

(19) 日本国特許庁(JP)

(12) 特 許 公 報(B2)

(11) 特許番号

特許第4107420号
(P4107420)

(45) 発行日 平成20年6月25日(2008.6.25)

(24) 登録日 平成20年4月11日(2008.4.11)

(51) Int.Cl.		F I		
G06F 21/20	(2006.01)	G06F 15/00	330F	
G09C 1/00	(2006.01)	G09C 1/00	640E	
H04L 9/32	(2006.01)	H04L 9/00	673D	
H04L 9/08	(2006.01)	H04L 9/00	601F	

請求項の数 13 (全 10 頁)

(21) 出願番号	特願2002-504068 (P2002-504068)	(73) 特許権者	591034154
(86) (22) 出願日	平成13年6月22日(2001.6.22)		フランス テレコム
(65) 公表番号	特表2004-501458 (P2004-501458A)		フランス国 パリ 75015 プラス
(43) 公表日	平成16年1月15日(2004.1.15)		ダルレ 6
(86) 国際出願番号	PCT/FR2001/001989	(74) 代理人	100092277
(87) 国際公開番号	W02001/099337		弁理士 越場 隆
(87) 国際公開日	平成13年12月27日(2001.12.27)	(72) 発明者	ゲラン, ディディエ
審査請求日	平成15年10月9日(2003.10.9)		フランス国 14000 カーン リュ
(31) 優先権主張番号	00/08070		マレシャル ガリエニ 81
(32) 優先日	平成12年6月23日(2000.6.23)	(72) 発明者	ジロー, マルク
(33) 優先権主張国	フランス (FR)		フランス国 14000 カーン リュ
			ベルナール ヴァニエ 9
		審査官	岩崎 志保

最終頁に続く

(54) 【発明の名称】 安全なバイOMETリック認証／識別方法、バイOMETリックデータ入力モジュールおよび検証モジュール

(57) 【特許請求の範囲】

【請求項1】

通信網を介して互いに接続されている検証モジュールと少なくとも1つのバイOMETリックデータ入力モジュールとを具備しており、前記少なくとも1つのバイOMETリックデータ入力モジュールがバイオセンサを少なくとも有しており、前記少なくとも1つのバイOMETリックデータ入力モジュールはいかなる秘密キーを保持していない、バイOMETリックデータ認証システムのための安全なバイOMETリック認証方法であって、

a) 前記少なくとも1つのバイOMETリックデータ入力モジュールは、前記バイOMETリックセンサがユーザのバイOMETリックデータを検出したとき当該バイOMETリックデータを記録し、

b) 前記少なくとも1つのバイOMETリックデータ入力モジュールは、前記検証モジュールに対して多様化値を発生するように要求し、

c) バイOMETリック認証毎に、前記検証モジュールは、前記少なくとも1つのバイOMETリックデータ入力モジュールからの前記要求にตอบสนองして多様化値を発生して、当該少なくとも1つのバイOMETリックデータ入力モジュールにその発生した前記多様化値を伝達し、

d) 前記少なくとも1つのバイOMETリックデータ入力モジュールは、前記検証モジュールから前記多様化値を受けて、記録した前記バイOMETリックデータを前記多様化値に連結し、その連結したバイOMETリックデータを暗号化し、その暗号化されたバイOMETリックデータを前記検証モジュールに伝送し、

e) 前記検証モジュールは、前記暗号化されたバイオメトリックデータを受信し、その受信したデータを唯一の秘密キーによって解読し、暗号化の際に所定の多様化値が考慮されたことを検証する

ことを特徴とする安全なバイオメトリック認証方法。

【請求項 2】

前記多様化値がランダムデータ要素であることを特徴とする請求項 1 に記載の安全なバイオメトリック認証方法。

【請求項 3】

前記多様化値が計数の結果であることを特徴とする請求項 1 ～ 2 のいずれか一項に記載の安全なバイオメトリック認証方法。

【請求項 4】

前記多様化値が時間データ要素（日付、時間）であることを特徴とする請求項 1 ～ 3 のいずれか一項に記載の安全なバイオメトリック認証方法。

【請求項 5】

暗号化アルゴリズムが公開キー非対称暗号化アルゴリズムであり、前記少なくとも 1 つのバイオメトリックデータ入力モジュールは、前記連結したバイオメトリックデータを前記公開キー非対称暗号化アルゴリズムの公開キーで暗号化し、前記検証モジュールは、前記暗号化された連結したバイオメトリックデータを解読するために、前記公開キー非対称暗号化アルゴリズムの秘密キーを前記唯一の秘密キーとして使用して解読することを特徴とする請求項 1 ～ 4 のいずれか一項に記載の安全なバイオメトリック認証方法。

【請求項 6】

前記検証モジュールは、各認証要求ごとに、前記公開キーを前記少なくとも 1 つのバイオメトリックデータ入力モジュールに伝達することを特徴とする請求項 5 に記載の安全なバイオメトリック認証方法。

【請求項 7】

前記少なくとも 1 つのバイオメトリックデータ入力モジュールは前記公開キーを記憶することを特徴とする請求項 5 または 6 に記載の安全なバイオメトリック認証方法。

【請求項 8】

前記少なくとも 1 つのバイオメトリックデータ入力モジュールに記憶されたキーが証明証の検証キーであり、前記証明証が前記検証モジュールの公開キーでありかつ当該検証モジュールによって前記少なくとも 1 つのバイオメトリックデータ入力モジュールに伝達されることを特徴とする請求項 5 ～ 7 のいずれか一項に記載の安全なバイオメトリック認証方法。

【請求項 9】

暗号化アルゴリズムが秘密キー対称アルゴリズムであり、秘密キーが前記少なくとも 1 つのバイオメトリックデータ入力モジュールにおいて生成され、前記秘密キーが非対称システムによって暗号化され、暗号化の結果が、前記秘密キー対称アルゴリズムで暗号化された前記連結されたバイオメトリックデータと共に前記検証モジュールに伝達され、当該検証モジュールがバイオメトリックデータを解読することを特徴とする請求項 1 ～ 4 のいずれか一項に記載の認証方法。

【請求項 10】

いかなる記憶した秘密キーも保持していないバイオメトリックデータ入力モジュールと、バイオメトリックデータ検証モジュールとを備えるバイオメトリックデータ認証システムであって、前記バイオメトリックデータ入力モジュールが、請求項 1 ～ 9 のいずれか一項に記載の各暗号操作ごとに、前記バイオメトリック検証モジュールによって発生されて当該バイオメトリックデータ入力モジュールに伝達された異なる多様化値を導入し、バイオメトリックデータを暗号化するための暗号操作を実行する第 1 の手段とを含むことを特徴とするバイオメトリックデータ認証システム。

【請求項 11】

前記バイオメトリックデータ検証モジュールが、通信網を介して受信した暗号化された

10

20

30

40

50

バイオメトリックデータを、前記検証モジュールのみが保持する秘密キーを用いて解読するための暗号解読操作を実行する第2の手段を含み、当該バイオメトリックデータは多様化値に連結されており、この多様化値は請求項1～9のいずれか一項に記載の各暗号化バイオメトリックデータ要素ごとに異なることを特徴とする、請求項10に記載のバイオメトリックデータ認証システム。

【請求項12】

前記バイオメトリックデータ検証モジュールが通信網によって複数のバイオメトリックデータ入力モジュールに接続されることを特徴とする請求項11に記載のバイオメトリックデータ認証システム。

【請求項13】

前記バイオメトリックデータ検証モジュールが安全でないまたは保護されていない通信網によって前記バイオメトリックデータ入力モジュールに接続されていることを特徴とする請求項11～12のいずれか一項に記載のバイオメトリックデータ認証システム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、安全なバイオメトリックデータの認証／識別方法に関する。

【0002】

説明を簡単にするために、認証方法の説明は後で述べる。

本発明はさらに、本発明方法を実行することができる、バイオメトリックデータ入力モジュールおよび上記データの検証方法に関し、これら2つのモジュールが協働して認証システムの実施態様の一部をなす。

【0003】

本発明は特に、通信網を介してある程度の距離離れた所に配置された装置による、検証を伴うバイオメトリック認証または識別の分野に適用することができる。

バイオメトリック入力モジュールとは、認証システムのユーザのバイオメトリック要素を記録することができるバイオメトリックセンサ等の装置を意味するものとする。

バイオメトリック検証モジュールとは、バイオメトリック情報を処理してその情報とその信憑性を検証することができる装置を意味するものとする。この装置は、データ処理コンピュータ、または処理システムに組み込まれる特定の電子カードにすることができる。

【0004】

【特許文献1】

1998年7月23日公開のW098/32093

上記特許文献にはバイオメトリックデータの再生防止方法が記載されている。

再生とは、認証システムのユーザのバイオメトリックデータを取り込んで、このデータを検証装置に送り込みし、そのユーザであると主張することからなる全ての悪意のある動作を意味するものとする。

この出願に記載の方法は、「細部」ともよばれる特徴的なバイオメトリック要素は二つの入力で同じ値になることはないことに基づくものである。上記の方法は、前回の認証および識別のテストから受信した「細部」を記憶する必要があることと、このシステムをだますために故意にわずかに変更した再生データに対して防止策を講じることが不可能であるという点で限界がある。

【0005】

また、「細部」の遠隔検証と、そのための通信網を介したデータの送信とによってバイオメトリック方法を実行することができるシステムもある。

この場合は、提案された解決策がデータの盗難および再生に関連する問題を考慮していないか、あるいはシステムの種々のモジュール内の暗号秘密を組み合わせたものとなっている。この解決策は例えば下記文献にみることができる。

【0006】

【特許文献2】

10

20

30

40

50

1998年11月06日公開の国際特許出願W098/25385

上記文献に記載の方法はデータがライン上で漏れるのを防ぐが、このデータの再生を防止することはできない。2つの通信モジュールが、一対のプライベートキーを使用可能にすることができる。

このシステムの各種モジュールに秘密が存在する場合には、これらの各種モジュールに記憶された秘密が盗まれるおそれがある。各種モジュールに記憶された秘密の盗難は、モジュール自身、特に一般市民がアクセスできるように置かれたバイオメトリック入力モジュールの実際上の盗難となる。

【0007】

従来のいくつかの解決策では、モジュール、特にバイオメトリック入力モジュールは秘密を内部記憶するように構成されていないが、この構成は例えばスマートカードまたはバッジによってユーザーから秘密が提供されたときに必要である。

このようなシステムは例えば下記文献に記載されている。

【0008】

【特許文献3】

1999年3月24日公開のドイツ国特許出願第2329499号

【特許文献4】

1998年1月27日公開の国際特許出願W097/05578号

後者の文献の解決策では、ユーザーが物理的ツール（スマートカードまたはバッジ）を着用または携帯するため、使い易さおよびバイオメトリックスの人間工学が未知数である。

【0009】

【発明が解決しようとする課題】

本発明の方法の目的は上記の欠点を解決することにある。

実際には、本発明は、必ずしも安全ではない通信網を介して一つまたは複数のバイオメトリック検証モジュールに接続されたバイオメトリック入力モジュールを中心に構成されたバイオメトリック識別または認証方法であって、データの再生による攻撃を避け、ユーザーに物理的物体（スマートカード）の着用を強制せず、バイオメトリック入力モジュール内に一つまたは複数の秘密が存在することを要求しない方法を提供するものである。

【0010】

従って、本発明は、データの再生を防止するための要素とデータの機密性を保証する暗号要素とを含み、これらの要素がいずれもバイオメトリック特徴が入力される場所に秘密が存在することを要求せず、このデータが「細部」等のバイオメトリックデータを含む、安全なバイオメトリック方法に関する。

バイオメトリック入力モジュールとして知られるローカルバイオメトリックモジュールと、バイオメトリック検証モジュールとして知られる遠隔モジュールとの間に保護を適用することができる。

【0011】

本発明方法の実行は、認証されたいユーザーにとっては明快である。ユーザーはこの方法を実行するのにいかなる物理的ツールも着用する必要がない。バイオメトリック検証モジュールは、各認証ごとに値を記憶する必要がなくなる。

本発明方法は特に、例えば通信網を介して接続された検証モジュールである遠隔バイオメトリックモジュールから特別な保護を全く必要とせずに、この認証を実施することができる。

【0012】

本発明の提案する認証方法によって、バイオメトリック入力モジュール内に秘密を記憶しなくてすむようにすることができる。また、バイオメトリックデータの送信のやり直しの不要を保証することもできる。

一般に、本発明はバイオメトリックシステムに適用可能である。

【0013】

【課題を解決する手段】

本発明の目的は特に、暗号化されたバイオメトリックデータを検証モジュールに伝達することを含む安全なバイオメトリック認証方法において、主に、バイオメトリックデータを暗号アルゴリズムによって暗号化し、次いで、実行された各暗号化操作ごとに異なる多様化値を導入することで構成されることを特徴とする方法を提供することにある。

【0014】

【発明の実施の形態】

一実施例では、多様化値が検証モジュールによって生成され、バイオメトリックデータ入力モジュールに送信される。

別の実施例では、多様化値が入力モジュールおよび検証モジュールによって生成される。多様化値はバイオメトリックデータと組み合わせられ、暗号操作はこの組み合わせで得られたデータ要素に対して実行される。

一変形例では、多様化値がランダムデータ要素である。

別の変形例では、多様化値が計数の結果である。

【0015】

別の変形例では、多様化値が時間データ要素（日付、時間）である。

一実施例では、暗号化アルゴリズムが公開キー非対称アルゴリズムである。

一変形例では、検証モジュールの公開キーが、各認証要求ごとに検証モジュールによって入力モジュールに送信される。

別の変形例では、公開キーがバイオメトリックデータ入力モジュールに記憶される。

別の変形例では、入力モジュールに記憶されたキーが証明証の検証キーであり、この証明証が検証モジュールの公開キーの証明証でありかつ検証モジュールによって入力モジュールに送信される。

【0016】

別の実施例では、暗号化アルゴリズムが秘密キー対称アルゴリズムである。

秘密キーは入力モジュールによって生成されるのが有利である。

秘密キーは非対称アルゴリズムによって暗号化され、暗号化の結果が検証モジュールに送信され、検証モジュールがバイオメトリックデータを解読することができるのが有利である。

【0017】

本発明はさらに、主に、バイオメトリックデータを暗号化するための暗号操作を実行する手段と、上記した各暗号操作ごとに異なる多様化値を導入する手段とを含むことを特徴とするバイオメトリックデータ入力モジュールに関するものである。

別の特徴によれば、多様化値がモジュール自身によって生成されるか、あるいは外部から提供される。

【0018】

本発明はさらに、主に、通信網を介して受信した暗号化されたバイオメトリックデータを解読するための暗号操作を実行する手段と、各暗号化バイオメトリックデータごとに異なる多様化値を保持する手段とを含むことを特徴とするバイオメトリックデータ検証モジュールに関するものである。

バイオメトリックデータ検証モジュールは通信網によって複数のバイオメトリックデータ入力モジュールに接続できるのが有利である。

別の特徴によれば、多様化値は検証モジュール自身によって生成される。

バイオメトリックデータ入力モジュールと検証モジュールとは保護されていない通信網によって接続することができる。

本発明の他の特性および利点は、添付図面を参照して下記の詳細な説明を読めば明らかになるであろう。

【0019】

【実施例】

先ず最初に、図1、すなわちバイオメトリック認証方法の第1および第2の作動法をそれぞれ示すパートIおよびIIを参照して以下説明する。

実施の態様は、暗号プロトコルとして、RSA（リベストシャミールアルドレマン）アルゴリズム等の公開キーアルゴリズムを使用する。

本発明方法の実行に適しているプロトコルはRSAアルゴリズムだけではない。全てのキー交換プロトコル、例えば下記の文献に記載されているもの：

【0020】

規格ISO/IEC DIS 11770-3「情報技術安全保護技術キー管理」のパート3の「非対称技術を使用したメカニズム」が、使用するメカニズムによってバイOMETリック識別／認証の検証に対して責任のあるエンティティを認証することができる範囲、および、このエンティティが以下に述べる多様化値を伝送する範囲において、適している。

10

【0021】

バイOMETリック入力モジュールSでは、ユーザのバイOMETリック要素の伝達が再生されるのを防止するために多様化値VDが使用される。この値はランダム値、カウンタから得られる結果、時間要素等にすることができる。

バイOMETリックプロセスは、ユーザがバイOMETリックセンサ1の前に現われることによって入力モジュールSを作動したときに作動する。

この作動によって多様化値VDが生成される。

【0022】

この図1に示される方法の実行の第1の態様では、多様化値の生成はバイOMETリック検証モジュールVによって実施される。

20

このようにして、本発明方法の作動は、この態様の場合には、検証モジュールVに対する入力モジュールSからの多様化値VDの要求によって表される（図では動作A）。

【0023】

バイOMETリック検証モジュールVは次いで、多様化値をバイOMETリック入力モジュールSに送信する（動作B）。バイOMETリック入力モジュールSは、バイOMETリック要素の特性要素Eを抽出し、この要素を多様化値VDと組合せ、公開非対称暗号関数 e_v の制御下でこれらのパラメータに主として関係する暗号化操作Cを行い、その結果Cを検証モジュールに送信する（動作C）。

暗号化操作は下記の式で表される：

$$C = e_v (E + VD)$$

30

（ここで、符号「+」はデータ連結操作を象徴的に示す。）

暗号計算によって、適切なプライベートキーを有する唯一の人が、送信されたバイOMETリックデータを正確に解釈し、多様化値が考慮に入れられたことを検証することができることが保証され、検証は、

$d_v(C)$ は $(E + VD)$ に等しい（ここで、 d_v は解読関数）である。

【0024】

所定の人、すなわち所定のバイOMETリックデータ要素Eを保持している人、に対して新しい認証手続が実行される場合に、生成された（さらに検証システムによって送信される）多様化値は同じものではなく、図1の概略図のパートIIで示すように値VD'に等しいので、再生が防止される。換言すれば、段階Iでライン上で情報Cを得ることに成功し、この暗号化情報Cを再生した権限のない人は、多様化値がもはやVDでなく、新しい値VD'となっているので検証時にそれ以上先に進むことができない。

40

上記の実施の態様では、多様化値VDはバイOMETリック検証モジュールによって生成され、次いで、バイOMETリック入力モジュールに送信される（動作A）。

【0025】

別の実施の態様では、バイOMETリック入力モジュール自身によって多様化値を生成することができる。この場合は、バイOMETリック検証モジュール自身もまたこの多様化値を生成することができる。この場合はランダム値ではなく、例えば日付に関係することは理解できよう。すなわち、検証モジュールは、送信されたデータが前回の送信の再生にならないことを検証することができる（この実施の態様では動作Aはない）。

50

【0026】

この実施の態様では、バイオメトリック入力モジュールは、そのメモリに公開キー非対称暗号アルゴリズムの公開キーを記憶しており、バイオメトリック検証モジュールの公開非対称暗号キーの制御下で暗号計算を行う。この暗号計算によって、既に述べたように適切なプライベートキー d_v を所持するバイオメトリック検証モジュールのみが、送信されたバイオメトリックデータを正確に解釈し、多様化値が考慮に入れられたことを検証することができる。

【0027】

別の実施の態様では、バイオメトリック入力モジュールのメモリに永久記憶されたキーを証明証の検証キーにすることができる。この場合は、バイオメトリック検証モジュールVは、バイオメトリック入力モジュールに多様化値VDとその証明された公開暗号化キーCert(PUB e_v)を送信する。この証明証は、バイオメトリック入力モジュールのメモリに永久記憶されたキーを用いて検証される。証明証の検証が肯定である場合は、その後、バイオメトリック入力モジュールがバイオメトリック検証モジュールの公開キーを使用して、バイオメトリック検証モジュールに次に転送されるバイオメトリックデータの機密性を確保することができる。

10

【0028】

別の実施の態様では、入力モジュールが秘密キーclを生成して、このclを使用する対称アルゴリズムを用いて送信用データを暗号化することができる。一般に、使用するアルゴリズムはDES(データ暗号化規格)アルゴリズムにすることができる。次いで、入力モジュールは、この対称アルゴリズムとこの目的のために生成された秘密キーclとを用いて、連結されたデータE+VDを暗号化し、この暗号化されたデータを検証モジュールに伝送する。検証モジュールが入力モジュールによって生成された秘密キーを保持していないときは、入力モジュールは、公開キーアルゴリズムによって暗号化された秘密キーを送信して、検証モジュールが受信したデータを解読できるようにする。検証モジュールは暗号化アルゴリズムに対応する逆関数を実施して、解読された値E+VDを得る。さらに、プライベートキーclを1つのランダム変数に連結し、得られたデータ要素を公開キーアルゴリズムを用いて暗号化することができる。

20

【0029】

次に、図2の概略図を参照する。この図はバイオメトリック入力モジュールSおよび遠隔バイオメトリック検証モジュールVにおける本発明方法の実行を示している。バイオメトリック入力モジュールは従来通り、バイオメトリックセンサ1を備える。このセンサは、システムのユーザの指紋を細部抽出モジュール22を与え、このモジュールはこの抽出で得られた要素Eをバイオメトリック入力モジュールS内の暗号モジュール20に送信することができる。暗号モジュールは例えば、公開キー、すなわちパラメータPUB e_v (このキーの名称がPUB e_v の場合)を含む不揮発性メモリ21と組み合わされた市販の暗号処理装置によって具体化される。

30

【0030】

この図に示された暗号化過程1から7に従う場合、オペレータは認証操作を行いたいときに、バイオメトリックセンサ1の前に出る、するとこのセンサがユーザのバイオメトリックデータ要素の指紋を作成する。センサはこの指紋を細部抽出モジュール22に送信する。抽出モジュールはこの抽出で得られたデータを暗号モジュールに送信し、次いで、暗号モジュールは遠隔バイオメトリック検証モジュールから多様化値VDを受信したあとに、このデータに関係する暗号化操作を暗号アルゴリズムのパラメータに基づいて行う。バイオメトリック検証モジュールはバイオメトリックセンサ1の作動時に作動される。

40

【0031】

検証モジュールVはさらに、プライベートキー、すなわち公開キー暗号アルゴリズムで使われる秘密、すなわちパラメータPRIV d_v (プライベートキーの名称がPRIV d_v の場合)を記憶する不揮発性メモリ201と組み合わされた暗号モジュール200を含む。

本発明および本発明の全ての実施の態様では、バイオメトリック入力モジュールにいかな

50

る秘密も記憶されていない。このバイオメトリック入力モジュールは公共の建物に設置することができるモジュールであり、秘密を保持するバイオメトリック検証モジュールVに通信網Rを介して接続される。

【0032】

図3の概略図は本発明の方法を実行する認証システムを示している。

図4の概略図からわかるように、本発明の方法は認証システムを設置するように完全に適合されており、このシステムでは複数の独立した、遠隔のバイオメトリック入力モジュールSを通信網を介して単一の所定のバイオメトリック検証モジュールVに接続することができる。

【0033】

すなわち、本発明によって（バイオメトリック入力モジュールおよびユーザーに対して）バイオメトリック検証を局所的に実施する必要がなく、バイオメトリック認証／識別方法を実行することができ、バイオメトリックデータの盗難の発生および再生の危険がなく、秘密の暗号要素をバイオメトリック入力モジュールに入れる必要がない。

例えば、図4に示すような単一の集中型バイオメトリック検証モジュールに接続された複数のバイオメトリック入力モジュールを有するバイオメトリックアクセス制御メカニズムが可能である。

例として、物理的なアクセスポイント（建物のドア等）または論理的アクセスポイント（コンピュータサーバー等）の開閉に適用されるアクセス制御サービスを考えることができる。

【図面の簡単な説明】

【図1】 本発明による、保護された認証方法の実行を概略的に示す。

【図2】 バイオメトリック入力モジュールおよび遠隔バイオメトリック検証モジュールで本発明方法を実行するための実行図を示す。

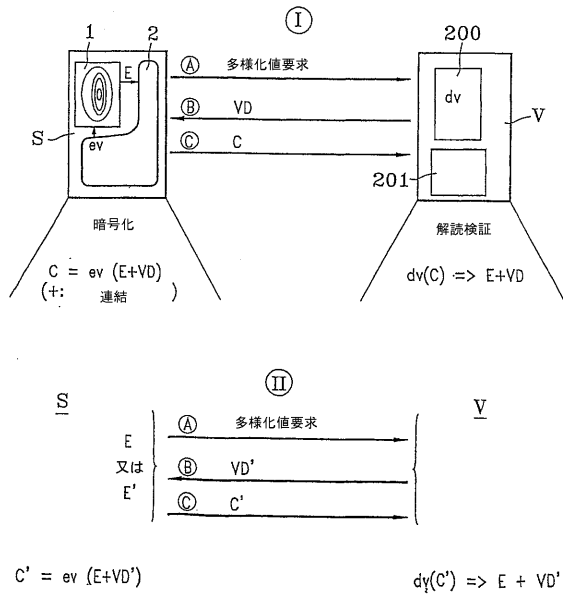
【図3】 本発明によるバイオメトリックデータ認証モジュールを示す。

【図4】 本発明の方法を実行する認証システムの変形例を示す。

10

20

【図 1】



フロントページの続き

- (56)参考文献 特開平11-338826 (JP, A)
特開平02-311946 (JP, A)
特開2000-092046 (JP, A)
特開2000-113085 (JP, A)
特開平7-50665 (JP, A)
D.W.Davies and W.L.Price, ネットワーク・セキュリティ, 日本, 日経マグローヒル社, 1985年12月5日, 第1版, p.126-130

(58)調査した分野(Int.Cl., DB名)

G06F 21/20
G09C 1/00
H04L 9/08
H04L 9/32