



uOttawa

Faculté de génie
Faculty of Engineering

PROJET 2 CSI 4506:

IDENTIFICATION PAR EMPREINTE DIGITALE

Souleymane Wilfried Sankara : #300100940

Maire Fabienne Sawadogo : #300101795

Les données biométriques sont utilisées depuis longtemps pour la reconnaissance et l'authentification des personnes en raison de leur universalité, leur unicité et leur disponibilité. Jusqu'à date, la nécessité d'identifier les personnes de manière fiable est devenu un problème majeur. Là où les moyens traditionnels (carte à puce, mot de passe...) ont montré leurs limites (falsification, perte...), la biométrie (analyse des caractéristiques biologiques d'un individu) et tente d'apporter une réponse. Les techniques biométriques sont divisées en deux catégories, à savoir les techniques physiologiques (empreintes digitales, ADN, visage, rétine, voix, , empreinte palmaire etc....) et comportementales (signature, attitude, démarche, etc.). L'empreinte digitale est le procédé le plus ancien et le plus abouti pour détecter l'identité humaine selon certaines propriétés qu'elle a telles que l'acceptabilité, l'individualité et l'immutabilité. Dans le cadre de notre recherche nous allons effectuer l'exploration complète de l'identification par empreinte digitale

I- Exploration de l'application

1- Mise en contexte

Depuis le XIXe siècle, l'analyse des empreintes digitales s'est imposée comme une méthode fiable d'identification des personnes. Les empreintes digitales font parties de données biométriques unique chez chaque individu sur la terre. Lorsqu'un doigt touche une substance solide, sa sécrétion est laissée sur la surface avec des motifs de crêtes caractéristiques appelés empreintes digitales.

2) Définitions

a) Empreinte digitale.

Une empreinte digitale est le motif caractéristique d'un doigt. Lorsqu'un doigt touche par exemple une substance solide, sa sécrétion est laissée sur la surface avec des motifs de crêtes caractéristiques appelés empreintes digitales. Les empreintes digitales ne se distinguent pas par leurs crêtes et leurs vallées, mais par les minuties, qui sont des points anormaux sur les crêtes. Les minuties constituent un motif universel, unique et permanent.

Chaque personne a ses propres empreintes digitales, dont l'unicité est permanente. Pour obtenir une image de l'empreinte d'un doigt, les avancées

technologiques ont permis d'automatiser la tâche au moyen de capteurs intégrés, remplaçant ainsi l'utilisation classique de l'encre et du papier.

b) Définition de l'application

Les systèmes de reconnaissance d'empreintes digitales fonctionnent en examinant un doigt pressé contre une surface lisse. Les crêtes et les vallées du doigt sont scannées à la recherche d'une série de points distincts où les crêtes et les vallées se terminent ou se rencontrent. Ces points sont appelés MUNITIES. Ces minuties sont les points que le système de reconnaissance des empreintes digitales utilise pour la comparaison. L'authentification par empreintes digitales fait référence à la procédure de sécurité qui implique l'utilisation des variations uniques sur les empreintes digitales appelée MUNITIES afin de vérifier que les personnes sont bien celles qu'elles prétendent être.

3) La place de l'application parmi d'autres applications ?

Les empreintes digitales font partie des données biométriques. Depuis toujours, les données biométriques sont utilisées pour l'authentification des hommes dû à leur caractère unique. L'empreinte digitale est le procédé le plus ancien pour détecter l'identité humaine. Un nouveau rapport de Prescient & Strategic Intelligence , prévoit que le marché mondial des capteurs d'empreintes digitales connaîtra une forte croissance de 13,6 % entre 2020 et 2030, stimulée par la demande de projets du secteur public et de l'électronique grand public. Comme pour la reconnaissance faciale, l'Asie-Pacifique devrait être la région avec le plus fort taux de croissance en ce qui concerne le domaine de l'identification par empreinte digitale.

On peut donc affirmer que le système d'identification automatique des empreintes digitales est une méthode efficace pour reconnaître l'identité humaine. L'authentification par empreinte digitale est alors utilisée dans plusieurs domaines et se retrouve parmi bien d'autres applications.

4) Qu'est-ce qui caractérise votre application? Pourquoi est-elle utile et pour qui?

La reconnaissance des empreintes digitales est désormais utilisée dans de nombreuses applications telles que:

L'authentification mobile : Les utilisateurs vérifient leur identité via la numérisation des empreintes digitales pour accéder à un appareil ou une application mobile.

Systèmes d'identité civile : Les Institutions gouvernementales utilisent la reconnaissance d'empreintes digitales pour vérifier les identités civiles pour le vote, la sécurité et les versements de prestations.

Contrôle d'accès physique : Utilisé par les entreprises et les employeurs Les employeurs et pour la gestion du temps, des présences et certains renseignements confidentiels.

Embarquement : Permet d'identifier les clients afin d'éviter la fraude et assurer la sécurité avant les laisser entrer dans un avion ou un bâtiment.

Gestion de l'identité : Les organisations utilisent la reconnaissance des empreintes digitales pour éviter les doublons ou les fausses identités.

II- Analyser votre application par rapport à la cognition humaine

Dans cette partie de notre analyse nous allons effectuer une analyse par rapport à la cognition humaine.

• Perception :

Pour observer les empreintes digitales dans le cadre de cette application, on utilise le sens du toucher. En effet, les scanners numériques capturent une image de l'empreinte digitale. Pour créer une empreinte digitale numérique, une personne place son doigt sur une surface de lecture optique ou en silicium et l'y maintient pendant quelques secondes. Le lecteur convertit les informations du scan en modèles de données numériques. Les entrées se présentent sous forme d'image en niveaux de gris, idéalement à une résolution de 500 ppi ou plus

• Attention :

L'application se focalise sur les points de minutie que comportent les empreintes digitales. Après la prise en photo de l'empreinte par un

capteur, elle est traitée pour réduire voire enlever toutes sortes de bruits qui s'y trouvent et mettre en évidence les points de minutie

- **Mémoire :**

L'enregistrement d'une empreinte digitale est un processus au cours duquel une empreinte digitale intacte est identifiée et stockée pour une utilisation ultérieure. L'empreinte digitale est scannée une ou plusieurs fois par un appareil spécialisé, puis numérisée. L'empreinte digitale numérisée est ensuite analysée pour vérifier sa validité. Si l'empreinte digitale est valide, elle est stockée dans une mémoire non volatile, comme une mémoire Flash ou EEPROM, avec les informations d'identification personnelle.

- **Apprentissage :**

Avant d'être statique, l'application apprend à travers de nombreux algorithmes à différencier les empreintes digitales soumises. Après qu'elle soit performant dans l'apprentissage, elle reste statique et effectue les mêmes tâches de reconnaissance

- **Processus de réflexion:**

Les grands points du processus de réflexion tels que comparer, rechercher sont impliqués dans l'application d'une façon ou d'une autre :

- la recherche dans le cadre d'une authentification par exemple ou l'on cherche dans la base de données des empreintes correspondante à celle que l'on a l'entrée.
- La comparaison dans le sens où les points de minuties sont comparée avec ceux d'une autre empreinte pour vérifier les points de similarités.

III- Exploration industrielle

L'identification par empreinte digitale est l'une des technologies biométriques les plus utilisées, et cela est dû sans doute à sa vitesse et à sa facilité d'utilisation.

1) Les clients et les domaines liées à l'application

De nos jours beaucoup d'entreprises sont intéressées par cette technologie et l'utilisent pour augmenter la qualité de leurs services ou de leurs produits. Parmi les clients de cette technologie nous avons :

- Les services de police et d'investigation : lorsqu'un crime ou un délit a lieu, il y a de nombreuses empreintes digitales qui sont laissées sur la scène de crime. Ainsi être capable d'identifier les personnes présentes sur la scène de crime à partir des empreintes digitales s'avère être un précieux atout.
- Les entreprises de téléphonie mobile et de fabrication d'ordinateurs : De nombreux fabricants de téléphone et d'ordinateur ont dernièrement ajouté la reconnaissance par empreinte digitale aux derniers modèles de leur produit. Cela est venu remplacer la méthode traditionnelle d'identification par mot de passe ou par code pin. Cette innovation à l'avantage d'être sécurisée (deux personnes ne peuvent avoir les mêmes empreintes digitales) et rapide. L'incorporation de cette technologie dans les téléphones portables a, par ricochet, touché d'autres domaines tels que la finance. Désormais, la reconnaissance d'empreinte digitale permet d'ouvrir les applications bancaires présentes sur les smartphones
- L'identification des citoyens par les gouvernements : Au niveau du gouvernement, de nombreux documents administratifs requiert maintenant des données biométriques et en l'occurrence des empreintes digitales. Ainsi, il y a des passeports qui contiennent des données des empreintes digitales et cela permet l'identification des personnes dans les aéroports.
- Des particuliers : L'utilisation de la reconnaissance par empreinte digitale n'est pas uniquement réservée aux entreprises ou aux services gouvernementaux, des personnes "lambda" peuvent aussi s'en procurer pour sécuriser leurs coffres forts où l'accès à des espaces qu'ils préfèrent garder privé.

De la liste des clients de cette technologie peuvent être dérivées ses domaines d'applications. Mais les domaines où la reconnaissance par empreinte digitale est la plus active sont surtout la cybersécurité, la criminologie et les investigations, et l'identification civile.

2)L'application est-elle mature pour être déployée dans le quotidien ?

La reconnaissance d'empreinte digitale est une technologie qui prend de plus en plus d'ampleur. Il est donc légitime de se demander si cette technologie peut être déployée dans notre quotidien. En réalité, elle a déjà été jugée assez mature pour qu'on puisse l'utiliser au quotidien. En effet, elle est déjà avec les smartphones et ordinateurs qui sont utilisés tous les jours par des milliers de personnes à travers le monde.

3)L'application est-elle davantage explorée par les start-ups ou les grandes entreprises ?

À la question de savoir si cette technologie est explorée par des start-up, la réponse est "oui". Au vu de l'impact et de l'utilité de cette technologie, il est donc normal que cette technologie soit étudiée et développée par des start-up. Les principales start-up impliquées dans le développement de cette technologie sont :

- Shenzhen Goodix (Chine)
- Fingerprint Cards AB (Suède)
- Synaptics (US)
- Apple Inc. (US)
- Egis Technology Inc. (Taiwan)
- Crucialtec (Corée du Sud)
- Qualcomm (US)

Il y a évidemment d'autres entreprises qui ne peuvent être toutes mentionnées mais une chose est sûre, c'est que la concurrence est rude.

L'un des aspects du marché par lequel les concurrents se distinguent se trouve dans la technologie utilisée pour la reconnaissance par empreinte digitale. Il y a la technologie de reconnaissance d'empreinte avec capteur 2D qui est la plus répandue à cause de son faible coût et parce qu'elle excelle dans la détection. Elle est surtout utilisée pour les téléphones portables. Il y a également la

technologie avec capteur 3D qui est utilisée dans pour les contrôles d'accès et d'autres domaines sensibles.

Un autre aspect du marché qui distingue les concurrents se trouve au niveau de l'utilisation de la technologie. Certains fabricants comme Synaptics se focalisent beaucoup plus sur la reconnaissance par empreinte digitale au niveau des smartphones et des ordinateurs tandis que Qualcomm fournit la technologie à capteur 3D pour les contrôles d'accès.

IV- Effectuer une exploration historique

C'est dans les années 1800 que le concept de reconnaissance par empreinte digitale est né d'une nécessité d'identifier les personnes dans plusieurs domaines courants de la vie. En 1877, le Britannique William James Herschel utilise les empreintes digitales pour éviter que les bénéficiaires de pension de l'armée ne la touchent plusieurs fois. À cette époque, elles servent aussi à identifier les marchands locaux qui refusent de remplir les termes de leurs contrats : Herschel fait apposer leurs empreintes digitales sur ces contrats. En 1888, l'anthropologue anglais Francis Galton introduit la notion de minuties pour réaliser la comparaison d'empreintes digitales (fingerprint matching en anglais). Quatre ans plus tard, Galton publie son ouvrage où il propose une classification rigoureuse des empreintes digitales et démontre qu'il y a seulement une chance sur 64 milliards que deux individus aient une même empreinte. Cet arrangement particulier des lignes papillaires forme des points caractéristiques, nommés minuties qui sont à l'origine de l'individualité des dessins digitaux . A ce jour, on considère qu'il faut 8 à 17 de points de minuties similaires pour qu'on estime avoir établi l'identification. Un chiffre inférieur au seuil minimum aboutit à l'exclusion de l'empreinte digitale comme élément de preuve. L'application a explosé au XXe siècle l'orsqu'une empreinte digitale, nettement visible sur la peinture fraîche, permet d'identifier Thomas Jennings pour une affaire de meurtre aux États-Uni. En France, c'est à partir d'octobre 1902, que les empreintes digitales sont devenues l'une des principales preuves lors des enquêtes policières. Les autorités ont alors cerné l'importance de se pencher sur ce sujet pour en faire une étude plus profonde.

Notons que l'anthropométrie (technique qui concerne la mesure des particularités dimensionnelles d'un être humain, en particulier l'empreinte digitale dans notre cas) a été le premier système scientifique utilisé par la police pour identifier les criminels. Avant cette époque, les criminels ne pouvaient être identifiés que par

leur nom ou leur photographie. Cette méthode a finalement été supplantée par les empreintes digitales.

La criminologie a donc été le premier domaine à se servir de l'identification par empreinte digitale, mais cette identification se faisait de façon traditionnelle depuis les années 1900 à l'œil nue et souvent assistée d'une loupe. C'est dans les années 2000 que cette méthode d'identification est devenue commerciale et n'a plus été réservée aux services gouvernementaux. En 2013, Apple inclut l'application dans le système de déverrouillage de ses iPhone, lançant ainsi une grande nouvelle tendance chez la plupart des fabricants de téléphone. De nos jours, la plupart des téléphones sont munis d'un système d'identification par empreinte digitale.

VI- Effectuer une exploration technologique

L'identification par empreinte digitale sollicite de nombreuses technologies au niveau de l'apprentissage machine et au niveau de la collecte de données.

Parmi les technologies que nous avons explorées durant le cours il y a notamment l'utilisation du réseau de neurone et le vecteur à support de machine (SVM plus couramment) qui interviennent dans le processus d'identification par empreinte digitale.

Les systèmes d'identification par empreinte digitale peuvent fonctionner différemment dépendamment de chaque système. Mais tous les systèmes suivent une structure similaire à la figure suivante :

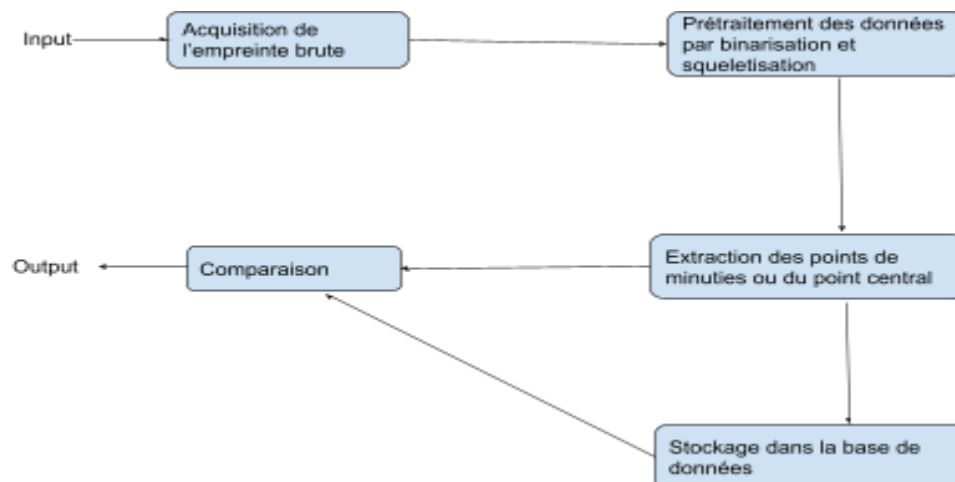


Figure 1

1) Acquisition de l'empreinte brute

Les empreintes peuvent être récoltées de plusieurs façons dépendamment de l'algorithme utilisé. Il s'agit de capturer les images numériques d'empreintes et à trouver les lignes tracées par les crêtes et les vallées. La qualité d'image de l'empreinte digitale peut varier selon plusieurs facteurs comme la propreté de la peau du doigt, l'humidité du milieu, la pression. Un bon système biométrique tiendra compte de ces facteurs. Les procédés utilisés vont alors varier en fonction des facteurs mentionnés ci-dessus. La manière la plus simple est la photographie. Les empreintes sont photographiées en haute résolution avec une échelle de mesure médico-légale. La qualité des images peut être ensuite améliorée en utilisant des sources lumineuses pales ou alternatives et certains produits chimiques.

Une autre méthode pour recueillir des empreintes digitales latentes consiste à saupoudrer une surface lisse ou non poreuse de poudre pour empreintes digitales. Si des empreintes apparaissent, elles sont photographiées, puis décollées de la surface avec du ruban adhésif transparent. Le ruban adhésif est ensuite placé sur une carte de levage latent pour préserver l'empreinte.

Enfin la méthode optique qui est une dérivation de la méthode de prise en photo normale. Elle utilise un appareil-photo CCD (Dispositif Chargé Couplé) au cœur du capteur optique. En général, le doigt est placé sur une surface en verre et l'appareil-photo CCD prend la photo. Le système CCD contient une rangée de LED qui illumine les creux et les bosses du doigt.

Les images obtenues sont ensuite prétraitées pour faciliter l'extraction des données importantes. Les algorithmes de reconnaissance des empreintes digitales sont sensibles à la qualité des images obtenue lors du prélèvement de l'empreinte. La qualité de ces images dépend de plusieurs facteurs tels que:

- La personne (âge, métiers manuels,...)
- Les substances parasites présentes sur le doigt (saletés, graisse,...)
- L'environnement où se produit l'acquisition (éclairage, degré d'humidité....)
- Les caractéristiques spécifiques du moyen d'acquisition utilisé.
- La profondeur de rides/vallée, etc.

L'étape de prétraitement est nécessaire avant d'effectuer les étapes suivantes car elle permet un meilleur rendement des algorithmes. Typiquement le

prétraitement peut se composer de lissage, segmentation et filtrage. Les empreintes ainsi obtenues sont enregistrées dans une base de données à des fins d'identification ou de comparaison.

2) Prétraitement des données

Lorsque l'image de l'empreinte digitale est recueillie, elle est contenue des parties de couleur grise et des parties de couleur blanche. La binarisation consiste à rendre les pixels de l'image dont le niveau de gris est en dessous d'un certain seuil noir et ceux au dessus blancs. Le but de la binarisation est de repérer les crêtes. Il existe des méthodes de binarisation qui déterminent le seuil en se basant sur le niveau de distribution de gris sur l'image.

La squelettisation est l'étape consistant à transformer l'empreinte en un ensemble de courbes. En effet la squelettisation amincit les crêtes en un seul pixel pour faciliter la détection des minuties.

3) L'extraction des minuties

Cette étape consiste à extraire dans l'image des composants qui permettent de rendre une empreinte unique et à leur affecter des coordonnées permettant de les localiser. Ces éléments sont généralement des bifurcations, des fins de lignes etc... La figure suivante montre les différents points de minutie sur une empreinte digitale.

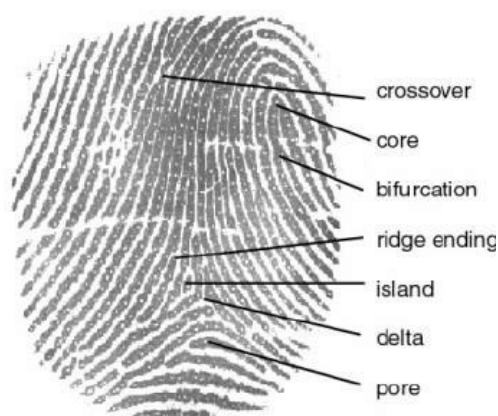


Figure 2

La figure suivante résume les étapes 2 et 3.

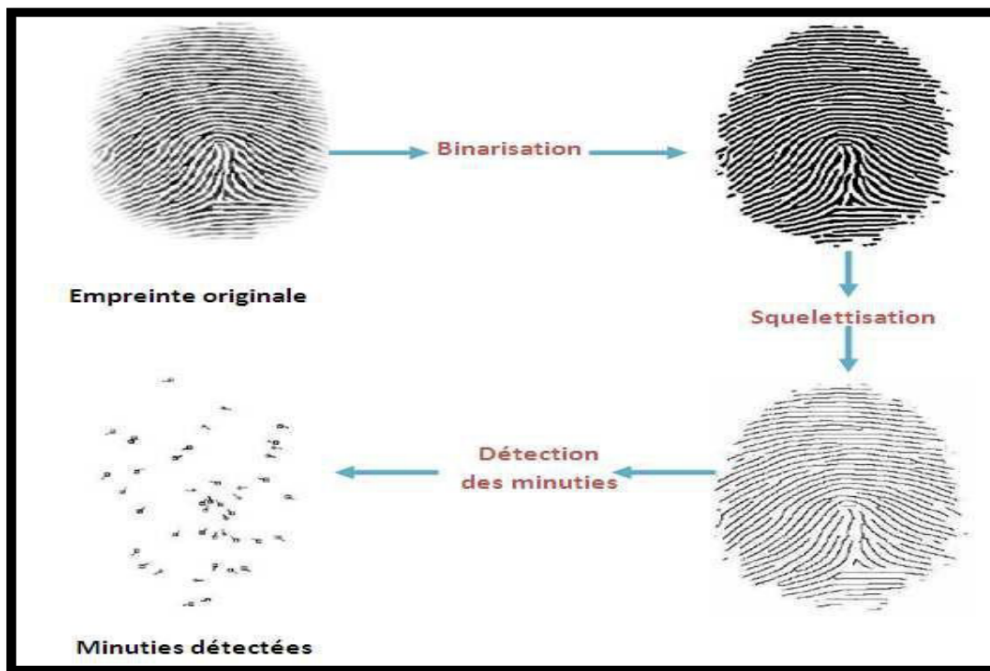


Figure 3

4) Stockage dans la base de données ou comparaison

La dernière étape consiste à stocker les données collectées dans une base de données si le but est d'enregistrer les empreintes pour les utiliser plus tard ou de comparer les données de l'empreinte digitale prise avec les empreintes déjà enregistrées dans la base de données.

Durant la phase de comparaison, différents algorithmes peuvent être utilisés pour vérifier la similarité de l'empreinte digitale avec une des empreintes déjà présente dans la base de données. C'est là qu'interviennent les algorithmes à réseau de neurones ou de machine à support de vecteur (SVM).

Parmi les algorithmes de reconnaissance d'empreinte digitale il y a :

a) La comparaison des minutes.

Dans chaque empreinte digitale il y a des points spéciaux qui permettent de différencier une empreinte digitale d'une autre et ces points sont appelés des minuties. (Voir figure 2)

En affectant des coordonnées à chaque minute dans une paire d'empreintes digitales F1 et F2, il suffit maintenant d'appliquer des formules mathématiques de calcul de distance. Si le calcul des distances est inférieur à un certain seuil, les minuties peuvent être considérées égales. Si le nombre de minuties jugés similaire est supérieur à un certain nombre (deux empreintes différentes ne peuvent pas avoir plus de 7 points de minutie similaires), les empreintes sont dites identiques.

D'un point de vue mathématique, les coordonnées en question sont représentées en

(x, y, Θ) où (x, y) représente les coordonnées du point de minutie et Θ représente la direction du point. Les deux types de distances calculées sont sd et dd et avec les conditions que ces deux distances soient inférieures à un certain nombre r_0 et θ_0 respectivement.

$$sd(m'_j, m_i) = \sqrt{(x'_j - x_i)^2 + (y'_j - y_i)^2} \leq r_0$$

$$dd(m'_j, m_i) = \min(|\theta'_j - \theta_i|, 360 - |\theta'_j - \theta_i|) \leq \theta_0$$

b) Réseau de neurone probabiliste

Cet algorithme procède en deux (02) étapes : l'étape de prétraitement et l'étape de décision. L'étape de prétraitement compare les images de deux empreintes et extrait le point central de chacune des deux empreintes. Ces deux points centraux sont ensuite envoyés à l'étape de décision qui représente à proprement dit le réseau de neurones et qui a été entraîné. L'étape de décision implémente une approche probabiliste Bayésien pour estimer la probabilité de correspondance. Le réseau est formé en utilisant la méthode de descente de gradient. La probabilité se situe entre 0 et 1.

Beaucoup de ces technologies utilisées pour l'identification des empreintes digitales sont open source. Il y a également des ensembles de données qui sont disponibles sur des plateformes comme Kaggle.

VII - Effectuer votre exploration de recherche

Les systèmes d'identification par empreinte digitale sont un sujet passionnant et suscite un centre d'intérêt dans le monde universitaire. En effet, nombreux sont des étudiants qui décident de rédiger leur mémoire de fin de cycle sur ce sujet. Voici quelques exemples de thèmes explorés par des étudiants :

- Etude d'un système complet de reconnaissance d'empreintes digitales pour un capteur microsystème à balayage (étudié par un étudiant de l'université de Grenoble en France)
- Identification rapide d'empreintes digitales, robuste à la dissimulation d'identité (Université de Caen en France)
- Identification biométrique par fusion multimodale de l'empreinte d'articulation, l'empreinte digitale et l'empreinte veineuse du doigt (Université des Sciences et de la Technologie d'Oran Mohamed Boudia en Algérie)

L'application est aussi sujet à des recherches et l'une de ces recherches est l'identification par empreinte digitale sans contact. L'identification par empreinte digitale sans contact est une application qui a fait l'objet de plusieurs études ces dernières années. La figure suivante montre le nombre de publications à ce sujet par an.

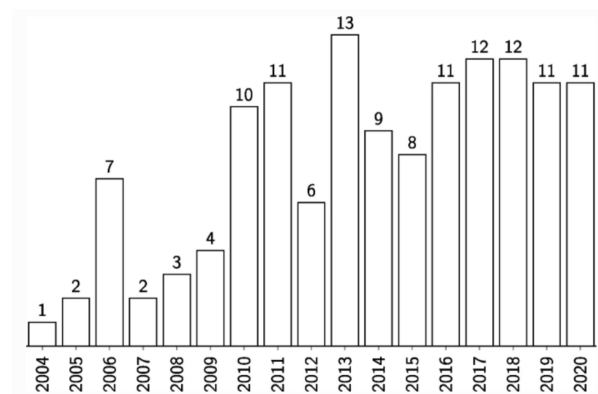


Figure 4

Le principe derrière cette application est de résoudre les contraintes liées à l'humidité, les cicatrices et autres aspects qui peuvent altérer la capture de

l'empreinte digitale par des capteurs. La figure 5 nous montre une empreinte digitale collectée par des capteurs et une empreinte digitale collectée sans contact.

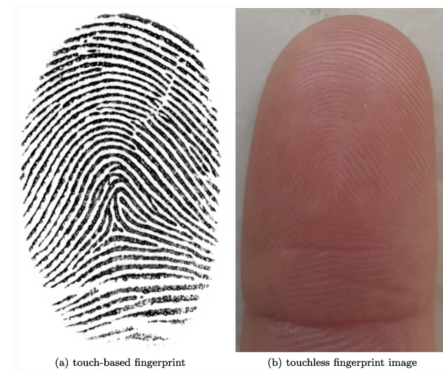


Figure 5

Le procédé d'identification par empreinte digitale demande un prétraitement supplémentaire pour extraire les données utiles à l'identification. L'acquisition des données se fait donc en plusieurs étapes.

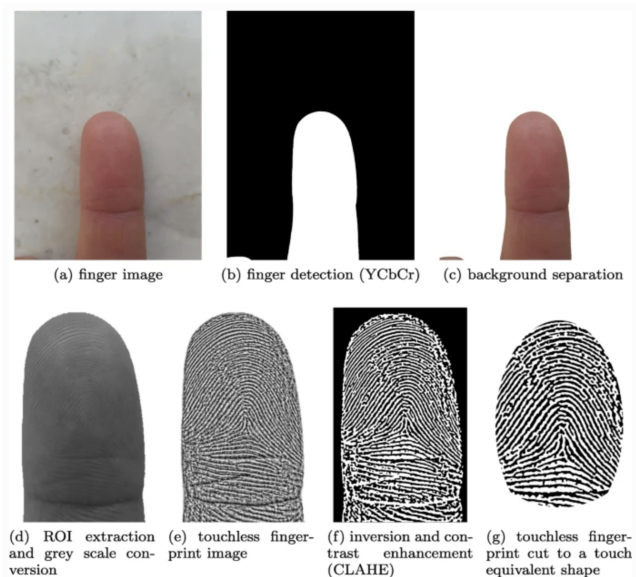


Figure 6

De nos jours, ce procédé fait face à de nombreux défis et ne montre pas encore des taux de réussite satisfaisants pour être déployé. Ces défis sont notamment liés à l'environnement : l'arrière-plan, les impuretés, l'éclairage, la position du doigt etc...

Références

<https://caiac.pubpub.org/pub/xvxo43ge/release/1>

<https://skyquestt.com/speak-with-analyst/fingerprint-sensor-market>

<https://www.globenewswire.com/news-release/2022/10/19/2537598/0/en/Global-Fingerprint-Sensor-Market-Sales-Revenue-to-Surpass-6-45-Billion-by-2028-Synaptics-to-Enjoy-Higher-Market-Share.html>

<https://www.rootstrap.com/blog/fingerprint-recognition-the-most-popular-biometric/>

<https://www.interpol.int/How-we-work/Forensics/Fingerprints>

<https://www.scirp.org/journal/paperinformation.aspx?paperid=66930#f1>

<http://cs229.stanford.edu/proj2016/report/Xu-FingerprintIdentificationUsingSVM-report.pdf>

http://www.univ-usto.dz/theses_en_ligne/doc_num.php?explnum_id=2059

<https://www.androidauthority.com/how-fingerprint-scanners-work-670934/>

https://www.researchgate.net/figure/Minutiae-points-on-a-fingerprint_fig2_41890634

https://www.researchgate.net/publication/310953762_Overview_of_Fingerprint_Recognition_System

<http://dspace.univ-eloued.dz/handle/123456789/1358>

https://fr.wikipedia.org/wiki/Syst%C3%A8me_d%27identification_automatique_par_empreintes_digitales

<https://bioconnect.com/2021/12/08/a-brief-history-of-biometrics/>

<https://theses.hal.science/tel-00009742>

<https://www.theses.fr/2020NORMC231>

http://www.univ-usto.dz/theses_en_ligne/doc_num.php?explnum_id=1547

<https://jivp-urasipjournals.springeropen.com/articles/10.1186/s13640-021-00548-4>

<https://link.springer.com/book/10.1007/978-981-15-4128-5>
<https://www.webology.org/abstract.php?id=735>