REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE
MINISTERE DE L'ENSEIGNEMENT SUPERIEUR
ET DE LA RECHERCHE SCIENTIFIQUE
UNIVERSITE MOULOUD MAMMERI DE TIZI-OUZOU

Faculté de Génie Electrique et d'Informatique
Département D'Electronique

Mémoire
De fin d'études

En vue de l'obtention du diplôme
d'Ingénieur d'Etat en Electronique
Option : Communication

THEME

Authentification biométrique des individus

Proposé par :

M^r^ LAZRI Mourad

M^me^ AMEUR Zohra

Réalisé par:

M^r^ CHERIFI Mehdi

M^r^ HADDAD Mohamed

Dirigé par:

M^r^ LAZRI Mourad

Promotion : Juin 2010

Remerciements

Au terme de ce travail, nous tenons à exprimer nos vifs remerciements à M^me^ AMEUR et M^r^ LAZRI pour leurs orientations et conseils tout au long de l'élaboration du présent mémoire.

Nous tenons à remercier tous les enseignants d'ELECTRONIQUE qui ont contribué à notre formation

Nous tenons à remercier aussi le personnel de la bibliothèque pour leur disponibilité.

Nos remerciements à tous ceux qui ont participé de prés ou de loin à l'élaboration de ce mémoire et qui se sont dévoués pour nous venir en aide.

Nos remerciements à nos familles et tous les amis (es)

Enfin, nous tenons à remercier également les membres de jury qui nous ferons l'honneur de juger notre travail.

Merci à tous

Dédicaces

Je dédie ce modeste travail :

À mes chers parents, pour leur soutien, leur patience et leur amour

À Mes deux sœurs Dyhia et Meriem

À Mes deux frères Ahmed et Brahim

À Mes grands parents

À Mes tantes et mes oncles

À Mes cousins et cousines

À Et a tous mes amis (es)

À mon binôme Mohamed ainsi que sa famille

À tous mes enseignants

Mehdi

Dédicaces

Je dédie ce modeste travail :

A mes parents qui m'ont encouragé et soutenu durant toute la durée de mes études

A mon frère Mourad et mes sœurs Radia et Hayat

A mes deux grand-mères

A mes oncles et tantes

A mes cousins et cousines

A mes amis (es)

A mon binôme Mehdi ainsi que sa famille

Mohamed

Résumé

La biométrie faciale est l'une des biométries les plus utilisées, elle sert à la reconnaissance des individus par leur visage dans différents contextes tels que l'identification des criminels et le contrôle d'accès. Notre travail consiste en la conception et la réalisation d'un système dédié à l'authentification de visages.

Pour réaliser un système performant, l'approche Analyse en Composantes Principales (ACP) est utilisée en limitant les images d'apprentissage à celles d'un seul individu, elle est appelée par certains auteurs « self eigenfaces ». La transformée en Cosinus (DCT2) est appliquée en amont l'ACP. Pour la phase de décision, un critère de ressemblance a été introduit, il est basé sur la distance euclidienne. L'architecture de notre système est constituée d'un PC (Personal Computer) muni d'une Webcam.

Les tests effectués en utilisant les bases d'images connues et inconnues montrent que le taux de reconnaissance obtenu avec la marge fixée avec les deux distances euclidiennes maximale et minimale est bon.

Mots clés : biométrie, vérification du visage, ACP, self eigenfaces.

Table des matières

Liste des tableaux

Liste des figures

Chapitre I — Introduction à la biométrie

Chapitre II — Reconnaissance des visages

Chapitre III — Analyse en composantes principales

Chapitre IV — La carte à puce

Liste des sigles et abréviations

ACP : Analyse en Composantes Principales
AFC : Analyse Factorielle des Correspondances
API: Application Programming Interface
ASC: Avec et Sans Contact
ATR: Answer To Reset
CCD: Charger Coupled Device
DCT: Discriminant Cosinus Transformation
DES: Data Encryption Standard
DF: Dedicated File
EBGM: Elastic bunch graph Matching
EER: Equal Error Rate
EF: Elementary File
EMV: Auropay Mastercard Visa
FA: False Acceptance
FAR: False acceptance Rate
FID: File Identifier
FFT: Fast Fourier Transform
FR: False Rejection
FRR: False Rejection Rate
GMM: Gaussian Micture Models
GSM: Global System for Mobile
GUIDE: Graphical User Interface Development Environment
HMM: Hidden Markov Model
HTER: Half Total Error Rate
IEC : International Electrotechnical Commission
IEF: Internal Elementary File
ISO: International Standard Organisation
LDA: Linear Disciminant Analysis
MF: Master File
NLDA: Null space Linear Disciminant Analysis
NN: Neural network
OLDA: Orthogonal Linear Disciminant Analysis
PC/SC: Personal Computer / Smart Card
PIN: Personal Identifier Number
RAM: Random Access Memory
ROC: Receiver Opertaing Characteristics
ROM: Read Only Memory
RSA: Rivest Shamir Adelman
SFI: Short File Identifier
SSO : Single Sign-On
SVM: Support Vector Machines
TER: Total Error Rate
TSR : Total Success Rate
ULDA: Uncorrelated Linear Disciminant Analysis
WEF: Working Elementary File
EO: Eigen Objects

Avant propos

Depuis quelques décennies, la biométrie connaît un essor dans le monde de la recherche mais aussi dans le domaine commercial. Le visage en particulier se démarque des autres biométries par son coût relativement bas et par le fait qu'il soit non intrusif donc bien intégré par l'utilisateur. Jusqu'à présent, aucune méthode aussi sophistiquée soit-elle n'a pu atteindre les capacités de l'homme dans son authentification en raison de multiples difficultés et complexité des représentations des visages humains. C'est pour cette raison que la biométrie suscite toujours un engouement par les chercheurs.

La technologie des cartes à puce permet, quant à elle, un éventail d'applications. Pas seulement dans la biométrie mais pour des applications plus vastes telles que la santé, le suivi de la scolarité, etc. Tout comme les autres systèmes embarqués (Pocket PC, Smart phone, etc.), la carte à puce connaît un développement important dans le domaine industriel mais aussi dans la recherche qui a pour but d'augmenter ses performances en terme de temps et d'espace pour en faire un support physique sécurisé, peu coûteux et peu encombrant de par sa petite taille

La conception des systèmes d'authentifications qui connaissent une ascension fulgurante ne peut que faire l'objet de recherche et d'applications pour être déployés là où la sécurité est impérative afin de se débarrasser des stratégies de sécurité conventionnelles telles que les badges ou mot de passe et surtout de réduire de façon significative la fraude.

Introduction

Un système biométrique est une application permettant l'identification ou l'authentification automatique d'une personne. Cette dernière se voit reconnaître par conséquent certains droits ou services notamment l'accès. Ce genre de système est basé sur la reconnaissance de particularités physiques (empreintes digitales, iris de l'oeil, etc.), de traces (ADN, sang, odeurs), ou d'éléments comportementaux (signature, démarche, etc.).

Jadis, les systèmes biométriques étaient surtout utilisés par la police à des fins de sécurité mais de nos jours, une personne a besoin d'un contrôle automatique de son identité et ce, dans divers contextes, citons le contrôle d'accès physique et virtuel. En effet, l'authentification est nécessaire à l'individu pour pénétrer dans son immeuble, ouvrir la porte de son appartement, pour accéder à son poste de travail, pénétrer dans des bâtiments et y circuler librement ou encore pour retirer de l'argent à un distributeur, accéder à sa messagerie, à Internet et plus généralement, partout où la sécurité est essentielle.

Parmi les différentes biométries, le visage est la caractéristique la plus utilisée par l'homme pour identifier un membre de son entourage. Afin de simuler ce comportement biologique, les chercheurs se sont mis à concevoir des systèmes de plus en plus performants. Dès lors, la reconnaissance des visages a connu un fort développement et elle reste un domaine qui suscite toujours des interrogations et un engouement par les chercheurs.
La reconnaissance par le visage ne nécessite pas beaucoup de coopération de la part de la personne à reconnaître par rapport aux autres méthodes et ainsi, elle est très bien intégrée par ses utilisateurs dans leur vie de tous les jours.

A cela, s'ajoute l'évolution fulgurante des systèmes embarqués. Cette nouvelle technologie a surgit après de grands progrès technologiques concernant le développement de processeurs de plus en plus puissants et de mémoires de stockage de plus en plus volumineuse. De par leurs performances en terme de temps et d'espace et de leur faible coût, les systèmes embarqués ont envahi le quotidien de l'homme, citons à titre d'exemple les téléphones sans fil, les smart phones, les pockets PC et les cartes à puce.

Actuellement, la biométrie est de plus en plus utilisée pour remplacer les mots de passe, les clés, les badges et les pièces d'identités. En effet, les caractéristiques biométriques d'un individu ne peuvent être oubliées ou perdues encore moins transmises à autrui, volées, dupliquées ou devinées.

Dans ce cadre, nous proposons un système de contrôle d'accès que nous baptisons SRF (Système Reconnaissance Facial) qui permet de réaliser le lien entre les caractéristiques biométrique d'une personne physique et celles de l'individu à partir de la base d'images préalablement sauvegardées lors de l'apprentissage. Nous avons opté, pour ce qui est de la reconnaissance faciale, pour l'Analyse en Composantes Principales (ACP) appliquée aux visages d'un seul individu « Self Eigenfaces » car notre système est dédié seulement à la vérification. Cette méthode rapide et efficace et simple à mettre en œuvre.

Le mémoire est structuré en une partie théorique regroupant les chapitres de 1 à 5, qui présentent toutes l'information récoltée dans la littérature et nécessaire pour introduire la partie pratique. Le chapitre 1 introduit la biométrie et ses différents types. Le chapitre 2 présente la biométrie faciale et ses multiples approches. L'Analyse en Composantes Principales et son application aux visages sont décrites dans le chapitre 3. Le chapitre 4 introduit la carte à puce, sa structure, son fonctionnement et ses applications. Le chapitre 5 décrit les architectures existantes pour les systèmes de reconnaissance faciale utilisant la carte à puce. La partie pratique, regroupant les trois derniers chapitres : le chapitre 6 décrit la conception du système SRF basé sur la distance euclidienne en ACP. La réalisation du système avec l'outil de développement est détaillée dans le chapitre 7. Le dernier chapitre présente les tests obtenus sur des images et démontre l'efficacité de l'approche choisie. Le mémoire est clôturé avec une conclusion générale proposant diverses perspectives. Les références bibliographiques sont présentées par chapitre de façon à alléger la lecture. Enfin des annexes sont ajoutées à la fin du mémoire pour apporter un complément d'informations au lecteur.

Chapitre I

Introduction à la biométrie

« La biométrie consiste à vérifier l'identité d'une personne à l'aide d'une ou plusieurs modalités qui lui sont propres » **[ber 04]**. Elle représente l'ensemble des techniques d'identification fondées sur la mesure du corps. En d'autres termes, c'est une approche permettant de déterminer l'identité d'un individu par la reconnaissance automatique de certaines de ses caractéristiques physiques ou comportementales préalablement enregistrées (empreintes digitales, visage, voix,…etc.). C'est vrai que pour identifier une personne, on utilise des codes, des mots de passe et autre, mais ces techniques n'assurent pas autant de fiabilité que l'utilisation de la biométrie. Cette dernière se base sur des caractéristiques qui sont propres à la personne c'est-à-dire qui peuvent la différencier de toute autre personne, mais aussi qui ne changent pas avec le temps. Il est aussi possible d'utiliser les techniques traditionnelles conjointement avec les systèmes biométriques, par exemple, sauvegarder les caractéristiques du visage sur une carte à microprocesseur qui ne peut être activée qu'avec un mot de passe.

1-Types de biométrie

Il y a deux grandes catégories de biométrie: la biométrie morphologique et la biométrie comportementale **[ani 98]**.

1-1 La biométrie morphologique (physiological biometrics)

Appelée aussi biométrie physiologique, elle se base sur les traits physiques particuliers qui, pour toute personne, sont uniques et permanents. Cette catégorie regroupe la reconnaissance des empreintes digitales, de la forme de la main, du visage, de la forme de l'oreille, de la rétine et de l'iris **[max 02]**.

1-2 **La biométrie comportementale** (behavioral biometrics)

Elle est basée sur l'analyse de certains comportements d'une personne comme le tracé de sa signature (inclinaison et vitesse de déplacement du stylo, la pression exercée), l'empreinte de sa voix, sa démarche et sa façon de taper sur un clavier (vitesse de frappe) **[max 02]**.

Il existe, par ailleurs, une autre catégorie qui est l'étude des traces biologiques telles que l'odeur et l'ADN.

On peut aussi classer la biométrie en deux catégories : la biométrie intrusive et la biométrie non intrusive. La première est contraignante pour l'utilisateur : elle impose un

certain nombre de contraintes d'utilisation du système biométrique. Tandis que la deuxième ne requière pas un contact direct avec l'individu.

2-Présentation des systèmes biométriques

La diversité des caractères biométriques de l'être humain a donné naissance à plusieurs systèmes biométriques.

2-1 Les empreintes digitales

C'est la plus ancienne technique connue dans la biométrie. Elle se base sur le fait que les boucles, les tourbillons, les lignes et les verticilles (cercle concentrique au centre d'un doigt) qui forment les empreintes sont propres à chaque individu et même à chaque doigt. Cette technique nécessite que l'utilisateur pose un doigt sur un capteur d'empreinte spécifique. Ensuite, un traitement est effectué sur l'image.

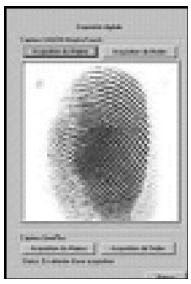

Figure I.1 Empreinte digitale **[jea 06]**

Cette technologie est résistante aux changements de températures jusqu'à un certain seuil, son coût est assez abordable, elle présente néanmoins quelques problèmes de fiabilité. En effet, les empreintes digitales d'un travailleur manuel le rendent réfractaire à toute identification.

Elle se caractérise aussi par des problèmes de contraste (doigt propre et sec devient trop clair tandis qu'un doigt humide et recouvert d'un film gras devient foncé) d'autre part le dispositif CCD peut s'user avec le temps et devenir moins fiable **[com 03].** Ce dernier inconvénient peut être pallié en utilisant un capteur sans contact. La reconnaissance des empreintes peut être utilisée comme système d'identification. Par exemple, les citoyens de HongKong sont tous munis de cartes d'identité biométriques comportant leurs empreintes. Elle peut aussi être utilisée pour le control d'accès. Par exemple, SAGEM a présenté en 2001, « MORPHOACCESS », un terminal de contrôle d'accès utilisant l'empreinte digitale comme moyen d'identification ou d'authentification **[biom]**.

2-2 La forme de la main ou des doigts de la main

Aussi ancienne que la reconnaissance par les empreintes digitales, cette technique nécessite que l'utilisateur pose sa main face à une caméra digitale avec un éclairage infrarouge (où alors l'image de la main peut être scannée). Ainsi, une centaine de caractéristiques sont récupérées, entre autres, la longueur et largeur des doigts, la longueur inter articulations,…etc. Le résultat est indépendant de l'humidité des doigts et de souillures éventuelles car il n'y a pas de contact direct avec le capteur, donc pas de risque d'encrassement. La reconnaissance par la forme de la main présente aussi d'autres avantages qui sont la facilité de l'enrôlement du point de vue de l'usager, une bonne acceptation psychologique ainsi qu'un faible volume de stockage par fichier. Cependant ces systèmes présentent un risque élevé de taux de fausses acceptations et faux rejets, à cause d'une blessure par exemple. Cette technique est surtout répandue aux États-Unis où plus de 90 % des centrales nucléaires l'utiliseraient, de même que l'armée américaine et plus récemment dans des écoles, des hôpitaux, des cafétérias et des banques **[max 02]**.

Figure I.2 Forme de la main scannée **[bio]**

2-3 Le visage

Francis Galton instaura les prémices de ce que devrait être la reconnaissance faciale dès 1888 dans son ouvrage "Personnal identification and description" **[biom].** Lorsque la puissance des ordinateurs est devenue suffisante et que les recherches les plus poussées ont commencé, on a vu alors apparaître des systèmes de reconnaissance faciale fonctionnels. Ces derniers nécessitent que l'utilisateur soit face à une caméra afin d'extraire les caractéristiques les plus importantes de son visage. C'est la technique la plus simple et la moins contraignante, néanmoins elle reste sensible à l'environnement lors de l'acquisition. En effet, ses performances peuvent être altérées en raison de l'angle de prise de vue, la luminosité, l'arrière plan, la distance entre la caméra et l'individu, un prétraitement est donc nécessaire avant d'entamer le processus de reconnaissance.

Actuellement, il existe des systèmes de reconnaissance faciale en 3D montrant de très bonnes performances, ils nécessitent néanmoins des ressources plus coûteuses que celles utilisés pour l'exploitation des visages en 2D.

Figure I.3 Acquisition du visage

2-4 La rétine

Cette technique se base sur le fait que les vaisseaux sanguins d'une rétine sont uniques pour chaque personne. La personne doit placer son oeil face à un orifice de capture situé sur le dispositif d'acquisition. Un faisceau lumineux traverse l'oeil jusqu'aux vaisseaux sanguins capillaires de la rétine. Le système localise et capture ainsi environ 400 points de référence **[ani 98].** Cette approche est résistante aux fraudes. De plus, la cartographie de la rétine est la même tout au long de la vie, en l'absence de maladies spécifiques. Cependant elle présente quelques inconvénients qui sont: un coût élevé, une installation délicate et elle est, de plus, mal acceptée par les utilisateurs car ces derniers doivent placer leurs yeux à très faible distance du capteur. Cette technique est utilisée dans les milieux à haute sécurité tels que la NASA [**flo 02]**.

Figure I.4 Détail de la rétine **[flo 02]**

2-5 L’iris

Même si la couleur de l’iris de l’oeil est déterminée génétiquement, sa texture détaillée est propre à chaque individu voir à chaque oeil. Pour cette technique, l’image de l’iris d’une personne est acquise par un appareil qui contient une caméra infrarouge ou ordinaire, ainsi, environ 250 caractéristiques sont alors capturées. Cette approche est fiable, elle est cependant intrusive pour les usagers et présente aussi des contraintes d’éclairage.

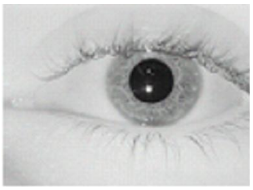

Figure I.5 Iris de l’oeil **[jea 06]**

La société japonaise « OKI Electric Industry » a développé un système de reconnaissance biométrique par analyse de l'iris à partir d'un simple Appareil photo numérique pour appareils mobiles. La reconnaissance de l’iris est utilisée dans le secteur financier pour les employés et les clients, dans les institutions carcérales, les hôpitaux, les aéroports et les écoles **[jea 06]**.

2-6 La voix

Comme la voix de tout individu est unique et qu’elle peut être représentée graphiquement, il suffit de faire lire à la personne une série de mots mainte fois et d’extraire par la suite plusieurs caractéristiques de sa voix telles que le débit, la dynamique et la forme des ondes produites. Il faut isoler les caractéristiques formant une empreinte unique car la voix d’une personne peut varier (maladie, états émotionnels, vieillissement, etc.).

On peut diviser la vérification du locuteur en deux modes : **[ani 98]**

- ***indépendant du texte***: il s’agit de systèmes qui n’ont aucune connaissance à priori du mot ou de la phrase qui va être prononcé. L’utilisateur peut donc dire ce qu’il souhaite lors de l’authentification.
- ***dépendant du texte:*** ces systèmes ont une connaissance préalable de ce qui va être prononcé.

Ces systèmes sont non intrusifs. Même si les imitateurs utilisent les caractéristiques vocales sensibles au système auditif humain, ils ne sont pas capables de recréer les harmoniques de la

voix servant de base à l'identification, il est quasi impossible d'imiter la voix stockée dans la base. Cette approche présente néanmoins des inconvénients qui sont : la sensibilité à l'état physique et émotionnel de la personne et la sensibilité aux conditions d'enregistrement du signal de la parole : bruit, parasites, qualité de l'équipement. Des fraudes sont possibles en utilisant un enregistrement de la voix de la personne autorisée, ces fraudes sont facilitées dans le cas de système basé sur la lecture d'un texte fixe.
Ces systèmes sont utilisés par les corps policiers, les hôpitaux et en téléphonie.

2-7 La thermographie faciale

Les différentes parties du visage émettent des quantités de chaleur qui varient d'un individu à un autre. Ceci est du au fait qu'elles dépendent de la localisation des veines, de la quantité de tissus, de muscles, de graisses, etc. Pour capturer l'image, il est possible d'utiliser un appareil photo ou une camera numérique dans le domaine de l'infrarouge.

Figure I.6 Images obtenues avec une caméra optique et une caméra thermique **[ani 98]**

La capture peut se faire dans n'importe quelle condition d'éclairage et même dans le noir complet, cette technique est efficace même après une chirurgie plastique.

Néanmoins, elle reste sensible à la pose ainsi qu'à la température corporelle ou l'état émotionnel de l'individu **[flo 02]**.

2-8 L'écriture (signature)

Peu utilisée, cette technique peut être exécutée de deux manières différentes.

- Reconnaissance « online » : nécessite que l'utilisateur signe avec un stylo électronique sur une tablette graphique (reconnaissance « online »), une extraction des caractéristiques spécifiques d'une signature comme la vitesse, la pression sur le crayon, le mouvement et les points sera effectuée.

- Reconnaissance « offline » : la signature est scannée puis comparée à une signature préalablement enregistrée.

Cette approche est non intrusive, elle dépend cependant de l'état émotionnel de la personne. Elle est utilisée dans les banques, les prisons et les services postaux.

Figure I.7 Tablette graphique **[rue]**

2-9 La dynamique de frappe au clavier

Comme tout ordinateur est muni d'un clavier, cette technique ne nécessite qu'un logiciel qui extrait des caractéristiques uniques lorsqu'une personne tape sur un clavier telles que la vitesse de frappe, les temps de frappe et les temps de pause entre les mots [**biom]**.

Ce dispositif biométrique est utilisé comme méthode de vérification dans le commerce électronique et comme mécanisme de contrôle d'accès à des bases de données. Cette approche est non intrusive, elle dépend néanmoins de l'état physique de l'usager (âge, maladie…).

2-10 L'analyse de la démarche

Les études médicales dans les années 1964-1967 ont révélé l'existence de 24 composants différents de la démarche humaine. Si l'on considère toutes ces mesures, la démarche est unique. Un cycle de démarche correspond à un cycle complet de la position debout: pied droit avant – par terre – pied gauche avant - par terre. Cette nouvelle biométrie, apparue dans les années 1990, est destinée à des applications telles que la surveillance à distance, le contrôle d'accès et le diagnostic médical. Son inconvénient majeur est qu'elle est sensible aux changements d'habits, chaussures, surface **[ani 98]**. Ceci rend cette approche limitée au monde de la recherche seulement.

2-11 L'oreille

La forme de l'oreille ainsi que la structure du tissu cartilagineux du pavillon de l'oreille sont utilisés pour distinguer un individu d'un autre. Les approches de reconnaissance par l'oreille sont basées sur la comparaison des vecteurs des distances des points saillants à partir de quelques points de repères (voir la figure I.8). Les caractéristiques du pavillon d'une oreille ne sont pas uniques à chaque individu. C'est pour cette raison qu'il n'existe aucun système

commercialisé basé sur la reconnaissance par l'oreille. Ce genre de système ne reste qu'un travail de recherche **[ani 98].**

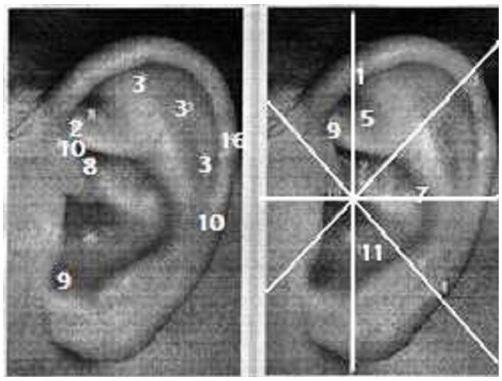

Figure I.8 l'oreille et de ses caractéristiques extraites pour la reconnaissance. **[ani 98]**

2-12 L'analyse de l'ADN

La génétique a permis de démontrer que l'ADN est la particularité la plus fiable pour identifier une personne. Cette technique est assez contraignante pour l'utilisateur (prélèvement sanguin ou capillaire) et nécessite beaucoup de temps, d'où sa non utilisation pour des applications à temps réel **[ani 98]**.

De nouvelles techniques sont en développement, citons à titre d'exemple, l'analyse de l'empreinte de la chaussure (shoe print). Quelques chercheurs classent cette technique dans la biométrie bien qu'elle ne le soit pas. Cette modalité peut aider les services de criminologie dans leurs quêtes à retrouver et à identifier un individu laissant des traces sur la scène du crime.

Il existe des techniques des plus inattendues comme la reconnaissance de mots (noms d'individus) et des différents styles de la parole (lente, rapide, relâchée et hyper articulée) en se basant sur les mouvements labiaux et mécanismes d'articulation **[ren 03]**.

3- Les parts de marché par technologie

La moitié du marché est consacré aux systèmes de reconnaissance par l'empreinte digitale (environ 58.9% du chiffre d'affaires total) (voir Figure I.9). Plus de la moitié de ce taux est consacré au système AFIS (automatic fingerprint identification system) utilisé en Suisse depuis 1984 **[ejp]**. Le succès de ces systèmes est dû essentiellement à leur précision et leur coût relativement bas. Vient ensuite la reconnaissance par l'analyse du visage qui a gagné, durant ces dernières années, des parts du marché en dépassant la reconnaissance de la

main qui avait, jadis, la deuxième place en termes de source de revenus **[biom].** De nos jours, la recherche est orientée vers la conception de systèmes bimodaux voir même multimodaux.

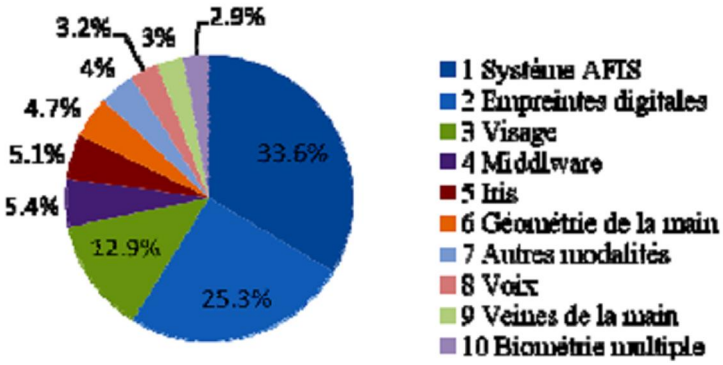

Figure I.9 Distribution des systèmes biométriques sur le marché en 2007**[biom]**

4 - Les modes opératoires d'un système biométrique

Un système biométrique peut avoir deux modes opératoires **[flo 02]** qui sont la vérification et l'identification ; l'identification consiste à reconnaître une personne parmi d'autres (1 parmi N). La vérification quant à elle, consiste à vérifier si la personne est bien ce qu'elle prétend être, en d'autres termes le système vérifie que l'identité de la personne correspond bien à celle déclinée par cet individu (1 parmi 1).

5- Evaluation des systèmes biométriques

Un système biométrique peut être évalué selon différents critères tels que : la précision, l'efficacité (vitesse d'exécution), ainsi que le volume de données stockés pour chaque individu. Nous nous intéresserons au premier aspect qui est la précision. L'identification et la vérification sont des modes opératoires différents. Elles nécessitent donc des mesures de précision différentes.

5-1 Evaluation de la vérification

La vérification est un problème de *décision* qui peut être formulé de la manière suivante :

Soient :

$H0$ l'hypothèse : « la capture C provient d'un imposteur ».

$H1$ l'hypothèse : « la capture C provient de l'utilisateur légitime ».

Il faut donc choisir l'hypothèse la plus probable. On considère que la capture C provient d'un utilisateur légitime si $P(H1|C) > P(H0|C)$.

En appliquant la loi de Bayes on obtient : **[flo 02]**

$$\frac{P(C\backslash H1)P(H1)}{P(C)} > \frac{P(C\backslash H0)P(H0)}{P(C)}$$

Et donc : $$\frac{P(C\backslash H1)}{P(C\backslash H0)} > \frac{P(H0)}{P(H1)}$$

Le ***score de vraisemblance*** (likelihood ratio) $S = \frac{P(C\backslash H1)}{P(C\backslash H0)}$ est comparé à un seuil θ appelé ***seuil de décision.***

Les valeurs *P* (*H*0) et *P* (*H*1) qui représentent respectivement la probabilité pour qu'un imposteur ou un utilisateur légitime essayent d'accéder au système sont des valeurs difficiles à estimer.

La figure I.10 représente la distribution hypothétique des taux de vraisemblance qu'obtiendraient les utilisateurs.

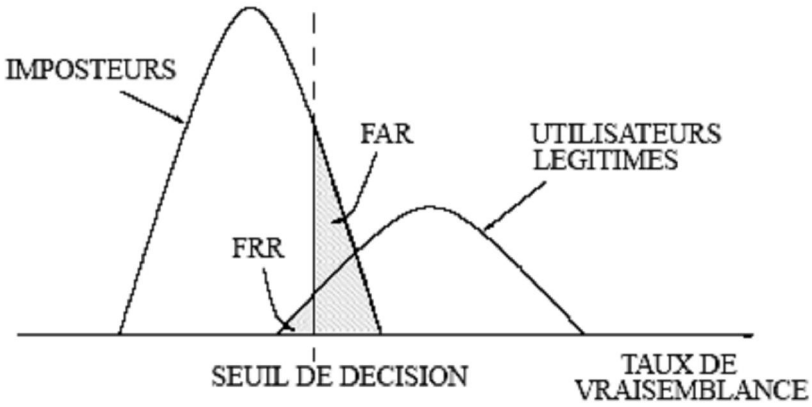

Figure I.10 Distributions des taux de vraisemblance des utilisateurs légitimes et des imposteurs dans un système biométrique. **[flo 02]**

Lors de la vérification, le score S est comparé au seuil de décision θ, si S est inférieur à θ alors l'individu est accepté sinon celui-ci est rejeté. Deux types d'erreurs peuvent être commises par le système:

- *La fausse acceptation* (FA): Correspond au cas où le système accepte un individu qui a proclamé une identité qui n'est pas la sienne.
- *Le faux rejet* (FR) : Correspond au cas où le système rejette un client légitime.

Les performances de ce type de système se basent principalement sur le taux de faux rejet et le taux de fausse acceptation : **[ate 04]**

FAR (taux de fausse acceptation) = $\frac{nombre\ de\ fausses\ acceptations}{nombre\ d'imposteurs\ présentés}$

FRR (taux de faux rejet) $= \frac{nombre\ de\ faux\ rejets}{nombre\ de\ clients\ présentés}$

On remarque à travers la figure I.10 que plus le seuil de décision θ est petit, plus le système acceptera de clients légitimes mais aussi des imposteurs, plus θ est grand plus le système rejettera d'imposteurs mais aussi des utilisateurs légitime. Le paramétrage d'un système consiste à trouver le bon équilibre entre ces deux taux.

Les performances d'un système biométrique peuvent être représentées graphiquement à l'aide de la courbe ROC (Receiver Opertaing Characteristics) sur laquelle les FRR's sont données en fonction des FAR's (voir Figure I.11). Cette courbe est obtenue en calculant un couple (FAR, FRR) pour chaque valeur de seuil de décision, ce dernier varie de la plus petite valeur des scores obtenus en phase de test à la plus grande valeur.

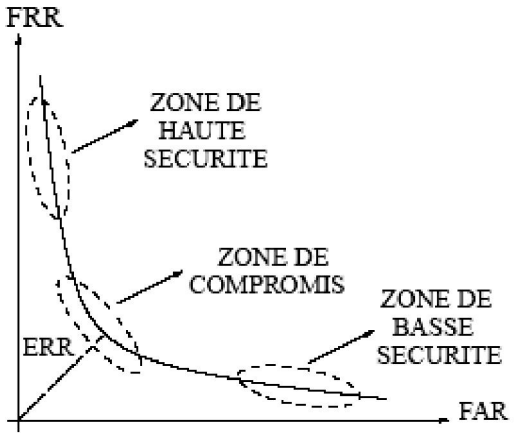

Figure I.11 Courbe ROC **[ani 98]**

Il existe d'autres critères fréquemment utilisés pour donner un aperçu des performances des systèmes de vérification :

- Le taux d'erreur égal (Equal Error Rate ou EER) correspond à l'intersection de la courbe ROC avec la première bissectrice, en d'autre terme L'EER correspond au point de fonctionnement pour lequel le taux de faux rejet est égal au taux de fausse acceptation.

§ Le HTER (Half Total Error Rate), il représente la moyenne du FAR et FRR.

$$HTER = (FAR + FRR) / 2$$

§ Le TER (Total Error Rate) : Taux d'erreur global, il correspond au taux d'erreur total (faux rejet et fausse acceptation) obtenu lors du test **[ate 04]**.

TER = (nombre de clients rejetés+nombre d'imposteurs acceptés)/nombre total d'accès

§ Le TSR (Total Success Rate) Taux de réussite global, c'est le complément du TER **[BC97].**

$$TSR = 1-TER$$

5-2 Evaluation de l'identification

Le type d'erreur commise par ce type de système est d'attribuer à l'individu présenté une identité autre que la sienne.

Les performances de ces systèmes sont mesurées à l'aide du taux d'identification correcte (TIC) **[jam 02]**

$$TIC = \frac{nombre\ de\ tests\ ayant\ amené\ à\ une\ identification\ correcte}{nombre\ total\ de\ tests}$$

Ce paramètre dépend du nombre de personnes contenues dans la base de données, en effet plus la base de données est volumineuse plus le taux d'erreur est grand.

6-La multi modalité dans la biométrie

Il existe différentes formes de multi modalités : **[flo 02]**

6-1 Systèmes multiples biométriques

Utiliser en même temps plusieurs modalités biométriques du corps humain, par exemple combiner le visage, les empreintes digitales ainsi que la voix.

6-2 Systèmes multiples d'acquisition

Utiliser plusieurs techniques d'acquisition sur la même modalité biométrique. Par exemple, utiliser deux scanners différents (l'un optique, l'autre thermique) pour la reconnaissance d'empreintes digitales.

6-3 Mesures multiples d’une même unité biométrique

Par exemple, faire la reconnaissance sur les deux iris au lieu d’un seul, ou bien faire la reconnaissance sur les dix doigts d’un même individu.

6-4 Instances multiples d’une même mesure

Faire une capture répétée du même attribut biométrique avec le même système d’acquisition. Par exemple, effectuer une authentification pour plusieurs images faciales d’un individu à partir d’une vidéo à des intervalles précis.

6-5 Algorithmes multiples

Utiliser différents algorithmes de reconnaissance sur le même signal d’entrée. Par exemple combiner les deux méthodes GMM et SVM pour la reconnaissance du locuteur.

Dans ce chapitre, nous avons abordé les différents systèmes biométriques existants ainsi que leur distribution dans le marché. L'objectif de chaque système est d'améliorer ses performances de reconnaissance en minimisant le taux d'erreur commise pour une identification et une vérification. Dans le but d'obtenir de meilleures performances, les chercheurs ont recourt à la combinaison de deux ou plusieurs modalités différentes. Dans le chapitre suivant, nous axerons notre étude sur une biométrie bien particulière : le visage.

Chapitre II

Reconnaissance des visages

Rien n'est plus naturel que d'utiliser le visage pour identifier une personne. En effet, les images faciales sont la caractéristique biométrique la plus communément employée par l'homme pour effectuer une identification personnelle.

De plus, c'est une biométrie non intrusive qui est bien tolérée par les utilisateurs. D'après le schéma ci-dessous, la reconnaissance par l'analyse du visage s'avère être un bon compromis entre le coût et la précision **[ber 04]**.

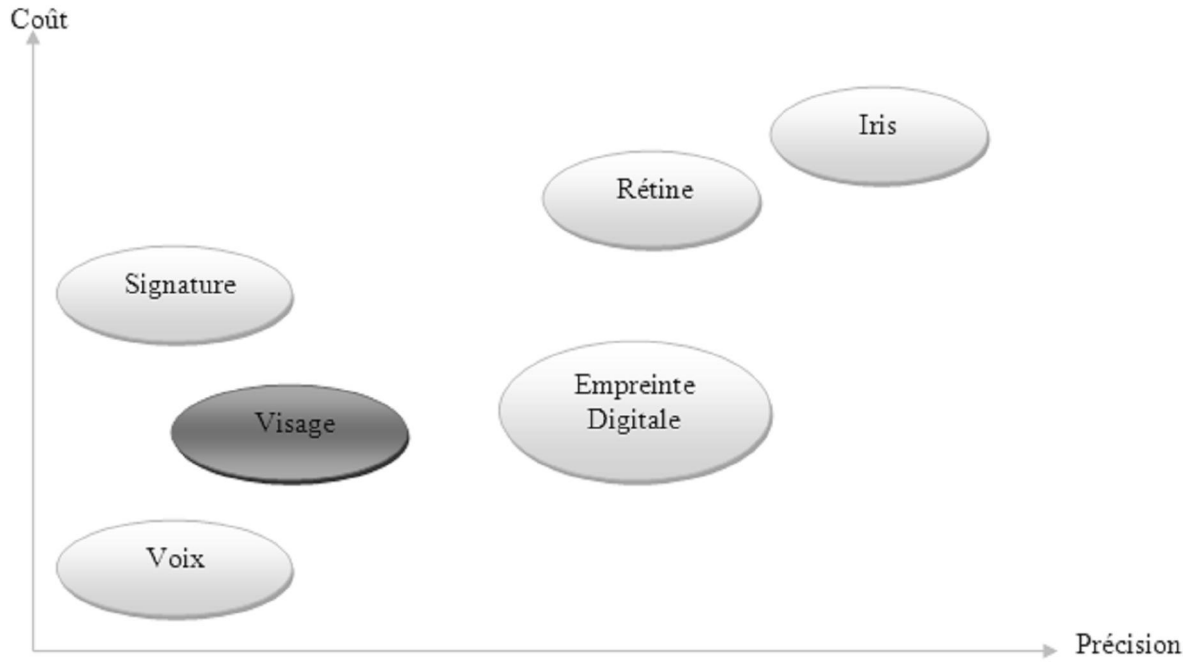

Figure II.1 Comparaison entre les différentes biométries existantes par rapport à leurs coûts et leurs précisions **[ber 04]**

1 - Etapes de fonctionnement d'un système biométrique

Que ce soit lors de la phase d'apprentissage ou la phase de test, le processus de reconnaissance de visage passe par plusieurs étapes :

- Acquisition ou capture de l'image
- Prétraitement de l'image
- Extraction des caractéristiques et calcul du modèle
- Prise de décision

1-1 Acquisition et numérisation d'une image

Cette étape exige la coopération du sujet car elle agit grandement sur la qualité des résultats de l'identification et de la vérification.

L'acquisition d'une image peut se faire moyennant un scanner, un appareil photo ou une caméra. Dans notre cas, elle se fait au travers d'une webcam. Ce dispositif électronique d'acquisition se charge de récolter les signaux, émis par les photodiodes, ligne par ligne, espacés d'un bref temps de synchronisation. Ce balayage renvoie le spectre de l'image qui est une fonction continue.

Vient ensuite la conversion des signaux analogiques en données numériques positives comprises entre 0 et 255 (0 : noir, 255 : blanc et entre les deux se situent les différents niveaux de gris), c'est ce que l'on appelle la numérisation.

Numériser une image c'est représenter son contenu par un ensemble structuré de données numériques. Une image est dite numérique après l'avoir échantillonnée et quantifiée.

L'*échantillonnage* (résolution spatiale) est le procédé de discrétisation spatiale d'une image consistant à associer à chaque zone rectangulaire R(x, y) d'une image continue (signal continu) une unique valeur I(x, y). Il dépend essentiellement de la taille d'ouverture du balayage. On parle de sous échantillonnage lorsque l'image est déjà discrétisée et que l'on veut diminuer le nombre d'échantillons.

La *quantification* (résolution tonale) désigne la limitation du nombre de valeurs différentes que peut prendre I(x, y). C'est-à-dire que l'on choisit le nombre de niveau de gris pour coder chaque pixel. Généralement, on choisit 256 niveaux de gris (représentation de chaque pixel sur 8 bits) ce qui est suffisant pour représenter les variations perceptibles par l'oeil humain **[ant 07]**.

1-2-Prétraitement

Le prétraitement des images sert à extraire des informations noyées dans le bruit ou abîmées par les défauts optiques des instruments, par exemple, réduire le bruit granuleux ou équilibrer les variations de la luminosité. Il opère point par point en utilisant l'histogramme: il agit sur chaque pixel indépendamment de ses voisins, ou alors, il opère d'une manière locale en utilisant les filtres : ces derniers agissent sur un pixel en observant son voisinage.

Au niveau de l'histogramme : on peut effectuer plusieurs opérations, entre autres : l'étirement et l'égalisation.

Au niveau des filtres : Selon la linéarité, il existe deux catégories : filtres linéaires et filtres non-linéaires. Selon le type d'amélioration effectuée sur l'image, il existe des filtres d'accentuation et des filtres de lissage (voir annexe 2). Ces différents filtres opèrent dans le domaine spatial ou fréquentiel (par transformation de Fourier, transformation en cosinus ou autres) (voir annexe 1).

1-3 Modélisation

Après acquisition et amélioration de l'image du visage, l'extraction de ses caractéristiques s'effectue selon une approche donnée pour générer le modèle biométrique de l'individu. Cette phase constitue l'étape clé du processus, car les performances du système entier dépendent de la précision avec laquelle les informations utiles sont extraites. De nombreuses méthodes ont été proposées, elles se répartissent en deux catégories : Les méthodes géométriques et les méthodes globales **[nic]** [**moa] [hug 03]**.

1-3-1 Les Méthodes Globales

Cette classe regroupe les méthodes qui mettent en valeur les *propriétés globales* de la forme. Le visage est traité *comme un tout*. C'est-à-dire que ces méthodes utilisent l'intégralité de la surface du visage comme source d'information.

1-3-1-1 Analyse en composantes principales (PCA : Principal Component Analysis)

L'ACP est appliquée dans la reconnaissance des visages en 1991 par Turk et Pentland au MITMediaLab **[mat 91]**, cette approche est connue sous le nom de Eigenfaces ou visages propres. Elle utilise une collection d'images de visages pour créer un espace propre. Chaque image est projetée dans ce sous espace pour obtenir un vecteur caractéristique de dimensions réduites sans grande perte d'information. On dira que ce visage appartient à une classe donnée si le score est en dessous d'un certain seuil. Cette approche est efficace et simple à mettre en oeuvre mais elle est sensible aux variations de lumière, de pose et d'expression faciale. Elle fera l'objet du chapitre suivant.

1-3-1-2 Analyse discriminante linéaire (LDA : Linear Discriminant Analysis)

Appliqué aux images en1997 par Belhumeur et al de la Yale University aux USA, l'algorithme LDA, aussi connu sous le nom de Fisherfaces, est très proche de celui du PCA sauf que la séparation de la base d'images en classes s'effectue en amont. Pour séparer en

classe la base d'images d'apprentissage de sorte que chaque classe comporte plusieurs images de la même personne, on calcule les matrices de dispersion interclasses et intra classes puis on cherche une projection qui minimise la dispersion intra classes (variation des images d'une même personne) et maximise la dispersion interclasses (variation des images de personnes différentes). Après application de la projection sur les images apprises et image teste, on utilise les mêmes critères que l'ACP pour effectuer l'association entre l'image teste et sa classe adéquate. Lorsque le nombre d'individus à traiter est plus faible que la résolution de l'image, les matrices de dispersion peuvent être non inversibles, ce qui rend difficile l'application de la LDA. Pour contourner ce problème, des variantes ont été mises au point telles que ULDA, OLDA, NLDA **[nic]**.

1-3-1-3 Réseaux de neurones (NN : Neural Networks)

Un réseau de neurones artificiels (RNA) est en général composé d'une succession de couches dont chacune prend ses entrées sur les sorties de la précédente. Chaque couche j est composée de N_j neurones prenant leurs entrées sur les N_{j-1} neurones de la couche précédente. Chaque neurone calcule la somme des entrées puis cette valeur passe à travers la fonction d'activation pour produire sa sortie **[jer 07]**.

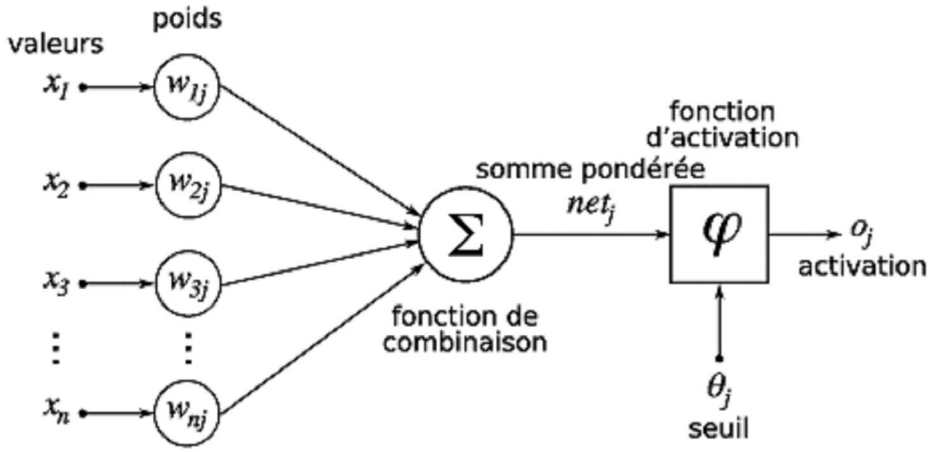

Figure II.2 Structure d'un neurone artificiel

Cette approche dépend grandement de l'apprentissage. L'avantage de ce modèle est le gain de temps considérable grâce au traitement parallèle. Cependant, l'utilisation d'exemples pour l'apprentissage apporte le risque de ne pouvoir résoudre que des situations déjà rencontrées,

où un phénomène de sur-apprentissage qui spécialiserait le réseau uniquement sur les exemples connus sans généraliser **[moa]**.

1-3-1-4 Machine à vecteurs de support (SVM : Support Vecteur Machine)

Cette approche a été introduite par Vapnik au milieu des années 90. Faisant partie de la famille des classifieurs binaires, les SVM recherchent le meilleur hyperplan séparant deux groupes pour que cette frontière linéaire produise une marge maximale. Le succès de ce type de méthodes est principalement dû à leur performance et à leur développement qui est très actif. La frontière de décision d'un SVM peut être très dépendante des données d'apprentissage, chose qui peut poser problème lorsque le nombre d'observations d'apprentissage est réduit. Aussi, les SVM sont des méthodes relativement coûteuses en temps de calcul et dont le paramétrage (choix du noyau, paramètres du noyau, la contrainte de violation) est souvent difficile. Enfin, les SVM ne considèrent que la discrimination entre deux classes. Pour cela, il existe des variantes de cette technique telle que l'algorithme de Friedman **[cha 06]**.

1-3-1-5 Mélange de gaussiennes (GMM : Gaussian Mixture Models)

La reconnaissance par mélanges de gaussiennes est l'une des techniques les plus récentes dans le domaine de la biométrie, elle a été proposée par Conrad Sanderson et al, cette approche consiste à modéliser la distribution des vecteurs DCT, issus des images acquises, par une combinaison de composantes (densités) gaussiennes. Chaque composante est caractérisée par un vecteur moyen et une matrice de covariance **[fre]**.

1-3-2 Les Méthodes locales

On les appelle aussi les méthodes géométriques **[nic]**, analytiques, à traits ou approche par composantes **[hug 03]**.

L'analyse du visage humain est donnée par la description individuelle de ses parties et de leurs relations. Son but est d'extraire les traits tels que les yeux, le nez et la bouche à partir d'une image du visage et de représenter ensuite le visage selon un modèle adéquat.

1-3-2-1 EBGM : Elastic bunch graph matching

Conçue en1997 par Wiskott et al de la Southern California University aux USA et de la Rurh University en Allemagne. Cette méthode commence tout d'abord par localiser des points précis sur le visage (nez, coins des yeux, de la bouche, etc.) manuellement ou d'une manière

automatique. Un treillis élastique virtuel relie les points localisés sur l'image. A chaque point ou noeud, on associe un Jet c'est-à-dire un jeu de coefficients (fréquence, orientation, phase) des ondelettes de Gabor. On obtient alors un Face Bunch Graph (FBG). On calcule ensuite la similarité entre les FBG de l'image teste et celle de la base d'apprentissage, et cela en maximisant la correspondance entre les deux treillis.

L'EBGM qui a trouvé ses fondements dans les neurosciences et qui agit localement sur des parties du visage, a une plus grande robustesse aux changements de luminosité, de pose et d'expression faciale. Néanmoins, son implémentation est moins évidente comparée à l'ACP ou LDA **[nic]**.

1-3-2-2 Modèles de Markov Cachés (HMM : Hidden markov model)

Les modèles de Markov cachés ou HMM de base sont utilisés pour des données modélisées dans une seule dimension. L'approche Embedded HMM (encastrés) manipulant l'image en deux dimensions, est la plus utilisée car elle génère des résultats supérieurs par rapport aux différentes variantes des HMM qui ont été proposées. Les Embedded HMM sont caractérisés par l'utilisation d'un HMM de base, modélisant l'apparence du visage de haut en bas. Ensuite, chacun des états de ce modèle général contient un autre HMM 1D, dénommé embedded (un HMM incorporé). Ceux-ci modélisent cette fois l'apparence du visage de la gauche vers la droite. Reposant sur certains coefficients de la transformée en cosinus discrète (DCT) comme source d'observations, les Embedded HMM constituent un algorithme de reconnaissance très performant. Par contre, les temps d'exécution des phases d'apprentissage et de test sont relativement élevés, nuisant donc à son utilisation en temps réel sur d'immenses bases d'images **[nou 07]**.

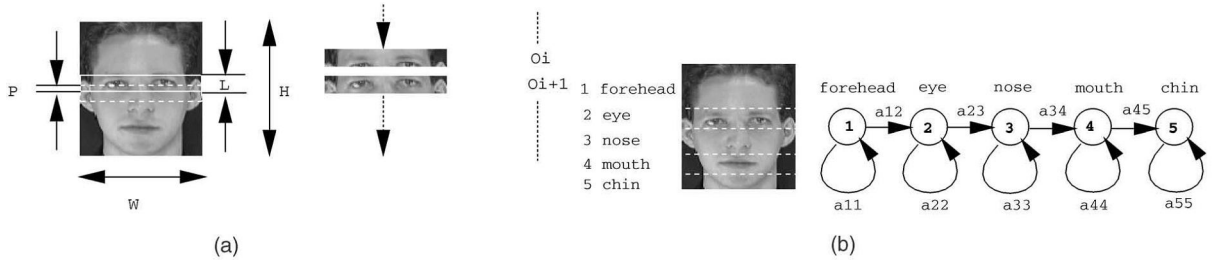

Figure II.3 La chaîne de Markov pour la localisation du visage **[min 02]**

1-3-2-3 EO : Eigen Objects

Cette méthode repose sur le même principe que l'Eigenfaces, la différence réside dans le fait que EigenObjects ne s'intéresse pas à tout le visage mais seulement à quelques régions du visage à savoir : les yeux, le nez, la bouche, les oreilles, etc. Elle a été conçue pour pallier au

problème des expressions faciales, car ces dernières affectent moins des parties du visage plutôt que le visage dans sa globalité. Lors de la phase de prétraitement, une localisation de ces régions est effectuée, la précision de cette tâche est donc cruciale.

Contrairement aux visages, les yeux et le nez se ressemblent davantage entre eux, ce qui rend les fausses identifications plus fréquentes. Par contre, grâce à la combinaison des représentations individuelles, certaines ressemblances peuvent être éliminées **[ale 03]**.

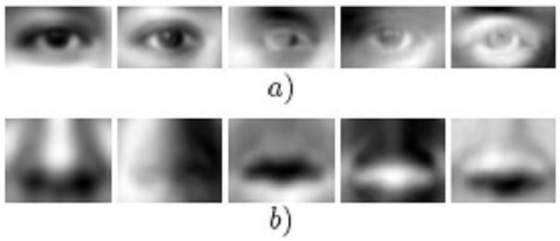

Figure II.4 EigenObjects : L'image moyenne et les 4 premiers vecteurs propres pour l'œil gauche (a) et le nez (b) **[ale 03]**

1-3-3 Approche fusion

Dans le but d'améliorer l'efficacité des algorithmes de reconnaissance faciale, les chercheurs ont pensé à combiner plusieurs approches afin de jumeler les avantages des méthodes choisies pour la fusion. Par exemple : DCT + PCA, LDA + PCA, EO + HMM, HMM + DCT + EO, DCT + EO, DCT + HMM, DCT + PCA + EO.

1-4 La vérification et l'identification

Lors d'une identification une comparaison 'un_pour_plusieurs' est effectuée entre le modèle de l'individu et les modèles de toutes les classes de visages de la base d'images.

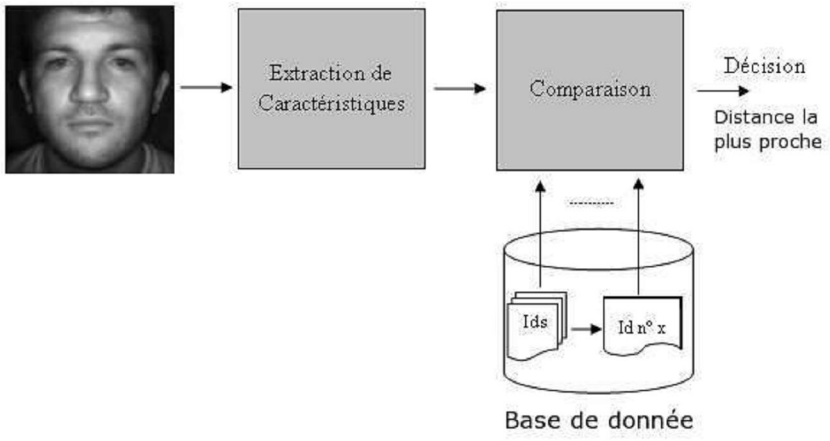

Figure II.5 Schéma d'identification du visage **[wal 09]**

Quant à la vérification, une comparaison directe dite ‘un_pour_un’ entre le gabarit calculé et le gabarit de référence est effectuée, autrement dit, le modèle de l’individu est comparé uniquement à la classe de ses visages. Suite à cette comparaison, le système fournira les personnes les plus ressemblantes dans le cas d’une identification. Concernant la vérification, le système nous indiquera si l’individu est bien ce qu’il prétend être. On trouve cette application dans le contrôle d’identité à l’entrée des Etats-Unis **[wal 09]**.

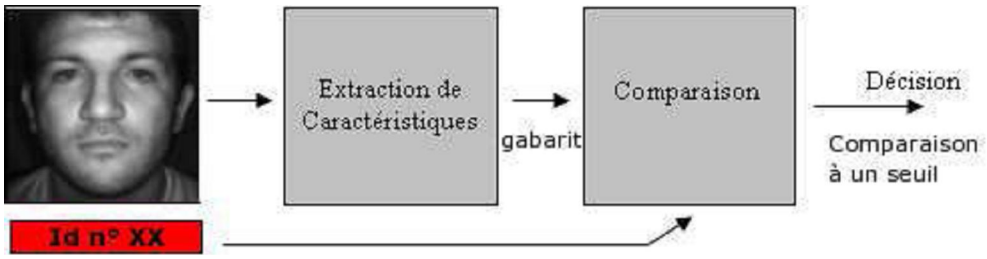

Figure II.6 Schéma de vérification du visage **[wal 09]**

2-Les systèmes biométriques existants pour la reconnaissance des visages

Les systèmes biométriques de reconnaissance des visages se trouvent être de plus en plus répandus. Voici cités ci-dessous quelques systèmes mis en oeuvre ainsi que les différents domaines d’utilisation de cette technologie en pleine expansion :

Le 14 octobre 1998, le *Borough de Newham* de Londres mît en service un système qui a diminué le nombre de crimes et délits de 10 % en 6 mois, grâce à l'utilisation du logiciel de reconnaissance de visage appelé « Mandrake ». Le système alertait les opérateurs de caméra dès qu'il y avait 80 % de concordances entre l'image préalablement numérisée d'un délinquant et ce que captaient les caméras.

Les systèmes de reconnaissance des visages sont déployés dans le transport aérien, le système « SmartGate » par exemple a été mis en oeuvre afin d’effectuer une vérification automatique de l'identité pour l'équipage d'Aéronef traversant la frontière de l'Australie. Ce dernier effectue une comparaison entre le visage d'une personne à sa photographie de passeport **[emi].**

En Janvier 2002, « Viisage Technology » le fournisseur de technologie et services de reconnaissance des visages a annoncé l'installation du premier système de reconnaissance des visages en Floride dans l'aéroport international St. Petersburg- Clearwater **[cub].** Cette technologie est aussi utilisée afin d'identifier les personnes recherchées en comparant les photos des passeports avec une base de personnes recherchées.

Il existe encore toute une panoplie d'utilisations de la reconnaissance des visages. Aujourd'hui Les ATM's (Automatic Teller Machine : Distributeurs automatiques de billet mis en services par les banques ou autres institutions financières) identifient les utilisateurs non

grâce à leurs numéros de carte bancaire, mais en se référant en plus à leur visage. En effet, l'ATM capture une image d'un visage et compare celle-ci avec la photo de la base afin de confirmer son identité.

Plusieurs entreprises ont orienté leurs activités vers cette technologie, on retrouve par exemple L'Entreprise « Widget » qui a mis au point le système « Snappy Face » qui permet d'identifier le visage du propriétaire de l'ordinateur pour sécuriser son accès grâce à une webcam.[**ube],** ou encore « Titanium Technology Entreprise » basée à Pékin qui a développé un logiciel de reconnaissance automatique de visages pour la surveillance (Automatic Face Recognition Systems ou AFRS) nommé « ProFacer iDVR » **[mes 04]**.

Dans ce chapitre, nous nous sommes intéressés au fonctionnement des systèmes de reconnaissance basés sur le visage. Puis nous avons énoncé quelques systèmes commercialisés sur le marché. Cet engouement pour les systèmes de reconnaissance des visages est justifié par les nombreux avantages de cette approche. En effet cette technologie est peu coûteuse, peu encombrante, elle est, de surcroît, peu contraignante pour les usagers. Dans le chapitre suivant, nous allons détailler une des méthodes utilisées dans la reconnaissance faciale qui est l'analyse en composantes principales.

Chapitre III

Analyse en composantes principales

Les méthodes factorielles telles que l'ACP et l'AFC simple ou multiple se basent sur la recherche d'axes principaux pour représenter les données ; Cette technique commune à ces méthodes est décrite dans l'analyse générale.

1-Méthode factorielle : Analyse générale d'un tableau de données [leb 81]

Soit X un tableau de données quantitatives, à n lignes et p colonnes.
Ce tableau étant de grande dimension, on cherchera à réduire les dimensions des données en minimisant la perte d'information. On considérera que :

- Les n lignes de X sont des vecteurs de R_p.
- Les p colonnes de X sont des vecteurs de R_n.

1-1 Ajustement par un sous espace vectoriel de R_p

On cherche à ajuster le nuage de n points de R_p par un espace vectoriel R_k (sous espace de R_p) muni de la distance euclidienne.
La première étape consiste à trouver une droite F1 qui passe par l'origine et qui ajuste au mieux le nuage de points au sens des moindres carrés. Posons u_1 le vecteur unitaire ($||u_1||^2 = 1$) porté par cette droite. Les coordonnées d'un vecteur x_i appartenant à l'espace R_p par rapport à u_1 est :

$$\mathbf{P_1 = < x_i, u_1 > = \sum_{j=1}^{p} x_i^j \, . u_1^j \quad avec \quad u_1 = {}^T[\, u_1^1 \; u_1^2 \; \ldots . u_1^p]}$$

Le vecteur des coordonnées des n points par rapport à cet axe est $\mathbf{X\, u_1} = \begin{bmatrix} p_1 \\ p_2 \\ \cdot \\ p_n \end{bmatrix}$

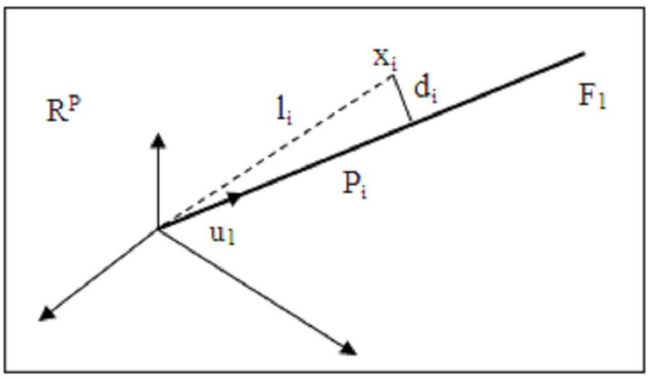

Figure III.1 droite d'ajustement du nuage de points

Ajuster au sens des moindres carrés revient à minimiser $\sum_{i=1}^{n} d_i^2$ (voir Figure III.1 **[leb 81]**)
Or $\forall$ i = 1, n : $\mathbf{l_i}^2 = \mathbf{d_i}^2 + \mathbf{p_i}^2$, d'où minimiser $\sum_{i=1}^{n} d_i^2$ revient à maximiser $\sum_{i=1}^{n} P_i^2$

Comme $\sum_{i=1}^{n} P_i^2 = {}^T u_1 \, {}^T XX \, u_1$ on a donc le résultat suivant :

On cherche $u \in R_p$ tel que $\begin{cases} {}^T u \, u = 1 \\ \text{et} \\ {}^T u \, {}^T XX \, u = \text{maximum} \end{cases}$

Le vecteur qui vérifie ces deux conditions est le vecteur propre de norme 1 associé à la plus grande valeur propre de la matrice ${}^T XX$.
D'une manière générale, une base orthonormée du sous espace vectoriel à k dimensions s'ajustant au mieux, au sens des moindres carrés, au nuage, est constituée par les k vecteurs propres correspondants aux k plus grandes valeurs propres de la matrice ${}^T XX$.

1-2 Ajustement par un sous espace de R_n

Dans l'espace R_n, le tableau X définit un nuage de p points.
On pose Y= ${}^T X$ et l'on refait la même étude que pour R_p .La matrice à diagonaliser est $X^T X$.

1-3 Relation entre les sous espaces de R_p et R_n

Soit r le rang de X qui est également le rang de ${}^T XX$ et de $X^T X$, r $\leq$min (n, p), ce qui signifie que nous avons r valeurs propres non nulles.
Soit λ une valeur propre de ${}^T XX$ dont le vecteur associé est u alors :

- ${}^T XX \, u = \lambda \, u \Rightarrow X ({}^T XX \, u) = \lambda \, X \, u \Rightarrow (X^T X) \, X \, u = \lambda \, X \, u \Rightarrow \lambda$ est une valeur propre de la matrice $X^T X$, le vecteur propre associé est Xu.

- Toute valeur propre non nulle de la matrice ${}^T XX$ est valeur propre de $X^T X$ et les vecteurs propres sont liés par les relations v = mXu où m est un constante, v vecteur propre de R_n, u vecteur propre de R_p.

De même si γ est une valeur propre de $X^T X$ de vecteur propre v alors :

- $X^T X \, v = \gamma \, v \Rightarrow {}^T XX ({}^T X \, v) = \gamma \, {}^T Xv \Rightarrow \gamma$ est une valeur propre de ${}^T XX$ et ${}^T Xv$ est le vecteur propre associé.

- Toute valeur propre non nulle de la matrice X^TX est valeur propre de ^TXX et les vecteurs propres sont liés par les relations u = m' ^TXv où m' est une constante, v vecteur propre de R_n.

Or $^T uu = 1$ et $^T vv = 1$ => m= m' = $\frac{1}{\sqrt{\lambda}}$

(v = mXu => $^T(v)$ v = $^T(mXu)$ mXu => 1= $m^2\, ^Tu(^TXXu)$ => 1 = $m^2\, ^Tu\ \lambda\ u$ =>1 = $m^2 \lambda$)

Conclusion : X^TX et ^TXX ont les mêmes valeurs propres et les vecteurs propres sont liés par la relation suivante (où u_i (resp. v_i) i ème vecteur propre de ^TXX (resp. X^TX)), et λ_i i ème valeur propre associée.

$$\mathbf{u_i} = \frac{^TX\, v_i}{\sqrt{\lambda_i}} \quad \textbf{et} \quad \mathbf{v_i} = \frac{X\, u_i}{\sqrt{\lambda_i}} \ \textbf{...(1)}$$

1-4 Nombre d'axes à retenir : taux d'inertie

La qualité globale de l'ajustement est mesurée par la quantité $\frac{\sum_{i=1}^{k} \lambda_i}{\sum_{i=1}^{p} \lambda_i}$

Elle nous informe sur le nombre d'axes à retenir, plus elle tend vers 1, plus on augmente le nombre d'axes à retenir, plus on capte d'information.

1-5 Reconstitution de X

La reconstruction de X à partir de tous les vecteurs propres est $\mathbf{X} = \sum_{i=1}^{p} \sqrt{\lambda_i}\, v_i\ ^Tu_i$

Une reconstitution approchée du tableau de X obtenue en se limitant aux k premiers axes

$$\mathbf{X} \quad \mathbf{X^*} = \sum_{i=1}^{k} \sqrt{\lambda_i}\, v_i\ ^Tu_i \ \textbf{... (2)}$$

2- Analyse en composantes principales ACP

C'est un cas particulier de l'analyse générale, elle permet de décrire un tableau de valeurs numériques continues de type ' Individus-Variables', le nuage des individus est projeté sur un sous espace vectoriel dont l'origine est le centre de gravité des points.

L'ACP est aussi connue sous le nom de transformée de Karhunen-loève ou de transformée de Hotelling (en l'honneur d'Harold Hotelling) **[csim]**.

Soit $X_{n,p}$ le tableau des données à analyser X= $(x_{i,j})$ i=1,n ; j=1,p.

La matrice à diagonaliser est soit :

a) La matrice des variances covariance Cov = ^{T}ZZ, où Z est la matrice dont les variables sont centrées ; Z a pour terme général $z_i^j = \frac{x_{ij} - \overline{x_j}}{\sqrt{n}}$ pour i=1..n, j=1..p , $\overline{x_j}$: la moyenne de la variables j.

b) La matrice des corrélations (si de plus les variables sont réduites) C = ^{T}RR, avec

$R = \frac{x_{ij} - \overline{x_j}}{\sqrt{n}\ \sigma_j}$, σ_j écart type de la variable j. Dans ce cas, on parle d'ACP normée.

2-1 But de l'ACP [bri 98]

L'objectif de l'ACP est de faire une étude sur les individus et, par dualité, sur les variables :

Etude des individus : cherche les individus proches et détermine les groupes. Deux individus sont proches lorsqu'ils possèdent des valeurs proches pour l'ensemble des variables.

Etudes des variables : chercher les liaisons entre elles et trouver les corrélations existantes entre ces variables.

2-2 La qualité de représentation d'un individu [leb 81] [ala 99]

La qualité de représentation de l'individu x sur le j ème axe est mesurée par le cosinus de l'angle formé entre le point et sa projection sur l'axe (voir Figure III.2 **[bri 98]**).

$$\varsigma^2 = \cos\theta^2 = \frac{(< x, u_j >)^2}{\|x\|^2} = \frac{p_j^2}{\|x\|^2}$$

Si la qualité de représentation d'un point sur un axe ou un plan est proche de 1, ce point est très proche de l'axe. « La distance entre deux points sur un plan ne traduit pas bien leur distance dans le nuage que si ces deux points sont bien représentés » **[bri 98]**.

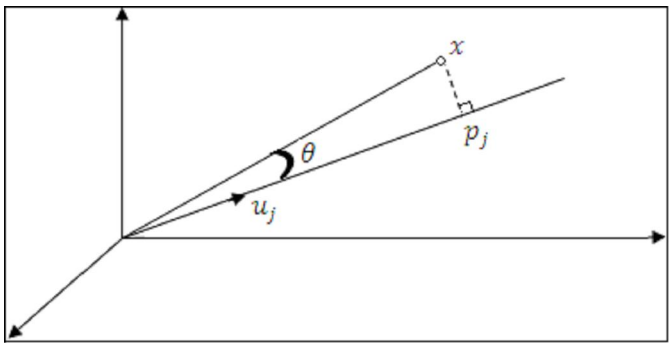

Figure III.2 Qualité de représentation d'un élément par un axe

On peut généraliser à plusieurs axes **[ala 99]**: $\varsigma^2 = \sum_{k=1}^{q} \frac{p_k^2}{\|x\|^2}$

3 - Approche Eigenfaces

« L'extraction des caractéristiques moyennant l'ACP appliquée aux visages est basée sur les covariances des teintes des pixels des images les unes par rapport aux autres. De telle sorte qu'en niveau de gris, des reliefs (zone de teintes) communs / dominants / émergeant de tous les visages décrivent une forme caractéristique, une définition d'un visage humain » ***[mde 04]***.

En 1987 Kirby et Sirovich **[lsi 87]** ont utilisé pour la première fois l'ACP pour la représentation des images faciales dans un espace de dimension réduite sans grande perte d'information.

En 1991, Turk et Pentland **[mat 91]** ont introduit le concept d'Eigenfaces en appliquant l'ACP pour la reconnaissance et la détection des visages. Cette approche consiste à exprimer M images de départ par rapport à la base formée par les vecteurs propres appelés Eigenfaces. Le but est d'extraire l'information caractéristique d'une image du visage, pour l'encoder (représenter dans un sous espace de dimension réduite) aussi efficacement que possible afin de la comparer à une base de données de modèles encodés de manière similaire.
En termes mathématiques, cela revient à trouver les vecteurs propres de la matrice de covariance formée par les différentes images de la base d'apprentissage **[lsi 87]**.

Une étape de pré-traitement est d'abord réalisée afin de rendre homogène les images à comparer. Ce prétraitement est effectué à la fois sur les images de la base de données et sur l'image de question. Il permet de convertir toutes les images dans un format identique, c'est-à-dire qu'à l'issue de ce traitement, l'image est en niveau de gris. Le prétraitement permet de passer de l'image originale à une image normalisée comme présenté en figure III.3 **[pat]**.

Figure III.3 Etape de Prétraitement **[pat]**

Une image I_i de dimension (m, n) est traitée comme un vecteur Xi (m×n, 1) dans un espace vectoriel de grande dimension (N = m×n), par concaténation des colonnes.

$$=> I_1 = \begin{pmatrix} x_{1,1} & x_{1,2} & \cdots & x_{1,m} \\ x_{2,1} & x_{2,2} & \cdots & x_{2,m} \\ \vdots & \vdots & \ddots & \vdots \\ x_{n,1} & x_{N,2} & \cdots & x_{n,m} \end{pmatrix} => X_1 = \begin{pmatrix} x_{1,1} \\ x_{2,1} \\ x_{3,1} \\ \vdots \\ \vdots \\ x_{N,1} \end{pmatrix}$$

Passage d'une image vers un vecteur dans un espace vectoriel de grande dimension. **[nic]** Où les coefficients $x_{i,j}$ représentent les valeurs des pixels en niveau de gris, codés de 0 à 255.

Apres avoir rassemblé les M images dans une unique matrice, nous obtenons une matrice d'images X, où chaque colonne représente une image Xi :

$$X = \begin{matrix} X_1 & X_2 & & X_M \end{matrix} \begin{pmatrix} x_{1,1} & x_{1,2} & \cdots & x_{1,M} \\ x_{2,1} & x_{2,2} & \cdots & x_{2,M} \\ \vdots & \cdots & \ddots & \vdots \\ x_{N,1} & x_{N,2} & \cdots & x_{N,M} \end{pmatrix}$$

Dans cette matrice, les individus sont en colonnes et les variables sont en lignes.

En appliquant l'ACP au tableau X ; remarquer que les individus sont en colonnes et les variables sont en lignes.

Cette matrice a la dimension suivante : **P*(m*n)** où P = le nombre d'images dans la base d'entraînement, et (m*n) le nombre de pixels dans une image **[pat]**.

Le visage moyen est donné par : $\boldsymbol{\mu} = \frac{1}{M} \sum_{1=1}^{M} X_i$

Les vissages centrés sont obtenus comme suit : $\mathbf{Z_i = X_i - \mu}$ i=1..M

La matrice à diagonaliser est $Z^T Z$ de dimension (N, N).

Dans le cas où N>M (la résolution est supérieure au nombre d'images) **[nic 09]**, il est préférable de diagonaliser la matrice $^T ZZ$ de dimension (M, M) plus réduite et d'utiliser les relations de transition (voir formule (1)) pour changer d'espace.

Par exemple, pour 100 images de résolution 320 x 240, nous pourrions diagonaliser la matrice $^T ZZ$ de dimension 100x100 au lieu de la matrice $Z^T Z$ de dimension 76800*76800. Le gain de temps de calcul serait considérable, nous passerions ainsi d'une complexité de l'ordre du nombre de pixels dans une image à une complexité de l'ordre du nombre d'images.

Une part de la grande efficacité de l'algorithme ACP vient de l'étape suivante qui consiste à ne sélectionner que les k meilleurs vecteurs propres (associés aux k plus grandes valeurs propres). A partir de là, on définit un espace vectoriel engendré par ces k vecteurs propres, que l'on appelle l'espace des visages $\mathbf{E_v}$ ("FaceSpace") ou l'espace propre ("EigenSpace").

Les images originelles peuvent être reconstituées par combinaison linéaire de ces vecteurs propres (voir formule (2)). Les représentations graphiques de ces vecteurs rappellent un peu des images fantômes, chacune mettant en avant une partie de l'information du visage. On les appelle Eigenfaces (voir figure III.4).

Figure III.4 Image moyenne et les 15 premiers visages propres **[nic]**

Nous allons maintenant projeter nos images de départ sur $\mathbf{E_v}$ afin d'extraire le vecteur de caractéristiques de chaque image. Une image Xi est alors transformée en ses composantes Eigenfaces par une simple opération de projection vectorielle moyennant la matrice des k vecteurs propres $U = [u_1\ u_2\ \ldots\ u_k]$

$$Y_i = {}^{T}U \,.\, Zi$$

Les vecteurs $\mathbf{Y_k}$ sont appelés poids et forment une matrice $\Omega^T = [Y_1, Y_2, \ldots, Y_M]$ qui décrit la contribution de chaque Eigenfaces dans la représentation de l'image d'entrée. Une image est représentée par une somme de poids des Eigenfaces stockés dans un vecteur.
$\mathbf{\Omega^T}$ est alors utilisée pour trouver quelle est, parmi un nombre prédéfini de classes, celle qui décrit le mieux une image d'entrée.

A présent que les vecteurs des images de la base et de l'image de test ont été calculés, il faut comparer l'image à la base de données en mesurant la distance entre les vecteurs de caractéristiques de chaque individu. L'image la plus proche de l'image teste est celle qui a la distance la plus faible. Afin de comparer ces vecteurs, il faut choisir une mesure de distance adéquate .Voici les cinq distances les plus utilisées **[pat]** :

- distance Euclidienne
- distance Cityblock
- distance de Mahalanobis
- distance Cosine
- fusion de ces quatre dernières mesures

Si A et B sont deux images, la distance entre les deux vecteurs est mesurée ainsi :

$$l_{\,euclidean}\,(A,B) = \sum_{i=1}^{N} \sqrt{(A_i - B_i)^2}$$

$$l_{\,cityblock}\,(A,B) = \sum_{i=1}^{N} \left| A_i - Bi \right|$$

$$l_{\,\cos ine}\,(A,B) = 1 - \frac{A_i.B_i}{\left\|A_i\right\|.\left\|B_i\right\|}$$

$$l_{\,mahalanobi\ s}\,(A,B) = -\sum_{i=1}^{N} A_i\, B_i \left(\frac{1}{\sqrt{\lambda}_{\ i}} \right)$$

$$l_{fusion}(A,B) = \frac{\sum \left\| l(A,B) \right\|}{4}$$

La distance Cityblock peut aussi être appelée distance de Manhattan, ou distance de Minkowski d'ordre 1. La distance euclidienne se nomme aussi distance de Minkowski d'ordre 2 **[pat]**.

L'ACP appliquée aux visages (eigenfaces) fait l'objet de bon nombre de travaux de recherche, citons à titre d'exemple :

Sehad et al **[seh 00]** ont utilisé l'ACP pour la reconnaissance faciale sous différentes vues (frontale, diagonale 45° et de profile 90°). Lors de l'apprentissage, trois espaces propres sont crées. Pour chaque classe (individu) de chaque espace, le centre de gravité et le seuil sont calculés. Le seuil consiste en la distance maximale séparant les vecteurs caractéristiques (vecteurs projetés) des images de l'apprentissage du centre de gravité de leur classe. L'image teste est projetée puis reconstituée dans chaque espace. L'orientation de l'image correspond à l'espace engendrant la plus petite erreur de reconstruction. Puis la distance entre le vecteur caractéristique test et le vecteur caractéristique moyen de chaque classe est comparé au seuil de la classe pour émettre une décision.

J. Yang et al **[jia 04]** ont utilisé une ACP à 2 dimensions. La matrice de covariance est calculée à partir de l'image moyenne. Les vecteurs de projection font passer une image d'une forme matricielle à une forme matricielle de dimension réduite. Les tests effectués sur les bases ORL, YALE et AR montrent l'efficacité de la 2D-ACP par rapport à l'ACP en termes de temps et de taux de reconnaissance. Afin de réduire la dimensionnalité, une application de l'ACP en aval à la 2D-ACP a été proposée.

Zhu, Vai et Mak **[zhu 03]** ont appliqué la 2D-DCT aux images faciales en amont de l'ACP obtenant ainsi un meilleur taux de reconnaissance mais aussi un gain en temps considérable.

4- ACP Limitée à une seule classe d'images (approche SelfEigenfaces)

Il existe une variante de la méthode Eigenfaces appelée par les auteurs de **[lui 00] [alb 05]** approche ***Self Eigenfaces.*** Celle-ci repose sur le même principe que celui des Eigenfaces, néanmoins le traitement est effectué seulement sur une seule classe d'images (les images d'un

même individu). On aura ainsi pour chaque personne une image moyenne, une matrice de projection (matrice des vecteurs propres) ainsi qu'une matrice des vecteurs projetés (caractéristiques). Elle est plus rapide et consomme moins d'espace que la méthode Eigenfaces. Elle est exclusivement utilisée pour la vérification et ne permet pas l'identification.

Dans **[lui 00] [alb 05]**, cette approche a été adoptée pour reconnaître une personne spécifique dans une séquence vidéo. La reconstitution du visage a été utilisée pour la phase de décision en se basant sur le principe suivant :

Soit E l'espace propre construit à partir d'un individu i :

- Si l'image teste est celle de l'individu i alors l'erreur de reconstruction est petite.
- Si l'image teste est celle d'un imposteur alors l'erreur de reconstruction est grande (voir Figure III.5).

La méthode de la reconstitution est efficace (avec un taux de reconnaissance atteignant 92.8% **[lui 00]**) mais a pour inconvénient un coût relativement élevé en termes de temps et d'espace **[and 05].**

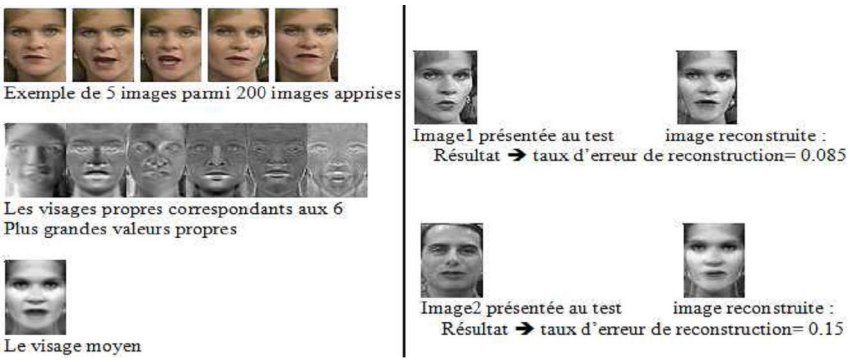

Figure III.5 Exemple de reconstruction d'un visage de client légitime et d'un intrus en utilisant les 26 plus grandes valeurs propres **[alb 05]**

5 - Avantages et Inconvénients de la méthode des Eigenfaces

L'ACP appliquée aux visages permet la réduction de la dimension de représentation du visage. C'est une approche rapide et très facile à mettre en oeuvre, néanmoins, elle présente quelques inconvénients tels qu'une baisse des performances **(**temps d'exécution plus long) dans le cas où la base d'images est volumineuse. De plus, pour l'approche Eigenfaces, l'ajout ou la suppression d'un individu de la base engendre le recalcule des visages propres.

Aussi, cette méthode n'est pas robuste aux variations

- d'échelle, mais un changement d'échelle préalable est toujours possible.
- de l'orientation du visage (visage plus ou moins de profile, visage incliné).
- d'expression du visage qui correspondent aux sept émotions suivantes : la **neutralité**, la **joie**, la **tristesse**, la **surprise**, la **peur**, la **colère** et le **dégoût [cvc].**
- de la lumière: Etant donné que le visage peut être exposé à la lumière lors de sa prise en photo, des zones d'ombre et de lumière peuvent apparaître sur le visage faussant ainsi l'authentification. En effet, deux images d'un même individu prises dans des conditions d'éclairage différentes, pourraient se retrouver éloignées dans l'espace propre.

Les systèmes utilisant l'ACP appliquée aux visages sont souvent confrontés à un problème majeur qui est la difficulté de l'estimation du seuil de décision **[kyu].**

Dans ce chapitre, nous avons décrit l'approche ACP sur les visages : Eigenfaces en général et Self Eigenfaces en particulier. Ceci achève l'aspect biométrie pour entamer, dans le chapitre suivant, une étude détaillée sur le support de stockage des données biométriques qui est la carte à puce.

Chapitre IV

La carte à puce

L’utilisation de la carte à puce est de plus en plus répandue dans le monde entier avec un rythme de croissance très important. Depuis son apparition dans les années soixante, la carte à puce a beaucoup évoluée et son utilisation s’est élargie à plusieurs domaines.
Aujourd’hui, elle est omniprésente dans le quotidien de l’homme. En outre, elle apparaît dans de multiples secteurs tels que la téléphonie, les banques, la santé, etc.

1- Historique de la carte à puce [did 07]

- En1968, deux Allemands Jurgen Dethloff et Helmut Grotrupp ont introduit un circuit intégré dans une carte plastique.
- En1974, le français Roland Moreno, dirigeant de la société «Innovatron» a conçu une carte à mémoire pour la conception d'un porte monnaie électronique.

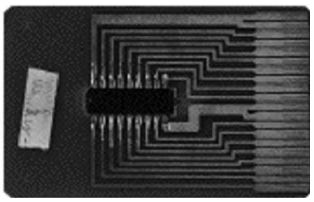

Figure IV.1 Premières cartes en verre époxy à circuit intégré **[did 07]**

- En 1977, au sein de sa direction technique, Michel Ugon a conçu la première carte à microprocesseur (Bull CP8 : munie d'une mémoire et d'un microprocesseur Motorola).
- En 1983, les cartes santé ont fait leur apparition, elles permettent aux médecins d’obtenir des renseignements plus précis concernant leurs malades en un minimum de temps.
- En 1984, un regroupement de banques françaises commercialise les premières cartes à mémoire bancaires conçues par Bull, Schlumberger et Philips. Et en 1985, Bull livre ses premières cartes bancaires "CB" dotées de microprocesseurs.
- La même année, est apparue la télécarte créée par Schlumberger pour France Télécom (cartes équipées de micromodules). Une carte d'abonnement qui a pour objectif de prélever chaque communication sur la facture téléphonique de l'abonné.

Dès lors, les cartes connaissent une croissance fulgurante : 2.000.000 de cartes vendues en 1986, et plus de 6.000.000 exemplaires vendues par mois en 1991 **[igm02]**. La carte à puce connaît alors un franc succès qui sort d'Europe pour s’étendre au niveau mondial. La plus grande innovation est l’apparition des JavaCards en1997.

2- Types de cartes et leurs architectures

Voici ci dessous les types de cartes et leurs architectures respectives : **[wol 03]**

2-1 Carte embossée (embossed card)

C'est la plus ancienne technologie connue pour les cartes d'identification. La carte embossée comporte des caractères gravés qui peuvent être facilement imprimés sur papier par un matériel peu coûteux. La nature et l'emplacement des caractères gravés sont spécifiés par le standard ISO 7811. Par exemple, une région est réservée pour l'ID de la carte, l'autre pour le nom et l'adresse du détenteur (4x27 caractères). La simplicité de cette technique a contribué à la prolifération des cartes de crédit car cette technologie ne demande ni énergie électrique ni réseau téléphonique.

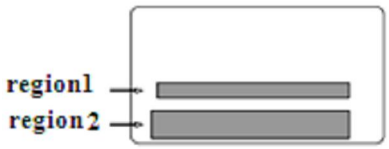

Figure IV.2 Carte embossée **[wol 03]**

2-2 Carte à pistes magnétiques (magnetic stripe cards)

L'inconvénient des cartes embossées est qu'elles nécessitent l'utilisation de papier ce qui est assez contraignant. Pour y remédier, les données ont été codées sur une bande magnétique au dos de la carte **[wol 03]**. Le principe de l'enregistrement magnétique repose sur la magnétisation de très petites zones de la bande. L'enregistrement /écriture s'effectue par une tête magnétique. **[Ahm 09]**. Ainsi, la lecture des données s'effectue d'une manière électronique sans utilisation de papier. Les parties 2, 4, 5 du standard ISO 7811 spécifient les propriétés de la bande magnétique, la technique de codage et l'emplacement des pistes.

Par exemple, les deux premières pistes sont en lecture seule, alors que la troisième est en lecture écriture **[wol 03]**.

Un contrôle de parité est utilisé pour la gestion d'erreurs [**Ahm 09]**.

Certes, cette carte a une plus grande capacité (1000 bits) mais les données peuvent être facilement altérées.

Dans le cas des cartes embossées, la manipulation des caractères ne peut se faire sans que l'on s'en rende compte à l'oeil nu. Alors que le contenu de la carte magnétique peut être facilement modifié avec un simple lecteur de carte. Pour cela, des techniques de protection ont été conçues mais elles restent trop coûteuses, comme par exemple, le rajout d'un code

invisible et inaltérable mais cela nécessite un senseur (capteur) ce qui augmente considérablement le coût de la carte**[wol 03]**.

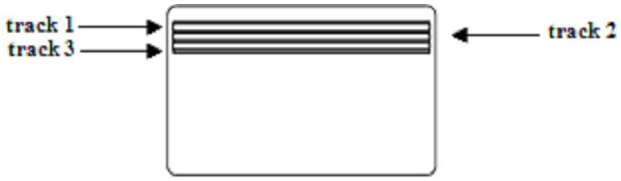

Figure IV.3 Carte à pistes magnétiques **[wol 03]**

2-3 Carte à puce (smart cards)

Plus récente, elle intègre un circuit embarqué muni d'un mécanisme de stockage et de transmission des données. Sa mémoire peut atteindre plus de 256K octets.

Fournit des moyens d'effectuer des transactions d'une manière flexible, bloquée, standard avec une intervention humaine minimale (peut fournir l'authentification forte par SSO, USB) **[Ahm 09]**.

Son avantage majeur est l'aspect sécurité : en effet, la donnée ne peut être accédée que par une interface sérielle contrôlée par un système d'exploitation et une logique de sécurité. Un programme de codage (décodage) et/ou un code (mot de passe) dans la puce, inaccessibles de l'extérieur, sont garants d'une bonne sécurité (au sens bancaire) **[Ahm 09]**.

Les cartes à puce peuvent être classées selon leurs composants en carte à mémoire et carte à microprocesseur, ou selon le mode d'accès à la carte avec contact ou sans contact :

2-3-1 Carte à mémoire (memory card)

La donnée est sauvegardée sur une EEPROM, son accès est contrôlé par une logique de sécurité (voir Figure IV.4 **[pie 05])** qui, dans le cas le plus simple, rajoute ou efface la protection pour une partie ou la totalité de la mémoire. La donnée est transférée via le port d'entrée sortie moyennant un protocole de transfert synchrone. La fonctionnalité de la carte est optimisée pour une application bien définie ; quoique cela restreint sa flexibilité. Peu coûteuse, cette carte est généralement utilisée comme carte téléphonique prépayée ou carte d'assurance médicale.

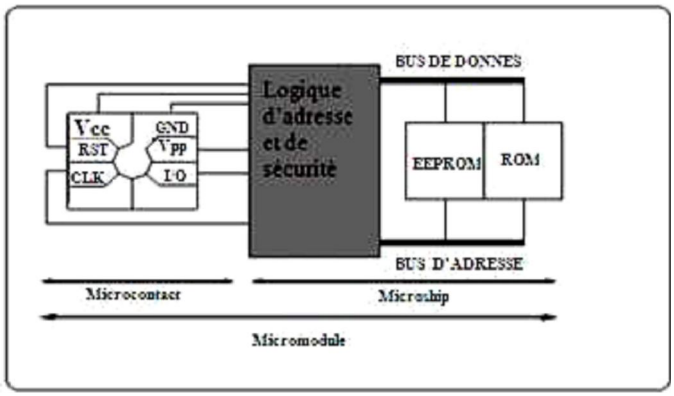

Figure IV.4 Carte à mémoire et à contact

2-3-2 Carte à microprocesseur (microprocessor card)

Elle contient, comme son nom l'indique, un processeur (4 à 8 Mhz) auquel se rajoute un masque au niveau de la ROM, une EEPROM (de 1 à plus de 128 Ko), une RAM (de 1 à 3 Ko) et un port d'entrée sortie. Le microprocesseur protège et peut gérer une ou plusieurs zones mémoire de type RAM ou ROM **[a3m]**. Le Masque ("Hard Mask") est le système d'exploitation de la carte, Il est généralement écrit en C ou en langage d'assemblage. Il est stocké en ROM lors de la fabrication et reste figé.

La validation du code secret porteur (PIN) résulte d'un calcul effectué par le microprocesseur.

Les données et codes programmes sont lus et écrits sur la EEPROM. La RAM, volatile, est exclusivement utilisée par le processeur. L'interface série d'entrée sortie est un registre de transfert bit à bit vers l'extérieur. Vu la capacité de la carte à exécuter des algorithmes de cryptage, il est possible d'implémenter plusieurs modules de sécurité pour répondre à des applications particulières.

Le protocole utilisé par les cartes à processeur est toujours asynchrone. On parle d'ailleurs souvent de cartes asynchrones en parlant de cartes avec processeur. Lorsqu'une carte est initialisée, par exemple lors de son insertion dans un lecteur, elle transmet immédiatement un message identifiant le type de processeur utilisé. Ce message est appelé le "Message To Reset string" **[ucl]**.

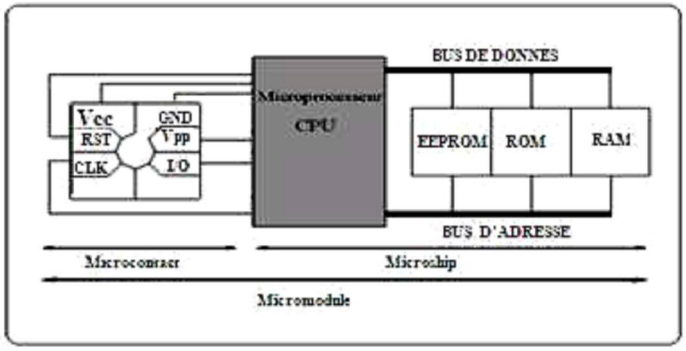

Figure IV.5 Architecture d'une carte à microprocesseur et à contact **[pie 05]**

2-3-3 Carte avec contact

Le micromodule (microcontact) est un circuit très mince où viennent se loger d'une part les contacts du connecteur sur une face et d'autre part les contacts avec la puce. Le design du micromodule varie selon les constructeurs. De plus, l'affectation des contacts (C1 à C8) varie selon le type de la puce : **[jer 00]**

La norme ISO 7816-2 définit les aspects électriques et la situation des contacts sur la carte **[tro 07]**

- Le contact 1 correspond à la tension d'alimentation en lecture (Vcc).
- Le contact 2 correspond au signal Reset (RST) : une tension appliquée sur ce contact déclenche l'initialisation physique et logique de la carte.
- Le contact 3 correspond au signal d'horloge (CLK), celui-ci est fourni par le lecteur, il est compris entre 1 et 5 Mhz. Le signal d'horloge de la carte est dérivé à partir de ce signal.
- Le contact 4 est réservé à une utilisation future (RFU : Reserved for Futur Use).
- Le contact 5 correspond à la masse (GND).
- Le contact 6 correspond à la tension d'alimentation (Vpp) à appliquer, sur demande de la carte, pour programmer la mémoire de données (tension en écriture). Il est seulement utilisé sur des cartes anciennes.
- Le contact 7 est le contact d'entrée/sortie (I/O) par lequel transitent en half-duplex toutes les données échangées entre la carte et le monde extérieur.
- Le contact 8 est réservé à une utilisation future (RFU).

Une norme utilisant les contacts RFU serait en cours de préparation pour l'utilisation de l'USB avec la carte.

2-3-4 Carte sans contact (Non-contact card)

Comme les contacts du micromodule des cartes à contact sont directement connectés aux entrées du circuit intégré, la puce risque d'être endommagée ou détruite par une décharge électrostatique. Afin d'y remédier, la carte sans contact a été conçue pour être accessible par radiofréquence à courte ou moyenne portée, via une antenne interne dont les spires sont moulées dans l'épaisseur de la carte. L'invocation de commande sur la carte est encodée sous la forme d'ondes radio. Le voltage nécessaire pour exécuter la commande est fourni par le support radio **[Kao 09]**. Ceci offre, par conséquent, de nouvelles applications potentielles: en effet, il est inutile d'insérer la carte dans le lecteur vu que les systèmes sans contact ont une portée de plus d'un mètre, ce qui est très utile dans un système d'accès : Par exemple, une porte qui s'ouvre avant même que l'individu autorisé ne l'atteigne. Cette carte est surtout utilisée dans le transport publique la où il faut identifier beaucoup d'individus en un temps réduit.

Son avantage majeur est la vitesse de transfert (moins de 150 ms) **[ADAE]**. Son inconvénient est le prix des terminaux qui est relativement élevé car depuis que plusieurs systèmes ont été standardisés et commercialisés, ces terminaux doivent être compatibles avec tout type de carte.

La plupart des cartes sont utilisées pour une unique fonction bien spécifique, aujourd'hui divers services ont été rajoutés. Par exemple : inclure le service payement aux cartes sans contact qui servent de ticket électronique en utilisant l'infrastructure existante des cartes à contact. Ceci a donné naissance aux cartes multifonctions nommées cartes avec et sans contact (ASC) ou cartes mixtes (dual interface cards).

Figure IV.6 Carte avec contact et carte sans contact **[pie 05]**

2-4 Carte à mémoire optique (optical memory card)

Tout comme les CD's (Compact disc) et les DVD's, cette carte est basée sur la technologie optique, qui lui permet une grande capacité de stockage, l'inconvénient est que la donnée n'est écrite qu'une seule fois. C'est les standards ISO/IEC 11693 et 11694 qui définissent les caractéristiques physiques de la carte. La combinaison du stockage à large capacité de la carte à mémoire optique et l'intelligence des cartes à puce a donné naissance à de nouvelles possibilités : les données peuvent être écrites cryptées dans la mémoire optique, la clé quant à elle serait stockée dans la mémoire privée de la puce pour assurer une meilleure sécurité. Actuellement l'utilisation de la carte à mémoire optique est assez limitée vu le coût élevé des équipements de lecture écriture. Une application dans le domaine médical est intéressante car la carte permettrait de sauvegarder des données de grande capacité comme les images à rayon X du patient.

3- standardisation dans le domaine des cartes à puce

Afin de pallier au problème d'incompatibilité entre les applications, les cartes et les lecteurs, des normes ont été établies notamment la norme ISO 7816 (resp. ISO 14443) destinée aux cartes à puce avec contacts (resp. sans contacts). Elle définit les paramètres physiques, électriques et logiciels de la carte. Aussi de nombreuses spécifications dédiées à des applications industrielles particulières des cartes à puce ont été conçues, entre autre, la spécification EMV pour l'industrie des finances (cartes de paiement), GSM pour l'industrie des télécommunications (téléphones mobiles).

Concernant l'interopérabilité des applications, telles que les API indépendantes des périphériques et les outils de développement, il existe le standard PC/SC qui permet de définir une interface "standard" pour l'utilisation de lecteurs de cartes à puce sous Windows. PC/SC permet donc à l'utilisateur de développer une seule application qui s'exécuterait sur n'importe quel lecteur conforme au standard PC/SC.

L'annexe 3 aborde en détail la standardisation dans le monde des cartes à puce.

4 - Cycle de vie d'une carte à puce

Le cycle de vie d'une carte à puce peut se résumer en trois phases :

4-1 Phase amont

Se charge du développement du système d'exploitation et la conception de la puce. Elle s'effectue en deux étapes :

- ***Le développement du masque*** (Le développement de l'applicatif) : Consiste à développer le système d'exploitation (masque) de la carte à puce et à spécifier des informations nécessaires à la pré-personnalisation.
- ***La création du schéma de conception*** de la puce à l'aide de logiciels spécifiques.

4-2 Phase de création

S'effectue en plusieurs étapes :

- ***Fabrication de la puce* :** La fabrication de la puce consiste à fabriquer le micromodule et le micro-circuit (puce) à partir des galettes de silicium (les micro-circuits se présentent en nombre sous forme de wafer). Un programme est inscrit en mémoire ROM définissant les fonctionnalités de base de la carte : "masque" figé sachant traiter un nombre limité de commandes pré-définies (gestion des entrées sorties, réponse au reset, etc.), c'est le système d'exploitation.
- ***Encartage*** : Consiste à assembler la puce, le micromodule et le support plastique.
- ***Tests*** : Plusieurs test sont effectués afin d'identifier les cartes défectueuses.
- ***Pré-personnalisation*** : Où un numéro de série sera inscrit dans la ROM de chaque carte.
- ***Initialisation*** : consiste à inscrire en mémoire des données spécifiques propres à l'application. Cette mémoire va être organisée et répartie suivant les différents besoins, de ce faite, des zones de travail seront définies et repérées par des indicateurs représentatifs de leur mode de fonctionnement : lecture seule, lecture/écriture, etc.

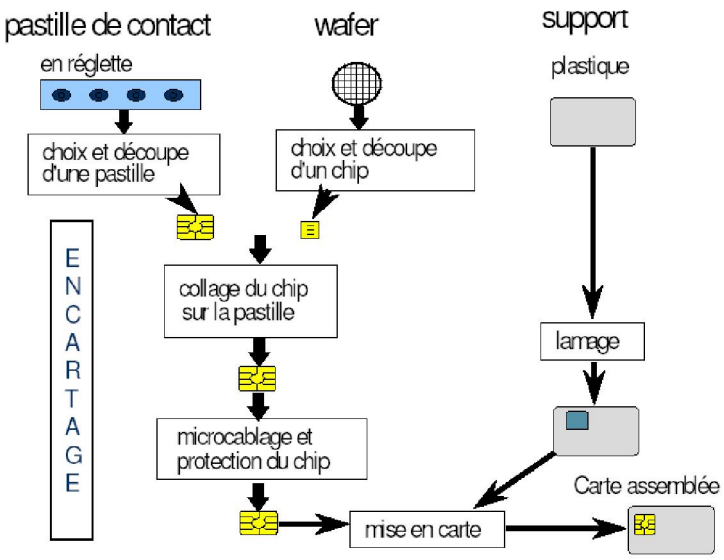

Figure IV.7 Cycle de vie d'une carte à puce : schéma de la phase de création **[ADAE]**

4-3 Phase de circulation

S'effectue selon plusieurs étapes :

4-3-1 La personnalisation de la carte

Cette étape, réalisée par l'émetteur, est dédiée à l'adaptation au porteur final de la carte. La personnalisation peut être électrique ou graphique :

• ***Personnalisation électrique*** *:* écriture par exemple du nom du porteur, son numéro d'abonné ou de toute autre information pertinente le concernant dans la ROM.

• ***Personnalisation graphique*** : impression et/ou embossage sur une face de la carte de tout logo, signe, photographie ou hologramme permettant une identification visuelle rapide de la carte. Actuellement des technologies d'impression très avancées (destinées pour les billets de banques) sont utilisées pour éviter toute copie frauduleuse de la carte.

4-3-2 La distribution

L'opérateur gère la distribution des cartes

- Remise de la carte (en face à face, par envoi postal, etc.)
- Remise du code PIN
- Communication éventuelle sur le fonctionnement (le public n'est pas encore habitué au sans contact par exemple)

4-3-3 L’utilisation et la gestion du parc

Durant l’utilisation de la carte, le masque de celle-ci va traiter différentes commandes, des modifications vont être apportées à la mémoire de la carte. L’opérateur doit gérer le parc (ensemble) de cartes, les pertes, les remplacements.

4-3-4 La fin de vie de la carte

Ceci peut être dû à un disfonctionnement du système d’exploitation, ou bien causé par l’utilisateur qui par un usage erroné, invalide sa carte, en se trompant plusieurs fois consécutivement de code PIN par exemple.

5- Le système d’exploitation (Operating System) dans les cartes à puce

Les cartes à puce disposent d’un système d’exploitation (masque) stocké dans la ROM, vu la contrainte d’espace de la carte, le système se caractérise par une taille réduite qui s’étend sur une plage de 3 à 250KB.

Au début de leurs apparitions, les cartes à puce étaient dotées de systèmes d’exploitation. Conçus pour un usage unique, d’où l’appellation de systèmes dédiés, on les retrouve dans les cartes bancaires, les cartes santé (Vitale), les cartes pour la téléphonie mobile (SIM), etc.

Depuis quelques années, les « plates-formes ouvertes » ont fait leurs apparitions telles que JavaCard (promu par Sun), Multos (utilisé pour l'application Mondex), Windows for Smart Card (WfSC) de Microsoft. Elles prennent en charge le système d’exploitation avec une couche de chargement d'applications, il devient donc possible de "charger" des applications après la réalisation du masque et l'encartage. Ces systèmes opératoires utilisent des machines virtuelles afin d’améliorer la portabilité du code.

Le système d’exploitation de la carte remplit les fonctionnalités suivantes : **[jea 04]**

- Gère les fichiers de la carte.
- Gère les communications avec le monde extérieur (lecteur).
- Exécute les commandes reçues via l’interface I/O.
- Supervise l’exécution des programmes exécutables stockés dans la carte.
- Permet un accès sécurisé à l’ensemble des fichiers.
- Assure les fonctions de cryptographie (DES, RSA …).

5-1 Les fichiers dans les cartes à puce

La plupart des systèmes d'exploitation des cartes à puce supportent un modeste système de fichier basé sur le standard ISO 7816. Les fichiers de la carte à puce sont constitués de blocs de mémoire contigus, leur structure est décrite ci-dessous.

5-1-1 Structure interne d'un fichier

Les fichiers sur les cartes à puce actuelles ont une structure orienté objet, toutes les informations concernant un fichier donné sont stockées dans le fichier lui-même, il est de ce fait constitué de deux parties :

- ***l'entête*** : contient les informations sur la structure du fichier ainsi que ses droits d'accès.
- ***Le corps*** : où les données modifiables par le client sont sauvegardées, cette seconde partie est reliée à l'entête par un pointeur.

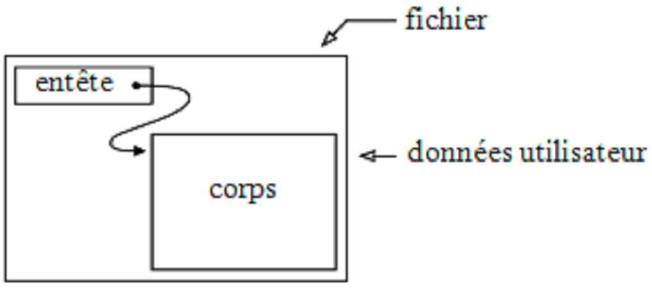

Figure IV.8 Structure interne d'un fichier dans les cartes à puce **[wol 03]**

5-1-2 Types de fichiers

On retrouve dans la carte à puce deux grandes catégories de fichiers :

Ø Fichier dédié (Dedicated File : DF): C'est un répertoire, il peut à son tour contenir plusieurs répertoires ainsi que des fichiers de données.

Ø Fichier élémentaire (Elementary File : EF) : C'est un fichier de données, il en existe deux catégories :

- Fichier élémentaire interne (Internal Elementary File : IEF) : il est utilisé pour le stockage des données qui sont utilisées par le système d'exploitation de la carte (par exemple: les fichiers clé, les fichiers Pin).
- Fichier élémentaire de travail (Working Elementary File : WEF) quant à lui contient les données qui seront lues ou écrites par le terminal, en d'autres

termes, ces données sont exclusivement utilisées par l'environnement extérieur à la carte, elles ne sont donc pas utilisées par le système d'exploitation.

Le fichier élémentaire de travail peut avoir une des structures internes suivantes :

- *Fichier à structure transparente* : c'est une séquence d'octets de données l'un à la suite de l'autre. Les trois autres types de fichiers sont structurés comme des séquences d'enregistrements individuellement identifiables.
- *Enregistrements séquentiels de longueur fixe.*
- *Enregistrements séquentiels de longueur variable.*
- *Enregistrements cycliques* : le dernier enregistrement pointe le premier.

L'organisation logique des données dans la carte a une structure arborescente hiérarchique contenant les fichiers MF, EF et DF. La racine de cette arborescence est le fichier MF (répertoire de base), c'est un type de répertoire avec un FID prédéfini (3F00h) **[wol 03],** ce fichier est implicitement créé par le système d'exploitation de la carte, il est unique dans la carte et ne peut être supprimé.

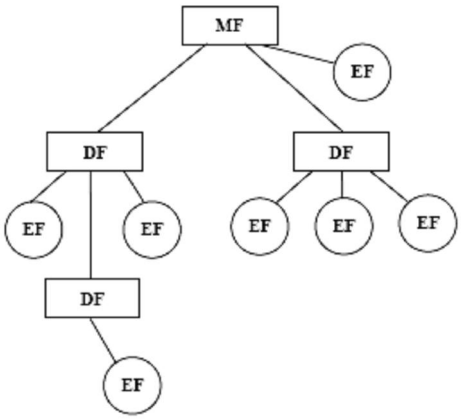

Figure IV.9 Système hiérarchique de fichiers **[wol 03]**

5-1-3 Sélection des fichiers

Un fichier peut être référencé de différentes manières selon son type :

a) Identificateur de fichier (FID : file Identifier)

Tous les fichiers DF et EF possèdent un FID sur 16 octets qui permet de les identifier. En règle générale, les FID's doivent être choisis de manière à ce qu'il n'y ait aucune ambiguïté lors de la sélection d'un fichier.

Les règles ci-dessous sont appliquées pour assurer l'unicité des FID's :

- Les fichiers DF et EF qui sont dans le même répertoire doivent avoir des FID's différents.
- Les fichiers DF's ne doivent pas avoir le même FID.

b) Nom du répertoire (DF name)

Comme, les deux caractères du FID ne suffisent pas en raison de l'augmentation du nombre de fichiers, chaque fichier DF est caractérisé par un nom (DF name) sur 16 octets en plus de son FID.

c) SFI : Short file identifier

Le système d'exploitation assigne automatiquement un identificateur SFI (qui varie entre 1 et 30) aux fichiers EF, sa taille est de 5 bits.

Il est possible d'accéder aux fichiers de différentes manières selon leur type:

- ***Sélection des répertoires***

  Le répertoire de base (MF) est automatiquement sélectionné par le système d'exploitation dès que le 'Reset' a été appliqué sur la carte.

La sélection d'un répertoire peut être effectuée en spécifiant son FID ou bien son nom. Les méthodes de sélection pour chaque répertoire sont déterminées à la création (utilisation exclusive du FID ou du nom du répertoire durant sa durée de vie).

- ***Sélection des fichiers de données***

  Un fichier EF peut être sélectionné en spécifiant son FID, toute fois, une sélection du répertoire dans lequel se trouve ce fichier doit être préalablement effectuée.

5-1-4 Conditions d'accès aux fichiers

Les conditions ou privilèges d'accès aux fichiers sont déterminés lors de leur création et ne peuvent être modifiés par la suite.

Il existe deux types de conditions d'accès:

- ***orientées état* :** elles consistent à comparer l'état de sécurité courant à celui correspondant au fichier (l'accès est permis dans le cas ou le premier est supérieur ou égal au deuxième).

Dans cette classe, il y a deux options : sécurité globale, sécurité locale. La première concerne le fichier MF, c'est à dire la carte dans sa globalité, la deuxième, quant à elle, concerne le répertoire courant.

- ***orientées commande* :** définissent les commande qui peuvent être exécutées avant même qu'on y a accède. Cette stratégie est largement utilisée dans le monde des cartes à puce telles que les cartes GSM. Elle utilise une table d'accès aux commandes qui contient des informations sur les commandes qui doivent être exécutées avec succès pour chaque type d'accès. Généralement, les commandes sont assignées à des clés spécifiques, par exemple, la lecture d'un fichier n'est permise que si l'identification s'est effectuée avec succès (PIN correcte).

La structure de cette technique est très simple, mais elle manque de flexibilité (en cas de rajout de nouveaux programmes, il faut étendre la table d'accès).

5-2 La transmission de données dans la carte à puce

Une fois la carte introduite dans le lecteur, une communication sera alors établie entre le lecteur et la carte comme suit :

- Le lecteur active le Reset de la carte.
- La carte répond en envoyant un message (ATR Answer To Reset) contenant des informations sur le protocole de communication.
- Le lecteur négocie le protocole de communication si la carte permet toute fois une modification des paramètres.
- Le lecteur envoie la première commande à la carte qui l'exécute et renvoie la réponse au lecteur. L'opération de l'envoie des commandes et des réponses est répétée tant que la carte est active.

6- Les commandes de la carte à puce

La majorité des commandes couramment utilisées par les cartes à puce sont définies dans le standard ISO 7815-4 **[jon 02]**:

6-1 Commandes de lecture, d'écriture et de mise à jour

Permettent respectivement la lecture, l'écriture et la mise à jour des données dans les fichiers élémentaires de travail selon des conditions d'accès spécifiques : seuls les utilisateurs autorisés ont la permission de lire et d'écrire sur ces fichiers.

Les commandes de lecture et d'écriture ou de mise à jour sur ces fichiers différent selon leur structure interne, en effet, READ BINARY, WRITE BINARY et UPDATE BINARY sont des commandes utilisées pour accéder aux fichiers ayant une structure transparente, quant aux commandes READ RECORD, WRITE RECORD et UPDATE RECORD, sont utilisées pour accéder aux fichiers structurés en enregistrements.

6-2 Commandes de recherche

Les commandes SEARCH RECORD et SEARCH BINARY sont utilisées respectivement pour rechercher une donnée dans un fichier structuré en enregistrements ou dans un fichier transparent.

6-3 Commandes de gestion de la sécurité

Les cartes à puce peuvent être utilisées pour authentifier des individus par l'échange d'une information secrète qui est connue seulement de l'utilisateur et de la carte (PIN par exemple).

La carte à puce reçoit le PIN par la commande VERIFY PIN, une comparaison est effectuée entre le pin reçu et le pin sauvegardé au niveau de la carte.

- La commande CHANGE PIN permet de modifier le PIN. Cette commande n'est pas autorisée dans le cas où le PIN est bloqué.
- La commande UNBLOCK PIN permet de débloquer le PIN, cette commande assigne une nouvelle valeur au PIN et remet à zéro le nombre d'essais du code PIN.
- La commande INTERNAL AUTHENTFICATION : Permet l'authentification de la carte vis-à-vis de l'application.
- La commande EXTERNAL AUTHENTICATE : permet d'authentifier l'application pour que le terminal puisse accéder à des données sensibles de la carte.

6-4 Commandes de gestion des fichiers

Les systèmes d'exploitation des cartes autorisent diverses opérations de gestion des fichiers :

- La commande CREATE FILE permet la création des fichiers EF et DF.
- Après que le fichier ait été créé, il peut être sélectionné par l'utilisation de la commande SELECT FILE on aura ainsi un accès à ce fichier.

- Les commandes DEACTIVATE FILE sont utilisées pour désactiver un fichier, lorsqu'un fichier est désactivé, toute opération de lecture ou d'écriture est interdite, seule la sélection du fichier est autorisée.
- La commande DELETE FILE permet la suppression d'un fichier de la carte.

7- La sécurité dans les cartes à puce

La sécurité est la principale qualité de la carte à puce. En effet, celle-ci offre un très haut niveau de sécurité. C'est d'ailleurs pour cette raison qu'elle a été choisie pour des applications de haute sécurité telles que les transactions bancaires. Cette sécurité accrue est rendue possible grâce à un ensemble de techniques variées.

7-1 La sécurité au niveau physique

Les cartes à puce disposent d'un bloc de sécurité qui vérifie que celles-ci sont utilisées dans des conditions normales. Ce bloc intègre des systèmes de détection de voltage, et de température. Par exemple, jadis, il était possible de baisser le voltage d'alimentation de la puce à 3,5 volts, ce qui autorisait un nombre infini d'essais du code au lieu des trois essais habituels. Bien évidemment, cette faille a depuis été corrigée par l'apport d'un capteur **[jer 00]**.

7-2 Les droits d'accès

L'accès à un fichier ne peut être effectué que si les conditions d'accès associées à ce fichier ont été vérifiées.

7-3 Le PIN (Personal Identifier Number)

Le système d'exploitation de la carte effectue une identification du porteur de la carte grâce au PIN. Le PIN est un code confidentiel destiné à authentifier le propriétaire d'une carte. La carte à puce contient deux codes PIN's : un PIN utilisateur et un PIN de déblocage.
Si l'utilisateur se trompe un certain nombre de fois dans la saisie de son code PIN, alors celui-ci est bloqué. A ce moment-là, tous les fichiers nécessitant le code PIN vont être inaccessibles. Pour pallier à cela, il faut saisir le code PIN de déblocage, mais si l'utilisateur se trompe plusieurs fois dans la saisie, il peut bloquer le code PIN de déblocage.
La mise en place du dispositif de blocage et déblocage du code PIN nécessite un compteur pour chaque code PIN.

Trois états sont possibles pour le code PIN :

- Le PIN a été correctement présenté : tous les fichiers qui ont comme condition d'accès la présentation de ce code PIN peuvent être activés. A chaque fois que le code PIN est présenté correctement, le compteur PIN est remis à sa valeur maximale de nombres d'essais, 3 par exemple.
- Le PIN a été incorrectement présenté : le compteur PIN est décrémenté d'une unité à chaque essai infructueux. Tous les fichiers ou les fonctions qui nécessitent le code PIN ne sont pas accessibles. Si le compteur PIN atteint zéro, le PIN est bloqué.
- Le PIN est bloqué : tous les fichiers ou fonctions nécessitant le PIN sont bloqués, y compris la fonction demandant la présentation du code PIN. La fonction demandant la présentation du code PIN de déblocage est activée. Si la présentation du PIN de déblocage est incorrecte, le compteur d'essai pour ce code PIN se décrémente et s'il atteint zéro, le code PIN de déblocage est bloqué. A ce moment-là, le code PIN de l'utilisateur ne pourra jamais être redébloqué.

7-4 La cryptographie

La cryptographie consiste à chiffrer (coder) et déchiffrer les messages échangés entre un émetteur et un récepteur. Un système cryptographique basé sur les cartes à puce utilise un algorithme de cryptage associé à une clé pour coder les données sauvegardées au niveau de la carte. Le décryptage ne peut être effectué que par un algorithme de décodage associé à une clé de décryptage.

Actuellement la majorité des cartes disposent d'un processeur de cryptographie qui exécute des algorithmes de cryptage tels que: RSA, DES et autres.

8- Avantages des cartes à puce

Les principaux avantages de la carte à puce sont la sécurité, le coût, la facilité d'utilisation et la personnalisation aussi bien pour le porteur de carte que pour le fournisseur de carte (ex. par embossage ou par personnalisation graphique). La carte à puce est résistante aux attaques grâce aux différents modes de sécurité vus précédemment.

La taille de la carte à puce permet sa portabilité et sa mobilité.

La technologie des cartes évolue très vite car ses composants suivent l'évolution générale de l'électronique: puissance des microprocesseurs (2005: 32 bits à plus de 10 MHz), capacité de

mémoire (plus de 256 ko d'EEPROM, 512 Ko de mémoire morte) et diversité des types de mémoire (mémoire Falsh de plusieurs Mo dès 2005) **[wol 03]**.

9- Applications des cartes à puce

La carte à puce est présente dans bon nombre d'applications, en voici quelques unes: **[chr 00]**

9-1 Cartes d'identification

Ces cartes sont utilisées pour identifier un individu, et/ou pour sécuriser l'accès aux informations personnelles sensibles. En voici quelques exemples:

- ***Carte d'identité*** : elle a fait son apparition en Finlande en décembre 1999, elle comporte les informations habituellement trouvées sur une pièce d'identité.
- ***Carte de sécurité sociale :*** diffusée en France sous le nom de « Carte Vitale », elle contient les informations concernant l'assuré social que l'on peut trouver sur une carte de sécurité sociale classique.
- ***Carte médicale :*** Elle contient les antécédents médicaux du malade. Ceci aide le médecin à retracer le passé médical de son patient et donc à faire un meilleur diagnostique. Les cartes de vaccination « Vaccicarte » sont un exemple typique de carte médicale.
- ***Permis de conduire :*** en plus des informations personnelles, il contient les points restants ainsi que la liste des procès verbaux infligés au conducteur. Cela permet de vérifier que ces contraventions ont bien été acquittées.
- ***Carte d'étudiant*** : permet aux étudiants de passer des examens, d'emprunter des ouvrages à la bibliothèque, d'accéder aux salles machines. Elle est utilisée dans de nombreuses universités telles que l'université polytechnique de Hong-Kong.
- ***Carte d'identification informatique*** : permet à un utilisateur de s'identifier pour une session de travail (login) après avoir inséré la carte dans le terminal et tapé un mot de passe. La carte peut aussi stocker le profil de l'utilisateur (paramètres de configuration, données personnelles,...), ce qui lui permet de travailler dans son environnement personnel depuis n'importe quel terminal.
- ***Carte d'accès :*** permet d'accéder à des locaux (parking, bureau ...). Elle peut aussi servir à contrôler les heures d'arrivée et de départ du lieu de travail.

- ***Carte bancaire*** : permet d'effectuer des achats par correspondance dans le monde entier (Carte Bleue Nationale, Visa, etc.). Elle sert uniquement à identifier le client, avant que la station n'envoie à la banque l'ordre de débit.
- ***Carte SIM :*** La carte « SIM » (Subscriber Identity Module) est utilisée dans les téléphones « GSM » (Global System for Mobile communications) pour vérifier l'identité de l'utilisateur. L'utilisation du téléphone ne peut se faire sans la carte. La carte peut aussi servir à stocker des données, comme le répertoire téléphonique de l'utilisateur.

9-2 Cartes à valeur monétaire

Ces cartes permettent de stocker et d'utiliser des unités à valeur marchande. Ces unités sont généralement achetées et stockées dans la carte. L'accès au service est limité par le nombre d'unités achetées jusqu'à un éventuel rechargement de la carte.

- ***Porte-monnaie électronique :*** Il permet de stocker une faible somme d'argent sous forme numérique.
- ***Carte téléphonique :*** répandue dans le monde entier, elle contient un certain nombre d'unités téléphoniques, que l'utilisateur consomme en utilisant les téléphones publics. On citera par exemple la Télécarte de France Télécom, la carte ORIA (Algérie) et la carte Algérie Télécom.

10- Marché des cartes à puce

En 2004, selon l'étude Gartner (Market Share: Chip Card and Semiconductor Vendors, Worldwide, 2004. Publié le: 13 mai 2005), le marché des cartes à puce, cartes à microprocesseur et cartes à mémoire reste dominé par les quatre acteurs de dimension mondiale que sont "Gemplus", "Axalto", "Giesecke & Devrient" et "Oberthur CardSystems" avec des parts de marché respectives de 27,1 %, 20,4 %, 13,8 % et 6,2 %. Le reste du marché est composé d'acteurs locaux de dimensions plus modestes **[obe 05]**. Voici deux tableaux de quelques cartes et lecteurs qui existent sur le marché.

Tableau IV.1 Exemples de cartes à puce existantes sur le marché

Nom de la carte	Fabricant	Caractéristiques
GemXpresso Pro	Gemplus	EEPROM : 4K, Processeur 32-bit, Supporte la norme ISO 7816 1-2-3, EMV 2000
Gemsafe16000	Gemplus	EEPROM : 16K, Supporte la norme ISO 7816-1/2/3/4
SLE5528 Secure Memory SmartCard	ShenZhen	EEPROM : 8K Supporte la norme ISO 7816
Crypto flex E-Gate Card	Axalto	EEPROM : 32K, Supporte la norme ISO 7816. Algorithmes de cryptages implémentés RSA, Triple-DES, DES
CRYPTOFLEX	SCHLUMBERGER	EEPROM : 8K, Algorithmes de cryptages implémentés : RSA, Triple-DES, DES
ACOSI	ACS	EEPROM : 1K, processeur 8bits
ASECARD CRYPTO	ATHENA	EEPROM : 64K, Supporte la norme ISO 7816-4, 8, 9. Utilisée dans les applications nécessitant une très haute sécurité, les algorithmes de cryptages implémentés sont RSA, Triple-DES, DES

Tableau IV.2 Exemples de quelques lecteurs de carte existants sur le marché

Nom du lecteur	Fabricant	Description
Reflex 60	Schlumberger	ISO 7816 compatible
Reflex 72	Schlumberger	ISO 7816 compatible, PC/SC supporté
ACR 10	ACS	Lit seulement les cartes mémoires
ACR 20	ACS	ISO 7816 compatible, PC/SC supporté
Gem 410X	Gemplus	ISO 7816 compatible, PC/SC supporté

Dans ce chapitre, nous avons abordé différents aspects de la carte à puce. Ce support de stockage est caractérisé par une sécurité accrue, de ce fait, la carte est utilisée dans divers contextes notamment la biométrie. Dans le chapitre suivant, nous décrirons les différentes architectures des systèmes biométriques utilisant la carte à puce.

Chapitre V

Utilisation de la carte à puce dans la biométrie

Le couplage de la biométrie et de la carte à puce permet d'être sûr que l'on est bien le propriétaire légitime de cette carte et des informations qu'elle contient, surtout que les cartes à puce sont des produits de plus en plus fiable pour sécuriser des informations grâce au code PIN ainsi qu'au cryptage. Ce type de système contourne le stockage de données personnelles sur une base de données, vivement critiqué par les organismes de protection des libertés individuelles **[vin 05]**, en faisant appel à un stockage sur une carte à puce. Chaque individu devient ainsi l'unique détenteur des informations sensibles le concernant.

Ces systèmes sont très performants car ils font appel à trois facteurs qui sont :

- quelque chose que vous connaissez (code PIN)
- quelque chose que vous possédez (carte à puce)
- quelque chose qui vous identifie (identification biométrique)

1-Classification des systèmes biométriques utilisant la carte à puce

Les systèmes biométriques utilisant une carte à puce peuvent être classés comme suit **[cla07]**:

1-1 **Les systèmes Match off Card** (ou **Template On Card [zel 07]**) : Les références biométriques (modèle biométrique) sont stockées dans la carte à puce. L'authentification ce fait à travers un terminal externe. La décision est prise par ce terminal externe, qui a accès aux références biométriques, ce qui les expose au monde extérieur.

1-2 **Les systèmes Match On Card** : L'identification utilise toujours un terminal externe pour acquérir la donnée biométrique. Mais cette fois-ci, c'est la carte à puce qui va comparer les données, et prendre la décision. Les références biométriques ne sortent donc pas de la puce, et ne sont donc pas exposées au monde extérieur.

Cette technologie garantit un respect absolu des données privées : aucune information biométrique ne peut être extraite de la carte à puce interdisant ainsi un usage frauduleux de cette dernière. Le possesseur de la carte à puce reste le seul maître de ses informations **[id3]**.

1-3 **Les systèmes Partial Match On Card** : Les cartes à puce ayant de faibles capacités de calcul, la solution Match On Card devient difficilement utilisable avec des paramètres biométriques de grande taille, qui offrent une sécurité accrue. Le partial Match On Card permet de laisser le terminal externe réaliser les calculs lourds et complexes, tout en laissant la décision à la carte à puce.