



## ING1 GROUPE 1

### RAPPORT DU PROJET GM1

---

# Empreintes digitales - Analyse

---

Auteurs :

Beauplet Gabriel  
Vincent Victor  
Laverdine Clément  
Caucheteux Léo-Paul  
Piotrowski Bastien

Professeurs :

Vernay Remi

20 mai 2016

# Table des matières

<b>1</b>	<b>Introduction</b>	<b>3</b>
1.1	Histoire de l'utilisation des empreintes digitales . . . . .	3
<b>2</b>	<b>Différentes méthodes d'identification</b>	<b>4</b>
2.1	La biométrie . . . . .	4
2.2	L'iris . . . . .	5
2.3	La rétine . . . . .	6
2.4	Le visage . . . . .	7
<b>3</b>	<b>La description d'une empreinte</b>	<b>8</b>
3.1	Qu'est ce qu'une empreinte? . . . . .	8
3.2	La formation des empreintes . . . . .	9
3.3	A quoi servent les empreintes digitales? . . . . .	9
3.4	Les applications des empreintes . . . . .	10
3.5	Les points faibles . . . . .	11
3.6	Minuties et points singuliers globaux . . . . .	11
3.7	Signature de l'empreinte . . . . .	13
3.8	Probabilité de trouver deux empreintes identiques . . . . .	14
<b>4</b>	<b>Comment relever une empreinte?</b>	<b>15</b>
4.1	Relevé involontaire . . . . .	15
4.2	Le relevé volontaire . . . . .	16
<b>5</b>	<b>Traitement informatique de l'empreinte</b>	<b>17</b>
5.1	Généralités . . . . .	17
5.2	Séparation . . . . .	17
5.3	Egalisation d'histogramme . . . . .	18
5.4	Filtre Passe-Haut . . . . .	19
5.5	Filtre median . . . . .	20
5.6	Binarisation de l'image . . . . .	21
5.7	Filtre directionnel . . . . .	21
5.8	Squelettisation . . . . .	23
<b>6</b>	<b>Comparaison de deux empreintes</b>	<b>25</b>
6.1	Comparer les minuties . . . . .	27
6.2	La vraie comparaison . . . . .	30

<b>7 Les fonctionnalités du programme</b>	<b>32</b>
7.1 Petit rappel sur le processus . . . . .	32
7.2 Précision sur le programme . . . . .	32
7.3 Comparer deux empreintes . . . . .	33
7.4 Comparer une empreinte avec un répertoire . . . . .	35
7.5 Retrouver les empreintes d'une même personne dans un répertoire . . . . .	36
7.6 Personnaliser le processus . . . . .	38
7.7 Traiter une image . . . . .	39
7.7.1 Histogramme . . . . .	40
7.7.2 Inverse couleur . . . . .	41
7.7.3 Filtre Passe haut . . . . .	41
7.7.4 Inverse sens de l'image . . . . .	42
7.7.5 Filtre median et moyenieur . . . . .	42
7.8 Aide . . . . .	43
7.9 Limites du programme . . . . .	44
7.10 Les regrets du programme . . . . .	44
<b>8 Organisation et communication</b>	<b>45</b>
8.1 Méthodes de communication . . . . .	45
8.2 Points forts et faibles . . . . .	45
8.3 Constitution de l'équipe . . . . .	46
8.4 Objectifs . . . . .	46
<b>9 Conclusion</b>	<b>47</b>
<b>10 Bibliographie</b>	<b>48</b>

# 1 Introduction

C'est quoi ton code secret ? A l'allure où vont les choses aujourd'hui, cette phrase sera bannie de votre vocabulaire d'ici 2030. En soit, le code secret est une bonne méthode pour s'identifier sur un ordinateur par exemple. Néanmoins, le code secret n'est pas infaillible, les algorithmes ne sont plus vraiment les mêmes qu'autrefois. Maintenant, ils ne se contentent pas de tester bêtement toutes les combinaisons possibles, ils commencent par les mots de passe les plus utilisés, puis utilisent quelques informations vous concernant afin de voir si vous n'avez pas été assez naïf pour utiliser votre date de naissance, ou le nom de votre frère comme mot de passe. De plus, ils ont un défaut, ils demandent un effort de mémorisation.

Un vite coup d'œil en classe afin de repérer les élèves ayant un portable qui permet la reconnaissance par empreinte digitale est suffisant pour s'apercevoir que toutes ces personnes là débloquent leur téléphone avec une faible pression sur un bouton : finis les mots de passe. Pourquoi un tel engouement pour ce procédé ? Ce rapport constitue une première analyse de cet art.

## 1.1 Histoire de l'utilisation des empreintes digitales

La police criminelle utilise les empreintes dans ses enquêtes depuis le XIXème siècle. En effet, le premier ouvrage qui établit l'unicité et la permanence des motifs est écrit en 1892 par Francis Galton. En 1912, l'étude des pores de la peau s'ajoute à la dactyloscopie pour résoudre des affaires criminelles. A la fin du XXème siècle, tous les fichiers d'empreintes sont centralisés par la police scientifique dans le FAED : le Fichier Automatisé des Empreintes Digitales (1987). En 2002, on y ajoute les empreintes palmaires suivant le même procédé.

Pour ce qui d'aujourd'hui, on retrouve les empreintes dans les passeports biométriques, mais seules deux empreintes doivent désormais être enregistrées dans la base centrale gérée par le ministère de l'intérieur, soit 30 minuties. Or, pour les criminels, elles sont conservées dans le FAED avec 15 minuties fiables pour les 10 empreintes, mais seulement 12 sont nécessaires à l'identification en réalité.

## 2 Différentes méthodes d'identification

### 2.1 La biométrie

La biométrie signifie : « mesure du vivant ». Dans le cas qui nous intéresse, on utilise le terme de biométrie quand on souhaite analyser l'identité d'une personne de manière certaine.

Afin d'identifier une personne, diverses techniques sont utilisées. Chacune d'elle nécessite une partie du corps particulière.

La plus connue des techniques de reconnaissance biométrique se base sur l'empreinte digitale. Son application la plus en vogue actuellement est le passeport dit "biométrique" qui est désormais associé à votre empreinte. Il image à lui seul le changement d'état d'esprit de la société qui souhaite identifier à tout va. Désormais, nous sommes des inconnus pour quasiment personne.

Néanmoins, les autres techniques ne sont pas en reste. La reconnaissance par empreinte digitale est très bien pour identifier une personne qui le souhaite, ou pour retrouver l'identité d'un criminel sur une scène de crime mais elle ne permet pas d'identifier tous les utilisateurs d'une ligne de métro simplement avec une caméra comme le permet la reconnaissance faciale.

Une biométrie simplifiée et efficace ouvrirait de nouvelles portes, peut être même que les attentats du 13 novembre dernier n'auraient jamais eu lieu si nous avions pu identifier les terroristes avant même qu'ils n'atteignent les lieux des massacres.

Cette partie passe en revue les principales méthodes de reconnaissance biométrique.

Il faut savoir que chaque année, plus de 210 000 personnes sont victimes d'une usurpation d'identité en France, et l'utilisation de la biométrie pourrait permettre de baisser ce chiffre du fait qu'elle amènerait une sécurité supplémentaire couplée à une certaine facilité d'utilisation.

## 2.2 L'iris



FIGURE 1 – Iris

Du fait de son caractère unique, l'iris est un parfait moyen d'identification biométrique. En effet, l'iris est la partie colorée, généralement bleu, vert, gris ou marron qui est, en fait, constituée de tubes très petits qui se croisent entre eux. Il est important de savoir que l'iris de chaque individu ne change quasiment pas au cours de notre vie ce qui en fait une méthode fiable d'identification, en ajoutant le fait que même des jumeaux ne peuvent avoir le même iris.

A l'aide d'une caméra, la position de l'iris dans l'œil va être trouvée puis on va scanner l'iris en entier. Par la suite, les tubes qui composent l'iris vont être analysés selon leur longueur, leur relief ou encore leur disposition pour, au final, relever 200 points distinctifs qui vont être envoyés et comparés dans une banque de données. L'image analysée est en noir et blanc, on ne prend donc pas la couleur en paramètre. Cela évite le problème du changement de couleur de l'iris qui s'opère chez certaines personnes qui peut être causé par un changement de lumière.

C'est donc une technique très performante d'identification, bien que compliquée à mettre en place dans la vie de tous les jours. En effet, il n'est que peu pratique d'aligner son œil sur un capteur pour déverrouiller son smartphone, cependant pour des objets plus gros comme une voiture ou même une maison, cela peut être une solution à envisager pour l'avenir.

## 2.3 La rétine

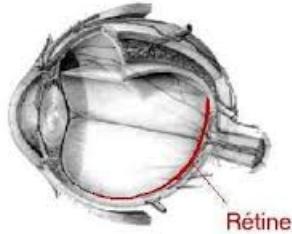


FIGURE 2 – Rétine

L’œil humain est composé de plusieurs éléments importants à son fonctionnement, comme l’iris vu précédemment. La rétine est également importante. En effet, elle joue le rôle d’un écran dans l’œil, ce qui signifie que tout ce que nous voyons et percevons par la vision se reflète dans la rétine et les images sont, par la suite, envoyées dans le cerveau pour que notre vision se mette en place. La composition de la rétine est très simple. Il y a une multitude de vaisseaux sanguins, que l’on appelle le réseau veineux rétinien. L’ensemble de ce réseau forme un dessin unique chez chaque individu.

L’avantage de cette méthode d’identification d’individu, dû au caractère unique de la rétine, est également le fait qu’il est très difficile voire impossible de créer un organe interne, comme l’est la rétine, pour frauder. Ce qui en fait donc une des méthodes les plus fiables et sûres au monde.

Ainsi, elle est aujourd’hui utilisée notamment pour des sites hautement sécurisés comme des sites militaires, et non pas dans le domaine public.

## 2.4 Le visage



FIGURE 3 – Visage

L'identification du visage se fait en plusieurs étapes. Tout d'abord, il faut pouvoir mettre en place l'analyse de l'image du visage par un logiciel. Donc dans un premier temps, il faut procéder à la capture de l'image du visage soit par une caméra photo, soit avec une caméra vidéo. Par la suite, cette image est envoyée dans le logiciel qui commence alors l'analyse.

Premièrement, le logiciel enregistre la position des yeux et leur alignement. Après s'être occupé des yeux, le logiciel relève plusieurs caractéristiques du visage comme la forme du menton, le positionnement du nez ou de la bouche. Ensuite, toutes ces informations sont enregistrées dans une base de données et elles pourront par la suite être utilisées dans le cas d'une autre capture comme celle-ci. Cette technique est l'une des plus simples et des plus acceptées dans la société car il suffit juste de se faire prendre en photo, comme pour une photo d'identité ou même une photo entre amis.

Cependant, c'est sans doute la moins précise du fait qu'elle est facile à contourner en mettant par exemple un chapeau, des lunettes de soleil, une fausse barbe ou des choses comme cela.

N'avons-nous pas omis un procédé d'identification ? Bien sûr ! Le plus connue de tous utilise l'empreinte digitale. Il sera développé plus en détail dans le reste du rapport.

## 3 La description d'une empreinte

### 3.1 Qu'est ce qu'une empreinte ?

Une empreinte digitale est une trace laissée par les doigts des mains ou des pieds au contact d'un objet. Elle se divise en deux catégories :

- les empreintes visibles à l'œil nu
  - les empreintes dites « latentes » laissées par les résidus, la sueur ou autres saletés présentes sur les doigts. Ces traces nécessitent souvent l'utilisation de certaines méthodes de révélation pour être exploitées.
- On réunit environ 95 % des empreintes digitales dans 3 groupes :
- les arches
  - les boucles ( à droite ou à gauche)
  - les tourbillons

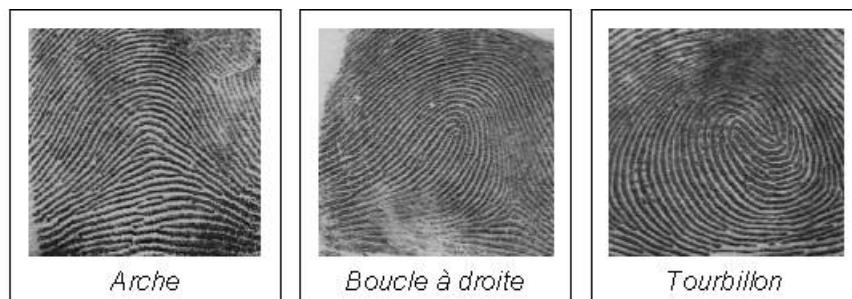


FIGURE 4 – Les Trois Catégories d'empreintes

Il en existe cependant des plus rares comme des empreintes dites en "double-spirales" par exemple :



FIGURE 5 – Les doubles spirales

### 3.2 La formation des empreintes

Comme expliqué précédemment, une empreinte se forme lors du contact des doigts avec un objet. Chaque individu a une empreinte spécifique et personnelle car cette empreinte dépend des motifs des doigts (or, les sillons et crêtes sont différents pour chaque individu). C'est pourquoi la police criminelle l'utilise dans ses enquêtes depuis le XIXème siècle.

Ces motifs apparaissent lors de la gestation, le fœtus perd ses coussinets et forme les motifs de ces doigts. Ils sont influencés par différents facteurs comme la pression sanguine, l'environnement, l'alimentation, etc. Ce sont ces différents facteurs qui rendent le procédé de création et donc la forme des motifs « hasardeuse », ainsi chaque personne mais aussi chaque doigt de cette personne possèdent un motif propre. Toutefois, il est important de noter qu'il existe une maladie extrêmement rare, appelée l'adermatolyphie, qui entraîne une absence totale d'empreintes digitales chez le malade. Autrement, même deux jumeaux similaires en tout point auront des empreintes différentes même si très proches l'une de l'autre : D'où la question de la police : A partir de quel pourcentage de concordance peut-on considérer une personne comme coupable ou du moins suspecte ?

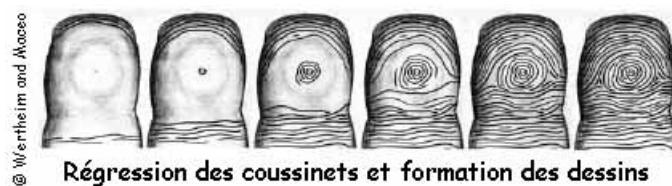


FIGURE 6 – Régression des coussinets et formation des dessins *Image tirée du site de la police scientifique*

### 3.3 A quoi servent les empreintes digitales ?

Les empreintes digitales sont utilisées dans la police criminelle pour trouver les coupables en comparant les empreintes recueillies sur la scène de crime

et celles de la base de données. On peut se demander à quoi nous servent-elles ?

Différentes études ont été faites à ce propos. L'une d'entre elles amène au fait que les dermatoglyphes ( motifs sur nos doigts ) servaient à mieux adhérer à la surface des objets. Mais elle a été mise en échec avec la preuve que sur certaines surfaces, ces dermatoglyphes réduisaient l'adhérence et qu'elles étaient trop petites pour avoir un réel impact. Une autre dit que les empreintes seraient des capteurs qui nous permettraient de mieux ressentir les objets de taille réduite tel que les cheveux sur un support ou encore ressentir les variations de texture entre différentes surfaces. En effet, au contact de ces objets ou textures, les crêtes présentent sur les motifs entreraient en vibrations ( légères bien sûr mais perceptible pour les nerfs présents sous la peau, les corpuscules de Pacini ). Nos sensations seraient ainsi décuplées et notre perception de l'environnement améliorée.

### **3.4 Les applications des empreintes**

Les empreintes digitales, en plus d'être utilisées par la police criminelle, sont utilisées dans le civil.

En effet, un peu plus d'un tiers des procédés biométriques se servent des empreintes digitales, que ce soit pour déverrouiller le coffre d'une banque ou un téléphone, un ordinateur sans taper le mot de passe. Les plus grandes entreprises spécialisées dans la recherche de nouvelles technologies se penchent sur le sujet afin de limiter le nombre d'oubli de mot de passe et de piratage enclenché par l'essor d'internet. Cette méthode jouit d'un gros succès auprès des entreprises car l'utilisation des empreintes digitales est plutôt bien perçue par l'opinion publique et que sa mise en application est peu coûteuse.

Mais il reste des réticences quant à l'utilisation des empreintes comme moyen d'identification. En 2008, le CNIL ( Commission Nationale de l'Informatique et des Libertés ) a refusé son utilisation dans les établissement scolaires. De plus, le CNIL limite l'utilisation des empreintes comme moyen de sécurité ( sauf impératif ) dans les entreprises en interdisant tout fichier central d'empreintes digitales. En effet, la crainte principale repose sur le fait qu'il est aisément de prélever à son insu l'empreinte de quelqu'un et donc d'usurper son identité via un faux doigt ou un autre type de substitution. De même, le

piratage des bases de données des empreintes peut entraîner une usurpation d'identité à grande échelle.

Au-delà de l'utilisation des simples empreintes digitales, la police se penche vers l'utilisation d'empreintes vocales, de l'iris ou de la rétine, ou encore génétiques.

La dernière application en date est de protéger l'accès à des contenus ou à des applications présentes sur un smartphone en utilisant ses empreintes digitales. Nous sommes ici dans la continuité du déverrouillage simple du téléphone grâce aux empreintes.

### 3.5 Les points faibles

Le point faible le plus important lors de l'utilisation d'un système exploitant les empreintes digitales est la netteté de l'image de l'empreinte. En effet, la propreté de l'empreinte joue un rôle important du fait qu'une empreinte d'un doigt propre sera plus lisible que l'empreinte d'un doigt sale (en supposant les mêmes conditions). De même si la peau est trop humide, trop sèche, trop huileuse ou trop abimée, l'image de l'empreinte sera grandement dégradée. Autre point important qui joue sur l'image, la pression que l'on met. Si l'empreinte utilisée a été créée avec une pression importante, elle sera nette mais si le doigt a juste effleuré la surface, l'empreinte sera très légère, avec peu de détails, et donc peu exploitable. L'objectif est d'avoir un système biométrique capable de tenir compte de ces aléas et pouvoir exploiter en toutes circonstances l'empreinte digitale.

Autre détail important à nos yeux. Nous parlons de reconnaissance d'empreintes digitales et au paragraphe précédent, de points faibles. L'un des principaux points faibles de la reconnaissance digitale est qu'elle est facilement "piratable". En effet, il est facile de tromper la reconnaissance de l'iPhone ou de n'importe quel téléphone avec de la patte à modeler ou bien avec une fausse empreinte en latex.

### 3.6 Minuties et points singuliers globaux

Aujourd'hui la classification n'est plus à l'ordre du jour car les fichiers automatisés détectent les vols d'identités. Malgré cela, les empreintes peuvent

être décrites, identifiées à l'aide d'un ancien système, celui de Henry. Ce système permet de définir différentes caractéristiques et familles telles que les boucles ( à gauche ou à droite ), les arches et les tourbillons.

Deux éléments permettent de différencier des empreintes digitales :

- Les points singuliers globaux : le noyau, c'est-à-dire le centre de l'empreinte et son delta, le lieu de divergence des stries. Les stries ou crêtes sont les lignes foncées qui caractérisent la forme de l'empreinte.
- Les minuties : Cela désigne les particularités des empreintes digitales ( bifurcations, terminaisons, lac, etc. ) qui seront traitées dans le processus d'authentification. Il en existe 12 sortes mais seulement 5 sont utiles à la reconnaissance. De nos jours, les plus fréquentes sont les bifurcations.

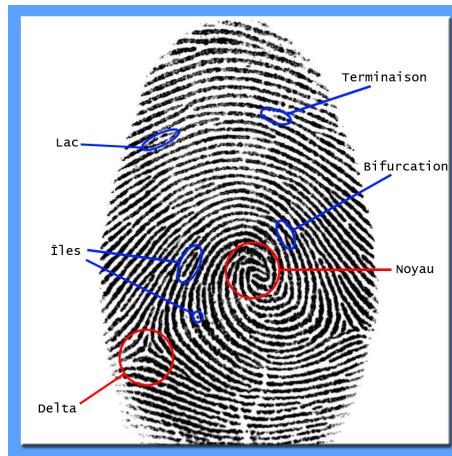


FIGURE 7 – Empreinte digitale avec minuties et points singuliers globaux

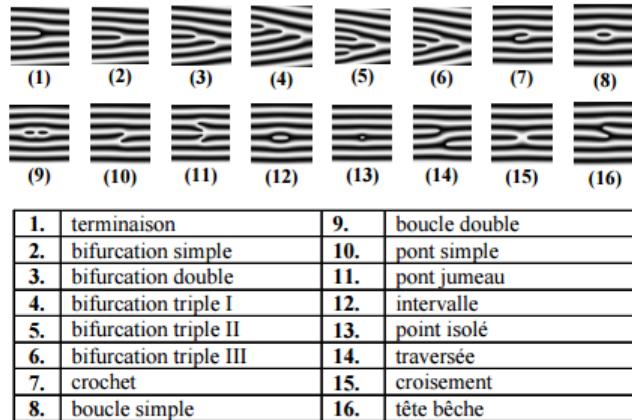


FIGURE 8 – Les différentes minuties

### 3.7 Signature de l'empreinte

A l'heure actuelle, selon la législation, seulement 12 minuties parmi les centaines que nous possédons permettent d'identifier une personne. Pour assurer le coup, l'ordinateur conserve les 15 minuties les plus fiables.

Cependant il est encore possible que deux signatures soient similaires, c'est-à-dire que les 15 minuties conservées ne permettent pas de départager un individu de l'autre. En effet, il est très compliqué de différencier les signatures de deux jumeaux comme nous l'avons déjà évoqué.

On pourrait bien sûr étudier les centaines de minuties de chacun des individus pour être certain du résultat. Mais cela demanderait une capacité de stockage beaucoup trop importante. En effet, une minutie est conservée sous 16 octets. Si on devait conserver les 100 minuties par empreinte de chaque Français (environ 65 millions), on obtiendrait un fichier beaucoup trop lourd et le temps de recherche serait conséquent.

Ainsi, pour éviter ce genre de mésaventure, l'ordinateur conserve les signatures les plus pertinentes à l'aide d'un algorithme de tri. Ensuite l'être humain doit être en mesure de distinguer quelle empreinte sera la plus adaptée à ses besoins.

### 3.8 Probabilité de trouver deux empreintes identiques

Comme nous l'avons énoncé précédemment, il y a environ 100 minuties par empreinte. Or pour avoir une valeur juridique, il est nécessaire que l'empreinte possède 12 points de concordances. En outre, la probabilité de trouver deux empreintes similaires est quasiment impossible, une chance sur 64 milliards selon les calculs du célèbre anthropologue Francis Galton. Ainsi, on comprend la raison du succès de la dactyloscopie, qui consiste à identifier les individus par leurs empreintes digitales. Ce système reste aujourd'hui l'un des moyens les plus utilisé pour différencier les individus les uns des autres.

**Comment Francis Galton est-il arrivé à ce résultat ?**

$$P(C) = A \times B \times C = \frac{1}{2^{24}} \times \frac{1}{2^4} \times \frac{1}{2^{36}} \approx 1.45 \times 10^{-11}$$

Avec :

- A : Probabilité de reconstituer correctement une configuration spécifique d'empreinte.
- B : Probabilité d'un type de forme spécifique.
- C : Probabilité de reconstituer le bon nombre de lignes crêtes entrant et sortant d'un carré.

Or  $2^{10} \approx 1000$  donc  $2^{36} \approx 64 \times 10^9$

$$\Rightarrow P = \frac{1}{64 \times 10^9}$$

Soit une chance sur 64 milliards que deux doigts distincts possèdent les mêmes empreintes digitales.

## 4 Comment relever une empreinte ?

Les empreintes digitales sont, de nos jours, un fabuleux moyen d'attester du passage d'un individu dans un endroit, ou encore de justifier de l'utilisation d'un objet, ce qui sert énormément dans le domaine judiciaire. Il existe deux manières de relever une empreinte : la manière volontaire ou la manière involontaire.

### 4.1 Relevé involontaire

Le relevé est dit involontaire lorsque les personnes dont on récupère les empreintes ne sont pas forcément au courant. Par exemple, si on découvre une victime dans un endroit donné, on va procéder à un relevé d'empreinte involontaire du fait que non seulement les empreintes du coupable vont être relevées, mais également celles de toutes les autres personnes ayant fréquentées ce lieu.

Il y a plusieurs cas de figures quant au prélèvement de ces empreintes. En effet, s'il existe des traces visibles à l'œil nu, alors on peut simplement prendre une photographie. Dans le cas contraire, c'est un peu plus compliqué. Effectivement, une poudre très fine composée de céruse, d'alumine, d'oxyde de cuivre et de poudre magnétique appliquée à l'aide d'un pinceau va permettre de faire ressortir les empreintes. On peut également noter le fait qu'il y a une couleur correspondant à un certains types de surface : de la poudre noire pour les surfaces blanches, de la poudre blanche pour les surfaces lisses, de la poudre fluorescente pour les fonds multicolores.



FIGURE 9 – Prélèvement d'empreinte

Une fois que l'empreinte devient visible à l'œil nu, elle doit être photographiée comme une empreinte visible dès le départ dans le but d'être numérisée par la suite. C'est à dire de convertir les informations de notre

support, la photo, en données numériques que des dispositifs informatiques pourront traiter.

## 4.2 Le relevé volontaire

A l'opposé du relevé involontaire, le relevé volontaire requiert une autorisation de la personne qui va se faire relever ses empreintes. De ce fait, la capture est plus facile. Il n'y a plus à fouiller de fond en comble une maison pour retrouver une empreinte quasiment inutilisable, mais simplement à poser ses doigts sur un capteur lors d'un renouvellement de carte d'identité par exemple.

Il existe d'ailleurs 3 types de capteurs : les capteurs optiques, les capteurs à silicium, et que les capteurs thermiques. Ces capteurs ont pour but de numériser l'empreinte, avant de la traiter sur ordinateur dans le but de vérifier que cette empreinte n'appartient pas à quelqu'un recherché par la police par exemple.

Dans un cadre criminel, les empreintes sont stockées dans le Fichier Automatisé des Empreintes Digitales (FAED), créé en 1987, qui a pour but de répertorier toutes les empreintes digitales appartenant aux auteurs de crimes ou de délits. Le but étant de comparer les empreintes trouvées sur le terrain avec ce fichier dans le but de savoir si une personne est coupable ou non. Ce fichier contient également des traces non identifiées présentes sur le terrain. Il se caractérise par 5 éléments : état civil de la personne arrêtée, motif de l'arrestation, date et lieu et signalisation, éléments de signalement et, enfin, les caractéristiques d'empreintes digitales.

Ces informations sont conservées durant 25 ans au plus pour les personnes, 3 ans pour les traces en rapport avec des délits et 10 ans pour des traces en rapport avec des crimes.

## 5 Traitement informatique de l'empreinte

### 5.1 Généralités

Une empreinte digitale est avant tout une image. Une image peut être modélisée par une matrice de pixels où chaque pixel est la combinaison de 3 couleurs RVB (rouge, vert et bleu). Les images codées en RVB sont souvent en 24 bits (8 bits 3x). L'intensité de chacune des couleurs ci-dessus varie entre 0 et 256 (8 bits). Si les trois couleurs sont à 256 : 256 x 256 x 256, alors la couleur du pixel est blanche. Si les trois couleurs sont à 0 : 0 x 0 x 0, alors la couleur du pixel est noire. Afin de faciliter le travail et dans un soucis de compression, on ne travaillera pas avec une image codée avec 24 bits mais plutôt avec une image en niveau de gris (8 bits=1 octet).



FIGURE 10 – Transformation d'une image en niveau de gris

### 5.2 Séparation

La première étape est la séparation. Pour analyser l'empreinte, ne sont nécessaires que les rides. Tout ce qui se trouve à l'extérieur et entre les rides ne nous intéresse pas. On effectue donc un travail de séparation de la partie qui nous intéresse et du reste.

La base de données d'empreintes fournie par le professeur est limitée et l'étape de séparation a déjà été effectué. Cependant, nous devons implémenter une fonction qui fasse cette étape préliminaire.

### 5.3 Egalisation d'histogramme

Ainsi, afin de faire ressortir les informations importantes, nous procéderons à une égalisation de l'histogramme qui permet de faire ressortir les informations importantes. Elle permet un ajustement du contraste qui utilise l'histogramme.

Pour cela, on calcule le nombre de pixel ayant tel niveau de gris :

Grey levels	0	1	2	3	4	5	6	7
$n_i$	6	14	0	0	7	4	2	18

FIGURE 11 – Nombre de pixels par niveau de gris

En l'occurrence dans notre exemple, le niveau de gris de la photo va de 0 à 7. Pour chaque niveau de gris, on associe la valeur suivante :

$$\frac{\text{max\_gray\_level}}{\sum_{i=1}^n n_i} * \sum_{i=1}^i n_i$$

On prend la valeur arrondie de ce nombre et on donne cette valeur au pixel.

Grey Level i	$n_i$	$\sum n_i$	$(7/51) \sum n_i$	Rounded Value
0	6	6	0.823	1
1	14	20	2.745	3
2	0	20	2.745	3
3	0	20	2.745	3
4	7	27	3.705	4
5	4	31	4.254	4
6	2	33	4.529	5
7	18	51	7	7

On a alors une nouvelle répartition :

Original Grey levels	0	1	2	3	4	5	6	7
New Grey Level	1	3	3	3	4	4	5	7

Voici un exemple d'égalisation :



FIGURE 12 – Mauvais contraste

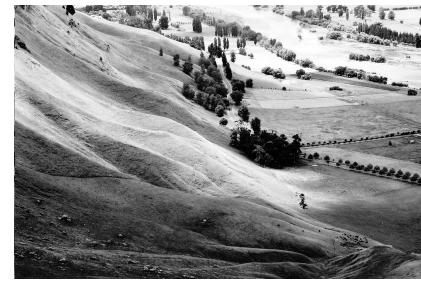


FIGURE 13 – Après égalisation

Une empreinte digitale est une des images ayant le plus de bruit. C'est notamment dû au fait que les doigts sont les intermédiaires pour toutes les taches que nous faisons au cours de la journée. Les doigts deviennent donc sales, coupés, humides, secs ... C'est donc pour cela qu'une étape est indispensable : le filtrage (« image enhancement » en anglais).

#### 5.4 Filtre Passe-Haut

Maintenant que les contrastes de l'image sont bons. On utilise un filtre passe-haut dont le noyau de convolution est le suivant :

0	-1	0
-1	5	-1
0	-1	0

FIGURE 14 – Filtre de convolution

$P_9$ $(i - 1, j - 1)$	$P_2$ $(i - 1, j)$	$P_3$ $(i - 1, j + 1)$
$P_8$ $(i, j - 1)$	$P_1$ $(i, j)$	$P_4$ $(i, j + 1)$
$P_7$ $(i + 1, j - 1)$	$P_6$ $(i + 1, j)$	$P_5$ $(i + 1, j + 1)$

FIGURE 15 – Matrice de voisinage

Ainsi, admettons que pour chaque pixel nous ayons la matrice ci-dessus ( où le pixel en question est le pixel au centre ). Si nous appliquons le noyau ci-dessus, on a alors :  $P1=(-1)*P2+(-1)*P4+(-1)*P6+(-1)*P8+5*P1$

## 5.5 Filtre median

Chaque pixel possède huit voisins. On peut illustrer le voisinage par cette matrice

$P_9$ $(i - 1, j - 1)$	$P_2$ $(i - 1, j)$	$P_3$ $(i - 1, j + 1)$
$P_8$ $(i, j - 1)$	$P_1$ $(i, j)$	$P_4$ $(i, j + 1)$
$P_7$ $(i + 1, j - 1)$	$P_6$ $(i + 1, j)$	$P_5$ $(i + 1, j + 1)$

FIGURE 16 – Matrice de voisinnage

On prend chacun des pixels et on les ajoute dans un tableau. Puis on trie les pixels par ordre croissant en fonction de l'intensité de niveau de gris. Enfin on attribue au pixel[i,j] le cinquième élément du tableau trié.

Exemple :

5	10	12
4	9	3
7	2	1

Le tableau trié :

1	2	3	4	5	7	10	12
---	---	---	---	---	---	----	----

On attribue donc au pixel la valeur de 5. L'usage du filtre médian et du filtre passe-haut aura pour but de réduire le bruit. Voici un exemple de filtre médian sur une empreinte de la base de données fournie :



FIGURE 17 – Filtre de convolution



FIGURE 18 – Matrice de voisinage

## 5.6 Binarisation de l'image

La binarisation de l'image correspond tout simplement à la transformation d'une image en niveau de gris en une image bicolore ( noire et blanche ). La valeur  $k$ , qui détermine la limite entre un futur pixel noir ou blanc, sera déterminée par l'expérience. Pour l'instant, nous l'avons fixé à 200.

Voici un exemple de transformation d'une empreinte originalement en niveau de gris en bicolore.



FIGURE 19 – Filtre de convolution



FIGURE 20 – Matrice de voisinage

## 5.7 Filtre directionnel

Le problème qui se pose maintenant est un problème majeur. La personne dont nous prenons l'empreinte peut ne pas suffisamment appuyer. Dans ce cas, les rides ne sont pas continues. Et donc on observe beaucoup de minuties (surtout des terminaisons) qui n'ont pas lieu d'être.

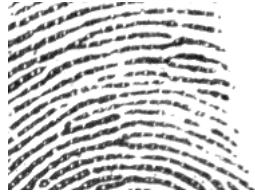


FIGURE 21 – Rides non continues

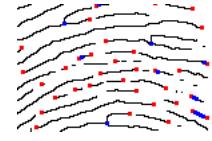


FIGURE 22 – Terminaisons

C'est pourquoi on utilise un filtre directionnel. Parmi ces filtres, on retrouve les filtres de Gabor ou la transformée de Fourier puis transformée de Fourier inverse.



C'est cette seconde solution que nous retiendrons. La transformée de Fourier est très souvent utilisée pour le traitement d'image. Comme l'empreinte a une structure de lignes parallèles qui se répètent, il est possible de déterminer la fréquence et l'orientation des rides en utilisant la FFT ( Fast Fourier Transform ). Rappelons ici qu'il y a deux transformée de Fourier : la transformée de Fourier discrète ( ou low ) car elle n'est pas optimisée et la FFT.

On divise alors l'image en blocs de 32x32. Pour chaque bloc, on applique la FFT puis on le multiplie par 2. Enfin on calcule sa transformée de Fourier inverse.

2D DFT :

$$F(k_x, k_y) = \frac{1}{\sqrt{N_x N_y}} \sum_{n_x=0}^{N_x-1} \sum_{n_y=0}^{N_y-1} f(n_x, n_y) e^{-j2\pi k_x n_x / N_x} e^{-j2\pi k_y n_y / N_y}$$

2D IDFT :

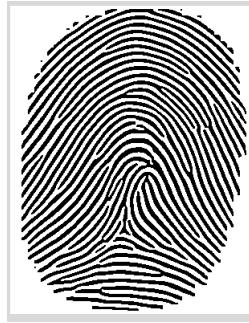
$$f(n_x, n_y) = \frac{1}{\sqrt{N_x N_y}} \sum_{k_x=0}^{N_x-1} \sum_{k_y=0}^{N_y-1} F(k_x, k_y) e^{+j2\pi n_x k_x / N_x} e^{+j2\pi n_y k_y / N_y}$$

Voici le résultat :



Comme vous le voyez, les lignes sont désormais continues et donc la détection des minuties est simplifiée. Les fausses minuties se feront donc beaucoup plus rares.

A ce niveau, l'idéal est d'avoir une empreinte de cette qualité :



## 5.8 Squelettisation

Dans l'image binarisée ( noire et blanche ) les lignes se voient clairement mais elles ont des tailles différentes. Pour pouvoir détecter rapidement les minuties ( terminaisons, bifurcations ), il est nécessaire d'obtenir une image dans laquelle toutes les lignes ont la même épaisseur ( 1 pixel ). Il existe

plusieurs algorithmes de squelettisation. Nous avons choisi celui de Zhang-Suen's car il était le plus facile à mettre en place.

Comme nous l'avons vu avant, nous pouvons décomposer chaque pixel sous la forme d'une matrice de 3X3. La case du milieu est le pixel en question et les 8 autres membres sont son voisinage.

$P_9$ $(i - 1, j - 1)$	$P_2$ $(i - 1, j)$	$P_5$ $(i - 1, j + 1)$
$P_4$ $(i, j - 1)$	$P_1$ $(i, j)$	$P_6$ $(i, j + 1)$
$P_3$ $(i + 1, j - 1)$	$P_8$ $(i + 1, j)$	$P_7$ $(i + 1, j + 1)$

Voici les conditions pour l'algorithme de Zhang-Suen's pour supprimer un pixel : ( $P_i = 0$  s'il est blanc et 1 s'il est noir )

- 1- Si le nombre de pixels voisins noirs parmi les 8 est compris entre 2 et 6
- 2- Si l'une des affirmations suivantes est vraie
  - $P_2 \times P_4 \times P_6 = 0$  ( l'un de ces trois pixels est blanc )
  - $P_2 \times P_4 * P_8 = 0$
- 3- Si l'une des affirmations suivantes est vraie
  - $P_4 \times P_6 \times P_8 = 0$
  - $P_2 \times P_6 \times P_8 = 0$
- 4- Le nombre de passage de 0 à 1 quand on parcours les voisins de  $P_2$  à  $P_9$  ( dans le sens des aiguilles d'une montre ) est égal à 1.

Si les 4 affirmations sont vraies alors on peut supprimer le pixel en question.

Voici une squelettisation réalisée avec l'algorithme de Zhang-Suen's que nous avons implémenté. Nous avons donc maintenant une empreinte dont tous les traits ont la même épaisseur. La reconnaissance des minuties devient plus facile. Néanmoins, comme nous avons bien commencé le programme et après avoir lu des avis sur plusieurs forums, nous soulignons que l'algorithme de squelettisation de Zhang-Suen's n'est pas parfait. En effet, il a tendance à ne pas vraiment suivre les courbes des rides mais plutôt de faire des traits droits.

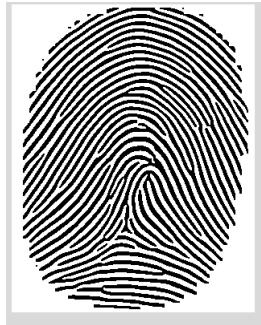


FIGURE 23 – Empreinte binarisée

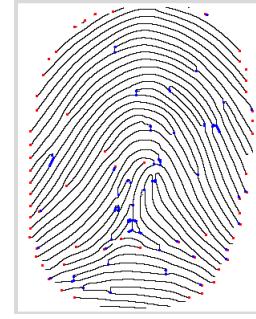


FIGURE 24 – Empreinte squelettisée

## 6 Comparaison de deux empreintes

Comme nous l'avons dit plus haut, on ne peut pas comparer chaque pixel de deux empreintes car il y a beaucoup de facteurs qui influent sur le rendu d'une empreinte : l'orientation du doigt, la force de pression sur le capteur, une cicatrice présente ... Il y a deux manières de comparer des empreintes. La première approche est basée sur les rides. On compare la forme des rides ainsi que leur texture et leur direction.

La deuxième approche est celle que nous avons retenu. C'est aussi la méthode la plus utilisée par les entreprises spécialisées dans la reconnaissance d'empreintes digitales. On identifie les différentes minuties sur l'empreinte. Comme nous l'avons vu précédemment, il y a plusieurs types de minuties sur une empreinte. Nous nous intéresserons à deux types : la bifurcation et la terminaison.

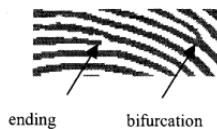


FIGURE 25 – Deux types de minuties

L'image ci-dessus est juste un zoom d'une empreinte classique. Dans la partie précédente, nous avons vu que nous squelettisions l'empreinte afin que chaque ride ait la même épaisseur. On peut donc travailler de manière plus

méthodique. Désormais, les bifurcations seront donc des pixels qui possèdent trois voisins et les terminaisons des pixels n'en ayant qu'un seul. Cependant, la squelettisation apporte parfois des minuties qui n'ont pas lieu d'être comme des ponts entre deux rides. On appelle cela des fausses minuties et il faut les enlever. En fait, trop de minuties dans une petite région est souvent un signe indiquant de fausses minuties engendrées par le bruit.

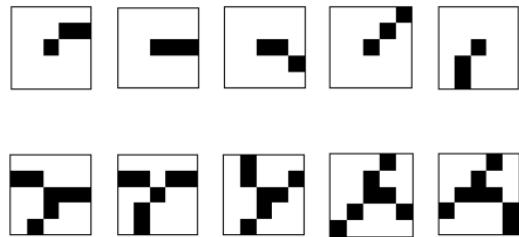


FIGURE 26 – Minuties sous forme pixelisées

## 6.1 Comparer les minuties

Nous allons donc comparer les minuties. Pour cela nous allons avoir besoin des coordonnées sur l'image de chaque minutie.

Cependant, vous vous dîtes probablement que les empreintes peuvent être positionnées différemment sur l'image. Par exemple, l'une peut être centrée et l'autre non, ainsi les coordonnées de chaque pixel ne correspondraient pas du tout : vous avez tout à fait raison !

C'est pour cela que nous ne comparons pas deux empreintes sur les coordonnées de chaque bifurcation mais plutôt sur un ratio. Voici un exemple de fichier signature d'une empreinte ( fichier issu d'une signature de l'une des empreintes de la base de données fournie ) :

```
0.434 0.533 0.566 0.467  
0.438 0.513 0.562 0.487  
0.443 0.572 0.557 0.428  
0.445 0.513 0.555 0.487  
0.451 0.397 0.549 0.603  
0.464 0.669 0.536 0.331  
0.484 0.555 0.516 0.445  
0.49 0.907 0.51 0.093
```

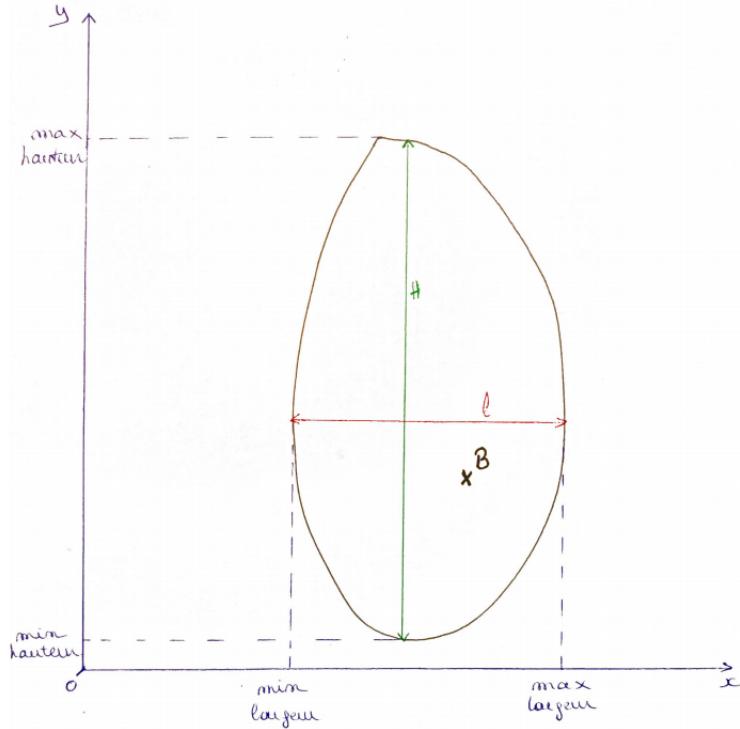
Chaque ligne correspond à une bifurcation. Vous vous demandez peut-être à quoi correspond chacun des chiffres ? En fait, l'opération que nous faisons est ce que l'on peut appeler : « centrer-réduire ».

On peut faire un parallèle avec la loi normale. Pour la loi normale, si nous souhaitons la centrer réduire, il faut d'abord soustraire la moyenne, puis diviser par la variance. Dans notre cas, l'opération est très ressemblante.

Voici le schéma un peu grossier d'une empreinte :

Sur le schéma ci-dessus, l'empreinte est caractérisée par plusieurs données :

- $x_{min}$ =Largeur minimale
- $x_{max}$ =Largeur maximale
- $y_{min}$ =Hauteur minimale
- $y_{max}$ =Hauteur maximale
- $l$ =largeur de l'empreinte= $x_{max} - x_{min}$
- $H$ =Hauteur de l'empreinte= $y_{max} - y_{min}$



Pour chaque empreinte, nous allons déterminer les 6 données en question, puis nous allons centrer et réduire.

Au final nous aurons 4 données pour chaque bifurcation dans notre signature (a,b,c,d). Soit B(x,y) une bifurcation, voici les opérations faites :

$$a = \frac{x - x_{min}}{largeur}$$

$$b = \frac{y - y_{min}}{hauteur}$$

Ainsi, nous avons la position de x par rapport à la bordure de gauche ( $x_{min}$ ) et la position de y relative à la bordure du bas ( $y_{min}$ ).

Désormais, nous souhaitons avoir la position de x par rapport à la bordure de droite ( $x_{max}$ ) et celle de y par rapport à la bordure du haut ( $y_{max}$ ) :

$$c = \frac{x_{max} - x}{hauteur}$$

$$b = \frac{y_{max} - y}{hauteur}$$

Une fois ces 4 données calculées, nous les inscrivons pour chaque bifurcation de l'empreinte. Au sein de la police, seul un petit nombre de bifurcations sont retenues car la qualité des bifurcations et surtout des étapes préliminaires ( les étapes sur le traitement de l'image ) est au rendez-vous. En effet, ils appliquent des filtres directionnels notamment, qui leur permettent d'avoir une squelettisation quasiment parfaite.

Dans notre cas, n'étant pas limité par la quantité de données et ne disposant pas de filtres nous rassurant quant à la qualité de l'empreinte finale, nous garderons toutes les bifurcations. Ainsi nos fichiers signatures sont souvent de l'ordre d'une cinquantaine de lignes ( et donc de bifurcations ).

Nous sommes maintenant capable de déterminer le fichier signature d'une empreinte !

## 6.2 La vraie comparaison

Vous l'aurez deviné, c'est le final du processus. Maintenant, il s'agit de comparer deux fichiers signatures. Rien de plus simple dans notre cas.

Lors de la comparaison, nous stockons dans un tableau toutes les coordonnées de chaque bifurcation.

Ainsi il ne reste qu'à comparer les deux tableaux. Pour cela, nous avons deux modèles. Le premier équivaut à dire que la valeur absolue de la différence de chaque coordonnées respective soit inférieure à 0,008.

Le second modèle, moins restrictif, vérifie que la somme des différences citées précédemment est inférieure à 0,025.

Finalement, nous vérifions combien de minuties ont été trouvées par chacun des deux modèles, puis faisons la moyenne des deux.

Mais pour vraiment comprendre, rien de mieux qu'un exemple :

Voici une ligne de deux signatures différentes :

0.421 0.36 0.579 0.64

0.503 0.572 0.497 0.428

Modèle 1 :

Reprendons les notation (a,b,c,d), et appelons la première signature A et la seconde B :

$ A.a-B.a = 0,421-0,523 =0,082$	Pas vérifié
$ A.b-B.b = 0,36-0,572 =0,082$	Pas vérifié
$ A.c-B.c = 0,579-0,497 =0,082$	Pas vérifié
$ A.d-B.d = 0,64-0,428 =0,212$	Pas vérifié

Toutes les différences sont inférieures à 0,008 donc les deux bifurcations sont différentes.

Modèle 2 :

Epargnons-nous les calculs des différences puisque nous les avons calculées juste avant. La différence ici est que nous les additionnons.

$$|A.a-B.a|+|A.b-B.b|+|A.c-B.c|+|A.c-B.c|=0,082 +0,082 + 0,082 + 0,212=0,588>0,025$$

Ici aussi notre modèle n'est pas vérifié.

Maintenant admettons qu'entre deux signatures, le nombre de minuties identiques trouvé par le premier modèle soit de 8 et de 16 par le second modèle. Nous faisons donc la moyenne des deux qui est égale à 12.

**Or, deux empreintes ne sont considérées identiques que si un minimum de 12 minuties correspondent. Ainsi, on conclut dans cet exemple que les deux empreintes sont identiques.**

## 7 Les fonctionnalités du programme

Auparavant, nous avons décrit de manière précise les modalités de chaque étape du processus ( ex : comment à lieu la squelettisation ). Dorénavant, nous allons parler du programme et passer en revue les différentes fonctionnalités qu'il offre.

### 7.1 Petit rappel sur le processus

- On applique sur ces deux empreintes un filtre médian. Après de nombreux essais, il se révèle être le meilleur.
- Puis on squelettise l'empreinte en utilisant l'algorithme de Zhang-Suen's afin que chaque ride ait une épaisseur d'un pixel.
- Finalement, on identifie les minuties et notamment les bifurcations. Celles-ci sont facilement remarquable car elles sont identifiables par un pixel ayant 3 voisins.
- Ainsi pour une empreinte, nous allons enregistrer sa signature dans un fichier texte. C'est à dire que nous allons inscrire dans un fichier texte les coordonnées exactes de la bifurcation.
- Ainsi lorsque nous souhaitons comparer deux empreintes, on ne compare plus deux images mais deux signatures. Ensuite, il ne reste qu'à déterminer si l'emplacement de chaque bifurcation d'une empreinte correspond à celui de l'autre empreinte.

### 7.2 Précision sur le programme

Depuis le début du rapport, nous parlons de deux types de minuties : bifurcations et terminaisons. Après de nombreux essais et compte tenu de la squelettisation souvent imparfaite, nous n'avons pas tenu compte des terminaisons car celles-ci sont beaucoup plus nombreuses et davantage soumises au bruit.

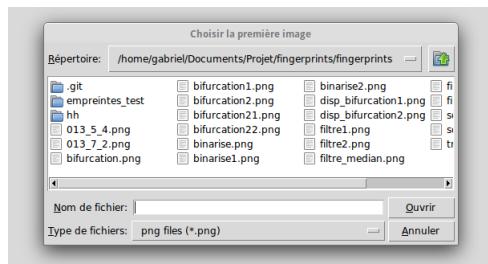
La consigne demandait de faire l'intégralité du traitement de l'image en C++ et l'interface graphique en Python.

Ainsi, tout ce qui vient d'être dit est uniquement en C++. Le C++ communique le résultat au Python via un fichier texte qui contient uniquement le nombre de minuties communes. Le programme python n'a donc juste qu'à

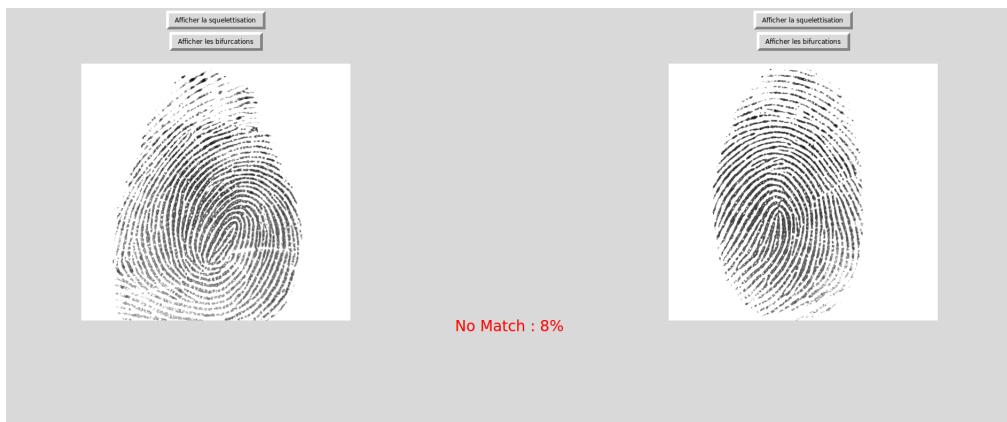
vérifier si ce résultat est supérieur au minimum légal qui est actuellement de 12 minuties.

### 7.3 Comparer deux empreintes

Le programme prend en entrée deux empreintes :



Puis fait les opérations citées au dessus et voici le résultat affiché à l'écran :

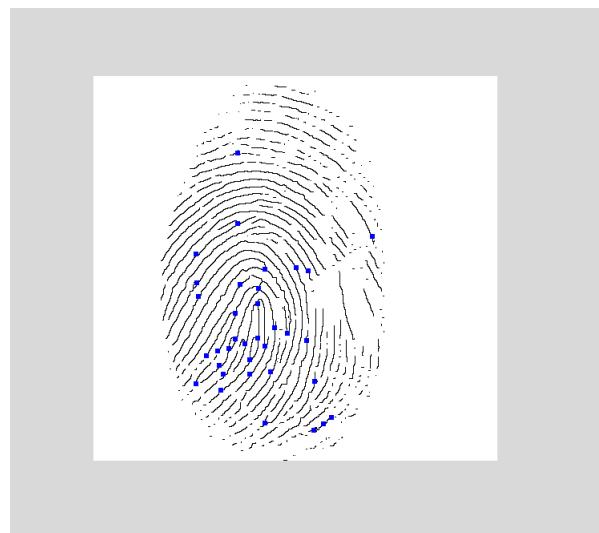


Par soucis de transparence vis à vis de l'utilisateur, nous montrons l'état de la squelettisation ainsi que les bifurcations trouvées. Ainsi, l'utilisateur peut juger par lui-même si toutes les opérations semblent correctes. **Nous invitons même l'utilisateur à visionner ces images.** Voici un exemple avec l'empreinte située à droite de l'image

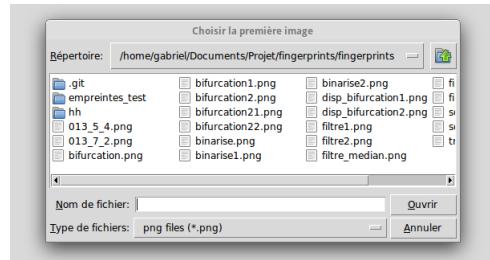
Voici ce qui se passe quand nous appuyons sur « squelettisation » :



Puis quand nous appuyons sur « bifurcations » :

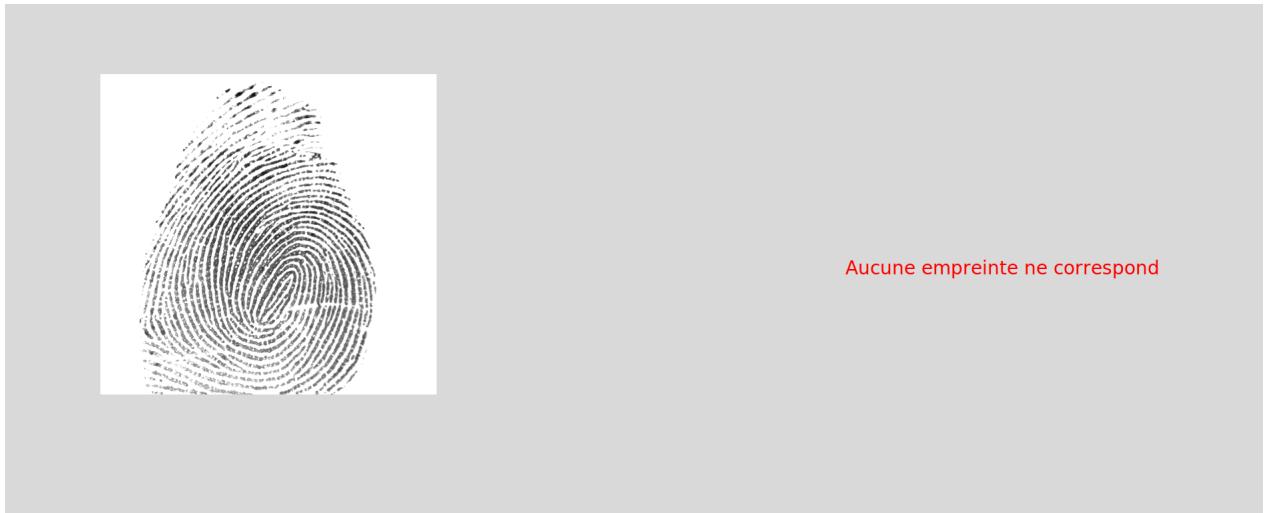


## 7.4 Comparer une empreinte avec un répertoire

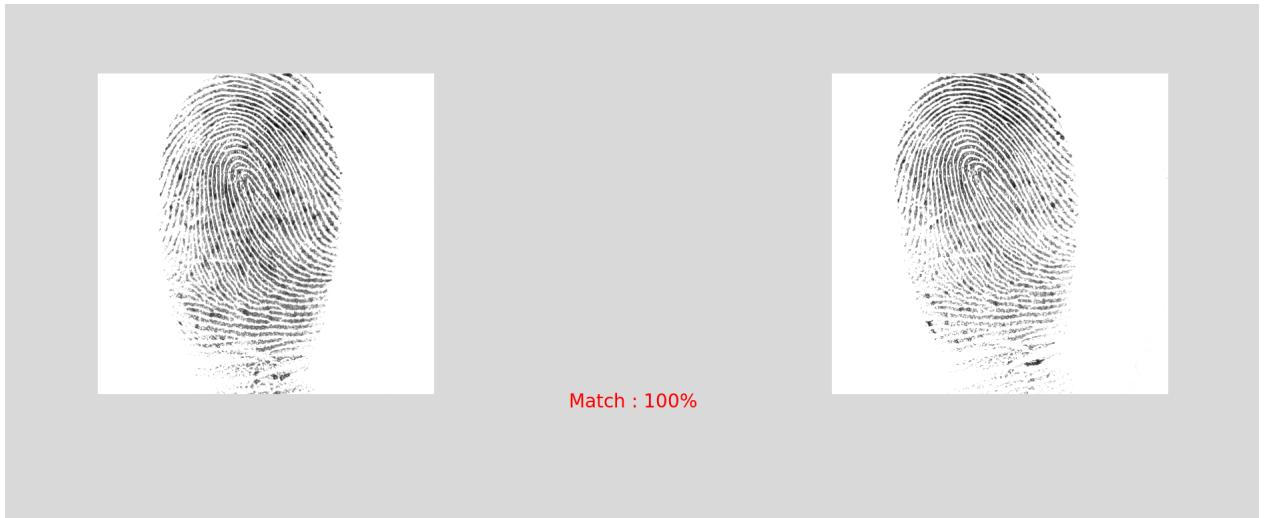


Choisissez donc une empreinte ainsi qu'un répertoire. Le programme va répéter le processus précédent pour toutes les empreintes contenues dans le répertoire puis va donner celle qui aura plus de 12 minuties correspondantes. Si elles sont plusieurs à satisfaire ce critère, le programme renverra celle qui aura le plus de minuties parmi toutes celles-ci.

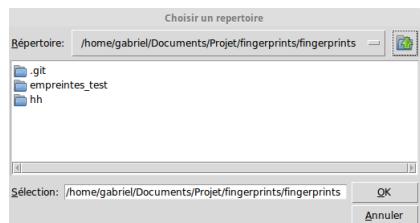
Voici un exemple de résultat négatif :



Voici un résultat positif



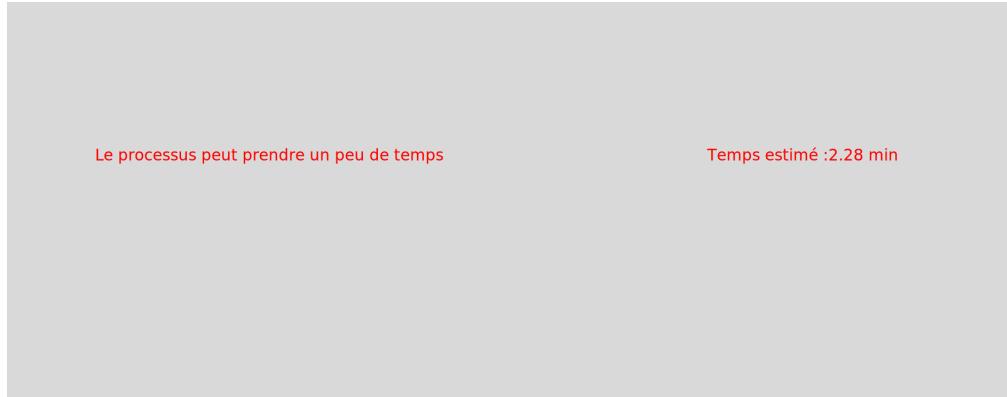
## 7.5 Retrouver les empreintes d'une même personne dans un répertoire



Vous choisissez le répertoire que vous souhaitez explorer.

Le fonctionnement du processus est assez simple. Il faut chercher pour chaque empreinte du répertoire, les empreintes qui satisfont notre critère (12 minutes). Puis, si une empreinte a trouvé une ou plusieurs empreintes similaires, elles sont toutes mises dans le même dossier ( nommé par un chiffre ). Si une empreinte n'a pas trouvé d'empreinte satisfaisant notre critère, elle est mise dans le dossier nommé « Orphelines ».

Le processus prend un peu de temps et beaucoup de ressources de l'ordinateur.



Voici le résultat (dans votre explorateur) :



Nous avions initialement 10 empreintes. Le programme réussit à regrouper dans 6 dossiers des empreintes différentes. Les empreintes restantes sont réunies dans le dossier « Orphelines ».

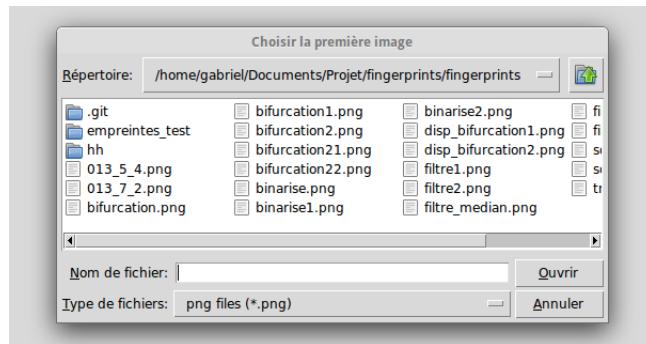
Cependant, vous noterez que le compte n'y est pas. En effet, c'est une des limites du programme. Nous y reviendrons plus tard.

## 7.6 Personnaliser le processus

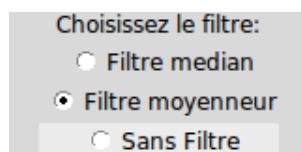
Cette fonction permet de choisir le filtre à appliquer. En effet lorsque vous choisissez de comparer une empreinte avec le premier mode, le filtre appliqué est le filtre médian car c'est lui qui fait le mieux le travail selon nous.

Ainsi, dans ce mode, vous avez trois choix. Vous pouvez appliquer le filtre médian, le filtre moyenneur ou ne pas mettre de filtre. Ce dernier choix est conseillé si votre empreinte a par exemple déjà été filtrée mais déconseillé si ce n'est pas le cas. En effet le filtre permet de combler beaucoup de défauts ( ex : les pores de l'empreinte ) qui vont entraîner un nombre conséquent de minuties qui n'ont pas lieu d'être.

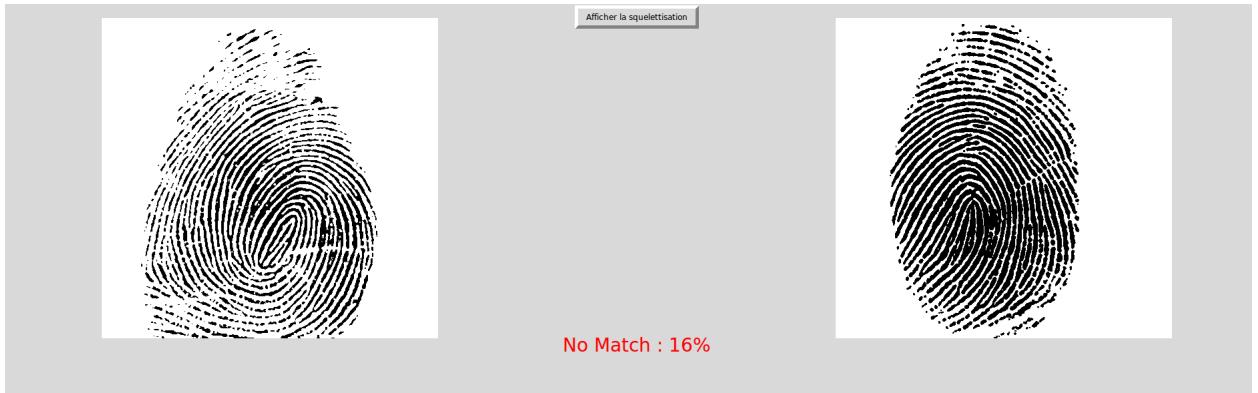
Choisissez d'abord les deux images que vous souhaitez traiter :



Une fois que les deux empreintes ont été choisies, choisissez le filtre :



Voici un exemple de résultat :



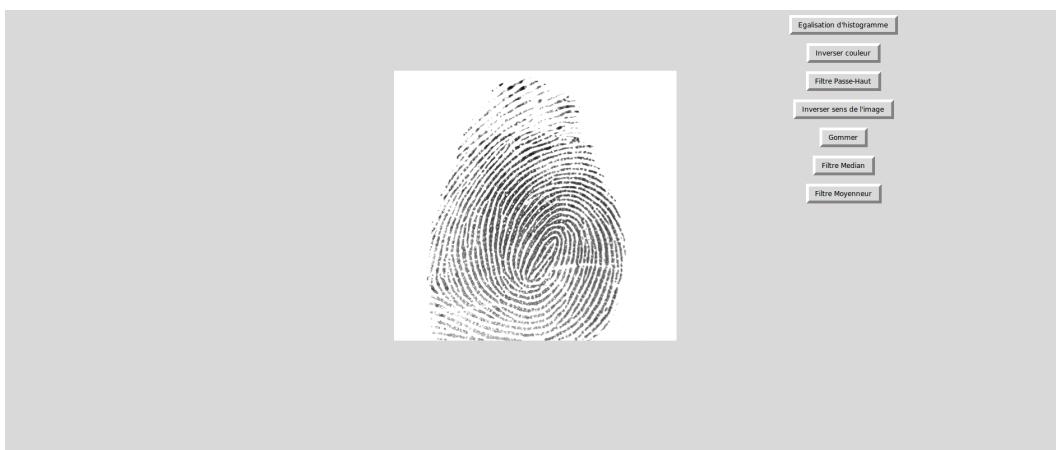
Un filtre médian a été choisi à gauche et un filtre moyenieur à droite.

## 7.7 Traiter une image

Ce mode vous permet de traiter une image indépendamment. Cette partie est en version alpha (encore en développement). Il manque certaines options comme la 'gomme' (qui est en développement).

Elle vous permet par exemple de voir à l'avance quel sera le résultat d'un filtre médian, d'un filtre moyenieur... .

Voici le choix proposé :



### 7.7.1 Histogramme



Il n'est pas utile dans ce cas là mais très utile dans certains cas :



Cet exemple a été réalisé avec notre algorithme et aussi disponible sur la page Wikipédia « égalisation d'histogramme ».

### 7.7.2 Inverse couleur

Dans beaucoup de cas, les empreintes sont données comme ci-dessous, c'est à dire avec des rides blanches. Or, notre algorithme nécessite d'avoir des rides noires. On peut donc inverser les couleurs.



### 7.7.3 Filtre Passe haut

Il permet de relier des rides qui ne sont pas reliées et peut être très utile dans certains cas.



#### 7.7.4 Inverse sens de l'image

Dans certains cas, nous avons du mal à discerner le sens de l'empreinte.



#### 7.7.5 Filtre median et moyenneur

Nous avons vu précédemment ces filtres. Ce mode sert par exemple à voir lequel de ces deux filtres semble le plus efficace.



FIGURE 27 – Le filtre médian

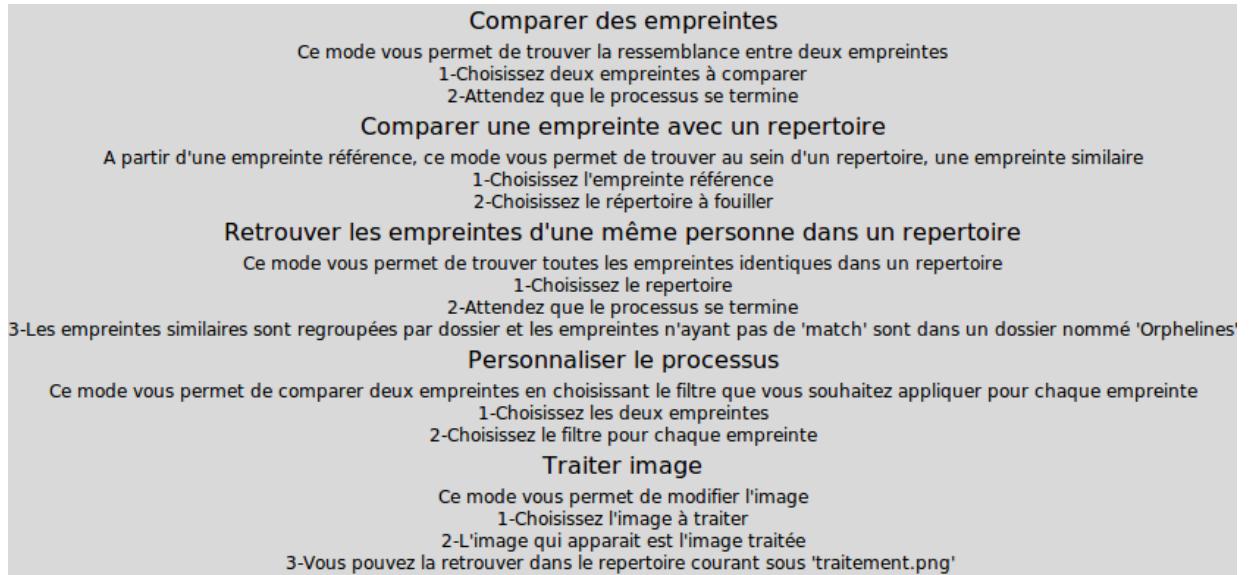


FIGURE 28 – Le moyenneur

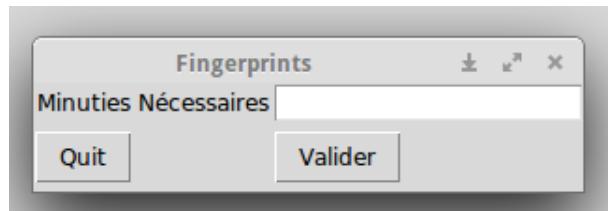
Avec les figures ci-dessus, on peut aisément voir que le filtre médian est meilleur.

## 7.8 Aide

Par ailleurs une aide est disponible en cas de besoin.



Plus important, notre souhait était de rendre le programme le plus modifiable possible. C'est pourquoi nous laissons à l'utilisateur le choix du nombre de minuties nécessaire pour matcher deux personnes. Il est par défaut défini à 12.



## 7.9 Limites du programme

C'est une partie importante du rapport. Nous nous sommes donnés du mal et sommes fier du programme que nous avons réalisé. Cependant, celui-ci n'est pas sans défaut. Nous allons les énumérer dans cette partie. Sachez que la liste ici n'est pas exhaustive mais recense seulement les défauts qui nous ont semblé les plus pertinents.

- Le principal défaut du programme est qu'il ne fonctionne pas parfaitement. En effet, deux empreintes non identiques peuvent se retrouver identique. Nous avons parfaitement identifié le problème. En effet, les étapes préliminaires qui concernent le retouchage de l'image sont primordiales. Malheureusement nous n'avons pas su trouver un filtre qui nous permette à coup sûr d'avoir une bonne squelettisation. C'est de loin notre principal regret. Bien-heureusement, ce type de cas se présente beaucoup moins fréquemment que le contraire.  
Par ailleurs, de ce défaut en découle un autre. En effet, à cause de celui-ci, la fonctionnalité qui permet de regrouper dans plusieurs dossiers les empreintes similaires peut être faussée.
- Le second défaut est l'optimisation du code. En effet, nous nous sommes concentrés sur les possibilités que pouvaient offrir notre programme et avons partiellement oublié l'optimisation. Ainsi, comme vous pourrez le voir en lisant le code, celui-ci n'est pas optimisé et certaines parties sont redondantes.

## 7.10 Les regrets du programme

- Il s'agit du premier projet où nous développions un programme avec une interface graphique ( hormis les sites web ). L'année dernière, certains d'entre nous avions touché à Qt et avons remarqué qu'il offrait énormément de possibilités. C'est pourquoi nous avons été rapidement déçu des fonctionnalités offertes par Tkinter.
- Avec un peu plus de temps, nous aurions pu peaufiner davantage le travail ( apporter un code plus clair par exemple )

## **8 Organisation et communication**

### **8.1 Méthodes de communication**

Durant notre travail sur ce projet, nous avons dû communiquer entre nous afin de mieux partager l'information. La communication est une facette importante du travail de groupe car elle impacte directement sur l'efficacité. Pour cela, nous avons utilisé différents moyens de communication :

- Des réunions hebdomadaires afin de faire le point sur certains aspects du projet ainsi que pour régler des questions sujettes à débats.
- Des discussions constantes via l'application WhatsApp en cas de besoin de conseil ou d'avis sur une partie du projet.
- Des échanges de mails et un Drive pour pouvoir travailler de manière plus efficace sur un même dossier sans avoir à attendre un contact physique pour continuer le travail.

### **8.2 Points forts et faibles**

Notre groupe est assez hétérogène en termes de capacité mais aussi en caractère, cela a pour conséquence l'existence de points forts mais aussi de points faibles au sein du groupe. Notre principale difficulté a été de bien gérer notre temps et de bien répartir le travail car les aléas du quotidien font que ce qui est prévu n'est pas toujours respecté. Une personne peut prendre plus de temps sur une facette du projet ou se rendre compte qu'elle est plus compliqué que prévue et donc avoir plus de travail que les autres membres du groupe. Mais ces complications se résolvaient car nous avons eu une très bonne entente entre les membres du groupe et que chaque membre possède des capacités autant informatiques que mathématiques. De plus, comme vu précédemment, la communication dans notre groupe est fluide et fréquente, ne laissant pas de place à une gêne ni à une tension, et les membres du groupe savent exprimer leurs idées clairement.

Par conséquent, notre groupe, de part sa constitution, a eu des moments plus difficiles que d'autres mais nous avons su les surmonter afin d'aboutir à un projet complet.

### **8.3 Constitution de l'équipe**

La taille de notre groupe implique forcément des temps de paroles de chaque membre moins longs que dans un groupe de taille plus réduite. Mais cela est compensé par la richesse d'idées et d'opinions qui sont apportées, d'autant plus que l'esprit critique de chacun permet d'avoir au final une idée complète et la plus "idéale" possible.

Lors du fonctionnement de l'équipe, les rôles se sont rapidement mis en place sans forcément qu'il n'y ait de discussion à ce propos. Nous nous sommes organisés dans une structure centralisée autour d'un leader. Cela a permis d'optimiser notre travail et d'améliorer notre gestion de celui-ci.

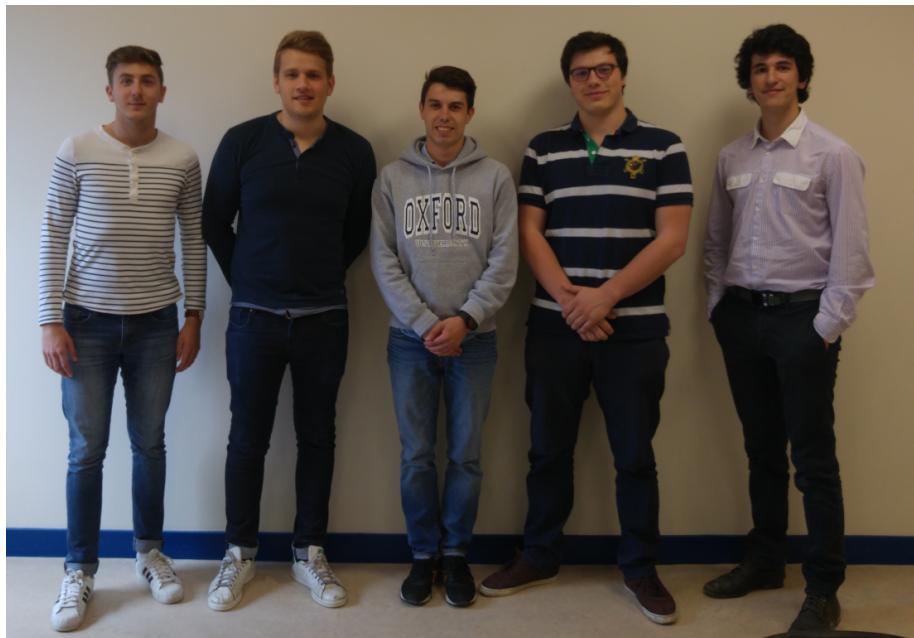


### **8.4 Objectifs**

Au cours de ce projet, nous avions différents objectifs. Au delà du fait de rendre un projet abouti et le plus complet possible, nous voulions chacun en ressortir plus expérimenté. Tout au long du projet, nous avions pour but de maintenir la bonne ambiance de travail qui s'était installée ainsi que la cohésion de notre groupe. Mais aussi, avoir déjà une idée de comment se passe ce genre de projet dans la vie professionnelle, avoir une organisation professionnelle, des rapports professionnels ainsi qu'une attitude professionnelle durant le projet. Et enfin, que tout le monde ressorte de ce projet avec une expérience et des compétences supplémentaires, que cela soit au niveau mathématiques, informatiques ou humaines.

## 9 Conclusion

Nous sommes au terme de ce projet. Au nom du groupe entier, nous sommes content de ce projet. Nous avons appris beaucoup au sujet des empreintes digitales et donc par conséquent sur la manière dont marche la reconnaissance digitale sur nos portables par exemple. Le programme que nous rendons présente malheureusement des petits défauts qui nous attristent car nous aurions aimé rendre un programme performant, à toutes épreuves. Néanmoins, nous pensons rendre ici un programme honnête sur lequel nous avons consacré beaucoup de temps, que ce soit en phase de test ou de programmation. Nous espérons qu'il saura répondre à vos attentes.



## 10 Bibliographie

Sites internets :

<http://tf2d.free.fr/>  
<http://empreintesdigitales.free.fr/>  
<http://tomtpe.lescigales.org/>  
<http://www.police-scientifique.com/>  
<http://www.biometrie-online.net/>  
<http://biometrics.over-blog.com/>