télécom saint-étienne
école d'ingénieurs nouvelles technologies

Les dispositifs optiques de reconnaissance d'empreintes digitales

Eva MATURANA
Alexandre NOBLET

Tuteur enseignant :
Nicolas CRESPO-MONTEIRO

École affiliée IMT
UNIVERSITÉ DE LYON
UNIVERSITÉ JEAN MONNET SAINT-ÉTIENNE

Table des matières

1 - Introduction

1-1. Contexte historique

La première utilisation des empreintes digitales remonte à l'ancienne Egypte (-3000 avant JC) et elles permettaient d'authentifier les documents. Evidemment, ce n'était que les prémices et rien ne permettait à l'époque d'attribuer avec certitudes quelle empreinte était à qui. Ainsi, des milliers d'années après, les hommes de sciences se sont à leur tour intéressés à ces empreintes. En 1858, William Herschel étudie la singularité des empreintes digitales et découvre qu'il est possible de différencier celles de chaque individu notamment avec la présence de vallées et de crêtes. Avec le temps, de plus en en plus de scientifiques s'y intéressent et la première révolution dans le domaine ne tardera pas à venir avec la résolution du 1er crime dans le monde avec une empreinte digitale en 1892. Inspiré par cette réussite, les pays occidentaux ne tarderont pas à suivre la tendance et à utiliser les empreintes digitales comme preuve dans les dossiers judiciaires. C'est alors qu'une nouvelle étape est franchie en France en 1987 avec la création du fichier automatisé des empreintes digitales dans le but de classer les malfaiteurs et les identifier plus facilement en cas de récidive. Plus d'un siècle plus tard, c'est l'arrivée du premier smartphone qui va révolutionner le domaine. Et si les empreintes digitales devenaient un moyen pratique de protéger nos biens, en l'occurrence ici son smartphone? En effet, il suffirait ainsi à un utilisateur de poser son doigt sur le capteur pour déverrouiller le smartphone. Depuis lors, les différents constructeurs ont créé innovations sur innovations pour rendre le dispositif plus efficace, plus rapide et plus sécurisé. Aujourd'hui, la quasi-totalité des smartphones (à l'exception des IPhones qui misent davantage sur la reconnaissance faciale 3D) utilisent l'empreinte digitale comme moyen d'authentification.

1-2. Support de notre projet

Pour structurer au mieux notre étude et s'appuyer sur quelque chose de concret, nous avons décidé d'utiliser les smartphones comme support principal. En effet, ces derniers ont une place importante dans notre quotidien et la quasi-totalité de la population en possède un. Ainsi, nous nous intéresserons surtout aux dispositifs de reconnaissance d'empreintes digitales au sein de ces derniers.

1-3. Fonctionnement général

D'une manière générale, la reconnaissance d'une empreinte digitale au sein d'un smartphone se passe globalement de la même manière selon les étapes suivantes :

1) L'utilisateur pose son doigt sur le dispositif de reconnaissance.
2) Le capteur reçoit une image et la représente sous forme d'un signal analogique.
3) Le signal analogique est converti en un signal numérique pour être envoyé au processeur.
4) Le processeur compare l'image reçue avec les empreintes digitales stockées en mémoire.
5) Le smartphone de l'utilisateur se déverrouille (ou non).

Malgré cette structure universelle au sein des smartphones, nous pouvons tout de même constater une différence au niveau de l'étape 2 et plus précisément au niveau du mot « capteur ». Par définition, un capteur est « un dispositif transformant l'état d'une grandeur physique observée en une grandeur utilisable, telle qu'une tension électrique » (1). Or, c'est dans l'expression « grandeur physique observée » que se niche la différence. En effet, il existe plusieurs types de capteurs pouvant être utilisés dans la reconnaissance d'une empreinte digitale : les capteurs optiques, les capteurs thermiques, les capteurs ultrasoniques et les capteurs capacitifs.

1-4. Les différents types de dispositifs de reconnaissance d'empreintes digitales

1-4-1. Les dispositifs capacitifs

Les dispositifs capacitifs sont à l'heure actuelle les systèmes les plus aboutis sur les smartphones. Ces-derniers sont fiables et admettent un très faible taux de rejet. Pour le moment, ces-derniers ne sont utilisés que sur les boutons physique (et non sous l'écran) d'un smartphone comme le bouton d'allumage. Il en existe deux types : ceux qui utilisent une seule électrode par pixel et ceux qui en utilisent deux.

Le doigt est un milieu que nous pouvons considérer comme conducteur électriquement parlant. Ainsi, lorsque l'utilisateur va poser son doigt sur le bouton, une différence de potentiel va être crée avec les micro-condensateurs intégrés dans le bouton. Par exemple, dans le cas d'un capteur à double électrode, les vallées et les crêtes vont être détectées au niveau de chaque pixel et cela va permettre au système de reconstituer une image dans une matrice en additionnant les informations délivrées par l'ensemble des micro-condensateurs.

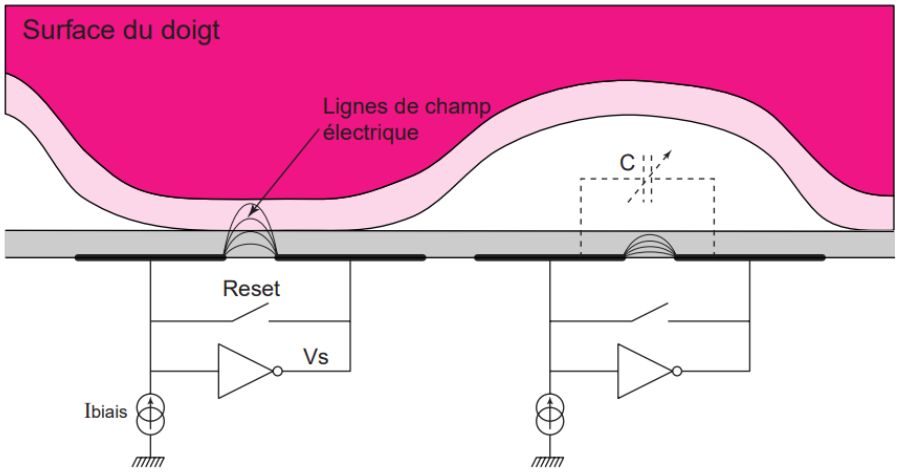


Figure 1. Capteur capacitif utilisant des pixels à double électrode (2)

1-4-2. Les dispositifs ultrasoniques dits « à ultrasons »

Les dispositifs ultrasoniques se basent principalement sur le fait qu'une onde est en partie renvoyée (réfléchie) lors du passage d'un milieu à un autre. Dans un smartphone, les deux milieux en question sont l'écran en verre et le doigt de l'utilisateur. En général, les dispositifs à ultrasons fonctionnent sur la modélisation 3D à partir d'ondes envoyés par un émetteur en rotation qui obtiendra une signature du doigt depuis 256 positions différentes.

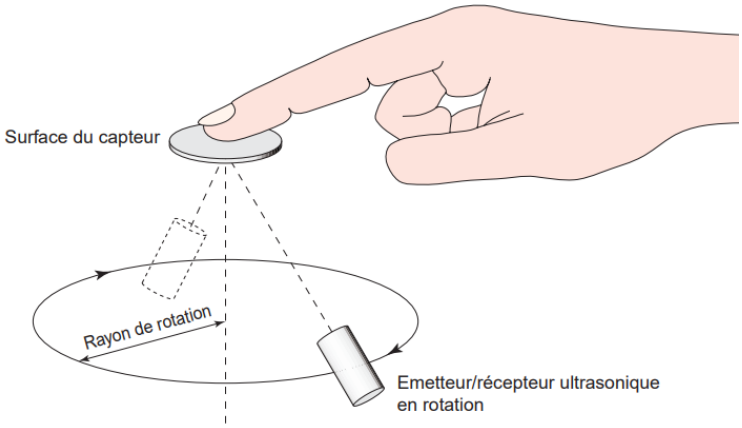


Figure 2. Principe de fonctionnement d'un capteur d'empreintes digitales ultrasonique à émetteur/récepteur en rotation (2)

Nous comprenons ainsi qu'en superposant les 256 images, le dispositif sera capable d'obtenir une image précise et en relief du doigt ce qui lui permet d'obtenir un meilleur niveau de sécurité que les capteurs capacitifs et optiques. Sa très haut définition lui permet également dessiner une image même lorsque le doigt admet des particularités. En voilà deux exemples :

- Chez les enfants, les sillons sont beaucoup plus fins que chez les adultes alors il est beaucoup plus compliqué pour le capteur de différencier crêtes et vallées. Là où un capteur capacitif ou optique échouerait certainement, le capteur ultrasonique pourra tout de même obtenir une image de haute qualité permettant au système informatique derrière de traiter l'image.

- Les ondes ultrasoniques sont très peu impactées par les imparités comme l'eau ou les saletés. Ainsi, si cela est bien sûr dans la limite du raisonnable, un utilisateur qui vient de jardiner ou qui vient de se laver les mains pourra quand même déverrouiller son téléphone ce qui ne serait pas forcément le cas des autres types de capteurs.

Ces avantages lui permettent donc d'obtenir un taux de rejet particulièrement faible puisque celui-ci serait aux alentours des 2%. En revanche, nous pouvons comprendre que ce type de capteur est plus couteux que les autres car son fonctionnement est d'autant plus complexe que sa qualité de sortie est bonne. Il faut en effet intégrer un système de rotation de l'émetteur/récepteur sous l'écran ce qui est bien plus difficile que de simplement intégrer une Led et un capteur optique, par exemple.

1-4-3. Les dispositifs optiques

Enfin, il reste le dispositif optique qui est actuellement le plus utilisé dans la plupart des smartphones bas de gamme et milieu de gamme. Il se base sur des lois simples qui découlent d'ailleurs du même principe que pour les ondes ultrasoniques c'est-à-dire la loi du changement du milieu et la loi de réflexion. Ainsi, sa simplicité de conception fait de lui un système pouvant être vendu à un prix abordable. Ainsi, nous comprenons pourquoi il est utilisé sur les smartphones les moins chers du marché. De plus, nous avons précédemment pu évoquer ses inconvénients par rapport aux autres types de capteur et à partir de ça nous pouvons aussi comprendre son absence sur les smartphones hauts de gamme. En revanche, nous n'avons pas expliqué les raisons de ces inconvénients et pour cela, il nous faut étudier son fonctionnement et ses caractéristiques plus en détails. Dans ce cas, il nous répondre à la question suivante : **comment fonctionnent les dispositifs optiques de reconnaissance d'empreintes digitales ?** Pour répondre à cette question, nous étudierions d'abord le fonctionnement optique des dispositifs optiques de reconnaissance d'empreintes digitales. Puis, nous expliquerons comment se passe le traitement des données une fois l'image reçue par le capteur.

2 - Étude du fonctionnement optique

2-1. Les différents types de dispositifs optiques

Les capteurs optiques intégrés qui sont actuellement sur le marché se répartissent principalement en trois modes d'acquisition différents :

- Capteurs à matrice complète est constitué d'un ensemble d'éléments sensibles dont la surface rectangulaire recouvre presque entièrement la surface du doigt. L'utilisateur place un doigt sur la surface et le système intégré lit séquentiellement toutes les lignes et colonnes de la matrice. L'image résultante est rectangulaire, aucune phase de reconstruction n'est nécessaire. Ce type de capteur nécessite une grande surface, ce qui entraîne des coûts de fabrication élevés.

- Capteur de balayage acquiert des images grâce à la position de mouvement du doigt de l'utilisateur qui balaye le long du capteur. Il existe deux types différents :
  - Capteurs à matrice partielle : dans ce cas, le capteur est constitué d'un nombre réduit de lignes d'éléments sensibles couvrant la largeur des doigts (entre 8 et 40 lignes). Un dispositif de balayage intégré produit une série d'images à différents moments lorsque le doigt défile. L'image finale de la surface du doigt est ensuite reconstruite par superposition à l'aide d'un algorithme dédié. Par rapport aux capteurs matrices entières, la surface obtenue est importante pour certains processus de reconstruction d'image.
  - Capteur à ligne unique, la surface du capteur est réduite au minimum, en effet le capteur est constitué d'une rangée d'éléments sensibles couvrant la largeur d'un doigt. Lorsqu'un doigt est balayé sur la surface du capteur, le fil balaye périodiquement pour créer une image de la surface du doigt. L'image résultante est directement liée à la vitesse à laquelle le doigt défile sur la surface du capteur. Cette vitesse n'étant jamais constante (phénomène de frottement solide), de fortes distorsions spatiales verticales peuvent être introduites dans l'image. Pour pallier cela, certains capteurs introduisent la mesure de la vitesse de défilement, d'autres font appel à certains traitements d'image.

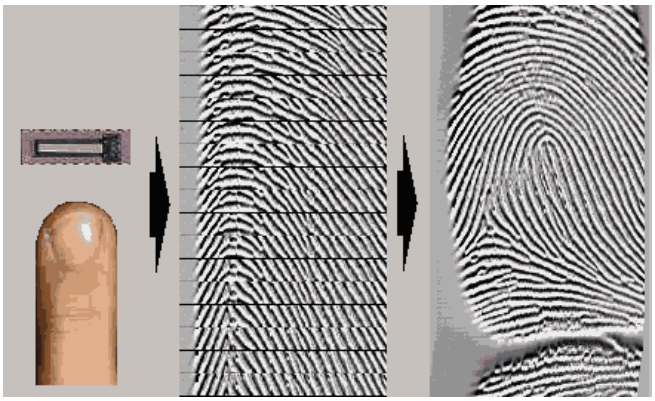


Figure 3. Fonctionnement d'un capteur par matrice (3)

2-2. Fonctionnement et caractéristiques des dispositifs optiques

2-2-1. Modèle optique

L'écran est représenté dans le schéma ci-dessous par un prisme translucide d'indice optique I1. Une Led se situe sous l'écran et envoie des rayons lumineux. Il y a alors deux possibilités en fonction de la position du doigt sur l'écran. Dans le cas d'une crête, le rayon est confronté à la peau qu'on considère comme un milieu entièrement réfléchissant car son indice optique est pratiquement identique à celui du verre. Ainsi, le rayon va être renvoyé vers le capteur qui comprendra qu'une crête se situe à cet endroit. Dans le cas d'une vallée, le rayon est d'abord confronté à l'air d'indice optique I2. Le rayon est donc légèrement dévié. Après ça, le rayon est réfléchi contre la peau et est renvoyé dans une direction. En fonction de l'angle, il ira dans une direction mais dans tous les cas, il n'atteindra pas le capteur assez vite pour être pris en compte. Ainsi, grâce à un très grand nombre de rayons lumineux, le capteur est capable de dessiner notre empreinte digitale.

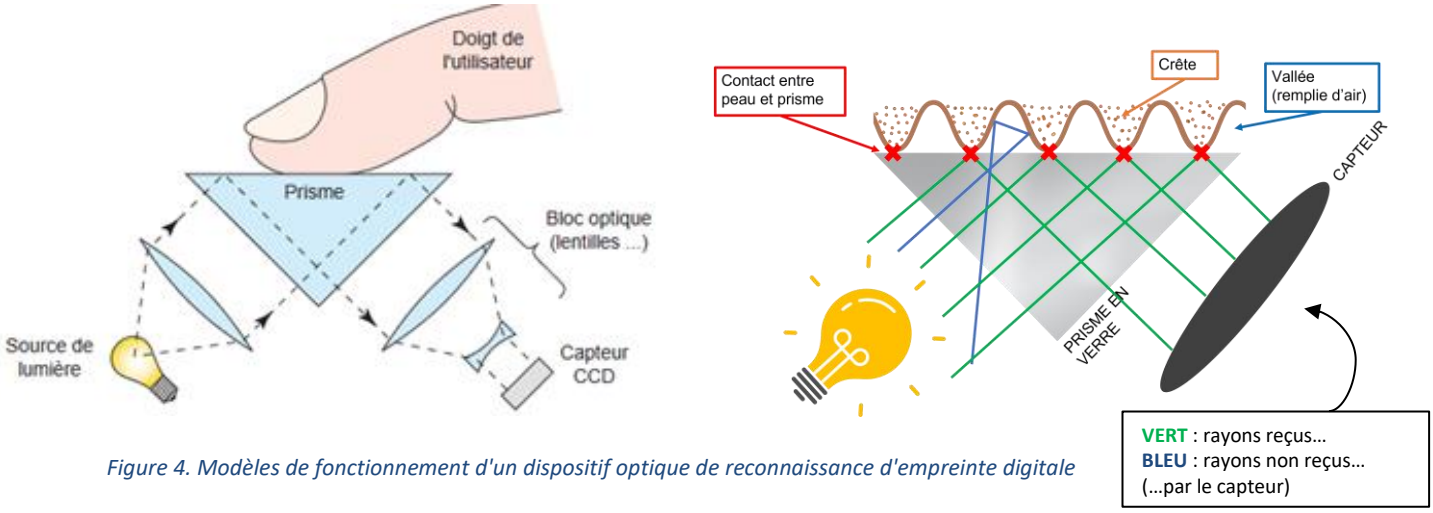


Figure 4. Modèles de fonctionnement d'un dispositif optique de reconnaissance d'empreinte digitale

2-2-2. La source de lumière

Le matériel utilisé comme source de lumière est une LED, un composant électronique qui émet de la lumière lorsqu'il est traversé par un courant électrique. Le rayonnement lumineux à partir duquel les photons sont émis est monochromatique, ce qui signifie que son rayonnement n'est contenu que dans une et une seule longueur d'onde. De plus, la couleur la plus fréquente est le vert car elle est celle qui est le plus facilement captée par les capteurs optiques. Sa longueur d'onde est aux environs des 575 nm.

2-2-3. L'écran considéré comme un prisme

La plupart de nos écrans aujourd'hui utilisés sont des écrans LCD (*Liquid Crystal Display*). Ces cristaux liquides sont des matériaux constitués de molécules de formes allongées et plongées dans un liquide. La position de ces batônnets peut être modifiée grâce à un champ électrique. Celui-ci va permettre de créer une structure ordonnée des cristaux liquides qui va influer sur la quantité de lumière perçue. Pour un écran LCD, on

utilise des cellules constituées de cristaux liquides coincés entre deux polariseurs. Au repos, ses polariseurs sont orientés pour que la lumière ne puisse pas traverser Il faut appliquer une tension électrique sur les cristaux liquides pour que leur alignement puisse changer. La polarisation de la lumière fait une rotation (qu'est ce qui rotationne ???) en conséquence (et) une partie de la lumière peut traverser la cellule. Ainsi, lorsque l'utilisateur va poser son doigt sur l'écran, celui-ci va être éclairé par la led et va créer une tension électrique. A l'aide de cette tension, la lumière de la led va être polarisée et nous allons pouvoir récupérer l'image de notre empreinte sur l'écran.

2-2-4. Les différents types de capteurs optiques

a. Le capteur CDD

Le capteur CCD (*Charge Coupled Device*) a été créé en 1969 par George Elwood Smith et Willard Boyle, des physiciens américains et canadiens. C'est un composant électronique sensibles à la lumière qui transforme un signal lumineux en un signal électrique. Il est indispensable pour réaliser un tableau de pixel qui va être la matière première version de notre image. Le capteur CCD se compose de 4 couches indispensables : une couche de photosites, une matrice RBV, une surface de microlentilles et une couche composée de filtres.

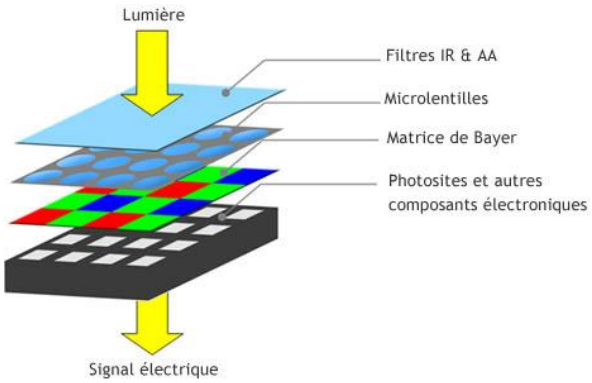


Figure 5. Schéma structurel d'un capteur CDD (4)

La couche de photosites est la couche la plus importante de toute puisqu'elle est la base de fonctionnement de capteur. Elle fonctionne un peu comme un piège à lumière lorsque l'utilisateur pose son doigt sur le bouton d'empreinte digitale du smartphone. Chaque photosite est lui-même composé de deux couches de silicium : une couche dopé en phosphore et une couche dopée en bore. Lorsqu'un photon rentre en contact avec le photosite, un électron est éjecté de l'atome de bore et se dirige donc vers la couche dopé en phosphore qui représente une zone positive.

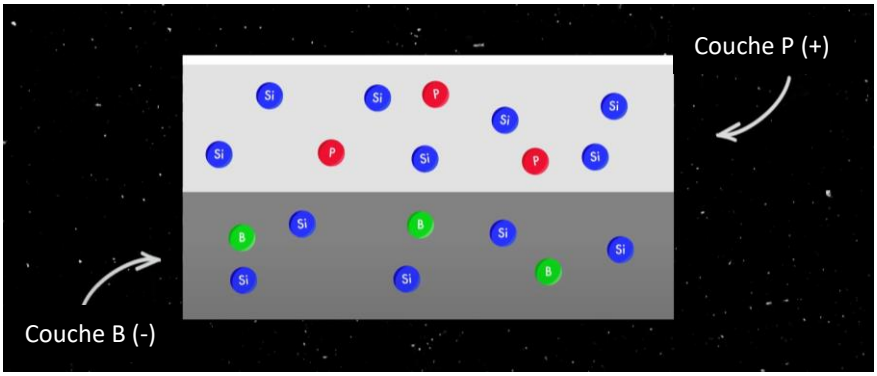


Figure 6. Photosite d'un capteur CDD (4)

Lorsqu'un photon rentre en contact avec le photosite, un électron est éjecté de l'atome de bore et se dirige alors vers la couche dopé en phosphore qui représente une zone positive. La différence de charge entre l'instant initial et l'instant final qui a été provoquée par le déplacement de l'électron permet donc au système de déterminer à quels endroits des photons (et donc des rayons lumineux) ont rencontrés le capteur. Cette opération va s'effectuer sur l'ensemble des photosites composant le capteurs et c'est seulement à la **fin** de

l'exposition que les informations contenues sous la forme de charges électriques au sein des photosites vont être converties en signal analogique via une technique de conversion dite grossièrement « de seau à seau ». En effet, chaque photosite va transmettre un à un l'information qu'il stocke jusqu'à que tous l'aient fait.

Photosite 1er à transmettre

Photosite 2ème à transmettre

Photosite 3ème à transmettre

Et ainsi de suite…

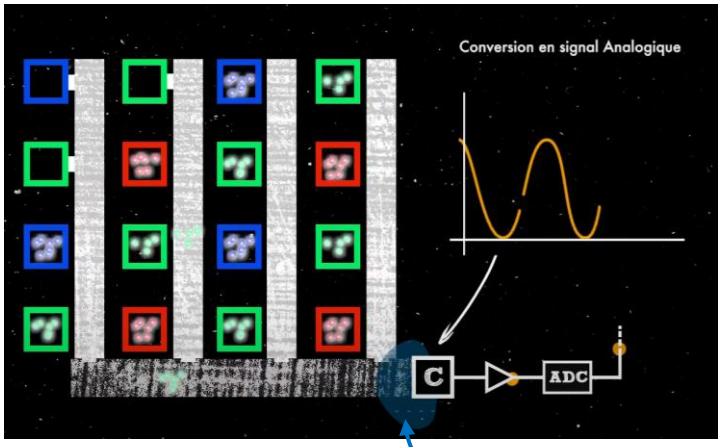


Figure 7. Technique du "seau à seau" (4)

Puit de potentiel attirant les électrons contenus dans chaque photosite.

Cependant, le problème des photosites est qu'ils ne sont sensibles qu'à la lumière blanche c'est-à-dire qu'ils ne vont pas faire la distinction entre les différentes couleurs. Pour y remédier, nous devons utiliser une matrice de filtre RVB appelé Matrice de Bayer. Celle-ci combine quatre photosites et trois couleurs pour coder un pixel : un photosite rouge, un photosite bleu et deux verts. Pourquoi deux photosites verts ? L'œil humain est plus sensible à cette longueur d'onde verte alors il est plus courant d'utiliser une majorité de couleurs vertes dans la capture d'une image. Cette matrice est une mosaïque de cellules élémentaires : chaque cellule élémentaire est composée de pixels et sous chaque pixel se trouve une électrode. Or, les pixels fonctionnent par pair : un pixel image sensible à la lumière est associé un autre pixel mémoire insensible à la lumière. Ainsi, lorsque que les pixels images sont exposés à la lumière, ils accumulent des charges électriques en fonction de l'intensité lumineuse reçue. Ainsi le potentiel des électrodes se modifient. De cette manière, les charges électriques des pixels images sont transférés vers les pixels mémoires.

La troisième couche qui se trouve par-dessus la matrice de Bayer est constituée des microlentilles. Leur objectif est simple : faire converger la lumière vers les photosites pour éviter d'avoir des pertes de photons et donc des pertes d'informations. Pour cela, les microlentilles sont des lentilles plan-convexes qui dévie les rayons lumineux vers le milieu de la lentille.

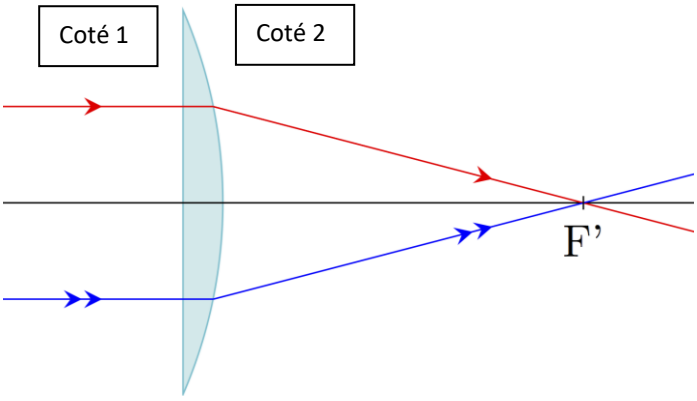


Figure 8. Schéma d'une lentille plan-convexe

$$\boldsymbol{V = V1 + V2}$$

Mais $V_1 = 0\ car\ R1 \to +\infty$

De plus, $V_2 = \frac{1}{f'}\ avec \frac{1}{f'} = \frac{1}{\overline{OA'}} - \frac{1}{\overline{OA}}$

Dans le cas de notre capteur, nous avons forcément :

$\overline{OA} > \overline{OA'}$ donc $\frac{1}{\overline{OA}} < \frac{1}{\overline{OA'}}$

Alors $\frac{1'}{f} > 0$ donc $V_2 > 0$

➔ Nous avons vérifié que la lentille est bien **convergente.**

Enfin, pour la dernière couche du capteur on va retrouver une série de filtres. Ces-derniers permettent notamment de réduire les ultraviolets, réduire la quantité de lumière reçue et protéger les photosites. Dit comme ça, ils n'ont pas l'air d'être indispensables mais si nous décidons d'ôter cette couche, nous nous rendrons compte que l'image reçue par le capteur sera de mauvaise qualité ce qui pourrait compliquer (voir rendre impossible) le traitement de l'image par le système.

b. Le capteur CMOS

Le deuxième capteur utilisé est le capteur CMOS (*Complementary metal-oxide-semiconductor*). Il a été créé par Éric R. Fossum dans les années 1990. Son mode de fonctionnement est globalement le même que celui du CCD car ses couches supérieures (matrice RVB, microlentilles, filtres) sont également présentes. En revanche, il y a une différence au niveau de la couche de photosite puisqu'un semi-conducteur à oxyde de métal complémentaire est rajouté pour relié la couche B et P dans chaque photosite. Ce-dernier permettra de mesurer les informations directement auprès de chaque photosite et donc ainsi d'éviter de procéder à la technique « seau à seau ».

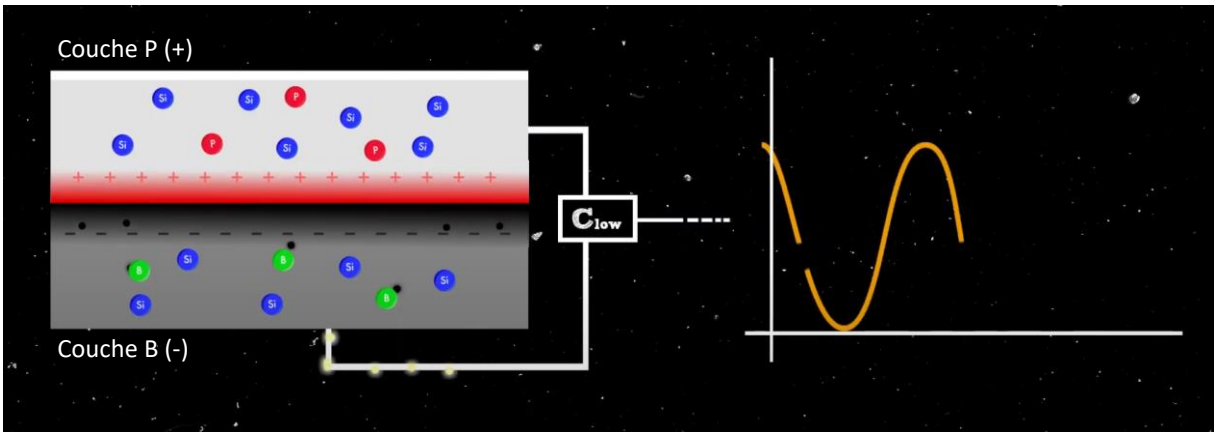


Figure 9. Photosite d'un capteur CMOS (4)

L'avantage principal de ce capteur est qu'il est alors possible de choisir de mesurer une zone en particulier sur le capteur (chaque photosite étant indépendant) et ainsi éviter au système d'effectuer des calculs en plus qui le feraient perdre du temps. Cependant, rajouter un circuit électrique au niveau de chaque photosite introduit également certains inconvénient comme l'apparition d'un bruit numérique plus élevé que sur les CCD mais aussi le fait que le capteur CMOS nécessitera donc davantage de place en surface pour fonctionner. C'est d'ailleurs pour ces raisons que la grande majorité des constructeurs de smartphones préfèrent le capteur intégrer un capteur CCD pour la reconnaissance des empreintes digitales. En effet, la qualité la plus recherchée dans ce domaine est la fiabilité alors les bruits que le capteur CMOS peut générer peuvent nuire à la qualité de l'image et donc au traitement par le système par la suite.

2-3. Limites du dispositif optique

Avant de passer au traitement des données, nous devons d'abord étudier les limites du dispositif optique. Pour cela, nous reprenons notre schéma de la figure 4 et nous l'adaptons pour correspondre à un cas limite c'est-à-dire la présence d'une poussière résiduelle dans une des vallées de l'empreintes digitales.

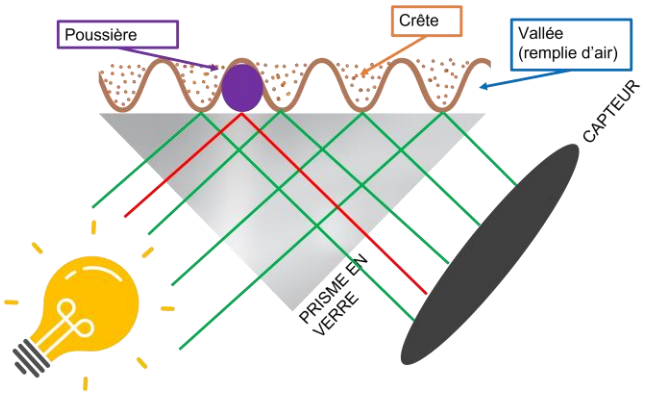


Figure 10. Cas n°1 : Présence d'une poussière dans une vallée

Nous remarquons ainsi que malgré l'absence d'une crête, la rayon lumineux en rouge sera tout de même renvoyé et capté par le capteur. Dans le cas d'une poussière unique, cela ne va pas avoir un impact assez important pour provoquer l'échec de l'authentification de l'empreinte digitale mais dans le cas où un grand nombre de poussières combleraient les vallées, le systèmes ne serait tout simplement plus capable de faire la différence entre crête et vallées.

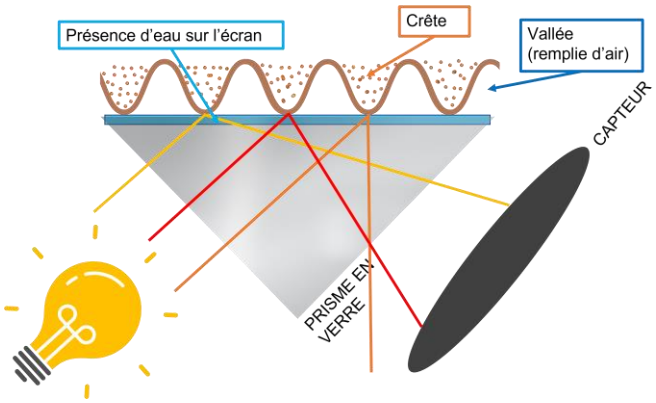


Figure 11. Cas n°2 : Présence d'eau sur le capteur

Dans ce cas, les rayons pourraient ne pas être correctement renvoyé car ceux-ci changeraient trois fois de milieu : Verre → Eau → Peau. Or l'eau n'a ni le même indice optique que la peau ni le même que le verre donc les rayons vont être déviés deux fois et cela fait qu'ils ne seront pas correctement renvoyés vers le capteur.

Finalement, nous comprenons assez simplement les limites du dispositif optique. En effet, ces-derniers se basent sur les rayons lumineux qui dépendent beaucoup de l'environnement dans lequel ils interviennent. Leur faible coût de production permet aux téléphones peu chers d'en être équipés mais dans le cas des smartphones haut de gammes (donc plus chers), ils ne représentent plus du tout une bonne solution.

3 - Étude du traitement des données

3-1. Conversion électronique des données analogiques envoyées par le capteur

Le processeur est un procédé informatique qui fonctionne selon deux valeurs : 0 et 1, c'est-à-dire de manière binaire. Il lui est donc impossible de lire directement le signal analogique que le capteur lui envoie. Ainsi, nous comprenons la nécessité de procéder à une conversion analogique-numérique qui sera effectuée via des procédés électroniques.

3-1-1. Echantillonnage

L'échantillonnage est la première étape de la conversion analogique-numérique. Il repose sur le fait de prélever une suite d'échantillons de la grandeur analogique (rendue propre par le filtrage du bruit) envoyée par le capteur. Posons $V(t)$, le signal d'entrée analogique, n un nombre entier représentant le nombre total d'échantillons et T la période associée à la fréquence à laquelle les échantillons sont capturés. Ainsi nous pouvons exprimer :

- La période $T = 1/f$
- Les temps successifs où les échantillons sont pris : $\{0, T, 2T, \dots, nT\}$
- Les valeurs échantillonnées $\{V(0), V(T), V(2T), \dots, V(nT)\}$

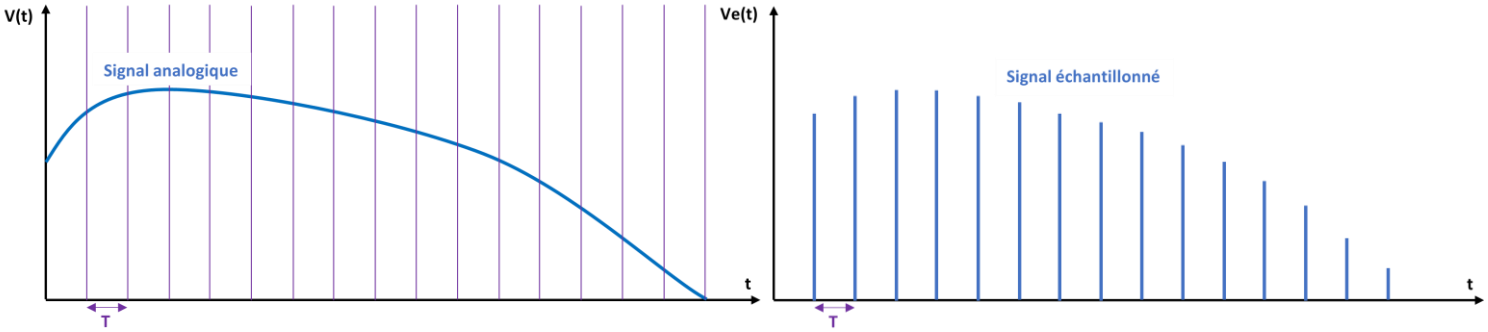


Figure 12. Fonctionnement général de l'échantillonnage

Nous comprenons alors que plus la fréquence est élevée, plus le nombre d'informations relevées sera grand et plus le signal échantillonné sera fidèle au signal analogique originel. Par analogie avec le reconnaissance d'empreintes digitales sur un smartphone, nous pouvons dire que plus la fréquence d'échantillonnage sera élevée, plus la qualité de l'image de l'empreinte sera meilleure.

En réalité, une étape supplémentaire vient compléter l'étape de l'échantillonnage : c'est le « blocage ». Nous avons décidé de ne pas nous y attarder car son fonctionnement est assez simple. L'objectif principal du blocage est de transformé le signal « bâtons » en un signal à échelons qui pourra ensuite être facilement numériser. Pour cela, le niveau de chaque échantillons est gardé en mémoire durant toute la durée de la période T :

$$Vb(t) = Ve(kT)\ pour\ kT \leq t < (K+1)T$$

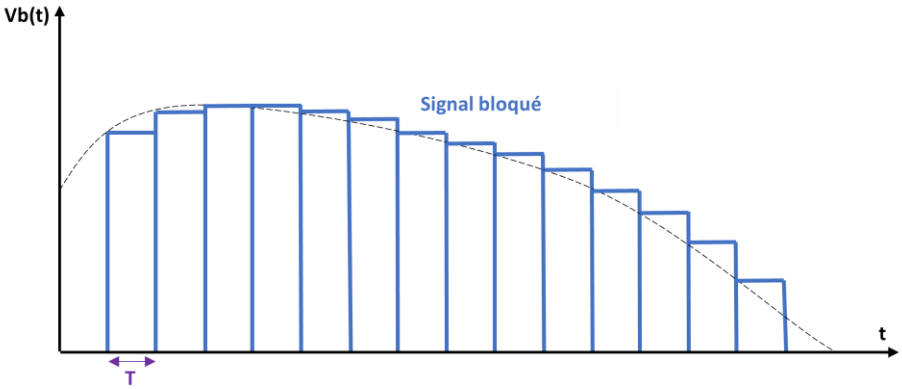


Figure 13. Fonctionnement général du blocage

3-1-2. Codage binaire

Le codage binaire est la dernière étape de la conversion analogique-numérique. Il consiste à attribuer une valeur binaire à une tension donnée. Il intervient juste après la quantification qui intervient elle-même juste après le blocage. En quelques mots, la quantification permet de « normaliser » les valeurs de tensions fournies par le signal bloquée. Plus la plage de quantification est importante, moins les valeurs de tensions $Vb(t)$ seront modifiées. Pour mieux comprendre ce processus, des explications complémentaires vous sont fournies en

annexe. Revenons donc à notre codage binaire. Prenons l'exemple d'un plage classique de quantification : $[0, +16383mV]$. (5) Pour chaque valeur de cette plage nous obtiendrons alors un codage binaire différent sur 14 bits :

Valeur en mV	Codage binaire													
	2^{13}	2^{12}	2^{11}	2^{10}	2^{9}	2^{8}	2^{7}	2^{6}	2^{5}	2^{4}	2^{3}	2^{2}	2^{1}	2^{0}
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	0	0	0	0	0	0	0	0	0	0	0	0	0	1
…	…	…	…	…	…	…	…	…	…	…	…	…	…	…
16382	1	1	1	1	1	1	1	1	1	1	1	1	1	0
16383	1	1	1	1	1	1	1	1	1	1	1	1	1	1

Une fois le codage de chaque échelon du signal $Vb(t)$ effectué, le signal de sortie sera donc numérique. Par exemple, les '0' pourront être traduit par 0V et les '1' par 5V.

3-2. Traitement informatique des données binaires par le processeur

Une fois l'image rendue lisible par le processeur (signal numérique) , le processeur créé une matrice avec toutes les informations qu'il reçoit. Cette matrice lui permettra de reconstruire l'image de l'empreintes digitales de l'utilisateur. Cependant, cette image doit d'abord être traitée avant d'être comparée avec l'image en mémoire.

3-2-1. Segmentation

L'objectif de la segmentation est de séparer l'empreinte digitales de l'arrière-plan de l'image pour éviter que celui-ci n'apporte de mauvaises informations au système. Nous avons précédemment vu que l'image envoyée par le capteur est en noir et blanc et avec un haut contraste alors il faut utiliser un masque gris pour éliminer tout ce qui n'est pas utile. En effet, les crête sont repérés par les taches noires sur l'image et les vallées par les taches blanches. Tout ce qui n'est ni noir ni blanc, donc gris en échelle noir-blanc, peut donc être considéré comme des impuretés (saletés, etc…). L'échelle de noir et blanc s'étale sur une plage de 256 nuances différentes (6), 255 correspondants au blanc et 0 au noir. Le masque gris appliqué, en général, dans ce cas est situé à $M = 128$.

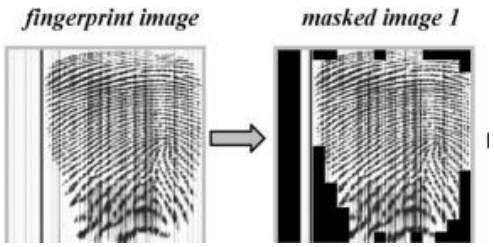


Figure 14. Application du masque gris (6)

Sur certains appareils, un deuxième masque est appliqué pour éliminer les bordures de l'image qui bien souvent ont été légèrement altérées par la lumière blanche émise par le soleil. Ainsi, nous pouvons retrouver uniquement le centre de l'image et les traits les plus définis de l'empreinte digitales.

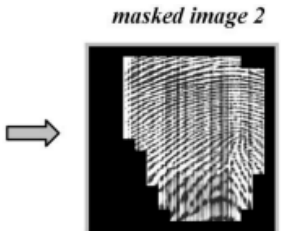


Figure 15. Application du masque supplémentaire (6)

3-2-2. Extraction

Avant d'en arriver à l'extraction, l'image de l'empreinte isolée a d'abord dû subir des traitements supplémentaires pour améliorer la qualité de l'image. Nous avons décidé là encore de ne pas entrer dans les détails mais vous pouvez retrouver ces traitements supplémentaires en **annexe**.

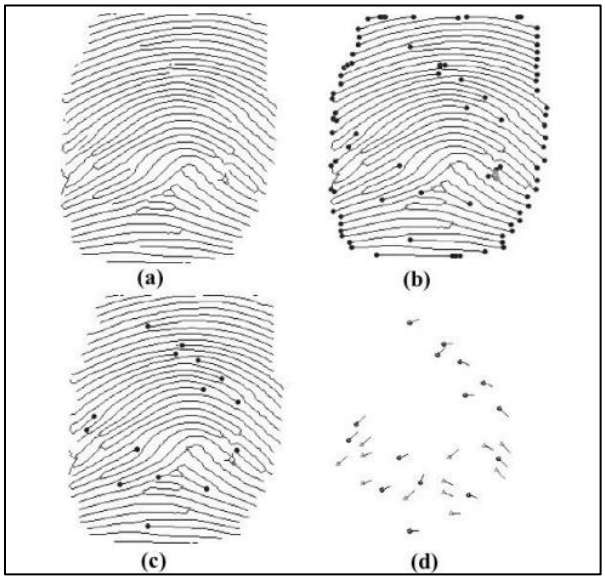
L'image est enfin prête à être extraite. Le processeur va alors devoir trouver des points particuliers appelés « minuties ». Pour cela, il utilise un algorithme reconnu appelé « *crossing numbers algorithm* » défini par la formule suivante (6) :

$$CN(p) = \frac{1}{2}\sum_{i=1}^{8}|P_i - P_{i-1}| \text{ avec } P_8 = P_0 \text{ and } P_i \in \{0,1\}$$

$CN(p)$ représentant le nombre de crêtes provenant du pixel P

Avec cette formule et dans le cas de la reconnaissance d'empreinte digitale au sein d'un smartphone, nous considérons particulièrement deux types de minuties exprimées par les valeurs suivantes :

$CN(P) = 1$: P est la fin d'une crête $\qquad$ $CN(P) = 3$: P est une bifurcation



(a) Image améliorée de l'empreinte digitale isolée de l'utilisateur
(b) Minuties détectées
(c) Minuties validées (les minuties au bord de l'image ne sont pas prises en compte par le processeur)
(d) Signature de l'image

Figure 16. Minuties reconnues par l'algorithme « crossing numbers » (7)

3-2-3. Reconnaissance des minuties

Une fois la signature de l'image obtenue, il ne reste plus qu'à la comparer avec les images stockées en mémoires (un smartphone peut contenir jusqu'à 3 empreintes digitales en mémoire pour que l'utilisateur puisse utiliser différent doigts).

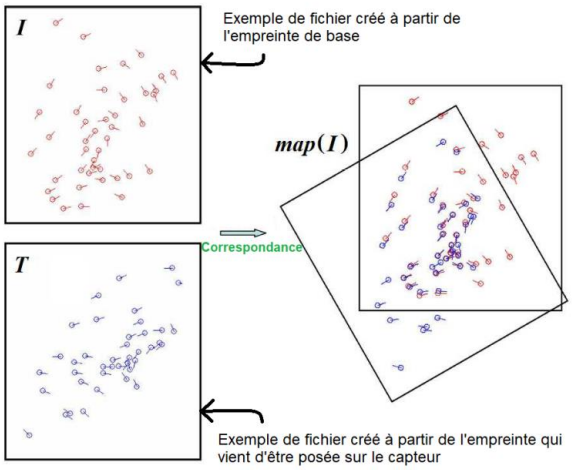


Figure 17. Comparaison de de l'image en mémoire et l'image reçue par le capteur (7)

Le processeur superpose les deux images et cherche les minuties similaires. Il est également capable de faire pivoter l'image obtenue quand l'utilisateur pose son doigt sur le capteur car la position ne ce-dernier à chaque prise ne peut statiquement pas être la même. C'est d'ailleurs pour cette raison que même en posant notre à 90° par rapport à la position « classique », cela fonctionnera quand même.

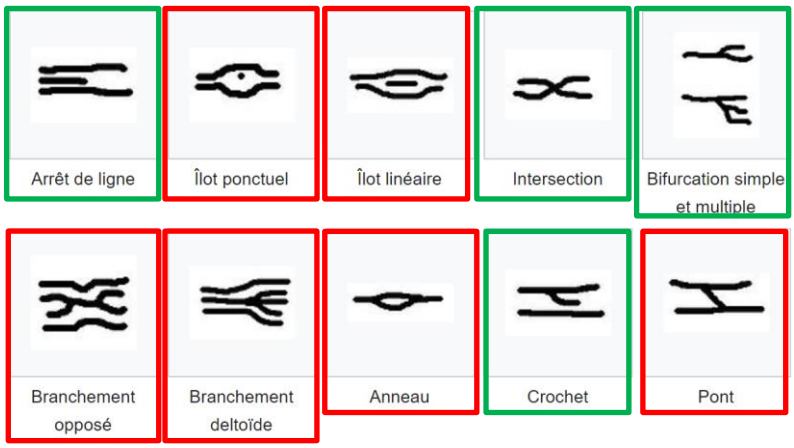
Au sein d'un smartphone, la sécurité est considérée comme moyenne car il faut que le déverrouillage soit rapide pour ne pas contraindre l'utilisateur à laisser son doigt trop longtemps sur le capteur. Nous pouvons écrire la relation proportionnelle suivante :

$$Temps\ de\ deverouillage = Niveau\ de\ sécurité * Nombre\ total\ de\ minuties$$

Le niveau de sécurité peut être exprimé sous la forme d'un pourcentage. Plus ce pourcentage est élevé, plus le processeur devra détecter de minuties et plus le temps de déverrouillage sera long. Ainsi, en fonction de l'utilisation du dispositif de reconnaissance d'empreinte digitales, il faut configurer le niveau de sécurité de telle façon à ce que celui-ci soit le plus optimisé possible.

Dans certains domaines comme celui de la Justice notamment, la reconnaissance d'empreintes digitales se fait en deux temps :

1) Un programme compare deux empreintes digitales et affiche un résultat.
2) Un humain vérifie manuellement chaque minutie similaire et vérifie que les deux images d'empreintes sont vraiment semblables notamment avec d'autres types de minuties que le logiciel ne traite pas.



VERT : minuties facilement traitables par un logiciel informatique grâce à l'algorithme des « *crossing numbers* »

ROUGE : minuties ne pouvant pas être détectées informatiquement

Cette double vérification permet d'éviter les coïncidences qui peuvent être liées à la programmation du niveau de sécurité. En effet, même si cela est statistiquement improbable il n'est pas impossible que le programme réussisse à trouver au moins 12 minuties similaires. (12 étant le seuil fixé en France dans le domaine judiciaire). C'est pour cela qu'un humain doit vérifier derrière que les deux empreintes correspondent bien et ne sont pas qu'une coïncidence malvenue.

4 - Conclusion

Lorsqu'un utilisateur pose son doigt sur la zone conçue pour la reconnaissance d'empreinte digitale, plein de choses se passent à l'intérieur du smartphone. Tout d'abord, nous avons vu pour le cas des dispositifs optiques que l'empreinte digitale est captée grâce à l'émission et la réception de rayon lumineux qui se réfléchissent contre la peau et sont ensuite captés par le capteur optique (CCD ou CMOS). Nous avons pu voir que cela s'appuie sur des lois physiques simple et que seules les crêtes étaient captées au niveau du capteur, les vallées étant justement représentées par l'absence d'information. Après ça, nous avons également pu voir qu'il y avait tout un processus de conversion des données que le capteur envoie car le processeur fonctionne en binaire et non en analogique. Une fois la conversion effectuée, nous avons finalement expliqué comment se passait la reconnaissance des minuties via l'algorithme des « *crossing numbers* ». Nous avons cependant évoqué les limites auxquelles les systèmes informatiques sont confrontés et pourquoi parfois il est quand même nécessaire qu'un être humain intervienne. En lien avec la reconnaissance d'empreintes digitales, nous aurions également pu nous poser d'autres questions telles que :

- **Quelles sont les limites éthiques dans la reconnaissance d'empreintes digitales ?**
- **Empreintes digitales ou reconnaissance faciale 3D, lequel est le mieux ?**
- **Les empreintes digitales, le futur de la signature ?**

5 - Problèmes rencontrés sur le projet et ressentis

Tout le long du projet, nous avons eu une principale crainte : vulgariser le sujet. En effet, les dispositifs optiques de reconnaissance d'empreintes digitales utilisent un tel nombre de procédés et traitements qu'il était difficile de tous les traiter sans aller trop vite et rester en surface. Nous avons donc essayé de nous concentrer sur le principal et d'en dire le maximum possible là-dessus et cela de manière scientifique. De notre ressenti, nous pensons finalement avoir réussi à le faire mais il est vrai qu'on a dû beaucoup bataillé pour ne pas tomber dans cette sorte de facilité. De plus, le secteur des empreintes digitales sur smartphone est un secteur dynamique qui évolue sans cesse donc il était d'autant plus difficile de trouver des sources fiables et à jour à la fois. Notre tuteur, **Mr. Nicolas Crespo-Monteiro** nous a d'ailleurs beaucoup aidé là-dedans en nous donnant les pistes nécessaires pour structurer et avancer efficacement dans notre étude.

6 - Annexes

6-1. Définitions

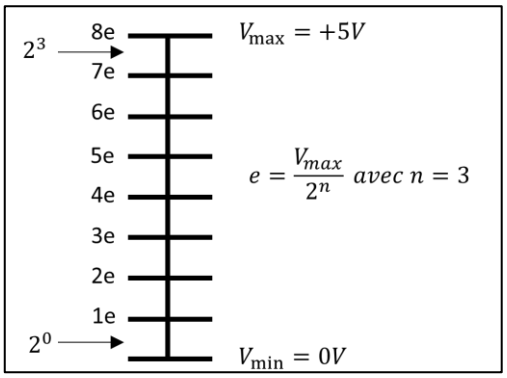
Taux de rejet : C'est le taux d'échec d'authentification auquel est confronté un dispositif de reconnaissance d'empreinte digitales lorsque l'empreinte de l'utilisateur devrait être reconnu mais ne l'est pas. Plus il est élevé, moins le système est fiable et plus l'utilisateur perdra de temps à déverrouiller son smartphone.

Minuties : Ce sont les formes particulières qui apparaissent au sein d'une empreintes digitales. Celles-ci peuvent être des bifurcations, des fins de crêtes, des embranchements spéciaux, etc… Certaines de ses minuties peuvent être retrouvées via l'algorithme des « *crossing numbers* » et donc être détectées par un programme informatique.

Photosite : « Un photosite est une cellule photoélectrique qui transforme une intensité lumineuse en signal électrique. Le nombre de photosites sur un capteur constitue ce que l'on appelle la définition du capteur. Cette définition est souvent donnée en millions de pixels. » (7)

6-2. Quantification

La quantification consiste à normaliser les valeurs de tensions d'un signal bloqué et échantillonné pour que ces-valeurs soient des multiples entier d'une grandeur appelée « échelon ». Une plage de quantification P est alors défini par 2^n le nombre d'échelons utilisés (qui s'apparentera par la suite à la résolution de l'image) et *e* le pas de quantification c'est-à-dire la valeur en tension d'un échelon.



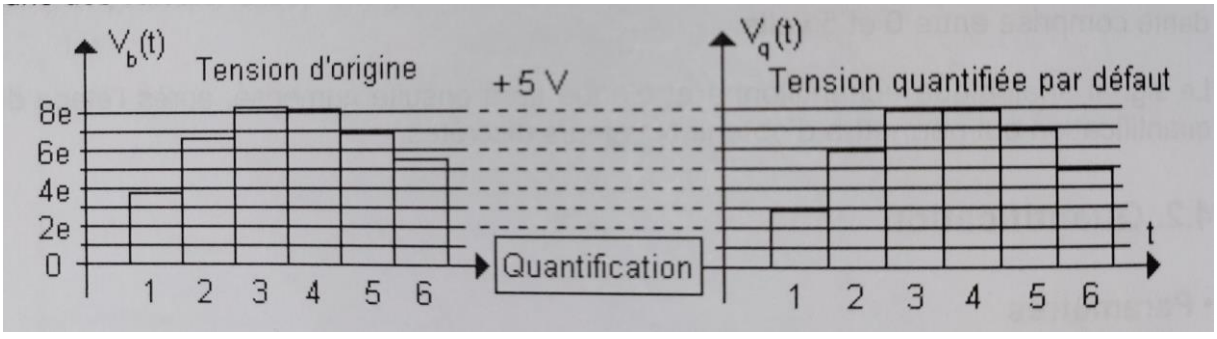
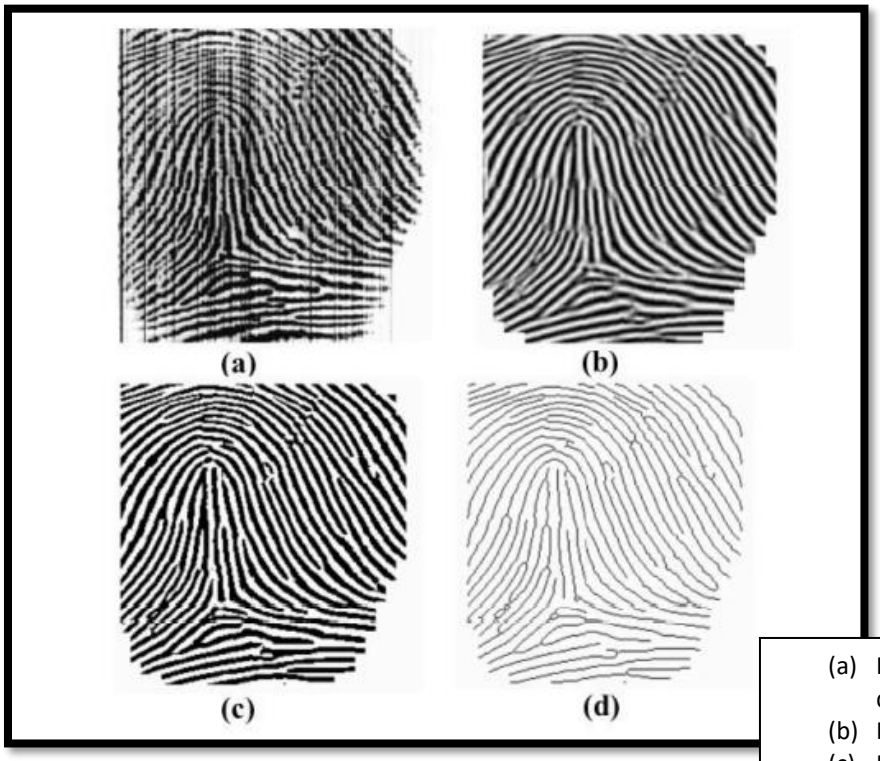


Figure 18. Fonctionnement général de la quantification (5)

6-3. Traitements pré-extraction



(a) Image de l'empreinte digitale isolée de l'utilisateur
(b) Filtre de Log-Gabor
(c) Binarisation
(d) Amincissement des traits

Figure 19. Traitements supplémentaires d'amélioration (2)

- Le filtrage de Log-Gabor permet d'éliminer tous les parasites qui peuvent être présents sur l'image. Celui-ci est effectué avec un système de calcul « voisins à voisins ». (…)

- La binarisation d'une image repose sur le fait de réduire la plage des nuances de gris à deux valeurs qui correspondent au noir et au blanc. Pour la plage classique $[0; 255]$ (0 représentant le noir et 255 le blanc), on applique donc les deux règles suivante :

$$i = 0, pour\ tout\ les\ i \leq 127$$

$$j = 255, pour\ tout\ les\ j \geq 128$$

Cela nous permet ainsi de transformer tout ce qui est plus sombre vers un noir pur et tout ce qui est plus clair vers un blanc uniforme. L'image est ainsi binaire : '0' pour absence d'information (blanc) et '1' pour la présence d'information (noir).

- L'amincissement des traits consiste à réduire l'épaisseur des crêtes sur l'empreintes digitales. Cette étape peut paraître futile mais elle permet en fait d'éviter un grand nombre d'éventuelles erreurs dans l'application de l'algorithme des « *crossing numbers* ».

7 - Bibliographie

1. **Wikipédia. [En ligne] fr.wikipedia.org.**

2. PARRAIN, Fabien. *Capteur intégré tactile d'empreintes digitales à microstructures piezorésistives.* INSTITUT NATIONAL POLYTECHNIQUE DE GRENOBLE. Grenoble : s.n., 2002. Thèse de doctorat.

3. TPE : Lecteur d'empreintes digitales optiques. *https://tpecapteurbiometrique.wordpress.com/2016/02/18/4les-leds-2/.* [En ligne] 2016. https://tpecapteurbiometrique.wordpress.com/2016/02/18/4les-leds-2/.

4. La différence entre les CAPTEURS CMOS ET CCD | EP13 - Le Guide. [En ligne] YOUTUBE, 2021. https://youtu.be/2jYbS4hrnXM.

5. TURRIER, Claude. *Photographie numérique - Bases théoriques, prise de vue, fichier image.* s.l. : Editions Ellipses, 2013.

6. ADDEPALLI, Jayanti and VASUDEV, Aseem. Fingerprint Sensor and Blackfin Processor Enhance Biometric-Identification Equipment Design. *AnalogDialogue.* [Online] https://www.analog.com/en/analog-dialogue/articles/fingerprint-sensor-blackfin-enhance-biometric-id-equip-design.html.

7. *Maxicours.* [En ligne] https://www.maxicours.com.

8. SAUZE, Erwan et MARCANDELLA, Axel. *La reconnaissance et l'utilisation des empreintes digitales dans le domaine de la sécurité.* Télécom Saint-Etienne. Saint-Etienne : s.n., 2021. Projet scientifique.

9. NGUYEN, Hubert. How Fingerprint Sensors Work. *Übergizmo.* [Online] 11 08, 2016. https://www.ubergizmo.com/articles/fingerprint-scanners-how-they-work/.

10. Larousse. [En ligne] www.larousse.fr.

8 - Tables des figures

télécom saint-étienne
école d'ingénieurs nouvelles technologies

Résumé

Résumé
Dans un monde rempli de smartphones, il est important de savoir comment fonctionne réellement ces-derniers. Dans ce projet scientifique, nous nous sommes plus particulièrement au fonctionnement des dispositifs optiques de reconnaissance d'empreintes digitales. En effet, bien qu'ils soient maintenant remplacés par des dispositifs plus efficaces et plus pratiques tels que ceux à ultrasons, thermiques et capacitifs, les dispositifs optiques ont été les premiers dispositif à apparaître sur le marché pour la reconnaissance d'empreintes digitales. Nous avons donc étudié leur fonctionnement et précisé leurs avantages mais aussi leurs limites.

Mots-Clés
Empreintes digitales, Sécurité, Smartphones, Optique, Informatique, Electronique

Abstract

Abstract
In a world full of smartphones, it's important to know how they actually work. In this scientific project, we focused more specifically on the operation of optical fingerprint recognition devices. Indeed, although they are now replaced by more efficient and practical devices such as ultrasonic, thermal, and capacitive, optical devices were the first devices to appear on the market for fingerprint recognition. We have therefore studied their operation and specified their advantages but also their limits.
Keywords
Fingerprint, Security, Smartphones, Optic, Informatic, Electronic