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

特許第5711430号
(P5711430)

(45)発行日　平成27年4月30日(2015.4.30)　(24)登録日　平成27年3月13日(2015.3.13)

(51)Int.Cl.		F I		
G06F 21/32	(2013.01)	G06F	21/32	
H04L 9/32	(2006.01)	H04L	9/00	673D
G06F 13/00	(2006.01)	G06F	13/00	650B

請求項の数 8　(全 8 頁)

(21)出願番号	特願2014-530092(P2014-530092)
(86)(22)出願日	平成24年11月10日(2012.11.10)
(65)公表番号	特表2014-529837(P2014-529837A)
(43)公表日	平成26年11月13日(2014.11.13)
(86)国際出願番号	PCT/CN2012/084422
(87)国際公開番号	WO2014/026443
(87)国際公開日	平成26年2月20日(2014.2.20)
審査請求日	平成25年5月27日(2013.5.27)
(31)優先権主張番号	201210285041.0
(32)優先日	平成24年8月13日(2012.8.13)
(33)優先権主張国	中国(CN)

(73)特許権者　513131615
鶴山世達光電科技有限公司
中華人民共和国５２９７２８広東省江門市鶴山市共和鎮新材料基地（鶴山市世逸電子科技有限公司エイチ座）
(74)代理人　110000338
特許業務法人HARAKENZO WORLD PATENT & TRADEMARK
(72)発明者　王国芳
中華人民共和国５２９７２８広東省江門市鶴山市共和鎮新材料基地（鶴山市世逸電子科技有限公司エイチ座）

最終頁に続く

(54)【発明の名称】身分認証管理装置及びその方法

(57)【特許請求の範囲】

【請求項１】

身分認証管理装置であって、

指紋情報を抽出する採集識別装置、及び指紋情報とその指紋情報と対応するユーザーのユーザー情報を保存するメモリを含む指紋センサーと、該指紋センサーと個別に接続され、該指紋センサーによって採集された指紋情報を登録又は識別する複数の端末装置と、を含むクライアントと、

端末装置と互いに接続する身分認証サーバーと、及び前記身分認証サーバーと互いに接続する複数のアプリケーション・マネージメント・エリアとを含むバックグラウンドとを含み、

前記アプリケーション・マネージメント・エリアはアプリケーションユニット及びアプリケーション・インフォーメーションを含み、

前記アプリケーションユニットは、友人管理ユニットを含み、

前記身分認証サーバーによって認証済みの第１のユーザーが、前記身分認証サーバーによって認証済みの第２のユーザーとチャットをする場合に、第１のユーザーの第１の端末装置と接続された指紋センサーが、第１のユーザーの指紋をスキャニングし、前記友人管理ユニットを介して、第１の端末装置から第２のユーザーの第２の端末装置へ請求が送信され、第２の端末装置は、当該請求と第１のユーザーの指紋情報とを受信した後、第２の端末装置と接続された指紋センサーが、第２のユーザーの指紋をスキャニングして取得した指紋情報を、第１の端末装置にフィードバックすることによって、第１の端末装置と第

２の端末装置との間で指紋情報が交換され、
　第１の端末装置では、送信しようとする第１のユーザーのメッセージを第２のユーザーの指紋情報を用いて暗号化した後、第２の端末装置へ送信する処理が行われ、第２の端末装置では、第１の端末装置から受信したメッセージを第２の端末装置において第２のユーザーの指紋情報用いた解読処理が行われる
ことを特徴とする身分認証管理装置。
【請求項２】
　前記身分認証サーバーはユーザー身分を識別するためのユーザー認証ユニット及び登録されたユーザー情報を保存するためのユーザーアーカイブ管理ユニットを含む
ことを特徴とする請求項１に記載の身分認証管理装置。
【請求項３】
　前記アプリケーション・マネージメント・エリアのアプリケーションユニットとはゲーム、メール、ウェッブサイトその中の一つ又は複数を含んでいる
ことを特徴とする請求項１に記載の身分認証管理装置。
【請求項４】
　前記アプリケーション・マネージメント・エリアのアプリケーション・インフォーメーションとはユーザー名、パスワードその中の一つ又は複数を少なくとも含む
ことを特徴とする請求項１に記載の身分認証管理装置。
【請求項５】
　前記アプリケーション・マネージメント・エリアのアプリケーションユニットはチャットユニットを含み、前記クライアントにはチャットユニットのチャット内容を解読又は暗号化させるチャットソフトウェアが設置されている
ことを特徴とする請求項１に記載の身分認証管理装置。
【請求項６】
　（１）指紋情報を抽出する採集識別装置、及び指紋情報とその指紋情報と対応するユーザーのユーザー情報を保存するメモリを含む指紋センサーと、該指紋センサーと個別に接続され、該指紋センサーによって採集された指紋情報を登録又は識別する複数の端末装置と、を含むクライアントと、（２）端末装置と互いに接続する身分認証サーバーと、及び前記身分認証サーバーと互いに接続する複数のアプリケーション・マネージメント・エリアとを含むバックグラウンドとを含み、（３）前記アプリケーション・マネージメント・エリアはアプリケーションユニット及びアプリケーション・インフォーメーションを含み、（４）前記アプリケーションユニットは、友人管理ユニットを含む身分認証管理装置による身分認証管理方法であって、
　前記身分認証サーバーによって認証済みの第１のユーザーが、前記身分認証サーバーによって認証済みの第２のユーザーとチャットをする場合に、第１のユーザーの第１の端末装置と接続された指紋センサーが、第１のユーザーの指紋をスキャニングし、前記友人管理ユニットを介して、第１の端末装置から第２のユーザーの第２の端末装置へ請求を送信する段階と、
　第２の端末装置が当該請求と第１のユーザーの指紋情報とを受信した後、第２の端末装置と接続された指紋センサーが、第２のユーザーの指紋をスキャニングして取得した指紋情報を、第１の端末装置にフィードバックすることによって、第１の端末装置と第２の端末装置との間で指紋情報を交換する段階と、
　第１の端末装置において、送信しようとする第１のユーザーのメッセージを第２のユーザーの指紋情報を用いて暗号化した後、第２の端末装置へ送信する段階と、
　第２の端末装置において、第１の端末装置から受信したメッセージを第２の端末装置において第２のユーザーの指紋情報を用いた解読処理が行われる段階と、
を含む
ことを特徴とする身分認証管理方法。
【請求項７】
　指紋センサーの採集識別装置はユーザーの指紋情報を抽出し；

端末装置は採集された指紋情報と対応するユーザー情報を確認し、指紋情報を登録し；
バックグラウンドの身分認証サーバーのユーザー認証ユニットは新規登録された指紋情報より新たなユーザー情報を生成し、当該ユーザー情報を身分認証サーバーのユーザーアーカイブ管理ユニットに保存する
ことを特徴とする請求項６に記載の身分認証管理方法。
【請求項８】
ユーザーは前記アプリケーションユニット又は前記アプリケーション・インフォーメーションに対して削除、追加又は補正その中の一つ又は複数の操作ができる
ことを特徴とする請求項７に記載の身分認証管理方法。
【発明の詳細な説明】
【発明の詳細な説明】
【０００１】
〔技術分野〕
本発明は、身分認証管理装置及びその方法（A Device and Method for Identity Authentication）に関わっている。
【０００２】
〔背景技術〕
インターネットの急速発展とともに、ネットは人々の生活の中により一層重要な役割を果たして、ウェッブページの閲覧、各種のアプリケーション、ほとんど生活の一部になった。現在、われわれはよくアクセスしたサイト又はよく利用したアプリケーションについて、迅速にアクセスするために、お気に入りを使って管理を行う、ところが、お気に入りには、ウェッブサイトリンクだけを保存され、クリックしてからサイトに迅速にアクセスして、他のユーザー登録など操作は全部リンクされたウェッブで行う。さらにユーザーが選択しやすいために、一部のホームではユーザーがよくアクセスしたサイトに対して記憶管理を行う。ただ、それにも欠点があり、如何なる当該コンピューターを訪問する人全員見られるため、ユーザーにとって私秘性が足りないし、安全性も高くない。どうすればそれらのサイトリンク及び各種のアプリケーションに対して集中に管理し、且つユーザーの登録情報も集中に管理され、本当に安全便利にサイトリンク及びアプリケーションを使い、ユーザーの私秘性を確保することは我々現在解決しなければならない問題である。
【０００３】
〔発明の概要〕
本発明は身分認証管理装置及びその方法を提供して、ユーザーは迅速に関連アプリケーションを利用するだけではなく、各ユーザーの間の私秘性も保証できる。
【０００４】
本発明が採用された技術案は身分認証管理装置であり、
指紋センサーが採集された指紋情報を登録又は確認する複数の端末装置と、指紋情報を抽出する採集識別装置、及び指紋情報とその指紋情報と対応するユーザーのユーザー情報を保存するメモリを含むとともにそれぞれ個別の端末装置と互いに接続する指紋センサーとを含むクライアントと、
端末装置と互いに接続する身分認証サーバー、及び前記身分認証サーバーと互いに接続する複数のアプリケーションマネージメントエリアを含むバックグラウンドを含み、
アプリケーション・マネージメント・エリアはアプリケーションユニット及びアプリケーション・インフォーメーションを含み、
指紋情報が端末装置より登録又は認可後、前記身分認証サーバーは指紋情報と対応するユーザー情報と生成又は比較を行い、当該ユーザーのアプリケーション・マネージメント・エリアに入り、
アプリケーション・マネージメント・エリアでアプリケーションユニット及びアプリケーション・インフォーメーションに対する操作できる。
【０００５】
好ましくは、身分認証サーバーはユーザー身分を識別するためのユーザー認証ユニット

及び登録されたユーザー情報を保存するためのユーザーアーカイブ管理ユニットを含む。
【０００６】
好ましくは、端末装置と身分認証サーバー、身分認証サーバーとアプリケーションサーバーはネットワークによって互いに接続する。
【０００７】
好ましくは、アプリケーション・マネージメント・エリアのアプリケーションユニットとはゲーム、メール、ウェッブサイトその中の一つ又は複数を含んで、でもそれらに限らない。
【０００８】
好ましくは、アプリケーション・マネージメント・エリアのアプリケーション・インフォーメーションとはユーザー名、パスワードその中の一つ又は複数を少なくとも含む。
【０００９】
好ましくは、前記アプリケーション・マネージメント・エリアのアプリケーションユニットは友人管理ユニットを含む、当該友人管理ユニットは指紋情報の交換によって友人管理及び友人の間の操作を行うことができる。
【００１０】
好ましくは、前記アプリケーション・マネージメント・エリアのアプリケーションユニットはチャットユニットを含む、前記クライアントにはチャットユニットのチャット内容を解読又は暗号化させるチャットソフトウェアが設置される。
【００１１】
身分認証管理装置による身分認証管理方法において、下記のステップを含む：
指紋情報の採集、指紋センサーの採集識別装置によってユーザーの指紋を抽出する；
指紋情報の登録又は識別段階、端末装置は採集された指紋情報を登録又は識別する；
ユーザー認証段階、バックグラウンドの身分認証サーバーは新規登録された指紋情報より新たなユーザー情報を生成し、又は指紋情報と対応するユーザー情報をマッチングする；
アプリケーション・マネージメント段階、アプリケーション・マネージメント・エリアで、ユーザーはアプリケーションユニット又はアプリケーション・インフォーメーションに対して操作できる。
【００１２】
好ましくは、指紋センサーの採集識別装置はユーザーの指紋情報を抽出する；端末装置は採集された指紋情報と対応するユーザー情報を確認し、指紋情報を登録する；バックグラウンドの身分認証サーバーのユーザー認証ユニットは新規登録された指紋情報より新たなユーザーを生成し、当該ユーザー情報を身分認証サーバーのユーザーアーカイブ管理ユニットに保存する。
【００１３】
好ましくは、指紋センサーの採集識別装置はユーザーの指紋情報を抽出し、端末装置は採集された指紋情報を識別し、バックグラウンドの身分認証サーバーのユーザー認証ユニットはユーザーアーカイブ管理ユニットに保存されたユーザー情報と指紋情報と対応するユーザー情報とマッチングする。
【００１４】
好ましくは、ユーザーはアプリケーションユニット又はアプリケーション・インフォーメーションに対して削除、追加又は補正その中の一つ又は複数の操作ができる。
【００１５】
本発明は上記の構造又は方法を採用して、下記の有益な効果を有する：
１、　　当該ホームで、ユーザーの身分は指紋認証を受けてアプリケーション・マネージメント・エリアに入れるため、ユーザーの私秘性を保証できる；
２、　　ユーザーが登録する際、相応する指紋センサーを配置して、且つ関連するユーザー情報が指紋センサーに保存され、ユーザーの安全性を向上させ、指紋センサー装置又はアカウントが紛失後ユーザーデーターへの影響を減少できる；

３、　　指紋情報によってユーザーのカスタムサイト又は他の関連アプリケーションを管理して、同時にカスタムサイト又は他の関連アプリケーションのアカウント及びパスワードを管理して、ユーザーは指定された指紋をスキャニングすることによって、迅速且つ正確に関連サイト又は他のアプリケーションにアクセスでき、相応するアカウントへのログインも完成でき、ユーザーの時間を節約すると同時に、違うサイトで重複にアカウントへのログインする手間も減少させ、且つ安全性も非常に向上できる；

友人追加及び友人対話機能を有して、解読しないと、第三方はプライベートメッセージの内容を見られない。

【００１６】

〔図面についての説明〕

図１は、本発明の中の構造図を示している。

【００１７】

図２は、本発明の中の新しいユーザー操作のフロー図を示している。

【００１８】

図３は、本発明の中の古いユーザー操作のフロー図を示している。

【００１９】

〔具体的な実施形態〕

以下では、図面を参照して本発明の好ましい実施形態について詳しく記述して、当業者が本発明の優れた点及びと特徴をより良く理解させ、本発明の範囲をより明確に限定できる。

【００２０】

図２及び図３を参照して、本発明の第一実施例の中、身分認証及び管理方法であり、下記のテップを含む：

（Ａ）指紋情報の採集、指紋センサーの採集識別装置によってユーザーの指紋を抽出する；

（Ｂ）指紋情報の登録又は識別段階は登録及び識別二つの段階に分けられる。

【００２１】

（Ｂ１）指紋情報の登録、新しいユーザーにとって：指紋センサーの採集識別装置はユーザーの指紋を抽出して、端末装置は採集された指紋情報と対応するユーザー情報を比較し、指紋情報を登録する。

【００２２】

（Ｂ２）指紋情報の識別、登録済み認証を受けたユーザーにとって：指紋センサーの採集識別装置はユーザーの指紋を抽出して、端末装置は採集された指紋情報を識別する。

【００２３】

（Ｃ）ユーザーの認証段階、バックグラウンドの身分認証サーバーよってユーザー情報を生成又はマッチングする；

（Ｃ１）新しいユーザーにとって、バックグラウンドの身分認証サーバーのユーザー認証ユニットは新規登録された指紋情報を新規ユーザーを生成して、当該ユーザーの情報を身分認証サーバーのユーザーアーカイブ管理ユニットに保存する。

【００２４】

（Ｃ２）登録済み認証を受けたユーザーにとって、バックグラウンドの身分認証サーバーのユーザー認証ユニットはユーザーアーカイブ管理ユニットに保存されたユーザー情報と、指紋情報と対応するユーザー情報とマッチングする。

【００２５】

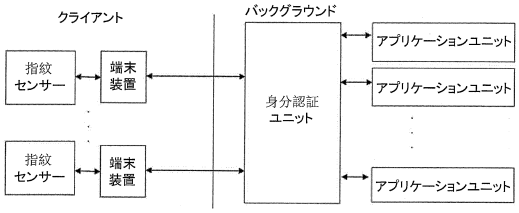
（Ｄ）アプリケーション・マネージメント段階、アプリケーション・マネージメント・エリアで、ユーザーはアプリケーションユニット又はアプリケーション・インフォーメーションを操作できる。このような操作は削除、追加又は補正等似通った動作である。

【００２６】

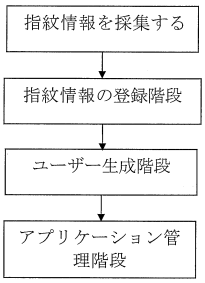
図２に示すように、新しいユーザーにとって、その操作ステップはＡ、Ｂ１、Ｃ１及びＤである。図３に示すように、古いユーザーにとって、その操作ステップはＡ、Ｂ２、Ｃ

２及びＤである。
【００２７】
図１に示すように、身分認証管理装置であって、クライアント及びバックグラウンドを含む。クライアントは複数の端末装置及びそれぞれの端末装置と互いに接続する指紋センサーを含み、指紋センサーは指紋情報を抽出する採集識別装置、及び指紋情報とその指紋情報と対応するユーザーのユーザー情報を保存するメモリを含む。端末装置はコンピューター、タブレット型コンピューター又は携帯電話その中の一つであり、端末装置が指紋センサーに採集された指紋情報を登録又は識別する。端末装置は少なくとも操作を表示できるディスプレー画面を有して、このディスプレー画面がユーザーの操作を表示できる。
【００２８】
バックグラウンドは端末装置と互いに接続する身分認証サーバー、及び身分認証サーバーと互いに接続する複数のアプリケーション・マネージメント・エリアを含む。
【００２９】
身分認証サーバーはユーザー身分を識別するためのユーザー認証ユニット及び登録されたユーザー情報を保存するためのユーザーアーカイブ管理ユニットを含む。
【００３０】
アプリケーション・マネージメント・エリアはアプリケーションユニット及びアプリケーション・インフォーメーションを含む。アプリケーション・マネージメント・エリアのアプリケーションユニットとはゲーム、メール、ウェッブサイトその中の一つ又は複数を含んで、でもそれらに限らない。アプリケーション・マネージメント・エリアのアプリケーション・インフォーメーションとはユーザー名、パスワードその中の一つ又は複数を少なくとも含む。
【００３１】
指紋情報が端末装置より登録又は認可された後、身分認証サーバーは指紋情報と対応するユーザー情報を生成又は比較を行い、当該ユーザーのアプリケーション・マネージメント・エリアに入り、アプリケーション・マネージメント・エリアでアプリケーションユニット及びアプリケーション・インフォーメーションに対して操作する。
【００３２】
アプリケーション・マネージメント・エリアのアプリケーションユニットは友人管理ユニットを含む。友人管理ユニットは指紋情報の交換によって友人管理及び友人の間の操作を行うことができる。既に認証登録済みの一人のユーザーAはもう一人の認証登録済みのユーザーＢを追加しようとする場合、指紋をスキャニングして友人管理ユニットよって請求を送信する。Ｂは請求及びＡの指紋情報を受信してから、指紋をスキャニングし確認するだけで、そしてＢの指紋情報をＡにフィードバックして、友人追加を実現できる。
【００３３】
アプリケーション・マネージメント・エリアのアプリケーションユニットはチャットユニットを含む、クライアントにはチャットユニットのチャット内容を解読又は暗号化させるチャットソフトウェアを設置される。
【００３４】
友人追加を完成してから、ＡとＢは秘密にチャットできる。Ａは送信しようとするメッセージをチャットソフトウェアを利用して指紋情報よって暗号化され、Ｂに送信する；Ｂはメッセージを受信した後、ダイアログ・ボックスの表示は文字化けだけど、Ｂは指紋情報及びチャットソフトウェアを利用して解読して、閲覧できる。解読後、元の乱雑な文字を自動的に正常の文字に形成できるし、マウスを乱雑な文字の如何なる位置において、如何なる位置の乱雑な文字は正常な字体又は拡大された文字に変わる。そのように、他のユーザーはクライアントで操作しても、Ｂの指紋情報を有しないので、チャット内容を解読できない。従いまして、本装置は以前と比べより良い安全性を有する。
【００３５】
端末装置と身分認証サーバー、身分認証サーバーとアプリケーションサーバーはネットワークによって互いに接続する。

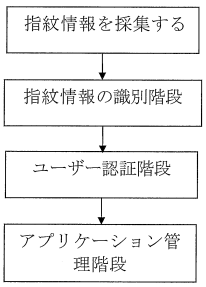
【００３６】
本発明は上記の構造又は方法を採用して、下記の有益な効果を有する：
１、当該ホームで、ユーザーの身分は指紋認証を受けてアプリケーション・マネージメント・エリアに入れるため、ユーザーの私秘性を保証できる；
２、ユーザーが登録する際、相応する指紋センサーを配置して、且つ関連するユーザー情報が指紋センサーに保存され、ユーザーの安全性を向上させ、指紋センサー装置又はアカウントが紛失後ユーザーデーターへの影響を減少できる；
３、指紋情報によってユーザーのカスタムサイト又は他の関連アプリケーションを統一に管理して、同時にカスタムサイト又は他の関連アプリケーションのアカウント及びパスワードを管理して、ユーザーは指定された指紋をスキャニングすることによって、迅速且つ正確に関連サイト又は他のアプリケーションにアクセスでき、相応するアカウントへのログインも完成でき、ユーザーの時間を節約すると同時に、違うサイトで重複にアカウントへのログインする手間も減少させ、且つ安全性も非常に向上できる；
４、友人追加及び友人対話機能を有して、解読しないと、第三方はプライベートメッセージの内容を見られない。
【００３７】
以上図を参照して本発明の特定の実施形態を記述したが、本発明の範囲及び趣旨の元に、現有技術及びプロセスに対して多くの改善ができる。本発明が所属された技術分野において、通常の常識を有すれば、本発明の技術趣旨の範囲以内多様な変更を行うことができる。
【図面の簡単な説明】
【００３８】
【図１】本発明の中の構造図を示している。
【図２】本発明の中の新しいユーザー操作のフロー図を示している。
【図３】本発明の中の古いユーザー操作のフロー図を示している。
【図１】



【図２】



【図３】



フロントページの続き

(72)発明者　程佩儀
中華人民共和国５２９７２８広東省江門市鶴山市共和鎮新材料基地（鶴山市世逸電子科技有限公司エイチ座）

審査官　宮司　卓佳

(56)参考文献　特開２０１０－２２６２５０（ＪＰ，Ａ）
特開２００２－２９７５５２（ＪＰ，Ａ）
特開２００６－１８９９６７（ＪＰ，Ａ）
特開２００５－３３２３２９（ＪＰ，Ａ）
国際公開第２０１２／０１１２２９（WO，Ａ１）
特開２００８－０４０９６０（ＪＰ，Ａ）
特開２００５－０３９８６８（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ　２１／３０－２１／４６
Ｇ０６Ｆ　１３／００
Ｈ０４Ｌ　９／３２