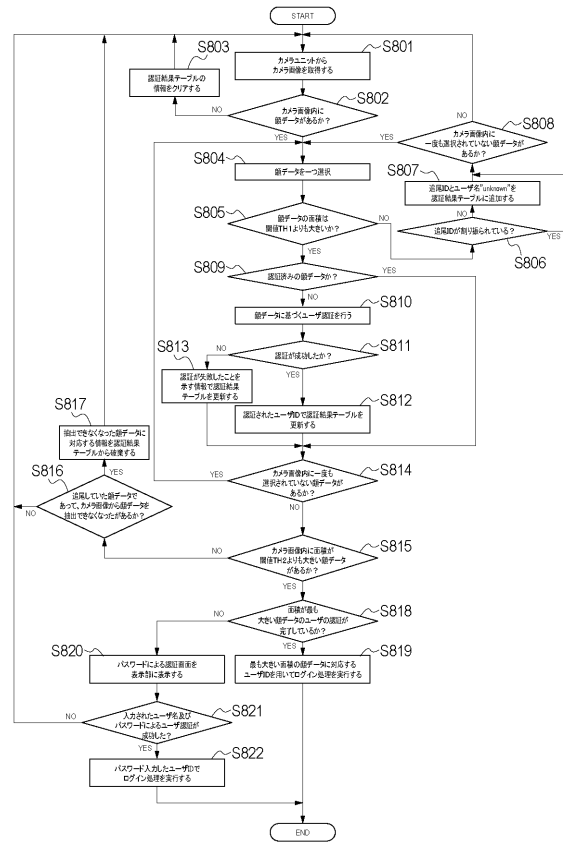
Black & White 100% Auto 1 Checking Settings

Select Color Copy Ratio Select Paper

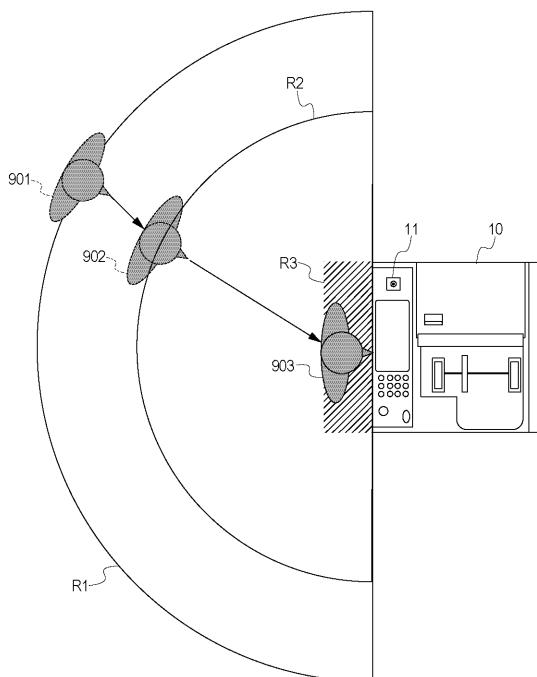
Finishing 2-Sided Density Original Type Copy ID Card

ユーザNo: 1

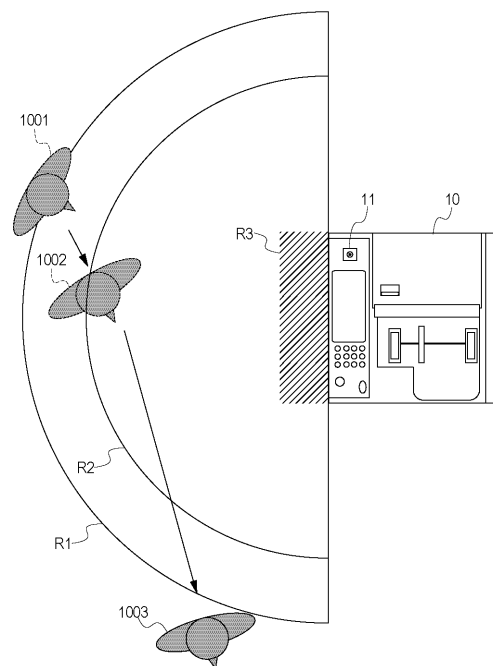
【図 8】



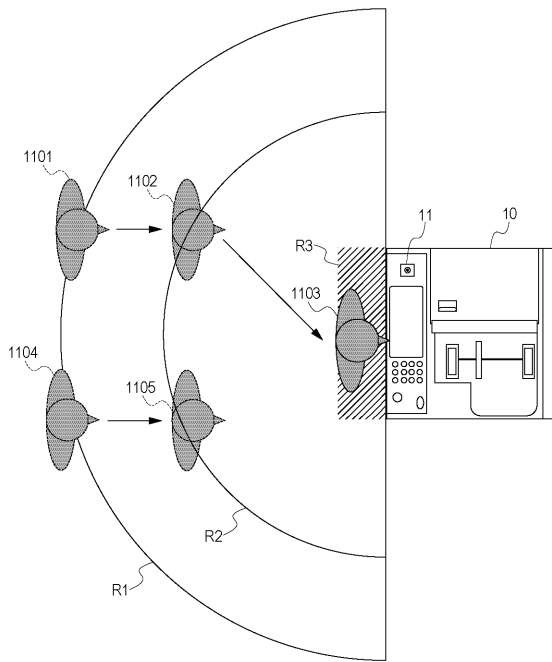
【図 9】



【図 10】



【図 11】



フロントページの続き

F ターム(参考) 2H270 LA58 LD03 LD08 LD14 LD15 NA02 NA04 NA05 QA03 QA46
ZC03 ZC04
5B043 AA05 AA09 BA04 DA05 EA02 GA01 HA02 HA09
5C062 AA02 AA05 AB17 AB20 AB23 AB40 AC58