

**Université de Cergy-Pontoise**

# **Rapport**

*pour le projet de Traitement d'Images Licence  
d'Informatique troisième année*

## **Empreintes Digitales**

rédigé par

Reyane Remache



|   |           |
|---|-----------|
| <b>Université de Cergy-Pontoise</b>         | <b>1</b>  |
| <b>Empreintes Digitales</b>                 | <b>1</b>  |
| <b>La Biométrie</b>                         | <b>4</b>  |
| Introduction:                               | 4         |
| Reconnaissance Faciale:                     | 5         |
| Avantages de la reconnaissance faciale:     | 6         |
| Inconvénients de la reconnaissance faciale: | 7         |
| LES ANALYSES DE LA RÉTINE:                  | 9         |
| LES ANALYSES DE L'IRIS:                     | 10        |
| LES EMPREINTES DIGITALES :                  | 11        |
| <b>Etat De L'Art</b>                        | <b>11</b> |
| Modèles De Base :                           | 11        |
| Caractéristiques Minutiae:                  | 12        |
| Lecteurs D'empreintes Digitales:            | 12        |
| <b>LE CODE SOURCE</b>                       | <b>13</b> |
| La Méthode CN (Crossing Number) :           | 17        |

# La Biométrie

## Introduction:

La biométrie est une mesure biologique - ou caractéristique physique - qui peut être utilisée pour identifier des individus. La cartographie des empreintes digitales, la reconnaissance faciale et les analyses de la rétine sont toutes des formes de technologie biométrique, mais ce ne sont que les options les plus reconnues.

Les chercheurs affirment que la forme d'une oreille, la façon dont quelqu'un s'assoit et marche, les odeurs corporelles uniques, les veines dans les mains et même les contorsions faciales sont d'autres identificateurs uniques.

Parce que les caractéristiques physiques sont relativement fixes et individualisées - même dans le cas de jumeaux - elles sont utilisées pour remplacer ou au moins augmenter les systèmes de mot de passe pour les ordinateurs, les téléphones et les salles et bâtiments à accès restreint.

La biométrie avancée est également utilisée pour protéger les documents sensibles. Citibank utilise déjà la reconnaissance vocale et la banque britannique Halifax teste des appareils qui surveillent le rythme cardiaque pour vérifier l'identité des clients. Ford envisage même d'installer des capteurs biométriques dans les voitures.

La biométrie est intégrée dans les passeports électroniques dans le monde entier. Aux États-Unis, les passeports électroniques ont une puce qui contient une photographie numérique du visage, des empreintes digitales ou de l'iris, ainsi qu'une technologie qui empêche la lecture de la puce - et les données écrémées - par des lecteurs de données non autorisés.

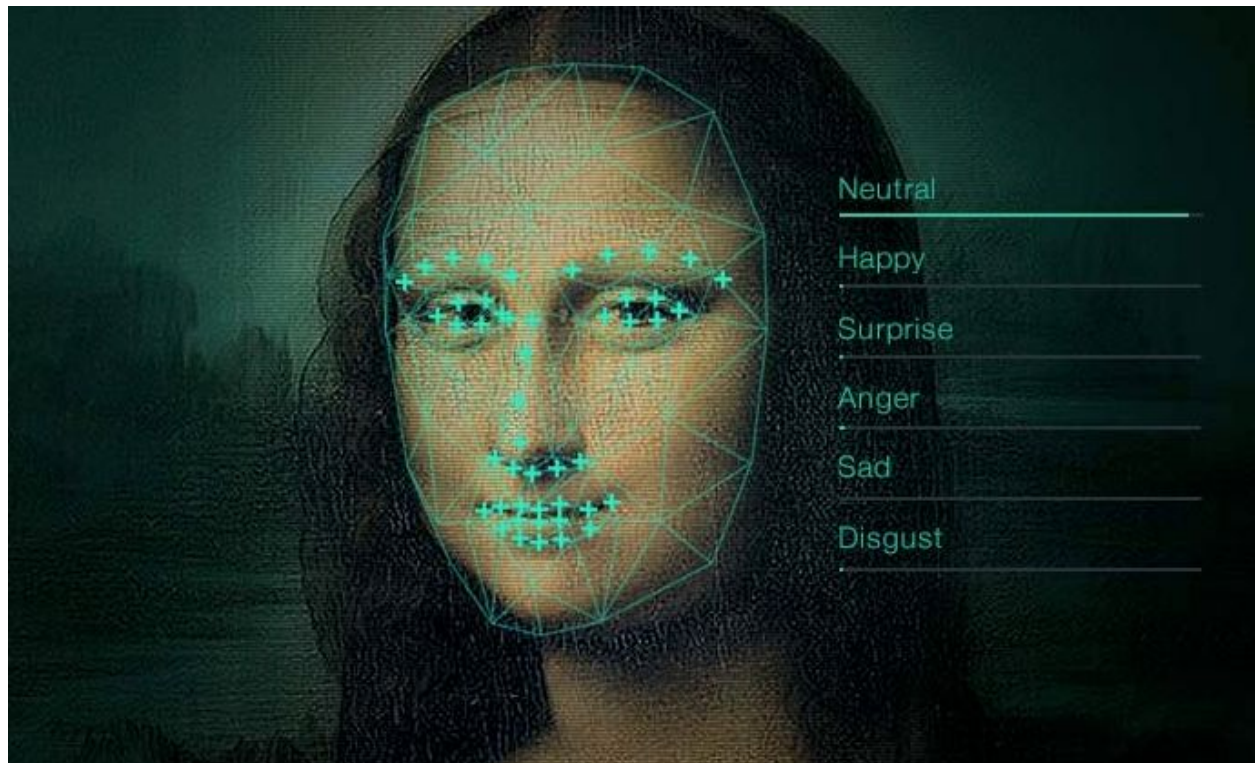
## Reconnaissance Faciale:

La technologie de reconnaissance faciale a toujours été un concept qui vivait dans des mondes fictifs, que ce soit un outil pour résoudre un crime ou ouvrir des portes. Aujourd'hui, notre technologie a considérablement développé ce domaine car nous le voyons devenir plus courant dans notre vie quotidienne. De la technologie Face ID d'Apple iPhone X à Rekognition d'Amazon, la reconnaissance faciale semble devenir plus lentement une réalité qu'un concept fictif.

Qu'est-ce que la reconnaissance faciale et comment fonctionne-t-elle exactement? La reconnaissance faciale est un type de logiciel biométrique capable d'identifier ou de vérifier une personne à partir d'une image numérique en cartographiant mathématiquement ses caractéristiques et en enregistrant les informations sous forme d'empreintes digitales. Cette technologie utilise des algorithmes d'apprentissage en profondeur pour comparer ces images afin de garantir qu'il s'agit de l'identité correcte de l'individu, ce qui la rend très similaire à d'autres technologies d'identification telles que la correspondance d'empreintes digitales, le balayage de la rétine et la reconnaissance vocale.

La technologie de reconnaissance faciale est en mesure d'effectuer cette tâche en trois étapes: détecter le visage, numériser et créer des empreintes digitales / cibles, et enfin faire correspondre et vérifier. Comme un outil de moteur de recherche visuel, cette technologie est capable d'identifier les facteurs clés dans un environnement visuel très occupé, ce qui la rend très utile pour sélectionner des individus même dans des endroits surpeuplés. Il existe de nombreuses applications différentes pour

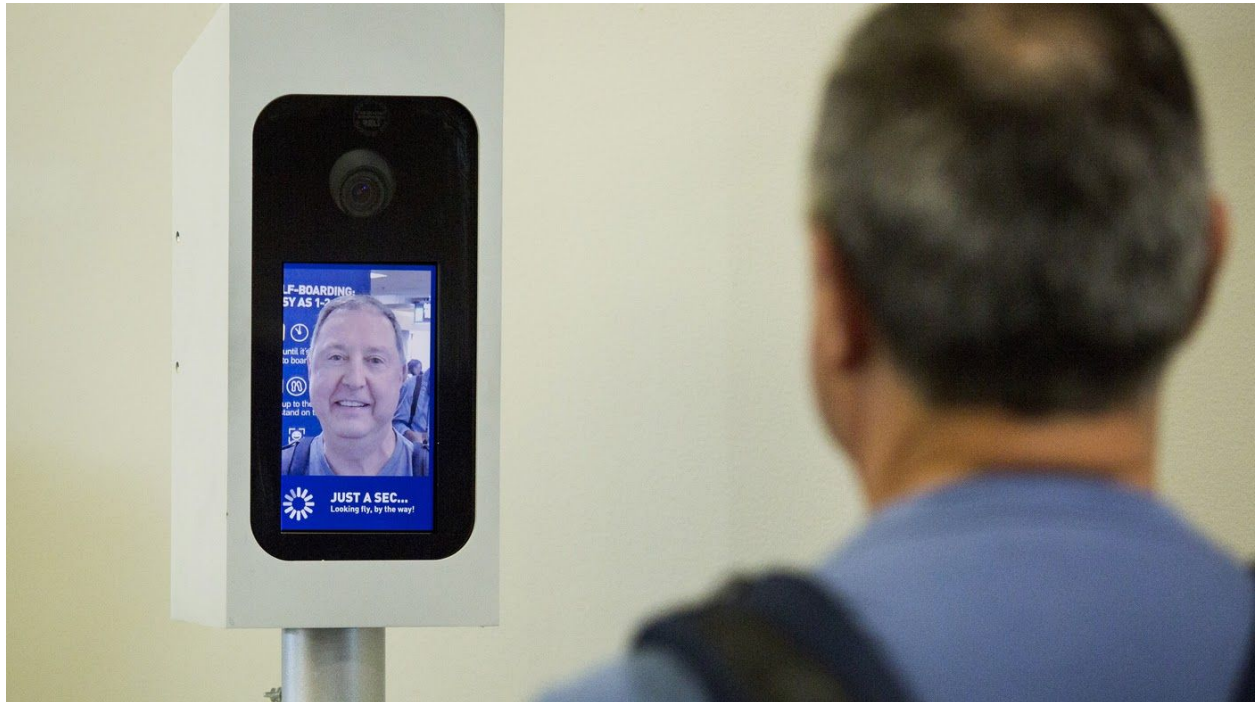
la technologie de reconnaissance faciale, cependant, selon la façon dont vous l'utilisez, elle peut présenter de nombreux avantages et inconvénients.



### **Avantages de la reconnaissance faciale:**

L'un des principaux avantages de la technologie de reconnaissance faciale est la sécurité et la sûreté. Les organismes chargés de l'application des lois utilisent la technologie pour découvrir des criminels ou pour retrouver des enfants ou des personnes âgées disparus. À New York, la police a pu appréhender un violeur présumé en utilisant la technologie de reconnaissance faciale dans les 24 heures suivant un incident où il a menacé une femme de viol au point de couteau. Dans les villes où la police n'a pas le temps de lutter contre la petite délinquance, les propriétaires d'entreprise installent des systèmes de reconnaissance faciale pour surveiller les gens et identifier les sujets d'intérêt lorsqu'ils viennent dans leurs magasins.

Les aéroports ajoutent de plus en plus la technologie de reconnaissance faciale aux points de contrôle de sécurité; le département américain de la Sécurité intérieure prévoit qu'il sera utilisé par 97% des voyageurs d'ici 2023.



Lorsque les gens savent qu'ils sont surveillés, ils sont moins susceptibles de commettre des délits, de sorte que la possibilité d'utiliser la technologie de reconnaissance faciale pourrait dissuader les délits.

Puisqu'il n'y a aucun contact requis pour la reconnaissance faciale comme c'est le cas avec les empreintes digitales ou d'autres mesures de sécurité, la reconnaissance faciale offre une expérience de vérification rapide, automatique et transparente. Il n'y a rien de tel qu'une clé ou une carte d'identité. qui peut être perdu ou volé.

La reconnaissance faciale peut ajouter des commodités. En plus de vous aider à étiqueter des photos sur Facebook ou votre stockage cloud via Apple et Google, vous pourrez commencer à payer dans les magasins sans retirer de l'argent ou des cartes de crédit - votre visage sera scanné.



À l'A.I. Bar, la technologie de reconnaissance faciale est utilisée pour ajouter des clients qui s'approchent du bar à une file d'attente pour se faire servir leurs boissons plus efficacement.

Bien que cela soit possible, il est difficile de tromper la technologie de reconnaissance faciale, ce qui peut également aider à prévenir la fraude.

### **Inconvénients de la reconnaissance faciale:**

Le plus grand inconvénient de la technologie de reconnaissance faciale dans l'opinion de la plupart des gens est la menace pour la vie privée d'un individu. En fait, plusieurs villes ont envisagé ou interdisent l'utilisation de la surveillance de la reconnaissance faciale en temps réel par les forces de l'ordre, notamment à San Francisco, Cambridge, Massachusetts, etc. Ces municipalités ont déterminé que les risques liés à l'utilisation de la technologie l'emportent sur les avantages. La police peut toujours utiliser des images provenant d'appareils personnels tels que des caméras Nest pour trouver des criminels; il ne permet tout simplement pas aux entités gouvernementales d'utiliser un logiciel de reconnaissance faciale en direct.

Alors que le King's Cross de Londres utilise la reconnaissance faciale, Londres est également à l'avant-garde des sociétés démocratiques dans ses tests de la technologie. Lors des événements tests, la ville espère déterminer la précision des systèmes tout en essayant de gérer les individus qui se cachent pour cacher leur identité aux caméras et à d'autres problèmes. De plus, les sociétés démocratiques doivent définir la base juridique pour vivre la reconnaissance faciale de la population en général, et quand l'utilisation générale de la technologie est justifiée.

La technologie n'est pas aussi efficace pour identifier les personnes de couleur et les femmes que les hommes blancs. L'une des raisons à cela est que l'ensemble de données sur lequel les algorithmes sont formés n'est pas aussi robuste pour les personnes de couleur et les femmes. Jusqu'à ce que cela soit corrigé, il y a des inquiétudes quant aux ramifications d'une mauvaise identification des personnes avec la technologie.

De plus, il y a des problèmes à résoudre qui peuvent perturber la technologie lorsqu'une personne change d'apparence ou que l'angle de la caméra n'est pas tout à fait correct (bien qu'ils s'efforcent de pouvoir identifier une personne uniquement avec leur lobe d'oreille). Il s'améliore considérablement; selon des tests indépendants effectués par le National Institute of Standards and Technology (NIST) des États-Unis, les systèmes de reconnaissance faciale ont 20 fois mieux trouvé une correspondance dans une base de données sur une période couvrant la période 2014-2018.

Un autre inconvénient potentiel est le stockage de données personnelles sensibles et les défis qui en découlent. La semaine dernière, nous avons appris qu'une base de données contenant des analyses faciales utilisées par les banques, les forces de police et les entreprises de défense avait été violée.

Afin de bénéficier des aspects positifs de la reconnaissance faciale, notre société va devoir surmonter des défis importants pour notre vie privée et nos libertés civiles. Les individus accepteront-ils l'invasion de leur vie privée comme un coût approprié pour être plus en sécurité et pour les commodités offertes par la reconnaissance faciale?



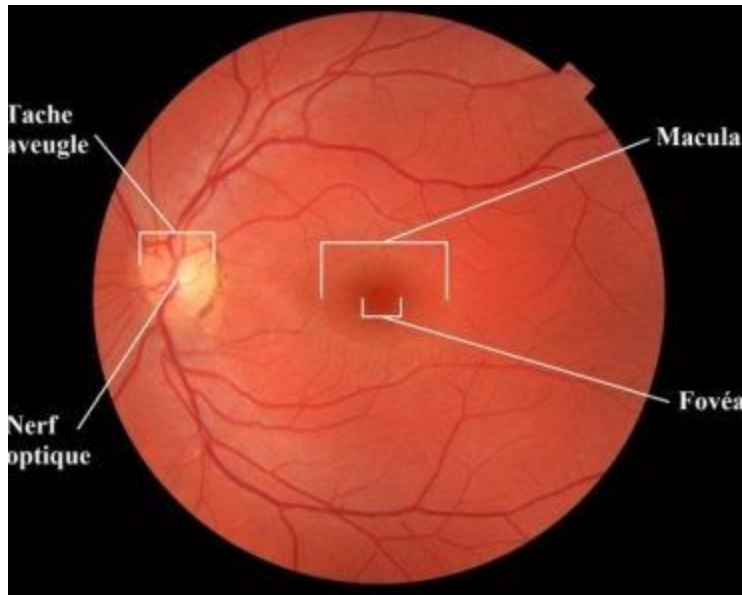
## **LES ANALYSES DE LA RÉTINE:**

La rétine humaine est un tissu mince composé de cellules neurales qui se trouve dans la partie postérieure de l'œil. En raison de la structure complexe des capillaires qui alimentent la rétine en sang, la rétine de chaque personne est unique. Le réseau de vaisseaux sanguins dans la rétine est si complexe que même des jumeaux identiques ne partagent pas un schéma similaire. Bien que les schémas rétinien puissent être modifiés en cas de diabète, de glaucome ou de troubles dégénératifs rétinien, la rétine reste généralement inchangée de la naissance à la mort.

L'identification biométrique connu sous le nom de scintigraphie rétinienne est utilisé pour cartographier les modèles uniques de la rétine d'une personne. Les vaisseaux sanguins de la rétine absorbent la lumière plus facilement que les tissus environnants et sont facilement identifiés grâce à un éclairage approprié. Un balayage rétinien est effectué en projetant un faisceau de lumière infrarouge à faible énergie non perçu dans l'œil d'une personne qui regarde à travers l'oculaire du scanner. Ce faisceau de lumière trace un chemin normalisé sur la rétine.

Parce que les vaisseaux sanguins rétinien sont plus absorbants de cette lumière que le reste de l'œil, la quantité de réflexion varie pendant le scan. Le modèle de variations est converti en code informatique et stocké dans une base de données. Le balayage rétinien a également des applications médicales. Les maladies transmissibles telles que le sida, la syphilis, le paludisme, la varicelle ainsi que les maladies héréditaires comme la leucémie, le lymphome et l'anémie falciforme ont un impact sur les yeux. La grossesse affecte également les yeux. De même, des indications de

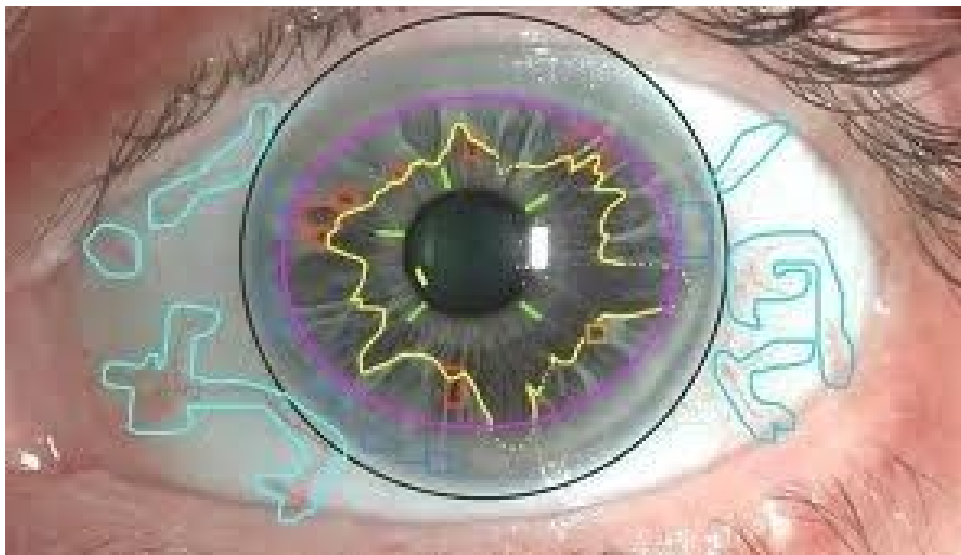
problèmes de santé chroniques tels que l'insuffisance cardiaque congestive, l'athérosclérose et les problèmes de cholestérol apparaissent d'abord dans les yeux.



## LES ANALYSES DE L'IRIS:

L'iris est une fine structure circulaire dans l'œil, chargée de contrôler le diamètre et la taille des pupilles et donc la quantité de lumière atteignant la rétine. La «couleur des yeux» est la couleur de l'iris, qui peut être verte, bleue ou brune. Dans certains cas, il peut être noisette (une combinaison de brun clair, vert et or), gris, violet ou même rose. En réponse à la quantité de lumière pénétrant dans l'œil, les muscles attachés à l'iris se dilatent ou contractent l'ouverture au centre de l'iris, appelée pupille. Plus la pupille est grande, plus la lumière peut entrer. La reconnaissance de l'iris est une méthode automatisée d'identification biométrique qui utilise des techniques mathématiques de reconnaissance des formes sur les images vidéo des iris des yeux d'un individu, dont les motifs aléatoires complexes sont uniques et peuvent être vus à une certaine distance.

Contrairement au balayage de la rétine, la reconnaissance de l'iris utilise la technologie de la caméra avec un éclairage infrarouge subtil pour acquérir des images des structures complexes et riches en détails de l'iris. Les modèles numériques encodés à partir de ces modèles par des algorithmes mathématiques et statistiques permettent une identification positive sans ambiguïté d'un individu. Les bases de données des modèles inscrits sont recherchées par les moteurs de correspondance à des vitesses mesurées en millions de modèles par seconde par processeur (monocœur), et avec des taux de fausses correspondances infiniment petits. Des centaines de millions de personnes dans des pays du monde entier ont été inscrites dans des systèmes de reconnaissance de l'iris, pour des raisons de commodité telles que les passages frontaliers automatisés sans passeport, et certains systèmes nationaux d'identification basés sur cette technologie sont en cours de déploiement. Un avantage clé de la reconnaissance de l'iris, en plus de sa vitesse d'appariement et de son extrême résistance aux faux matches, est la stabilité de l'iris en tant qu'organe de l'œil interne, protégé, mais visible de l'extérieur.



## **LES EMPREINTES DIGITALES :**

La reconnaissance des empreintes digitales fait référence à la méthode automatisée d'identification ou de confirmation de l'identité d'un individu sur la base de la comparaison de deux empreintes digitales. La reconnaissance des empreintes digitales est l'une des biométries les plus connues, et c'est de loin la solution biométrique la plus utilisée pour l'authentification sur les systèmes informatisés. Les raisons pour lesquelles la reconnaissance des empreintes digitales est si populaire sont la facilité d'acquisition, l'utilisation établie et l'acceptation par rapport à d'autres biométries, et le fait qu'il existe de nombreuses (dix) sources de cette biométrie sur chaque individu.

## Etat De L'Art

### Modèles De Base :

Les trois modèles de base des crêtes d'empreintes digitales sont l'arc, la boucle et le verticille. Une arche est un motif où la crête pénètre d'un côté du doigt, puis monte au centre en formant une arche et sort de l'autre côté du doigt. Avec une boucle, la crête entre dans un côté du doigt, puis forme une courbe et sort du même côté du doigt d'où elle est entrée. Les boucles sont le motif le plus courant dans les empreintes digitales. Enfin, un verticille est le motif que vous avez lorsque les crêtes se forment de manière circulaire autour d'un point central.

Reportez-vous aux images de droite pour des exemples de chaque motif.

## **Caractéristiques Minutiae:**

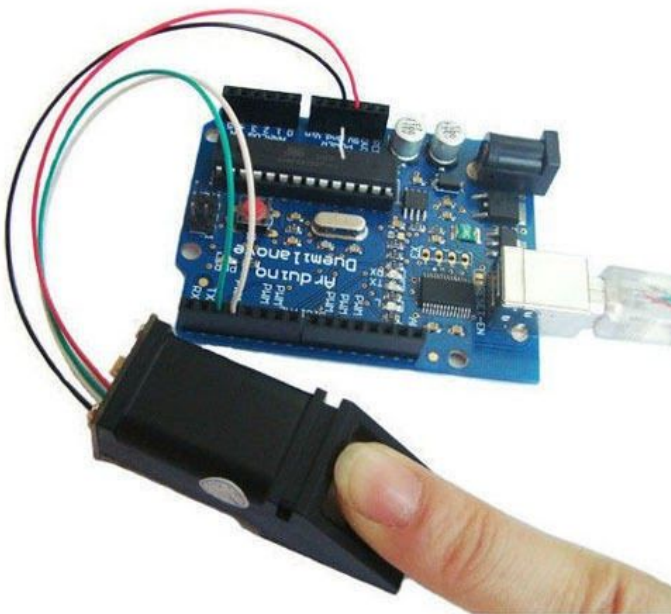
Les minuties font référence à des points spécifiques d'une empreinte digitale, ce sont les petits détails d'une empreinte digitale qui sont les plus importants pour la reconnaissance des empreintes digitales.

Il existe trois principaux types de caractéristiques de minutie: la fin de la crête, la bifurcation et le point (également appelé crête courte). La fin de la crête est, comme l'indique son nom, l'endroit où se termine une crête. Une bifurcation est l'endroit où une crête se divise en deux arêtes. Les tâches sont ces crêtes d'empreintes digitales qui sont beaucoup plus courtes que les autres crêtes.



## **Lecteurs D'empreintes Digitales:**

Les lecteurs optiques sont le type le plus courant de lecteurs d'empreintes digitales. Le type de capteur d'un lecteur optique est un appareil photo numérique qui acquiert une image visuelle de l'empreinte digitale. Les avantages sont que les lecteurs optiques commencent à des prix très bon marché. Les inconvénients sont que les lectures sont impactées par les doigts sales ou marqués, et ce type de lecteur d'empreintes digitales est plus facile à tromper que les autres.



Les lecteurs capacitifs, également appelés lecteurs CMOS, ne lisent pas l'empreinte digitale à l'aide de la lumière. Au lieu de cela, un lecteur CMOS



utilise des condensateurs et donc du courant électrique pour former une image de l'empreinte digitale. Les lecteurs CMOS sont plus chers que les lecteurs optiques, bien qu'ils soient encore relativement bon marché avec des prix commençant bien en dessous de 100 euros.

Un avantage important des lecteurs capacitifs par rapport aux lecteurs optiques est qu'un lecteur capacitif nécessite une véritable forme d'empreinte digitale plutôt que seulement une image visuelle. Cela rend les lecteurs CMOS plus difficiles à tromper.

Les lecteurs à ultrasons sont le type le plus récent de lecteurs d'empreintes digitales, ils utilisent des ondes sonores à haute fréquence pour pénétrer la couche épidermique (externe) de la peau. Ils lisent l'empreinte digitale sur la couche cutanée cutanée, ce qui élimine le besoin d'une surface propre et non marquée. Tous les autres types de lecteurs d'empreintes digitales acquièrent une image de la surface extérieure, ce qui nécessite de nettoyer les mains et de ne pas laisser de cicatrices avant de les lire. Ce type de lecteur d'empreintes digitales est beaucoup plus cher que les deux premiers, mais en raison de leur précision et du fait qu'ils sont difficiles à tromper, les lecteurs à ultrasons sont déjà très populaires.

Les lecteurs thermiques détectent, sur une surface de contact, la différence de température entre les crêtes des empreintes digitales et les vallées. Les lecteurs d'empreintes digitales thermiques présentent un certain nombre d'inconvénients tels qu'une consommation d'énergie plus élevée et des performances qui dépendent de la température de l'environnement.

## LE CODE SOURCE

On calcule l'Histogramme et on effectue un Seuillage optimal de l'image.

```
clear all;
close all;

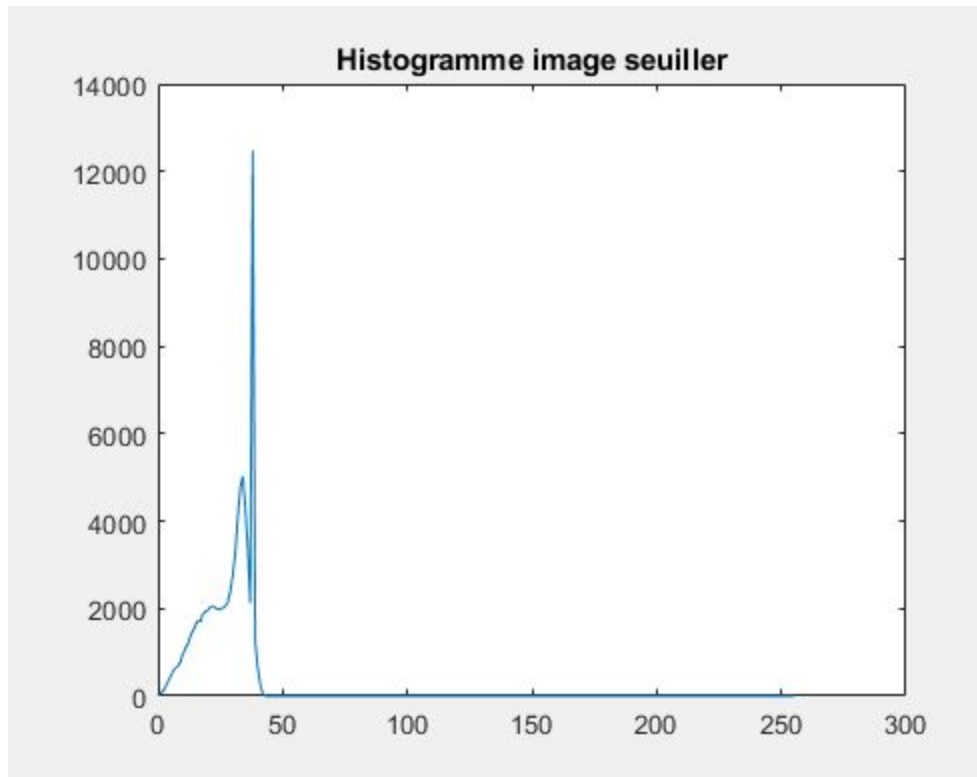
% Chargement et affichage de l'image %
I = imread('ED_3_6_originale.png');
% I = imread('/ED_5_1_originale.png');
figure(1);
subplot(2,3,1);
imshow(I);
title('Image initiale');

% Création histogramme %
H = zeros(1,256);
K = [0:255];
[NL,NC] = size(I);

for i = 1:NL
    for j = 1:NC
        H(I(i,j)+1) = H(I(i,j)+1)+1;
    end
end

subplot(2,3,2);
plot(K,H);
title('Histogramme image initiale');

% Seuillage %
```



On va ensuite travailler sur l'Amincissement/la Squelettisation de l'image. Pour cela nous utilisons l'algorithme de Hilditch. Pour pouvoir utiliser cet algorithme, il faut d'abord "inverser" l'image. C'est à-dire qu'il faut que tout ce qui est noir dans l'image devienne blanc et que tout ce qui est blanc dans l'image devient noir car l'algorithme ne travaille qu'avec des images claires. L'algorithme est le suivant :

### Définitions :

1.  $A(P1)$  : Nombre de transitions de 0(noir) à 1(blanc) sur chaîne  $P2, P3, P4, P5, P6, P7, P8, P9, P2$
2.  $B(P1)$  : Nombre de voisins différents de 0

### Conditions :

$P1=0$  si :

1.  $A(P1)=1$
2.  $2 \leq B(P1) \leq 6$
3.  $P2 \cdot P4 \cdot P8 = 0$  ou bien  $A(P2)$  est différent de 1
4.  $P2 \cdot P4 \cdot P6 = 0$  ou bien  $A(P4)$  est différent de 1

```

% Amincissement / Squelettisation %
for i = 2:NL-1
    for j = 2:NC-1
        % Calcul de A et B
        A = 0;
        B = 0;
        P = [I(i-1,j) I(i-1,j+1) I(i,j+1) I(i+1,j+1) I(i+1,j) I(i+1,j-1) I(i,j-1) I(i-1,j-1) I(i-1,j)];
        for k = 1:8
            if P(k+1)-P(k) == 1
                A = A + 1;
            end
        end
        B = sum(sum(I(i-1:i+1,j-1:j+1)))-I(i,j);

        if (A == 1) && (B <= 6) && (B >= 2) && (P(1)*P(3)*P(7) == 0) && (P(1)*P(3)*P(5) == 0)
            I(i,j) = 0;
        end
    end
end
end

```

Image squelettisée



### **La Méthode CN (Crossing Number) :**

Le CN est la méthode d'extraction des minuties la plus utilisée dans la catégorie des images binaires amincies. Elle est préférée aux autres méthodes en raison de son efficacité de calcul et de sa simplicité intrinsèque

Dans cette méthode, une image squelette est utilisée lorsque le modèle d'écoulement de crête est connecté à huit. Comme le montre la figure ci-dessous, le voisinage local de chaque pixel de crête dans l'image est numérisé à l'aide d'une fenêtre  $3 \times 3$  à partir de laquelle les minuties sont extraites.

|    |    |    |
|----|----|----|
| P4 | P3 | P2 |
| P5 | P  | P1 |
| P6 | P7 | P8 |

La valeur CN est ensuite calculée, qui est définie comme la moitié de la somme des différences entre les paires de pixels voisins.

$$CN_{(x,y)} = \frac{1}{2} \sum_{i=1}^8 |p_i - p_{i+1}|, \quad p_1 = p_9$$

;

| CN | Propriétés           |
|----|----------------------|
| 0  | Point isolé          |
| 1  | Fin de crête         |
| 2  | Crête continue       |
| 3  | Point de bifurcation |
| 4  | Point de passage     |

```
% Crossing number %

Minuties = zeros(NL,NC);

I = double(I);

subplot(2,3,5);

title('Carte des minuties');

for i = 2:NL-1
    for j = 2:NC-1
        if I(i,j) == 1
            S = 0;

            P = [I(i,j+1) I(i-1,j+1) I(i-1,j) I(i-1,j-1) I(i,j-1) I(i+1,j-1) I(i+1,j) I(i+1,j+1) I(i,j+1)];

            for k = 1:8
                S = S + abs(P(k)-P(k+1));
            end

            S = S/2;

            switch S
                case 0
                    Minuties(i,j) = 1;

                    hold on;

                    plot(i,j,'xr');
                case 1
                    Minuties(i,j) = 1;
                    hold on;
                    plot(i,j,'xr');
                case 2
                    Minuties(i,j) = 1;
                    hold on;
                    plot(i,j,'xr');
                case 3
                    Minuties(i,j) = 1;
                    hold on;
                    plot(i,j,'xr');
                case 4
                    Minuties(i,j) = 1;
                    hold on;
                    plot(i,j,'xr');
            end
        end
    end
end
```

```

%           case 1
%           Minuties(i,j) = 2;
%           hold on;
%           plot(i,j,'or');
%           case 2
%           Minuties(i,j) = 3;
%           hold on;
%           plot(i,j,'ob');
%           case 3
%           Minuties(i,j) = 4;
%           hold on;
%           plot(i,j,'xb');
%           case 4
%           Minuties(i,j) = 5;
%           hold on;
%           plot(i,j,'oy');
end
end
end
end
end

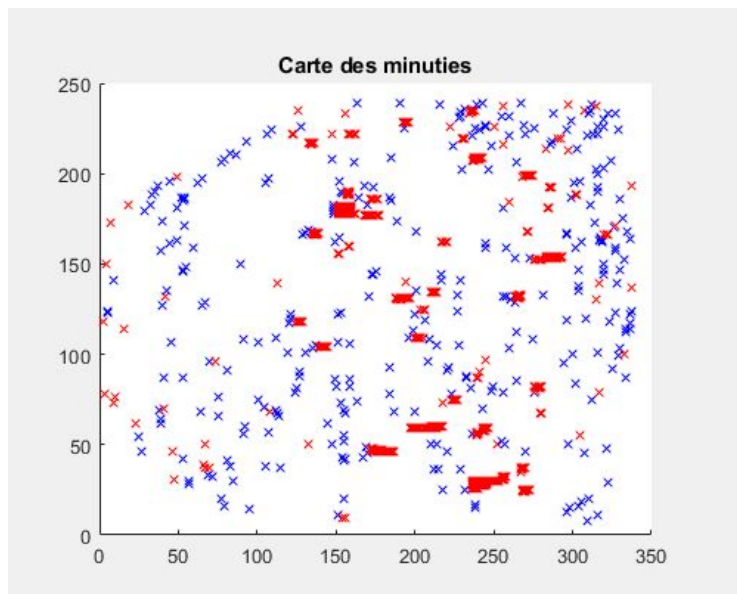
```

### **Carte des minuties:**

Pour identifier une personne à l'aide de ses empreintes digitales, il y a plusieurs conditions. Pour cela on compare une empreinte digitale à une banque (base de données) d'empreintes digitales et on vérifie si ces conditions sont satisfaites. Ces conditions sont eu nombre de 4. Si 3 des 4 conditions sont satisfaites alors, les empreintes digitales sont identiques. Si jamais une des 3 premières conditions ne sont pas satisfaites, on passe à la 4ème condition. Les conditions sont les suivantes :



1. Nombre total de points de l'image 1 = Nombre total de points de l'image 2
2. Nombre de points terminaux de l'image 1 = nombre de points terminaux de l'image 2
3. Nombre de points de bifurcation de l'image 1 = nNombre de points de bifurcation de l'image 2
4. Calcul de distance euclidienne entre les points de terminaison et bifurcation des deux images ou méthode de la distance de Hausdorff



Et finalement on compare les cartes des minutes

```
% Comparaison des cartes de minutes %  
  
res = true;  
  
for i = 1:NL  
    for j = 1:NC  
        if Minuties(i,j) ~= Minuties2(i,j)  
            res = false;  
        end  
    end  
end
```

---