

# Authentification Biométrique



## Table des matières

Qu'est ce que l'Authentification Biométrique ?.....	2
Biométrie physique.....	2
Biométrie comportementale.....	2
Numérisation d'empreintes digitales.....	3
Avantages et inconvénients.....	3
Reconnaissance vocale.....	3
Avantages et inconvénients.....	4
Reconnaissance de l'Iris.....	4
Avantages et inconvénients.....	5
Reconnaissance faciale.....	5
Avantages et inconvénients.....	5
Reconnaissance de l'écriture manuscrite.....	6
Avantages et inconvénients.....	6

# Qu'est ce que l'Authentification Biométrique ?

L'authentification Biométrique est une méthode de sécurité pour accéder a des applications ou a d'autres ressource sur un réseau, basé sur les traits physiques, comportementaux ou encore biologique d'un individu. Les données biométriques sont des données à caractère personnel car elles permettent d'identifier une personne. Elles ont, pour la plupart, la particularité d'être uniques et permanentes (ADN, empreintes digitales, etc.).

Il existe deux types de systèmes biométriques:

- la biométrie physique
- la biométrie comportementale.

## ○ **Biométrie physique**

Grace a des dispositifs spéciaux ( scanners, capteurs, et autres... ), les données biométrique que le système enregistre sont directement envoyé dans une base de données où elles seront enregistré. Les informations que le système reçoit, les convertit en données numérique

Les caméras et enregistreurs vidéo modernes pour smartphones peuvent facilement reconnaître les visages à l'aide de capteurs intégrés alimentés par des réseaux de neurones. En ce sens, l'image devient l'identifiant d'une personne. Cette technologie peut être utilisée non seulement pour déverrouiller des téléphones, mais également pour des tâches plus complexes telles que la confirmation d'achats ou l'accès à des services financiers.

## ○ **Biométrie comportementale**

La biométrie comportementale est un système de reconnaissance qui identifie une personne en fonction de caractéristiques dynamiques ou comportementales. Ces caractéristiques peuvent inclure le dynamisme lors d'une écriture ou d'une signature, le rythme que notre voix ou notre parole peut avoir, la reconnaissance gestuelle, la vitesse de frappe sur un appareil électronique ou encore la façon dont une personne marche ou encore comment elle tient son téléphone.

## Numérisation d'empreintes digitales

La reconnaissance d'empreintes digitales est un type de biométrie physique. Pour cette méthode d'authentification, un scanner d'empreintes digitales est utilisé pour authentifier les données. nous pouvons simplement les diviser en trois types qui fonctionnent de trois manières différentes:

- convertir une empreinte digitale en code numérique avec un capteur optique,
- enregistrer la conversion à l'aide d'un capteur thermique linéaire
- convertir une empreinte digitale avec un capteur d'authentification capacitif

Au final, l'utilisateur aura juste besoin de placer son doigt devant le scanner ou à travers un capteur pour être authentifié



### Avantages et inconvénients

Avantages	Inconvénients
<ul style="list-style-type: none"><li>• Les empreintes digitales sont des identifiants uniques propres à l'individu</li></ul>	<ul style="list-style-type: none"><li>• Les blessures, temporaires ou permanentes, peuvent interférer avec les scans</li></ul>
<ul style="list-style-type: none"><li>• La plupart des gens connaissent cette méthode d'authentification</li></ul>	<ul style="list-style-type: none"><li>• C'est une technologie qui peut être contournée avec une réplique d'empreintes</li></ul>
<ul style="list-style-type: none"><li>• Les scanners d'empreintes digitales sont relativement bon marché</li></ul>	<ul style="list-style-type: none"><li>• Il peut être contourné en utilisant le doigt de quelqu'un d'autre.</li></ul>

## Reconnaissance vocale

La voix est une caractéristique aussi inhérente à chaque personne que ses empreintes digitales ou son visage. De plus, la reconnaissance vocale est très pratique pour les utilisateurs et nécessite un minimum d'effort de leur part.

La technologie d'authentification biométrique vocale est largement utilisée dans plusieurs domaines directement liés au traitement des voix des utilisateurs.

Cette technologie biométrique permet:

- Accélérer le service,
- Faciliter le travail des agents
- Aider à devenir plus efficaces.

Dans les grands projets, en particulier lorsque la nécessité de protéger les informations confidentielles est grande, l'identification vocale peut être appliquée avec une autre méthode d'authentification telle que la numérisation d'empreintes digitales.



## **Avantages et inconvénients**

Avantages	Inconvénients
<ul style="list-style-type: none"> <li>• La voix est une caractéristique unique qui est extrêmement difficile à falsifier</li> </ul>	<ul style="list-style-type: none"> <li>• Les endroits bruyants peuvent empêcher l'authentification réussie</li> </ul>
<ul style="list-style-type: none"> <li>• C'est une méthode largement utilisée et familière aux utilisateurs</li> </ul>	<ul style="list-style-type: none"> <li>• Une maladie respiratoire grave peut diminuer le taux de réussite de l'authentification</li> </ul>
<ul style="list-style-type: none"> <li>• Cela fait gagner du temps aux utilisateurs et aux agents</li> </ul>	<ul style="list-style-type: none"> <li>• Les utilisateurs peuvent ne pas comprendre comment leurs données sont stockées</li> </ul>

## **Reconnaissance de l'Iris**



La technologie de balayage de l'iris a été présentée en 1936 par l'ophtalmologiste Frank Bursch. En 1990, John Dufman d'Iridian Technologies a breveté un algorithme pour détecter les différences dans l'iris. A ce jour, c'est encore la méthode d'authentification biométrique la plus précise.

Cette technologie fonctionne de la façon suivante :

- La pupille est localisé, puis la détection des paupières et de l'iris
- Ensuite les parties inutiles ( paupières, etc ) sont supprimer pour laisser que l'iris
- Qui est pour finir convertie en valeurs numériques

## Avantages et inconvénients

Avantages	Inconvénients
<ul style="list-style-type: none"><li>• L'iris est un organe invariant avec un haut niveau d'aléatoire entre les individus</li></ul>	<ul style="list-style-type: none"><li>• Cette technologie est relativement nouvelle et nécessite encore des améliorations</li></ul>
<ul style="list-style-type: none"><li>• Pas besoin de mémoriser des mots de passe compliqués</li></ul>	<ul style="list-style-type: none"><li>• C'est une méthode qui nécessite une courte distance entre l'appareil et l'œil de l'utilisateur</li></ul>
<ul style="list-style-type: none"><li>• L'iris est un organe interne bien protégé contre les dommages par une membrane hautement transparente et sensible</li></ul>	<ul style="list-style-type: none"><li>• Dans des conditions de faible luminosité, les chances de reconnaissance de l'iris sont vraiment faibles</li></ul>

## Reconnaissance faciale

La reconnaissance faciale est la localisation automatique d'un visage humain dans une image ou une vidéo. Si nécessaire, la technologie de reconnaissance faciale peut être utilisée pour confirmer l'identité d'une personne sur la base des données disponibles.



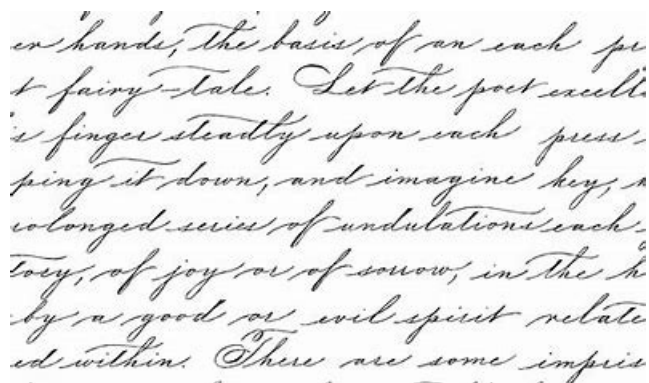
Une image du visage d'une personne stockée dans une base de données sous forme de code mathématique. L'intérêt pour cette technologie est élevé car cette méthode peut être appliquée en vidéoconférence.

## Avantages et inconvénients

Avantages	Inconvénients
<ul style="list-style-type: none"><li>• Nécessite peu d'interaction avec l'appareil</li></ul>	<ul style="list-style-type: none"><li>• Les changements de luminosité peuvent affecter les performances</li></ul>
<ul style="list-style-type: none"><li>• Pas besoin de mémoriser des mots de passe complexe</li></ul>	<ul style="list-style-type: none"><li>• Les expressions faciales peuvent modifier la perception</li></ul>
<ul style="list-style-type: none"><li>• Très efficace lorsqu'il est combiné avec d'autres méthodes biométrique</li></ul>	<ul style="list-style-type: none"><li>• L'utilisation d'accessoires faciaux peut rendre difficile la reconnaissance</li></ul>

# Reconnaissance de l'écriture manuscrite

La vérification dynamique de la signature peut être appliquée dans des domaines nécessitant une automatisation du flux de travail, tels que les systèmes bancaires ou judiciaires. La reconnaissance de signature est basée sur des algorithmes de reconnaissance de formes ou des méthodes mathématiques d'analyse de courbes, car un ensemble de points peut représenter une signature.



## Avantages et inconvénients

Avantages	Inconvénients
<ul style="list-style-type: none"><li>• Les signatures ont été utilisées pour confirmer les identités pendant des siècles</li></ul>	<ul style="list-style-type: none"><li>• Beaucoup de gens ont des signatures incohérentes</li></ul>
<ul style="list-style-type: none"><li>• La technologie ne nécessite pas d'appareils avancés pour fonctionner</li></ul>	<ul style="list-style-type: none"><li>• Des blessures comme des bras ou des doigts cassés peuvent rendre impossible l'utilisation de cette technologie</li></ul>
<ul style="list-style-type: none"><li>• C'est intuitif et naturel et ne nécessite pas beaucoup d'explications</li></ul>	<ul style="list-style-type: none"><li>• Cette méthode ne convient qu'aux opérations de sécurité de bas niveau</li></ul>