La biométrie et Les empreintes digitales

1.1 Introduction

La biométrie est une technique naissante qui nous permet de vérifier l'identité d'un individu en employant un ou plusieurs de ses caractéristiques personnelles. Cette technique est utilisée de plus en plus aujourd'hui pour établir la reconnaissance des personnes dans un grand nombre d'applications diverses.
Dans ce chapitre nous commençons par présenter la biométrie de manière générale ainsi que les diverses applications qui en découlent, en focalisant plus particulièrement sur l'utilisation des empreintes digitales, ou nous détaillons les différentes étapes qui composent son système complet de reconnaissance.

1.2 Biométrie

1.2.1 Définition de la biométrie

Le terme de biométrie est originaire d'une contraction des deux anciens termes grecs : « bios » qui signifie : la vie « métrique » qui se traduit par : mesure.C'est-à-dire « mesure du vivant ». La biométrie consiste à vérifier ou déterminer l'identité d'un individu à partir de ses caractéristiques biologiques (comme l'ADN), comportementales (comme la voix) ou morphologiques (comme l'empreinte digitale).

Les techniques biométriques permettent la mesure et la reconnaissance de ce que l'on est, à la différence d'autres techniques de même finalités, mais permettant de mesurer ou vérifier ce que l'on possède (cadre, badge, document..) ou ce que l'on sait (mot de passe, code pin..)[1].

1.2.2 Système biométrique et leur mode de fonctionnement

Un système biométrique est un système de reconnaissance des formes qui procède en premier par l'acquisition des données biométriques de l'individu à reconnaître, puis extrait des caractéristiques à partir de celles ci, enfin il compare ces caractéristiques avec les modèles de la

base de données. Selon le contexte de l'application, un système biométrique peut fonctionner soit en mode d'enrôlement, de vérification ou d'identification[2].

1.2.2.1 Mode d'enrôlement

L'enrôlement est la première phase de tout système biométrique. Il s'agit de l'étape pendant laquelle un utilisateur est enregistré dans le système pour la première fois. Pendant l'enrôlement, la caractéristique biométrique est mesurée en utilisant un capteur biométrique afin d'extraire une représentation numérique[3]. Cette représentation est ensuite réduite, en utilisant un algorithme d'extraction bien défini, afin de réduire la quantité de données à stocker pour ainsi faciliter la vérification et l'identification. le modèle biométrique retenu, est stocké dans une base de données centrale.(voir **la figure 1.1**)

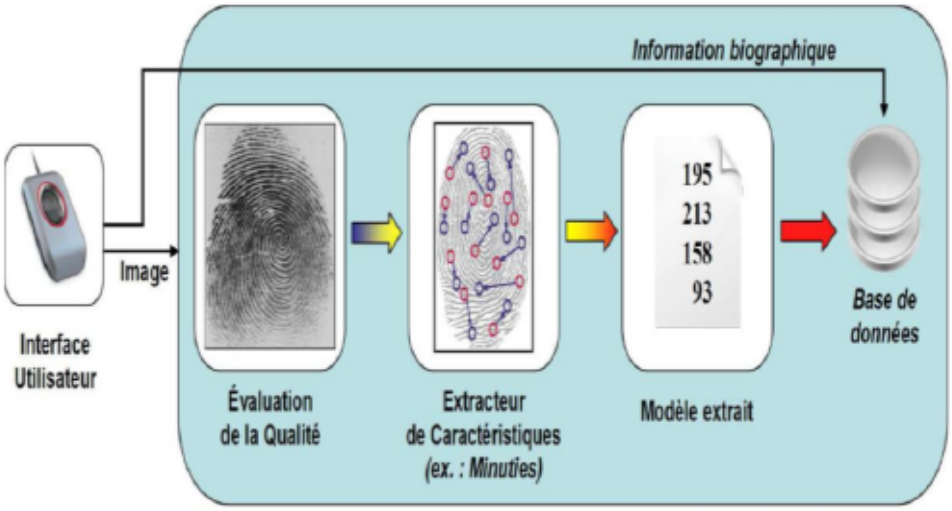

FIGURE 1.1 – Enrôlement dans un système biométrique.

1.2.2.2 Mode de vérification

Le système vérifie l'identité d'une personne en comparant les données biométriques acquises avec celles stockées dans la base de données. Dans un tel système, la personne revendique une identité, généralement via un code PIN (Personal Identification Number), un nom d'utilisateur, une carte à puce,etc. le système effectue alors une comparaison afin de déterminer si la déclaration est vraie ou non. La vérification de l'identité est généralement utilisée pour empêcher que plusieurs personnes n'utilisent la même identité[3].**la figure 1.2**

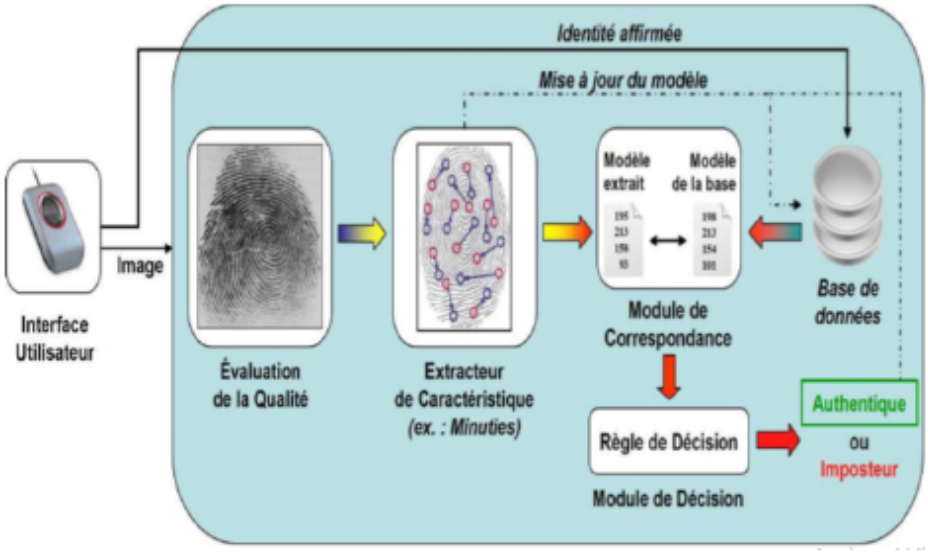

FIGURE 1.2 – Authentification d'un individu dans un système biométrique.

1.2.2.3 Mode d'identification

le système cherche à reconnaître un individu en comparant son modèle avec tous les modèles existants dans la base de données pour une éventuelle correspondance. Par conséquent, le système effectue une comparaison, du modèle de la personne, avec plusieurs modèles pour établir son identité. Ici l'individu n'a pas à revendiquer une identité. L'identification de l'identité est généralement utilisée pour empêcher qu'une personne n'utilise plusieurs identités[3].(voir **la figure 1.3**)

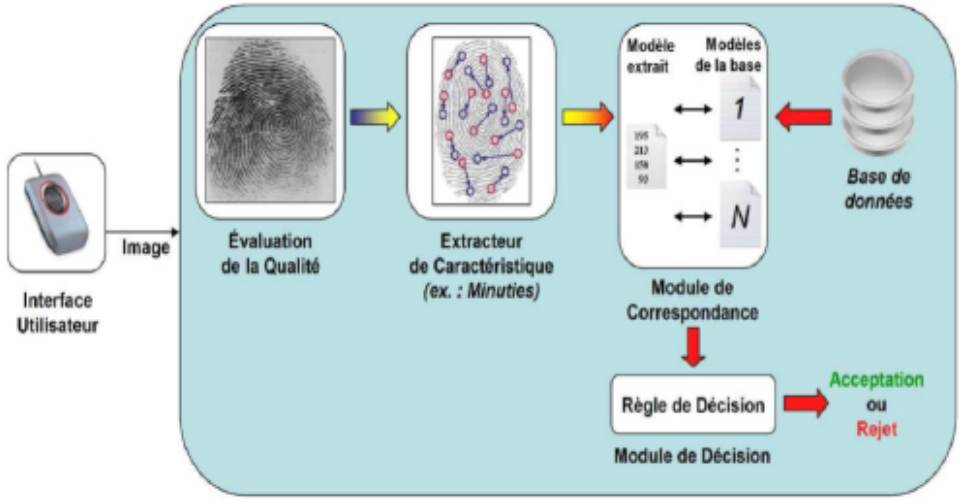

FIGURE 1.3 – Identification d'un individu dans un système biométrique.

1.2.3 Modalités biométriques

l'identification biométrique repose sur l'exploitation de caractéristiques humaines bien particulières qui constituent les différentes modalités biométriques[4]. ces modalités biométriques illustrées à **la figure 1.4** , sont regroupées en trois catégories :

1.2.3.1 Modalités morphologiques

Pour cette catégorie, l'authentification s'effectue à partir de caractéristiques physiques qui sont propres à chaque individu. On peut citer en particulier les empreintes digitales, le visage, l'iris, la rétine,..etc.

Les empreintes digitales : ce procédé est le plus répandu et le plus ancien, la donnée de base est le dessin représenté par les crêtes et sillons de l'épiderme (jonctions, terminaisons aveugles, croisements). Une empreinte est caractérisée par une centaine de points particuliers (appelés minuties),Les minuties représentent les fins de crêtes, les bifurcations, les lacs, les lots et les points qui composent l'empreinte digitale. La combinaison des minuties est quasi infinie[1].

Le visage : est la biométrie la plus commune et la plus populaire. Elle reste la plus acceptable puisqu'elle correspond à ce que les humains utilisent dans l'interaction visuelle. Les caractéristiques jugées significatives pour la reconnaissance du visage sont : les yeux, la bouche et le tour du visage. Le problème de cette méthode vient des possibles perturbations pouvant transformer le visage (maquillage, faible luminosité, présence d'une barbe ou des lunettes, expression faciale inhabituelle, changement avec l'age, etc).[5]

L'iris : est la région, sous forme d'anneau, située entre la pupille et le blanc de l'oeil, il est unique. L'iris a une structure extraordinaire et offre de nombreuses caractéristiques de texture qui sont uniques pour chaque individu. La reconnaissance de l'iris est développée dans les années 80 c'est pour cela elle est une technologie plus récente. l'image de l'iris est capturée par un appareil qui contient une caméra infrarouge, lorsque la personne se place a une courte distance de l'appareil[6].

La rétine : La reconnaissance de la rétine permet d'observer les ramifications vasculaires qui tapissent le fond de l'oeil (surface interne antérieure) et qui sont uniques pour chaque personne. L'utilisateur doit placer son oeil face a un orifice de capture situé sur le dispositif d'acquisition, Le capteur enregistre la disposition des veines dans l'oeil en balayent la rétine a l'aide d'un faisceau lumineux dans le globe oculaire. Cette technique requiert une collaboration étroite de la part de l'utilisateur, car il doit placer son oeil extrêmement près de la caméra[**?**]7

1.2.3.2 Modalités biologiques

L'authentification s'effectue à partir d'éléments biologiques tels que la salive, ADN (Acide désoxyribo Nucléique), le sang. Elles sont très complexes à mettre en oeuvre et sont réservées exclusivement pour des applications judiciaires.

L'ADN : est l'outil d'identification par excellence, plusieurs états à travers le monde possédent ou programment la mise sur pied d'une base de données génétique et projettent de l'egiférer sur ce plan. L'analyse des empreintes génétiques est une méthode d'identification d'individus extrêmement précise, elle est issue directement de l'évolution de la biologie moléculaire.[5]

1.2.3.3 Modalités comportementales

L'authentification se base sur la différence comportemental d'un individu, tels que la démarche, la signature, la dynamique de frappe au clavier, la voix.

La démarche :Il s'agit de reconnaître un individu par sa façon de marcher et de bouger (vitesse, accélération, mouvements du corps..etc), en analysant des séquences d'images. La démarche serait en effet étroitement associée à la musculature naturelle et donc très personnelle[1].

La signature : toute personne a son propre style d'écriture. A partir de la signature d'une personne, nous pouvons définir un modèle qui pourra être employé pour son identification. La signature étant utilisée dans beaucoup de pays comme élément juridique ou administratif, elle est utilisée pour justifier la bonne fois d'une personne ou pour la confondre devants des documents préalablement signés. la signature est examinée sous la forme d'une trace statique de stylo sur le papier. Sous forme numérisée, la géométrie statique de la signature ne suffit pas a garantir l'unicité de son auteur[8].

La voix : La biométrie de la voix traite des données qui proviennent à la fois de facteurs physiologiques dépendants de l'âge, du sexe, de la tonalité, de l'accent et de facteurs comportementaux comme la vitesse et le rythme. Ils ne sont en général pas imitables. C'est la seule technique qui permette à l'heure actuelle de reconnaître une personne à distance et qui est en général bien accepté par les usagers[5].

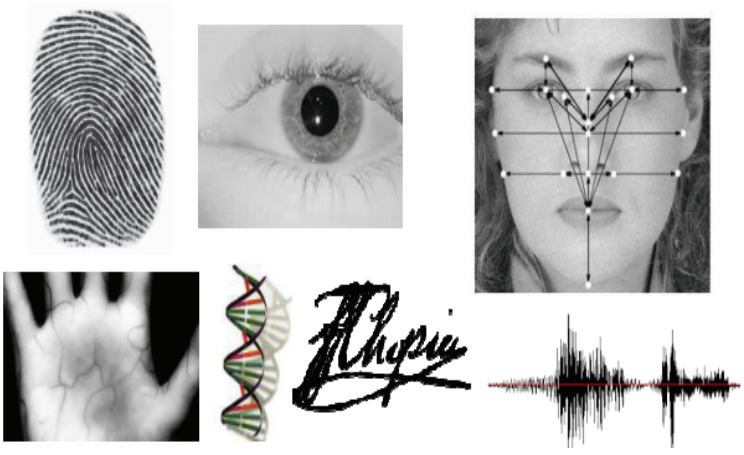

FIGURE 1.4 – Différentes modalités biométriques

Parmi les nombreuses méthodes d'identification biométrique l'utilisation des empreintes digitales est la méthode la plus aboutie avec 59% de parts de marché, nous y reviendrons

plus en détail dans la section suivante. Néanmoins d'autres méthodes commencent à trouver leur place sur le marché de la biométrie (voir **la figure 1.5**) :

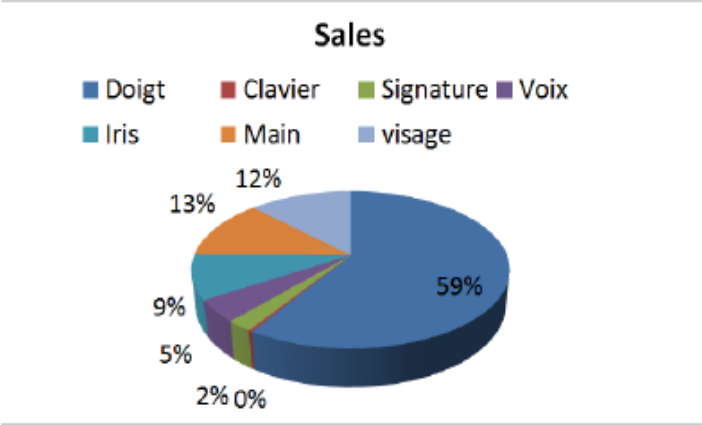

FIGURE 1.5 – Part de marché comparatif par technologie biométrie

1.2.4 Architecture d'un système biométrique

L'architecture d'un système biométrique contient cinq modules comme le montre **la figure 1.6** :

1.2.4.1 Module de capture :

qui consiste à acquérir les données biométriques afin d'extraire une représentation numérique. Cette représentation est ensuite utilisée pour l'enrôlement, la vérification ou l'identification. Il s'agit d'un capteur biométrique qui peut être de type sans ou avec contact.

1.2.4.2 Module de traitement du signal :

qui permet de réduire la représentation numérique extraite afin d'optimiser la quantité de données à stocker lors de la phase d'enrôlement, ou pour faciliter le temps de traitement pendant la phase de vérification et l'identification. Ce module peut avoir un test de qualité pour contrôler les données biométriques acquises.

1.2.4.3 Module du stockage :

qui contient les modèles biométriques des utilisateurs enrôlés du système.

1.2.4.4 Module de similarité :

qui compare les données biométriques extraites par le module d'extraction de caractéristiques a un ou plusieurs modèles préalablement enregistrés. Ce module détermine ainsi le degré de similarité (ou de divergence) entre deux vecteurs biométriques.

1.2.4.5 Module de décision :

qui détermine si l'indice de similarité retourné est suffisant pour déterminer l'identité d'un individu.[9]

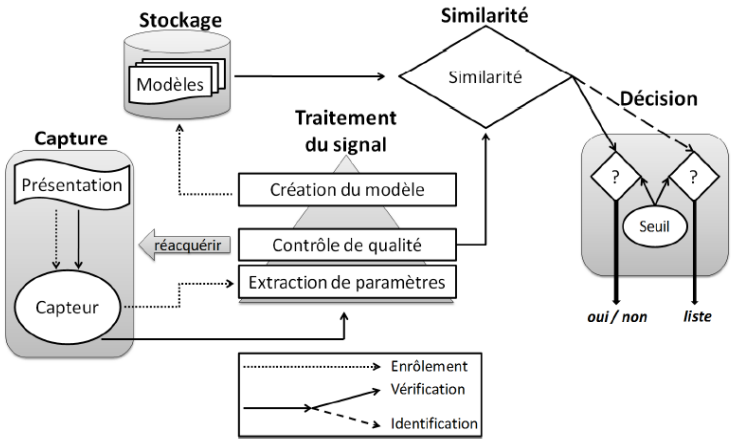

FIGURE 1.6 – Architecture complète d'un système biométrique.

1.2.5 Performance d'un système biométrique :

En biométrie, chaque système est en face de deux populations :

1. Les clients appartenant au système, ceux qui sont autorisés à pénétrer dans la zone protégée.
2. Les imposteurs n'appartenant pas au système, mais généralement qui essayent de rentrer.

Pour évaluer les performances d'un système biométrique plusieurs mesures sont employées :

✓ **Le taux de faux rejets (TFR)** : ("False Reject Rate"ou FRR), c'est la possibilité que le système produise un faux rejet. Ce taux représente le pourcentage des personnes censées être reconnues mais qui sont rejetées par le système.

$$TFR = \frac{\text{nombre de client rejeté(FR)}}{\text{tenombre total d'acces clientsxt}} \tag{1.1}$$

✓ **Le taux de fausse acceptation (TFA)** ("False Accepte Rate" ou FAR) : est la probabilité qu'un système biométrique identifie de manière incorrecte une personne ou ne réussisse pas à rejeter un imposteur. Il mesure le pourcentage d'intrants non valides qui sont acceptés à tort. Il est 'également connu sous le nom de 'taux de faux Positif".

$$TFA = \frac{\text{nombre imposteurs acceptés (FA)}}{\text{nombre total d'acces imposteurs}} \tag{1.2}$$

✓ **Le taux d'erreur (TEE)**("Equal Error Rate" ou EER) : ce taux est calculé à partir des deux premiers critères et constitue un point de mesure performance courant. Ce point correspond au lieu où FRR = FAR, c'est- à -dire le meilleur compromis entre le faux rejet et la fausse acceptation.

$$TEE = \frac{\text{nombre de fausses acceptations (FA)} + \text{nombre de faux rejets (FR)}}{\text{nombre totale d'acces}} \tag{1.3}$$

✓ **GAR** :«Genuine Accept Rate» c'est le taux des véritables clients acceptés par le Système biométrique. GAR est calculé par l'équation :

$$TFA = GAR(T) = 1 - FRR(T) \tag{1.4}$$

La relation entre FAR et FRR et le seuil T sont montrés sur **la Figure 1.7** où on constate que si on choisit le seuil T faible, le système laissera passer tous les gentils utilisateurs (clients), mais il laissera passer aussi les imposteurs facilement ce qui donne un système de faible sécurité. Et si on choisit le seuil T fort, le système bloquera les imposteurs mais malheureusement bloquera aussi quelques clients.

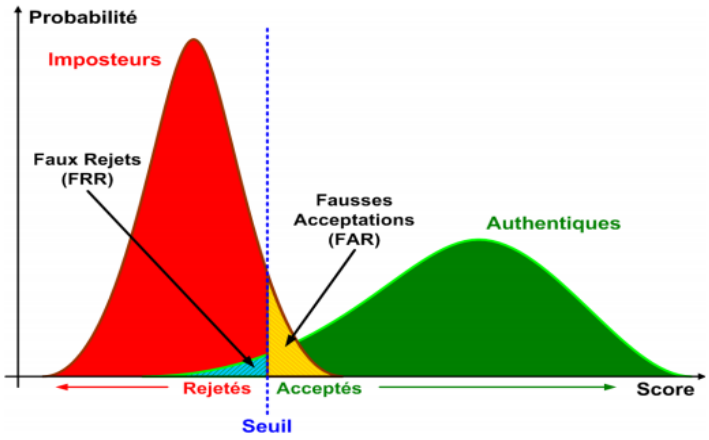

FIGURE 1.7 – Illustration du FRR et du FAR .
[29]

La courbe DET est la liaison entre le FAR et le FRR pour différentes valeurs de seuil comme montre **la Figure 1.8** .

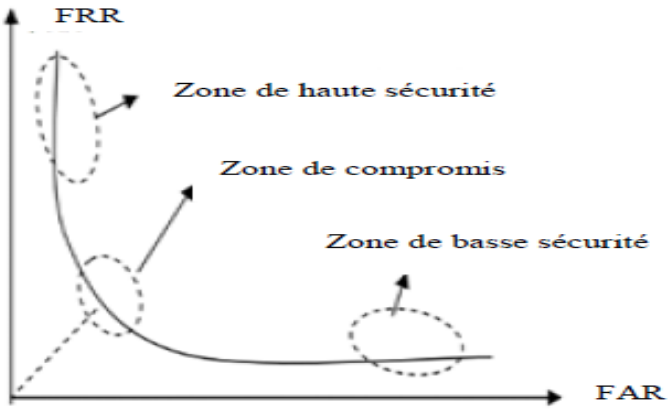

FIGURE 1.8 – Courbes DET.

Comparaison des performances Le vrai taux positif (TPR) P_{TPR} et le taux de faux positifs (FPR) P_{FPR} ont été calculés comme suit [28] :

$$T_{TPR} = \frac{\text{n similaire}}{\text{N identique}} \tag{1.5}$$

$$T_{FPR} = \frac{\text{n distinct}}{\text{N identique}} \tag{1.6}$$

Où n similaire est le nombre des paires d'images visuellement identiques correctement identifiées comme des images similaires, N identique est le nombre total de paires d'images visuellement identiques, n distinct est le nombre des paires d'images distinctes considérées par erreur comme des images similaires, et N différent est le nombre total de paires d'images différentes. Il est clair que le TPR et le FPR sont respectivement des indicateurs de robustesse et de discrimination.

1.2.6 Applications d'un système biométrique

Les techniques biométriques sont appliquées dans plusieurs domaines et leurs champ d'application couvrent potentiellement tous les domaines de la sécurité où il est nécessaire de connaître l'identité des personnes[1]. Les applications de la biométrie peuvent être divisées en trois groupes principaux **figure 1.9** :

- **Applications commerciales** : telles que l'ouverture de réseau informatique, la sécurité de données électroniques, l'e-commerce, l'accès Internet, la carte de crédit, le contrôle d'accès physique, le téléphone cellulaire, la gestion des registres médicaux, l'étude à distance, etc.
- **Applications gouvernementales** : telles que la carte d'identité nationale, le permis de conduire, la sécurité sociale, le contrôle des frontières, le contrôle des passeports, etc.

❖ **Applications légales** : telles que l'identification de corps, la recherche criminelle, l'identification de terroriste, etc.

FIGURE 1.9 – Quelques applications de la biométrie.

1.3 Reconnaissance des empreintes digitales :

1.3.1 Empreinte digitale :

L'empreinte digitale se compose d'un ensemble de lignes localement parallèles dessinées sur l'épiderme appelées "les stries"(ou les crêtes qui sont les reliefs en contacts avec la surface au toucher) et des creux entre les stries appelées "les vallées" (ou les sillons), (**Figure 1.8**).

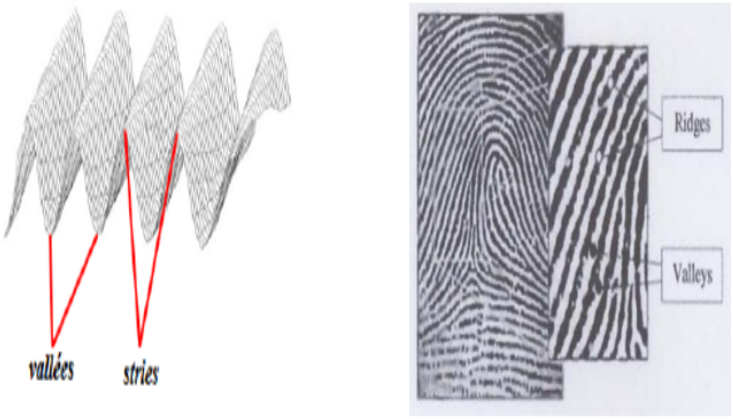

FIGURE 1.10 – Les vallées (valleys) et les crêtes (ridges) sur une empreinte.

1.3.2 Caractéristiques d'une empreinte digitale :

Plusieurs représentations des empreintes digitales sont proposées, et elles sont classifiées dans deux types principaux : représentation locale et représentation globale. La représentation

globale est un attribut entier du doigt et la représentation locale se compose de plusieurs composants, chaque composant typiquement dérivé d'une région dans l'espace limitée de l'empreinte digitale. Généralement, des représentations globales sont employées pour la classification d'empreinte digitale et des représentations locales sont employées pour la comparaison d'empreinte digitale.

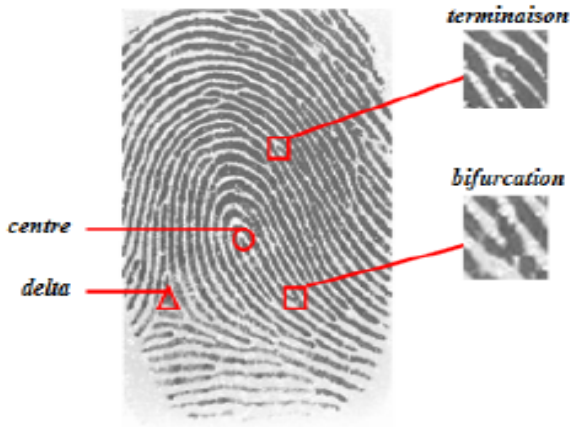

FIGURE 1.11 – Caractéristiques d'une empreinte digitale.

1.3.2.1 Représentation globale

chaque empreinte digitale a un ensemble des points singuliers globaux qui sont les centres et les deltas, symbolisés respectivement par θ et $\triangle$. Le centre est le lieu de convergence des stries (il est aussi appelé le core), alors que le delta correspond au lieu de divergence. La position et le nombre de ces points permettent la classification des empreintes digitales, c'est ainsi que Francis Galton les a subdivisées en trois grandes familles[10] :

- ✓ **Les Boucles (Loops)** une empreinte est de classe boucle si ses stries rentrent d'un côté et ressortent du même côté et si elle possède un point singulier de type boucle et un point singulier de type delta. Les boucles représentent 65% des empreintes des doigts humains.
- ✓ **Les Spires (Whorls)** une empreinte appartient à la classe spire si elle possède au moins une strie qui fait 360°. Elle peut aussi contenir jusqu'à deux régions singulières de type boucles et deux régions singulières de type deltas. Les spires représentent 30% des empreintes des doigts humains.
- ✓ **Les Arches (Archs)** : une empreinte est de classe arche si elle possède des stries qui rentrent d'un côté et ressortent du côté opposé et si elle ne contient ni boucle ni delta comme points singuliers. Les arches ne représentent que 5% des empreintes des doigts humains.

Edward Henry les a classées en six sous-classes principales : arche, boucle à gauche (left loop), boucle à droite (right loop), arche penchée (tented arch), spires et spires imbriquées ou boucles jumelles[11] (**figure 1.12**)

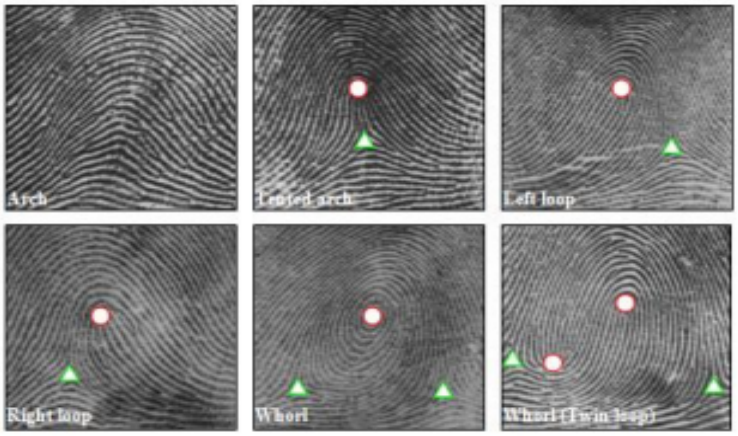

FIGURE 1.12 – Les principales classes d'empreintes digitales selon la classification de Galton-Henry .

1.3.2.2 Représentation locale

Il s'agit des caractéristiques les plus utilisées "les minuties" (littéralement : petits détails), qui sont en fait les points d'irrégularités qui se trouvent sur les lignes capillaires. Nous pouvons distinguer jusqu'à seize types de minuties différentes , mais dans les algorithmes on n'en s'intéresse qu'aux deux types suivants parce qu'ils sont facilement détectables :

- ✓ **La bifurcation** c'est le point où la strie se divise en deux.
- ✓ **La terminaison** c'est le point où la strie s'arrête .

En fait les autres types de minuties ne sont que les résultats des combinaisons des minuties de terminaison et de bifurcation. Par exemple, les boucles peuvent être visualisées en tant que deux bifurcations. Chaque minutie est représentée par les cordonnées (x, y) de sa position dans l'image, et l'angle Θ qui est la direction associé à la strie (**la figure 1.13**). Donc chaque minutie de l'empreinte est repérée par un vecteur de la forme[12] : (Type de minutie, x, y,Θ).

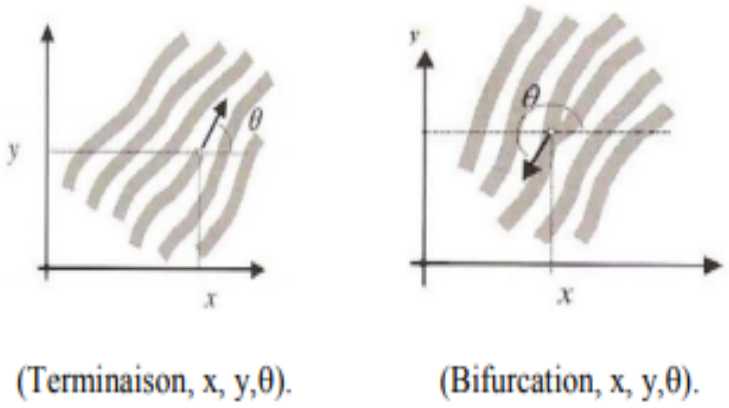

FIGURE 1.13 – Représentation des vecteurs de terminaison et de bifurcation. [30]

1.3.3 Structure d'un système de reconnaissance d'empreintes digitales :

Un système automatique complet de reconnaissance d'empreintes digitales est une chaîne de processus qui à partir du doigt d'un utilisateur en entrée renvoie un résultat en sortie, permettant ainsi à l'utilisateur d'accéder ou non à des éléments nécessitant une protection. La réalisation d'un tel système a fait l'objet de très nombreuses recherches et des méthodes très différentes de traitement ont été proposées. Cependant ces systèmes répondent toujours à la même structure (**figure 1.14**) :

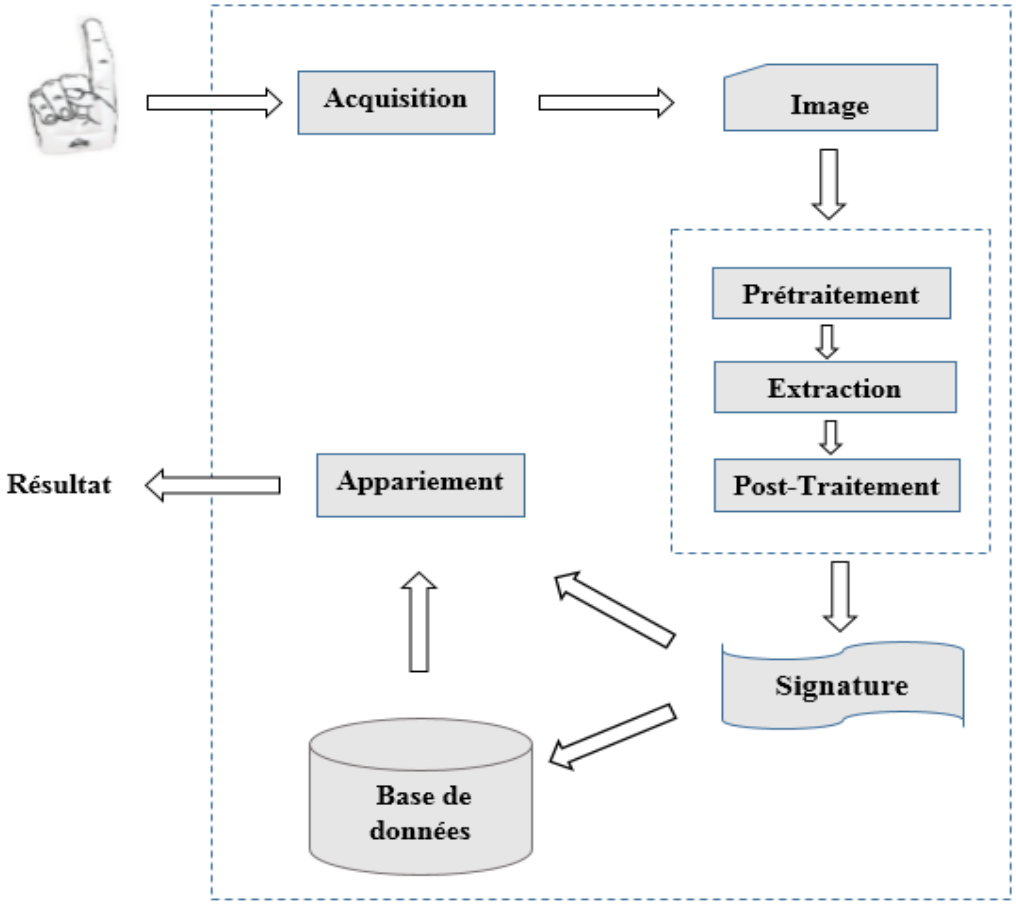

FIGURE 1.14 – Architecture générale d'un système complet de reconnaissance d'empreintes.

1.3.3.1 L'acquisition de l'image d'empreinte

La première phase d'un système de reconnaissance consiste à obtenir une image de l'empreinte du doigt.

La capture de l'image d'une empreinte digitale consiste à trouver les lignes tracées par les crêtes (en contact avec le capteur) et les vallées (creux). L'image d'une empreinte est acquise par des procèdes directs (online) ou indirects (offline) :

L'acquisition directe : ce sont les capteurs, où on peut citer :

Les capteurs optiques (les plus répondus, dont le principe de fonctionnement est le même que celui du scanner ainsi ses prix acceptables), les capteurs thermiques, les capteurs à ultrasons qui sont assez chers, les capteurs intégrés au silicium .

L'acquisition indirecte : où il existe 2 méthodes :

- ✓ **L'empreinte acquise par encre** : après l'avoir enduit d'encre, le doigt est imprimé sur un bout de papier. Ce papier passe ensuite au scanner standard pour être numérisé.
- ✓ **les empreintes latentes** : elles sont formées suite à une légère trace laissée sur un objet due à la sécrétion constante de la sueur. Les services de sécurité décèlent ce genre de détails sur les lieux du crime à l'aide d'une poudre spéciale.

1.3.3.2 Pré-traitement

La reconnaissance d'une empreinte digitale est directement liée à la qualité de l'image obtenue au moyen du capteur. Ainsi dans la plupart des cas, un pré-traitement (**figure 1.16**) est nécessaire pour améliorer la qualité de l'image. Pour limiter les calculs des étapes suivantes du système l'image brute de l'empreinte est filtrée. Une opération de filtrage utilisant les caractéristiques locales de l'empreinte est ensuite appliquée à l'image de manière à améliorer sa qualité en éliminant le bruit[13].

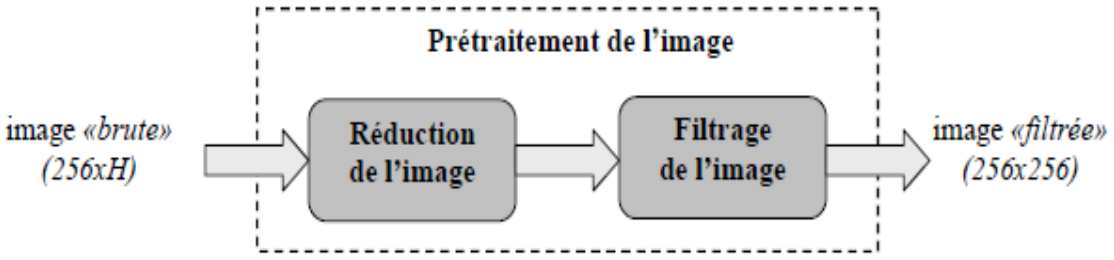

FIGURE 1.15 – Principe du pré-traitement de l'image.

1.3.3.3 Extraction des caractéristiques

La méthode classique : La méthode la plus répandue consiste à extraire les minuties à partir d'un squelette de l'image. Comme le montre la **figure 1.17** l'image est d abord préparée à l'étape d'extraction au moyen d une binarisation et d'une squelettisation, ensuite un fichier signature est extrait de l'empreinte après la détection et l'extraction des minuties[13].

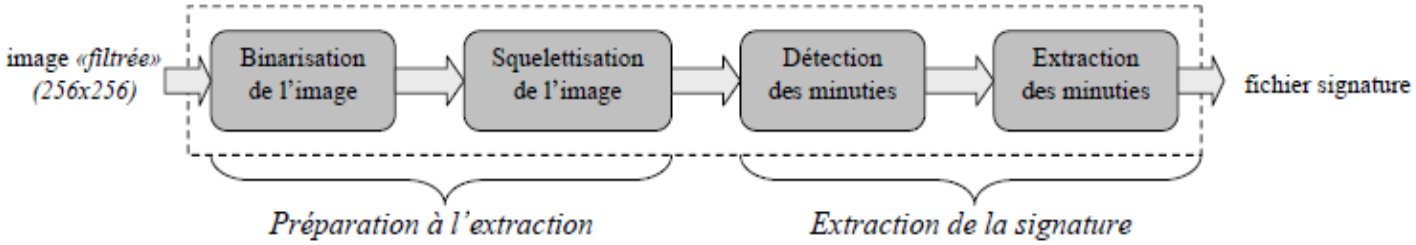

FIGURE 1.16 – La phase d'extraction de la signature

Estimation de champ d'orientation : Le champ d'orientation d'une image d'empreintes digitales représente la nature intrinsèque d'empreintes digitales (**figure 1.18**). C'est un étage essentiel pour déterminer les rides d'empreintes digitales et pour trouver la région d'intérêt d'image d'empreintes digitales, Il existe plusieurs méthodes pour estimer le champ d'orientation des images d'empreintes digitales. **Anil Jain** et **al** ont proposés une méthode efficace pour estimer le champ d'orientation d'une image.

FIGURE 1.17 – Le champ d'orientation d'une image d'empreinte digitale

L'idée principale de cette méthode est que l'image d'impatience digitale se divise en plusieurs fenêtres de taille WxW[32]. Pour tout pixel dans chaque fenêtre, on calcule les gradients Gx et Gy et puis on calcule l'orientation locale de ce pixel en utilisant la formule suivante :

$$v_x(i,j) = \sum_{u=i-\frac{w}{2}}^{i+\frac{w}{2}} \sum_{u=j-\frac{w}{2}}^{j+\frac{w}{2}} (2G_x(u,v)G_y(u,v)) \tag{1.7}$$

$$v_x(i,j) = \sum_{u=i-\frac{w}{2}}^{i+\frac{w}{2}} \sum_{u=j-\frac{w}{2}}^{j+\frac{w}{2}} (2G_x^2(u,v) - G_y^2(u,v)) \tag{1.8}$$

$$\theta(i,j) = \frac{1}{2}\tan^{-1}(\frac{v_x(i,j)}{v_y(i,j)}) \tag{1.9}$$

Avec : W : la taille de la fenêtre locale

G_x et G_y : sont les grandeurs de gradient dans des directions de x et de y respectivement

(i, j) : est l'orientation locale du pixel (i, j).

Segmentation : Après avoir estimé le champ d'orientation d'une image d'empreintes digitales, un algorithme de segmentation qui est basé sur le niveau de certitude du champ d'orientation est employé pour localiser la région d'intérêt dans l'image d'empreintes digitales[32]. Le niveau de certitude du champ d'orientation au pixel (i, j) est défini comme suit :

$$CL(i,j) = \sqrt{\frac{1}{w^2}\frac{v_x^2(i,j) + v_y^2(i,j)}{v_e(i,j)}} \tag{1.10}$$

Tel que :

$$v_e(i,j) = \sum_{u=i-\frac{w}{2}}^{i+\frac{w}{2}} \sum_{u=j-\frac{w}{2}}^{j+\frac{w}{2}} (2G_x^2(u,v) + G_y^2(u,v)) \tag{1.11}$$

Avec :

W : la taille de la fenêtre locale.

Gx et Gy : les grandeurs de gradient dans des directions de x et de y respectivement.

CL (i, j) : l'orientation locale du pixel (i, j).

Pour chaque pixel, si son niveau de certitude du champ d'orientation est inférieur d'un certain seuil T, il est marqué comme pixel de fond. Sinon il est marqué comme un pixel de la région d'intérêt.

La Binarisation : Pour permettre la squelettisation, l'image doit d'abord être binarisée, c'est-à-dire que l'image en 256 niveaux de gris dont nous disposons à ce stade est transformée en image binaire où les pixels noirs correspondent aux stries et les pixels blancs aux vallées[14]. Pour effectuer ce traitement la valeur de chaque pixel P(x, y) est comparée à un seuil T et si cette valeur est supérieure au seuil le pixel prend la valeur de un (noir), sinon il prend la valeur de zéro (blanc),(**figure 1.18**).

$$P(X,Y) = \{ \text{ 1 si } P(x,y) \geqslant T$$
$$\{0 \text{ si } P(X,y) \leqslant T$$

FIGURE 1.18 – Résultats de de binarisation

La squelettisation : Pour faciliter l'extraction des minuties l'image doit être squelettisée : une suite d'opérations morphologiques d érosion va réduire l'épaisseur des stries jusqu'à ce que cette dernière soit égale à un pixel tout en conservant la connexité des stries (c'est-à-dire que la continuité des stries doit être respectée, il ne faut pas introduire de trous). Nous avons utilisé l'algorithme de Rosenfeld[15] pour sa simplicité. Pour chaque pixel p_0 on considère son voisinage immédiat de 8 pixels $P_i, i \in [1..8]$. Pour l'algorithme de squelettisation on considère les définitions suivantes :

1. P_0 est un point frontière Nord si $P_2 = 0$
2. P_0 est un point frontière Est si $P_4 = 0$
3. P_0 est un point frontière Sud si $P_6 = 0$
4. P_0 est un point frontière Ouest si $P_8 = 0$
5. P_0 est un point 8-terminal si un seul de ses voisins est noir ($\exists i \in [1..8], p_i = 1$), il s'agit d'une minutie de type terminaison .
6. P_0 est un point 8-isolé si aucun de ses voisins n'est noir ($\forall i \in [1..8], p_i = 0$)
7. P_0 est un point 8-simple si la connexité de ses 8 voisins n'est pas altérée quand on le transforme en pixel blanc.

P_1	P_2	P_3
P_8	P	P_4
P_7	P_6	P_5

La squelettisation consiste à répéter les opérations d'érosion suivantes jusqu'à ce que plus aucun pixel ne soit changé :

- **Etape 1** : tous les pixels noirs vérifiant (1) et (7) et ne vérifiant pas (5) et (6) sont changés en pixels blancs (érosion des points frontières Nord) .
- **Etape 2** : tous les pixels noirs vérifiant (2) et (7) et ne vérifiant pas (5) et (6) sont changés en pixels blancs (érosion des points frontières Est)
- **Etape 3** : tous les pixels noirs vérifiant (3) et (7) et ne vérifiant pas (5) et (6) sont changés en pixels blancs (érosion des points frontières Sud) .
- **Etape 4** : tous les pixels noirs vérifiant (4) et (7) et ne vérifiant pas (5) et (6) sont changés en pixels blancs (érosion des points frontières Ouest). La propriété (7) peut être ignorée dans les étapes d'érosion car bien qu'un point unique corresponde à une minutie sa présence à ce stade du traitement est très probablement due à un résidu de bruit, il vaut donc mieux l effacer. Il est à noter que plus l'épaisseur des stries sera importante et plus le processus sera long. La **figure 1.20** montre le résultat obtenu à partir d'une image binaire filtrée.

FIGURE 1.19 – Résultats de de squelettisation

La détection des minuties : Les deux étapes de préparation à l extraction (binarisation et squelettisation) ont grandement facilité cette phase. En effet nous disposons maintenant d'une image binaire squelettisée : un pixel noir prend la valeur 1, un pixel blanc prend la valeur 0 et la largeur des stries est égale à 1 pixel. Si l'on calcule le nombre de transitions divisé par 2 entre un pixel blanc et un pixel noir pour chaque point du squelette, on obtient le nombre CN de stries partant de ce point (Crossing Number) et nous pouvons donc déterminer simplement le type d'un pixel[13] (voir **figure 1.21**).

Ainsi pour chaque pixel P appartenant à une strie (c'est-à-dire pour chaque pixel qui prend la valeur de 1), le calcul de CN peut prendre cinq valeurs :

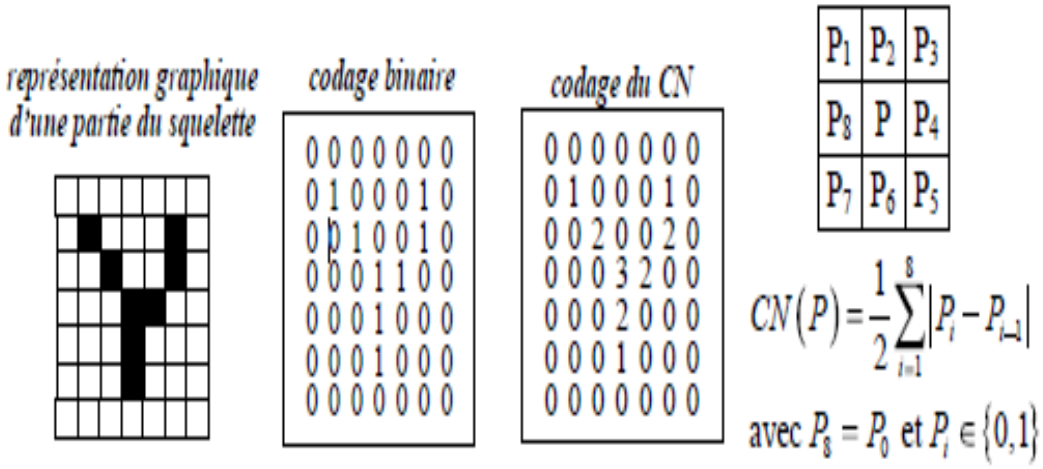

FIGURE 1.20 – Les différentes représentations du squelette.

— CN (P) =0 : dans ce cas il s'agit d'un pixel isolé et nous n'en tenons pas compte, car même si ce type de minutie existe, il est très rare et à ce stade du traitement il est probablement dû à un résidu de bruit.
— CN (P)=1 : dans ce cas nous avons à faire à une minutie de type terminaison.
— CN (P)=2 : c'est le cas le plus courant, le pixel se situe sur une strie, il n'y a pas de minutie.
— CN (P)=3 : nous sommes en présence d'une bifurcation triple.
— CN (P)=4 : nous sommes en présence d'une bifurcation quadruple. Ce type de minutie étant assez rare il est probablement dû au bruit que nous l'ignorons.

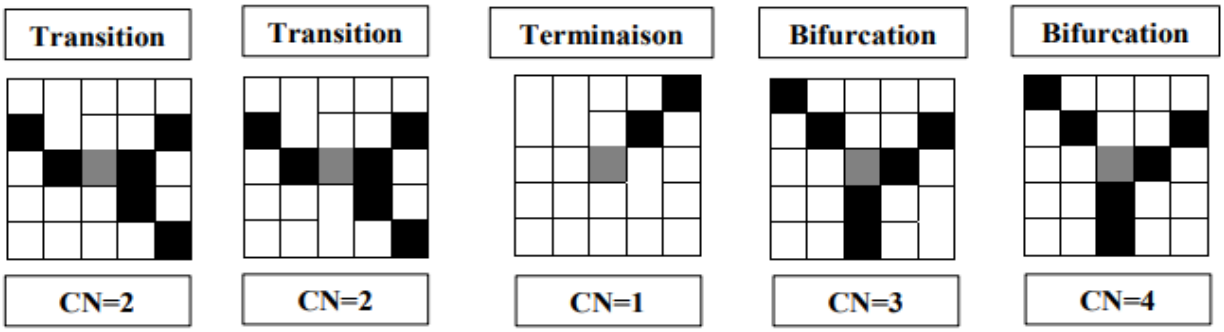

FIGURE 1.21 – Exemples de détermination du type de minutie en fonction du calcul de CN.

1.3.3.4 Post-traitement

L'objectif de ce processus est d'éliminer au maximum les fausses minuties tout en conservant les vraies détectées. Pour cela, on utilise des considérations empiriques[16],[17] basées sur le fait que la distance entre deux minuties voisines est toujours supérieure à un certain seuil. En effet, pratiquement, il est extrêmement rare de trouver deux vraies minuties très

proches, par contre on a quasiment toujours une concentration locale de plusieurs fausses minuties.

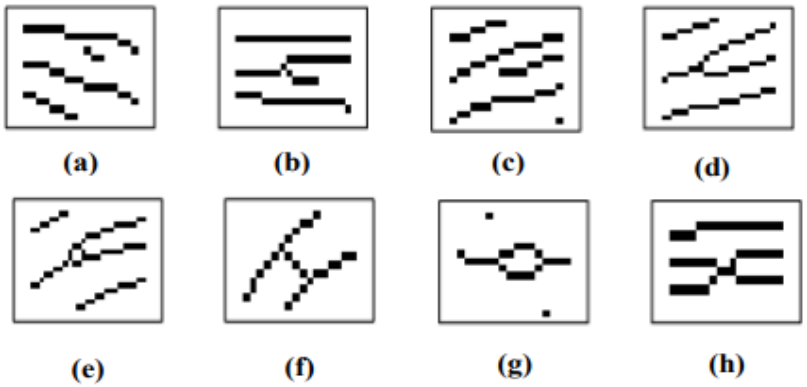

FIGURE 1.22 – Exemples de détermination du type de minutie en fonction du calcul de CN.

Traitement des terminaisons détectées

Pour éliminer les fausses terminaisons, nous suivons les règles suivantes : S'il existe un bloc adjacent au bloc contenant la terminaison T (XT ; YT) et appartenant au bord de l'image, alors T est une fausse minutie et nous élimine.

Pour les terminaisons restantes T, on parcourt la strie qui lui est associée sur une distance maximum K1, jusqu'à atteindre le point A.

FIGURE 1.23 – Validation des terminaison détéctes : vrai terminaison(a), branche parasite(b), segment trop court(c)

Traitement des bifurcations détectées

Lorsqu'on détecte un point B candidat pour le titre de bifurcation (CN (B)=3), on parcourt les trois stries qui lui sont associées sur une distance maximum de K jusqu'à atteindre trois points A_1, A_2 et A_3 (**Figure 1.25**). Plusieurs cas peuvent se produire et ils sont traités dans l'ordre suivant :

— $d < K_1$, $d < K_2$, $d < K_3$ la zone circulaire de centre B et de rayon K1 contient au moins quatre minuties. On considère alors que nous sommes dans une zone très bruitée (regroupement important) et que B est une fausse bifurcation.

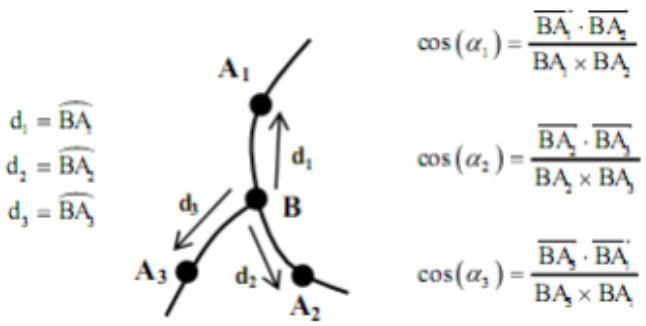

FIGURE 1.24 – Définitions associée a une bifurcation lors de la phase de validation.

CN (A_1)=1, CN (A_2)=1, CN (A_3)=1 : au moins une des stries mène à une terminaison. On est dans le cas d'une branche parasite, le point B et les terminaisons atteints ne sont pas validés.

— A_1= A_2 ou $A_2 = A_3$ où $A_3 = A_1$: deux des stries mènent au même point. On est dans le cas d'un îlot , le point B et la bifurcation atteinte ne sont pas validés.

— Nous avons deux des stries qui mènent à deux bifurcations A_1 et A_2 (CN (A_1) =3, CN (A_2)=3). Dans ce cas, on calcule la différence angulaire $\alpha 1$ ainsi que la distance $\| \overrightarrow{A_1A_2} \|$ entre les deux bifurcations rencontrées. Si les conditions $|\cos(\alpha 1)| > \cos(\Pi \div 4)$ et $\| \overrightarrow{A_1A_2} \| \leq \lambda$ (B correspond à la distance inter-strie locale du bloc contenant B) sont réunies, alors on est dans le cas d'un triangle et on considère que B est une vraie bifurcation tandis que A1 et A2 sont des fausses.

— Une seule des stries mène à une bifurcation A1 (CN (A_1) = 3). On calcule les différences angulaires $\alpha 1$ et $\alpha 2$ ainsi que la distance entre A1 et B.$|\cos(\alpha 2)| > \cos(\Pi \div 4), |\cos(\alpha 1)| > \cos(\Pi \div 4)$ et $|BA_1| \leq \lambda$ alors on est dans le cas d'un pont et A_1 et B sont considérés comme de fausses minuties.

— Dans tous les autres cas, le point B est validé en tant que vraie bifurcation. La **figure 1.26** du processus d'extraction des minuties ainsi que la phase d'élimination des fausses terminaisons et bifurcations.

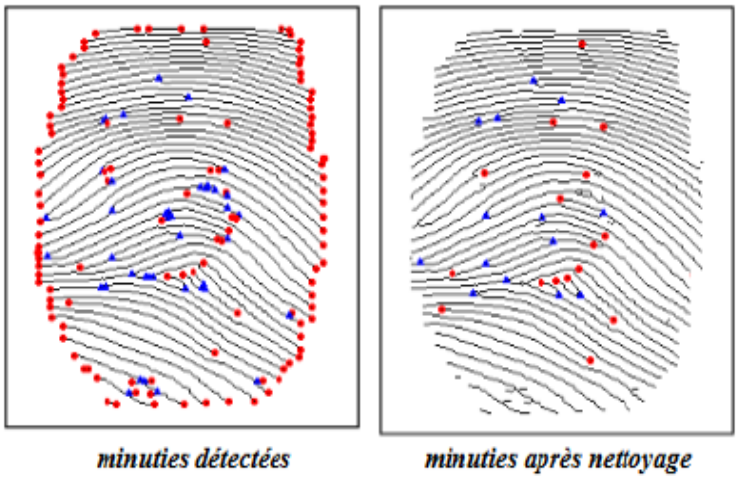

FIGURE 1.25 – Résultat de la phase d'élimination des fausses minuties.

1.3.4 Comparaison des empreintes digitales

La comparaison des empreintes digitales consiste à réaliser un accord entre la signature à identifier et les signatures stockées dans la base de données. Cependant cette tâche n'est pas facile[18], notamment à cause de la variabilité dans les différentes impressions d'une même empreinte (variation intra-classe)**figure 1.27**.

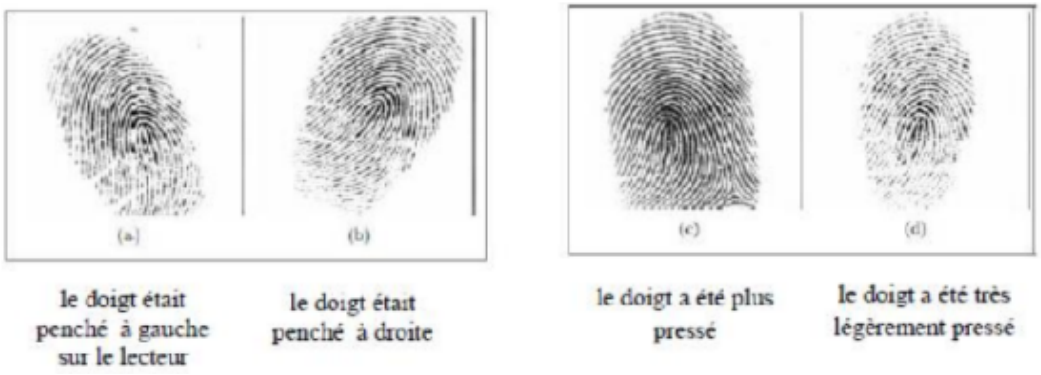

FIGURE 1.26 – Les différentes positions de même doigt.

Il existe plusieurs approches classifiées en 3 catégories principales :

1.3.4.1 Approches basées sur la corrélation

Cette approche est basée sur la corrélation des pixels de deux empreintes digitales, Elle consiste à comparer tout simplement les matrices de pixels des images de deux empreintes, et calculer la corrélation de pixels.

1.3.4.2 Approches basées sur les crêtes

Dans cette approche, on utilise des caractéristiques extraites des crêtes (orientation, texture, forme de ride, etc.) pour comparer les empreintes digitales. L'avantage de cette approche est que les caractéristiques de crêtes peuvent être extraites plus exactement, cependant les distinctions de ces caractéristiques sont faibles.

1.3.4.3 Approches basées sur les minuties

C'est l'approche la plus utilisée dans la littérature, des minuties sont extraites à partir des deux empreintes digitales et stockées sous forme d'un ensemble de points dans le plan de deux dimensions. L'assortiment basé sur minuties essentiellement se compose de trouver l'alignement entre les minuties du motif et les minuties d'entrée. Le résultat est le nombre maximum des pairs de minuties.

1.4 Conclusion

Dans ce premier chapitre, nous avons présenté une vue générale de la biométrie, un survol sur quelques techniques biométriques, ainsi que l'architecture d'un système biométrique, ses applications et ses avantages. Ensuite, nous avons entamé d'une façon détaillée la technique à utiliser dans notre travail et qui est celle de l'empreinte digitale, où nous avons spécifié les caractéristiques d'une empreinte digitale, la structure générale d'un système de reconnaissance d'empreintes digitales, ainsi que les différentes approches de comparaison pour déterminer la correspondance entre deux empreintes.

Dans le chapitre suivant, nous allons présenter les cryptosystémes biométriques et ses méthodes, en détaillant la technique proposé et qui est notre intérêt dans ce mémoire.