(19) RÉPUBLIQUE FRANÇAISE

INSTITUT NATIONAL
DE LA PROPRIÉTÉ INDUSTRIELLE

PARIS

(11) N° de publication : **2 649 509**
(à n'utiliser que pour les commandes de reproduction)

(21) N° d'enregistrement national : **89 09091**

(51) Int Cl[5] : G 06 F 11/00.

(12) DEMANDE DE BREVET D'INVENTION A1

(22) Date de dépôt : 6 juillet 1989.

(30) Priorité :

(43) Date de la mise à disposition du public de la demande : BOPI « Brevets » n° 2 du 11 janvier 1991.

(60) Références à d'autres documents nationaux apparentés :

(71) Demandeur(s) : *Mohammed ACHEMLAL, Richard COLLOT et Michel MOURIER.* — FR.

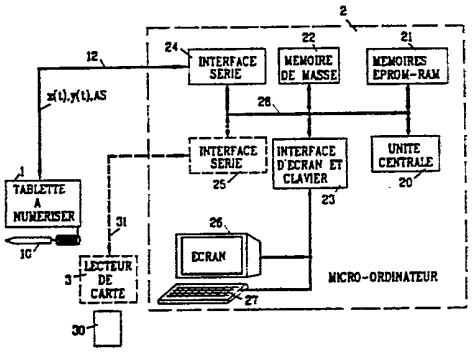
(72) Inventeur(s) : Mohammed Achemlal ; Richard Collot ; Michel Mourier.

(73) Titulaire(s) :

(74) Mandataire(s) : Martinet et Lapoux.

(54) Procédé et systèmes de vérification de signatures à optimisation de paramètres dynamiques.

(57) Un système selon l'invention comprend une tablette à numériser 1 équipée d'un stylo 10, un micro-ordinateur 2 et un lecteur de carte à puce 3. La tablette est de type classique et délivre des signaux (x(t), y(t)) indiquant la position de la pointe du stylo sur la tablette lors du tracé d'une signature. A partir des signaux fournis par la tablette, le micro-ordinateur calcule différents paramètres de type dynamique par exemple relatifs à la vitesse, l'accélération. Chaque signataire est en possession d'une carte à puce mémorisant un code d'identification et des valeurs moyennes de référence des différents paramètres correspondant à sa signature. Le micro-ordinateur transmet vers la carte à puce les valeurs des paramètres correspondants à la signature à vérifier et un traitement de décision est effectué dans la carte par calcul de distance par rapport aux valeurs moyennes de référence. Le procédé selon l'invention se caractérise par un algorithme d'optimisation implanté dans le micro-ordinateur afin de sélectionner spécifiquement pour chaque signature les paramètres qu'il convient d'utiliser pour minimiser l'erreur de décision.



FR 2 649 509 - A1

Procédé et systèmes de vérification de signatures à optimisation de paramètres dynamiques

La présente invention concerne plus particulièrement des systèmes de vérification de signatures de type dynamique. Néanmoins, l'invention est applicable également pour des systèmes de vérification de signatures de type mixte dans lesquels sont traités des paramètres statiques et des paramètres dynamiques.

Un système de vérification dynamique de signatures traite des signaux produits lors du tracé des signatures tels par exemple que des signaux de pression, de vitesse et/ou d'accélération de la pointe d'un stylo avec lequel sont tracées les signatures. Le système est conçu pour authentifier des signatures, c'est-à-dire pour vérifier leur conformité, par comparaison avec des références de signatures préalablement enregistrées dans le système. Une signature est représentée par un ensemble de paramètres dérivés des signaux produits lors du tracé de la signature.

La signature manuscrite est un moyen d'authentification universellement accepté et a une valeur juridique reconnue. Les systèmes de vérification de signatures trouvent des applications importantes dans le domaine de la sécurité d'accès à des systèmes informatiques et de manière plus générale dans le domaine de l'identification des personnes. A titre d'exemple, un système de vérification de signatures est utilisable pour vérifier l'identité d'une personne effectuant un paiement par chèque ou carte bancaire, ou désirant accéder à des ressources informatiques telles que des fichiers de données et programmes de calcul, ou encore désirant accéder à des locaux et zones réservés.

Différents systèmes de vérification dynamique de signatures sont disponibles actuellement et présentent de manière générale les inconvénients suivants :

- ils doivent nécessairement être équipés de tablettes à numériser spécifiques, développées et dédiées uniquement pour la saisie des signatures ;

- l'ensemble des paramètres utilisés pour représenter les signatures est déterminé une fois pour toutes et ne varie pas en

fonction des personnes ; une telle approche est sujette à critiques car la fiabilité d'un paramètre varie sensiblement d'une personne à l'autre et un paramètre très stable pour un individu est parfois très variable pour une autre personne ; et

- les principes de traitement et les paramètres utilisés par ces systèmes doivent généralement rester confidentiels et ne pas être connus des personnes à identifier, ce qui est souvent mal perçu par lesdites personnes.

La présente invention vise à fournir un procédé et des systèmes de vérification de signatures ne présentant pas les inconvénients ci-dessus.

A cette fin, le procédé selon l'invention pour vérifier la conformité de signatures échantillons avec des signatures de référence selon lequel les signatures sont représentées par des fichiers comprenant les valeurs de plusieurs paramètres notamment de type dynamique, est caractérisé en ce que les fichiers sont composés d'un nombre variable de paramètres sélectionnés spécifiquement parmi un ensemble prédéterminé de paramètres par un algorithme d'optimisation de manière à minimiser des erreurs de décision.

Un système de vérification de signatures selon l'invention pour la mise en oeuvre du procédé ci-dessus est caractérisé en ce qu'il comprend des moyens pour produire des signaux numériques représentatifs des signatures échantillons à traiter des moyens pour indiquer au système l'identité supposée de chaque signataire, des moyens activés lors d'une phase d'apprentissage pour déterminer les fichiers de référence par sélection des paramètres optimaux et calcul de leurs valeurs moyennes à partir de plusieurs échantillons de signatures de référence, des moyens pour mémoriser les fichiers de référence, des premiers moyens activés pendant une phase opérationnelle pour calculer des fichiers de paramètres correspondant aux signatures échantillons, des seconds moyens pour calculer des distances entre les valeurs des paramètres des fichiers, et des moyens pour décider de la conformité des signatures échantillons avec les signatures de référence en fonction desdites distances.

L'invention sera mieux comprise à la lecture de la description suivante du procédé et de plusieurs réalisations préférées des systèmes de vérification de signatures selon l'invention en référence aux dessins annexés correspondants dans lesquels :

- la Fig. 1 est un bloc-diagramme montrant la structure matérielle de plusieurs réalisations préférées d'un système selon l'invention pour la vérification des signatures ;

- la Fig. 2 est un bloc-diagramme fonctionnel correspondant à une première réalisation préférée du système ;

- la Fig. 3 montre un exemple de signature ;

- les Figs. 4 à 8 montrent des signaux produits par le système et relatifs à l'exemple de signature de la Fig. 3 ;

- les Figs. 9 et 10 sont des courbes montrant l'évolution de taux d'erreur en fonction de seuils de décision respectivement lorsque les paramètres sont quelconques et lorsque les paramètres sont sélectionnés à l'aide d'un algorithme d'optimisation ;

- la Fig. 11 montre en détail l'algorithme d'optimisation des paramètres qui est mis en oeuvre dans le système ; et

- la Fig. 12 est un bloc-diagramme fonctionnel correspondant à une seconde réalisation préférée du système selon laquelle il est prévu un lecteur de carte à puce.

En référence à la Fig. 1, une première réalisation préférée du système selon l'invention comprend une tablette à numériser 1 et un micro-ordinateur 2. Une seconde réalisation du système décrite plus précisément ci-après en référence à la Fig. 12 comprend également un lecteur de carte à puce 3.

La tablette à numériser 1 également appelée tablette graphique, est par exemple constituée par le modèle MM961 commercialisé sous la marque déposée SUMMAGRAPHICS. La tablette 1 est équipée d'un stylo 10. De préférence, un cadre de dimensions prédéterminées est apparent sur le plan de la tablette 1 et indique le lieu où il convient de signer en utilisant le stylo 10. La tablette 1 délivre en sortie des coordonnées x(t) et y(t) de la pointe du stylo 10 par rapport à un repère orthogonal du plan de la tablette 1. Un signal d'information AS indiquant à l'état "1" l'appui de la pointe du stylo 10 sur le plan de la tablette 1 est également produit par la tablette 1. Les coordonnées x(t), y(t) et

le signal AS sont échantillonnés par la tablette 1 typiquement à la fréquence de 100 Hz et sont transmis vers le micro-ordinateur sous la forme de mots numériques sérialisés.

Le micro-ordinateur 2 comprend essentiellement une unité centrale 20, des mémoires de programme et de travail 21 de types EPROM et RAM, une mémoire de masse 22 par exemple sous la forme d'un disque dur, des interfaces 23 et 24, et des moyens de dialogue homme-machine sous la forme d'un écran vidéo 26 et d'un clavier 27.

L'unité centrale 20 est constituée par exemple par un microprocesseur. L'unité centrale 20 est connectée de manière classique par des bus de données, d'adresse et de commande 28 à chacun des éléments du micro-ordinateur 2.

La mémoire de masse 22 est essentiellement destinée à stocker des fichiers de référence pour la vérification des signatures. Eventuellement, et dans le cas notamment où la capacité de la mémoire EPROM 21 n'est pas de taille suffisante, la mémoire de masse 22 héberge partiellement ou en totalité un programme et des utilitaires de gestion du système ainsi que des algorithmes de calcul de paramètres et de vérification de signatures.

L'interface 23 a pour fonction de connecter l'écran 26 et le calvier 27 au bus 28.

L'interface 24 est une interface série de type UART pour connecter la tablette à numériser 1 au micro-ordinateur 2.

Pour la seconde réalisation préférée du système, une seconde interface série 25 de type UART équipe le micro-ordinateur 2 afin de connecter le lecteur de carte 3 à travers une seconde liaison série 31 de type RS232C.

En référence à la Fig. 2, les traitements effectués par le micro-ordinateur 2 lors d'une phase d'apprentissage et lors d'une phase opérationnelle d'authentification de signatures sont maintenant décrits.

La phase d'apprentissage est prévue afin de calculer et mettre en place dans le micro-ordinateur 2 des fichiers de paramètres de référence qui sont nécessaires pour la vérification des signatures lors de la phase opérationnelle d'authentification.

Il est supposé en exemple de réalisation que le système est configuré pour la vérification de I=100 signatures différentes S_1, $S_2 \ldots S_i, \ldots S_I$.

I=100 fichiers de paramètres de référence FR_1, $FR_2 \ldots FR_i, \ldots FR_I$ correspondant respectivement aux I=100 signatures S_1, $S_2 \ldots S_i, \ldots S_I$ sont mémorisés dans le micro-ordinateur 2. Les fichiers FR_i ont des tailles différentes et contiennent chacun un nombre variable de paramètres qui sont déterminés pour une vérification optimale de la signature S_i correspondante. Un fichier de paramètres de référence FR_i représentatif d'une signature S_i est identifié à l'aide d'une adresse AD_i.

Pendant la phase d'apprentissage, pour chaque signature S_i, par exemple J=10 signatures échantillons S_{i1}, $S_{i2} \ldots S_{ij}, \ldots S_{iJ}$ correspondant à la signature de référence S_i sont successivement délivrés par le signataire. De préférence, les deux premières et les deux dernières signatures ne sont pas utilisées par le système afin de tenir compte d'un temps d'adaptation du système au départ et de la fatigue du signataire à la fin de la série des 10 signatures échantillons.

Dans le micro-ordinateur 2, les signaux échantillonnés x(t), y(t) et AS sont traités dans un module de programme de traitement 4A. Le traitement effectué par le module 4A consiste essentiellement en un filtrage des signaux x(t), y(t) et AS et en des translations effectuées sur les signaux x(t) et y(t) afin de les représenter dans un repère orthogonal (O, X, Y) différent du repère de la tablette à numériser 1. Le repère (O, X, Y) est montré à la Fig. 3 et est déterminé de telle manière que des points extrêmes de la signature, en bas et à gauche de la signature, soient compris respectivement dans l'axe X et l'axe Y du repère. De préférence, un contrôle visuel du dessin de la signature après traitement est également effectué par un opérateur à partir de l'écran 26.

Schématiquement, un interrupteur 4B ayant deux positions PA et PO est représenté à la Fig. 2. Les positions PA et PO correspondent respectivement à la phase d'apprentissage et à la phase opérationnelle d'authentification. Lorsque le système est en phase d'apprentissage PA, les signaux x(t), y(t) et AS délivrés par le

module 4A sont transférés vers un module de calcul et choix de paramètres de référence optimaux 4C.

Typiquement pour chaque signature échantillon S_{ij}, 34 paramètres $c1_{ij}$ à $c34_{ij}$ sont calculés par le module 4C. La liste de ces paramètres est donnée ci-dessous :

- Vitesse moyenne de la pointe du stylo lors du tracé de la signature (paramètre c1) ;
- Vitesse maximale de la pointe du stylo (paramètre c2) ;
- Instant du maximum de vitesse de la pointe du stylo par rapport au début de la signature (paramètre c3) ;
- Amplitude du premier pic positif de vitesse de la pointe du stylo selon l'axe X (paramètre c4) ;
- Instant du premier pic positif de vitesse de la pointe du stylo selon l'axe X (paramètre c5) ;
- Amplitude du second pic positif de vitesse de la pointe du stylo selon l'axe X (paramètre c6) ;
- Instant du second pic positif de vitesse de la pointe du stylo selon l'axe X par rapport au début de la signature (paramètre c7) ;
- Durée de la signature (paramètre c8) ;
- Somme des durées des levées de la pointe du stylo lors du tracé de la signature (paramètre c9) ;
- Vitesse minimale de la pointe du stylo selon l'axe X (paramètre c10) ;
- Instant du minimum de la vitesse de la pointe du stylo selon l'axe X par rapport au début de la signature (paramètre c11) ;
- Accélération maximale de la pointe du stylo (paramètre c12) ;
- Nombre de composantes de la signature (paramètres c13) ;
- Instant de début d'une seconde composante de la signature par rapport au début de la signature (paramètre c14) ;
- Direction de départ de la signature (paramètre c15) ;
- Direction d'un vecteur reliant le début de la signature au début de la seconde composante de la signature (paramètre c16) ;
- Direction d'un vecteur reliant la fin d'une première composante de la signature au début de la seconde composante (paramètre c17) ;

- Direction de départ de la seconde composante (paramètre c18) ;
- Direction d'un vecteur reliant le début de la signature à la fin de la signature (paramètre c19) ;
- Moyenne d'une composante positive de la vitesse de la pointe du stylo selon l'axe X (paramètre c20) ;
- Moyenne d'une composante positive de la vitesse de la pointe du stylo selon l'axe Y (paramètre c21) ;
- Moyenne d'une composante négative de la vitesse de la pointe du stylo selon l'axe X (paramètre c22) ;
- Moyenne d'une composante négative de la vitesse de la pointe du stylo selon l'axe Y (paramètre c23) ;
- Durée totale de la composante positive de la vitesse de la pointe du stylo selon l'axe X (paramètre c24) ;
- Durée totale de la composante positive de la vitesse de la pointe du stylo selon l'axe Y (paramètre c25) ;
- Durée totale de la composante négative de la vitesse de la pointe du stylo selon l'axe X (paramètre c26) ;
- Durée totale de la composante négative de la vitesse de la pointe du stylo selon l'axe Y (paramètre c27) ;
- Nombre de passages à zéro de la vitesse de la pointe du stylo selon l'axe X (paramètre c28) ;
- Nombre de passages à zéro de la vitesse de la pointe du stylo selon l'axe Y (paramètre c29) ;
- Différence entre la vitesse maximale de la pointe du stylo selon l'axe X et la vitesse moyenne de la pointe du stylo selon le même axe (paramètre c30) ;
- Différence entre la vitesse maximale de la pointe du stylo selon l'axe Y et la vitesse moyenne de la pointe du stylo selon le même axe (paramètre c31) ;
- Différence entre les vitesses maximale et minimale de la pointe du stylo selon l'axe X (paramètre c32) ;
- Différence entre la vitesse maximale de la pointe du stylo selon l'axe X et la vitesse maximale de la pointe du stylo selon l'axe Y (paramètre c33) ; et
- Différence entre les vitesses maximale et minimale de la pointe du stylo selon l'axe Y (paramètre c34).

Les différents paramètres c1 à c34 sont maintenant explicités en référence à un exemple de signature montré à la Fig. 3 et aux formes d'onde des signaux x(t), y(t) et SA(t) et vitesses Vx(t) et Vy(t) correspondantes montrées aux Figs. 4 à 8.

Les vitesses Vx(t) et Vy(t) selon les axes X et Y sont déduites par calcul de dérivation respectivement à partir des signaux x(t) et y(t), les calculs étant effectués par le micro-ordinateur 2.

Le paramètre c1 correspondant à la vitesse moyenne de la pointe du stylo est définie par l'égalité suivante :

$C1 = \int_{DT} [Vx(t)]dt = \int_{DT} (Vx(t)^2 + Vy(t)^2)^{1/2} \cdot dt$,

où [V(t)] représente le module de la vitesse de la pointe du stylo et DT correspond au paramètre c8 et représente la durée totale de la signature.

La maximalisation de l'expression : $V(t) = (Vx(t)^2 + Vy(t)^2)^{1/2}$ permet de déterminer les paramètres $c2 = VM = (VMx^2 + VMy^2)^{1/2}$ et $c3 = t_0$ correspondant à la vitesse maximale VM et à l'instant t_0 de vitesse maximale (Figs. 5 et 8).

Les premier et second pics positifs de la vitesse Vx(t) interviennent respectivement à des instants t_1=c5 et t_2=c7 et ont des amplitudes VP1=c4 et VP2=c6 (Fig. 5).

Le signal SA est représenté à la Fig. 6. La durée totale de la signature DT=c8 est délimitée entre un premier front montant et un dernier front descendant du signal SA. Dans l'exemple de signature qui est ici considéré, le signataire ne lève la pointe du stylo qu'une seule fois et cela pendant une durée t_3, d'où c9=t_3.

Comme montré à la Fig. 5, le minimum Vmx=c10 de la vitesse Vx(t) est négatif et intervient un instant $t_4=t_0$=c11 après le début de la signature.

L'accélération A(t) de la pointe du stylo est déduite par un calcul de dérivation au second degré à partir des signaux x(t) et y(t). L'accélération maximale correspondant au paramètre c12 est obtenue par maximilisation de l'expression :

$A(t) = [[d^2x(t)/dt^2]^2 + [d^2y(t)/dt^2]^2]^{1/2}$.

Le paramètre c13 a une valeur égale à 2, la signature étant constituée de deux composantes C1 et C2 (Figs. 3 et 6). Une composante de signature est une portion de tracé executée sans

levée du stylo. Le paramètre c14 correspond à l'instant t_3 montré à la Fig. 6.

Les vecteurs de direction D1 à D4 montrés à la Fig. 3 correspondent respectivement aux paramètres c15 à c19. Les valeurs attribuées aux paramètres c15 à c19 sont par exemple des valeurs d'angle θ des directions des vecteurs par rapport à l'axe X.

Soit la fonction VPx(t) égale à la vitesse Vx(t) lorsque Vx(t) est positive et nulle lorsque Vx(t) est négative, le paramètre C20 est défini par l'égalité :

$c20 = \int_{DT} VPx(t).dt.$

Le paramètre c21 est défini par l'égalité :

$c21 = \int_{DT} VPy(t).dt$, où VPy(t) est une fonction analogue à VPx(t) définie pour la vitesse Vy(t).

Soit la fonction VNx(t) égale à la vitesse Vx(t) lorsque Vx(t) est négative et nulle lorsque Vx(t) est positive, le paramètre c22 est défini par l'expression :

$c22 = \int_{DT} VNx(t).dt.$

Le paramètre c23 est défini par l'égalité :

$c23 = \int_{DT} VNy(t).dt$, où VNy(t) est une fonction analogue à VNx(t) définie pour la vitesse Vy(t).

Les paramètres c24, c25, c26 et c27 représentent les durées pendant lesquelles respectivement les fonctions VPx(t), VPy(t), VNx(t) et VNy(t) sont non nulles.

Dans l'exemple considéré, les vitesses Vx(t) et Vy(t) passent respectivement 23 et 22 fois par zéro, d'où le paramètre c28=23 et c29=22.

En référence à nouveau à la Fig. 2, le module 4C calcule les paramètres $c1_{ij}$ à $c34_{ij}$ correspondant à chaque signature échantillon S_{ij} et organise lesdits paramètres en I=100 fichiers de paramètres primaires FP_1 à FP_I. Les fichiers FP_i sont sauvegardés en mémoire et sont représentés à la Fig. 2 par le module 4D. Un fichier FP_i est identifié par une adresse correspondante AD_i et contient des paramètres $c1_{i1}$ à $c34_{i1}$, $c1_{i2}$ à $c34_{i2}$, ... $c1_{iJ}$ à $c34_{iJ}$ correspondant aux J=10 échantillons S_{i1} à S_{iJ} d'une même signature S_i. L'adresse AD_i est transmise du module 4C au moyen du clavier 27.

Le traitement réalisé par le module 4C afin de déterminer les paramètres optimaux pour chaque signature S_i est maintenant décrit.

Pour chaque signature S_i, il est considéré deux classes de signatures, une classe de signatures authentiques SA et une classe de signatures fausses ou imitées SF. La classe de signatures authentiques SA correspondant à la signature S_i est constituée par les J=10 échantillons de la signature S_i délivrés par le signataire. La classe de signatures fausses pour la signature S_i est constituée par exemple de 50 signatures échantillons de 50 personnes différentes choisies aléatoirement parmi les signatures échantillons correspondant aux signatures $S \neq S_i$. Selon une variante autorisant de meilleurs résultats dans la vérification des signatures, la classe des signatures fausses pour la signature S_i est constituée par exemple de 10 signatures échantillons imitées qui sont fournies par 10 personnes différentes imitant au mieux la signature S_i.

Pour chaque signature S_i, à partir de l'ensemble des paramètres correspondants c_{i1} à $c34_{i1}$, $c1_{i2}$ à $c34_{i2}$, ... $c1_{iJ}$ à $c34_{iJ}$, il est calculé une représentation statistique sous la forme de 30 paramètres moyens $\overline{c1}_i$ à $\overline{c34}_i$.

Pour décider si une signature S_k est vraie ou fausse, c'est-à-dire est conforme ou non conforme à la signature S_i, il est calculé une distance $D(\overline{S}_i, S_k)$ entre un premier ensemble de paramètres moyens $\overline{d1}_i$ à $\overline{dQ}_i$, où Q est un indice entier au maximum égal à 34, pris parmi les paramètres $\overline{c1}_i$ à $\overline{c34}_i$ et un second ensemble de paramètres $d1_k$ à dQ_k représentatif de la signature à vérifier S_k et pris parmi les paramètres $c1_k$ à $c34_k$ correspondant à la signature S_k. La distance D est définie de la manière suivante :

$$D(\overline{S}_i, S_k) = (1/Q) \cdot \sum_{q=1}^{q=Q} [(dq_k - \overline{dq}_i)/\overline{dq}_i]$$

où $[(dq_k - \overline{dq}_i)/\overline{dq}_i]$ est la valeur absolue de l'expression $(dq_k - \overline{dq}_i)/\overline{dq}_i$.

Le traitement d'optimisation des paramètres pour la signature S_i consiste à sélectionner les Q paramètres $d1_i$ à dQ_i qu'il convient de choisir parmi les 34 paramètres disponibles $c1_i$ à $c34_i$. L'algorithme d'optimisation est décrit ci-après en référence à la

Fig. 11 et est de type "Jacknife" ou "Leave-one-out". Le critère de sélection utilisé est la maximalisation d'un écart de seuil ES :

$ES = S_f - S_v$.

Le seuil S_v est le seuil de décision tel que si la distance D est supérieure au seuil S_v alors toutes les signatures vraies sont acceptées.

Le seuil S_f est le seuil de décision tel que si la distance D est inférieure au seuil S_f alors toutes les signatures fausses sont rejetées.

En référence à la Fig. 9, dans le cas où les paramètres ne sont pas sélectionnés, le seuil S_v est de manière générale supérieur au seuil S_f, l'écart de seuil ES est négatif et il en résulte un taux minimal d'erreur de décision ED qui est non nul, le taux ED étant égal au taux moyen entre un taux de vraies signatures rejetées EDV et un taux de fausses signatures acceptées EDF.

En référence à la Fig. 10, dans le cas où les paramètres sont sélectionnés, le seuil S_v est inférieur au seuil S_f, l'écart de seuil ES est positif et il en résulte un taux minimal d'erreur de décision ED qui est théoriquement nul.

En référence à la Fig. 11, l'algorithme de sélection des paramètres optimaux $d1_i$ à dQ_i correspondant à la signature S_i est décomposable en 8 blocs de traitement notés BL1 à BL8.

Dans le bloc BL1, une initialisation est effectuée. Le nombre de paramètres Q est affecté de la valeur 34 et l'ensemble des paramètres $d1_i$ à dQ_i est pris égal à l'ensemble des paramètres possibles c1 à c34.

Dans le bloc BL2, il est considéré les Q combinaisons différentes C_1, C_2,... C_q, ...C_Q de Q-1 paramètres chacune pris dans l'ensemble de paramètres $d1_i$ à dQ_i. Chacune des combinaisons C_1 à C_Q est composée de l'ensemble des paramètres $d1_i$ à dQ_i excepté de l'un d'entre eux :

$C_1 = (d2_i, d3_i, \ldots d(q-1)_i, dq_i, d(q+1)_i, \ldots dQ_i)$,

$C_2 = (d1_i, d3_i, \ldots d(q-1)_i, dq_i, d(q+1)_i, \ldots dQ_i)$,

$C_q = (d1_i, d2_i, \ldots d(q-1)_i, d(q+1)_i, \ldots dQ_i)$,

$C_{Q-1} = (d1_i, d2_i, \ldots d(q-1)_i, dq_i, d(q+1)_i, \ldots d(Q-2)_i, dQ_i)$,

et

$C_Q = (d1_i, d2_i, \ldots d(q-1)_i, dq_i, d(q+1)_i, \ldots d(Q-2)_i, d(Q-1)_i)$.

Pour chaque combinaison de paramètres C_q, il est calculé les distances $D(\bar{S}_i, S_k)$ afin de déterminer des seuils de distance $(S_f)_q$ et $(S_v)_q$ et des écarts de seuil correspondants ES_q.

Dans le bloc BL3, un écart de seuil maximum ES^* parmi tous les écarts de seuil calculés ES_1 à ES_Q est détecté et la combinaison de paramètres correspondante C^* est retenue.

Dans le bloc BL3, l'écart de seuil maximum ES^* et la combinaison de paramètres correspondante C^* sont mémorisées dans une table TB.

Dans le bloc BL4, la valeur du nombre Q est décrémentée de 1.

Dans le bloc BL5, une comparaison est effectuée sur la valeur du nombre Q.

Dans le cas où la valeur du nombre Q est différente de zéro, dans le bloc BL6, l'ensemble de paramètres dl_i à dQ_i est identifié à la dernière combinaison retenue C^* (BL6) et un nouveau passage de boucle est effectué à partir du bloc BL2.

Dans le cas où la valeur du nombre Q est égale à zéro, 34 passages ont été effectués à travers les blocs BL2 à BL4 et la table TB contient 34 écarts de seuil maximum et 34 combinaisons correspondantes C^*_1 à C^*_{34}. Consécutivement le bloc BL7 est activé et une combinaison C^{**} correspondant à une valeur maximum ES^{**} est détectée dans la table TB. La sélection est alors terminée et les paramètres optimaux dl_i à dQ_i pour la vérification de la signature S_i sont contenus dans la combinaison C^{**}.

En référence à la Fig. 2, le module 4E renferme I=100 fichiers de paramètres de référence optimaux FR_1 à FR_I correspondant respectivement aux I=100 signatures S_1 à S_I. Un fichier FR_i contient les Q paramètres optimaux moyens $\bar{dl}_i$ à $\bar{dQ}_i$ correspondant à la signature S_i.

En phase opérationnelle d'authentification, l'interrupteur 4B est en position PO et les signaux x(t), y(t) et AS correspondant à une signature S_k sont transmis vers un module de calcul de paramètres 4F.

Une adresse AD_i est fournie au module 4E au moyen du clavier 27 et sélectionne dans ce module le fichier de paramètres de référence FR_i correspondant. Le module 4F reçoit des informations IP transmises par le module 4E et lui indiquant les paramètres dl_k

à dQ_k qu'il convient de calculer. Les paramètres calculés dl_k à dQ_k et les paramètres $\overline{dl}_i$ à $\overline{dQ}_i$ contenus dans le fichier FR_i sont ensuite transmis respectivement par les modules 4F et 4E et sont fournis à un module de calcul de distance et décision 4G.

Le module 4G calcule la distance $D(\overline{S}_i, S_k)$ à partir des paramètres $\overline{bl}_i$ à $\overline{bQ}_i$ et bl_k à bQ_k. La distance calculée D est comparée à un seuil de décision SD_i spécifique à la signature S_i et qui a été préalablement déterminé de telle sorte que toutes les signatures vraies soient acceptées. Le seuil DS_i est mémorisé avec le fichier FR_i et est fourni au module 4G par le module 4E. Dans le cas où la distance D est inférieure au seuil SD_i, la signature S_k est considérée conforme à la signature S_i et est acceptée. Dans le cas où la distance D est supérieure au seuil SD_i, la signature S_k est considérée différente de la signature S_i et est refusée.

En référence aux Figs. 1 et 12, la seconde réalisation préférée du système selon l'invention est équipée du lecteur de carte à puce 3 et est conçue pour fonctionner avec des cartes à puce 30.

Les cartes à puce sont attribuées nominativement aux signataires. Dans chacune des cartes à puce 30 sont mémorisés le fichier de paramètres de référence optimaux FR_i et le seuil de décision SD_i correspondant au signataire. Le fichier FR_i et le seuil SD_i sont chargés dans la carte 30 pendant la phase d'apprentissage. Pendant la phase opérationnelle d'authentification, le signataire introduit sa carte 30 dans le lecteur 3 avant de signer sur la tablette à numériser 1, afin d'avoir accès au système. Le lecteur 3 lit la carte 30 et délivre consécutivement l'information IP, les paramètres de référence $\overline{dl}_i$ à $\overline{dQ}_i$ et le seuil de décision SD_i correspondants. De même que pour la première réalisation préférée du système, l'information IP est transmise au module 4F et les paramètres $\overline{dl}_i$ à $\overline{dQ}_i$ et le seuil SD_i sont transmis au module 4G. Une signature S_k est ensuite apposée sur la tablette 1 par le détenteur de la carte 30. Le module 4F à partir des signaux x(t), y(t) et AS calcule les paramètres dl_k à dQ_k indiqués par l'information IP. Le module 4G calcule ensuite la distance D entre les paramètres dl_k à dQ_k et $\overline{dl}_i$ à $\overline{dQ}_i$, compare la

distance D au seuil SD_i et accepte ou refuse la signature S_k comme conforme à la signature de référence S_i.

Selon une variante correspondant à cette seconde réalisation préférée du système selon l'invention, le module de programme de calcul de distance et décision 4G est implanté également dans la carte à puce 30 et les calculs correspondants sont effectués par un microprocesseur inclus dans la carte. Cette variante apporte une plus grande sécurité du fait que les paramètres de référence restent protégés dans la carte et ne sont pas accessibles de l'extérieur. De plus, il est impossible de forcer le système à travers le clavier du micro-ordinateur afin par exemple de permettre un autre essai de signature, puisque le traitement est effectué dans la carte à puce et n'est pas sous le contrôle du micro-ordinateur.

REVENDICATIONS

1 - Procédé de vérification de signatures pour vérifier la conformité de signatures échantillons (S_k) avec des signatures de référence (S_i) selon lequel les signatures sont représentées par des fichiers (FR_i) comprenant les valeurs de plusieurs paramètres notamment de type dynamique (d1 à dQ), caractérisé en ce que les fichiers (FR_i) sont composés d'un nombre variable (Q) de paramètres sélectionnés spécifiquement parmi un ensemble prédéterminé de paramètres (c1 à c30) par un algorithme d'optimisation de manière à minimiser des erreurs de décision.

2 - Procédé conforme à la revendication 1, caractérisé en ce qu'il inclut un algorithme d'optimisation de type "Jacknife" ou "Leave-one-out" afin de produire les fichiers de référence.

3 - Procédé conforme à la revendication 1 ou 2, caractérisé en ce que pour vérifier la conformité d'une signature échantillon (S_k) avec une signature de référence (S_i) il est calculé une distance D entre les paramètres (dq_k et dq_i) des fichiers correspondants, ladite distance D étant définie par la relation suivante :

$$D = (1/Q) \cdot \sum_{q=1}^{q=Q} [(dq_k - \overline{dq}_i)/\overline{dq}_i],$$

dans laquelle dq_k correspond à des valeurs des paramètres représentatifs de la signature échantillon indicée k, $\overline{dq}_i$ correspond à des valeurs moyennes des paramètres représentatifs de la signature de référence indicée i, $[dq_k - \overline{dq}_i)/\overline{dq}_i]$ est la valeur absolue de l'expression $(dq_k - \overline{dq}_i)/\overline{dq}_i$, et Q est le nombre de paramètres compris dans les fichiers.

4 - Système de vérification de signatures pour la mise en oeuvre du procédé conforme à l'une quelconque des revendications 1 à 3, caractérisé en ce qu'il comprend des moyens (1, 10, 4A) pour produire des signaux numériques (x(t), y(t), AS) représentatifs des signatures échantillons à traiter, des moyens (27, 30 et 3) pour indiquer au système l'identité supposée (AD_i) de chaque signataire, des moyens (4C, 4D) activés lors d'une phase d'apprentissage pour déterminer les fichiers de référence (FR_i) par sélection des paramètres optimaux (d1 à dQ) et calcul de leurs valeurs moyennes ($\overline{d1}$ à $\overline{dQ}$) à partir de plusieurs échantillons de signatures de

référence (S_{i1} à S_{iJ}), des moyens (4E, 32) pour mémoriser les fichiers de référence, des premiers moyens (4F) activés pendant une phase opérationnelle pour calculer des fichiers de paramètres correspondant aux signatures échantillons, des seconds moyens (4G) pour calculer des distances (D) entre les valeurs des paramètres (dq_k et $\overline{dq}_i$) des fichiers, et des moyens (4G) pour décider de la conformité des signatures échantillons (S_k) avec les signatures de référence (S_i) en fonction desdites distances (D).

5 - Système de vérification de signatures conforme à la revendication 4, caractérisé en ce que

les moyens pour déterminer les fichiers de référence (4C, 4D), les moyens pour mémoriser (4E), les premiers et seconds moyens pour calculer (4F, 4G) et les moyens pour décider (4G) sont réalisés par des modules de programme implantés dans un micro-ordinateur (2) compris dans le système.

6 - Système de vérification de signatures conforme à la revendication 4, caractérisé en ce qu'il comprend également un lecteur de carte à puce (3) pour recevoir des cartes à puce (30) attribuées nominativement aux signataires, et en ce que les moyens pour mémoriser (4E) sont répartis dans les cartes à puce (30) et correspondent à des mémoires comprises dans les cartes dans lesquelles sont chargés respectivement les fichiers de référence correspondants pendant la phase d'apprentissage.

7 - Système de vérification de signatures conforme à la revendication 6, caractérisé en ce que chacune des cartes à puce (30) comprend également les moyens pour décider (4G) sous la forme d'un module de programme implanté dans la carte (30).

8 - Système de vérification de signatures conforme à l'une quelconque des revendications 4 à 7, caractérisé en ce que les moyens pour produire les signaux numériques représentatifs comprennent une tablette à numériser (1) et un stylo (10) pour apposer des signatures sur la tablette (1), la tablette (1) et le stylo (10) étant tous deux de type classique.

FIG.1

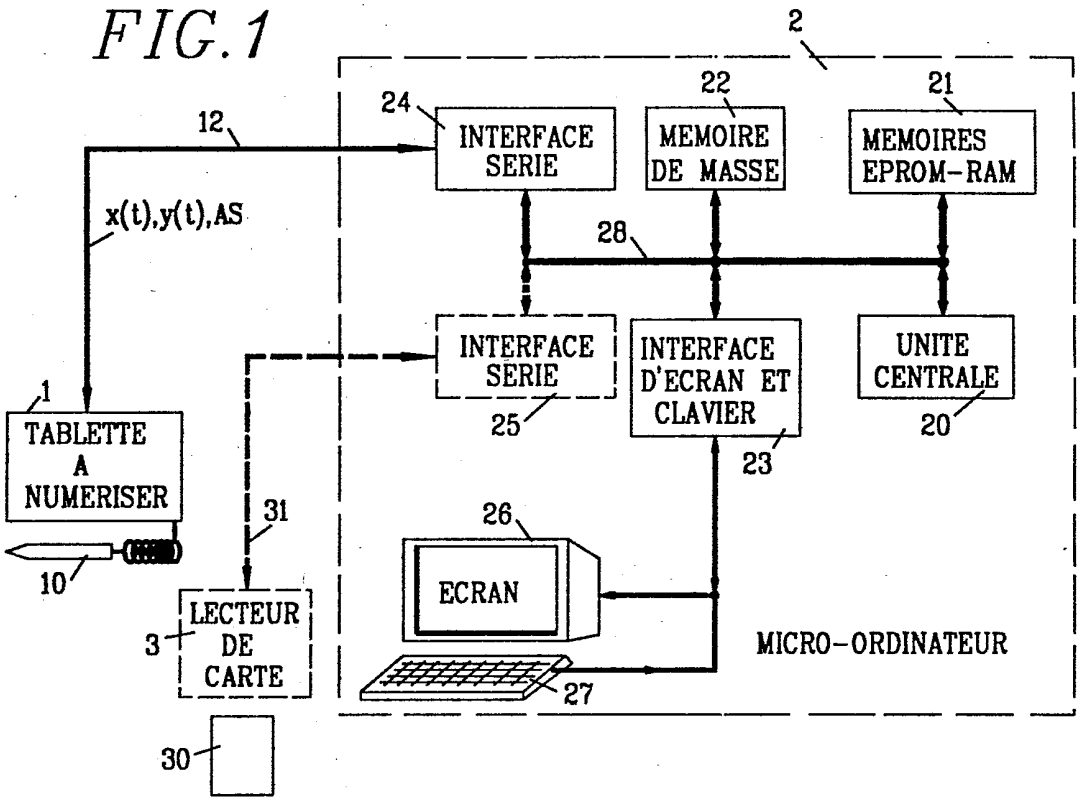

2
24
INTERFACE SERIE
22
MEMOIRE DE MASSE
21
MEMOIRES EPROM-RAM
12
x(t),y(t),AS
28
INTERFACE SERIE
25
INTERFACE D'ECRAN ET CLAVIER
23
UNITE CENTRALE
20
1
TABLETTE A NUMERISER
10
31
26
ECRAN
LECTEUR DE CARTE
3
MICRO-ORDINATEUR
27
30

FIG.2

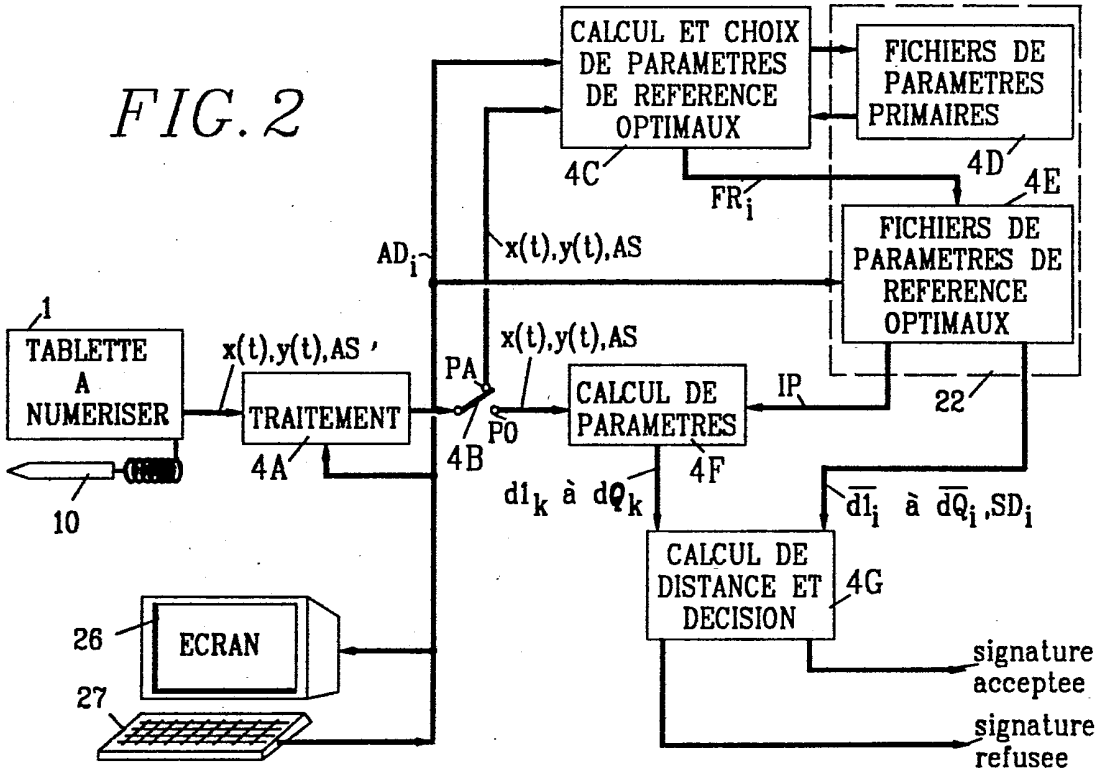

CALCUL ET CHOIX DE PARAMETRES DE REFERENCE OPTIMAUX
FICHIERS DE PARAMETRES PRIMAIRES
4C
4D
4E
FR_i
AD_i
x(t),y(t),AS
FICHIERS DE PARAMETRES DE REFERENCE OPTIMAUX
1
TABLETTE A NUMERISER
x(t),y(t),AS
TRAITEMENT
PA
P0
4A
4B
CALCUL DE PARAMETRES
IP
22
4F
10
dl_k à dQ_k
dl_i à dQ_i,SD_i
CALCUL DE DISTANCE ET DECISION
4G
26
ECRAN
27
signature acceptee
signature refusee

FIG. 3

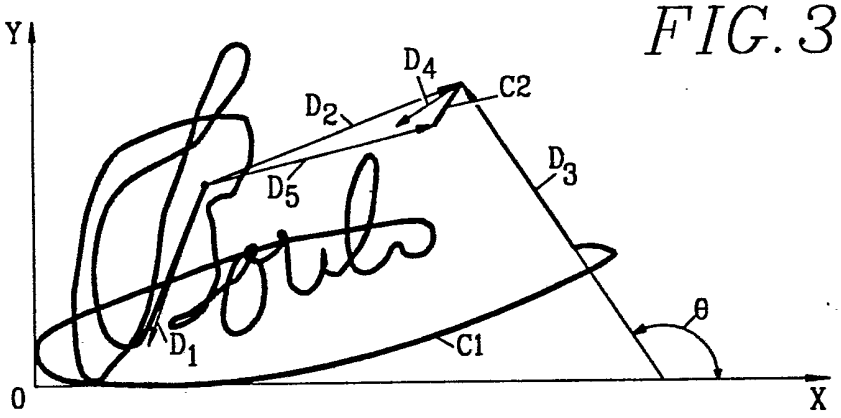


FIG. 4

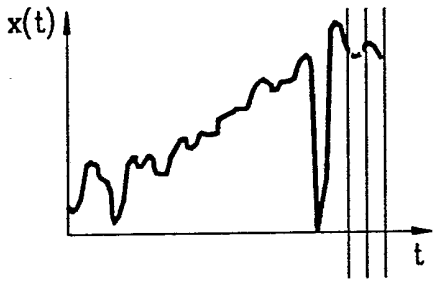


FIG. 7

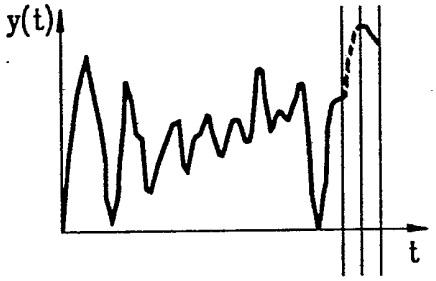


FIG. 5

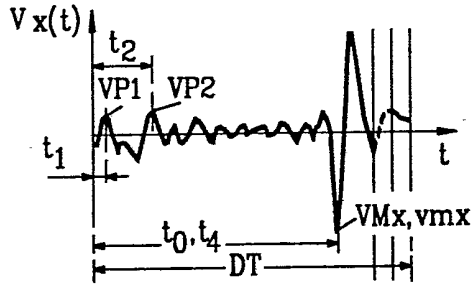


FIG. 8

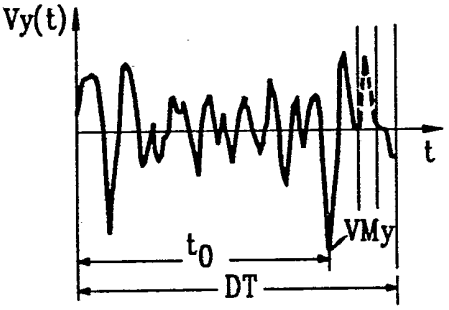


FIG. 6

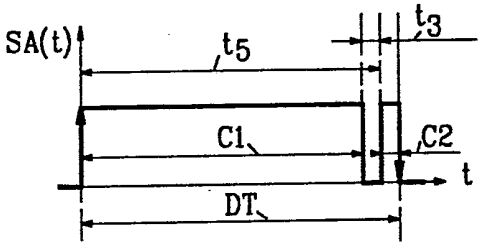


FIG.9

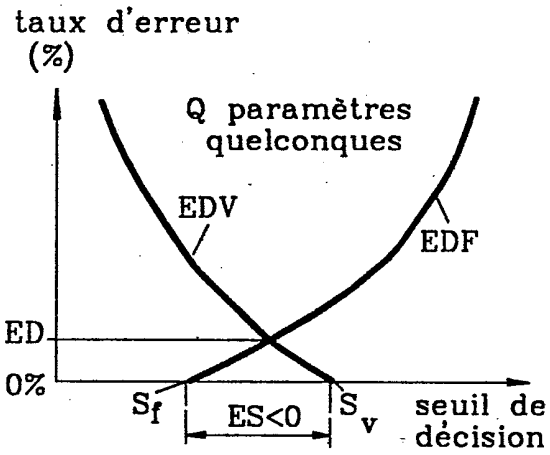


FIG.10

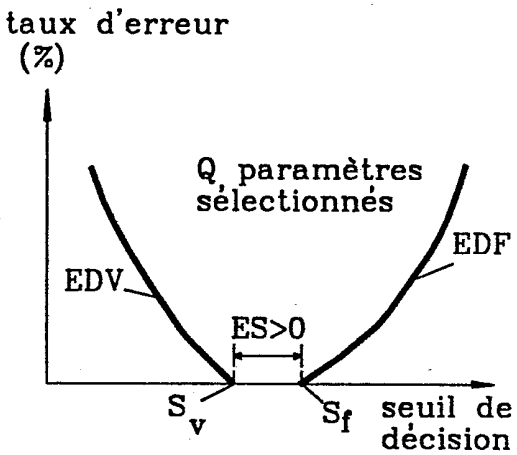


FIG.12

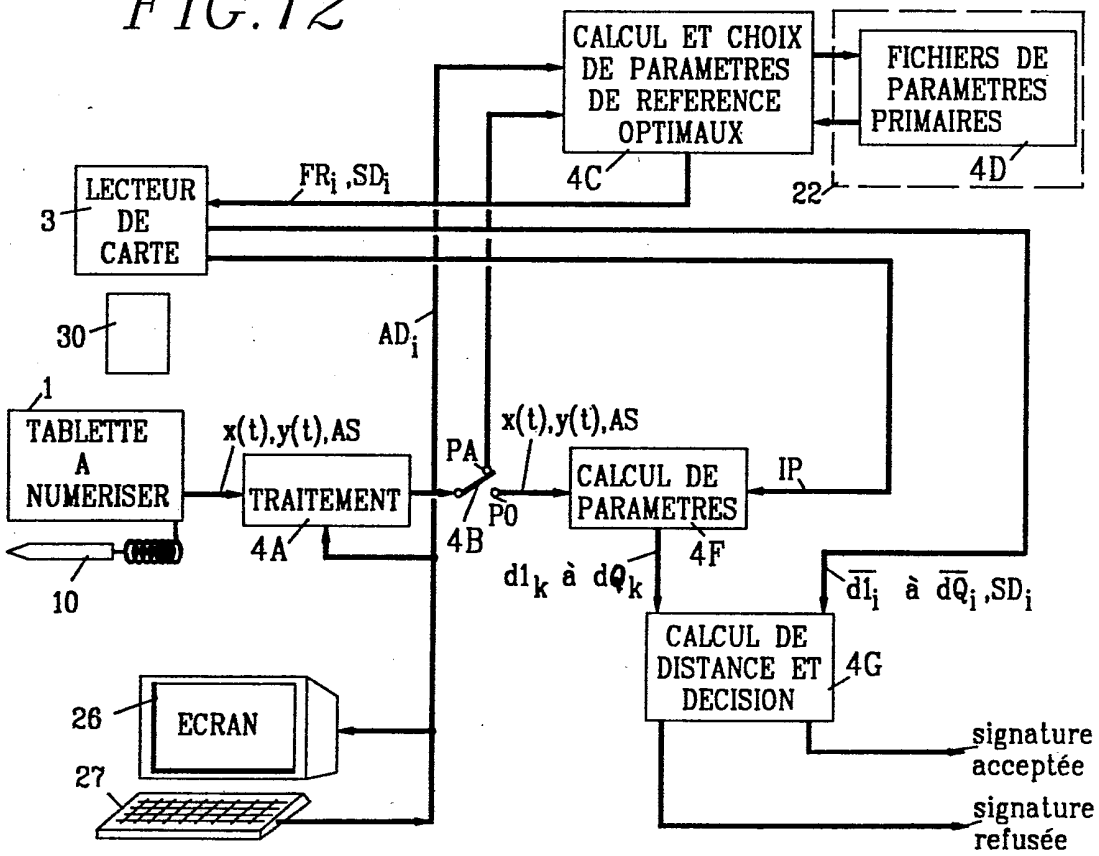
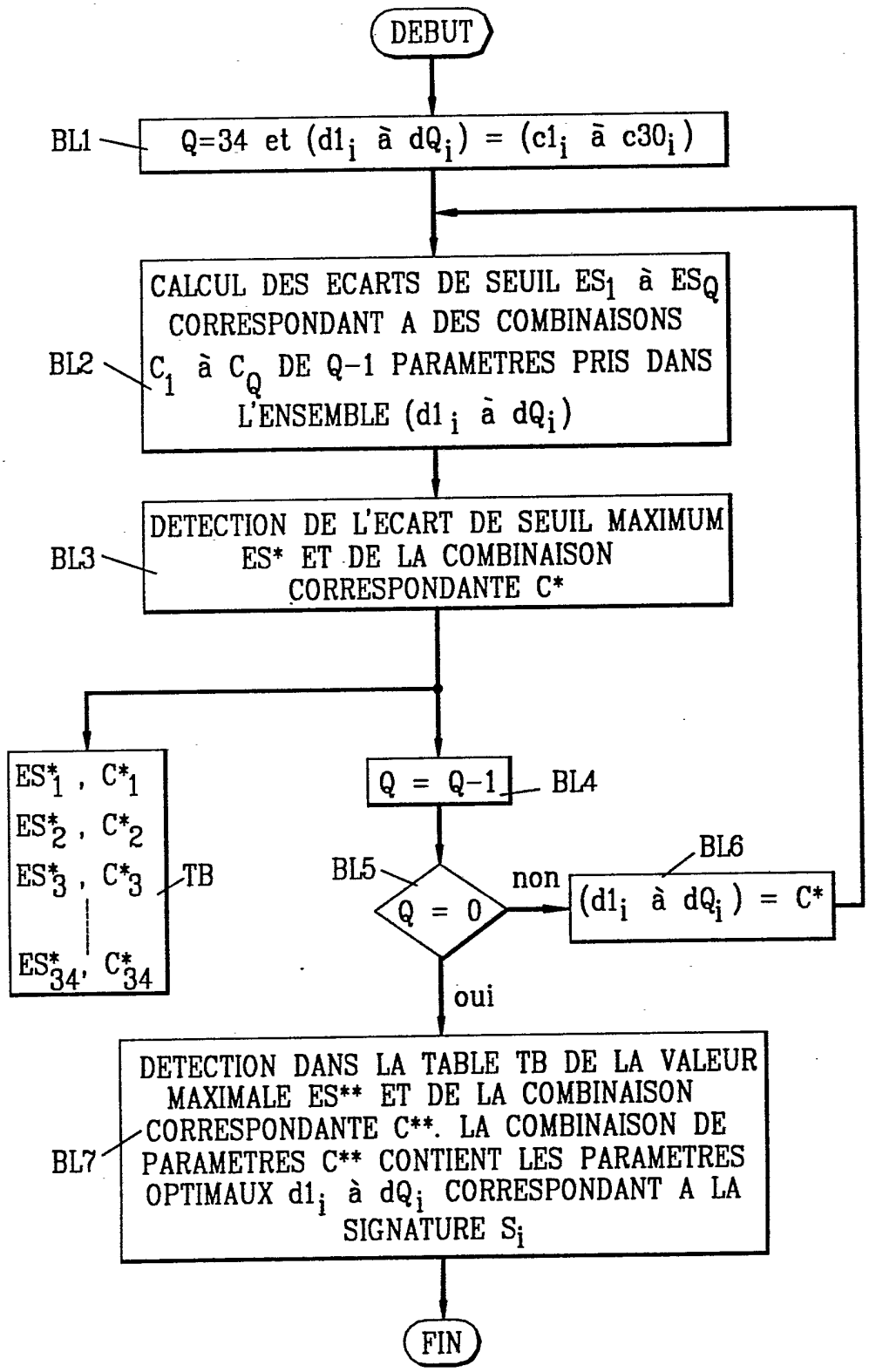


FIG.11


DEBUT
BL1
Q=34 et (d1i à dQi) = (c1i à c30i)
CALCUL DES ECARTS DE SEUIL ES1 à ESQ CORRESPONDANT A DES COMBINAISONS C1 à CQ DE Q-1 PARAMETRES PRIS DANS L'ENSEMBLE (d1i à dQi)
BL2
DETECTION DE L'ECART DE SEUIL MAXIMUM ES* ET DE LA COMBINAISON CORRESPONDANTE C*
BL3
ES*1 , C*1
ES*2 , C*2
ES*3 , C*3
ES*34, C*34
TB
Q = Q-1
BL4
BL5
Q = 0
non
BL6
(d1i à dQi) = C*
oui
DETECTION DANS LA TABLE TB DE LA VALEUR MAXIMALE ES** ET DE LA COMBINAISON CORRESPONDANTE C**. LA COMBINAISON DE PARAMETRES C** CONTIENT LES PARAMETRES OPTIMAUX d1i à dQi CORRESPONDANT A LA SIGNATURE Si
BL7
FIN