

# IDENTIFICATION ET AUTHENTIFICATION BIONUMERIQUES



# SOMMAIRE

Sommaire.....	2
Préambule.....	3
Problématique.....	3
Petit glossaire.....	4
Identification et authentification par biométrie .....	5
1 - Analyse morphologique .....	5
Identification par l’empreinte digitale réduite (EDR).....	5
Identification par la morphologie de la main .....	5
Identification par l’iris .....	5
Identification par la rétine.....	6
Reconnaissance faciale .....	6
Identification par thermographie .....	7
2 - Analyse comportementale .....	7
Authentification par une signature biométrique .....	7
Identification par la voix.....	7
3 - Analyse de traces biologiques.....	8
Tableau récapitulatif des principales techniques .....	8
Exemple de reconnaissance de l'empreinte digitale .....	9
1 - Stockage de l'empreinte par scanner, caméra, fichier. ....	9
2 - Filtrage des images (Segmentation). ....	9
3 - Evaluation de la qualité de l'empreinte capturée.....	9
4 - Squelettisation de l'empreinte. ....	9
5 - Extraction des minuties. ....	9
Implémentation et impact d’une solution biométrique.....	11
Réflexion sur les systèmes biométriques .....	14

# PREAMBULE

## *Problématique*

Nous entendons parler de plus en plus de la biométrie car elle est chaque jour plus présente dans notre entourage. Les systèmes d'authentification biométriques peuvent être une solution fiable et rapide pour contrôler notre identité et surveiller des zones sensibles. Cette technologie émergente est certes intéressante dans bien des situations, mais il est nécessaire de prendre en considération certains points avant d'envisager de telles solutions :

- Les appareils de reconnaissance automatique ne sont pas fiables à 100 % : il faut être conscient qu'il peut y avoir des défauts. Il en va de même pour les logiciels qui les exploitent. De ce fait, il faut définir les conditions de fiabilité d'une signature numérique afin de calculer les risques d'erreur.

- Les usagers peuvent changer, les accès ou permissions peuvent être modifiées. Il faut aussi définir les conditions de validité d'une identification.

- Il est important de bien connaître les utilisations et buts de ces authentifications. Il faut penser au consentement des personnes analysées, ainsi qu'aux éventuelles atteintes à la vie privée. La mise en oeuvre des systèmes biométriques est soumise en France à la loi 78-17 du 6 janvier 1978, relative aux fichiers et aux libertés. Cette mise en oeuvre sur le territoire français ne peut intervenir qu'après autorisation de la Commission Nationale de l'Informatique et des Libertés (CNIL). Une autorisation qui garantit au public l'absence de toute atteinte à la vie privée, ou aux libertés individuelles et publiques.

- En cas de litige, les validations des authentifications peuvent-elles être reconnues d'un point de vue juridique ?

- Pour accroître la sécurité, est-il utile de sécuriser les appareils validant les autorisations, ainsi que les certificats numériques (chiffrage) ?

- Concernant les informations d'authentification enregistrées, doivent-elles ou non rester confidentielles ?

- Autre point qui peut aussi se révéler être un avantage : il est impossible d'utiliser plusieurs comptes, plusieurs profils, avec une seule empreinte biométrique (comment root peut devenir user ?).

- Il faut évidemment aussi étudier les possibilités d'implémentation en fonction des besoins de l'entreprise, et calculer leurs coûts.

Nous allons passer en revue les différents aspects des systèmes de reconnaissance automatisés qui existent, afin d'avoir une vue plus globale de ces nouvelles solutions d'identification et d'authentification.

Je développerai ensuite les possibilités d'implémentation de ces systèmes, avec leurs avantages et leurs contraintes, notamment dans le cadre informatique.

Dans le but de mieux introduire le sujet, il me paraît utile d'aborder certaines notions.

### **Petit glossaire**

L'**identité** : (en latin, *identitas* ; de *idem*, le même) est un ensemble de circonstances qui font qu'une personne est bien telle personne déterminée. Le but est d'associer une identité à une personne.

Quelque chose d'**authentique** ne peut être contesté, et s'avère véridique, exact. L'authentification permet de confirmer ou d'infirmer une identité proclamée.

L'**anthropométrie** permet de mesurer des éléments morphologiques des humains. Par extension, la **biométrie** consiste à transformer les caractéristiques physiques ou comportementales d'un individu en une empreinte numérique, ou « **signature numérique** ». Ces caractéristiques doivent être universelles, uniques, permanentes, collectables et mesurables.

L'identification et l'authentification par biométrie désignent les systèmes et pratiques permettant de relier les identités numériques d'une personne (physique ou morale) à son identité physique, et de savoir démontrer une identité de manière probante.

Les systèmes biométriques opèrent une **comparaison statistique** entre l'identité numérique de référence et l'empreinte captée. Toutefois, ces comparaisons mesurées peuvent présenter une part d'incertitude ou d'erreur :

Selon les statistiques calculées, il en résulte trois mesures. :

- un taux de rejet (**FTE** ou Failure To Enroll). Il s'agit du pourcentage de cas qui ne pourront être analysés à cause d'une qualité insuffisante de l'image ou de défauts trop importants.

- un taux de faux rejets (**FRR** ou False Rejection Rate) : pourcentage de personnes rejetées par erreur.

- un taux de fausses acceptations (**FAR** ou False Acceptation Rate) : pourcentage de personnes acceptées alors qu'elles ne sont pas autorisées.

Idéalement,  $FTE=FRR=FAR=0$ .

# IDENTIFICATION ET AUTHENTIFICATION PAR BIOMETRIE

Il existe sur le marché différents appareils permettant ce type d'identifications et d'authentifications. Nous pouvons les regrouper en trois catégories de techniques:

## **1 - Analyse morphologique**

### **Identification par l'empreinte digitale réduite (EDR)**

Ce procédé est le plus répandu et le plus ancien puisqu'il a été inauguré par Alphonse Bertillon en 1882.

La donnée de base est le dessin représenté par les crêtes et sillons de l'épiderme (jonctions, terminaisons aveugles, croisements...). Une empreinte est caractérisée par une centaine de points particuliers (appelés minuties), dont seuls une douzaine suffisent pour une identification.

Certains modules de reconnaissance d'empreintes vérifient la température du doigt, sa conductivité, les battements de cœur, ainsi que d'autres paramètres biologiques - pour éviter de confondre un vrai doigt avec une fausse empreinte en gélatine.

### **Identification par la morphologie de la main, ou « empreinte palmaire »**

90 caractéristiques de la main sont analysées, dont la forme générale, les longueurs et largeurs des doigts, les formes des articulations... Le taux d'erreurs peut être élevé entre personnes d'une même famille.

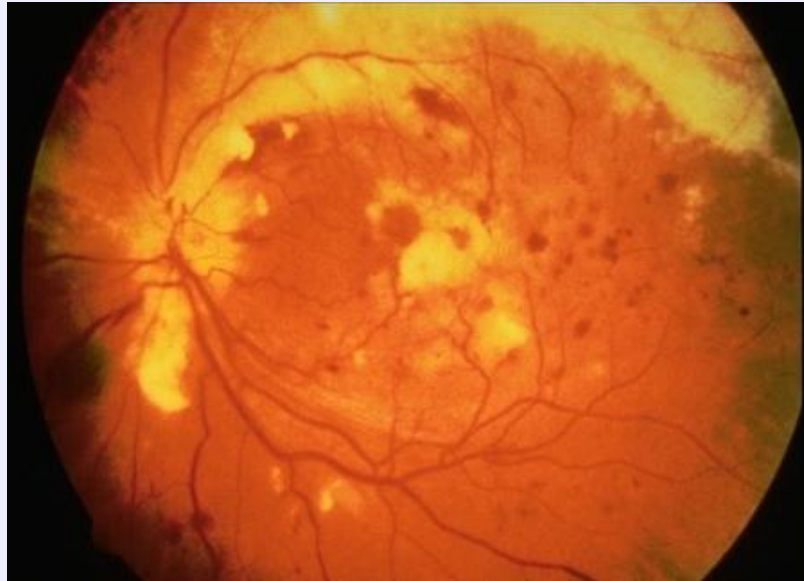
### **Identification par l'iris**

Cette technique peut être exploitable très tôt dans le vie d'une personne car la structure de l'iris est définitive dès la 8<sup>ième</sup> semaine de maternité ! Elle est très fiable du fait qu'il est possible de définir plus de 240 points caractéristiques. Certains systèmes d'identification évolués permettent de contrôler que l'iris change bien de taille avec l'intensité de la lumière.



## Identification par la rétine

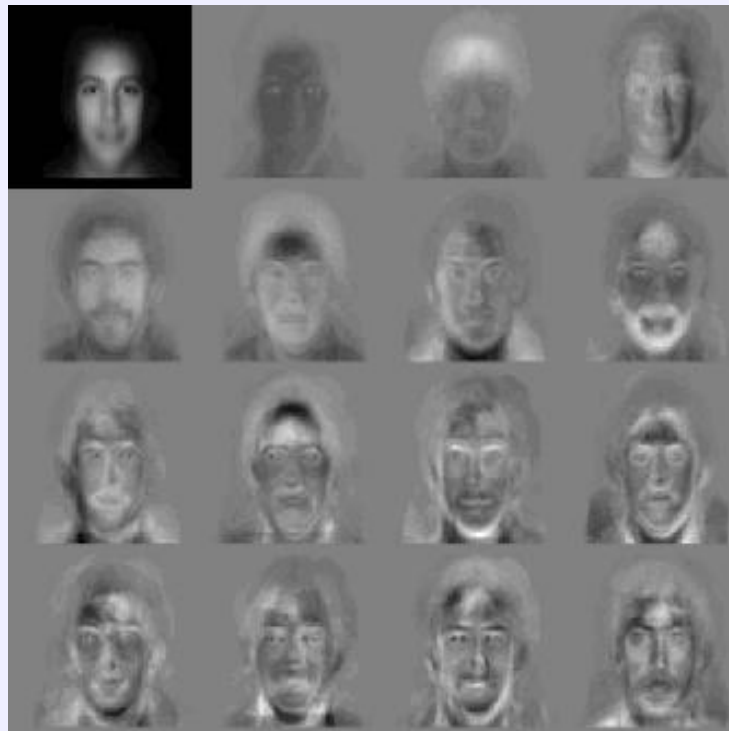
Les schémas des vaisseaux sanguins de la rétine sont uniques pour chaque individu. Jusqu'à 400 points caractéristiques permettent de les différencier. La contrainte majeure de ce procédé est la proximité de l'œil par rapport au capteur (collaboration étroite de la part du sujet).



© Société Canadienne d'ophtalmologie

## Reconnaissance faciale

Elle se base sur une photographie du visage décomposée en plusieurs images faites de nuances de gris, chacune mettant en évidence une caractéristique particulière non sujette à modification (haut des joues, coins de la bouche,...). Elle est très variable selon l'éclairage, l'expression...



© MIT

Cette technique peut être utilisée sans obtenir le consentement de la personne identifiée.

## **Identification par thermographie**

Une caméra infrarouge établit une cartographie des températures des différentes régions du visage - une caractéristique biologique qui est propre à chaque individu. On peut aller même aller plus loin, en établissant une cartographie du système veineux



© anonymous

## **2 - Analyse comportementale**

Par opposition à la biométrie basée sur des caractéristiques physiques, l'analyse comportementale est dynamique, et est plus difficile à reproduire.

### **Authentification par une signature biométrique**

Elle est basée sur l'analyse et le calcul de la dynamique d'une signature. Ce système est basé sur des critères précis comme la pression, l'accélération, la souplesse, les courbes et plusieurs dizaines d'autres paramètres.

### **Identification par la voix**

Elle est basée essentiellement sur la tonalité, la fréquence vocale et la distance entre la formation des lettres, et dépend grandement de la qualité d'enregistrement et de la méthode utilisée : on distingue les systèmes à texte prédéterminé où l'utilisateur doit répéter un texte qu'il ne choisit pas, et les systèmes où la personne peut parler librement. De plus, on doit tenir compte de la variabilité de la voix du locuteur dans le temps comme dans le cas de maladie (rhume,...), et des états émotionnels.

Cette technique peut être utilisée sans obtenir le consentement de la personne identifiée.

### **3 - Analyse de traces biologiques**

Ces procédés se basent sur des prélèvements (salive, urine, sang, ADN, odeur).

***Tableau récapitulatif des principales techniques***

<b>Méthode</b>	<b>Utilisation %</b>	<b>Nombre de points mesurables</b>	<b>Fiabilité</b>
Empreintes digitales	50	(80)	Assez bonne
Reconnaissance faciale	15	Selon la photo	Variable
Reconnaissance de la main	10	(90)	Bonne
iris	6	(244)	Proche de 99%
signature	< 5	Selon la signature	Variable
voix	Peu utilisé	Dépend des bruits de fond	Peu fiable
Rétine	Rare	400	Excellente

La finalité d'un système biométrique est l'identification et l'authentification d'une personne grâce à la mesure et à la reconnaissance de ce qu'elle est, en se basant sur ses caractéristiques physiologiques ou comportementales. Cette approche est différente des autres systèmes d'identification qui se basent sur ce qu'elle possède (carte, badge, document..) ou ce qu'elle sait (mot de passe, code pin...).

## **EXEMPLE DE RECONNAISSANCE DE L'EMPREINTE DIGITALE**

Pour illustrer un principe d'identification, nous allons analyser les différentes étapes de la reconnaissance d'empreinte. Ces étapes sont au nombre de six, et sont énumérées ci-dessous :

### ***1 - Stockage de l'empreinte par scanner, caméra, fichier.***

Le mode d'acquisition importe peu. Il doit être suffisamment précis pour pouvoir collecter le plus de détails possibles.

### ***2 - Filtrage des images (Segmentation).***

Suppression des zones de bruit et en faisant ressortir la plus grande partie possible d'information utile au système.

### ***3 - Evaluation de la qualité de l'empreinte capturée.***

Le système calcule un facteur de qualité qui permet d'établir un critère de fiabilité de la "signature" de l'empreinte.

### ***4 - Squelettisation de l'empreinte.***

Il est nécessaire d'obtenir une image schématique de l'empreinte, dans laquelle toutes les lignes ont la même épaisseur (1 pixel) afin de pouvoir détecter rapidement les minuties.

### ***5 - Extraction des minuties.***



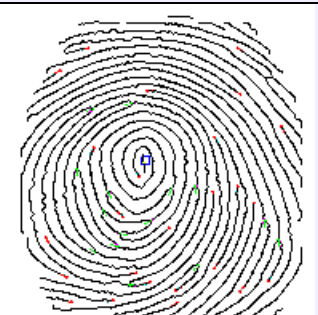



C'est le processus final qui complète l'obtention de la "signature" de l'empreinte. A partir d'une image de l'empreinte préalablement traitée, on extrait grâce à différents algorithmes une structure de données (ou signature).

La signature retenue pour caractériser l'empreinte est basée sur un ensemble suffisant et fiable de minuties (environ 14). Il est alors possible d'identifier une empreinte parmi plusieurs millions d'exemplaires.


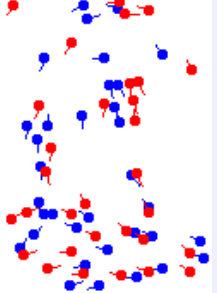
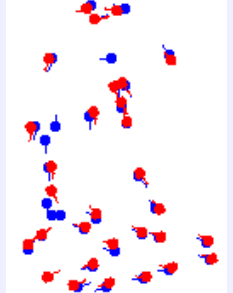
Généralement, chaque minutie occupe environ un espace de 16 octets.

Lors du processus d'extraction, on détecte initialement 100 minuties en moyenne, parmi lesquelles environ 60 % correspondent à de fausses minuties qui seront identifiées lors d'un processus ultérieur. Le logiciel extrait donc une quarantaine de minuties réelles de l'empreinte. Cette valeur est nettement supérieure au minima (légalement 12), ce qui augmente la fiabilité. De plus, ce chiffre est loin du total de minuties détectées, ce qui laisse supposer que n'ayant conservé que les plus fiables, on a éliminé les minuties erronées qui auraient pu détériorer le comportement du système.

## Enregistrement de l'empreinte

Empreinte	Image numérisée	Recherche des minuties
		
Extraction des minuties	Numérisation	Enregistrement
		

## Comparaison de deux empreintes

Extraction des minuties	Chevauchement	Rotation – concordance
		

© 1999 Thomson TCS fingership

L'empreinte digitale ne peut pas être recrée à partir de l'information stockée. De ce fait, il n'y a aucun risque de violation de l'intégrité personnelle de l'utilisateur.

## IMPLEMENTATION ET IMPACT D'UNE SOLUTION BIOMETRIQUE

L'authentification des individus peut être utile pour des applications diverses, tels que :

- la surveillance et le contrôle d'accès aux zones sensibles. Les aéroports utilisent la biométrie pour faire face à la croissance du trafic aérien et l'augmentation des passagers. Cela leur permet d'accroître la sécurité des passagers, et de réduire le temps de contrôle au niveau de l'enregistrement et de l'embarquement.

- l'accès aux zones restreintes (laboratoires, bâtiments militaires, casinos, parkings...), ou privées (coffres...).

- la comptabilisation et la traçabilité d'utilisateurs (gestion des présences, du temps de travail...)

- la validation de transactions en ligne (ordres boursiers, achat dans les sites marchands...)

- la sécurité informatique (permissions et restrictions des utilisateurs, des groupes, audits...)

- la personnalisation d'environnements informatiques (enregistrement des préférences de travail...)

Dans le cadre d'un service informatique, plusieurs fournisseurs proposent divers produits qui s'adaptent simplement à un réseau.

Afin de sécuriser l'accès physique aux zones restreintes comme les salles machines, et de remplacer les clés ou badges, un lecteur d'empreinte digitale peut être une solution idéale :



© actronix

**Caractéristiques :**

- Jusqu'à 4000 empreintes mémorisées au sein d'un même boîtier permettant les opération d'enrôlement et de vérification
  - Interface utilisateur intuitive avec 3 témoins lumineux et signaux sonores.
  - Détection automatique du doigt permettant une identification simple et instinctive.
  - Boîtier compact et ergonomique.
  - Options multiples d'administration :
    - en autonome (en connectant un PC portable)
    - en réseau (option Ethernet)
- Temps de vérification : < 1 seconde pour 100 utilisateurs enrôlés  
Temps d'enrôlement : < 3 secondes

Taux :		
Fausse Acceptation	Rejet	d'Egal Erreur (EER)
0,005 %	0,01 %	0.1%

Prix : environ 1 400 €

Contrairement aux systèmes de reconnaissance palmaires ou de l'iris, cette solution reste abordable, et peut s'intégrer aisément sans trop de contraintes. Nous pouvons de même constater que les taux d'erreurs restent acceptables, ce qui prouve une assez bonne fiabilité.

Du point de vue du contrôle d'accès logiciel, là aussi il existe plusieurs solutions possibles. L'une des plus conviviales reste la reconnaissance de l'empreinte digitale capturée par un appareil spécifique, ou alors intégrée dans une souris ou un clavier.

### Connexion par port U.S.B



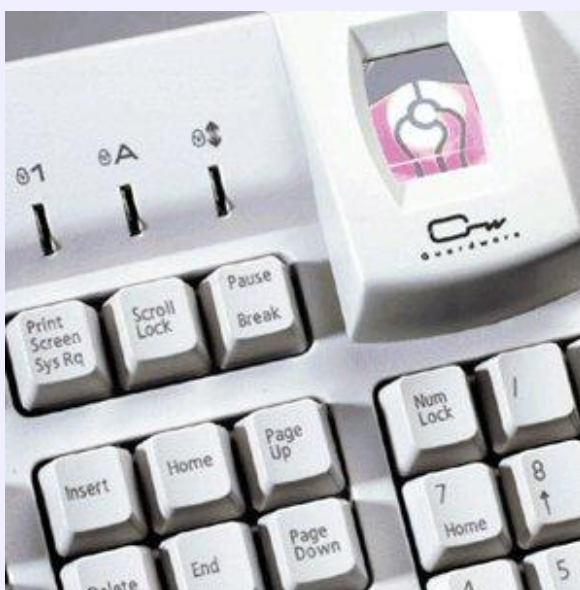
© actronix

### Capteur intégré à la souris



© istec

### Lecteur d'empreinte sur le clavier



© actronix

Pour récapituler les caractéristiques et les besoins communs pour ce type d'appareils, nous pouvons établir la liste suivante:

- Lecture et reconnaissance d'une nouvelle empreinte digitale inférieur à ½ seconde.
- Tolérance de positionnement: rotation de 45°.
- Placement à 5 mm du centre.
- 10 utilisateurs possibles pour 1 PC.
- Faux rejets : 0,01%.

Besoins du système :

- Intel 80486 DX100 et supérieur.
- 16 Mo de mémoire RAM.
- 15 Mo sur le disque dur.
- Un port USB ou parallèle (ne bloque pas le port imprimante).
- Un lecteur CD-ROM pour installation.
- Microsoft Windows 9x/ME/NT/2K/XP, Novell.

Prix : entre 100 et 170 €

Ces produits ne nécessitent presque pas de place, ils reconnaissent rapidement les empreintes digitales, et ne requièrent pas d'ordinateurs puissants pour fonctionner. Leurs coûts n'est pas élevé à l'unité, mais peut rapidement devenir important selon le nombre d'utilisateurs.

Mis à part l'acquisition de ces matériels, il reste à choisir un logiciel pour la gestion des droits d'accès. Parmi ceux-ci, certains permettent en plus de la simple authentification :

- la localisation d'une personne identifiée (dans une entreprise).
- la gestion du temps de présence par système de pointage.
- la protection des fichiers et les dossiers avec un encryptage par empreinte digitale.
- la sortie de l'écran de veille via l'identification par empreinte digitale.
- des paramétrages multi utilisateurs travaillant avec le même système.
- le stockage des tentatives d'accès illégaux sur le PC.

Nous pouvons trouver ces logiciels à un prix avoisinant les 1 000 €.

En prenant en compte ces paramètres, il est tout à fait envisageable d'intégrer des systèmes d'authentification biométriques dans une entreprise, encore faut-il connaître les réels besoins de sécurité.

## REFLEXION SUR LES SYSTEMES BIOMETRIQUES

L'automatisation de la reconnaissance et de l'authentification des individus présente bien des avantages. Grâce à de tels systèmes, il n'est plus indispensable pour l'utilisateur de retenir son login et son mot de passe, ni d'avoir à le changer régulièrement. Cela supprime de ce fait les problèmes de mots de passes trop simples, faciles à retrouver pour les pirates.

Pour les administrateurs systèmes, la gestion des couples logins / passwords est supprimée et remplacée par une signature numérique difficilement falsifiable, et de très faible encombrement (9 octets pour la main, 512 octets pour l'iris).

La mise en place et l'installation de solutions biométriques sont rapides, et leurs utilisations sont relativement fiables (en fonction de leurs taux de faux rejets FRR et FAR).

Le coût des équipements sont de plus en plus abordables, mais restent pour l'heure plutôt réservés à un nombre de personnes restreint.

Par ailleurs, la biométrie n'est pas une science exacte : elle reste dépendante de la qualité des captures, du traitement de celles-ci, et donne des réponses en termes de « pourcentage de similitude ». Il faut donc tenir compte d'un facteur risque.

D'autre part, le couple « login / password » à été testé et approuvé depuis des années pour l'identification, et d'autres solutions existent pour renforcer l'authentification des personnes (clés publiques / privées).

Nous devons aussi tenir compte de l'existence d'autres systèmes fonctionnels mis en œuvre dans beaucoup de sociétés, tel les badges qui restent une solution peu coûteuse...

Mais tous ces procédés évolués ne nous font-ils pas perdre des valeurs essentielles, telle la confiance ? Il existe heureusement bien d'autres systèmes basés sur cette dernière, qui reste tout à fait envisageables !

Quel avenir construisons-nous ? Sommes nous prêts à être surveillés continuellement par des machines parfois à l'insu de notre plein gré ? Pour quelles raisons, et pour quels buts ? Où est notre vie privée, est-ce légal (la CNIL considère la plupart des techniques biométriques comme "porteuses de sécurité, mais redoutables pour nos libertés") ?

Les systèmes automatisés font toutefois partie de notre avenir ; il reste à savoir mesurer les tenants et conséquences d'un point de vue utile, tout en restant pragmatique.