Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Préposé fédéral à la protection des données et à la transparence
PFPDT

Tour d'horizon des technologies biométriques

Projet CCT – PFPDT – juin 2012

Table des matières

1. Introduction

Au travers de ce projet, le Centre de Compétences Technologiques (CCT) du PFPDT propose un tour d'horizon des différentes technologies biométriques. Ce projet permet d'obtenir un aperçu plus ou moins exhaustif des technologies utilisées actuellement, de leur fiabilité, de leur facilité d'utilisation et de leurs principales qualités ou défauts, d'un point de vue essentiellement technique.

Certaines technologies ont pu être testées dans le cadre du laboratoire d'analyse du PFPDT, afin d'évaluer la commodité d'utilisation des différents périphériques et des logiciels nécessaires à l'enregistrement et à la capture des empreintes biométriques.

N'ayant ni l'accès à des bases de données biométriques, ni les ressources nécessaires pour développer nos propres tests, nous nous référons à la littérature scientifique pour l'évaluation quantitative et qualitative des différentes technologies.

Le PFPDT a également publié un «Guide relatif aux systèmes de reconnaissance biométrique», disponible sur le site Internet du préposé (http://www.leprepose.ch > Brochures > Protection des données)

Terminologie

Authentification: 1 à 1 (est-il bien celui qu'il prétend être?)
Identification: 1 à N (qui est-il parmi toutes les personnes enregistrées?)

Méthode d'analyse

Les points ci-dessous sont observés pour chacune des technologies biométriques évaluées:

- **Type**: S'agit-il d'une biométrie comportementale ou physique, est-elle invasive ou non, est-elle facilement imitable ou non, etc.?
- **Contexte**: Dans quel contexte la caractéristique est-elle le plus utilisée, se retrouve-t-elle le plus fréquemment? Quels types d'applications sont concernés par cette biométrie?
- **Protection des données**: Quels risques pour la protection des données sont associés à une caractéristique? Celle-ci laisse-t-elle des traces?
- **Avantages/Désavantages**: Quels sont les avantages/désavantages de la technologie?
- **Technique**: Quels sont les algorithmes utilisés, les images conservées, les taux de faux rejet (FRR), de fausse acceptation (FAR)?
- **Produits**: Quels produits sont disponibles sur le marché?
- **Tests**: Quels sont les constatations issues des tests, s'ils ont pu être pratiqués? Si les tests n'ont pas pu être pratiqués, nous donnons certains renseignements obtenus lors de projets similaires extérieurs au PFPDT.

Sur la base des informations disponibles sur internet et dans la littérature, ainsi que sur la base des connaissances des collaborateurs du PFPDT impliqués dans ce projet, ces différents champs seront renseignés ci-après pour chaque caractéristique.

2. Réseau veineux

L'analyse du réseau veineux est une technologie très récente dans le domaine de la biométrie. Grâce à une caméra infrarouge, les veines de la paume ou du doigt sont extraites. Le réseau veineux de chaque individu est unique, également celui de jumeaux. Il n'évolue plus avec le temps, une fois la croissance terminée. Le réseau est extrêmement complexe, ce qui augmente les difficultés pour une éventuelle falsification, en plus du fait que le réseau n'est pas visible à l'œil nu.

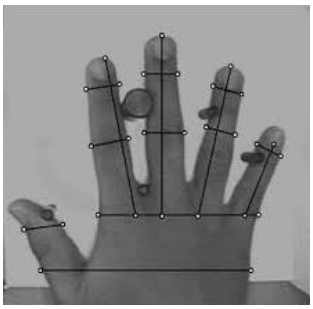
Réseau veineux	**Observations:**
Type	Biométrie physique. Très peu invasive, facilement acceptable. Falsification extrêmement difficile puisque le réseau est invisible à l'œil nu.
Contexte	En général, applications nécessitant une sécurité importante et des taux de faux rejet et de fausse acceptation très bas. Au Japon, dans les bancomats, hôpitaux, universités.
Protection données	Pas de risques spécifiques liés à la protection des données. Technologie sans traces.
Avantages	Technologie très peu invasive (sans contact avec le lecteur) et très fiable. Aucun changement dans le temps, grande stabilité. Rapport qualité-coût très intéressant. Garantie d'une grande sécurité. Lecteur intégré à des périphériques courants, tels que clavier et souris.
Désavantages	Technologie récente, pas de bases de données libres qui permettent des tests indépendants.
Technique	Traitement sur l'image capturée par des caméras infrarouges puis mesures des distances entre différents points, un peu à l'image des minuties des empreintes digitales. Avec le PalmSecure de Fujitsu, FRR de 0.01% et FAR de 0.00008%.
Produits	Fujitsu propose un lecteur fiable.
Tests	Le lecteur **Fujitsu** a été installé dans le laboratoire. Il s'agit d'un lecteur intégré à une souris (voir illustration ci-après). *Facilité d'installation*: Le lecteur Fujitsu est livré avec un logiciel de tests qui permet de s'enrôler dans le système, puis de s'authentifier (1 à 1) ou de s'identifier (1 à n). *Facilité d'utilisation*: Du fait que la main n'est posée sur aucun support, il faut un certain temps d'adaptation pour comprendre comment l'orienter et à quelle distance la positionner pour que le lecteur puisse lire une empreinte: la prise en main n'est donc pas complètement intuitive. Lors de nos brefs tests, nous avons été confrontés à des cas de faux rejet. Le lecteur de réseau veineux pour le doigt de **Hitachi** que nous avons également testé est plus simple d'utilisation puisqu'il permet de guider le doigt et de le positionner correctement (cf. illustration ci-après). Toutefois, il

	s’agit d’un périphérique additionnel à installer sur la machine et est de ce fait moins intéressant que la souris Fujitsu. De plus, le réseau veineux du doigt, puisque moins complexe, est moins sûr que celui de la main. Il est possible de s’identifier dans la version de démonstration et de s’authentifier dans la version complète.

Fujitsu PalmSecure Mouse

Hitachi Finger Vein Scanner

3. Dos de la main



Cette caractéristique concerne la géométrie du dos de la main. Les mesures sont effectuées sur la longueur et la largeur, mais également l'épaisseur des doigts avec des jeux de miroirs lors de la capture.

Cette biométrie est utilisée depuis le début des années 1980.

Dos de la main	Observations:
Type	Biométrie physique. Peu invasive, facilement acceptable. Falsification difficile puisque cela nécessite la fabrication d'un moule entier de la main (obligatoirement en 3D avec un effet de rendu de la peau réaliste suivant les systèmes utilisés).
Contexte	En général, applications nécessitant une sécurité basse à moyenne mais une rapidité d'exécution importante. Par exemple, application de gestion du temps.
Protection données	Risques liés à la couleur de la peau, au sexe. Pour récupérer une trace d'une main, il faudrait une série de photographies pour reconstituer la main en 3D, donc peu de traces.
Avantages	Technologie peu invasive et facile d'utilisation Rapidité de traitement
Désavantages	Machine assez encombrante: elle nécessite de positionner la main de manière déterminée (doigts écartés, par exemple) afin d'améliorer les taux de faux rejet.
Technique	La partie délicate est dans la détection de la main et des points d'ancrage pour les mesures à effectuer. C'est pour simplifier ceci que la main est parfois positionnée dans le lecteur à l'aide d'un modèle. Les mesures sont principalement effectuées sur les doigts (largeur, longueur, épaisseur). On constate un FAR assez élevé, en général entre personnes de la même famille ou de jumeaux.
Produits	Entre autres, la société française Abiova propose deux types de lecteurs, qui respectent les normes de la CNIL.
Tests	Pas de tests effectués auprès du PFPDT (pas de produits disponibles). Toutefois, une expérience antérieure montre que le système à mettre en place est relativement complexe pour garantir la prise d'une photo utilisable et facilement analysable.

4. Empreinte digitale

Les empreintes digitales sont les caractéristiques les plus populaires. Elles sont utilisées comme empreintes biométriques depuis très longtemps dans les milieux policiers et judiciaires. Elles ont de ce fait une connotation négative qui rebute souvent les utilisateurs, alors qu'ils acceptent plus facilement d'autres techniques. Elles n'en restent pas moins des biométries fiables puisque chaque individu a des empreintes digitales quasiment uniques. Ce sont les arêtes de l'empreinte qui sont pertinentes pour l'analyse. Des minuties en sont extraites. Il s'agit de points de rencontre entre arêtes, de points de séparation ou rebroussement d'arêtes ou d'autres motifs particuliers.

Empreinte digitale	Observations:
Type	Biométrie physique. Très populaire, malgré une connotation négative. Les empreintes digitales peuvent être facilement récupérées et des copies bon marché à base de colle blanche par exemple peuvent être produites. La popularité de cette biométrie rend sa falsification également maîtrisée.
Contexte	Applications nécessitant une sécurité moyenne qui supposent également une bonne acceptation de la part des utilisateurs. Par exemple, applications à utiliser chez soi: portable, e-banking, etc.
Protection données	Risques liés à la protection des données, en particulier à la reconnaissance de la race. Traces évidentes: les empreintes sont faciles à récupérer et à falsifier.
Avantages	Technologie connue et maîtrisée. Relativement bon marché.
Désavantages	Soumise aux aléas de la vie quotidienne, tels que les accidents domestiques (coupures). Risque de détérioration de l'empreinte.
Technique	Deux types de lecteurs: thermique et infrarouge. Les lecteurs thermiques demandent moins d'entretien mais sont plus compliqués d'utilisation et peuvent produire des images de moins bonne qualité selon les conditions extérieures. Les lecteurs infrarouges, pour autant qu'ils soient régulièrement nettoyés, rendent des images claires et uniformes. Les algorithmes se basent sur la détection des minuties et la mesure de distances entre minuties. Les taux FAR/FRR sont très dépendants de problèmes liés au hardware et au software, mais également de problèmes physiologiques (qualité du doigt – mouillé, sec…) ou opérationnels (pression du doigt sur le capteur, etc.).
Produits	Il existe énormément de lecteurs d'empreintes digitales. Certains sont intégrés sur des périphériques ou directement sur les ordinateurs portables.
Tests	Une certaine adaptation est nécessaire lors de la prise en main des différents lecteurs. Le lecteur thermique en particulier demande un certain entraînement pour produire une empreinte lisible et utilisable (vitesse de passage, pression).

5. Paume de la main

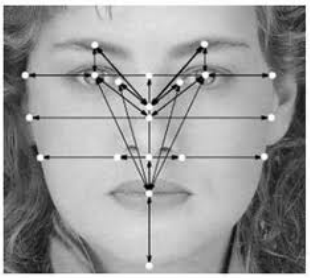
La biométrie de la paume de la main permet de combiner plusieurs techniques telles que la géométrie de la main (cf. dos de la main) et les empreintes digitales de plusieurs doigts. De plus, certaines techniques s'intéressent aussi à des analyses fines de la texture de la paume qui est, semble-t-il, tout à fait discriminante. Bien évidemment, le réseau veineux de la main peut également être considéré lorsque la paume de la main est captée. Cela en fait une caractéristique forte et sûre du fait du nombre de techniques utilisables sur une seule empreinte, pour autant que le lecteur soit adapté aux différentes caractéristiques. Les avantages et désavantages sont ceux détaillés dans chaque section correspondante. Cette caractéristique est utilisée par des applications nécessitant un confort d'utilisation et une sécurité importante.

6. Voix

La voix est une caractéristique extrêmement recherchée dans des systèmes liés à des applications à distance où la personne s'authentifie par téléphone par exemple. Elle est toutefois une caractéristique très délicate à utiliser car elle est extrêmement soumise aux conditions extérieures (maladie, stress de la personne, etc.). De ce fait, elle est une caractéristique à la fois physique et comportementale. Elle est parfois choisie en combinaison avec une autre caractéristique (voix et écriture par exemple).

Voix	Observations:
Type	Biométrie physique avec des composantes comportementales. Peu invasive, facilement acceptable pour des applications à distance. Falsification difficile, éventuellement avec entraînement.
Contexte	Applications nécessitant des connexions à distance via le téléphone par exemple.
Protection données	Peu de risques liés à la protection des données. Traces possibles: enregistrement, éventuellement à distance avec des micros directionnels.
Avantages	Biométrie peu invasive. Utilisable à distance. Technologie peu coûteuse puisqu'elle ne nécessite pas de lecteur particulier (micro et logiciel d'analyse uniquement).
Désavantages	Beaucoup de changements peuvent survenir dans l'empreinte vocale en fonction de conditions extérieures telles que maladie, stress, vieillissement, etc. L'environnement et les bruits extérieurs ont également une influence sur la voix et sur la qualité de la capture. L'appareil utilisé pour la communication (type de téléphone, microphone, etc.) influence également la qualité de la reconnaissance. Pour parer à ces éventualités, un nombre important d'échantillons de voix doit être stocké, la mémoire utilisée par de telles applications est donc importante.
Technique	Des modèles statistiques sont extraits de l'onde vocale et stockés. Lors d'une authentification/identification, les extraits sont comparés à ces modèles. Le taux de faux rejet peut être relativement élevé, selon la qualité des conditions extérieures.
Produits	De nombreux logiciels de reconnaissance vocale existent sur le marché, il faut distinguer les logiciels de dictée des applications biométriques qui permettent l'authentification.
Tests	Pas de tests effectués au laboratoire.

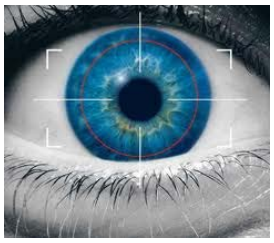
7. Visage



La biométrie du visage s'intéresse à la forme de celui-ci. Les mesures sont effectuées en particulier sur la distance entre les yeux, la longueur et la largeur du nez, la profondeur des orbites, la forme des pommettes, la longueur du menton, etc. Environ 80 points du visage peuvent être utilisés pour définir les mesures. Il s'agit d'une biométrie appréciée lorsque les connexions se font à distance au moyen d'une webcam, mais également pour les tâches de surveillance (stades, casinos, etc.). Comme l'ensemble des biométries basées sur des images, elle n'exige que peu d'espace mémoire.
On fait une distinction entre la reconnaissance du visage en 2D, une seule caméra de face capture le visage, et la reconnaissance du visage en 3D où un mécanisme incluant plusieurs prises de vue crée un modèle en trois dimensions du visage.

Visage	Observations:
Type	Biométrie physique. Peu invasive, puisqu'elle ne nécessite pas de contact physique avec un lecteur. Falsification peu aisée puisque une simple photo d'un visage ne suffit pas à berner les systèmes les plus récents: un moule du visage est nécessaire, même pour les systèmes 2D.
Contexte	En général, applications pour des zones critiques de grande échelle. Par exemple, identification de personnes, entrées de stades/casinos/…, surveillance des rues.
Protection données	Risques liés à la protection des données: race, sexe, couleur de peau, etc. 2D avec traces, 3D pratiquement sans traces puisque le système à mettre en place pour retrouver l'entier du visage est extrêmement compliqué.
Avantages	Biométrie facile d'utilisation. Exige peu de mémoire, donc permet un traitement rapide et suppose une technologie peu coûteuse. En effet, les lecteurs peuvent être des caméras simples, voire des webcams.
Désavantages	Les conditions extérieures (luminosité, ombres, positionnement de la personne, expression du visage, etc.) peuvent réduire la qualité de la reconnaissance. La reconnaissance 3D implique un matériel beaucoup plus conséquent et est donc plus coûteuse.
Technique	Sur la base des points détectés sur le visage et des distances entre ces points, des mesures sont effectuées et permettent d'identifier ou d'authentifier la personne. Certaines techniques utilisent également des modèles statistiques pour construire les gabarits (templates). En règle générale, le taux de faux rejet est élevé, principalement en raison de l'influence des conditions extérieures sur la reconnaissance.
Produits	La technologie a pu se développer avec l'installation de caméras de bonne qualité directement intégrées aux ordinateurs. KeyLemon est un produit suisse qui permet de se connecter à sa session sans mot de passe mais simplement en se plaçant devant la caméra.
Tests	KeyLemon a été testé au laboratoire dans sa version de base qui inclut seulement la capture du visage et la construction du modèle associé.

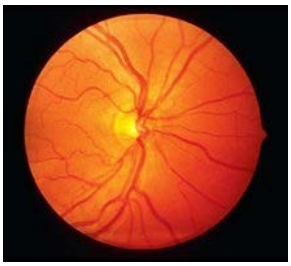
8. Iris



L'iris est la partie colorée de l'œil, elle ne doit pas être confondue avec la rétine, le fond de l'œil, qui est également utilisée comme biométrie. Le dessin de chaque iris est unique et permet d'obtenir une très grande exactitude dans l'analyse. C'est une caractéristique difficile à falsifier, puisqu'elle est non seulement difficile à obtenir mais également difficile à reproduire.

Iris	Observations:
Type	Biométrie physique. Biométrie stable au court du temps et unique (probabilité de similitude extrêmement faible: $1/10^{72}$). Relativement invasive puisque l'utilisateur doit se tenir à environ 30 cm d'une caméra numérique qui lui balaie l'œil pour capturer l'image de l'iris. La falsification est peu aisée. L'iris d'un œil mort se dégrade très vite et ne peut pas berner le système.
Contexte	Cette caractéristique est beaucoup utilisée dans des applications aux frontières pour l'immigration. C'est l'une des trois biométries enregistrées dans les futurs passeports biométriques. Elle a été mise en œuvre à l'aéroport Schiphol d'Amsterdam mais également en Arabie Saoudite, dans différents aéroports au Canada et aux USA ainsi que dans des camps de réfugiés de l'UNHCR au Pakistan.
Protection données	Le contour de l'œil peut donner des informations relatives à la couleur de la peau. Certaines maladies, telles que l'alcoolisme, peuvent être détectées dans l'iris. Pas de traces.
Avantages	Biométrie facile d'utilisation. Exige peu de mémoire, donc permet un traitement rapide et suppose une technologie peu coûteuse. En effet, les lecteurs peuvent être des caméras numériques assez simples.
Désavantages	Les conditions extérieures doivent être contrôlées pour obtenir une bonne image de l'iris avant l'analyse. La reconnaissance est plus délicate avec les personnes aux yeux bridés dont l'iris est partiellement caché.
Technique	On recense environ 240 caractéristiques dans la texture (ou le motif) de l'iris. Les caractéristiques les plus utilisées pour la reconnaissance biométrique sont la collerette, les taches pigmentaires, la taille de la pupille, etc. L'algorithme le plus courant détermine le centre et le tour de l'iris puis découpe des bandes rectangulaires pour obtenir un code iridien qui forme le gabarit.
Produits	EyeLock est un produit, parmi d'autres, pour la reconnaissance de l'iris.
Tests	Pas de tests effectués au laboratoire.

9. Rétine



Cette biométrie capture le fond de l'œil et la reconnaissance s'effectue sur le réseau rétinien. Il n'existe pas de technique connue à ce jour pour falsifier une rétine, la technologie est donc extrêmement sûre. À l'image du réseau veineux, il existe très peu de risques de collision entre les rétines de deux personnes distinctes. Du point de vue de la protection des données, il faut signaler que cette caractéristique permet de connaître l'état de santé de la personne qui s'authentifie puisque certaines maladies transmissibles ou héréditaires peuvent être perçues lors d'un examen de la rétine.

Rétine	Observations:
Type	Biométrie physique. Biométrie unique et stable au cours du temps, pour autant que l'utilisateur demeure en bonne santé. Très invasive, le lecteur peut rebuter l'utilisateur qui pense qu'il risque des dommages à son œil. La falsification n'est pas possible.
Contexte	Applications nécessitant une sécurité haute. Utilisée tout d'abord par le FBI ou la CIA, elle est employée aujourd'hui dans certaines prisons, bancomats, etc.
Protection données	De plus, des informations sur la santé de l'utilisateur peuvent être déduites lors de l'analyse, ce qui représente un risque du point de vue de la protection des données. Aucune trace.
Avantages	Très grande fiabilité. Le taux de reconnaissance est très élevé: peu de risques d'erreur lors de l'authentification/identification. Risques pratiquement inexistants de falsification.
Désavantages	Les cataractes ou certaines formes d'astigmatisme peuvent détériorer les mesures prises sur la rétine. Lecteur très coûteux. Réticence à l'utilisation assez courante. Temps de comparaison assez long suivant la taille de la base de données.
Technique	Les caractéristiques du réseau veineux de la rétine sont codées sous forme de gabarit (template), puis comparées lors de l'authentification. Les taux FAR et FRR sont extrêmement bas.
Produits	Il n'existe pas de produits grand public pour ce type de biométrie.
Tests	Pas de tests effectués au laboratoire.

10. Oreille

La biométrie de l'oreille est l'une des caractéristiques les moins courantes et les moins utilisées. Elle peut rebuter l'utilisateur par son aspect peu conventionnel qui lui conférera une image peu sécurisante. Elle présente toutefois certains avantages par rapport à la biométrie de l'œil ou du visage. Elle est ainsi moins soumise aux conditions extérieures.

Oreille	Observations:
Type	Biométrie physique. Peu invasive, mais peu commune. La falsification requiert la fabrication d'un moule puisque les mesures effectuées peuvent concerner les trois dimensions.
Contexte	Il n'existe pas d'applications commerciales dignes d'intérêt à ce jour mais la recherche s'intéresse à cette biométrie qui comporte certains avantages en termes de confort d'utilisation et d'acceptabilité.
Protection données	Peu de risques liés à la protection des données, mis à part la couleur de la peau. Peu de traces. Les policiers utilisent les empreintes d'oreille contre les portes pour retrouver les malfrats (écoute aux portes avant les cambriolages).
Avantages	L'oreille est moins soumise aux conditions extérieures que l'œil par exemple. Les cheveux ou les lunettes ne gênent pas la reconnaissance, comme pourraient le faire des lentilles de contact. Selon les chercheurs du domaine, la forme de l'oreille ne change pas au cours de la vie. La reconnaissance atteint un taux de 99.6 %.
Désavantages	Technologie encore peu connue et peu utilisée sauf dans l'identification policière. Peu de recul.
Technique	On peut définir un certain nombre de points communs sur chaque oreille. Les positions relatives de ces points les uns par rapport aux autres sont propres à chaque individu. Certaines recherches se concentrent également sur le tour de l'oreille uniquement qui semble être unique.
Produits	Il n'existe pas de produits populaires sur le marché.
Tests	Pas de tests effectués au laboratoire.

11. Signature/Écriture

Cette caractéristique peut se décliner sous plusieurs formes. Il est possible d'utiliser la signature de la personne mais également des textes écrits. De plus, elle peut s'effectuer de manière statique – comparaison du dessin du résultat uniquement – ou de manière dynamique – la «manière» d'écrire est prise en compte.
La dynamique d'une signature/écriture nécessite un matériel adéquat pour être capturée: une tablette graphique ou un stylo spécial équipé de capteurs électroniques. La vitesse, l'inclinaison du stylo, la pression exercée peuvent ainsi être calculées, en plus du dessin de l'empreinte. Une empreinte statique est plus facilement falsifiable puisqu'elle nécessite qu'un simple entraînement, tandis qu'une empreinte dynamique nécessite la réalisation fidèle d'une imitation en temps réel.
Il s'agit d'une caractéristique qui peut être combinée avec d'autres, comme la voix (on dit ce qu'on écrit), pour renforcer la sécurité des systèmes.

Signature/Écriture	Observations:
Type	Biométrie comportementale. Peu invasive, elle est facilement acceptable puisque la signature, par exemple, est déjà utilisée dans un grand nombre d'administrations comme preuve de l'identité d'une personne. La falsification est plus ou moins compliquée selon que l'on a à faire à un système statique ou dynamique. La falsification d'une signature est également plus aisée que celle d'un texte plus long à rédiger.
Contexte	Beaucoup d'applications bancaires par exemple utilisent ce type de biométrie. La signature était déjà très présente lors des transactions et le moyen d'acquisition a simplement été amélioré pour rendre ces transactions plus sûres.
Protection données	Pas de risques liés à la protection des données. Traces dans les systèmes statiques, pas de traces dans les systèmes dynamiques.
Avantages	Cette caractéristique peut être utilisée à distance, à l'aide de tablettes numériques. L'utilisateur «choisit» sa biométrie: il se sent rassuré en traçant une signature plus compliquée que sa signature habituelle, par exemple. Facilement combinable avec d'autres caractéristiques. Technologie peu coûteuse et facile d'utilisation – tablette numérique, stylo numérique.
Désavantages	L'écriture et la signature évoluent avec le temps. Cela peut être plus problématique lors de l'analyse statique que dynamique. Un entraînement peut amener à maîtriser la falsification. La signature et l'écriture peuvent être conditionnées par des éléments extérieurs tels que le stress de la personne concernée.
Technique	Lors d'une comparaison statique, des mesures de distance sont prises entre les points représentatifs des deux images. Lors d'une analyse dynamique, on tient également compte de tous les vecteurs calculés par le matériel (pression, inclinaison du stylo, etc.) ainsi que d'autres aspects tels que la vitesse d'exécution par exemple.
Produits	Des tablettes graphiques peu coûteuses sont maintenant disponibles sur le marché. De nombreuses entreprises proposent des stylos numériques,

	dont Logitech par exemple.
Tests	Pas de tests effectués au laboratoire. Par expérience, on peut signaler que l'entraînement pour imiter une signature dynamique est compliqué et long à réaliser. Il l'est évidemment beaucoup moins pour une signature statique, où l'on peut se permettre de prendre le temps de l'exécution.

12. Démarche

Chaque individu, en fonction de son corps et plus spécifiquement de sa musculature, développe une démarche qui lui est propre. En analysant, entre autres, la distance entre les pas, les enjambées, la vitesse, la cadence, l'angle des pieds, etc., il devient possible d'utiliser la démarche comme caractéristique biométrique.

Démarche	**Observations:**
Type	Biométrie comportementale. Très peu utilisée. Peu invasive mais ne respecte pas véritablement la sphère privée, puisqu'elle permet de reconnaître les personnes à distance, sur un enregistrement vidéo d'une foule par exemple. Elle peut être falsifiée en s'entrainant.
Contexte	Applications nécessitant d'identifier les gens à distance, par exemple, dans une foule. Cette technologie n'est que peu utilisée pour l'identification de personnes mais est utilisée dans les hôpitaux à des fins médicales ou par les sportifs pour l'amélioration de leurs performances.
Protection données	Risques liés à la protection des données typiques (couleur de la peau, race, origine) mais également, selon les vêtements/attributs de la personne (religion, santé…). Peu de traces (la récupération de l'image de la démarche demande une grande logistique).
Avantages	Possibilité de reconnaître les personnes à distance.
Désavantages	Peu respectueuse de la sphère privée puisque la personne n'a pas forcément conscience d'être identifiée. L'identification prend beaucoup de temps puisqu'une image ne suffit pas, il faut une séquence qui permette de calculer les différentes mesures nécessaires à la comparaison.
Technique	La technologie est surtout utilisée par les sportifs et les médecins. Des techniques d'analyse d'images sont appliquées sur les séquences vidéo pour extraire les caractéristiques pertinentes d'une démarche.
Produits	Une simple caméra est nécessaire ainsi qu'un logiciel de traitement des images adéquat.
Tests	Aucun test effectué au laboratoire.

13. Frappe au clavier (frappologie)

Cette technique de reconnaissance biométrique est basée sur la dynamique des frappes sur le clavier. Chaque individu se distingue par le temps qu'il utilise pour appuyer sur une touche ainsi que le temps nécessaire pour passer d'une touche à la suivante. Le rythme de saisie est donc propre à chacun. Cette technique est intéressante car elle peut facilement être combinée avec la saisie d'un mot de passe par exemple. Elle remplace ainsi avantageusement l'authentification à deux facteurs.

Frappe au clavier	**Observations:**
Type	Biométrie comportementale. Très peu utilisée. Très peu invasive puisqu'elle ne nécessite pas de périphérique supplémentaire autre que le clavier. Pas d'informations sur les efforts à fournir pour berner un système.
Contexte	Applications nécessitant une authentification à deux facteurs, pour renforcer la sécurité du mot de passe. La dynamique de frappe est combinée à la saisie du mot de passe pour déterminer l'identité de l'utilisateur.
Protection données	Pas de risques liés à la protection des données. Pas de traces.
Avantages	Peu coûteuse puisque seul un logiciel est nécessaire, pas de matériel. Facile à mettre en œuvre pour une augmentation de la sécurité des systèmes conséquente. Pas de risques de perte (badge, carte…).
Désavantages	Dépendant du type de clavier (QWERTY, AZERTY…). Dépendant de conditions extérieures: le mot de passe devrait toujours être tapé de manière constante à travers le temps.
Technique	Lors de l'enrôlement, l'utilisateur tape en moyenne une dizaine de fois son mot de passe. Les temps d'appui et de changement moyens entre touches sont calculés pour créer un profil de référence. Le taux FAR est inférieur à 0.5% pour des mots de passe à 8 caractères.
Produits	La CNIL a autorisé une société à utiliser son logiciel à des fins de démonstration.
Tests	Pas de tests concluants effectués.

14. Conclusion

Chaque système de reconnaissance biométrique a ses qualités et ses défauts. D'un point de vue de protection des données, les caractéristiques qui respectent la sphère privée et évitent de laisser des traces derrière soi sont évidemment à privilégier. À cet égard, le réseau veineux et le visage 3D présentent un avantage certain. Toutefois, lors de l'installation d'un système biométrique, il y a d'autres facteurs à prendre en compte, tels que l'acceptabilité des utilisateurs et la sécurité de la technologie.