

# Exposé sur la technologie d'empreinte digitale<sup>1</sup>

Gerik Alexander von Graevenitz

Bergdata Biometrics GmbH, Bonn, Germany

[gerik@graevenitz.de](mailto:gerik@graevenitz.de)

## La biométrie

La biométrie se réfère à l'identification automatique d'une personne vivante grâce à ses caractéristiques physiologiques ou comportementales. Il existe différents types de technologies biométriques sur le marché: la reconnaissance faciale, la reconnaissance d'empreinte digitale, l'identification de la géométrie des doigts et de la main, l'identification de l'iris, l'identification de veine, l'identification de la voix et l'identification de la signature.

La méthode d'identification biométrique est préférée aux méthodes traditionnelles, impliquant des mots de passe et des codes PIN, pour différentes raisons:

La personne à identifier doit être physiquement présente au point d'identification. La reconnaissance, basée sur des techniques biométriques, évite ainsi la nécessité de se rappeler d'un mot de passe, de se servir d'un badge de proximité ou d'une carte de proximité (carte sans contact).

L'augmentation rapide de l'utilisation des mots de passe et des codes PIN, due à la révolution des technologies de l'information, amène à devoir limiter l'accès aux données confidentielles et personnelles. En remplaçant les codes PIN et les mots de passe, les techniques biométriques sont plus commodes pour l'utilisateur et peuvent potentiellement empêcher l'accès non autorisé ou l'utilisation frauduleuse de distributeurs de billets, de systèmes de gestion des horaires, de téléphones portables, de cartes à puce, de postes de travail et de réseaux informatiques. Les codes PIN et les mots de passe peuvent être oubliés, ainsi que les autres méthodes d'identification, comme les passeports, les permis du conduire et les cartes d'assurance, pouvant être aussi volés ou perdus.

---

<sup>1</sup> publiée avec le titre «Sensing Fingerprints » dans A&S International, Volume 52, Taipei, 2003, pp. 102-104

Différents types de systèmes biométriques sont utilisés pour la reconnaissance en temps réel; les plus populaires sont basés sur la reconnaissance faciale et de l'empreinte digitale. Cependant, d'autres systèmes biométriques utilisent l'iris et la rétine, la voix, le visage, et la géométrie de la main.

### **Les technologies d'identification d'empreinte digitale**

La reconnaissance d'empreinte digitale représente la méthode la plus ancienne d'identification biométrique. Son histoire remonte au moins à 6000 Av. JC. L'utilisation des empreintes digitales en tant que code personnel a une longue tradition et été déjà employée par les Assyriens, les Babyloniens, les Chinois et les Japonais. Depuis 1897, la dactyloscopie (synonyme de l'identification par l'empreinte digitale sans aide d'un ordinateur) est utilisée pour l'identification criminelle. Une empreinte digitale se compose de creux (lignes au travers de l'empreinte) et de bosses (espaces entre les creux). Le modèle de creux et de bosses est unique pour chaque individu.

Il y a deux méthodes principales de comparaison d'empreinte : la comparaison Minutiae et la comparaison de modèle global. La première approche analyse les bifurcations des creux et les terminaisons, la deuxième méthode s'attache à une approche plus macroscopique. Cette dernière approche considère l'ensemble des creux en termes de, par exemple, de cambrures, de boucles et de spirales. Le taux d'erreur étant bas, l'identification d'empreinte digitale est, de ce fait, très précise. Le prix de tels systèmes, comparé à d'autres systèmes biométriques, reste bon marché et les utilisateurs les apprécient fortement. Le point fort de l'identification par empreinte digitale est qu'elle peut être utilisée dans des environnements très divers. C'est une technologie prouvée et le fait de pouvoir utiliser différents doigts permet d'augmenter considérablement l'exactitude du système ainsi que sa flexibilité.

### **Les capteurs optiques d'empreinte**

La méthode optique est une des méthodes les plus communes. Un appareil-photo CCD (dispositif couplé chargé) est utilisé au cœur du capteur optique. Un appareil-photo CCD se compose simplement d'une rangée de diodes sensibles légères appelées photosites. En général, le doigt est placé sur



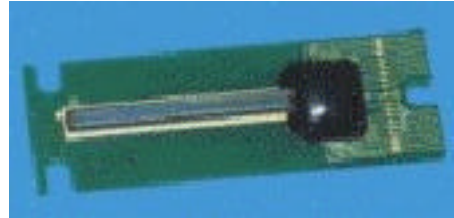
**DELSY CMOS-Sensor**

une surface en verre et l'appareil-photo CCD prend la photo. Le système CCD contient une rangée de LED (diodes électroluminescentes) qui illumine les creux et les bosses du doigt. Un prix avantageux constitue l'avantage principal des systèmes optiques ; leur inconvénient est qu'il sont faciles à détourner. L'autre

problème est celui des empreintes latentes : l'empreinte digitale du doigt précédent, qui a été placée sur le capteur, peut rester. Les principaux fabricants de capteurs optiques sont Delsy, Dermalog, Smiths Heimann Biometrics.

### **Les capteurs électriques-thermique**

La méthode électrique-thermique est moins habituelle. Actuellement, le seul capteur thermique est le FingerChip® fabriqué par Atmel.



**Atmel FingerCHIP™**

La méthode unique du FingerChip®, pour reconnaître l'empreinte, consiste à faire glisser le doigt le long du capteur. Les images successives ainsi capturées sont analysées par un logiciel spécial qui reconstruit l'image de l'empreinte digitale. Cette méthode permet au FingerChip® de renvoyer une haute qualité, 500 dpi et 256 niveaux de gris.

Le capteur mesure le différentiel de température entre les creux de la peau et l'air capturé dans les bosses de l'empreinte digitale. Cette méthode donne une image d'excellente qualité même sur des empreintes de qualité médiocre telles que celles provenant de doigt secs avec peu de profondeur entre les creux et les bosses. La technologie thermique fonctionne également dans des conditions environnementales difficiles, comme lors de températures extrêmes, de taux d'humidité ou de poussière élevé, ou de contamination d'eau.

Cette méthode a également l'avantage de nettoyer le capteur, évitant ainsi que les empreintes digitales restent après le passage de chaque personne. En effet, les empreintes latentes peuvent poser des problèmes de lecture à chaque passage mais peuvent aussi être copiées et utilisées pour parvenir aux accès contrôlés. En fait, cette méthode, s'appuyant sur la technologie thermique, permet au FingerChip® d'être un des plus résistant par rapport aux autres technologies. Le FingerChip® fonctionne aussi dans des environnements où la température peut être basse et le taux d'humidité élevé.

L'avantage de cette technologie est donc la possibilité d'avoir une image bonne qualité et un capteur toujours propre. L'inconvénient est que la qualité de l'image dépend des compétences de l'utilisateur à savoir manipuler le capteur. Le deuxième inconvénient est le chauffage du capteur qui augmente la consommation électrique. La chaleur du capteur est nécessaire afin d'éviter un équilibre thermique entre le capteur et la surface du doigt.

## Capteurs capacitifs

La méthode capacitive est une des méthodes les plus populaires. Comme les autres capteurs, le capteur capacitif d'empreinte digitale reproduit l'image des creux et des bosses qui composent une empreinte digitale. Le capteur capacitif emploie des condensateurs de mesure pour mesurer l'empreinte digitale. Un capteur capacitif se compose d'une rangée de cellules minuscules. Chaque cellule inclut deux plaques conductrices recouvertes par un revêtement protecteur.



**Veridicom 5th sense™**



**Infineon FingerTIP™**

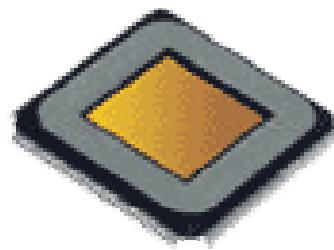
courant électrique pour

L'avantage principal des capteurs capacitifs est qu'ils demandent une réelle empreinte digitale. Mais ils rencontrent des difficultés avec les doigts secs et humides. Des doigts humides rendent l'images noire, tandis que des doigts secs la rendent pâle.

Les principaux fabricants de capteurs capacitifs sont Infineon, Veridicom, Sony et ST Microelectronics.

## Capteurs de champ-électrique

Le capteur de champ-électrique fonctionne avec un champ-électrique et le mesure au delà de la couche extérieure de la peau où l'empreinte digitale commence. La technologie de champ-électrique peut être utilisée dans des conditions extrêmes, c'est-à-dire même si le doigt est sale ou sec.



**Authentec AES4000**

La technologie de champ-électrique crée un champ entre le doigt et le semi-conducteur adjacent qui imite la forme des creux et des bosses de la couche épidermique du doigt. Un amplificateur de sous-Pixel est utilisé pour mesurer les signaux. Les capteurs fonctionnent ensemble afin de rendre une image plus claire correspondant exactement au modèle de l'empreinte digitale. On parvient ainsi à une image plus claire que ce que peuvent donner les technologies optiques ou capacitives. Cela permet à la technologie de champ-électrique d'obtenir des images d'empreinte digitale que d'autres technologies ne parviendraient pas à avoir.

Dans la technologie de champ-électrique, les rangées d'antenne mesurent la surface de la peau en générant et en détectant les formes linéaires géométriques. La couche vivante des cellules de la peau commence sous la surface de la peau..

Cela est contraire aux géométries sphériques ou tubulaires de champ produits par le capteur capacitif simple, qui lit seulement la surface supérieure de la peau. En conséquence, des doigts, qui seraient difficiles ou impossibles à scanner par des capteurs capacitifs, le seraient avec succès grâce à la technologie de champ-électrique.



**Authentec  
AES2500**

Dans les prochains mois, une version de la technologie de champ-électrique mettra sur le marché un nouveau capteur dont la capture de l'image se fera par balayage du doigt sur le capteur.

L'inconvénient est la basse résolution d'images et une trop petite zone d'image, ce qui a pour conséquence de générer un haut taux d'erreur (EER = Equal-Error-Rate).

### **Le capteur de pression**

Le principe du capteur de pression réside dans le fait que lorsqu'un doigt est placé au-dessus de la zone du capteur, seules les bosses de l'empreinte digitale rentrent en contact avec les rayons piezo du capteur. Les creux en contraste n'ont aucun contact avec les cellules du capteur. Une des différences fondamentales pour la reconnaissance et la comparaison d'empreinte digitale, par rapport aux capteurs sur le marché,



**BMF BLP100-Sensor**

demeure le capteur de pression qui génère une image binaire de 1-bit. Une image de 1-bit contient moins d'information qu'une image de niveau de gris de 8-bit.

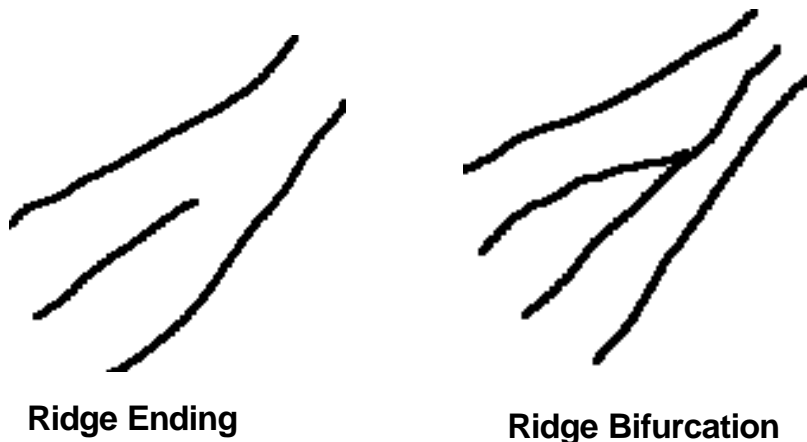
Un capteur de pression est capable d'enregistrer des doigts aussi bien humides que secs. De plus, sa large zone d'enregistrement permet de scanner complètement l'empreinte digitale ce qui amène à un faible taux d'erreur (EER = Equal-Error-Rate).

## **Le capteur sans contact**

Le capteur sans contact fonctionne comme un capteur optique. En général, il y a une glace optique de précision à une distance de 5 à 7 cm de l'empreinte digitale lorsque le doigt est scanné. L'empreinte digitale est mise sur un support avec une ouverture. Un des inconvénients à considérer est que la poussière et la saleté peuvent se déposer sur la vitre optique, donnant un mauvais résultat d'image. D'autre part, les empreintes digitales scannées sont sphériques ce qui amène à des algorithmes de comparaison plus complexes.

## **La reconnaissance de l'empreinte digitale**

L'identification par reconnaissance d'empreinte digitale peut être classée en deux catégories : la comparaison Minutiae (analyse de la structure locale) et la comparaison de modèle global (analyse de la structure globale). Actuellement, l'identification d'empreinte digitale assistée par ordinateur emploie la comparaison Minutiae. Les points de minuties sont des creux locaux qui apparaissent en tant que terminaison ou bifurcation.



La spécificité d'une empreinte digitale peut être déterminée à partir des creux et bosses dont l'empreinte digitale est faite. Une empreinte digitale complète se compose d'environ 100 points de minuties. La zone d'empreinte extraite se compose d'environ 30 à 60 points de minuties selon le doigt et la zone du capteur.

Ces points de minuties sont représentés par un nuage de points dans un système coordonné. Ils sont stockés ainsi que les valeurs des angles des tangentes de ces points de minuties dans un code d'empreinte ou directement dans une empreinte

de référence. Une empreinte peut se composer de plus d'un code d'empreinte pour augmenter la quantité de l'information et pour augmenter la zone de balayage de l'empreinte digitale enregistrée. En général, ceci mène à une qualité plus élevée d'empreinte et donc à une valeur plus élevée de similitude entre l'empreinte et l'échantillon.

Les tailles d'empreinte varient entre 100 octets et 1500 octets selon l'algorithme et la qualité de l'empreinte digitale. Néanmoins, certaines empreintes digitales n'ont pas de points de minuties ce qui amène à un échec d'enregistrement (FER = Failure to Enroll Rate). Mais cette situation est rare. Il est également difficile d'extraire les points de minuties quand l'empreinte digitale est de mauvaise qualité.

## **Conclusion**

Opter pour une technologie biométrique, soit un capteur d'empreinte digitale, semble ne pas être évident. Chaque technologie de capteur possède ses avantages et ses inconvénients. De ce fait, il apparaît comme impossible de faire des recommandations d'ordre général pour une technologie spécifique. Le choix du capteur d'empreinte digitale dépend de la technologie biométrique que le client souhaite mettre en place. Tout dépend fortement de l'environnement. Le taux d'erreur (EER = Equal-Error-Rate) dépend de l'ensemble joué par les algorithmes et le capteur d'empreinte digitale.