

(19) 日本国特許庁(JP)

(12) 特 許 公 報(B2)

(11) 特許番号

特許第3596595号

(P3596595)

(45) 発行日 平成16年12月2日(2004.12.2)

(24) 登録日 平成16年9月17日(2004.9.17)

(51) Int. Cl.⁷

F I

G06F 1/00

G06F 1/00 370E

G06F 15/00

G06F 15/00 330F

G06T 7/00

G06F 15/00 330G

G06T 7/00 510A

請求項の数 2 (全 10 頁)

(21) 出願番号	特願平11-237669	(73) 特許権者	000000295 沖電気工業株式会社 東京都港区虎ノ門1丁目7番12号
(22) 出願日	平成11年8月25日(1999.8.25)	(74) 代理人	100082050 弁理士 佐藤 幸男
(65) 公開番号	特開2001-67137(P2001-67137A)	(72) 発明者	和田山 豊 東京都港区虎ノ門1丁目7番12号 沖電 気工業株式会社内
(43) 公開日	平成13年3月16日(2001.3.16)	審査官	富吉 伸弥
審査請求日	平成15年1月30日(2003.1.30)		

最終頁に続く

(54) 【発明の名称】 個人認証システム

(57) 【特許請求の範囲】

【請求項1】

被認証者の生体情報を取得する生体情報入力部と、
 予め登録された登録者の生体情報と前記生体情報とを比較して前記被認証者が前記登録者であるか否かを判定する制御部とを備える個人認証システムにおいて、
 前記登録者の生体情報の取得時に乱数を発生する乱数発生部と、
 前記乱数に基く分割率により前記登録者の生体情報を分割し、該分割した一方の生体情報部分を記憶部に記憶させる分割手段と、
 前記分割した他方の生体情報部分を前記登録者に付与する可搬型記憶部に記憶させる書込手段と、
 前記判定のために前記可搬型記憶部から前記他方の生体情報部分を読み取る読取手段と、
 前記読み取った他方の生体情報部分と前記記憶部の一方の生体情報部分とを合成して前記登録者の生体情報を生成する生体情報生成手段と、
 を含むことを特徴とする個人認証システム。

【請求項2】

被認証者の生体情報を取得する生体情報入力部と、
 予め登録された登録者の生体情報と前記生体情報とを比較して前記被認証者が前記登録者であるか否かを判定する制御部とを備える個人認証システムにおいて、
 前記登録者の生体情報の取得時に該登録者が分割するための分割率を入力するための分割率入力部と、

該入力した分割率により前記登録者の生体情報を分割し、該分割した一方の生体情報部分を記憶部に記憶させる分割手段と、
前記分割した他方の生体情報部分を前記登録者に付与する可搬型記憶部に記憶させる書込手段と、
前記判定のために前記可搬型記憶部から前記他方の生体情報部分を読み取る読取手段と、
前記読み取った他方の生体情報部分と前記記憶部の一方の生体情報部分とを合成して前記登録者の生体情報を生成する生体情報生成手段と、
を含むことを特徴とする個人認証システム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、人間の生体情報（アイリス、網膜、指紋、声紋、等）を利用した個人認証システムに関する。

【0002】

【従来の技術】

近年、高度情報社会の発達によりセキュリティに関する要求が高まっている。この要求を満たすために暗証番号、カード又は生体情報を用いた認証システムの開発が進められている。このシステムでは予め認証装置内に格納されている生体情報と認証装置の生体情報入力部から入力された生体情報を比較することにより個人認証が行われている。

【0003】

【発明が解決しようとする課題】

ところで、上記のような従来の技術には、次のような解決すべき課題が残されていた。即ち、上記システムでは、装置内の生体情報が盗難にあった場合に、2度とその人の生体情報は、認証用に使用されることが不可能になるという解決すべき大きな課題が残されていた。

【0004】

【課題を解決するための手段】

本発明は以上の点を解決するため次の構成を採用する。

構成1

被認証者の生体情報を取得する生体情報入力部と、予め登録された登録者の生体情報と前記生体情報とを比較して前記被認証者が前記登録者であるか否かを判定する制御部とを備える個人認証システムにおいて、前記登録者の生体情報の取得時に乱数を発生する乱数発生部と、前記乱数に基く分割率により前記登録者の生体情報を分割し、該分割した一方の生体情報部分を記憶部に記憶させる分割手段と、前記分割した他方の生体情報部分を前記登録者に付与する可搬型記憶部に記憶させる書込手段と、前記判定のために前記可搬型記憶部から前記他方の生体情報部分を読み取る読取手段と、前記読み取った他方の生体情報部分と前記記憶部の一方の生体情報部分とを合成して前記登録者の生体情報を生成する生体情報生成手段とを含むことを特徴とする個人認証システム。

【0005】

構成2

被認証者の生体情報を取得する生体情報入力部と、予め登録された登録者の生体情報と前記生体情報とを比較して前記被認証者が前記登録者であるか否かを判定する制御部とを備える個人認証システムにおいて、前記登録者の生体情報の取得時に該登録者が分割するための分割率を入力するための分割率入力部と、該入力した分割率により前記登録者の生体情報を分割し、該分割した一方の生体情報部分を記憶部に記憶させる分割手段と、前記分割した他方の生体情報部分を前記登録者に付与する可搬型記憶部に記憶させる書込手段と、前記判定のために前記可搬型記憶部から前記他方の生体情報部分を読み取る読取手段と、前記読み取った他方の生体情報部分と前記記憶部の一方の生体情報部分とを合成して前記登録者の生体情報を生成する生体情報生成手段とを含むことを特徴とする個人認証システム。

10

20

30

40

50

【 0 0 0 7 】

【 発明の実施の形態 】

以下、本発明の実施の形態を具体例を用いて説明する。

具体例 1

本発明では、生体情報を X と Y に分割率 M で分割する。この一方の X を認証装置内に格納し、他方の Y を操作者（登録者又は認証者）が携帯する可搬型記憶部に格納する。認証時に X + Y を求めて、認証者から直接受け入れた生体情報と比較して認証する。従って仮に X、Y のどちらかが盗難にあっても分割率 M を変更して再度 X、Y を求めることによって盗難にあった生体情報の悪用を防止できる。以上の目的を達成するために具体例 1 による個人認証システムは以下のように構成される。

10

【 0 0 0 8 】

図 1 は、具体例 1 による個人認証システムの構成図である。

図 1 より、具体例 1 による個人認証システムは、認証装置 1 と、可搬型記憶部 2 によって構成される。

認証装置 1 は、操作者 4 が自己の生体情報を登録したり、認証したりする装置であり以下に記す部分を備える。

【 0 0 0 9 】

認証装置 1 は、生体情報入力部 1 1 と、可搬型記憶部リーダ/ライタ 1 2 と、制御部 1 3 と、乱数発生部 1 4 と、外部制御部 1 5、認証記憶部 1 6 を備える。

生体情報入力部 1 1 は、操作者 4（登録者又は認証者）から生体情報を読み込む部分である。

20

可搬型記憶部リーダ/ライタ 1 2 は、生体情報を可搬型記憶部 2 に書き込む部分であり、又生体情報を可搬型記憶部 2 から読み込む部分でもある。

【 0 0 1 0 】

制御部 1 3 は、認証装置 1 全体を制御する部分である。

乱数発生部 1 4 は、生体情報を後に説明する分割に際しての分割率を設定する数値を生成する部分である。

外部制御部 1 5 は、外部 I / O を制御する部分である。

【 0 0 1 1 】

認証記憶部 1 6 は、情報を格納する部分であり、メモリ A と、メモリ B と、メモリ C が配置されている。

30

メモリ A は、装置全体の制御プログラムを格納するメモリである。

メモリ B は、生体情報の認証、或いは、登録に際してワークエリアの役目を果たすメモリである。

メモリ C は、個人の生体情報等を格納するメモリでありサブメモリ C 1、サブメモリ C 2、サブメモリ C 3、サブメモリ C 4 よって構成されている。

【 0 0 1 2 】

サブメモリ C 1 は、後に説明する生体情報分割率を格納するメモリである。

サブメモリ C 2 は、個人の生体情報を格納するメモリである。

サブメモリ C 3 は、個人認証システムが稼働した履歴、即ち、認証ログを格納するメモリである。

40

サブメモリ C 4 は、個人を特定するための個人情報情報を格納するメモリである。

以上で具体例 1 による個人認証システムの構成についての説明を終了して次に具体例 1 による個人認証システムの登録動作について説明する。

【 0 0 1 3 】

具体例 1 の動作

図 2 は、具体例 1 による個人認証システムの動作説明図（その 1）である。

この図 2 は、具体例 1 による個人認証システムにおける登録の動作の流れについて説明する図である。

図 1 を参照しながら図 2 のステップに従って具体例 1 による個人認証システムの動作につ

50

いて説明する。

【 0 0 1 4 】

動作説明のための前提条件を以下のように定める。

前提条件 1

全生体情報を一例として 2 5 6 バイトに限定する。

前提条件 2

乱数 N は 0 ~ 2 5 6 に限定する。下記の動作説明では仮に $N = 6 4$ と定める。

前提条件 3

分割率 M を一例として以下の数式から算出する。

$$Y = N (0 \sim 2 5 6)$$

$$X + Y = 2 5 6 (\text{バイト})$$

$$M = Y / (X + Y)$$

Y は、サブメモリ C 2 (図 1) に、X は、可搬型記憶部 2 (図 1) に格納されるものとする。

【 0 0 1 5 】

ステップ S 1

具体例 1 による個人認証システムの登録には、生体情報の分割率 M が必要である。

この分割率 M は登録毎にランダムな値に定められる。制御部 1 3 (図 1) は、ランダムな値を得るために乱数発生部 1 4 (図 1) に命じて乱数 N を発生させる。

【 0 0 1 6 】

ステップ S 2

制御部 1 3 (図 1) は、乱数発生部 1 4 (図 1) から乱数出力 $N = 6 4$ (上記前提条件 2 より) を受け入れて分割率 M を算出する。上記前提条件 3 より、

$$M = (6 4 / 2 5 6) = 0 . 2 5 \text{ を得る。}$$

制御部 1 3 (図 1) は、この分割率 $M = (6 4 / 2 5 6) = 0 . 2 5$ をサブメモリ C 1 (図 1) に格納する。

【 0 0 1 7 】

ステップ S 3

制御部 1 3 (図 1) は、生体情報入力部 1 1 (図 1) に命じて操作者 4 (図 1) (ここでは登録者) から生体情報を読み取る。この生体情報は上記前提条件 1 より、2 5 6 バイトに限定されている。

【 0 0 1 8 】

ステップ S 4

制御部 1 3 (図 1) は、生体情報入力部 1 1 (図 1) を介して受け入れた操作者 4 (図 1) の生体情報 2 5 6 バイトを分割率 $M = 0 . 2 5$ に従って分割して、生体情報 $Y = 2 5 6 \times 0 . 2 5 = 6 4$ (バイト) と生体情報 $X = 2 5 6 \times 0 . 7 5 = 1 9 2$ (バイト) に分割する。

【 0 0 1 9 】

ステップ S 5

制御部 1 3 (図 1) は、上記生体情報 $Y = 2 5 6 \times 0 . 2 5 = 6 4$ (バイト) をサブメモリ C 2 (図 1) に格納し、個人情報をサブメモリ C 4 (図 1) に格納する。

【 0 0 2 0 】

ステップ S 6

制御部 1 3 (図 1) は、可搬型記憶部リーダ/ライタ 1 2 (図 1) を介して上記生体情報 $X = 2 5 6 \times 0 . 7 5 = 1 9 2$ (バイト) と個人情報を可搬型記憶部 2 (図 1) に格納する。

【 0 0 2 1 】

以上で登録動作についての説明を終了する。

次に具体例 1 による個人認証システムの認証動作について説明する。

図 3 は、具体例 1 による個人認証システムの動作説明図 (その 2) である。

10

20

30

40

50

この図3は、具体例1による個人認証システムにおける認証の動作の流れについて説明する図である。

図1を参照しながら図3のステップに従って具体例1による個人認証システムの認証動作について説明する。

【0022】

動作説明のための前提条件を上記登録動作と同様とし更に以下に記す前提条件4を加える。

前提条件4

メモリCに格納されている生体情報Yと可搬型記憶部2(図1)に格納されている生体情報Xから、生体情報Z = 生体情報Y + 生体情報Xを求める。この生体情報Zと操作者4(図1)から生体情報入力部11(図1)を介して読み取った生体情報とを比較して求めた一致率を と置く。この が予め定めてある規定値 と比較して

の時、認証OKと判断し < の時、認証NGと判断するものとする。

【0023】

ステップS1

操作者4(図1)(ここでは認証者)は、可搬型記憶部2(図1)を可搬型記憶部リーダー/ライター12(図1)へ挿入する。

【0024】

ステップS2

制御部13(図1)は、可搬型記憶部リーダー/ライター12(図1)を介して可搬型記憶部2(図1)に格納されている個人情報から上記生体情報X = 192(バイト)を読み取る。

【0025】

ステップS3

制御部13(図1)は、サブメモリC2(図1)から生体情報Y = 64(バイト)を読み取り、サブメモリC4(図1)から個人情報を読み取る。

ステップS4

制御部13(図1)は、生体情報Z = 生体情報X + 生体情報Yを構成してメモリB(図1)に格納する。

【0026】

ステップS5

制御部13(図1)は、生体情報入力部11(図1)を介して操作者4(図1)から生体情報を読み出す。

ステップS6

制御部13(図1)は、生体情報ZをメモリB(図1)から読み出して上記操作者4(図1)から読み出した生体情報とを比較してその一致率(上記前提条件4)を求める。

【0027】

ステップS7

制御部13は(図1)は、の時認証OKと判断し < の時認証NGと判断する。

以上で具体例1による個人認証システムの認証動作について説明を終了する。

【0028】

以上の説明では生体情報の大きさを256バイトに限定して説明したが、これは説明の都合上限定したのであって本発明がこの値に限定されるものではない。即ち本発明による個人認証システムが採用される装置の仕様によって生体情報の大きさは適宜決定される。

更に、分割率Mを $Y = N(0 \sim 256)$ 、 $X + Y = 256$ (バイト)、 $M = Y / (X + Y)$ として求めたが、これも一例であって本発明がこの数式に限定されるものではない。予め定めてある特定された数式であればどのような数式であっても良い。

【0029】

具体例1の効果

生体情報をXとYに分割率Mで分割することによって以下の効果を得る。

10

20

30

40

50

1. X又はYのどちらかが盗難にあった場合に、分割率Mを変更した値で再度分割して、認証装置1内と、可搬型記憶部2に別々に格納することによって盗難にあったX又はYのどちらかによって不正使用されることが無くなる。

2. その結果信頼度の高い個人認証システムを得ることができる。

【0030】

具体例2の構成

図4は、具体例2による個人認証システムの構成図である。

図4より具体例2による個人認証システムは、認証装置20と、可搬型記憶部2によって構成される。

認証装置20は、操作者4が自己の生体情報を登録したり、認証したりする装置であり以下に記す部分を備える。 10

【0031】

認証装置20は、生体情報入力部11と、可搬型記憶部リーダ/ライタ12と、制御部13と、外部制御部15と、認証記憶部16と、分割率入力部21を備える。

分割率入力部21は、操作者4がメモリC内に格納する分割率Mを自己の意志により自由に入力する部分である。

その他の構成は全て具体例1と同様なので説明を割愛する。

次に具体例1による個人認証システムの登録動作について説明する。

【0032】

具体例2の動作 20

図5は、具体例2による個人認証システムの動作説明図(その1)である。

この図5は、具体例2による個人認証システムにおける登録の動作の流れについて説明する図である。

図4を参照しながら図5のステップに従って具体例1による個人認証システムの動作について説明する。

【0033】

動作説明のための前提条件を以下のように定める。

前提条件1

全生体情報を一例として256バイトに限定する。

前提条件2 30

操作者4が入力する分割率を一例として $M = 0.25$ と仮定する。

【0034】

ステップS1

具体例2による個人認証システムの登録には、生体情報の分割率Mが必要である。

この分割率Mは、操作者4(図4)(ここでは登録者)がメモリC(図1)内に格納する分割率Mを自己の意志により自由に入力する。ここでは上記前提条件2より操作者4(図4)が $M = 0.25$ を分割率入力部21(図4)を介して制御部13(図4)へ送る。制御部13(図4)は、この $M = 0.25$ をサブメモリC1へ格納する。

【0035】

ステップS2 40

制御部13(図4)は、生体情報入力部11(図4)に命じて操作者4(図4)から生体情報を読み取る。この生体情報は上記前提条件1より、256バイトに限定されている。

【0036】

ステップS3

制御部13(図4)は、生体情報入力部11(図4)を介して受け入れた操作者4(図4)の生体情報256バイトを分割率 $M = 0.25$ に従って分割して、生体情報 $Y = 256 \times 0.25 = 64$ (バイト)と生体情報 $X = 256 \times 0.75 = 192$ (バイト)に分割する。

【0037】

ステップS4 50

制御部 13 (図 4) は、上記生体情報 $Y = 256 \times 0.25 = 64$ (バイト) をサブメモリ C2 (図 4) に格納し、個人情報 をサブメモリ C4 (図 4) に格納する。

ステップ S5

制御部 13 (図 4) は、可搬型記憶部リーダ/ライタ 12 (図 4) を介して上記生体情報 $X = 256 \times 0.75 = 192$ (バイト) と個人情報 を可搬型記憶部 2 (図 4) に格納する。

【0038】

以上で登録動作についての説明を終了する。

次に具体例 2 による個人認証システムの認証動作について説明する。

図 6 は、具体例 2 による個人認証システムの動作説明図 (その 2) である。

10

この図 6 は、具体例 1 による個人認証システムにおける認証の動作の流れについて説明する図である。

図 4 を参照しながら図 6 のステップに従って具体例 1 による個人認証システムの認証動作について説明する。

【0039】

動作説明のための前提条件を上記登録動作と同様とし更に以下に記す前提条件 3 を加える。

前提条件 3

メモリ C (図 4) に格納されている生体情報 Y と可搬型記憶部 2 (図 4) に格納されている生体情報 X から、生体情報 $Z = \text{生体情報 Y} + \text{生体情報 X}$ を求める。この生体情報 Z と操作者 4 (図 4) から生体情報入力部 11 (図 4) を介して読み取った生体情報とを比較して求めた一致率を と置く。この が予め定めてある規定値 と比較しての時認証 OK と判断し < の時認証 NG と判断するものとする。

20

【0040】

ステップ S1

操作者 4 (図 4) (ここでは認証者) は、可搬型記憶部 2 (図 4) を可搬型記憶部リーダ/ライタ 12 (図 4) へ挿入する。

【0041】

ステップ S2

制御部 13 (図 4) は、可搬型記憶部リーダ/ライタ 12 (図 4) を介して個人情報から可搬型記憶部 2 (図 4) に格納されている上記生体情報 $X = 192$ (バイト) を読み取る。

30

【0042】

ステップ S3

制御部 13 (図 4) は、サブメモリ C2 (図 4) から生体情報 $Y = 64$ (バイト) を読み取り、サブメモリ C4 (図 4) から個人情報を読み取る。

ステップ S4

制御部 13 (図 4) は、生体情報 $Z = \text{生体情報 X} + \text{生体情報 Y}$ を構成してメモリ B (図 4) に格納する。

【0043】

40

ステップ S5

制御部 13 (図 4) は、生体情報入力部 11 (図 4) を介して操作者 4 (図 4) から生体情報を読み出す。

ステップ S6

制御部 13 (図 4) は、生体情報 Z をメモリ B (図 4) から読み出して上記操作者 4 (図 4) から生体情報を読み出した生体情報を比較してその一致率 (上記前提条件 3) を求める。

【0044】

ステップ S7

制御部 13 は (図 4) は、の時認証 OK と判断し < の時認証 NG と判断する。

50

以上で具体例 2 による個人認証システムの認証動作について説明を終了する。

以上の説明では生体情報の大きさを 256 バイトに限定して説明したが、これは説明の都合上限定したのであって本発明がこの値に限定されるものではない。即ち本発明による個人認証システムが採用される装置の仕様によって生体情報の大きさは適宜決定される。

【0045】

具体例 2 の効果

分割率 M を操作者 4 が自由に設定することによって具体例 1 の効果に加えて以下の効果を得る。

即ち、分割率 M を操作者 4 が自由に設定することにより操作者 4 のプライバシーを保護することが可能になる。

10

【図面の簡単な説明】

【図 1】具体例 1 による個人認証システムの構成図である。

【図 2】具体例 1 による個人認証システムの動作説明図（その 1）である。

【図 3】具体例 1 による個人認証システムの動作説明図（その 2）である。

【図 4】具体例 2 による個人認証システムの構成図である。

【図 5】具体例 2 による個人認証システムの動作説明図（その 1）である。

【図 6】具体例 2 による個人認証システムの動作説明図（その 2）である。

【符号の説明】

- 1 認証装置
- 2 可搬型記憶部
- 3 外部 I / O
- 4 操作者
 - 1 1 生体情報入力部
 - 1 2 可搬型記憶部リーダー/ライター
 - 1 3 制御部
 - 1 4 乱数発生部
 - 1 5 外部制御部
- A, B, C メモリ
 - C 1, C 2, C 3, C 4 サブメモリ

20

フロントページの続き

- (56)参考文献 特開昭57-055468(JP,A)
特開平11-025246(JP,A)
特開平11-134302(JP,A)
特開平10-154132(JP,A)
特開平09-330140(JP,A)

(58)調査した分野(Int.Cl.⁷, DB名)

G06F 1/00 370,
G06F 15/00 330,
G06T 7/00 510