

CONFÉDÉRATION SUISSE
INSTITUT FÉDÉRAL DE LA PROPRIÉTÉ INTELLECTUELLE

(11) **CH** **716 900 A2**

(51) Int. Cl.: **G06F** 21/32 (2013.01)
G06K 9/00 (2006.01)
G04G 21/02 (2010.01)

Demande de brevet pour la Suisse et le Liechtenstein

Traité sur les brevets, du 22 décembre 1978, entre la Suisse et le Liechtenstein

(12) **DEMANDE DE BREVET**

(21) Numéro de la demande: 01558/19

(71) Requéant:
Tissot SA, Chemin des Tourelles 17
2400 Le Locle (CH)

(22) Date de dépôt: 06.12.2019

(72) Inventeur(s):
Edoardo Franzi, 1400 Cheseaux-Noréaz (CH)
Mattia Bertschi, 1093 La Conversion (CH)

(43) Demande publiée: 15.06.2021

(74) Mandataire:
ICB Ingénieurs Conseils en Brevets SA,
Faubourg de l'Hôpital 3
2001 Neuchâtel (CH)

(54) **Procédé de sécurisation d'accès à l'utilisation de fonctions d'une montre.**

(57) L'invention concerne un procédé de sécurisation d'accès à l'utilisation de fonctions d'une montre comportant les étapes suivantes :

- authentification du porteur de la montre en vue d'autoriser un accès audites fonctions, et
- contrôle discret à période déterminée de l'identité du porteur de la montre par une vérification de la validité d'un élément d'identification numérique déterminé à partir d'au moins un élément d'information biométrique compris dans une portion de peau d'un porteur de ladite montre en vue de conserver/supprimer l'autorisation d'accès audites fonctions.

Description

Domaine technique

[0001] La présente invention concerne un procédé de sécurisation d'accès à l'utilisation de fonctions d'une montre et un système mettant en oeuvre un tel procédé.

[0002] L'invention concerne également une montre comprenant un tel système ainsi qu'un programme d'ordinateur.

Art antérieur

[0003] Une montre comprend un ensemble de fonctions qui peut être utilisé par le porteur. De telles fonctions peuvent concerner en plus du réglage de l'heure ou de la date, une utilisation de données confidentielles ou privées propres au porteur et utiles pour accéder à des services personnalisés. Ces données sont par exemple des clés, certificats, codes d'authentification, mots de passe et codes personnels qui permettent de réaliser une connexion sécurisée de la montre à un réseau privé d'une entreprise, une authentification auprès de serveurs sécurisés comme un serveur bancaire, ou une messagerie sécurisée pour l'envoi et la réception de courriels signés et/ou chiffrés. Dès lors, on comprend alors qu'il est important de pouvoir sécuriser l'accès à l'utilisation des fonctions d'une telle montre.

[0004] Pour ce faire, on connaît dans l'état de la technique des procédés prévoyant de sécuriser l'accès à l'utilisation des fonctions d'une montre en renforçant les critères d'authentification autorisant cet accès par exemple en mettant en oeuvre des étapes supplémentaires d'authentification relatives à de la biométrie.

[0005] Toutefois un des inconvénients majeurs de tels procédés est lié au fait qu'une fois que le porteur de la montre est authentifié il est alors possible à n'importe quel individu d'avoir accès aux fonctions de la montre notamment dans le cas où cette dernière a été volée.

[0006] On comprend qu'il existe un besoin de trouver une solution alternative, notamment qui ne présente pas les inconvénients de l'art antérieur.

Résumé de l'invention

[0007] Un but de la présente invention est par conséquent de proposer un procédé de sécurisation d'accès à l'utilisation de fonctions d'une montre qui soit fiable et robuste.

[0008] Un tel procédé a pour avantage de s'assurer de l'identité du porteur de la montre de manière automatique, transparente et non intrusive pour le porteur.

[0009] Dans ce dessein, l'invention concerne un procédé de sécurisation d'accès à l'utilisation de fonctions d'une montre comportant les étapes suivantes :

- authentification du porteur de la montre en vue d'autoriser un accès audites fonctions, et
- contrôle discret à période déterminée de l'identité du porteur de la montre par une vérification de la validité d'un élément d'identification numérique déterminé à partir d'au moins un élément d'information biométrique compris dans une portion de peau d'un porteur de ladite montre en vue de conserver/supprimer l'autorisation d'accès audites fonctions.

[0010] Dans d'autres modes de réalisation :

- l'étape de contrôle comprend une sous-étape d'acquisition par au moins un capteur biométrique multispectral de peau compris dans la montre, d'une pluralité d'images d'une portion de peau du porteur adjacente audit capteur, lesdites images comprenant ledit au moins un élément d'information biométrique compris dans cette portion de peau ;
- l'étape de contrôle comprend une sous-étape de génération d'un élément d'identification numérique à partir dudit au moins un élément d'information biométrique ;
- l'étape de contrôle comprend une sous-étape de validation d'un élément d'identification numérique généré en prévision du contrôle de l'identité du porteur ;
- la sous-étape de validation comprend une phase de comparaison comportant une sous-phase de conservation de l'autorisation d'accès audites fonctions de la montre si l'élément d'identification numérique généré est sensiblement similaire ou similaire à un élément d'identification numérique de référence ;
- la sous-étape d'acquisition comprend une phase d'éclairage de la portion de peau selon différentes longueurs d'onde ;
- la sous-étape d'acquisition comprend une phase de capture d'images de la portion de peau éclairée à différentes longueurs d'onde ;
- la sous-étape de génération comprend une phase de caractérisation dudit au moins un élément d'information biométrique compris dans les images acquises relatives à ladite portion de peau ;
- la sous-étape de génération comprend une phase de conception de l'élément d'identification numérique à partir de la caractérisation dudit élément d'information biométrique ;
- l'élément d'information biométrique est relatif à un réseau vasculaire ou à une texture de cette peau.

[0011] L'invention concerne également un système de sécurisation d'accès à l'utilisation de fonctions d'une montre mettant en oeuvre un tel procédé, le système comprenant les éléments suivants reliés entre eux : une unité de traitement, un capteur biométrique multispectral de peau, une interface de saisie et une interface de diffusion d'une information visuelle.

[0012] L'invention concerne également une montre, notamment une montre mécanique connectée, comportant un tel système.

[0013] L'invention concerne aussi un programme d'ordinateur comprenant des instructions de code de programme pour l'exécution des étapes de ce procédé lorsque ledit programme est exécuté par une unité de traitement (2).

Brève description des figures

[0014] D'autres particularités et avantages ressortiront clairement de la description qui en est faite ci-après, à titre indicatif et nullement limitatif, en référence aux figures annexées, dans lesquelles :

- la figure 1 est une représentation schématique d'une montre comprenant un système de sécurisation d'accès à l'utilisation de fonctions d'une montre, selon un mode de réalisation de l'invention, et
- la figure 2 est un logigramme relatif à un procédé de sécurisation d'accès à l'utilisation de ces fonctions, selon le mode de réalisation de l'invention.

Description détaillée de l'invention

[0015] Sur la figure 1 est représenté une montre 100 comprenant un système de sécurisation d'accès à l'utilisation de fonctions de cette montre 100. Un tel système 1 est compris dans la montre 100 qui est de préférence une montre 100 mécanique connecté à affichage hybride. Dans ce contexte, ce dispositif électronique 100 comprend un corps tel que la boîte de montre, et un élément d'attache tel qu'un bracelet permettant de fixer ce corps par exemple au poignet du porteur. Ce système 1 comprend plus précisément de manière non limitative et/ou non exhaustive :

- une unité de traitement 2 comportant des ressources matérielles et logicielles en particulier au moins un processeur coopérant avec des éléments de mémoire 6;
- une interface de diffusion d'une information visuelle 3 telle qu'un cadran d'affichage hybride pourvu d'une première composante d'affichage analogique et d'une deuxième composante d'affichage numérique et/ou alphanumérique ;
- une interface de diffusion d'une information sonore 4 telle qu'un haut-parleur ;
- une interface de communication sans fil 5 (par exemple cellulaire, WLAN Bluetooth, etc.) ;
- une interface de saisie 25 tel qu'un clavier ou encore une interface tactile comprise par exemple dans l'interface de diffusion d'une information visuelle 3, et
- un capteur biométrique multispectral de peau 24 comprenant au moins un capteur photographique 26, au moins une source d'éclairage multispectral 27 et au moins un capteur d'image thermique 28, la source d'éclairage 27 pouvant émettre un rayonnement lumineux dans des longueurs d'ondes comprises entre 300 et 1100 nm, de plus cette source d'éclairage 27 peut être du type laser.

[0016] Dans ce système 1, l'unité de traitement 2 est reliée entre autres aux interfaces de diffusion d'une information visuelle et sonore 3, 4, à l'interface de saisie 25 ainsi qu'à l'interface de communication sans fil 5 et au capteur biométrique multispectral 24. On notera en complément que le capteur biométrique multispectral 24 est agencé dans le corps du dispositif électronique 100 et/ou dans l'élément d'attache.

[0017] Ce système 1 implémenté dans le dispositif électronique 100 est apte à assurer le contrôle de l'identité du porteur authentifié de la montre de manière discrète c'est-à-dire sans intervention/interaction directe du porteur avec cette montre 100, afin qu'il puisse utiliser les fonctions de la montre 100 tout le temps qu'il la porte et ce, sans avoir à s'authentifier de nouveau. L'identification du porteur est alors effectuée de manière transparente et discrète et ce, à partir d'au moins un élément d'information biométrique compris dans la peau de ce porteur tel que le réseau vasculaire de la peau ou encore la texture de cette peau. Cette peau du porteur qui recouvre son corps a une particularité, moins évidente à envisager par l'homme de l'art car non visualisable naturellement par l'oeil humain, liée aux caractéristiques d'absorption et de réflexion à différentes longueurs d'onde (spectre) des composantes de la peau, situées à différentes profondeurs. Dans un modèle simplifié, la peau est constituée d'une couche nommée „épiderme“, semi transparente et située en surface puis, sous l'épiderme, d'une couche nommée le „derme“ et comprenant, entre autres, les vaisseaux sanguins (ou réseau vasculaire) dans lesquels l'hémoglobine est fortement réfléchissante aux longueurs d'onde élevées proches du rouge en étant comprises par exemple entre 760 et 930 nm ce qui permet ici de révéler ou mettre en évidence le réseau vasculaire de la peau du porteur. En d'autres termes, le spectre d'absorption lumineux des composantes de l'épiderme et du derme constituant la peau n'étant pas uniforme selon les longueurs d'ondes électromagnétiques, l'apparence et la couleur de la peau résultent d'une combinaison complexe de ces phénomènes. Ainsi, lorsqu'il s'agit de mettre en évidence ou de révéler un élément d'information biométrique comme la texture de la peau de ce porteur, texture essentiellement formée de crevasses ou cavités, l'éclairage de la peau peut être alors assuré par une source d'éclairage restreinte aux longueurs d'onde aux alentours du rouge qui tend à faire disparaître le phénomène d'ombres du fond des crevasses. En effet, il se produit un effet de rétro projection par réflexion sur le derme et à travers l'épiderme de ces longueurs d'onde proches du rouge, alors que l'éclairage de la peau par une source de spectre colorimétrique éloigné du rouge, typiquement la bande de longueurs d'onde située entre le violet (400 nm) et jusqu'au jaune-orangé (600 nm), permet au contraire de mettre fortement en contraste ces crevasses de la peau par l'apparition d'ombres au fond de ces crevasses. On notera que l'identification d'un élément d'information biométrique compris dans la peau peut être améliorée par l'utilisation du capteur d'image thermique 28 de préférence sans éclairage. A titre d'exemple, pour la mise en évidence de la texture de la peau

notamment lorsque la portion de la peau concernée de ce porteur est pourvue de poils, l'utilisation du capteur d'image thermique 28 permet de révéler les crevasses de cette texture de la peau qui sont généralement plus chaudes que la peau environnante et les poils plus froids que cette peau environnante. Ainsi dans cette configuration les poils peuvent être distingués thermiquement des crevasses de la texture de la peau du fait de cette différence entre leur température respective.

[0018] On notera que la capture d'images thermiques peut être réalisée sous un éclairage dans une longueur d'onde donnée selon l'élément d'information biométrique qu'il convient de mettre en évidence ou de révéler.

[0019] On comprend donc, selon le principe de l'invention, que l'identification périodique du porteur est réalisée à partir d'au moins un élément d'information biométrique compris dans des images d'une portion de peau de ce porteur qui peut être éclairée le cas échéant selon différentes longueurs d'onde afin de capturer des images comprenant l'élément d'information biométrique recherché. Ainsi, cet élément d'information biométrique, compris dans ces images, peut être mis en évidence par l'éclairage effectué dans différentes longueurs d'onde ou sans éclairage par exemple lorsqu'il s'agit de réaliser une capture d'images thermiques.

[0020] Dans ce système 1, les éléments de mémoire 6 de l'unité de traitement 2 comprennent des données relatives à un élément d'identification numérique de référence préalablement défini/généré. Ces éléments de mémoire 6 comportent également des algorithmes de traitement numérique 29 d'images permettant de caractériser au moins un élément d'information biométrique relatif à la peau du porteur et qui est compris dans les images relatives à la portion de peau du porteur. Ces éléments de mémoire 6 comportent aussi des algorithmes de génération 30 de l'élément d'identification numérique de référence mais aussi de l'élément d'identification numérique qui est généré périodiquement dans le cadre du contrôle de l'identité du porteur.

[0021] Un tel système 1 de la montre 100 est apte à mettre en oeuvre un procédé de sécurisation d'accès à l'utilisation des fonctions de la montre 100, représenté sur la figure 2. Un tel procédé vise à s'assurer de manière discrète c'est-à-dire de manière non intrusive et automatique de l'identité d'un porteur authentifié afin qu'il puisse utiliser les fonctions de la montre 100 tout le temps qu'il la porte sans avoir à s'authentifier de nouveau. Les fonctions de la montre 100 peuvent concerner le réglage de l'heure, de la date ou encore l'utilisation d'un chronomètre, d'un système de navigation, un podomètre, d'un traceur d'activité, d'une messagerie, un accès à des données confidentielles ou privées propres au porteur et utiles pour accéder à des services personnalisés, etc...

[0022] Ce procédé comprend une étape d'authentification 10 du porteur de la montre 100 en vue d'autoriser un accès audites fonctions de cette montre 100. Cette étape 10 permet au porteur d'apporter la preuve de son identité. En effet, le porteur peut interagir avec l'interface de saisie 25 pour une authentification à partir d'un authentifiant ou d'un code secret.

[0023] Ce procédé comprend ensuite une étape de contrôle 12 discret à période déterminée de l'identité du porteur de la montre par une vérification de la validité d'un élément d'identification numérique déterminé à partir d'au moins un élément d'information biométrique compris dans une portion de peau de ce porteur de ladite montre en vue de conserver/supprimer l'autorisation d'accès audites fonctions. Lors de cette étape 12, la période déterminée est une période de contrôle régulière ou irrégulière qui peut être configurée automatiquement par l'unité de traitement 2 ou définie par le porteur. A titre d'exemple, cette période peut être de quelques secondes ou quelques minutes. Une telle étape de contrôle 12 permet de vérifier à l'issue de chaque période que le porteur de la montre est toujours le même par le contrôle de son identité „biométrique“ à partir d'un élément d'identification numérique établi en fonction d'au moins un élément d'information biométrique compris dans la peau de ce porteur.

[0024] Cette étape de contrôle 12 comprend ensuite une sous-étape d'acquisition 13 par le capteur 24 d'une pluralité d'images d'une portion de peau du porteur, ladite peau étant agencée de manière adjacente audit capteur, lesdites images comprenant ledit au moins un élément d'information biométrique compris dans cette portion de peau. Cette sous-étape 13 comprend une phase d'éclairage 14 de la portion de peau selon différentes longueurs d'onde. Plus précisément, lors de cette phase 14, l'unité de traitement 2 pilote le capteur biométrique multispectral 24 et en particulier la source d'éclairage 27 de manière à ce que cette dernière émette un rayonnement lumineux en direction de la portion de peau selon une longueur d'onde précise adaptée à la mise en évidence ou à révéler ledit au moins un élément d'information biométrique spécifique de la peau, ici recherché dans le cadre du contrôle de l'identité du porteur, et qui est compris dans cette portion de la peau du porteur. Une fois l'éclairage configuré, la sous-étape d'acquisition 13 comprend une phase de capture 15 d'images de cette portion de peau éclairée à au moins une longueur d'onde susceptible de mettre en évidence ou de révéler ledit au moins un élément d'information biométrique. Lors de cette phase 15, l'unité de traitement 2 pilote le capteur biométrique multispectral 24 de peau et en particulier le capteur photographique 26 de manière synchrone avec l'activation/désactivation de la source d'éclairage 27 et ce, afin de réaliser une capture d'au moins une image relative à la portion de peau éclairée pour au moins une longueur d'onde.

[0025] Cette sous-étape d'acquisition 13 peut comprendre aussi une phase de capture 16 d'au moins une image thermique de la portion de peau. Une telle phase 16 est réalisée de préférence sans éclairage mais dans d'autres alternatives un éclairage de la portion peut être effectué dans au moins une longueur d'onde donnée, cela dépendant évidemment de l'élément d'information biométrique qu'il convient de mettre en évidence ou de révéler. Cette phase 16 peut être réalisée avant ou après les phases d'éclairage 14 et de capture 15 d'images.

[0026] L'étape de contrôle 12 comprend ensuite une sous-étape de génération 17 de l'élément d'identification numérique à partir dudit au moins un élément d'information biométrique compris dans les images acquises de la portion de peau. Une telle sous-étape 17 comprend une phase de caractérisation 18 dudit élément d'information biométrique compris dans les images relatives à ladite portion de peau. Lors de cette phase 124, l'unité de traitement 2 met en oeuvre des algorithmes de traitement 29 des images acquises visant à identifier/détecter dans chacune d'entre elles ledit au moins un élément d'information biométrique qu'elles comprennent. Ainsi que nous l'avons déjà évoqué précédemment, il peut s'agir d'éléments d'information relatifs par exemple à la texture de la peau ou au réseau vasculaire compris dans cette portion de peau du porteur. La mise en oeuvre de ces algorithmes 29, 30 par l'unité de traitement 2 peut à titre d'exemple prévoir un processus de découpe en segments de ces images. On comprend ici que chaque image acquise donne une vue globale de la portion de la peau du porteur, et comporte alors des zones de pertinence variables pour l'identification dudit au moins un élément d'information biométrique. Un tel processus de découpe participe à extraire les segments à traiter et à éliminer les parties à ne pas traiter dans ces images. Ces algorithmes 29 peuvent ensuite prévoir un indexage de ces segments d'image comprenant des caractéristiques relatives audit au moins un élément d'information biométrique particulier à identifier, par zones de localisation dans la portion de peau et ce, afin de pouvoir affecter à chaque zone le traitement adéquat vis-à-vis de la typologie morphologique de la caractéristique de cette zone géographique de la portion. Dans ce contexte, ces algorithmes 29 traitent chaque segment de ces images en mettant en évidence les informations portées par les pixels de chacune de ces images par la réalisation d'opérations d'analyse d'image de type traitements, transformations et détections. Par la suite, ces algorithmes 29 effectuent des opérations de filtrage et d'extraction de caractéristiques ou de vectorisation, afin de convertir les données images relatives audit au moins un élément d'information biométrique identifié et extrait, en des données paramétriques, typiquement des valeurs numériques relatives exprimées par exemple en indice ou en pourcentage.

[0027] On comprend ici que l'acquisition de plusieurs images représentant la même portion de peau, participe à améliorer la précision et l'efficacité de cette phase de caractérisation 18.

[0028] Par la suite, la sous-étape de génération 16 comprend une phase de conception 19 de l'élément d'identification numérique à partir de la caractérisation dudit au moins un élément d'information biométrique. Lors de cette phase 19, l'unité de traitement 2 met en oeuvre des algorithmes de génération 30 d'un tel élément d'identification numérique spécifiquement prévus pour le traitement des données paramétriques obtenues lors de la phase de caractérisation 18, lesquelles données paramétriques étant relatives à l'élément d'information biométrique.

[0029] Ensuite, l'étape de contrôle 12 comprend une sous-étape de validation 20 de l'élément d'identification numérique généré en prévision d'un contrôle de l'identité du porteur. Cette sous-étape de validation 20 comprend une phase de comparaison 21, mise en oeuvre par l'unité de traitement 2, entre l'élément d'identification numérique généré et l'élément d'identification numérique de référence. Dans ce procédé, l'élément d'identification numérique de référence peut être créé, dès lors que le porteur a été dûment authentifié et que son identité est certaine et ce, lors d'une étape de définition 11 de cet élément d'identification numérique de référence prévoyant des sous-étapes similaires aux sous-étapes de d'acquisition 13 et de génération 17 mises en oeuvre durant l'étape de contrôle 12. Dans ce procédé, une fois que le porteur de la montre 100 est authentifié, l'unité de traitement 2 met en oeuvre cette étape de définition 11 et effectue ensuite un archivage de l'élément d'identification numérique de référence obtenu dans les éléments de mémoire 6 de l'unité de traitement 2. Cet élément d'identification numérique de référence peut donc être déterminé automatiquement par l'unité de traitement 2 ou configuré par le porteur durant un processus de réglage visant à guider le porteur dans la définition de cet élément d'identification numérique de référence.

[0030] Cette phase de comparaison 21 comprend une sous-phase de suppression 22 de l'autorisation d'accès audites fonctions de la montre 100 si l'élément d'identification numérique généré est sensiblement différent ou différent de l'élément d'identification numérique de référence. Dans ce cas de figure, l'accès aux fonctions de la montre 100 est alors supprimé car le porteur et propriétaire de la montre 100 peut ne plus être en sa possession. Dès lors dans ce contexte pour utiliser de nouveau les fonctions de la montre 100, il est nécessaire de s'authentifier.

[0031] La phase de comparaison 21 comprend aussi une sous-phase de conservation 23 de l'autorisation d'accès audites fonctions de la montre 100 si l'élément d'identification numérique généré est sensiblement similaire ou similaire à l'élément d'identification numérique de référence. Dans ce cas, l'unité de contrôle 2 exécute de nouveau, selon la période déterminée, les sous-étapes d'acquisition 13 et de génération 17 de l'étape de contrôle 12 afin de réaliser une autre fois la phase de comparaison 21.

[0032] Ainsi, l'invention permet de contrôler en permanence de manière automatique et non-intrusive l'identité du porteur de la montre notamment dès qu'il est authentifié.

[0033] L'invention porte aussi sur un programme d'ordinateur comprenant des instructions de code de programme pour l'exécution des étapes 10 à 23 de ce procédé lorsque ledit programme est exécuté par l'unité de traitement 2 de la montre 100.

Revendications

1. Procédé de sécurisation d'accès à l'utilisation de fonctions d'une montre (100) comportant les étapes suivantes :

CH 716 900 A2

- authentification (10) du porteur de la montre (100) en vue d'autoriser un accès audites fonctions, et
 - contrôle (13) à période déterminée de l'identité du porteur de la montre par une vérification de la validité d'un élément d'identification numérique déterminé à partir d'au moins un élément d'information biométrique compris dans une portion de peau d'un porteur de ladite montre en vue de conserver/supprimer l'autorisation d'accès audites fonctions.
2. Procédé selon la revendication précédente, caractérisé en ce que l'étape de contrôle comprend une sous-étape d'acquisition (13) par au moins un capteur biométrique multispectral de peau (24) compris dans la montre (100), d'une pluralité d'images d'une portion de peau du porteur adjacente audit capteur (24), lesdites images comprenant ledit au moins un élément d'information biométrique compris dans cette portion de peau.
 3. Procédé selon l'une quelconque des revendications précédentes, caractérisé en ce que l'étape de contrôle (13) comprend une sous-étape de génération (17) d'un élément d'identification numérique à partir dudit au moins un élément d'information biométrique.
 4. Procédé selon l'une quelconque des revendications précédentes, caractérisé en ce que l'étape de contrôle (13) comprend une sous-étape de validation (20) d'un élément d'identification numérique généré en prévision du contrôle de l'identité du porteur.
 5. Procédé selon la revendication précédente, caractérisé en ce que la sous-étape de validation (20) comprend une phase de comparaison (21) comportant une sous-phase de conservation (22) de l'autorisation d'accès audites fonctions de la montre si l'élément d'identification numérique généré est sensiblement similaire ou similaire à un élément d'identification numérique de référence.
 6. Procédé selon l'une quelconque des revendications 2 à 5, caractérisé en ce que la sous-étape d'acquisition (13) comprend une phase d'éclairage (14) de la portion de peau selon différentes longueurs d'onde.
 7. Procédé selon l'une quelconque des revendications 2 à 6, caractérisé en ce que la sous-étape d'acquisition (13) comprend une phase de capture (15) d'images de la portion de peau éclairée à différentes longueurs d'onde.
 8. Procédé selon l'une quelconque des revendications 3 à 7, caractérisé en ce que la sous-étape de génération (17) comprend une phase de caractérisation (18) dudit au moins un élément d'information biométrique compris dans les images acquises relatives à ladite portion de peau.
 9. Procédé selon l'une quelconque des revendications 3 à 8, caractérisé en ce que la sous-étape de génération (17) comprend une phase de conception (19) de l'élément d'identification numérique à partir de la caractérisation dudit élément d'information biométrique.
 10. Procédé selon l'une quelconque des revendications 1 à 9, caractérisé en ce que l'élément d'information biométrique est relatif à un réseau vasculaire ou à une texture de cette peau.
 11. Système de sécurisation d'accès à l'utilisation de fonctions d'une montre (100) mettant en oeuvre le procédé selon l'une quelconque des revendications précédentes, le système (1) comprenant les éléments suivants reliés entre eux : une unité de traitement (2), un capteur biométrique multispectral de peau (24), une interface de saisie (25) et une interface de diffusion d'une information visuelle (3).
 12. Montre (100), notamment une montre (100) mécanique connectée, comportant un système (1) selon la revendication précédente.
 13. Programme d'ordinateur comprenant des instructions de code de programme pour l'exécution des étapes (10 à 23) du procédé selon l'une quelconque des revendications 1 à 10 lorsque ledit programme est exécuté par une unité de traitement (2).

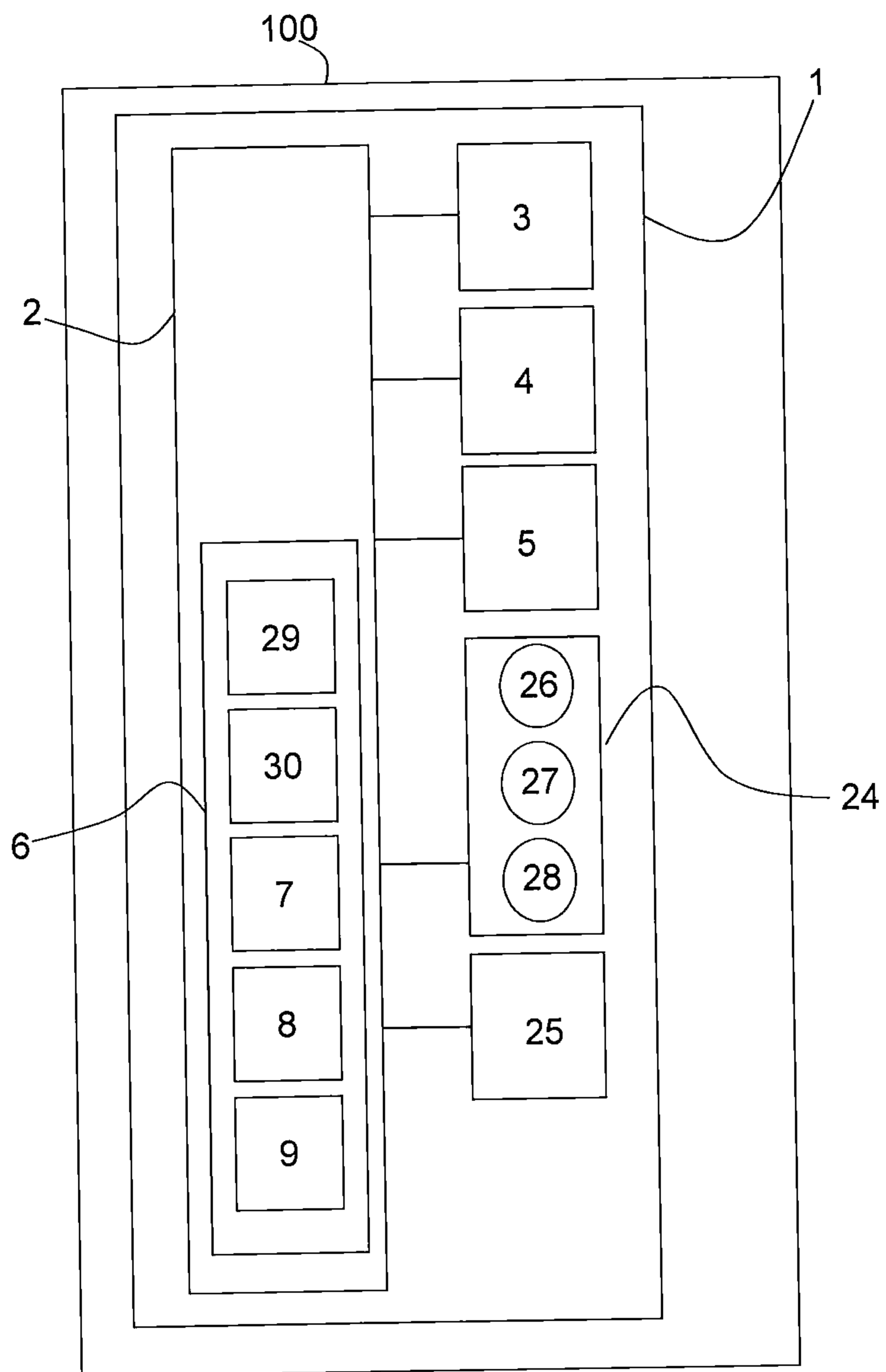


FIG. 1

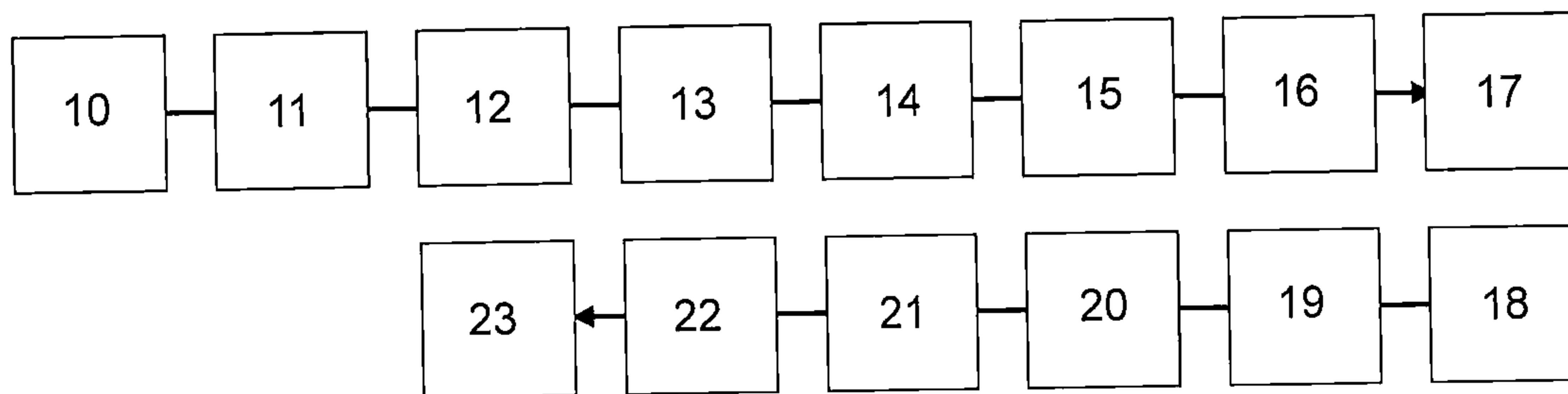


FIG. 2